J. reine angew. Math., Ahead of Print
DOI 10.1515/crelle-2015-0041

Journal für die reine und angewandte Mathematik

Local zero estimates and effective division in rings of algebraic power series

By *Guillaume Rond* at Marseille

Abstract. We give a necessary condition for algebraicity of finite modules over the ring of formal power series. This condition is given in terms of local zero estimates. In fact, we show that this condition is also sufficient when the module is a ring with some additional properties. To prove this result we show an effective Weierstrass Division Theorem and an effective solution to the Ideal Membership Problem in rings of algebraic power series. Finally, we apply these results to prove a gap theorem for power series which are remainders of the Grauert–Hironaka–Galligo Division Theorem.

Contents

The author was partially supported by ANR projects STAAVF (ANR-2011 BS01 009) and SUSI (ANR-12-JS01-0002-01).

1. Introduction

The goal of this paper is to give a necessary condition in term of local zero estimates for a finite module defined over the ring of formal power series to be the completion of a module defined over the ring of algebraic power series. Finding conditions for the algebraicity of such modules is a long-standing problem (see [28] or [3] for instance). Let us recall that an algebraic power series over a field $\mathbb{k}$ in the variables $x_1, \dots, x_n$ is a formal power series $f(x) \in \mathbb{k}[\![x]\!]$ (from now on we denote the tuple $(x_1, \dots, x_n)$ by x) such that

$$P(x, f(x)) = 0$$

for a non-zero polynomial $P(x, T) \in \mathbb{k}[x, T]$. The set of algebraic power series is a subring of $\mathbb{k}[\![x]\!]$ denoted by $\mathbb{k}\langle x\rangle$.

For an algebraic power series f, we define the height of f, $\mathrm{H}(f)$, to be the maximum of the degrees of the coefficients of the minimal polynomial of f (see Definition 3.2). If f is a polynomial, its height is equal to its degree as a polynomial.

Let M be a $\mathbb{k}[\![x]\!]$-module. The order function ord_M is defined as follows:

$$\mathrm{ord}_M(m) := \sup\{c \in \mathbb{N} : m \in (x)^c M\} \quad \text{for all } m \in M \setminus \{0\}.$$

Let $p \in \mathbb{k}[x]^s$ (resp. $\mathbb{k}\langle x\rangle^s$). The *degree* (resp. *height*) of p is the maximum of the degrees (resp. heights) of its components. Then our main result is the following:

Theorem 1.1. *Let $\mathbb{k}$ be any field and let M be a finite $\mathbb{k}[\![x]\!]$-module,*

$$M = \mathbb{k}[\![x]\!]^s/N$$

for some integer s and some $\mathbb{k}[\![x]\!]$-submodule N of $\mathbb{k}[\![x]\!]^s$. Let us assume that the submodule N is generated by a $\mathbb{k}\langle x\rangle$-submodule of $\mathbb{k}\langle x\rangle^s$. Then there exists a function

$$C : \mathbb{N} \to \mathbb{R}_{>0}$$

such that

$$\mathrm{ord}_M(f) \leq C(\mathrm{Deg}(f)) \cdot \mathrm{H}(f) \quad \textit{for all } f \in \mathbb{k}\langle x\rangle^s \setminus N. \tag{1.1}$$

Here $\mathrm{Deg}(f)$ *denotes the degree of the field extension* $\mathbb{k}(x) \to \mathbb{k}(x, f)$*. Moreover, when we have* $\mathrm{char}(\mathbb{k}) = 0$*, then C depends polynomially on* $\mathrm{Deg}(f)$.

Corollary 1.2. *With the notations of Theorem* 1.1*, let us assume that N is generated by a $\mathbb{k}\langle x\rangle$-submodule of $\mathbb{k}\langle x\rangle^s$. Then there exists a constant $C' > 0$ such that*

$$\mathrm{ord}_M(p) \leq C' \cdot \deg(p) \quad \textit{for all } p \in \mathbb{k}[x]^s \setminus N. \tag{1.2}$$

Proof. Indeed, for a vector of polynomials $p \in \mathbb{k}[x]^s$ we have

$$\mathrm{Deg}(p) = 1 \quad \text{and} \quad \mathrm{H}(p) = \deg(p),$$

so the inequality is satisfied with $C' = C(1)$ where C is the function of Theorem 1.1. □

We also prove a partial converse of Corollary 1.2:

Theorem 1.3. *Let R be a ring of the form $\Bbbk[\![x]\!]/I$ for some ideal I such that*

$$I = P_1^{n_1} \cap \cdots \cap P_l^{n_l}$$

where the P_i are prime ideals with $\operatorname{ht}(P_i) = \operatorname{ht}(P_j)$ for all i and j, and the n_i are positive integers. If there exists a constant $C > 0$ such that

$$\operatorname{ord}_R(p) \leq C \cdot \deg(p) \quad \text{for all } p \in \Bbbk[x] \setminus I,$$

then I is generated by algebraic power series.

Remark 1.4. We remark that the hypothesis of Theorem 1.3 are satisfied for a principal ideal I. In particular, Theorems 1.1 and 1.3 provide a criterion for a principal ideal to be generated by an algebraic power series.

Remark 1.5. We will see in Section 9 that Theorem 1.3 is not true in general.

These two results are generalizations of previous results of S. Izumi (see [15–17] where he proved Corollary 1.2 when $\operatorname{char}(\Bbbk) = 0$, $s = 1$ and N is a prime ideal of $\Bbbk[\![x]\!]$) and Theorem 1.3 when I is prime and $\operatorname{char}(\Bbbk) = 0$.

The proof of Theorem 1.3 uses Hilbert–Samuel functions and is inspired by the proof given in [15]. The proof of Theorem 1.1 is more difficult and is the main subject of this paper. In fact, the first difficulty occurs already when $s = 1$ and N is an ideal of $\Bbbk[\![x]\!]$ which is not prime. Corollary 1.2 in the case of a prime ideal has been proven by S. Izumi in [16] in the complex analytic case using resolution of singularities of Moishezon spaces and then for any field of characteristic zero using basic field theory in [17]. But when N is not prime, his proof does not adapt at all and the general case cannot be reduced to the case proven by S. Izumi.

The proof of Theorem 1.1 that we give here is done by induction on s and n. The induction steps require two effective division results in the rings of algebraic power series which may be of general interest. These are the following ones:

(i) In the case of the Weierstrass division of an algebraic power series f by another algebraic power series it is proven by J.-P. Lafon that the remainder and the quotient of the division are algebraic power series [20]. The problem solved here is to bound the complexity of the division, i.e. bound the complexity of the quotient and the remainder of the division in function of the complexity of the input data. This is Theorem 4.5 and is the main tool to solve the next division problem. Let us mention that this problem is partially solved in [4, Section 4, see Theorem 4.6].

(ii) Bounding the complexity of the Ideal Membership Problem in the ring of algebraic power series, i.e. if an algebraic power series f is in the ideal generated by algebraic power series $g_1, \dots, g_p$, bound the complexity of algebraic power series $a_1, \dots, a_p$ such that

$$f = a_1 g_1 + \cdots + a_p g_p.$$

This is Theorem 6.1.

The complexity invariants associated to an algebraic power series f are its degree and its height. The first one is the degree of the field extension $\Bbbk(x) \to \Bbbk(x, f)$ and the second one has been defined above. In particular, we will prove that the previous complexity problems admit a solution which is linear with respect to the height of f (but it is not linear which respect to the other data). This is exactly what we need to prove Theorem 1.1.

Finally, we apply our main theorem to give a partial answer to a question of H. Hironaka. When $f, g_1, \dots, g_s$ are formal power series, we can write

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

where the non-zero monomials in the expansion of r are not divisible by the initial terms of the g_i (see Section 10 for precise definitions). When the power series f and the g_i are convergent, then r is also convergent. This result has been proven by H. Grauert in order to study versal deformations of isolated singularities of analytic hypersurfaces [9] and then by H. Hironaka to study resolution of singularities [12]. But when f and the g_i are algebraic power series, then r is not an algebraic power series in general and H. Hironaka raised the problem of characterizing such power series r (see [13]). In this case we prove that such power series r are not too transcendental (see Theorem 12.1). More precisely, if we write r as $r = \sum_{k=0}^{\infty} r_{n(k)}$ where $r_{n(k)}$ is a non-zero homogeneous polynomial of degree $n(k)$ and the sequence $(n(k))_k$ is strictly increasing, we show that

$$\limsup_{k\to\infty} \frac{n(k+1)}{n(k)} < \infty.$$

Let us mention that this division problem appears also in combinatorics: the generating series of walks confined in the first quadrant are solutions of such a division but are neither algebraic nor D-finite in general (see [10] or [19]).

Let us mention that the kind of estimates given in Corollary 1.2, i.e. estimates of the form

$$\operatorname{ord}_M p \le \gamma(\deg(p))$$

where $\gamma : \mathbb{N} \to \mathbb{N}$ is an increasing function, $s = 1$ and N is an ideal of analytic functions are called *zero estimates* in the literature. Finding such estimates for particular classes of functions is an important subject of research in transcendence theory, in particular when the ideal N is generated by analytic functions of the form

$$x_k - f_k(x_1, \dots, x_{k-1}), \dots, x_n - f_n(x_1, \dots, x_{k-1})$$

for some $k < n$ and $f_k, \dots, f_n$ solutions of differential equations (see [6, 23, 31] for instance) or functional equations (q-difference equations or Mahler functions – see [24] for instance).

We should also mention that the complexity of the Weierstrass division for restricted power series defined over the ring of p-adic integers which are algebraic over $\mathbb{Q}[x]$ has been solved in [4]. The complexity of the Ideal Membership Problem is also solved in this situation. In this case the definition of the height of an algebraic power series is more complicated.

The paper is organized as follows: after giving the list of notations used in the paper in Section 2, we define the height of an algebraic power series in Section 3 and give the first properties of it. In Section 4 we prove an effective Weierstrass Division Theorem (see Theorem 4.5). In Section 5 we give some results about the Ideal Membership Problem in rings which are localizations of rings of polynomials (see Theorem 5.2 and Proposition 5.3) and in Section 6 we give an effective Ideal Membership theorem for algebraic power series rings (see Theorem 6.1). Then Section 7 is devoted to the proof of Theorem 1.1 and Section 8 to the proof of Theorem 1.3. In Section 9 is given an example showing that the hypothesis of Theorem 1.3 cannot being relaxed. The next three sections concern the Grauert–Hironaka–Galligo Division Theorem: in Section 10 we state this theorem and give the example of Gabber–Kashiwara showing that the remainder of such division of an algebraic power series by another one is not algebraic in general. We show in Section 11 that the example of Gabber–Kashiwara is generic in some sense, i.e. in general the division of an algebraic power series by another one does not have an algebraic remainder (see Proposition 11.3). Finally, we prove in Section 12 our gap theorem for remainders of such a division (see Theorem 12.1).

Remark 1.6. We show in Example 10.4 that the bound in Corollary 1.2 is sharp. For Theorem 1.1 it is not clear if such bound is sharp. Indeed, let f be an algebraic power series and $M = \Bbbk[\![x]\!]/I$ where I is an ideal generated by algebraic power series. Let

$$a_d(x)T^d + a_{d-1}(x)T^{d-1} + \cdots + a_0(x)$$

be the minimal polynomial of f. Then we have

$$(a_d f^{d-1} + a_{d-1} f^{d-2} + \cdots + a_1) f = -a_0.$$

We set $g := a_d f^{d-1} + a_{d-1} f^{d-2} + \cdots + a_1$. If $a_0 \notin I$, then

$$\operatorname{ord}_M(f) \leq \operatorname{ord}_M(gf) = \operatorname{ord}_M(a_0) \leq C\,\mathrm{H}(f)$$

where C is the constant of Corollary 1.2 since $a_0(x)$ is a polynomial of degree $\leq \mathrm{H}(f)$. This shows that in general the function C of Theorem 1.1 can be chosen to be independent of $\mathrm{Deg}(f)$ except maybe when $a_0(x) \equiv 0$ in M.

Acknowledgement. The author would like to thank Paco Castro-Jiménez and Herwig Hauser for the discussions they had about the Weierstrass Division Theorem in the algebraic case. He would like also thank Matthias Aschenbrenner for communicating the reference [4].

The author is really grateful to the referee for their helpful suggestions for improving the readability of the article.

2. Notations

In the whole paper $\Bbbk$ denotes a field of any characteristic. Let n be a non-negative integer and set

$$x := (x_1, \dots, x_n) \quad \text{and} \quad x' := (x_1, \dots, x_{n-1}).$$

The ring of polynomials in n variables over $\Bbbk$ will be denoted by $\Bbbk[x]$ and its field of fractions by $\Bbbk(x)$. The ring of formal power series in n variables over $\Bbbk$ is denoted by $\Bbbk[\![x]\!]$ and its field of fractions by $\Bbbk((x))$. An algebraic power series is a power series $f(x) \in \Bbbk[\![x]\!]$ such that

$$P(x, f(x)) = 0$$

for some non-zero polynomial $P(x,T) \in \Bbbk[x,T]$ where T is a single indeterminate. The set of algebraic power series is a local subring of $\Bbbk[\![x]\!]$ denoted by $\Bbbk\langle x\rangle$.

When $\mathbb{k}$ is a valued field, we denote by $\mathbb{k}\{x\}$ the ring of convergent power series in n variables over $\mathbb{k}$. We have

$$\mathbb{k}[x] \subset \mathbb{k}\langle x\rangle \subset \mathbb{k}\{x\} \subset \mathbb{k}[\![x]\!].$$

We will denote by $\mathbb{K}_{n-1}$ an algebraic closure of $\mathbb{k}((x')) = \mathbb{k}((x_1, \ldots, x_{n-1}))$.

For a polynomial $p \in \mathbb{k}[x]$ we denote by $\deg(p)$ its total degree with respect to the variables $x_1, \ldots, x_n$. If $y := (y_1, \ldots, y_m)$ is a new set of indeterminates and $p \in \mathbb{k}[x, y]$, we denote by

$$\deg_{(y_1,\ldots,y_m)}(p)$$

the degree of p seen as a polynomial in $\mathbb{K}[y]$ where $\mathbb{K} := \mathbb{k}(x)$. When $p \in \mathbb{k}[x]^s$ for some s, we denote by $\deg(p)$ the maximum of the degrees of the components of p.

For an algebraic power series $f \in \mathbb{k}\langle x\rangle$, the height of f is the maximum of the degrees of the coefficients of the minimal polynomial of f (see Definition 3.2). The height of a vector of algebraic power series is the maximum of the heights of its components.

When $(A, \mathfrak{m})$ is a local ring, we set

$$\mathrm{ord}_A(x) := \sup\{k \in \mathbb{N} : x \in \mathfrak{m}^k\} \in \mathbb{N} \cup \{\infty\} \quad \text{for all } x \in A.$$

If M is a finite A-module, we set

$$\mathrm{ord}_M(m) := \sup\{k \in \mathbb{N} : m \in \mathfrak{m}^k M\} \quad \text{for all } m \in M.$$

When $A = \mathbb{k}[\![x]\!]$, we write ord instead of $\mathrm{ord}_{\mathbb{k}[\![x]\!]}$. For an ideal of $\mathbb{k}[\![x]\!]$ generated by $g_1, \ldots, g_p$ we define

$$\mathrm{ord}_{g_1,\ldots,g_p}(f) := \sup\{k \in \mathbb{N} : f \in (g_1, \ldots, g_p)^k\} \in \mathbb{N} \cup \{\infty\}.$$

3. Height and degree of algebraic power series

Definition 3.1. Let α be an element of an algebraic closure of $\mathbb{k}(x)$ (for example an algebraic power series). The morphism $\varphi : \mathbb{k}[x, T] \to \mathbb{k}(x, \alpha)$ defined by sending every polynomial $P(x, T)$ onto $P(x, \alpha)$ is not injective and its kernel is a prime ideal $\mathfrak{p}$ of $\mathbb{k}[x, T]$. If $\mathrm{ht}(\mathfrak{p}) \geq 2$, then $\mathfrak{p} \cap \mathbb{k}[x] \neq (0)$ and there would exist a non-zero polynomial $P(x) \in \mathbb{k}[x]$ whose image by φ is zero which is not possible. Thus $\mathrm{ht}(\mathfrak{p}) = 1$ and $\mathfrak{p}$ is a principal ideal. If $P(x, T)$ is a generator of $\mathfrak{p}$, then any other generator of this ideal is equal to $P(x, T)$ times a non-zero element of $\mathbb{k}$. Such a generator is called a minimal polynomial of α. By abuse of language we will often refer to such an element by *the* minimal polynomial of α.

Definition 3.2 ([1]). Let $P(x, T) \in \mathbb{k}[x, T]$. The height of P is the maximum of the degrees of the coefficients of $P(x, T)$ seen as a polynomial in T.

Let α be an algebraic element over $\mathbb{k}(x)$. The height of α is the height of its minimal polynomial and is denoted by $\mathrm{H}(\alpha)$. Its degree is the degree of its minimal polynomial or, equivalently, the degree of the field extension $\mathbb{k}(x) \to \mathbb{k}(x, \alpha)$ and is denoted by $\mathrm{Deg}(\alpha)$.

When $\alpha = (\alpha_1, \ldots, \alpha_m)$ is a vector of algebraic elements over $\mathbb{k}(x)$, the height of α, $\mathrm{H}(\alpha)$, is the maximum of the heights of the components of α and the degree of α, $\mathrm{Deg}(\alpha)$, is the degree of the field extension $\mathbb{k}(x) \to \mathbb{k}(x, \alpha_1, \ldots, \alpha_m)$.

Remark 3.3. If $P(x,T) \in \mathbb{k}[x,T]$ is the minimal polynomial of an algebraic element α, then we have $\mathrm{H}(\alpha) = \deg_x(P)$ and $\mathrm{Deg}(\alpha) = \deg_T(P)$. In particular, for $Q(x,T) \in \mathbb{k}[x,T]$ with $Q(\alpha) = 0$, P divides Q hence we have $\mathrm{H}(\alpha) \leq \deg_x(Q)$ and $\mathrm{Deg}(\alpha) \leq \deg_T(Q)$.

Example 3.4. Let f be a polynomial in $\mathbb{k}[x]$. Then $\mathrm{H}(f) = \deg(f)$ and $\mathrm{Deg}(f) = 1$ since the minimal polynomial of f is $T - f$.

Let f/g be a rational function in $\mathbb{k}(x)$. Then we have $\mathrm{H}(f/g) = \max\{\deg(f), \deg(g)\}$ and $\mathrm{Deg}(f/g) = 1$ since the minimal polynomial of f/g is $gT - f$.

If α is algebraic over $\mathbb{k}(x)$, then $1/\alpha$ also and $\mathrm{H}(1/\alpha) = \mathrm{H}(\alpha)$ and $\mathrm{Deg}(1/\alpha) = \mathrm{Deg}(\alpha)$. If $f(x)$ is an algebraic power series and $M \in \mathrm{Gl}_n(\mathbb{k})$, then $f(Mx)$ is also algebraic and we have $\mathrm{H}(f(Mx)) = \mathrm{H}(f(x))$ and $\mathrm{Deg}(f(Mx)) = \mathrm{Deg}(f(x))$.

Remark 3.5. There exists another measure of the complexity of an algebraic element α over $\mathbb{k}(x)$ (and so, in particular, of an algebraic power series). This one is defined to be the total degree of the minimal polynomial of α and denoted by $\mathrm{co}(\alpha)$ (cf. [27] or [2]). Thus we have

$$\frac{\mathrm{H}(\alpha) + \mathrm{Deg}(\alpha)}{2} \leq \max\{\mathrm{H}(\alpha), \mathrm{Deg}(\alpha)\} \leq \mathrm{co}(\alpha) \leq \mathrm{H}(\alpha) + \mathrm{Deg}(\alpha).$$

This shows that $\mathrm{co}(\alpha)$ is equivalent to $\mathrm{H}(\alpha) + \mathrm{Deg}(\alpha)$. Moreover, these bounds are sharp. Indeed, let $P_n(T) := (1 + x^n)T^n - 1$ (where x is a single variable and $n \in \mathbb{N}$ is not a multiple of the characteristic of $\mathbb{k}$). Then $P_n(T)$ is irreducible and has a root f_n in $\mathbb{k}\langle x\rangle$. Thus

$$\mathrm{H}(f_n) = \mathrm{Deg}(f_n) = n \quad \text{and} \quad \mathrm{co}(f_n) = 2n.$$

On the other hand the polynomial $Q_n(T) := T^n - (1 + x^n)$ is irreducible and has a root g_n in $\mathbb{k}\langle x\rangle$. Thus $\mathrm{H}(g_n) = \mathrm{Deg}(g_n) = \mathrm{co}(g_n) = n$.

For an algebraic power series f we choose to use $\mathrm{H}(f)$ instead of $\mathrm{co}(f)$ since the complexity of the Weierstrass Division Theorem is linear in $\mathrm{H}(f)$ but not in $\mathrm{co}(f)$ (it is not linear in $\mathrm{Deg}(f)$ – see Theorem 4.5). Indeed, we need to prove the existence of a bound in Theorem 1.1 which is linear in $\mathrm{H}(f)$.

Lemma 3.6 ([1, Lemma 4.1]). *Let $\alpha_1, \dots, \alpha_p$ be algebraic elements over $\mathbb{k}(x)$ and let $a_1, \dots, a_p \in \mathbb{k}(x)$. Then we have:*

(i) $\mathrm{Deg}(a_1\alpha_1 + \dots + a_p\alpha_p) \leq \mathrm{Deg}(\alpha_1)\cdots\mathrm{Deg}(\alpha_p)$,

(ii) $\mathrm{H}(a_1\alpha_1 \dots + a_p\alpha_p) \leq p \cdot \mathrm{Deg}(\alpha_1)\cdots\mathrm{Deg}(\alpha_p)(\max_i\{\mathrm{H}(\alpha_i)\} + \max_j\{\mathrm{H}(a_j)\})$,

(iii) $\mathrm{H}(a_1 + \alpha_1) \leq \mathrm{H}(\alpha_1) + \mathrm{Deg}(\alpha_1) \cdot \mathrm{H}(a_1)$,

(iv) $\mathrm{H}(a_1\alpha_1) \leq \mathrm{H}(\alpha_1) + \mathrm{Deg}(\alpha_1) \cdot \mathrm{H}(a_1)$,

(v) $\mathrm{Deg}(\alpha_1 \cdots \alpha_p) \leq \mathrm{Deg}(\alpha_1)\cdots\mathrm{Deg}(\alpha_p)$,

(vi) $\mathrm{H}(\alpha_1 \cdots \alpha_p) \leq p \cdot \mathrm{Deg}(\alpha_1)\cdots\mathrm{Deg}(\alpha_p)\max_i\{\mathrm{H}(\alpha_i)\}$.

Proof. All these inequalities are proven in [1] except the third and the fourth ones that we prove here. Let us begin with the third one. Let $P(x,T)$ be the minimal polynomial of α_1 and let us write $a_1(x) = b(x)/c(x)$ for some polynomials $b(x)$ and $c(x)$. Then

$$Q(x,T) := c(x)^{\deg_T(P)} P(x, T - a_1)$$

is a polynomial vanishing at $\alpha_1 + a_1$. Thus

$$\mathrm{H}(\alpha_1 + a_1) \leq \deg_x(Q(x,T)) \leq \mathrm{H}(\alpha_1) + \mathrm{Deg}(\alpha_1)\,\mathrm{H}(a_1)$$

since $\mathrm{Deg}(\alpha_1) = \deg_T(P)$ and $\mathrm{H}(a_1) \geq \max\{\deg(b(x)), \deg(c(x))\}$.

To prove inequality (iv), let $P(x,T)$, b, c as above. Then $b^{\deg_T(P)} P(x, c/bT)$ is a polynomial vanishing at $a_1\alpha_1$. So

$$\mathrm{H}(a_1\alpha_1) \leq \mathrm{Deg}(\alpha_1) \cdot \mathrm{H}(a_1) + \mathrm{H}(\alpha_1). \qquad \square$$

Lemma 3.7. *For an algebraic power series f we have*

$$\mathrm{ord}(f) \leq \mathrm{H}(f).$$

Moreover, for any integer $1 \leq i \leq n$ we have

$$\mathrm{H}(f(0,\dots,0,x_i,\dots,x_n)) \leq \mathrm{H}(f)$$

and

$$\mathrm{ord}_{x_i,\dots,x_n}(f(0,\dots,0,x_i,\dots,x_n)) \leq \mathrm{H}(f).$$

Proof. Let $P(T) = a_dT^d + \cdots + a_1T + a_0$ be the minimal polynomial of f. Since $P(f) = 0$, there are two integers $0 \leq i < j \leq d$ such that $\mathrm{ord}(a_if^i) = \mathrm{ord}(a_jf^j)$. Thus

$$\mathrm{ord}(f) = \frac{\mathrm{ord}(a_i) - \mathrm{ord}(a_j)}{j-i} \leq \mathrm{ord}(a_i) \leq \deg(a_i).$$

This proves the first inequality. The second inequality is proven by noticing that if we have $P(x_1,\dots,x_n, f(x_1,\dots,x_n)) = 0$, then $P(0,x_2,\dots,x_n, f(0,x_2,\dots,x_n)) = 0$. Since P is the minimal polynomial of f, it follows that P is not divisible by x_1, thus

$$P(0,x_2,\dots,x_n,T) \neq 0.$$

This proves that $f(0,x_2,\dots,x_n)$ is an algebraic power series and its minimal polynomial divides $P(0,x_2,\dots,x_n,T)$, hence

$$\mathrm{H}(f(0,x_2,\dots,x_n)) \leq \mathrm{H}(f).$$

The first inequality implies

$$\mathrm{ord}_{x_2,\dots,x_n}(f(0,x_2,\dots,x_n)) \leq \mathrm{H}(f).$$

Hence the last two inequalities are proven by induction on i. $\square$

Remark 3.8. A formal power series f is said to be x_n-regular if $f(0,\dots,0,x_n) \neq 0$. In this case we say that f is x_n-regular of order d if $f(0,\dots,0,x_n)$ is a power series of $\Bbbk[\![x_n]\!]$ of order d.

By the previous lemma, if an algebraic power series f is x_n-regular of order d, then we have $d \leq \mathrm{H}(f)$.

Remark–Definition 3.9. Let $\mathbb{K}_{n-1}$ be an algebraic closure of the field $\Bbbk((x'))$ where $x' := (x_1,\dots,x_{n-1})$. The (x')-valuation $\mathrm{ord}_{x'}$ defined on $\Bbbk((x'))$ extends uniquely to $\mathbb{K}_{n-1}$ and is still denoted by $\mathrm{ord}_{x'}$. The completion of $\mathbb{K}_{n-1}$ for the valuation $\mathrm{ord}_{x'}$ is denoted by $\widehat{\mathbb{K}}_{n-1}$. Let $\alpha \in \widehat{\mathbb{K}}_{n-1}$ such that $\mathrm{ord}_{x'}(\alpha) > 0$ and f be a formal power series. Then $f(x',\alpha)$ is well defined in $\widehat{\mathbb{K}}_{n-1}$. If $f(x',\alpha) = 0$, we call α a *root* of f.

If f is an algebraic power series, $P(x,T)$ is the minimal polynomial of f and α is a root of f, then $P(x',\alpha,0)=0$ thus α is algebraic over $\Bbbk(x')$.

Let f be a formal power series which is x_n-regular of order d. Then, by the Weierstrass Preparation Theorem, there exist a unit v and a Weierstrass polynomial

$$P = x_n^d + a_1(x')x_n^{d-1} + \cdots + a_d(x')$$

such that $f = vP$. The polynomial P is called the *Weierstrass polynomial of* f. Let $\alpha \in \mathbb{K}_{n-1}$ be a root of P. Since $\mathrm{ord}_{x'}(a_i(x')) > 0$ for any i, we have $\mathrm{ord}_{x'}(\alpha) > 0$. Thus $f(x',\alpha)$ and $v(x',\alpha)$ are well defined in $\widehat{\mathbb{K}}_{n-1}$ and $f(x',\alpha)=0$. On the other hand if $\alpha \in \widehat{\mathbb{K}}_{n-1}$ is a root of f, then since $\mathrm{ord}_{x'}(\alpha) > 0$ we have $v(x',\alpha) \neq 0$ in $\widehat{\mathbb{K}}_{n-1}$, thus $P(x',\alpha)=0$. In particular, α is a root of the polynomial P in the usual sense thus $\alpha \in \mathbb{K}_{n-1}$.

This proves that the roots of f are exactly the roots (in the usual sense) of P seen as a polynomial in x_n and are elements of $\mathbb{K}_{n-1}$.

Lemma 3.10. *Let $\alpha \in \mathbb{K}_{n-1}$ be a root of an x_n-regular algebraic power series f. Then α is algebraic over $\Bbbk(x)$ and*

$$\mathrm{H}(\alpha) \leq \mathrm{H}(f) \quad \textit{and} \quad \mathrm{Deg}(\alpha) \leq \mathrm{H}(f).$$

Moreover, if $\alpha_1,\dots,\alpha_d$ are distinct roots of f, then

$$[\Bbbk(x',\alpha_1,\dots,\alpha_d) : \Bbbk(x')] \leq \mathrm{H}(f)!.$$

Proof. Let $P(x,T)$ be the minimal polynomial of f. Since $f(x',\alpha)=0$, we have

$$P(x',\alpha,0)=0.$$

Thus $P(x',T,0)$ is a non-zero polynomial vanishing at α, proving that α is algebraic, and

$$\mathrm{H}(\alpha) \leq \deg_{x'}(P(x',T,0)) \leq \deg_{(x',x_n)}(P(x',x_n,T)) = \mathrm{H}(f)$$

and

$$\mathrm{Deg}(\alpha) \leq \deg_T(P(x',T,0)) \leq \deg_{x_n}(P(x',x_n,T)) \leq \mathrm{H}(f).$$

Moreover, $P(x',T,0)$ is a polynomial having $\alpha_1,\dots,\alpha_d$ as roots. Thus a splitting field of $P(x',T,0)$ over $\Bbbk(x')$ contains these roots, thus

$$[\Bbbk(x',\alpha_1,\dots,\alpha_d) : \Bbbk(x')] \leq \deg_T(P(x',T,0))!. \qquad \square$$

Lemma 3.11. *Let α be algebraic over $\Bbbk(x)$ with* $\mathrm{ord}_x(\alpha) > 0$. *Let $g(x,y)$ be an algebraic power series where y is a single variable. Then $g(x,\alpha)$ is algebraic over $\Bbbk(x)$ and*

$$\mathrm{H}(g(x,\alpha)) \leq \mathrm{H}(g)\cdot(\mathrm{H}(\alpha)+\mathrm{Deg}(\alpha)) \quad \textit{and} \quad \mathrm{Deg}(g(x,\alpha)) \leq \mathrm{Deg}(\alpha)\cdot\mathrm{Deg}(g).$$

Proof. Let $P(x,y,T) \in \Bbbk[x,y,T]$ be the minimal polynomial of the algebraic power series g and let $Q(x,T) \in \Bbbk[x,T]$ be the minimal polynomial of α. Then

$$P(x,\alpha,g(x,\alpha))=0$$

and $P(x,\alpha,T) \neq 0$ otherwise $P(x,y,T)$ is divisible by $Q(x,y)$ which is impossible since P is assumed to be irreducible. Thus $g(x,\alpha)$ is algebraic over $\Bbbk(x,\alpha)$, hence over $\Bbbk(x)$. If we denote by $R(x,T)$ the resultant of $P(x,y,T)$ and $Q(x,y)$ seen as polynomials in y, i.e.

$$R(x,T) := \mathrm{Res}_y(P(x,y,T),Q(x,y)) \neq 0,$$

then $R(x,T)$ is a polynomial of $\mathbb{k}[x][T]$ vanishing at $g(x,\alpha)$. Let us write

$$P(x,y,T) = a_0(x,T) + a_1(x,T)y + \cdots + a_h(x,T)y^h \quad \text{with} \quad a_h \neq 0.$$

Moreover, since $P(x,y,T)$ is the minimal polynomial of g (as a polynomial in T), for all i we have

$$\begin{aligned}
\deg_x(a_i) + i &\leq \mathrm{H}(g), \\
\deg(a_i) &\leq \mathrm{H}(g) + \mathrm{Deg}(g) - i \leq \mathrm{H}(g) + \mathrm{Deg}(g), \\
\deg_T(a_i) &\leq \mathrm{Deg}(g).
\end{aligned}$$

In particular, $h \leq \mathrm{H}(g)$ and $\deg_x(a_i) \leq \mathrm{H}(g)$ for all i. We write

$$Q(x,y) = b_0(x) + b_1(x)y + \cdots + b_e(x)y^e$$

with $e = \mathrm{Deg}(\alpha)$ and $\deg(b_i) \leq \mathrm{H}(\alpha)$ for all i. Since $R(x,T)$ is homogeneous of degree h in $b_0,\dots,b_e$ and homogeneous of degree e in $a_0,\dots,a_h$, we see that

$$\deg_T(R(x,T)) \leq e \cdot \mathrm{Deg}(g) = \mathrm{Deg}(\alpha)\cdot \mathrm{Deg}(g)$$

and

$$\mathrm{H}(R(x,T)) \leq h \cdot \mathrm{H}(\alpha) + e \cdot \mathrm{H}(g).$$

This proves the lemma. □

Corollary 3.12. *Let f be an x_n-regular algebraic power series and let $\alpha_1,\dots,\alpha_d$ be distinct roots of f in $\mathbb{K}_{n-1}$. Let $g \in \mathbb{k}\langle x\rangle$ be any algebraic power series. Then*

$$\left[\mathbb{k}(x',\alpha_1,\dots,\alpha_d, g(x',\alpha_1),\dots,g(x',\alpha_d)) : \mathbb{k}(x')\right] \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^d.$$

Proof. By Lemmas 3.10 and 3.11 the degree of this field extension is finite. By the proof of Lemma 3.11 we have, for any i,

$$\left[\mathbb{k}(x',\alpha_1,\dots,\alpha_d, g(x',\alpha_i)) : \mathbb{k}(x',\alpha_1,\dots,\alpha_d)\right] \leq \mathrm{Deg}(g).$$

Thus

$$\left[\mathbb{k}(x',\alpha_1,\dots,\alpha_d, g(x',\alpha_1),\dots,g(x',\alpha_d)) : \mathbb{k}(x',\alpha_1,\dots,\alpha_d)\right] \leq \mathrm{Deg}(g)^d.$$

Hence the result follows by Lemma 3.10. □

Remark 3.13. Let $g(x,y)$ be an algebraic power series where $y = (y_1,\dots,y_m)$ is a tuple of indeterminates and let $a_1(x),\dots,a_m(x)$ be algebraic power series vanishing at 0. If $P(x,y,T)$ is the minimal polynomial of g, then

$$P(x,a(x),g(x,a(x)) = 0$$

but it may happen that

$$P(x,a(x),T) = 0.$$

Hence the previous proof does not extend directly to this case. For example let

$$\begin{aligned}
P_1(x,y_1) &:= y_1^2 - (1+x), \\
P_2(x,y_2) &:= y_2^2 - (1+x)
\end{aligned}$$

where x is a single variable and $\Bbbk$ is a field of characteristic $\neq 2$ in which -7 is a square. Then P_1 and P_2 have a common root in $\Bbbk\langle x\rangle$, say $a(x)$. Let

$$P(x,y,T) := (P_1 + P_2)T^2 + P_1 T + P_2.$$

The discriminant of P is equal to

$$\begin{aligned}\Delta &:= P_1^2 - 4P_2(P_1 + P_2)\\ &= y_1^4 - 2(1+x)y_1^2 + (1+x)^2 + 4(y_2^2 - (1+x))(2(1+x) - y_1^2 - y_2^2)\\ &= y_1^4 + 2(1 + x - 2y_2^2)y_1^2 + 12(1+x)y_2^2 - 4y_2^4 - 7(1+x)^2\end{aligned}$$

and is not a square in $\Bbbk[x, y_1, y_2]$, thus P is irreducible in $\Bbbk[x,y,T]$. But Δ is unit in $\Bbbk\langle x,y\rangle$ since $\Delta(0,0,0) = -7$, and $P_1 + P_2$ is also a unit. So Δ has a root square in $\Bbbk\langle x,y\rangle$ since $\mathrm{char}(\Bbbk) \neq 2$ and -7 is a square in $\Bbbk$. Thus in this case $P(x,y,T)$ has two distinct roots in $\Bbbk\langle x,y\rangle$. But here

$$P(x, a(x), a(x), T) = 0.$$

Nevertheless, we can extend Lemma 3.11 as follows:

Lemma 3.14. *Let $g(x,y)$ be an algebraic power series where $y = (y_1,\dots,y_m)$ is a tuple of indeterminates and let $a_1(x),\dots,a_m(x)$ be algebraic power series vanishing at 0. Then*

$$\mathrm{H}(g(x,a(x))) \leq \left(\prod_{i=1}^{m}(\mathrm{H}(a_i) + \mathrm{Deg}(a_i))\right)\cdot \mathrm{H}(g),$$
$$\mathrm{Deg}(g(x,a(x))) \leq \left(\prod_{i=1}^{m}\mathrm{Deg}(a_i)\right)\cdot \mathrm{Deg}(g).$$

Proof. Let us set

$$\begin{aligned} g_0(x,y_1,\dots,y_m) &:= g(x,y),\\ g_1(x,y_2,\dots,y_m) &:= g_0(x,a_1(x),y_2,\dots,y_m),\\ g_2(x,y_3,\dots,y_m) &:= g_1(x,a_2(x),y_3,\dots,y_m),\\ &\vdots\\ g_m(x) &:= g_{m-1}(x,a_m(x)) = g(x,a(x)).\end{aligned}$$

Then by Lemma 3.11, we have

$$\mathrm{Deg}(g_i) \leq \mathrm{Deg}(a_i)\cdot\mathrm{Deg}(g_{i-1}) \quad \text{and} \quad \mathrm{H}(g_i) \leq \mathrm{H}(g_{i-1})(\mathrm{H}(a_i) + \mathrm{Deg}(a_i)).$$

This proves the lemma. □

Lemma 3.15. *Let f be an algebraic power series. Then $\frac{\partial f}{\partial x_n}$ is an algebraic power series and*

$$\mathrm{H}\left(\frac{\partial f}{\partial x_n}\right) \leq 4\,\mathrm{Deg}(f)^{2\,\mathrm{Deg}(f)+4}\,\mathrm{H}(f),$$
$$\mathrm{Deg}\left(\frac{\partial f}{\partial x_n}\right) \leq \mathrm{Deg}(f).$$

Proof. Let $P(x,T)$ be the minimal polynomial of f. Since $P(x,f)=0$, we have

$$\frac{\partial P}{\partial x_n}(x,f(x))+\frac{\partial f}{\partial x_n}(x)\frac{\partial P}{\partial T}(x,f(x))=0.$$

Since f is separable over $\mathbb{k}(x)$ (indeed $\mathbb{k}\langle x\rangle$ is the Henselization of $\mathbb{k}[x]_{(x)}$ and the morphism from a local ring to its Henselization is always a separable morphism – see [26, p. 180]), we have $\frac{\partial P}{\partial T}\neq 0$. Moreover, P is the minimal polynomial of f so $\frac{\partial P}{\partial T}(x,f(x))\neq 0$. Thus $\frac{\partial f}{\partial x_n}(x)$ is an algebraic power series and

$$\frac{\partial f}{\partial x_n}(x)=-\frac{\frac{\partial P}{\partial x_n}(x,f(x))}{\frac{\partial P}{\partial T}(x,f(x))}\in\mathbb{k}(x,f).$$

So we obtain

$$\operatorname{Deg}\left(\frac{\partial f}{\partial x_n}(x)\right)\le\operatorname{Deg}(f)$$

and, by Lemma 3.6 (vi),

$$\mathrm{H}\left(\frac{\partial f}{\partial x_n}(x)\right)\le 2\operatorname{Deg}(f)^2\max\left\{\mathrm{H}\left(\frac{\partial P}{\partial x_n}(x,f(x))\right),\mathrm{H}\left(\frac{\partial P}{\partial T}(x,f(x))\right)\right\}. \tag{3.1}$$

We have

$$\frac{\partial P}{\partial T}(x,f(x))=\sum_{i=0}^{\operatorname{Deg}(f)-1}a_i(x)f(x)^i$$

for some polynomials $a_i(x)$ with $\deg(a_i)\le\mathrm{H}(f)$. Thus, by Lemma 3.6 (ii),

$$\begin{aligned}\mathrm{H}\left(\frac{\partial P}{\partial T}(x,f(x))\right)&\le\operatorname{Deg}(f)\cdot\operatorname{Deg}(f^0)\cdots\operatorname{Deg}(f^{\operatorname{Deg}(f)-1})\Big(\max_j\{\mathrm{H}(f^j)+\mathrm{H}(a_j)\}\Big)\\&\le\operatorname{Deg}(f)^{\operatorname{Deg}(f)}((\operatorname{Deg}(f)-1)\operatorname{Deg}(f)^{\operatorname{Deg}(f)-1}\mathrm{H}(f)+\mathrm{H}(f))\\&\le\operatorname{Deg}(f)^{2\operatorname{Deg}(f)}\mathrm{H}(f)\end{aligned}$$

since $f^0=1$, $f^i\in\mathbb{k}(x,f)$ for all i and

$$\mathrm{H}(a_i)=\deg(a_i)\le\mathrm{H}(f),\quad \mathrm{H}(f^i)\le i\operatorname{Deg}(f)^i\,\mathrm{H}(f)\quad\text{for all } i$$

by Lemma 3.6 (vi).

We also have

$$\frac{\partial P}{\partial x_n}(x,f(x))=\sum_{i=0}^{\operatorname{Deg}(f)}b_i(x)f(x)^i$$

for some polynomials $b_i(x)$ with $\deg(b_i)\le\mathrm{H}(f)$. Thus in the same way

$$\begin{aligned}\mathrm{H}\left(\frac{\partial P}{\partial x_n}(x,f(x))\right)&\le\operatorname{Deg}(f)\cdot\operatorname{Deg}(f^0)\cdots\operatorname{Deg}(f^{\operatorname{Deg}(f)})\Big(\max\{\mathrm{H}(f^i)+\mathrm{H}(f)\}\Big)\\&\le\operatorname{Deg}(f)^{\operatorname{Deg}(f)+1}(\operatorname{Deg}(f)\operatorname{Deg}(f)^{\operatorname{Deg}(f)}\mathrm{H}(f)+\mathrm{H}(f))\\&\le 2\operatorname{Deg}(f)^{2\operatorname{Deg}(f)+2}\mathrm{H}(f).\end{aligned}$$

Replacing these inequalities in inequality (3.1) we are done. □

Lemma 3.16. *Let $f(x,y)$ be an algebraic power series where $x=(x_1,\dots,x_n)$ and y is a single variable. Let q be a positive integer. Then $f(x,y^q)$ is an algebraic power series with the same degree as $f(x,y)$ and*

$$\mathrm{H}(f(x,y)) \leq \mathrm{H}(f(x,y^q)) \leq q\,\mathrm{H}(f(x,y)).$$

Proof. If $P(x,y,T)$ is the minimal polynomial of $f(x,y)$, then $P(x,y^q,T)$ is a polynomial having $f(x,y^q)$ as a root. Thus $f(x,y^q)$ is an algebraic power series. Since $\Bbbk[x,y,T]$ is a free $\Bbbk[x,y^q,T]$-module with basis $1,y,\dots,y^{q-1}$, if $Q(x,y,T)$ is the minimal polynomial of $f(x,y^q)$, we can write in a unique way

$$Q(x,y,T) = Q_0(x,y^q,T) + Q_1(x,y^q,T)y + \cdots + Q_{q-1}(x,y^q,T)y^{q-1}$$

where the $Q_i(x,y^q,T)$ are polynomials. Since $Q(x,y,f(x,y^q))=0$, we see that

$$Q_i(x,y^q,f(x,y^q)) = 0 \quad \text{for all } i.$$

Since Q is the minimal polynomial of $f(x,y^q)$, the polynomial Q divides all the $Q_i(x,y^q,T)$, hence $Q=Q_0$ and $Q_i=0$ for all $i>0$. This shows that the minimal polynomial of $f(x,y^q)$ has coefficients in $\Bbbk[x,y^q]$.

Now if $Q(x,y^q,T)$ is the minimal polynomial of $f(x,y^q)$, then $Q(x,y,f(x,y))=0$. This proves that $P(x,y,T)$ is the minimal polynomial of $f(x,y)$ if and only if $P(x,y^q,T)$ is the minimal polynomial of $f(x,y^q)$. Since

$$\deg_T(P(x,y,T)) = \deg_T(P(x,y^q,T)),$$

we see that $f(x,y)$ and $f(x,y^q)$ have the same degree. Moreover,

$$\deg_{(x,y)}(P(x,y,T)) \leq \deg_{(x,y)}(P(x,y^q,T)) \leq q\cdot\deg_{(x,y)}(P(x,y,T)).$$

This shows the inequalities concerning the heights. □

Lemma 3.17. *Let $f(x,y)$ be an algebraic power series where y is a single variable and let q be a positive integer. Let us write $q=rp^e$ where $p=\mathrm{char}(\Bbbk)$, $e\in\mathbb{N}$ and $\gcd(r,p)=1$ (we set $e=0$ when $\mathrm{char}(\Bbbk)=0$ and by convention $q=r$). Let us write*

$$f(x,y) = f_0(x,y^q) + f_1(x,y^q)y + \cdots + f_{q-1}(x,y^q)y^{q-1}.$$

Then the power series $f_i(x,y^q)$ are algebraic and for any $0\leq i\leq q-1$ we have

$$\mathrm{H}(f_i(x,y^q)) \leq \begin{cases} q^2 p^{\frac{e(e+1)}{2}} 4^q \,\mathrm{Deg}(f)^{2q\,\mathrm{Deg}(f)+5q}\left(\mathrm{H}(f)+\frac{q(q-1)}{2}\right) & \text{if } e>0,\\ q\,\mathrm{Deg}(f)^q(q\,\mathrm{H}(f)+q-1) & \text{if } e=0,\end{cases}$$

$$\mathrm{Deg}(f_i(x,y^q)) \leq \mathrm{Deg}(f)^r.$$

Proof. We need to consider several cases.

Case (1). First we assume that $e=0$ i.e. $\gcd(q,p)=1$. By taking a finite extension of $\Bbbk$ we may assume that $\Bbbk$ contains a primitive q-th root of unity. Let ξ be such a primitive root of unity. Then

$$f(x,\xi^l y) = \sum_{k=0}^{q-1} f_k(x,y^q)\xi^{lk}y^k \quad \text{for all } k,l.$$

Thus we have

$$\widetilde{f} = V(\xi)F$$

where $\widetilde{f}$ is the vector with entries $f(x, \xi^l y)$, $1 \leq l \leq q$, F is the vector with entries $f_0(x, y^q)$, $yf_1(x, y^q), \dots, y^{q-1} f_{q-1}(x, y^q)$ and $V(\xi)$ is the Vandermonde matrix

$$\begin{bmatrix} 1 & \xi & \xi^2 & \cdots & \xi^{q-1} \\ 1 & \xi^2 & \xi^4 & \cdots & \xi^{2(q-1)} \\ 1 & \xi^3 & \xi^6 & \cdots & \xi^{3(q-1)} \\ \vdots & \vdots & \vdots & \dots & \dots \\ 1 & \xi^q & \xi^{2q} & \cdots & \xi^{(q-1)q} \end{bmatrix}.$$

Thus

$$F = V(\xi)^{-1} \widetilde{f}.$$

Since the entries of $V(\xi)^{-1}$ are in $\Bbbk$ and $\mathrm{H}(f(x, \xi^l y)) = \mathrm{H}(f(x, y))$, by Lemma 3.6 (ii) and (i) we have

$$\mathrm{H}(F) \leq q \operatorname{Deg}(f)^q \mathrm{H}(f) \quad \text{and} \quad \operatorname{Deg}(F) \leq \operatorname{Deg}(f)^q.$$

Thus by Lemma 3.6 (iv),

$$\mathrm{H}(f_i(x, y^q)) \leq q \operatorname{Deg}(f)^q \mathrm{H}(f) + \operatorname{Deg}(f)^q (q-1) = \operatorname{Deg}(f)^q (q \mathrm{H}(f) + q - 1)$$

and

$$\operatorname{Deg}(f_i(x, y^q)) \leq \operatorname{Deg}(f)^q \quad \text{for all } i.$$

Case (2). If $q = p > 0$, then we have

$$\begin{aligned} \frac{\partial f}{\partial y} &= f_1 + 2f_2 y + \cdots + (p-1) f_{p-1} y^{p-2}, \\ &\vdots \\ \frac{\partial^{p-1} f}{\partial y^{p-1}} &= (p-1)! f_{p-1}. \end{aligned}$$

Thus we have

$$\Delta f = M \widetilde{f}$$

where Δf is the vector of entries $\frac{\partial^k f}{\partial y^k}$, $0 \leq k \leq p-1$, $\widetilde{f}$ is the vector with entries $f_l(x, y^p)$, $0 \leq l \leq p-1$, and M is a upper triangular matrix with entries in $\Bbbk[y]$ and whose determinant is in $\Bbbk$. We can check that the $(p-1) \times (p-1)$ minors of M are polynomials of degree $\leq \frac{p(p-1)}{2}$. Thus the height of the coefficients of M^{-1} is less than $\frac{p(p-1)}{2}$. Since

$$\widetilde{f} = M^{-1} \Delta f,$$

by Lemma 3.6 (ii) we obtain

$$\mathrm{H}(f_k(x, y^p)) \leq p \operatorname{Deg}(f) \prod_{j=1}^{p-1} \operatorname{Deg}\Big(\frac{\partial^j f}{\partial y^j}\Big) \Big(\max_{0 \leq i \leq p-1} \Big\{ \mathrm{H}\Big(\frac{\partial^i f}{\partial y^i}\Big) \Big\} + \frac{p(p-1)}{2} \Big).$$

Thus by Lemma 3.15 we have

$$\mathrm{H}(f_k(x,y^p)) \leq p\,\mathrm{Deg}(f)^p\left(\max_{0\leq i\leq p-1}\left\{\mathrm{H}\left(\frac{\partial^i f}{\partial y^i}\right)\right\}+\frac{p(p-1)}{2}\right).$$

By applying Lemma 3.15 $p-1$ times we obtain

$$\mathrm{H}\left(\frac{\partial^{p-1} f}{\partial y^{p-1}}\right) \leq 4^{p-1}\,\mathrm{Deg}(f)^{(2\,\mathrm{Deg}(f)+4)(p-1)}\,\mathrm{H}(f).$$

Thus we have

$$\mathrm{H}(f_k(x,y^p)) \leq p4^{p-1}\,\mathrm{Deg}(f)^{2(p-1)\,\mathrm{Deg}(f)+5p-4}\left(\mathrm{H}(f)+\frac{p(p-1)}{2}\right).$$

Moreover, still by Lemma 3.15 we have

$$\mathrm{Deg}(f_k(x,y^p)) \leq \mathrm{Deg}(f) \quad \text{for all } k.$$

Case (3). If $q=rp^e$ where $\gcd(r,p)=1$ and $e>0$, we write

$$\begin{aligned}
f &= \widetilde{f_0}(x,y^p)+\widetilde{f_1}(x,y^p)y+\cdots+\widetilde{f_{p-1}}(x,y^p)y^{p-1},\\
\widetilde{f_i}(x,y^p) &= \widetilde{f_{i,0}}(x,y^{p^2})+\widetilde{f_{i,1}}(x,y^{p^2})y^p+\cdots+\widetilde{f_{i,p-1}}(x,y^{p^2})y^{p(p-1)},\\
\widetilde{f_{i,j}}(x,y^{p^2}) &= \widetilde{f_{i,j,0}}(x,y^{p^3})+\widetilde{f_{i,j,1}}(x,y^{p^3})y^{p^2}+\cdots+\widetilde{f_{i,j,p-1}}(x,y^{p^3})y^{p^2(p-1)},\\
&\ \ \vdots\\
\widetilde{f_{i_1,\dots,i_{e-1}}}(x,y^{p^{e-1}}) &= \widetilde{f_{i_1,\dots,i_{e-1},0}}(x,y^{p^e})+\cdots+\widetilde{f_{i_1,\dots,i_{e-1},p-1}}(x,y^{p^e})y^{p^{e-1}(p-1)},\\
\widetilde{f_{i_1,\dots,i_e}}(x,y^{p^e}) &= \widetilde{f_{i_1,\dots,i_e,0}}(x,y^q)+\cdots+\widetilde{f_{i_1,\dots,i_e,r-1}}(x,y^q)y^{p^e(r-1)}.
\end{aligned}$$

Then by (2) we obtain, for $k\leq e$,

$$\mathrm{Deg}(\widetilde{f_{i_1,\dots,i_k}}(x,y^p)) \leq \mathrm{Deg}(\widetilde{f_{i_1,\dots,i_{k-1}}}(x,y))$$

and

$$\begin{aligned}
\mathrm{H}(\widetilde{f_{i_1,\dots,i_k}}(x,y^p)) \leq p4^{p-1}\,&\mathrm{Deg}(\widetilde{f_{i_1,\dots,i_{k-1}}}(x,y))^{2(p-1)\,\mathrm{Deg}(\widetilde{f_{i_1,\dots,i_{k-1}}}(x,y))+5p-4}\\
&\times\left(\mathrm{H}(\widetilde{f_{i_1,\dots,i_{k-1}}}(x,y))+\frac{p(p-1)}{2}\right).
\end{aligned}$$

Thus by Lemma 3.16 we have

$$\begin{aligned}
&\frac{1}{p^{k-1}}\,\mathrm{H}(\widetilde{f_{i_1,\dots,i_k}}(x,y^{p^k}))\\
&\quad\leq p4^{p-1}\,\mathrm{Deg}(\widetilde{f_{i_1,\dots,i_{k-1}}}(x,y^{p^{k-1}}))^{2(p-1)\,\mathrm{Deg}(\widetilde{f_{i_1,\dots,i_{k-1}}}(x,y^{p^{k-1}}))+5p-4}\\
&\qquad\times\left(\mathrm{H}(\widetilde{f_{i_1,\dots,i_{k-1}}}(x,y^{p^{k-1}}))+\frac{p(p-1)}{2}\right).
\end{aligned}$$

By (1) we obtain

$$\begin{aligned}
\mathrm{Deg}(\widetilde{f_{i_1,\dots,i_{e+1}}}(x,y^r)) &\leq \mathrm{Deg}(\widetilde{f_{i_1,\dots,i_e}}(x,y))^r,\\
\mathrm{H}(\widetilde{f_{i_1,\dots,i_{e+1}}}(x,y^r)) &\leq \mathrm{Deg}(\widetilde{f_{i_1,\dots,i_e}}(x,y))^r(r\,\mathrm{H}(\widetilde{f_{i_1,\dots,i_e}}(x,y))+r-1)
\end{aligned}$$

and, by Lemma 3.16,

$$\frac{1}{p^e}\,\mathrm{H}(\widetilde{f}_{i_1,\dots,i_{e+1}}(x,y^q)) \leq \mathrm{Deg}(\widetilde{f}_{i_1,\dots,i_e}(x,y^{p^e}))^r(r\,\mathrm{H}(\widetilde{f}_{i_1,\dots,i_e}(x,y^{p^e}))+r-1).$$

Since the power series $f_i(x,y^q)$ of the statement of the lemma are expressed by the power series

$$\widetilde{f}_{i_1,\dots,i_{e+1}}(x,y^q),$$

by induction and Lemma 3.16 we deduce

$$\mathrm{Deg}(f_i(x,y^q)) \leq \mathrm{Deg}(f)^r$$

and

$$\begin{aligned}\mathrm{H}(f_i(x,y^q)) &\leq p^{\frac{e(e+1)}{2}}q4^{p^e-1}\,\mathrm{Deg}(f)^{r+2(p-1)e\,\mathrm{Deg}(f)+(5p-4)e}\left(r\,\mathrm{H}(f)+(e+1)\frac{r(r-1)}{2}\right)\\ &\leq q^2p^{\frac{e(e+1)}{2}}4^q\,\mathrm{Deg}(f)^{2q\,\mathrm{Deg}(f)+5q}\left(\mathrm{H}(f)+\frac{q(q-1)}{2}\right). \qquad \square\end{aligned}$$

4. Effective Weierstrass Division Theorem

In this section we prove an effective Weierstrass Division Theorem for algebraic power series. The proof (thus the complexity) is more complicated in the positive characteristic case since the Weierstrass polynomial associated to the divisor f may have irreducible factors that are not separable. The proof we give here is essentially the same as the one given in [20].

Lemma 4.1 (Weierstrass Preparation Theorem). *Let $\Bbbk$ be any field, and let f be an algebraic power series which is x_n-regular of order d. Then there exist a unit $u\in\Bbbk\langle x\rangle$ and a Weierstrass polynomial $P\in\Bbbk\langle x'\rangle[x_n]$ such that*

$$f = u\cdot P$$

and

$$\mathrm{Deg}(P)\leq \mathrm{H}(f)!,\quad \mathrm{H}(P)\leq 2d\,\mathrm{H}(f)^{d+1}.$$

Proof. The existence of u and P comes from the Weierstrass Preparation Theorem for formal power series.

Let $\alpha_1,\dots,\alpha_d\in\mathbb{K}_{n-1}$ be the roots of $P(x_n)$ counted with multiplicities. Then we have $P=\prod_{i=1}^d(x_n-\alpha_i)$. By Remark 3.9 the roots of $P(x_n)$ are the roots of f thus, by Lemma 3.10, P is an algebraic power series. Hence u is also an algebraic power series.

By Lemma 3.6 (iii)

$$\mathrm{H}(x_n-\alpha_i)\leq \mathrm{H}(\alpha_i)+\mathrm{Deg}(\alpha_i)$$

and

$$\mathrm{Deg}(x_n-\alpha_i)=\mathrm{Deg}(\alpha_i)\leq \mathrm{H}(f)$$

for all i by Lemma 3.10. Thus, by Lemma 3.6 (vi),

$$\begin{aligned}\mathrm{H}(P)&\leq d\cdot\mathrm{Deg}(\alpha_1)\cdots\mathrm{Deg}(\alpha_d)\cdot\max_i\{\mathrm{H}(\alpha_i)+\mathrm{Deg}(\alpha_i)\}\\ &\leq d\,\mathrm{H}(f)^d(\mathrm{H}(f)+\mathrm{H}(f)).\end{aligned}$$

Moreover, $P \in \mathbb{k}(x, \alpha_1, \dots, \alpha_d)$. But

$$[\mathbb{k}(x, \alpha_1, \dots, \alpha_d) : \mathbb{k}(x)] \leq \mathrm{H}(f)!$$

by Lemma 3.10 hence

$$\mathrm{Deg}(P) \leq \mathrm{H}(f)!. \qquad \square$$

Lemma 4.2. *Let f be an algebraic power series which is x_n-regular of order d and let us assume that f has d distinct roots in $\mathbb{K}_{n-1}$. Let g be any algebraic power series. Then there exist unique algebraic power series q and r such that $r \in \mathbb{k}\langle x'\rangle[x_n]$ is of degree $< d$ in x_n and*

$$g = fq + r.$$

Moreover, if $r = r_0 + r_1 x_n + \cdots + r_{d-1}x_n^{d-1}$, we have

$$\begin{aligned}\mathrm{H}(r_i) &\leq 4d(\mathrm{H}(f)!)^{d+1}\,\mathrm{H}(f)^2\,\mathrm{Deg}(g)\max\left\{d!\frac{d(d-1)}{2}\,\mathrm{H}(f)^{\frac{d(d-1)}{2}}(\mathrm{H}(f)!)^{d!+2}, \mathrm{H}(g)\right\}\\ &\leq 4\,\mathrm{H}(f)^{\mathrm{H}(f)^{O(d)}}\,\mathrm{Deg}(g)(\mathrm{H}(g)+1) \quad \text{for all } i,\end{aligned}$$

where $O(d)$ denotes a function of d bounded by a linear function in d,

$$\mathrm{H}(r) \leq d\left(\mathrm{H}(f)!\,\mathrm{Deg}(g)^d\right)^d\left(\max_i\{\mathrm{H}(r_i)\} + d - 1\right)$$

and

$$\mathrm{Deg}(r_i), \mathrm{Deg}(r) \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^d \quad \text{for all } i.$$

Proof. The Weierstrass Division Theorem for algebraic power series is well known (see [20]), the only improvement is the inequalities on the heights and degrees. The Weierstrass Division Theorem for formal power series gives the existence and unicity of q and r. Thus we have to show that q and r are algebraic and to prove the bounds on the heights and degrees. Let $\alpha_1, \dots, \alpha_d \in \mathbb{K}_{n-1}$ be the roots of f. Then we have

$$g(x', \alpha_i) = r(x', \alpha_i) \quad \text{for all } i.$$

By writing $r = r_0 + r_1 x_n + \cdots + r_{d-1}x_n^{d-1}$ with $r_j \in \mathbb{k}[\![x']\!]$ for all j, we obtain

$$V(\alpha)\widetilde{r} = \widetilde{g}(\alpha)$$

where $V(\alpha)$ is the $d \times d$ Vandermonde matrix of the α_i:

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{d-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_d & \alpha_d^2 & \cdots & \alpha_d^{d-1} \end{bmatrix},$$

$\widetilde{r}$ is the $d \times 1$ column vector with entries r_k, and $\widetilde{g}(\alpha)$ is the $d \times 1$ column vector with entries $g(x', \alpha_j)$. Since the α_i are distinct, it follows that $V(\alpha)$ is invertible and we obtain

$$\widetilde{r} = V(\alpha)^{-1}\widetilde{g}(\alpha). \tag{4.1}$$

By Lemmas 3.10 and 3.11 we see the $g(x',\alpha_j)$ are algebraic. Then equality (4.1) shows that the r_i and r are algebraic power series, thus q is also an algebraic power series. Again by Lemmas 3.10 and 3.11 we have, for all i,

$$\mathrm{H}(g(x',\alpha_i)) \leq 2\,\mathrm{H}(g)\cdot\mathrm{H}(f), \quad \mathrm{Deg}(g(x',\alpha_i)) \leq \mathrm{H}(f)\cdot\mathrm{Deg}(g).$$

The determinant of $V(\alpha)$ is the sum of $d!$ elements of the form

$$\alpha^0_{\sigma(0)}\alpha^1_{\sigma(1)}\alpha^2_{\sigma(2)}\cdots\alpha^{d-1}_{\sigma(d-1)}$$

where σ is a permutation of $\{0,\dots,d-1\}$. Each of these elements belongs to $\Bbbk(x',\alpha_1,\dots,\alpha_d)$ so their degree is bounded $\mathrm{H}(f)!$ by Lemma 3.10. Again by Lemma 3.10, $\mathrm{H}(\alpha_i)\leq\mathrm{H}(f)$ and $\mathrm{Deg}(\alpha_i)\leq\mathrm{H}(f)$ for any i, thus by Lemma 3.6 (vi) we see that for any permutation σ we have

$$\mathrm{H}(\alpha^0_{\sigma(0)}\alpha^1_{\sigma(1)}\alpha^2_{\sigma(2)}\cdots\alpha^{d-1}_{\sigma(d-1)}) \leq \frac{d(d-1)}{2}\,\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}.$$

Thus by Lemma 3.6 (ii) we have

$$\mathrm{H}(\det(V(\alpha))) \leq d!\frac{d(d-1)}{2}\,\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}(\mathrm{H}(f)!)^{d!}.$$

The entries of $V(\alpha)^{-1}$ are $(d-1)\times(d-1)$ minors of $V(\alpha_i)$ divided by $\det(V(\alpha))$. Exactly as above the height of such an $(d-1)\times(d-1)$ minor is bounded by

$$(d-1)!\frac{(d-1)(d-2)}{2}\,\mathrm{H}(f)^{\frac{(d-1)(d-2)}{2}+1}(\mathrm{H}(f)!)^{(d-1)!}$$

and its degree is bounded by $\mathrm{H}(f)!$ since it is an element of $\Bbbk(x',\alpha_1,\dots,\alpha_d)$ (see Lemma 3.10). Hence by Lemma 3.6 (vi) the height of the entries of $V(\alpha)^{-1}$ is bounded by

$$\begin{aligned}\mathrm{H}_V &:= 2d!(\mathrm{H}(f)!)^2(\mathrm{H}(f)!)^{d!}\frac{d(d-1)}{2}\,\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}\\ &= 2d!\frac{d(d-1)}{2}\,\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}(\mathrm{H}(f)!)^{d!+2}.\end{aligned}$$

Moreover, their degree is bounded by $\mathrm{H}(f)!$ since they belong to $\Bbbk(x,\alpha_1,\dots,\alpha_d)$.

If v is an entry of $V(\alpha)^{-1}$, Lemma 3.6 (vi) shows

$$\mathrm{H}(vg(x',\alpha_i)) \leq 2\,\mathrm{H}(f)!\,\mathrm{Deg}(g(x',\alpha_i))\max\{\mathrm{H}_V,\mathrm{H}(g(x',\alpha_i))\} \quad \text{for all } i.$$

Since r_j is of the form $v_1 g(x',\alpha_1)+\cdots+v_d g(x',\alpha_d)$ where $v_1,\dots,v_d$ are entries of $V(\alpha)^{-1}$ (by equation (4.1)), we obtain from Lemma 3.6 (ii) that

$$\mathrm{H}(r_j) \leq d(\mathrm{H}(f)!)^d \max_i\bigl\{2\,\mathrm{H}(f)!\,\mathrm{Deg}(g(x',\alpha_i))\max\{\mathrm{H}_V,\mathrm{H}(g(x',\alpha_i))\}\bigr\}.$$

Hence Lemmas 3.10 and 3.11 show

$$\begin{aligned}\mathrm{H}(r_j) &\leq 4d(\mathrm{H}(f)!)^{d+1}\,\mathrm{H}(f)\,\mathrm{Deg}(g)\\ &\qquad\times\max\Bigl\{d!\frac{d(d-1)}{2}\,\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}(\mathrm{H}(f)!)^{d!+2},\mathrm{H}(f)\,\mathrm{H}(g)\Bigr\}\\ &= 4d(\mathrm{H}(f)!)^{d+1}\,\mathrm{H}(f)^2\,\mathrm{Deg}(g)\max\Bigl\{d!\frac{d(d-1)}{2}\,\mathrm{H}(f)^{\frac{d(d-1)}{2}}(\mathrm{H}(f)!)^{d!+2},\mathrm{H}(g)\Bigr\}.\end{aligned}$$

Moreover, r_j and r belong to $k(x', \alpha_1, \dots, \alpha_d, g(x', \alpha_1), \dots, g(x', \alpha_d))$, hence we have (by Corollary 3.12):

$$\mathrm{Deg}(r_j) \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^d, \quad \mathrm{Deg}(r) \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^d.$$

Since

$$r = r_0 + x_n r_n + \cdots + x_n^{d-1} r_{d-1},$$

we have

$$H(r) \leq d\big(\mathrm{H}(f)!\,\mathrm{Deg}(g)^d\big)^d \Big(\max_i\{\mathrm{H}(r_i)\} + d - 1\Big)$$

by Lemma 3.6 (ii). □

Lemma 4.3. *Let assume that $\Bbbk$ is a field of characteristic $p > 0$. Let f be an irreducible algebraic power series which is x_n-regular of order d and let us assume that its Weierstrass polynomial is not separable. Let g be any algebraic power series. Then there exist unique algebraic power series q and r such that $r \in \Bbbk\langle x'\rangle[x_n]$ is of degree $< d$ in x_n and*

$$g = fq + r.$$

Moreover, if $r = r_0 + r_1 x_n + \cdots + r_{d-1} x_n^{d-1}$, we have

$$\mathrm{H}(r_i) \leq (2\,\mathrm{H}(f))^{(2\,\mathrm{H}(f))^{O(d)}}\,\mathrm{Deg}(g)^{2d(\mathrm{Deg}(g)+2)}(\mathrm{H}(g)+1) \quad \textit{for all } i,$$
$$\mathrm{H}(r) \leq (2\,\mathrm{H}(f))^{(2\,\mathrm{H}(f))^{O(d)}}\,\mathrm{Deg}(g)^{O(d\,\mathrm{Deg}(g))}(\mathrm{H}(g)+1)$$

and

$$\mathrm{Deg}(r_i), \mathrm{Deg}(r) \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^d \quad \textit{for all } i.$$

Proof. Let P denote the Weierstrass polynomial of f. Since f is an irreducible power series, it follows that P is an irreducible monic polynomial of $\Bbbk[\![x']\!][x_n]$ hence P is an irreducible polynomial of $\Bbbk((x'))[x_n]$. Then we can write

$$P = \prod_{k=1}^{D} (x_n - \alpha_i)^{p^e}$$

where $\alpha_1, \dots, \alpha_D$ are the distinct roots of $P(x_n)$ in $\mathbb{K}_{n-1}$ and e is a positive integer. Thus $P \in \Bbbk\langle x'\rangle[x_n^{p^e}]$ by Lemma 4.1 and $d = Dp^e$. By the Weierstrass Division Theorem for formal power series we have

$$g = Pq + r$$

where

$$r = r_0 + r_1 x_n + \cdots + r_{d-1} x_n^{d-1}$$

and $r_i \in \Bbbk[\![x']\!]$. Let us write

$$g = g_0(x', x_n^{p^e}) + g_1(x', x_n^{p^e}) x_n + \cdots + g_{p^e-1}(x', x_n^{p^e}) x_n^{p^e-1}$$

where $g_i := g_i(x', x_n^{p^e}) \in \Bbbk\langle x', x_n^{p^e}\rangle$ for all i by Lemma 3.17 .

We define $\widetilde{P}$ by

$$\widetilde{P}(x', x_n^{p^e}) = P(x', x_n).$$

Then $\widetilde{P}(x', x_n)$ is a Weierstrass polynomial in x_n of degree D with algebraic power series coefficients and $\mathrm{H}(\widetilde{P}(x', x_n)) \leq \mathrm{H}(P(x', x_n))$ by Lemma 3.16. Let us perform the Weierstrass division of $g_i(x', x_n)$ by $\widetilde{P}$:

$$g_i(x', x_n) = \widetilde{P} q_i + \sum_{j=0}^{D-1} r_{i,j}(x') x_n^j.$$

By Lemma 4.2 the $r_{i,j}(x')$ are algebraic power series and

$$\begin{aligned}(4.2)\quad \mathrm{H}(r_{i,j}) \leq{}& 4D(\mathrm{H}(P)!)^{D+1}\,\mathrm{H}(P)^2 \operatorname{Deg}(g_i(x', x_n)) \\ &\times \max\left\{D!\frac{D(D-1)}{2}\,\mathrm{H}(P)^{\frac{D(D-1)}{2}}(\mathrm{H}(P)!)^{D!+2}, \mathrm{H}(g_i(x', x_n))\right\}.\end{aligned}$$

By Lemma 3.16 we have

$$\operatorname{Deg}(g_i(x', x_n)) \leq \operatorname{Deg}(g(x', x_n^{p^e})) \quad \text{for every } i$$

thus, by Lemma 3.17, we have

$$\operatorname{Deg}(g_i(x', x_n)) \leq \operatorname{Deg}(g).$$

Again by Lemma 3.16 we have

$$\mathrm{H}(g_i(x', x_n)) \leq \mathrm{H}(g(x', x_n^{p^e})).$$

Moreover, by Lemma 4.1, $\mathrm{H}(P) \leq 2d\,\mathrm{H}(f)^{d+1}$. Thus we obtain (by using Lemma 3.17 and since $D \leq d$, $p^e \leq d$ and $d \leq \mathrm{H}(f)$ by Lemma 3.7)

$$\begin{aligned}(4.3)\quad \mathrm{H}(r_{i,j}) \leq{}& 4d((2d\,\mathrm{H}(f)^{d+1})!)^{d+1}(2d\,\mathrm{H}(f)^{d+1})^2 \operatorname{Deg}(g) \\ &\times \max\Big\{d!\frac{d(d-1)}{2}(2d\,\mathrm{H}(f)^{d+1}))^{\frac{d(d-1)}{2}}((2d\,\mathrm{H}(f)^{d+1})!)^{d!+2}, \\ &\quad p^{2e} p^{e(e+1)/2} 4^{p^e} \operatorname{Deg}(g)^{2p^e \operatorname{Deg}(g)+5p^e}\left(\mathrm{H}(g) + \frac{p^e(p^e-1)}{2}\right)\Big\} \\ \leq{}& (2\,\mathrm{H}(f))^{(2\,\mathrm{H}(f))^{O(d)}} \operatorname{Deg}(g)^{2d(\operatorname{Deg}(g)+2)}(\mathrm{H}(g)+1).\end{aligned}$$

Finally, since

$$g_i(x', x_n^{p^e}) = P\,q_i(x', x_n^{p^e}) + \sum_{j=0}^{D-1} r_{i,j}(x') x_n^{jp^e},$$

we have

$$r = \sum_{i=0}^{p^e-1}\sum_{j=0}^{D-1} r_{i,j}(x') x_n^{jp^e+i}$$

by unicity of the remainder in the Weierstrass division. Thus Lemma 3.6 (ii) shows

$$\mathrm{H}(r) \leq p^e D \cdot \operatorname{Deg}(r_{i,j}(x'))^{p^e D} \max_{i,j}\{\mathrm{H}(r_{i,j}(x')) + jp^e\}.$$

Moreover,

$$\operatorname{Deg}(r_{i,j}), \operatorname{Deg}(r) \leq \mathrm{H}(f)!\operatorname{Deg}(g_i)^D \quad \text{for all } i, j$$

since $r_{i,j}$ and r belong to $\Bbbk(x', \alpha_1, \ldots, \alpha_D, g_i(x', \alpha_1), \ldots, g_i(x', \alpha_D))$ (as shown in the proof of Lemma 4.2). Hence

$$\mathrm{H}(r) \leq (2\,\mathrm{H}(f))^{(2\,\mathrm{H}(f))^{O(d)}} \operatorname{Deg}(g)^{O(d \operatorname{Deg}(g))}(\mathrm{H}(g)+1). \qquad \square$$

We will use at several places the following basic lemma:

Lemma 4.4. *For any $\varepsilon > 0$, $a > 0$ and $d \in \mathbb{N}$ we have*

$$(2d)^{(2d)^{ad}} \leq 2^{2^{O(d^{1+\varepsilon})}}.$$

Proof. Let $a > 0$ and $\varepsilon > 0$. There exists a constant $C > 0$ such that for any d large enough we have

$$ad \ln(2d) + \ln(\ln(2d)) \leq C \ln(2) d^{1+\varepsilon} + \ln(\ln(2)).$$

Thus

$$(2d)^{ad} \ln(2d) \leq \ln(2) 2^{Cd^{1+\varepsilon}}$$

and

$$(2d)^{(2d)^{ad}} \leq 2^{2^{Cd^{1+\varepsilon}}}. \qquad \square$$

Theorem 4.5 (Weierstrass Division Theorem). *Let $\mathbb{k}$ be a field. Let f be an algebraic power series which is x_n-regular of order d. Let g be an algebraic power series. Then there exist unique algebraic power series q and r such that $r \in \mathbb{k}\langle x'\rangle[x_n]$ is of degree $< d$ in x_n:*

$$r = r_0 + r_1 x_n + \cdots r_{d-1} x_n^{d-1}, \quad r_i \in \mathbb{k}\langle x'\rangle \text{ for all } i$$

and

$$g = fq + r.$$

Moreover, we have the following bounds (for any $\varepsilon > 0$):

(i) *if* $\operatorname{char}(\mathbb{k}) = 0$,

$$\mathrm{H}(r) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{d^4+d^3+6d^2-5d+3}(\mathrm{H}(g)+1),$$
$$\mathrm{H}(r_i) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{O(d^4)}(\mathrm{H}(g)+1) \quad \text{for all } i,$$
$$\mathrm{H}(q) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{d^4+d^3+6d^2-3d+5} \operatorname{Deg}(f)(\mathrm{H}(g)+1).$$

(ii) *if* $\operatorname{char}(\mathbb{k}) > 0$,

$$\mathrm{H}(r) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{O(d^4 \operatorname{Deg}(g)^4)}(\mathrm{H}(g)+1),$$
$$\mathrm{H}(r_i) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{O(d^4 \operatorname{Deg}(g)^4)}(\mathrm{H}(g)+1) \quad \text{for all } i,$$
$$\mathrm{H}(q) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{O(d^4 \operatorname{Deg}(g)^4)} \operatorname{Deg}(f)(\mathrm{H}(g)+1).$$

In both cases we have

$$\operatorname{Deg}(r) \leq \mathrm{H}(f)! \operatorname{Deg}(g)^d,$$
$$\operatorname{Deg}(r_i) \leq \mathrm{H}(f)! \operatorname{Deg}(g)^d \quad \text{for all } i,$$
$$\operatorname{Deg}(q) \leq \mathrm{H}(f)! \operatorname{Deg}(g)^{d+1} \operatorname{Deg}(f).$$

Proof. Let us write $f = u.P$ where u is a unit and P a Weierstrass polynomial in x_n. Let us decompose P into the product of irreducible Weierstrass polynomials

$$P = P_1 \cdots P_s.$$

Let us consider the following Weierstrass divisions:

$$\begin{aligned} g &= P_1Q_1 + R_1, \\ Q_1 &= P_2Q_2 + R_2, \\ &\vdots \\ Q_{s-1} &= P_sQ_s + R_s. \end{aligned}$$

Then

$$g = P_1 \cdots P_s Q_s + R_1 + P_1R_2 + P_1P_2R_3 + \cdots + P_1 \cdots P_{s-1}R_s.$$

Thus, by unicity of the Weierstrass division, we have

$$u \cdot q = Q_s$$

and

$$r := R_1 + P_1R_2 + P_1P_2R_3 + \cdots + P_1 \cdots P_{s-1}R_s$$

are the quotient and the remainder of the division of g by P. Here $s \leq d$ since P is monic of degree d in x_n. Let d_i be the degree in x_n of the polynomial P_i for $1 \leq i \leq s$. Let us choose $1 \leq i \leq s$ and let us denote by $\alpha_1, \ldots, \alpha_{d_i} \in \mathbb{K}_{n-1}$ the roots of P_i.

First let us prove the lemma when $\mathrm{char}(\Bbbk) = 0$. In this case these roots are distinct. Then

$$P_i = \prod_{i=1}^{d_i} (x_n - \alpha_i).$$

We have

$$\mathrm{H}(x_n - \alpha_i) \leq \mathrm{H}(\alpha_i) + \mathrm{Deg}(\alpha_i) \leq 2\,\mathrm{H}(f)$$

(by Lemma 3.6 (iii)) and

$$\mathrm{Deg}(x_n - \alpha_i) = \mathrm{Deg}(\alpha_i) \leq \mathrm{H}(f).$$

Then, by Lemma 3.6 (vi) and since $d_i \leq d \leq \mathrm{H}(f)$ (by Lemma 3.7), we have

$$\mathrm{H}(P_i) \leq d_i\,\mathrm{H}(f)^{d_i} \cdot 2\,\mathrm{H}(f) \leq 2\,\mathrm{H}(f)^{\mathrm{H}(f)+2}.$$

Moreover,

$$\mathrm{Deg}(P_i) \leq \mathrm{H}(f)!$$

since P_i is in the extension of $\Bbbk(x)$ generated by the roots of f.

Exactly as in the proof of Lemma 4.2 we have

$$R_i \in \Bbbk(x, \alpha_1, \ldots, \alpha_d, Q_{i-1}(x', \alpha_1), \ldots, Q_{i-1}(x', \alpha_d)).$$

Since $Q_{i-1} = \frac{Q_{i-2} - R_{i-1}}{P_{i-1}}$, we obtain, by induction,

$$Q_{i-1}(x', \alpha_k) \in \Bbbk(x', \alpha_1, \ldots, \alpha_d, Q_{i-2}(x', \alpha_1), \ldots, Q_{i-2}(x', \alpha_d))$$

thus

$$R_i, Q_i, P_i \in \Bbbk(x, \alpha_1, \ldots, \alpha_d, g(x', \alpha_1), \ldots, g(x', \alpha_d)) \quad \text{for all } i \tag{4.4}$$

and

$$\mathrm{Deg}(R_i), \mathrm{Deg}(Q_i), \mathrm{Deg}(r), \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^d \quad \text{for all } i$$

by Corollary 3.12. Since $q = \frac{g-r}{f}$, we have

$$q \in \Bbbk(x, \alpha_1, \ldots, \alpha_d, g(x', \alpha_1), \ldots, g(x', \alpha_d), g, f)$$

and

$$\deg(q) \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^{d+1}\,\mathrm{Deg}(f).$$

Thus the inequalities on the degrees are proven.

Let ε be a positive real number. By Lemma 4.2 the height of R_1 is bounded by

$$d_1(\mathrm{H}(P_1)!\,\mathrm{Deg}(g)^{d_1})^{d_1}(4\,\mathrm{H}(P_1)^{\mathrm{H}(P_1)^{O(d_1)}}\,\mathrm{Deg}(g)(\mathrm{H}(g)+1)+d_1-1)$$

and so we obtain

$$\mathrm{H}(R_1) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \cdot \mathrm{Deg}(g)^{d^2+1}(\mathrm{H}(g)+1) \tag{4.5}$$

by Lemma 4.4 since $\mathrm{H}(P_1) \leq 2\,\mathrm{H}(f)^{\mathrm{H}(f)+2}$ and $d_1 \leq d \leq \mathrm{H}(f)$.

By Lemma 3.6 (ii) and (vi) we have

$$\begin{aligned}
\mathrm{H}(Q_1) &= \mathrm{H}\left(\frac{g-R_1}{P_1}\right)\\
&\leq 2\,\mathrm{Deg}(P_1)\,\mathrm{Deg}(g-R_1)\max\bigl\{\mathrm{H}(P_1), 2\,\mathrm{Deg}(g)\,\mathrm{Deg}(R_1)\max\{\mathrm{H}(g),\mathrm{H}(R_1)\}\bigr\}\\
&\leq 4\,\mathrm{H}(f)!\,\mathrm{Deg}(g)^2\,\mathrm{Deg}(R_1)^2\max\bigl\{\mathrm{H}(P_1),\mathrm{H}(g),\mathrm{H}(R_1)\bigr\}
\end{aligned}$$

since $\mathrm{Deg}(P_1) \leq \mathrm{H}(f)!$ and $d \leq \mathrm{H}(f)$. Hence by Lemma 4.4 and the bound (4.5) on $\mathrm{H}(R_1)$ we obtain

$$\mathrm{H}(Q_1) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}}\,\mathrm{Deg}(g)^{d^2+2d+3}(\mathrm{H}(g)+1). \tag{4.6}$$

Still by Lemma 4.2, and as we have shown for $\mathrm{H}(R_1)$, we have

$$\mathrm{H}(R_i) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}}\,\mathrm{Deg}(Q_{i-1})^{d^2+1}(\mathrm{H}(Q_{i-1})+1), \tag{4.7}$$

and by Lemma 3.6 (ii) and (vi), and as we have done for $\mathrm{H}(Q_1)$, we have

$$\begin{aligned}
\mathrm{H}(Q_i) &\leq 2\,\mathrm{Deg}(P_i)\,\mathrm{Deg}(Q_{i-1}-R_i)\\
&\qquad\times\max\bigl\{\mathrm{H}(P_i), 2\,\mathrm{Deg}(R_i)\,\mathrm{Deg}(Q_{i-1})\max\{\mathrm{H}(R_i),\mathrm{H}(Q_{i-1})\}\bigr\}\\
&\leq 4\,\mathrm{H}(f)!\,\mathrm{Deg}(Q_{i-1})^2\,\mathrm{Deg}(R_i)^2\max\bigl\{\mathrm{H}(P_i),\mathrm{H}(Q_{i-1}),\mathrm{H}(R_i)\bigr\}\\
&\leq 4(\mathrm{H}(f)!)^5\,\mathrm{Deg}(g)^{4d}\max\bigl\{\mathrm{H}(P_i),\mathrm{H}(Q_{i-1}),\mathrm{H}(R_i)\bigr\}.
\end{aligned}$$

The previous bound (4.7) on $\mathrm{H}(R_i)$ gives

$$\mathrm{H}(Q_i) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}}\,\mathrm{Deg}(g)^{4d}\,\mathrm{Deg}(Q_{i-1})^{d^2+1}(\mathrm{H}(Q_{i-1})+1).$$

Since $d \leq \mathrm{H}(f)$, $\mathrm{Deg}(Q_i) \leq \mathrm{H}(f)!\,\mathrm{Deg}(g)^d$ for i, and by using the bound (4.6) on $\mathrm{H}(Q_1)$, we obtain by induction on i,

$$\mathrm{H}(Q_i) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}}\,\mathrm{Deg}(g)^{(d^3+d^2+4d)(i-1)+d^2+2d+3}(\mathrm{H}(g)+1) \quad \text{for all } i \geq 1.$$

Thus the bound (4.7) gives

$$\mathrm{H}(R_i) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}}\,\mathrm{Deg}(g)^{(d^3+d^2+4d)i+d^2-6d+3}(\mathrm{H}(g)+1) \quad \text{for all } i \geq 2. \tag{4.8}$$

By Lemma 3.6 (vi), for all $i \geq 2$,

$$\begin{aligned}
\mathrm{H}(P_1 \cdots P_{i-1} R_i) &\leq i \operatorname{Deg}(P_1) \cdots \operatorname{Deg}(P_{i-1}) \operatorname{Deg}(R_i) \max\{\mathrm{H}(P_1), \dots, \mathrm{H}(P_{i-1}), \mathrm{H}(R_i)\} \\
&\leq i (\mathrm{H}(f)!)^i \operatorname{Deg}(g)^d \max\{\mathrm{H}(P_1), \dots, \mathrm{H}(P_{i-1}), \mathrm{H}(R_i)\} \\
&\leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{(d^3+d^2+4d)i+d^2-5d+3}(\mathrm{H}(g)+1)
\end{aligned}$$

by (4.8). We have $P_i, R_i \in k(x, \alpha_1, \dots, \alpha_d, g(x(, \alpha_1), \dots, g(x', \alpha_d))$ for all i, then

$$\operatorname{Deg}(P_1 \cdots P_{i-1} R_i) \leq \mathrm{H}(f)! \operatorname{Deg}(g)^d \quad \text{for all } i.$$

Thus by Lemma 3.6 (ii) we obtain

$$\begin{aligned}
\mathrm{H}(r) &\leq s(\mathrm{H}(f)! \operatorname{Deg}(g)^d)^s \cdot 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{(d^3+d^2+4d)s+d^2-5d+3}(\mathrm{H}(g)+1) \\
&\leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{d^4+d^3+6d^2-5d+3}(\mathrm{H}(g)+1)
\end{aligned}$$

since $s \leq d$ and $d \leq \mathrm{H}(f)$. Thus by Lemma 3.6 (ii) and (vi),

$$\begin{aligned}
\mathrm{H}(q) &= \mathrm{H}\left(\frac{g-r}{f}\right) \\
&\leq 2 \operatorname{Deg}(g-r) \operatorname{Deg}(f) \max\{\mathrm{H}(f), 2 \operatorname{Deg}(g) \operatorname{Deg}(r) \max\{\mathrm{H}(g), \mathrm{H}(r)\}\} \\
&\leq 4 \operatorname{Deg}(g)^2 \operatorname{Deg}(r)^2 \operatorname{Deg}(f) \cdot 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{d^4+d^3+6d^2-5d+3}(\mathrm{H}(g)+1) \\
&\leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{d^4+d^3+6d^2-3d+5} \operatorname{Deg}(f)(\mathrm{H}(g)+1).
\end{aligned}$$

If we write $r(x) = r_0(x') + r_1(x')x_n + \cdots + r_{d-1}(x')x_n^{d-1}$, we have

$$r_0(x') = r(x', 0)$$

and

$$r_{i+1}(x') = \left(\frac{r - (r_0 + r_1 x_n + \cdots + r_i x_n^i)}{x_n^i}\right)(x', 0) \quad \text{for all } i \geq 0. \tag{4.9}$$

In particular, from (4.4), we have

$$r_i \in \mathbb{k}(x', \alpha_1, \dots, \alpha_d, g(x', \alpha_1), \dots, g(x', \alpha_d)) \quad \text{for all } i$$

hence $\operatorname{Deg}(r_i) \leq \mathrm{H}(f)! \operatorname{Deg}(g)^d$ for all i by Corollary 3.12.

From (4.9), Lemma 3.7 and Lemma 3.6 (ii) we obtain

$$\begin{aligned}
\mathrm{H}(r_{i+1}) &\leq \mathrm{H}\left(\frac{r - (r_0 + r_1 x_n + \cdots + r_i x_n^i)}{x_n^i}\right) \\
&= \mathrm{H}\left(\frac{r}{x_n^i} - \frac{r_0}{x_n^i} - \cdots - \frac{r_{i-1}}{x_n} - r_i\right) \\
&\leq (i+2) \operatorname{Deg}(r) \operatorname{Deg}(r_0) \cdots \operatorname{Deg}(r_i) \\
&\qquad \times \max\{\mathrm{H}(r)+i, \mathrm{H}(r_0)+i, \dots, \mathrm{H}(r_{i-1})+1, \mathrm{H}(r_i)\} \\
&\leq (d+1)(\mathrm{H}(f)! \operatorname{Deg}(g)^d)^{d+1}\big(\max\{\mathrm{H}(r), \mathrm{H}(r_0), \dots, \mathrm{H}(r_{i-1}), \mathrm{H}(r_i)\} + d\big).
\end{aligned}$$

Thus, by induction on i and using the bound on $\mathrm{H}(r)$ proven above, we see that

$$\mathrm{H}(r_i) \leq 2^{2^{O(\mathrm{H}(f)^{1+\varepsilon})}} \operatorname{Deg}(g)^{O(d^4)}(\mathrm{H}(g)+1) \quad \text{for all } i.$$

In the case $\operatorname{char}(\mathbb{k}) = p > 0$ the proof is completely similar using Lemma 4.3 instead of Lemma 4.2 so we skip the details. □

Remark 4.6. We could prove directly the Weierstrass Division Theorem from the Weierstrass Preparation Theorem as done in [7]. But this would give a bound on the height of the remainder which is not linear in $\mathrm{H}(g)$. This linear bound in $\mathrm{H}(g)$ is exactly what we need to prove Theorem 1.1.

5. Ideal membership problem in localizations of polynomial rings

Before bounding the complexity of the Ideal Membership Problem in the ring of algebraic power series we review this problem in the ring of polynomials and give extensions to localizations of the ring of polynomials that may be of independent interest.

Let $\mathbb{k}$ be a field and $x := (x_1, \dots, x_n)$. The following theorem is well known (such a result has first been proven by G. Hermann [11] but a modern and correct proof is given in the appendix of [22]):

Theorem 5.1 ([11,22]). *Let $\mathbb{k}$ be a infinite field and M a submodule of $\mathbb{k}[x]^q$ generated by vectors $f_1, \dots, f_p$ whose components are polynomials of degrees less than d. Let $f \in \mathbb{k}[x]^q$. Then $f \in M$ if and only if there exist $a_1, \dots, a_p \in \mathbb{k}[x]$ of degrees $\leq \deg(f) + (pd)^{2^n}$ such that*

$$f = a_1 f_1 + \cdots + a_p f_p.$$

If we work over the local ring $\mathbb{k}[x]_{(x)}$, the situation is a bit different. Saying that $f \in \mathbb{k}[x]^q$ is in $\mathbb{k}[x]_{(x)}M$ is equivalent to saying that there exist polynomials $a_1, \dots, a_p$ and u, $u \notin (x)$, such that

$$uf = a_1 f_1 + \cdots + a_p f_p. \tag{5.1}$$

There exists an analogue of Buchberger algorithm to compute Gröbner basis in local rings introduced by T. Mora [25] but it does not give effective bounds on the degrees of the a_i. We can also do the following: Saying that (5.1) is satisfied is equivalent to saying that there exist polynomials $a_1, \dots, a_p, b_1, \dots, b_n$ such that

$$f = a_1 f_1 + \cdots + a_p f_p + b_1 x_1 f + \cdots + b_n x_n f.$$

In this case $u = 1 - \sum_i x_i b_i$.

Thus by applying Theorem 5.1, we see that $f \in \mathbb{k}[x]_{(x)}M$ if and only if (5.1) is satisfied for polynomials $u, a_1, \dots, a_p$ of degrees $\leq \deg(f) + ((p+n)\max\{d, \deg(f)+1\})^{2^n}$. But this bound is not linear in $\deg(f)$ any more, which may be interesting if $f_1, \dots, f_p$ are fixed and f varies.

Nevertheless, we can prove the following result:

Theorem 5.2. *For any n, q and $d \in \mathbb{N}$ there exists an integer $\gamma(n,q,d)$ such that*

$$\gamma(n,q,d) = (2d)^{2^{O(n+q)}}$$

and satisfying the following: Let $\mathbb{k}$ be an infinite field, let M be a submodule of $\mathbb{k}[x_1, \dots, x_n]^q$

generated by vectors $f_1, \dots, f_p$ *of degree* $\leq d$ *and let* $f \in \mathbb{k}[x]^q$*. Let* P *be a prime ideal of* $\mathbb{k}[x]$*. Then* $f \in \mathbb{k}[x]_P M$ *if and only if there exist polynomials* $a_1, \dots, a_p$ *of degrees at most* $\deg(f) + \gamma(n, q, d)$ *and* u*,* $u \notin P$*, of degree at most* $\gamma(n, q, d)$ *such that*

$$uf = a_1 f_1 + \cdots + a_p f_p.$$

Proof. Let R be the ring defined as follows (this is the idealization of M – see [26]): the set R is equal to $\mathbb{k}[x] \times \mathbb{k}[x]^q$ and we define the sum and the product as follows:

$$(p, f) + (p', f') := (p + p', f + f')$$

and

$$(p, f).(p', f') := (pp', pf' + p'f)$$

for all $(p, f), (p', f') \in \mathbb{k}[x] \times \mathbb{k}[x]^q$. Let $I := \{0\} \times M \subset R$. Then I is an ideal of R and it is generated by $(0, f_1), \dots, (0, f_q)$. Moreover, R is isomorphic to the ring

$$R' := \mathbb{k}[x_1, \dots, x_n, y_1, \dots, y_q]/(y_1, \dots, y_q)^2$$

and the isomorphism $\sigma : R \to R'$ is defined as follows: If $(p, f) \in R$, $f := (f^{(1)}, \dots, f^{(q)})$, then $\sigma(p, f)$ is the image of $p + f^{(1)}y_1 + \cdots + f^{(q)}y_q$ in R'.

The image I by σ is an ideal of R' and we denote by I' an ideal of $\mathbb{k}[x, y]$ whose image in R' is equal to $\sigma(I)$. Thus, by identifying R and R', we have the following equivalences:

$$f \in M \iff (0, f) \in I \iff f^{(1)}(x)y_1 + \cdots + f^{(q)}(x)y_q \in I' + (y)^2.$$

Let us assume that the theorem is proven when $q = 1$. We will apply it when

$$M = I' + (y)^2$$

is an ideal of $\mathbb{k}[x, y]$. If we write $f_i = (f_{i,1}, \dots, f_{i,q})$ for $1 \leq i \leq p$, then $I' + (y)^2$ is generated by

$$\widetilde{f_1}(x, y) := \sum_{j=1}^{q} f_{1,j} y_j, \dots, \widetilde{f_p}(x, y) := \sum_{j=1}^{q} f_{p,j} y_j$$

and the $y_i y_j$ for $1 \leq i \leq j \leq q$, whose degrees are less than $d + 2$. Thus, by assumption, there exist $u(x, y)$, $a_1(x, y), \dots, a_p(x, y)$, $a_{i,j}(x, y)$ for $1 \leq i \leq j \leq$ with $u(0, 0) \neq 0$ and such that

$$u\big(f^{(1)}(x)y_1 + \cdots + f^{(q)}(x)y_q\big) = \sum_{i=1}^{p} a_i \widetilde{f_i} + \sum_{1 \leq i \leq j \leq q} a_{i,j} y_i y_j \tag{5.2}$$

and

$$\deg(a_k), \deg(a_{i,j}) \leq \deg(f) + \gamma(n + q, 1, d + 2)$$

where $\gamma(n + q, 1, d + 2) \leq (2d)^{2^{O(n+q)}}$. By identifying the coefficients of $y_1, \dots, y_q$ of both sides of equality (5.2), we obtain

$$u(x, 0) f(x) = \sum_{i=1}^{p} a_i(x, 0) f_i(x)$$

and this proves the theorem. Thus we only need to prove the theorem when $M = I$ is an ideal of $\mathbb{k}[x]$ (i.e. for $q = 1$).

Let $I = Q_1 \cap \cdots \cap Q_s$ be an irredundant primary decomposition of I in $\mathbb{k}[x]$. Let us assume that $Q_1, \ldots, Q_r \subset P$ and $Q_i \not\subset P$ for $i > r$. Then

$$I\mathbb{k}[x]_P = Q_1\mathbb{k}[x]_P \cap \cdots \cap Q_r\mathbb{k}[x]_P$$

is an irredundant primary decomposition of $I\mathbb{k}[x]_P$ in $\mathbb{k}[x]_P$ (see [33, Chapter 4, Theorem 17]). Let J be the ideal of $\mathbb{k}[x]$ defined by $J = Q_1 \cap \cdots \cap Q_r$. Obviously, $I\mathbb{k}[x]_P = J\mathbb{k}[x]_P$ and moreover for any $f \in \mathbb{k}[x]$, $f \in J\mathbb{k}[x]_P$ if and only if $f \in J$.

If $r = s$, then $I = J$ and for every $f \in \mathbb{k}[x]$, $f \in I\mathbb{k}[x]_P$ if and only if $f \in I$. So this case is exactly Theorem 5.1.

In the general case $r < s$ the problem can also be reduced to Theorem 5.1 as follows. Each ideal Q_i may be generated by polynomials of degree $\leq (2d)^{2^{O(n)}}$ and this bound depends only on n and d (see [30, Statements 63, 64 and 65]). By [30, Statement 56], the ideal J is generated by polynomials of degrees $\leq (2d)^{2^{O(n)}}$ and once more this bound depends only on n and d. Let $g_1, \ldots, g_t$ be such generators of J. Since $\deg(g_i) \leq (2d)^{2^{O(n)}}$ for any i, it follows that t will be bounded by the number of monomials in $x_1, \ldots, x_n$ of degree $\leq (2d)^{2^{O(n)}}$, thus

$$t \leq \binom{(2d)^{2^{O(n)}} + n}{n} \leq (2d)^{2^{O(n)}}$$

also.

If $f \in I\mathbb{k}[x]_P$, then $f \in J$ and by Theorem 5.1, there exist polynomials $c_1, \ldots, c_t$ such that

$$f = c_1 g_1 + \cdots + c_t g_t$$

where

$$\deg(c_i) \leq \deg(f) + (td)^{2^n} \leq \deg(f) + (2d)^{2^{O(n)}} \quad \text{for every } i.$$

Let J' be the ideal of $\mathbb{k}[x]$ equal to $Q_{r+1} \cap \cdots \cap Q_s$. Then as for J, J' is generated by polynomials of degrees $\leq (2d)^{2^{O(n)}}$. Since $J' \not\subset P$, one of these generators is not in P. Let u be such a polynomial. Then we have $ug_i \in J \cap J' = I$ for every i. Thus there exist polynomials $b_{i,j}$, for $1 \leq i \leq t$ and $1 \leq j \leq p$, such that

$$ug_i = \sum_j b_{i,j} f_j.$$

Still by Theorem 5.1, we may choose the $b_{i,j}$ such that $\deg(b_{i,j}) \leq (2d)^{2^{O(n)}}$. Hence

$$uf = \sum_j \Big(\sum_i c_i b_{i,j}\Big) f_j.$$

Then the result follows since $\deg(u) \leq (2d)^{2^{O(n)}}$ and

$$\deg\Big(\sum_i c_i b_{i,j}\Big) \leq \deg(f) + (2d)^{2^{O(n)}}. \qquad \square$$

Let S be a multiplicative closed subset of $\mathbb{k}[x]$. The proof of Theorem 5.2 gives also the following result.

Proposition 5.3. *Let $\mathbb{k}$ be an infinite field. Let M be a submodule of $\mathbb{k}[x_1,\dots,x_n]^q$ generated by the vectors $f_1,\dots,f_p$ and let S be a multiplicative closed subset of $\mathbb{k}[x]$. Then there exists a constant $C>0$ (depending only on M) such that the following holds: For any $f\in\mathbb{k}[x]^q$, $f\in S^{-1}M$ if and only if there exist polynomials $a_1,\dots,a_p$ of degrees at most $\deg(f)+C$ and u, $u\in S$, of degree at most C such that*

$$uf=a_1f_1+\cdots+a_pf_p.$$

Proof. We can adapt the proof of Theorem 5.2 as follows (we keep the same notations): the reduction to the case where $M=I$ is an ideal of $\mathbb{k}[x]$ remains the same. Then if $I=Q_1\cap\cdots\cap Q_s$ is an irredundant primary decomposition of I in $\mathbb{k}[x]$, we may assume that $Q_1,\dots,Q_r\subset\mathbb{k}[x]\setminus S$ and $Q_i\cap S\neq\emptyset$ for $i>r$. Then as before

$$I\cdot S^{-1}\mathbb{k}[x]=Q_1\cdot S^{-1}\mathbb{k}[x]\cap\cdots\cap Q_r\cdot S^{-1}\mathbb{k}[x]$$

is an irredundant primary decomposition of $I\cdot S^{-1}\mathbb{k}[x]$. If J denotes the ideal $Q_1\cap\cdots\cap Q_r$ of $\mathbb{k}[x]$, then for any $f\in\mathbb{k}[x]$, we also have

$$f\in I\cdot S^{-1}\mathbb{k}[x]=J\cdot S^{-1}\mathbb{k}[x]\iff f\in J.$$

Then we follow the proof of Theorem 5.2: if $f\in\mathbb{k}[x]$ and $f\in I\cdot S^{-1}\mathbb{k}[x]$, then $f\in J$ and there exist polynomials $c_1,\dots,c_t$ such that

$$f=c_1g_1+\cdots+c_tg_t$$

where

$$\deg(c_i)\leq\deg(f)+(td)^{2^n}\leq\deg(f)+(2d)^{2^{O(n)}}\quad\text{for any } i$$

and $g_1,\dots,g_t$ are generators of J. Moreover, the degrees of the g_i and the integer t are bounded by $(2d)^{2^{O(n)}}$.

Now the only difference with the proof of Theorem 5.2 is that $\mathbb{k}[x]\setminus S$ is not an ideal of $\mathbb{k}[x]$. So let us choose a non-zero polynomial $u\in Q_{r+1}\cap\cdots\cap Q_s\cap S$ (such a polynomial exists since S is a multiplicative system and $Q_i\cap S\neq\emptyset$ for all $i>r$) and let us denote by D its degree: $D=\deg(u)$. Then $ug_i\in I$ for every i.

Still by following the proof of Theorem 5.2 we see by Theorem 5.1 that there exist polynomials $b_{i,j}$, for $1\leq i\leq t$ and $1\leq j\leq p$, such that

$$ug_i=\sum_j b_{i,j}f_j$$

with $\deg(b_{i,j})\leq D+(2d)^{2^{O(n)}}$ for every i and j. Then

$$uf=\sum_j\Big(\sum_i c_ib_{i,j}\Big)f_j$$

and

$$\deg\Big(\sum_i c_ib_{i,j}\Big)\leq\deg(f)+D+(2d)^{2^{O(n)}}.$$

So the proposition is proven with $C=D+(2d)^{2^{O(n)}}$. □

6. Ideal membership in rings of algebraic power series

Theorem 6.1. *Let $\mathbb{k}$ be any infinite field. Then there exists two computable functions $C_1(n,q,p,H_1,D_1,D_2)$ and $C_2(n,q,p,H_1,D_1,D_2)$ such that the following holds: Let n, q, p, H_1, H_2, D_1 and D_2 be integers, and let*

$$f=(f_1,\dots,f_q),\ g_1=(g_{1,1},\dots,g_{1,q}),\dots,g_p=(g_{p,1},\dots,g_{p,q})$$

be vectors of $\mathbb{k}\langle x_1,\dots,x_n\rangle^q$ satisfying

$$\begin{aligned} \mathrm{H}(g_i)\le H_1 \quad \textit{for all } i, \quad \mathrm{H}(f)\le H_2,\\ \big[\mathbb{k}(x,g_{i,j})_{1\le i\le p,\,1\le j\le q}:\mathbb{k}(x)\big]\le D_1,\\ \big[\mathbb{k}(x,f_j)_{1\le j\le q}:\mathbb{k}(x)\big]\le D_2.\end{aligned}$$

Let us assume that f is in the $\mathbb{k}\langle x\rangle$-module generated by the vectors g_i. Then there exist algebraic power series a_i for $1\le i\le p$ such that

$$f_j=\sum_{i=1}^{p}a_i g_{i,j},\quad 1\le j\le q, \tag{6.1}$$

and

$$\begin{aligned} \mathrm{H}(a_i)&\le C_1(n,q,p,H_1,D_1,D_2)\cdot(H_2+1) && \textit{for all } i,\\ \mathrm{Deg}(a_i)&\le C_2(n,q,p,H_1,D_1,D_2) && \textit{for all } i.\end{aligned}$$

Proof. The theorem is proven by induction on n. For $n=0$ and any q, p, H_1, H_2, D_1, D_2 any solution (a_i) of (6.1) will have height equal to 0 and degree equal to 1. Let us assume that the theorem is proven for an integer $n-1\ge 0$ and any integers q, p, H_1, H_2, D_1, D_2 and let us prove it for n.

We set

$$\begin{aligned} H_g&:=\max_{i,j}\mathrm{H}(g_{i,j}), & D_g&:=\max_{i,j}\mathrm{Deg}(g_{i,j}),\\ H_f&:=\max_{j}\mathrm{H}(f_j), & D_f&:=\max_{j}\mathrm{Deg}(f_j).\end{aligned}$$

Let G be the $p\times q$ matrix whose entries are the $g_{i,j}$. We assume that the rank of G is $q\le p$ (otherwise some equations may be removed) and that the first q columns are linearly independent. Let Δ be the determinant of these first q columns. By a linear change of coordinates we may assume that Δ is x_n-regular of degree d since $\mathbb{k}$ is infinite. By Lemma 3.7, $d\le \mathrm{H}(\Delta)$. Moreover, Δ is a sum of $q!$ elements which are the product of q entries of G. Thus by Lemma 3.6 (ii) and (vi) we have

$$\mathrm{H}(\Delta)\le q!D_g^{q!}\big(qD_g^{q}H_g\big)=q!qD_g^{q!+q}H_g.$$

Of course, $\Delta\in\mathbb{k}(x,g_{i,j})_{1\le i\le p,\,1\le j\le q}$ thus

$$\mathrm{Deg}(\Delta)\le D_g.$$

By Lemma 4.1 we can write $\Delta=u\cdot P$ where u is a unit and P a Weierstrass polynomial of degree d with

$$\mathrm{H}(P)\le 2d\,\mathrm{H}(\Delta)^{d+1}\le 2\,\mathrm{H}(\Delta)^{\mathrm{H}(\Delta)+2}\le 2\big(q!qD_g^{q!+q}H_g\big)^{q!qD_g^{q!+q}H_g+2}.$$

Set

$$F_j(x,A) := \sum_{i=1}^{p} g_{i,j}(x)A_i - f_j(x) \quad \text{for all } j$$

where $A_1, \dots, A_p$ are new variables.

Let $a_{i,k}(x')$ be algebraic power series of $\Bbbk\langle x'\rangle$ for $1 \le i \le p$ and $0 \le k \le d-1$. Then let us set

$$\begin{aligned} a_i^* &:= \sum_{k=0}^{d-1} a_{i,k}(x')x_n^k \quad \text{for } 1 \le i \le p, \\ a^* &:= (a_1^*, \dots, a_p^*). \end{aligned} \tag{6.2}$$

Let $A_{i,k}$, $1 \le i \le p$, $0 \le k \le d-1$, be new variables and let us set

$$A_i^* := \sum_{k=0}^{d-1} A_{i,k}x_n^k, \quad 1 \le i \le p,$$

and

$$A^* := (A_1^*, \dots, A_p^*).$$

Let us consider the Weierstrass division of $F_j(x, A^*)$ by Δ with respect to the variable x_n:

$$F_j(x, A^*) = \Delta.Q_j(x, A^*) + R_j$$

where

$$R_j = \sum_{l=0}^{d-1} R_{j,l}(x', A^*)x_n^l.$$

Let us consider the following Weierstrass divisions:

$$g_{i,j}(x)x_n^k = \Delta.Q_{i,j,k}(x) + R_{g_{i,j}}$$

where

$$R_{g_{i,j}} = \sum_{l=0}^{d-1} R_{i,j,k,l}(x')x_n^l,$$

and

$$f_j(x) = \Delta.Q'_j(x) + R_{f_j}$$

where

$$R_{f_j} = \sum_{l=0}^{d-1} R'_{j,l}(x')x_n^l.$$

By unicity of the remainder and the quotient of the Weierstrass division we obtain

$$\begin{aligned} Q_j(x, A^*) &= \sum_{i=1}^{p}\sum_{k=0}^{d-1} Q_{i,j,k}(x)A_{i,k} - Q'_j(x), \\ R_{j,l}(x', A^*) &= \sum_{i=1}^{p}\sum_{k=0}^{d-1} R_{i,j,k,l}(x')A_{i,k} - R'_{j,l}(x'). \end{aligned} \tag{6.3}$$

Hence $Q_j(x', A^*)$ and $R_{j,l}(x', A^*)$ are linear with respect to the variables $A_{i,k}$.

If

$$R_{j,l}(x', a^*) = 0 \quad \text{for all } j \text{ and } l, \tag{6.4}$$

then $F_j(x, a^*) \in (\Delta)$ for all j. This means that there exists a vector of $\Bbbk\langle x\rangle^q$, denoted by $b(x)$, such that

$$G(x).a^*(x) - f(x) = \Delta(x).b(x) \tag{6.5}$$

where $G(x)$ is the $q \times p$ matrix with entries $g_{i,j}(x)$ and $f(x)$ is the vector with entries $f_j(x)$. In fact, we can choose $b(x)$ to be the vector of entries $Q_j(x, a^*)$.

Let $G'(x)$ be the adjoint matrix of the $q \times q$ matrix built from $G(x)$ by taking only the first q columns. Then

$$G'(x).G(x) = \begin{pmatrix} \Delta(x).\mathbb{1}_q & \star \end{pmatrix}.$$

Thus, by multiplying (6.5) by $G'(x)$ on the left-hand side, we have

$$\begin{bmatrix} \Delta(x)a_1^*(x) + P_1(a_{q+1}^*(x), \dots, a_p^*(x)) \\ \Delta(x)a_2^*(x) + P_2(a_{q+1}^*(x), \dots, a_p^*(x) \\ \vdots \\ \Delta(x)a_q^*(x) + P_q(a_{q+1}^*(x), \dots, a_p^*(x)) \end{bmatrix} - G'(x).f(x) = \Delta(x).G'(x).b(x)$$

for some P_i depending linearly on $a_{q+1}^*(x), \dots, a_p^*(x)$. Then we set

$$a_i(x) := a_i^*(x) - c_i(x) \quad \text{for } 1 \leq i \leq q, \tag{6.6}$$

$$a_i(x) := a_i^*(x) \quad \text{for } q < i \leq p \tag{6.7}$$

where $c(x)$ is the vector $G'(x).b(x)$. Since $G'(x)$ has rank q, this shows that

$$G(x).a(x) - f(x) = 0$$

i.e. $a(x)$ is a solution of (6.1).

Now we have to bound the height and the degree of $a(x)$ in terms of the height and the degree of a^*. For simplicity we will bound the height and the degree of $a(x)$ when $\mathrm{char}(\Bbbk) = 0$. The bounds in positive characteristic are obtained in the same way and they are similar (the only difference comes from Theorem 4.5 – see also Remark 6.2).

First by Lemma 3.6 (iv) we have

$$\mathrm{H}(g_{i,j}(x)x_n^k) \leq H_g + kD_g.$$

Let us remind that $d \leq \mathrm{H}(\Delta) \leq q!qD_g^{q!+q}H_g \leq q^q D_g^{q!+q} H_g$. Thus by Theorem 4.5 we have (by choosing $\varepsilon = 1$ for simplicity and since $k < d$):

$$\begin{aligned} \mathrm{H}(R_{i,j,k,l}(x')) &\leq 2^{2^{O(\mathrm{H}(\Delta)^2)}} D_g^{O(d^4)}(H_g + kD_g + 1) \\ &\leq 2^{2^{O(q^{2q}D_g^{2(q!+q)}H_g^2)}}, \\ \mathrm{H}(R'_{i,l}(x')) &\leq 2^{2^{O(\mathrm{H}(\Delta)^2)}} D_f^{O(d^4)}(H_f + 1) \\ &\leq 2^{2^{O(q^{2q}D_g^{2(q!+q)}H_g^2)}} D_f^{O(d^4)}(H_f + 1), \\ \mathrm{H}(Q_{i,j,k}(x)) &\leq 2^{2^{O(q^{2q}D_g^{2(q!+q)}H_g^2)}} D_g^{d^4+d^3+6d^2-3d+5}\,\mathrm{Deg}(\Delta)(H_g + kD_g + 1) \\ &\leq 2^{2^{O(q^{2q}D_g^{2(q!+q)}H_g^2)}}, \end{aligned}$$

$$\begin{aligned}
\mathrm{H}(Q'_j(x)) &\le 2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_f^{d^4+d^3+6d^2-3d+5}\,\mathrm{Deg}(\Delta)(H_f+1)\\
&\le 2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_f^{8d^4}(H_f+1),\\
\mathrm{Deg}(R_{i,j,k,l}(x')) &\le \mathrm{H}(\Delta)!D_g^{\mathrm{H}(\Delta)}\\
&\le (\mathrm{H}(\Delta)D_g)^{\mathrm{H}(\Delta)}\\
&\le (q!qD_g^{q!+q+1}H_g)^{q!qD_g^{q!+q}H_g}\\
&\le 2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}},\\
\mathrm{Deg}(R'_{i,l}(x')) &\le \mathrm{H}(\Delta)!D_f^{\mathrm{H}(\Delta)}\\
&\le (q!qD_g^{q!+q}D_fH_g)^{q!qD_g^{q!+q}H_g}\\
&\le (2D_f)^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}},\\
\mathrm{Deg}(Q_{i,j,k}(x)) &\le \mathrm{H}(\Delta)!D_g^{\mathrm{H}(\Delta)+1}\,\mathrm{Deg}(\Delta)\\
&\le (q!qD_g^{q!+q+1}H_g)^{q!qD_g^{q!+q}H_g+2}D_g\\
&\le 2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}},\\
\mathrm{Deg}(Q'_j(x)) &\le (q!qD_g^{q!+q}D_fH_g)^{q!qD_g^{q!+q}H_g}D_f^{q!qD_g^{q!+q}H_g}\\
&\le (2D_f)^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}}.
\end{aligned}$$

We set

$$D_{a^*} := \mathrm{Deg}(a^*), \quad H_{a^*} := \mathrm{H}(a^*).$$

By Lemma 3.6 (vi) we have

$$\begin{aligned}
\mathrm{H}(Q_{i,j,k}(x)a_{i,k}(x')) &\le 2\,\mathrm{Deg}(Q_{i,j,k}(x))D_{a^*}\max\{\mathrm{H}(Q_{i,j,k}(x')), H_{a^*}\}\\
&\le 2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_{a^*}H_{a^*}.
\end{aligned}$$

Moreover,

$$\mathrm{Deg}(Q_{i,j,k}(x)a_{i,k}(x')) \le 2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_{a^*}.$$

Since the components of $b(x)$ are the $Q_j(x,a^*)$, we obtain by (6.3) and Lemma 3.6 (ii)

$$\begin{aligned}
\mathrm{H}(b(x)) \le (pd+1)\Big(2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_{a^*}\Big)^{pd} \max_j\{\mathrm{Deg}(Q'_j(x))\}\\
\times \max\Big\{2^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_{a^*}H_{a^*}, \mathrm{H}(Q'_j(x))\Big\}.
\end{aligned}$$

Since $d \le \mathrm{H}(\Delta) \le q!qD_g^{q!+q}H_g$, we get

$$\mathrm{H}(b(x)) \le (2^{p+1}D_f)^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_{a^*}^{pd+1}\max\{H_{a^*}, (H_f+1)\}. \tag{6.8}$$

Moreover, (6.3) gives

$$\mathrm{Deg}(b(x)) \le (2^{p+1}D_f)^{2^{O(q^{2q} D_g^{2(q!+q)} H_g^2)}} D_{a^*}. \tag{6.9}$$

We have

$$\mathrm{H}(\Delta) \leq q.q!D_g^{q!+q}H_g$$

and, by Lemma 3.6 (ii) and (vi) the height any $(q-1)\times(q-1)$ minor of G is bounded by

$$(q-1)!D_g^{(q-1)!}((q-1)D_g^{q-1}H_g) \leq q.q!D_g^{q!+q}H_g.$$

Thus, by Lemma 3.6 (vi), the height of the coefficients of $G'(x)$ is less than

$$2D_g^2 q.q!D_g^{q!+q}H_g = 2q!qD_g^{q!+q+2}H_g.$$

Hence, by Lemma 3.6 (ii) and (vi), using (6.8), (6.9) and since $\mathrm{Deg}(G'(x)) \leq D_g$ we obtain

$$\begin{aligned}\mathrm{H}(G'(x).b(x)) &\leq q(\mathrm{Deg}(G'(x))\,\mathrm{Deg}(b(x)))^q \\ &\qquad\times\big(2\,\mathrm{Deg}(G'(x))\,\mathrm{Deg}(b(x))\max\{\mathrm{H}(G'(x)),\mathrm{H}(b(x))\}\big) \\ &\leq (2^{p+1}D_f)^{2^{O(q^{2q}D_g^{2(q!+q)}H_g^2)}} D_{a^*}^{q+pd+1}\max\{H_{a^*},(H_f+1)\}.\end{aligned}$$

Hence, by (6.6) and Lemma 3.6 (ii)

$$\mathrm{H}(a(x)) \leq (2D_f+2^p)^{2^{O(q^{2q}D_g^{2(q!+q)}H_g^2)}} D_{a^*}^{2H_g p+3}\max\{H_{a^*},(H_f+1)\}.$$

Moreover,

$$\mathrm{Deg}(a(x)) \leq D_{a^*}\,\mathrm{Deg}(b(x)) \leq (2^{p+1}D_f)^{2^{O(q^{2q}D_g^{2(q!+q)}H_g^2)}} D_{a^*}^2.$$

Let

$$\Phi := q^{2q}D_g^{2(q!+q)}H_g^2.$$

By the inductive assumption we can find a solution $a'(x') = (a_{i,k}(x'))_{1\leq i\leq p,\ 0\leq k\leq d-1}$ of the system (6.4) such that

$$\mathrm{H}(a'(x')) \leq C_1\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_f)^{2^{O(\Phi)}}\Big)\cdot D_f^{O(\Phi^2)}2^{2^{O(\Phi)}}(H_f+1)$$

and

$$\mathrm{Deg}(a'(x')) \leq C_2\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_f)^{2^{O(\Phi)}}\Big).$$

Since

$$D_{a^*} \leq \mathrm{Deg}(a'(x'))$$

and

$$H_{a^*} \leq d\cdot\mathrm{Deg}(a'(x'))^d(\mathrm{H}(a'(x'))+d-1)$$

by (6.2) and Lemma 3.6 (ii), the solution $a(x)$ of (6.1) satisfies

$$\begin{aligned}\mathrm{H}(a(x)) \leq (2D_f+2^p)^{2^{O(\Phi)}} &C_2\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_f)^{2^{O(\Phi)}}\Big)^{2H_g p+3} \\ &\times C_1\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_f)^{2^{O(\Phi)}}\Big)\cdot D_f^{O(\Phi^2)}2^{2^{O(\Phi)}}(H_f+1)\end{aligned}$$

and

$$\mathrm{Deg}(a(x)) \leq (2^{p+1}D_f)^{2^{O(\Phi)}} C_2\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_f)^{2^{O(\Phi)}}\Big)^2.$$

Then with

$$\begin{aligned}
\Phi &= q^{2q} D_1^{2(q!+q)} H_1^2,\\
C_1(n,q,p,H_1,D_1,D_2) &= (2D_2+2^p)^{2^{O(\Phi)}}\\
&\quad \times C_2\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_2)^{2^{O(\Phi)}}\Big)^{2H_1p+3}\\
&\quad \times C_1\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_2)^{2^{O(\Phi)}}\Big)\\
&\quad \times D_2^{O(\Phi^2)} 2^{2^{O(\Phi)}},\\
C_2(n,q,p,H_1,D_1,D_2) &= (2^{p+1}D_2)^{2^{O(\Phi)}} C_2\Big(n-1, qd, pd, 2^{2^{O(\Phi)}}, 2^{2^{O(\Phi)}}, (2D_2)^{2^{O(\Phi)}}\Big)^2
\end{aligned}$$

the result is proven. □

Remark 6.2. The proof of this result does not give a nice bound on the two functions $C_1(n,q,p,H_1,D_1,D_2)$ or $C_2(n,q,p,H_1,H_2,D_1,D_2)$. One can check that the function $C_2(n,q,p,H_1,H_2,D_1,D_2)$ is bounded by a tower of exponentials of length $2n+1$ of the form

$$(2^{p+1}D_2)^{2^{2^{\cdot^{\cdot^{\cdot^{O(qD_1H_1)}}}}}}.$$

For $C_1(n,q,p,H_1,D_1,D_2)$ we obtain the same kind of bound.

In positive characteristic, the bounds are more complicated and are not polynomial in D_2 since the bounds on the complexity of the Weierstrass division are not polynomial in D_2.

7. Proof of Theorem 1.1

In this section we will denote by R_n the ring of algebraic power series in n variables over a field $\Bbbk$ and $\widehat{R}_n$ its $(x_1,\dots,x_n)$-adic completion. If $\Bbbk$ is a finite field, we replace $\Bbbk$ by $\Bbbk(t)$ where t is transcendental over $\Bbbk$ – this does not change the problem. Thus we may assume that $\Bbbk$ is infinite.

For any $\Bbbk\langle x\rangle$-module M, we have

$$\operatorname{ord}_M(m) = \operatorname{ord}_{\widehat{M}}(m) \quad \text{for all } m \in M,$$

thus we may assume that M is equal to R_n^s/N for some R_n-submodule N of R_n^s.

We set $e := (e_1,\dots,e_s)$ where the $e_1,\dots,e_s$ is the canonical basis of R_n^s. Let us assume that N is generated by $L_1(e),\dots,L_l(e)$ where

$$L_i(e) = \sum_{j=1}^{s} l_{i,j} e_j \quad \text{for } 1 \le i \le l,$$

and let H (resp. D) be a bound on the height (resp. the degree) of the $l_{i,j}$.

The proof is done by a double induction on s and n. Let

$$f = f_1e_1 + \cdots + f_se_s \in R_n^s \setminus N.$$

We consider the following cases.

Case (1). If $s = 1$ and $N = (0)$, then $M = R_n$ and in this case

$$\mathrm{ord}_M(f) = \mathrm{ord}_{R_n}(f) \leq \mathrm{H}(f)$$

for any algebraic power series f by Lemma 3.7.

Case (2). Assume that $s = 1$ and $N \neq (0)$ is an ideal of R_n. After a linear change of variables there exists a Weierstrass polynomial $g(x) \in N$ with respect to x_n, whose coefficients are in R_{n-1}, of degree d in x_n. Then M is isomorphic to R_{n-1}^d/N' for some submodule N' of R_{n-1}^d. The isomorphism $M \simeq R_{n-1}^d/N'$ is induced by the morphism $R_n \to R_{n-1}^d$ sending a power series $f(x) \in R_n$ onto $(r_0, \dots, r_{d-1})$ where

$$r = r_0 + r_1 x_n + \cdots + r_{d-1} x_n^{d-1}$$

is the remainder of the Weierstrass division of $f(x)$ by $g(x)$. Then N' is the R_{n-1}-submodule of R_{n-1}^d generated by the vectors of coefficients of the remainders of the Weierstrass division of the elements of M by $g(x)$.

If $f(x) \in R_n$, the remainder r of the division of f by g has height less than $C_1 \cdot (\mathrm{H}(f)+1)$ for some $C_1 > 0$ depending only on $g(x)$ and $\mathrm{Deg}(f)$ (by Theorem 4.5 – moreover C_1 is polynomial in $\mathrm{Deg}(f)$ when $\mathrm{char}(\mathbb{k}) = 0$). We remark that f and r have the same image in M. If $r = r_0 + r_1 x_n + \cdots + r_{d-1} x_n^{d-1}$, with $r_i \in R_{n-1}$ for all i, then $(r_0, r_1, \dots, r_{d-1})$ has height less that $C_1 \cdot (\mathrm{H}(f) + 1)$ again by Theorem 4.5. Moreover, $\mathrm{ord}_M(f) = \mathrm{ord}_M(r)$. Since x_n is integral over R_{n-1}, there exists a constant $a > 0$ such that $x_n^a \in (x')$, with $x' = (x_1, \dots, x_{n-1})$. Thus $(x)^{ac} \subset (x')^c$ for any integer c. So we have

$$\begin{aligned}\mathrm{ord}_{R_{n-1}^d/N'}(r) &= \sup\{c \in \mathbb{N} : r \in (x')^c R_{n-1}^d/N'\} \\ &\geq \frac{1}{a+1} \mathrm{ord}_M(r).\end{aligned}$$

By the induction hypothesis on n there exists a constant $C > 0$ such that

$$\mathrm{ord}_{R_{n-1}^d/N'}(r) \leq C \cdot \mathrm{H}(r) \quad \text{for all } r \in R_{n-1}^d.$$

Thus we have

$$\begin{aligned}\mathrm{ord}_M(f) &= \mathrm{ord}_M(r) \\ &\leq (a+1)\,\mathrm{ord}_{R_{n-1}^d/N'}(r) \\ &\leq (a+1)C\ \mathrm{H}(r) \\ &\leq (a+1)CC_1\,(\mathrm{H}(f)+1).\end{aligned}$$

If $\mathrm{char}(\mathbb{k}) = 0$ and C is assumed to depend polynomially on $\mathrm{Deg}(r)$ by the induction hypothesis, then $(a+1)CC_1$ depends polynomially on $\mathrm{Deg}(f)$ by Theorem 4.5.

Case (3). Assume that $s \geq 2$ and f_s is in the ideal of R_n generated by $l_{1,s}, \dots, l_{\kappa,s}$. Then we can write

$$f_s = a_1 l_{1,s} + \cdots + a_\kappa l_{\kappa,s}$$

where the a_i are algebraic power series with $\mathrm{H}(a_i) \leq C_2 \cdot (\mathrm{H}(f_s) + 1)$ for all i and $C_2 > 0$ depends only on the $l_{i,s}$ and $\mathrm{Deg}(f_s)$ (by Theorem 6.1). Moreover, when $\mathrm{char}(\mathbb{k}) = 0$, the function C_2 depends polynomially on $\mathrm{Deg}(f_s) \leq \mathrm{Deg}(f)$ by Remark 6.2. Let us set

$$f' := f - \sum_{i=1}^{\kappa} a_i L_i(e).$$

Set $N' = N \cap (R_n^{s-1} \times \{0\})$. We denote by M' the submodule of M equal to $(R_n^{s-1} \times \{0\})/N'$. By the Artin–Rees Lemma there exists a constant $c_0 > 0$ such that

$$(x)^{c+c_0} M \cap M' \subset (x)^c M' \quad \text{for all } c \in \mathbb{N}.$$

Hence we have

$$\mathrm{ord}_M(f) = \mathrm{ord}_M(f') \leq \mathrm{ord}_{M'}(f') + c_0.$$

By the induction hypothesis on s, there exists a constant $C' > 0$ depending on $\mathrm{Deg}(f')$ (thus on $\mathrm{Deg}(f)$ by Theorem 6.1) such that

$$\mathrm{ord}_{M'}(f') \leq C' \cdot \mathrm{H}(f').$$

If $\mathrm{char}(\Bbbk) = 0$ and we assumed that C' depends polynomially on $\mathrm{Deg}(f')$ by the induction hypothesis, then C' depends polynomially on $\mathrm{Deg}(f)$ by Remark 6.2. Hence

$$\begin{aligned}\mathrm{ord}_M(f) &\leq \mathrm{ord}_{M'}(f') + c_0 \\ &\leq C' \cdot \mathrm{H}(f') + c_0 \\ &\leq (C' + c_0)\,\mathrm{H}(f')\end{aligned}$$

and $C' + c_0$ depends polynomially on $\mathrm{Deg}(f)$ in characteristic zero.

Case (4). Assume that $s \geq 2$ and f_s is not in the ideal of R_n generated by $l_{1,s}, \ldots, l_{\kappa,s}$. Then by the case $s = 1$, there exists a constant $C > 0$ depending only on the $l_{i,s}$ and $\mathrm{Deg}(f_s)$ such that

$$\mathrm{ord}_{R_n}(f_s + a_1 l_{1,s} + \cdots + a_\kappa l_{\kappa,s}) \leq C \cdot \mathrm{H}(f_s) \quad \text{for every } a_i \in R_n.$$

Moreover, C depends polynomially on $\mathrm{Deg}(f_s) \leq \mathrm{Deg}(f)$ when $\mathrm{char}(\Bbbk) = 0$. Let us remark that for every $f \in R_n^s$ we have

$$\begin{aligned}\mathrm{ord}_M(f) &= \sup\{k : f \in (x)^k M\} \\ &= \sup\{k : f \in (x)^k R_n^s \text{ modulo } N\} \\ &= \sup\{k : \text{there are } a_1, \ldots, a_\kappa \in R_n,\ f + a_1 L_1(e) + \cdots + a_\kappa L_\kappa(e) \in (x)^k R_n^s\} \\ &= \sup_{a_1,\ldots,a_\kappa \in R_n} \{\mathrm{ord}_{R_n^s}(f + a_1 L_1(e) + \cdots + a_\kappa L_\kappa(e))\}.\end{aligned}$$

Thus

$$\mathrm{ord}_M(f) \leq \sup_{a_1,\ldots,a_\kappa \in R_n} \{\mathrm{ord}_{R_n}(f_s + a_1 l_{1,s} + \cdots + a_\kappa l_{\kappa,s})\} \leq C \cdot \mathrm{H}(f_s) \leq C \cdot \mathrm{H}(f)$$

since

$$\mathrm{ord}_{R_n^s}(g) = \min_{i=1,\ldots,s} \{\mathrm{ord}_{R_n}(g_i)\} \leq \mathrm{ord}_{R_n}(g_s)$$

for every $g = (g_1, \ldots, g_s) = g_1 e_1 + \cdots + g_s e_s \in R_n^s$.

8. Proof of Theorem 1.3

Let I be an ideal of $\widehat{R}_n$. We set $J := I \cap \mathbb{k}[x]$. We have the following lemma.

Lemma 8.1. *We have* $\mathrm{ht}(I) \geq \mathrm{ht}(J)$ *and if I is generated by algebraic power series, then* $\mathrm{ht}(I) = \mathrm{ht}(J)$. *On the other hand, if I is the intersection of a finite number of ideals which are powers of prime ideals of the same heights, i.e.*

$$I = P_1^{n_1} \cap \cdots \cap P_l^{n_l} \quad \textit{for some primes } P_i \textit{ with } \mathrm{ht}(P_i) = \mathrm{ht}(P_j) \textit{ for all } i, j,$$

then the equality $\mathrm{ht}(I) = \mathrm{ht}(J)$ *implies that I is generated by algebraic power series.*

Proof. We have

$$I = \mathbb{k}[\![x]\!] \iff J = \mathbb{k}[x].$$

Thus we may assume that I and J are proper ideals. In this case $J \subset (x)\mathbb{k}[x]$ so

$$\mathrm{ht}(J) = \mathrm{ht}(J\mathbb{k}[x]_{(x)}).$$

Since the morphism $\mathbb{k}[x]_{(x)} \to \mathbb{k}[\![x]\!]$ is faithfully flat, we have

$$\mathrm{ht}(J\mathbb{k}[x]_{(x)}) = \mathrm{ht}(J\mathbb{k}[\![x]\!]).$$

Then $\mathrm{ht}(J) \leq \mathrm{ht}(I)$ because $J\mathbb{k}[\![x]\!] \subset I$.

Let us assume that I is generated by algebraic power series. By Noetherianity there exists a finite number of algebraic power series $a_1, \ldots, a_r \in \mathbb{k}\langle x\rangle$ that generate I. Since $\mathbb{k}\langle x\rangle$ is the Henselization of $\mathbb{k}[x]_{(x)}$, there exists an étale map $\mathbb{k}[x]_{(x)} \to A$ where A is a local ring such that $\mathbb{k}[x]_{(x)} \to \mathbb{k}\langle x\rangle$ factors through $\mathbb{k}[x]_{(x)} \to A$ and $a_1, \ldots, a_r$ are images of elements $a'_1, \ldots, a'_r \in A$. By the faithful flatness of $A \to \mathbb{k}\langle x\rangle$ we have

$$\mathrm{ht}((a'_1, \ldots, a'_r) \cdot A) = \mathrm{ht}(I).$$

Since the morphism $\mathbb{k}[x]_{(x)}/J \to A/(a'_1, \ldots, a'_r)$ is a localization of a finite injective morphism, we get

$$\dim(\mathbb{k}[x]_{(x)}/J) = \dim(A/(a'_1, \ldots, a'_r) \cdot A),$$

so

$$\mathrm{ht}(J) = \mathrm{ht}((a'_1, \ldots, a'_r) \cdot A) = \mathrm{ht}(I).$$

Now we assume that $\mathrm{ht}(I) = \mathrm{ht}(J)$. First we consider the case where I is a prime ideal. Then J is also a prime ideal. If $\mathrm{ht}(J) = \mathrm{ht}(I)$, then $\mathrm{ht}(J\mathbb{k}[\![x]\!]) = \mathrm{ht}(I)$ and since $J\mathbb{k}[\![x]\!] \subset I$, then I is a prime associated to $J\mathbb{k}[\![x]\!]$. Since the ideal J is radical, it follows that $J\mathbb{k}\langle x\rangle$ is also a radical ideal: indeed, since $\mathbb{k}[x]/J$ is reduced, its completion $\mathbb{k}[\![x]\!]/J\mathbb{k}[\![x]\!]$ is also reduced (see [14, p. 180, (1)]) so $\mathbb{k}\langle x\rangle/J\mathbb{k}\langle x\rangle$ is reduced. If $J\mathbb{k}\langle x\rangle = P'_1 \cap \cdots \cap P'_r$ is a prime decomposition of $J\mathbb{k}\langle x\rangle$, then the ideals $P'_i\mathbb{k}[\![x]\!]$ are prime ideals by [18, Lemma 5.1] so

$$J\mathbb{k}[\![x]\!] = P'_1\mathbb{k}[\![x]\!] \cap \cdots \cap P'_r\mathbb{k}[\![x]\!]$$

is a prime decomposition of $J\mathbb{k}[\![x]\!]$ and I is equal to one of the $P'_i\mathbb{k}[\![x]\!]$, let us say $P'_1\mathbb{k}[\![x]\!] = I$. In particular, I is generated by algebraic power series.

Now let us assume that $I = P_1 \cap \cdots \cap P_l$ where the P_i are prime ideals of the same height. Let $J_i := P_i \cap \mathbb{k}[x]$. Then $J = J_1 \cap \cdots \cap J_l$. Since

$$\mathrm{ht}(J) \leq \mathrm{ht}(J_i) \leq \mathrm{ht}(P_i) = \mathrm{ht}(I) = \mathrm{ht}(J) \quad \text{for every } i,$$

we have $\mathrm{ht}(J_i) = \mathrm{ht}(P_i)$ for all i, thus P_i is generated by algebraic power series by the previous case, thus I is also generated by algebraic power series.

Finally, let us assume that $I = P_1^{n_1} \cap \cdots \cap P_l^{n_l}$ where the P_i are prime ideals of the same height and the n_i are positive integers. Let us set $J_i = P_i \cap \mathbb{k}[x]$. Then $P_i^{n_i} \cap \mathbb{k}[x]$ is an ideal containing $J_i^{n_i}$ whose radical is J_i. So $\sqrt{J} = J_1 \cap \cdots \cap J_l$. Since

$$\mathrm{ht}(\sqrt{J}) = \mathrm{ht}(J) = \mathrm{ht}(I) = \mathrm{ht}(\sqrt{I}),$$

it follows that $\sqrt{I}$ is generated by algebraic power series by the previous case. Thus the associated primes ideals of $\sqrt{I}$, i.e. the P_i, are generated by algebraic power series. Hence the $P_i^{n_i}$ are generated by algebraic power series and I also. □

From now on we assume that

$$I = P_1^{n_1} \cap \cdots \cap P_l^{n_l} \quad \text{for some primes } P_i \text{ with } \mathrm{ht}(P_i) = \mathrm{ht}(P_j) \text{ for all } i, j$$

and R denotes the ring $\mathbb{k}[\![x]\!]/I$.

Let $\mathbb{k}[x]_d$ be the set of polynomials of degree $\leq d$ and $J_d := J \cap \mathbb{k}[x]_d$ for every integer d. We set for every integer $d \geq 0$,

$$\Phi(d) := \dim_{\mathbb{k}}(\mathbb{k}[x]_d / J_d).$$

The function $d \mapsto \Phi(d)$ coincides with a polynomial function of degree

$$p := \dim(\mathbb{k}[x]/J) = n - \mathrm{ht}(J)$$

for d large enough. Then we define for every integer $d \geq 0$,

$$\Psi(d) := \dim_{\mathbb{k}}(R/(x)^d).$$

The function $d \mapsto \Psi(d)$ coincides with a polynomial function of degree

$$q := \dim(R) = n - \mathrm{ht}(I)$$

for d large enough. So $\Psi(d^p)$ and $\Phi(d^q)$ are polynomial functions of same degree (equal to pq) for d large enough. By choosing $a > 0$ large enough the leading coefficient of $\Phi(ad^q)$ will be strictly greater than the leading coefficient of $\Psi(d^p)$. Thus for such a constant $a > 0$ we have

$$\Psi(d^p) < \Phi(ad^q) \quad \text{for all } d \gg 0.$$

This means that the canonical $\mathbb{k}$-linear map

$$\mathbb{k}[x]_{ad^q}/J_{ad^q} \to R/(x)^{d^p}$$

is not injective for d large enough. For every d large enough let p_d be a non-zero element of the kernel of this map. By assumption there exists a constant C such that

$$\mathrm{ord}_R(p_d) \leq C \cdot \deg(p_d) \leq Cad^q \quad \text{for all } d.$$

Since p_d is in the kernel of the previous $\mathbb{k}$-linear map, we have $\mathrm{ord}_R(p_d) \geq d^p$, thus

$$Cad^q \geq d^p.$$

But such an inequality is satisfied (for some constant $a > 0$) if and only if $q \geq p$, i.e. if $\dim(R) \geq \dim(\Bbbk[x]/J)$. This last inequality is equivalent to $\mathrm{ht}(I) \leq \mathrm{ht}(J)$. Thus, by Lemma 3.10, such an inequality is satisfied if and only if $\mathrm{ht}(I) = \mathrm{ht}(J)$, i.e. if and only if I is generated by algebraic power series. This proves Theorem 1.3.

9. An example

In this section we show through an example that Lemma 8.1 and Theorem 1.3 are not true in general.

Let $\Bbbk = \mathbb{C}$ and $n = 3$. For simplicity we denote the variables x_1, x_2, x_3 by x, y, z. We set

$$f(z) := -\log(1-z) = \sum_{k\geq 1} \frac{1}{k} z^k.$$

Let $Q = (x,y)^2 = (x^2, y^2, xy)$ and $Q' = Q + (x + f(z)y)$ be ideals of $\mathbb{C}[\![x,y,z]\!]$. Then

$$\sqrt{Q} = \sqrt{Q'} = (x,y).$$

Claim 1. *The ideal Q' is not generated by algebraic power series but*

$$\mathrm{ht}(Q' \cap \mathbb{C}[x,y,z]) = \mathrm{ht}(Q') = 2.$$

We have $(x,y)^2 = Q \subsetneq Q'$ since $x + f(z)y \notin (x,y)^2$, but there is no algebraic power series $g(x,y,z)$ such that

$$x + f(z)y = g(x,y,z) \text{ modulo } Q.$$

Indeed, if it were the case, by replacing x^2, y^2 and xy by zero in the expansion of g, we would find an algebraic power series $h(z)$ such that

$$x + f(z)y = x + h(z)y$$

which is not possible since $f(z)$ is transcendental. So $Q' \cap \mathbb{C}[x,y,z] = (x,y)^2$ and Q' is not generated by algebraic power series. Since $(x,y)^2 \subset Q' \subset (x,y)$, we have

$$\mathrm{ht}(Q') = 2 = \mathrm{ht}((x,y)^2) = \mathrm{ht}(Q' \cap \mathbb{C}[x,y,z]).$$

This proves the claim.

Claim 2. *The ideal $A' = \mathbb{C}[\![x,y,z]\!]/Q'$ satisfies the local zero estimate* (1.2) *of Corollary* 1.2*:*

$$\mathrm{ord}_{A'}(p) \leq 2\deg(p) \quad \textit{for all } p \in \mathbb{C}[x,y,z] \setminus Q'. \tag{9.1}$$

Since $Q \subset Q' \subset (x,y)$, we have the canonical quotient morphisms

$$A := \mathbb{C}[\![x,y,z]\!]/Q \to A' := \mathbb{C}[\![x,y,z]\!]/Q' \to B := \mathbb{C}[\![x,y,z]\!]/(x,y).$$

We consider two cases.

Case (a). If p is a polynomial of $\mathbb{k}[x,y,z]$, $p \notin (x,y)$, we have $\operatorname{ord}_{A'}(p) \leq \operatorname{ord}_{B}(p)$. But we claim that $\operatorname{ord}_B(p) \leq \deg(p)$. Indeed, let $f \in \mathbb{C}[\![x,y,z]\!]$ be equal to p modulo (x,y). Since $p \notin (x,y)$, it follows that p has a non-zero monomial of the form az^k for some $a \in \mathbb{C}$ and $k \leq \deg(p)$. Since $f - p \in (x,y)$, we obtain that f has also a non-zero monomial az^k. So $\operatorname{ord}_{\mathbb{C}[\![x,y,z]\!]}(f) \leq k$. Thus we have

$$\operatorname{ord}_{A'}(p) \leq \deg(p) \quad \text{for all } p \in \mathbb{C}[x,y,z] \setminus (x,y). \tag{9.2}$$

Case (b). Now let p be a polynomial with $p \in (x,y)$ but $p \notin Q'$. In particular, $p \neq 0$. Then there exists a unique polynomial p' of the form

$$p' = a(z)x + b(z)y$$

where $a(z), b(z) \in \mathbb{k}[z]$, $\deg(p') \leq \deg(p)$ and

$$p' \equiv p \text{ modulo } Q.$$

Let n be an integer such that $n+1 \leq \operatorname{ord}_{A'}(p) = \operatorname{ord}_{A'}(p')$. This means that

$$p' \in (x,y,z)^{n+1} + (x,y)^2 + (x + f(z)y),$$

thus

$$p' = \varepsilon + \eta + c \cdot (x + f(z)y)$$

for some $\varepsilon \in (x,y,z)^{n+1}$, $\eta \in (x,y)^2$ and $c \in \mathbb{C}[\![x,y,z]\!]$, . Since $p' = a(z)x + b(z)y$, we obtain

$$\begin{aligned} (a(z) - c(0,0,z))x + (b(z) - c(0,0,z)f(z))y \\ = \eta + (c - c(0,0,z))(x + f(z)y) + \varepsilon. \end{aligned} \tag{9.3}$$

But $\eta' := \eta + (c - c(0,0,z))(x + f(z)y) \in (x,y)^2$. Moreover, ε can be written as

$$\varepsilon = \varepsilon'(x,y,z) + \varepsilon_x(z)x + \varepsilon_y(z)y + \varepsilon_1(z)$$

where $\varepsilon'(x,y,z) \in (x,y)^2$, $\varepsilon_x(z), \varepsilon_y(z) \in (z)^n\mathbb{C}[\![z]\!]$, $\varepsilon_1(z) \in (z)^{n+1}\mathbb{C}[\![z]\!]$. Thus (9.3) shows that

$$a(z) - c(0,0,z) = \varepsilon_x, \quad b(z) - c(0,0,z)f(z) = \varepsilon_y(z), \quad \eta' + \varepsilon' = 0, \quad \varepsilon_1(z) = 0.$$

This proves that if $\operatorname{ord}_{A'}(p) \geq n+1$, then there exists $c(z) \in \mathbb{C}[\![z]\!]$ such that

$$\operatorname{ord}_z(a(z) - c(z)) \geq n \quad \text{and} \quad \operatorname{ord}_z(b(z) - c(z)f(z)) \geq n.$$

Let us write

$$a(z) = \sum_k a_k z^k, \quad b(z) = \sum_k b_k z^k, \quad c(z) = \sum_k c_k z^k.$$

If $\deg(p) \leq d$ for some integer d, then $\deg(a), \deg(b) \leq d-1$ thus

$$a_k = b_k = 0 \quad \text{for all } k \geq d.$$

Since $\operatorname{ord}_z(a(z) - c(z)) \geq n$, we obtain

$$a_k = c_k \quad \text{for all } k < n.$$

In particular, if $d < n$, we have

$$b_d = \cdots = b_{n-1} = c_d = \cdots = c_{n-1} = 0.$$

Since $\operatorname{ord}_z(b(z) - c(z)f(z)) \geq n$, it follows that

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 1 & 0 & 0 & 0 \\ \vdots & \vdots & \dots & \dots & \vdots \\ \frac{1}{n-1} & \frac{1}{n-2} & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{bmatrix}.$$

There are two cases to be considered: either $\operatorname{ord}_{A'}(p) \leq \deg(p)$ and the local zero estimate (9.1) is satisfied, or $\operatorname{ord}_{A'}(p) > \deg(d)$. In the latter case we can choose $n \geq d$. In particular,

$$\begin{bmatrix} \frac{1}{d} & \frac{1}{d-1} & \frac{1}{d-2} & \cdots & 1 \\ \frac{1}{d+1} & \frac{1}{d} & \cdots & \cdots & \frac{1}{2} \\ \vdots & \vdots & \dots & \dots & \vdots \\ \frac{1}{n-1} & \frac{1}{n-2} & \cdots & \cdots & \frac{1}{n-d} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{bmatrix} = \begin{bmatrix} cb_d \\ b_{d+1} \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{9.4}$$

Let us assume that the local zero estimate (9.1) is not satisfied, i.e. $\operatorname{ord}_{A'}(p) > 2\deg(p)$. Then we can choose $n = 2d$. But for $n = 2d$ the matrix

$$\begin{bmatrix} \frac{1}{d} & \frac{1}{d-1} & \cdots & 1 \\ \frac{1}{d+1} & \frac{1}{d} & \cdots & \frac{1}{2} \\ \vdots & \vdots & \dots & \vdots \\ \frac{1}{2d-1} & \frac{1}{2d-2} & \cdots & \frac{1}{d} \end{bmatrix}$$

is a Hilbert matrix and is not singular. This means that equation (9.4) for $n = 2d$ has no non-trivial solution, hence $c_0 = \cdots = c_{n-1} = 0$. This proves that $a_k = b_k = 0$ for every k which contradicts the assumption that $p \neq 0$. This proves that for every polynomial $p \in \mathbb{C}[x, y, z]$, $p \notin Q'$, we have

$$\operatorname{ord}_{A'}(p) \leq 2\deg(p). \tag{9.5}$$

10. Grauert–Hironaka–Galligo division of power series

Let λ be a linear form on $\mathbb{R}^n$ with positive coefficients. Let us consider the following order on $\mathbb{N}^n$: for all $\alpha, \beta \in \mathbb{N}^n$, we say that $\alpha \leq \beta$ if

$$(\lambda(\alpha), \alpha_1, \dots, \alpha_n) \leq_{\text{lex}} (\lambda(\beta), \beta_1, \dots, \beta_n)$$

where $\leq_{\text{lex}}$ is the lexicographic order. This order induces an order on the set of monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$: we set $x^\alpha \leq x^\beta$ if $\alpha \leq \beta$. This order is called the *monomial order induced by* λ. If

$$f := \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha \in \Bbbk[\![x]\!],$$

the *initial exponent* of f with respect to the previous order is

$$\exp(f) := \min\{\alpha \in \mathbb{N}^n : f_\alpha \neq 0\} = \inf \mathrm{Supp}(f)$$

where the *support* of f is

$$\mathrm{Supp}(f) := \{\alpha \in \mathbb{N}^n : f_\alpha \neq 0\}.$$

The *initial term* of f is $f_{\exp(f)} x^{\exp(f)}$ and is denoted by $\mathrm{in}(f)$. This is the smallest non-zero monomial in the expansion of f with respect to the previous order.

Let $g_1, \dots, g_s$ be elements of $\Bbbk[\![x]\!]$. Set

$$\Delta_1 := \exp(g_1) + \mathbb{N}^n$$

and

$$\Delta_i = (\exp(g_i) + \mathbb{N}^n) \setminus \bigcup_{1 \leq j < i} \Delta_j \quad \text{for } 2 \leq i \leq s.$$

Finally, set

$$\Delta_0 := \mathbb{N}^n \setminus \bigcup_{i=1}^{s} \Delta_i.$$

We have the following theorem:

Theorem 10.1 ([8, 9, 13]). *Set $f \in \Bbbk[\![x]\!]$. Then there exist some unique power series $q_1, \dots, q_s, r \in \Bbbk[\![x]\!]$ such that*

$$f = g_1 q_1 + \cdots + g_s q_s + r$$

and

$$\exp(g_i) + \mathrm{Supp}(q_i) \subset \Delta_i \quad \text{and} \quad \mathrm{Supp}(r) \subset \Delta_0.$$

The power series r is called the remainder *of the division of f by $g_1, \dots, g_s$ with respect to the given monomial order. Moreover, if $\Bbbk$ is a valued field and f, $g_1, \dots, g_s$ are convergent power series, then the q_i and r are convergent power series.*

The uniqueness of the division comes from the fact the Δ_i are disjoint subsets of $\mathbb{N}^n$. The existence of such decomposition in the formal case is proven through the division algorithm:

Division Algorithm. Set $\alpha := \exp(g)$. Then there exists an integer i_1 such that $\alpha \in \Delta_{i_1}$.

- If $i_1 = 0$, then set $r^{(1)} := \mathrm{in}(g)$ and $q_i^{(1)} := 0$ for any i.
- If $i_1 \geq 1$, then set $r^{(1)} := 0$, $q_i^{(1)} := 0$ for $i \neq i_1$ and $q_{i_1}^{(1)} := \frac{\mathrm{in}(g)}{\mathrm{in}(g_{i_1})}$.

Finally, set

$$g^{(1)} := g - \sum_{i=1}^{s} g_i q_i^{(1)} - r^{(1)}.$$

Thus we have $\exp(g^{(1)}) > \exp(g)$. Then we replace g by $g^{(1)}$ and we repeat the preceding process.

In this way we construct a sequence $(g^{(k)})_k$ of power series such that, for any $k \in \mathbb{N}$,

$$\exp(g^{(k+1)}) > \exp(g^{(k)})$$

and

$$g^{(k)} = g - \sum_{i=1}^{s} g_i q_i^{(k)} - r^{(k)}$$

with

$$\exp(g_i) + \mathrm{Supp}(q_i^{(k)}) \subset \Delta_i \quad \text{and} \quad \mathrm{Supp}(r^{(k)}) \subset \Delta_0.$$

At the limit $k \to \infty$ we obtain the desired decomposition.

But in general if f and the g_i are algebraic power series (or even polynomials), then r and the q_i are not algebraic power series as shown by the following example:

Example 10.2 (Kashiwara–Gabber's example, [13, p. 75]). Let us perform the division of xy by

$$g := (x - y^a)(y - x^a) = xy - x^{a+1} - y^{a+1} + x^a y^a$$

as formal power series in $\mathbb{k}[\![x, y]\!]$ with an integer $a > 1$ (here we choose a monomial order induced by the linear form $\lambda(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2$). By symmetry the remainder of this division can be written $r(x, y) := s(x) + s(y)$ where $s(x)$ is a formal power series. By substituting y by x^a we get

$$s(x^a) + s(x) - x^{a+1} = 0.$$

This relation yields the expansion

$$s(x) = \sum_{i=0}^{\infty} (-1)^i x^{(a+1)a^i}.$$

Thus the remainder of the division has Hadamard gaps and thus is not algebraic if $\mathrm{char}(\mathbb{k}) = 0$. Hadamard gaps are defined as follows.

Definition 10.3. Let $x = (x_1, \dots, x_n)$. A power series

$$f = \sum_k f_k$$

where f_k is a homogeneous polynomial of degree k for every k has Hadamard gaps if the indices $n_1 < n_2 < n_3 < \cdots$ of all non-zero homogeneous terms of f satisfy the condition $n_{k+1} > C n_k$ for all k where $C > 1$.

Over a characteristic zero field, a power series having Hadamard gaps cannot be algebraic.

Example 10.4. Let $\mathbb{k}$ be a field of any characteristic. Set

$$f_n := xy - \sum_{i=0}^{n} (-1)^i x^{(a+1)a^i}.$$

Then by the previous example

$$f_n \equiv \sum_{i>n} (-1)^i x^{(a+1)a^i} \text{ modulo } (g).$$

Thus

$$\mathrm{ord}_{\Bbbk[\![x]\!]/(g)}(f_n) \geq (a+1)a^{n+1}.$$

Since f_n is a polynomial of degree $(a+1)a^n$, this shows that the bound of Corollary 1.2 is optimal.

11. Generic Kashiwara–Gabber example

In this section we will investigate a particular case of division. Mainly, we will consider the problem of dividing an algebraic power series $f(x,y)$ in two variables by an algebraic power series $g(x,y)$ whose initial term is equal to xy with respect to a given monomial order as defined in the previous section. In this case the remainder of the division is the sum $R(x)+S(y)$ of one power series in x and one power series in y.

Definition 11.1. Let $\Bbbk$ be a characteristic zero field and x a single variable. A *D-finite power series* f is a formal power series in $\Bbbk[\![x]\!]$ satisfying a linear differential equation with polynomial coefficients, i.e. there exist $D \in \mathbb{N}$ and $a_j(x) \in \Bbbk[x]$ for $0 \leq j \leq D$ (not all equal to 0) such that

$$a_D f^{(D)} + a_{D-1} f^{(D-1)} + \cdots + a_0 f = 0.$$

Let us mention that by [32] any algebraic power series is D-finite. In Example 10.2, if $\mathrm{char}(\Bbbk) = 0$, the remainder is not D-finite since D-finite power series have no Hadamard gaps (see [32] or [21] for instance). We will show that the situation of Example 10.2 is generic in some sense.

Set

$$g_{\underline{a}}(x,y) = xy - \sum_{(i,j)\in E} a_{i,j} x^i y^j$$

where $\underline{a}$ denotes the vector of entries $a_{i,j} \in \Bbbk$ for some field $\Bbbk$ and E is a finite subset of $\mathbb{N}^2$ such that:

(1) $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1) \notin E$,

(2) $\{(2,0),(0,2)\} \not\subset E$.

If $(0,2) \notin E$, let us choose the linear form λ defined by $\lambda(e_1,e_2) = 3e_1 + 2e_2$. Then for any $e = (e_1,e_2) \in E$ we have $\lambda(e) = 3e_1 + 2e_2 > \lambda(1,1) = 5$ since only three situations may occur:

- $e_1 \geq 2$ so $\lambda(e) \geq 6$,
- $e_1 = 1$ and $e_2 \geq 2$ so $\lambda(e) \geq 7$,
- $e_1 = 0$ and $e_2 \geq 3$ so $\lambda(e) \geq 6$.

This means that there exists a monomial order induced by a linear form such that xy is the initial term of $g_{\underline{a}}(x,y)$. By symmetry this is also true if $(2,0) \notin E$. From now on we fix such monomial order and we perform the division of xy by $g_{\underline{a}}(x,y)$:

$$xy = g_{\underline{a}}(x,y) Q_{\underline{a}}(x,y) + R_{\underline{a}}(x) + S_{\underline{a}}(y).$$

Lemma 11.2. *Let $\Bbbk = \mathbb{Q}(\underline{a})$ where $\underline{a}$ is the set of new undeterminates $a_{i,j}$, $(i,j) \in E$. Then $R_{\underline{a}}(x)$ (resp. $S_{\underline{a}}(y)$, $Q_{\underline{a}}(x,y)$) is a power series with coefficients in $\mathbb{Q}[\underline{a}]$. In particular, if $\Bbbk$ is a characteristic zero field and $\underline{\alpha} \in \Bbbk^{\mathrm{Card}(E)}$ is a vector of elements $\alpha_{i,j} \in \Bbbk$ for every $(i,j) \in E$, then the coefficients of $R_{\underline{\alpha}}(x)$ (resp. $S_{\underline{\alpha}}(y)$, $Q_{\underline{\alpha}}(x,y)$) are those of $R_{\underline{a}}(x)$ (resp. $S_{\underline{a}}(y)$, $Q_{\underline{a}}(x,y)$) evaluated in $\underline{\alpha}$.*

Proof. Since the coefficient of the leading term xy of $xy - \sum_{(i,j)\in E} a_{i,j}x^i y^j$ is equal to 1, we see directly from the division algorithm given in Section 10 that the coefficients of $R_{\underline{a}}(x)$, $S_{\underline{a}}(y)$ and $Q_{\underline{a}}(x,y)$ are in $\mathbb{Q}[\underline{a}]$. Then by evaluating the terms of the equality

$$xy = g_{\underline{a}}(x,y)Q_{\underline{a}}(x,y) + R_{\underline{a}}(x) + S_{\underline{a}}(y)$$

in $\underline{a}$ we necessarily obtain the equality

$$xy = g_{\underline{\alpha}}(x,y)Q_{\underline{\alpha}}(x,y) + R_{\underline{\alpha}}(x) + S_{\underline{\alpha}}(y)$$

by unicity of the division. □

For every $k \in \mathbb{N} \setminus \{0,1\}$ we set

$$E_k = \{(0,k+1),(k+1,0),(k,k)\}.$$

We have the following result:

Proposition 11.3. *Let E be a finite set as before such that $E_k \subset E$ for some integer $k > 1$. Let $(\alpha_{i,j}) \in \mathbb{C}^{\mathrm{Card}(E)}$ whose coordinates are algebraically independent over $\mathbb{Q}$. Then $R_{\underline{\alpha}}(x)$ is not a D-finite power series. In particular, this is not an algebraic power series.*

Proof. Let $N = \mathrm{Card}(E)$. The proof is made by induction on N.

If $N = 3$, we have $E = E_k$. If $\alpha_{0,k+1}, \alpha_{k+1,0}, \alpha_{k,k} \in \mathbb{C}$ are algebraically independent over $\mathbb{Q}$ and $R(x) := R_{\underline{\alpha}}(x)$ is a D-finite power series, then $R(x)$ satisfies the differential equation

$$P_d(x)R^{(d)}(x) + \cdots + P_1(x)R(x) + P_0(x) = 0 \tag{11.1}$$

where $P_1(x), \ldots, P_d(x) \in \mathbb{C}[x]$. If we expand this relation in terms of a $\mathbb{Q}(\underline{\alpha})$-basis of the $\mathbb{Q}(\underline{\alpha})$-vector space $\mathbb{C}$, we obtain at least one non-trivial relation of the same type where the $P_i(x)$ are in $\mathbb{Q}(\underline{\alpha})[x]$. So we assume that $P_i(x) \in \mathbb{Q}(\underline{\alpha})[x]$ for all i and even $P_i(x) \in \mathbb{Q}[\underline{\alpha}][x]$ for all i by multiplying this relation by a common denominator of the coefficients of the P_i. Since $\alpha_{k+1,0}, \alpha_{0,k+1}$ and $\alpha_{k,k}$ are algebraically independent over $\mathbb{Q}$, we are reduced to assume that $R_{a,b,c}(x)$ is D-finite over $\mathbb{Q}[a,b,c]$ where a, b, c are new indeterminates and $R_{a,b,c}(x)$ is the x-depending part of the remainder of the division of xy by $xy - ax^{k+1} - by^{k+1} - cx^k y^k$:

$$xy = \left(xy - ax^{k+1} - by^{k+1} - cx^k y^k\right)Q_{a,b,c}(x,y) + R_{a,b,c}(x) + S_{a,b,c}(y).$$

By Lemma 11.2, $R_{a,b,c}(x) \in \mathbb{Q}[a,b,c]\llbracket x\rrbracket$ and $S_{a,b,c}(y) \in \mathbb{Q}[a,b,c]\llbracket y\rrbracket$, and for every point $\alpha = (\alpha_{0,k+1}, \alpha_{k+1,0}, \alpha_{k,k}) \in \mathbb{C}^3$, the power series $R_\alpha(x)$ and $S_\alpha(y)$ are equal to $R_{a,b,c}(x)$ and $S_{a,b,c}(y)$ evaluated in α. We may assume that the polynomials $P_i = P(a,b,c,x)$, coefficients of relation (11.1), are globally coprime, otherwise we factor out their common divisor.

For $0 \leq i \leq d$, let V_i be the subvariety of $\mathbb{C}^3$ which is the zero locus of the coefficients of $P_i(a,b,c,x)$ (seen as a polynomial in x). Let V be the intersection of $V_0, \dots, V_d$. Then if $(\underline{\alpha}) \notin V$, one of the $P_i(\underline{\alpha}, x)$ is non-zero and $R_{\underline{\alpha}}(x)$ is D-finite over $\mathbb{C}[x]$. Since we have assumed that the $P_i(a,b,c,x)$ are globally coprime, V is a finite union of algebraic curves and points, except if all but one P_i are equal to 0. In this latter case, we have

$$P_d(a,b,c,x) R^{(d)}_{a,b,c}(x) = 0$$

which means that $R^{(d)}_{a,b,c}(x) = 0$, thus we may replace P_d by 1 and in this case $V = \emptyset$.

From now on we replace c by $-ab$ and we have the relation

$$xy = (x - by^k)(y - ax^k) Q_{a,b,-ab}(x,y) + R_{a,b,-ab}(x) + S_{a,b,-ab}(y). \tag{11.2}$$

By symmetry we have $R_{b,a,-ab}(y) = S_{a,b,-ab}(y)$. If we replace (x,y) by (by, ax) in (11.2), we get

$$abxy = ab(y - a^k x^k)(x - b^k y^k) Q_{a,b,-ab}(by, ax) + R_{a,b,-ab}(by) + S_{a,b,-ab}(ax),$$

thus we obtain

$$\frac{1}{ab} R_{a,b,-ab}(by) = S_{a^k,b^k,-(ab)^k}(y). \tag{11.3}$$

By replacing y by ax^k in (11.2) we obtain

$$ax^{k+1} = R_{a,b,-ab}(x) + S_{a,b,-ab}(ax^k)$$

so

$$a^k x^{k+1} = R_{a^k,b^k,-a^k b^k}(x) + S_{a^k,b^k,-a^k b^k}(a^k x^k)$$

and

$$a^k x^{k+1} = R_{a^k,b^k,-a^k b^k}(x) + \frac{1}{ab} R_{a,b,-ab}(a^k b x^k) \tag{11.4}$$

by (11.3). By writing

$$R_{a,b,-ab}(x) = \sum_{l \geq 1} r_l(a,b) x^l$$

and plugging it in (11.4) we obtain

$$r_l(a,b) = 0 \quad \text{for all } l \leq k \qquad \text{and} \qquad r_{k+1}(a^k, b^k) = a^k.$$

Moreover, the coefficient of x^{kl} on both sides of (11.4), for every $l \geq 1$, is equal to

$$0 = r_{kl}(a^k, b^k) + \frac{1}{ab} r_l(a,b) a^{kl} b^l$$

hence

$$r_{kl}(a^k, b^k) = -r_l(a,b) a^{kl-1} b^{l-1}.$$

Thus

$$r_{k+1}(a,b) = a, \quad r_{k(k+1)}(a,b) = -a^{k+1} b, \quad r_{k^2(k+1)}(a,b) = a^{k(k+1)+1} b^{k+1}$$

and by induction

$$r_{k^i(k+1)}(a,b) = (-1)^i a^{\sum_{j=0}^{i} k^j} b^{\sum_{j=0}^{i-1} k^j} = (-1)^i a^{\frac{k^{i+1}-1}{k-1}} b^{\frac{k^i-1}{k-1}} \quad \text{for all } i \geq 1$$

and $r_l(a,b) = 0$ if $\frac{l}{k+1}$ is not a power of k. Thus we obtain

$$R_{a,b,-ab}(x) = \sum_{i=0}^{\infty} (-1)^i a^{\frac{k^{i+1}-1}{k-1}} b^{\frac{k^i-1}{k-1}} x^{(k+1)k^i}.$$

Exactly as in the example of Kashiwara–Gabber, this shows that $R_{\alpha,\beta,-\alpha\beta}(x)$ is not D-finite if $\alpha\beta \neq 0$.

Let $S \subset \mathbb{C}^3$ be the surface of the equation $ab + c = 0$. In particular, the surface S is not included in V since the components of V have dimension at most 1. Then we see that for any $(\alpha,\beta,\gamma) \in S \setminus \{ab = 0\}$, $R_{\alpha,\beta,\gamma}(x)$ is not D-finite. This contradicts the assumption that $R_{a,b,c}(x)$ is D-finite since we have shown that this would imply that $R_{\alpha,\beta,\gamma}(x)$ is D-finite for every $(\alpha,\beta,\gamma) \notin V$. Thus $R_{a,b,c}(x)$ is not D-finite.

Let us assume that $N > 3$ and that the proposition is proven for every set of cardinal $N-1$ containing E_k. Let us assume that $R_{\underline{a}}(x)$ is D-finite, i.e. there exist polynomials $P_i \in \mathbb{C}(\underline{a})[x]$, for $1 \leq i \leq d$, such that

$$P_d(\underline{a},x)R_{\underline{a}}^{(d)}(x) + \cdots + P_1(\underline{a},x)R_{\underline{a}}(x) + P_0(\underline{a},x) = 0.$$

As we did before, we may assume that $P_i \in \mathbb{Q}[\underline{a},x]$ for all i. By dividing the previous relation by a common divisor of the P_i, we may assume that the P_i are globally coprime. For $0 \leq i \leq d$ let V_i denote the subvariety of $\mathbb{C}^N$ which is the zero locus of the coefficients of $P_i(x)$ (seen as a polynomial with coefficients in $\mathbb{Q}[\underline{a}]$). Let V be the intersection of $V_0,\ldots,V_d$. As in the previous case, since the P_i are globally coprime, we have $\operatorname{codim}_{\mathbb{C}^N}(V) \geq 2$.

Let $(i_0,j_0) \in E \setminus E_k$ and set $E' = E \setminus \{(i_0,j_0)\}$. We set $W = \{a_{i_0,j_0} = 0\}$; we have $\operatorname{codim}_{\mathbb{C}^N}(W) = 1$. By the inductive assumption, $R_{\underline{\alpha}}(x)$ is not D-finite for every $\underline{\alpha} \in W$ such that $\operatorname{tr.deg}_{\mathbb{Q}}\mathbb{Q}(\underline{\alpha}) = N-1$. But if $\underline{\alpha} \in W \setminus V$ and $\operatorname{tr.deg}_{\mathbb{Q}}\mathbb{Q}(\underline{\alpha}) = N-1$ (we may find such an $\underline{\alpha}$ since $\operatorname{codim}_{\mathbb{C}^N}(V)$ is strictly larger than $\operatorname{codim}_{\mathbb{C}^N}(W)$), we see that $R_{\underline{\alpha}}(x)$ is not D-finite which is a contradiction since $\underline{\alpha} \notin V$. Thus $R_{\underline{a}}(x)$ is not D-finite and the proposition is proven for sets E of cardinal N. □

Example 11.4. If E does not contain any of the sets E_k for $k > 1$, then Proposition 11.3 is no valid in general. For instance, let us consider

$$E \subset \{(i, i+j) : (i,j) \in \mathbb{N}^2,\ i > 0,\ j > 0\}.$$

We set $F = \{(i,j) : (i,i+j) \in E\}$. Let us consider the Weierstrass division

$$z = \left[z - \sum_{(i,j)\in F} a_{i,i+j} z^i y^j \right] Q(z,y) + R(y)$$

where Q and R are algebraic power series by Lafon Division Theorem. Then by replacing z by xy, we obtain the division of xy by $g_{\underline{a}}(x,y)$:

$$xy = \left[xy - \sum_{(i,j)\in E} a_{i,j} x^i y^j \right] Q(xy,y) + R(y).$$

Thus $R_{\underline{a}}(x) = R(x)$ is an algebraic power series.

Example 11.5. Let $h(x,y)$ and $d(x,y)$ be two algebraic power series over $\mathbb{C}$ and let us assume that the initial term of $d(x,y)$ is xy. The division of h by d yields the relation

$$h(x,y) = d(x,y)Q(x,y) + R(x) + S(y).$$

By the Newton–Puiseux Theorem there exist $n \in \mathbb{N}$ and $x(y) \in \mathbb{C}\langle y\rangle$, $y(x) \in \mathbb{C}\langle x\rangle$ such that

$$d(x(y), y^n) = d(x^n, y(x)) = 0.$$

Thus we obtain

$$h(x(y^{\frac{1}{n}}), y) = R(x(y^{\frac{1}{n}})) + S(y)$$

and

$$h(x^n, y(x)) = R(x^n) + S(y(x)).$$

This yields the relation

$$R(x^n) - R(x(y(x)^{\frac{1}{n}})) = h(x^n, y(x)) - h(x(y(x)^{\frac{1}{n}})).$$

By replacing x by x^n we see that there exist two algebraic power series $f(x)$ and $g(x)$ such that

$$R(x^{n^2}) - R(g(x)) = f(x).$$

But this is impossible if $R(x) = e^x$ by Schanuel's conjecture [5]. This shows that in general D-finite power series (here e^x) which are not algebraic are not remainders of such a Weierstrass division.

12. Gap theorem for remainders of division of algebraic power series

By a theorem of Schmidt (see [29, Hilfssatz 5]) an algebraic power series has no large gaps in its expansion. More precisely, his result asserts that if an algebraic power series f is written as $f = \sum_k f_{n(k)}$ where $f_{n(k)}$ is a non-zero homogeneous polynomial of degree $n(k)$ and $(n(k))_k$ is increasing, then

$$\limsup_{k\to\infty} \frac{n(k+1)}{n(k)} < \infty.$$

We prove here the same result for remainders of the Grauert–Hironaka–Galligo division, i.e. it does not have more than Hadamard gaps.

Theorem 12.1. *Let $g_1, \dots, g_s \in \Bbbk\langle x\rangle$ and let us fix a monomial order induced by a linear form as in Section* 10. *Then there exists a function $C : \mathbb{N} \to \mathbb{R}_{>0}$ such that the following holds: Let $f \in \Bbbk\langle x\rangle$ be an algebraic power series and let r be the remainder of the division of f by $g_1, \dots, g_s$ with respect to the given monomial order. Let us write $r = \sum_{k=1}^{\infty} r_{n(k)}$ where r_h is a homogeneous polynomial of degree h, $(n(k))_k$ is an increasing sequence of integers and $r_{n(k)} \neq 0$ for any $k \in \mathbb{N}$. Then*

$$n(k+1) \leq C(\mathrm{Deg}(f)) \cdot n(k) \quad \text{for all } k \gg 0.$$

In particular,

$$\limsup_{k\to\infty} \frac{n(k+1)}{n(k)} < \infty.$$

Proof. Let I denote the ideal generated by $g_1, \dots, g_s$. Let us set

$$f_k := f - \sum_{i=1}^{k} r_{n(i)} \quad \text{for every } k \in \mathbb{N}.$$

The remainder of the division of f by $g_1, \dots, g_s$ is $\sum_{i=k+1}^{\infty} r_{n(i)}$, thus

$$\operatorname{ord}_{\mathbb{k}[\![x]\!]/I}(f_k) = \operatorname{ord}_{\mathbb{k}[\![x]\!]/I}\left(\sum_{i=k+1}^{\infty} r_{n(i)}\right) \geq n(k+1).$$

On the other hand, by Lemma 3.6 (iii)

$$\mathrm{H}(f_k) \leq \mathrm{H}(f) + \operatorname{Deg}(f) \cdot n(k)$$

thus $\mathrm{H}(f_k) \leq 2\operatorname{Deg}(f) \cdot n(k)$ for k large enough since $(n(k))_k$ is increasing. Hence, by Theorem 1.1, and since $\operatorname{Deg}(f_k) = \operatorname{Deg}(f)$, there exists a constant $C' > 0$ depending on $\operatorname{Deg}(f)$ such that

$$\operatorname{ord}_{\mathbb{k}[\![x]\!]/I}(f_k) \leq 2C' \cdot \operatorname{Deg}(f) \cdot n(k)$$

for k large enough. So the theorem is proven with $C = C' \cdot \operatorname{Deg}(f)$. □

Remark 12.2. Example 10.4 shows that this result is sharp.

References

[1] *B. Adamczewski* and *J. Bell*, Diagonalization and rationalization of algebraic Laurent series, Ann. Sci. Éc. Norm. Supér.(4) **46** (2013), 963–1004.

[2] *M. E. Alonso*, *T. Mora* and *M. Raimondo*, On the complexity of algebraic power series, in: Applied algebra, algebraic algorithms and error-correcting codes (Tokyo 1990), Lecture Notes in Comput. Sci. **508**, Springer, Berlin (1991), 197–207.

[3] *M. Artin*, Etale coverings of schemes over Hensel rings, Amer. J. Math. **88** (1966), 915–934.

[4] *M. Aschenbrenner*, An effective Weierstrass division theorem, preprint 2005, `http://www.math.ucla.edu/~matthias/publications.html`.

[5] *J. Ax*, On Schanuel's conjectures, Ann. of Math. (2) **93** (1971), 252–268.

[6] *D. Bertrand* and *F. Beukers*, Équations différentielles linéaires et majorations de multiplicités, Ann. Sci. Éc. Norm. Supér. (4) **18** (1985), 181–192.

[7] *R. Cluckers* and *L. Lipshitz*, Strictly convergent analytic structures, preprint 2014, `http://arxiv.org/abs/1312.5932v2`.

[8] *A. Galligo*, Théorème de division et stabilité en géométrie analytique locale, Ann. Inst. Fourier (Greoble) **29** (1979), no. 2, 107–184.

[9] *H. Grauert*, Über die Deformation isolierter Singularitäten analytischer Mengen, Invent. Math. **15** (1972), 171–198.

[10] *H. Hauser* and *C. Koutschan*, Multivariate linear recurrences and power series division, Discrete Math. **312** (2012), no. 24, 3553–3560.

[11] *G. Hermann*, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Ann. **95** (1926), no. 1, 736–788.

[12] *H. Hironaka*, Resolution of singularities of an algebraic variety over a field of characteristic zero. I and II, Ann. of Math. (2) **79** (1964), 109–203; ibid. **79** (1964), 205–326.

[13] *H. Hironaka*, Idealistic exponents of singularity, in: Algebraic geometry (Baltimore 1976), The John Hopkins Centennial Lectures, John Hopkins University Press, Baltimore (1977), 52–125.

[14] *C. Huneke* and *I. Swanson*, Integral closure of ideals, rings, and modules, London Math. Soc. Lecture Note Ser. **336**, Cambridge University Press, Cambridge 2006.

[15] *S. Izumi*, A criterion for algebraicity of analytic set germs, Proc. Japan Acad. Ser. A **68** (1992), 307–309.
[16] *S. Izumi*, Increase, convergence and vanishing of functions along a Moishezon space, J. Math. Kyoto Univ. **32** (1992), 245–258.
[17] *S. Izumi*, Transcendence measures for subsets of local algebras, in: Real analytic and algebraic singularities (Nagoya/Sapporo/Hachioji 1996), Pitman Res. Notes Math. Ser. **381**, Longman, Harlow (1998), 189–206.
[18] *H. Kurke*, *G. Pfister*, *D. Popescu*, *M. Roczen* and *T. Mostowski*, Die Approximationseigenschaft lokaler Ringe, Lecture Notes in Math. **634**, Springer, Berlin 1978.
[19] *I. Kurkova* and *K. Raschel*, On the functions counting walks with small steps in the quarter plane, Publ. Math. Inst. Hautes Études Sci. **116** (2012), 69–114.
[20] *J.-P. Lafon*, Séries formelles algébriques, C. R. Acad. Sci. Paris Sér. A-B **260** (1965), 3238–3241.
[21] *L. Lipshitz* and *L. Rubel*, A gap theorem for power series solutions of algebraic differential equations, Amer. J. Math. **108** (1986), no. 5, 1193–1213.
[22] *E. Mayr* and *A. Meyer*, The complexity of the word problems for commutative semigroups and polynomial ideals, Adv. Math. **46** (1982), no. 3, 305–329.
[23] *Y. V. Nesterenko*, Measures of algebraic independence of numbers and functions, in: Journées arithmétiques de Besançon (Besançon 1985), Astérisque **147–148**, Société Mathématique de France, Paris (1987), 141–149.
[24] *K. Nishioka*, On an estimate for the orders of zeros of Mahler type functions, Acta Arith. **56** (1990), no. 3, 249–256.
[25] *T. Mora*, An algorithm to compute the equations of tangent cones, in: Computer algebra (Marseille 1982), Lecture Notes in Comput. Sci. **144**, Springer, Berlin (1982), 158–165.
[26] *M. Nagata*, Local rings, Interscience, New York 1962.
[27] *R. Ramanakoraisina*, Complexité des fonctions de Nash, Comm. Algebra **17** (1989), 1395–1406.
[28] *P. Samuel*, Algébricité de certains points singuliers algébroïdes, J. Math. Pures Appl. (9) **35** (1956), 1–6.
[29] *F. K. Schmidt*, Mehrfach perfekte Körper, Math. Ann **108** (1933), 1–25.
[30] *A. Seidenberg*, Constructions in algebra, Trans. Amer. Math. Soc. **197** (1974), 273–313.
[31] *A. Shidlovskii*, On a criterion for the algebraic independence of the values of a class of entire functions, Izv. Akad. Nauk. SSSR **23** (1959), 35–66.
[32] *R. Stanley*, Differentiably finite power series, European J. Combin. **1** (1980), 175–188.
[33] *O. Zariski* and *P. Samuel*, Commutative algebra I, D. Van Nostrand Company, Princeton 1958.

Guillaume Rond, Aix-Marseille Université, CNRS, Centrale Marseille, I2M, UMR 7373,
13453 Marseille, France
e-mail: guillaume.rond@univ-amu.fr

Eingegangen 12. Juni 2014, in revidierter Fassung 21. April 2015