Approximate contact factorization of germs of plane curves

Joris van der Hoeven, Grégoire Lecerf

Approximate contact factorization of germs of plane curves[*†]

JORIS VAN DER HOEVEN[a], GRÉGOIRE LECERF[b]

CNRS, École polytechnique, Institut Polytechnique de Paris
Laboratoire d'informatique de l'École polytechnique (LIX, UMR 7161)
Bâtiment Alan Turing, CS35003
1, rue Honoré d'Estienne d'Orves
91120 Palaiseau, France

a. Email: vdhoeven@lix.polytechnique.fr
b. Email: lecerf@lix.polytechnique.fr

Preliminary version of August 4, 2022

Given an algebraic germ of a plane curve at the origin, in terms of a bivariate polynomial, we analyze the complexity of computing an irreducible decomposition up to any given truncation order. With a suitable representation of the irreducible components, and whenever the characteristic of the ground field is zero or larger than the degree of the germ, we design a new algorithm that involves a nearly linear number of arithmetic operations in the ground field plus a small amount of irreducible univariate polynomial factorizations.

KEYWORDS: contact factorization, approximate root, polynomial factorization, algebraic curve, complexity

1. INTRODUCTION

1.1. Motivation

Algebraic curves play a central role in algebraic geometry and various applications in effective algebra. In particular, efficient algorithms are needed to compute topological or analytic invariants, arithmetic genus, desingularized models, integral closures, Riemann–Roch spaces, etc. Usual applications in computer algebra concern the irreducible factorization of multivariate polynomials, the integration of rational functions, the construction of algebraic geometry error correcting codes, the bi-linear complexity of polynomial multiplication, etc. In the present paper, we are interested in computing the irreducible factorization of any given polynomial $P \in \mathbb{K}[[z]][x]$, where $\mathbb{K}$ denotes an *effective* field. Here "effective" means that algorithms are at our disposal for the arithmetic operations and the zero test in $\mathbb{K}$.

Let $\mathbb{K}((z))$ denote the fraction field of $\mathbb{K}[[z]]$ of Laurent series in z. The field

$$\mathbb{K}\langle\langle z\rangle\rangle := \bigcup_{i \geqslant 1} \mathbb{K}((z^{1/i}))$$

[*]. This paper is part of a project that has received funding from the French "Agence de l'innovation de défense".

[†]. This article has been written using GNU $\text{T}_\text{E}\text{X}_{\text{MACS}}$ [43].

of power series with fractional exponents is called the field of *Puiseux series* (or *Puiseux expansions*) over $\mathbb{K}$. Let $\bar{\mathbb{K}}$ denote the algebraic closure of $\mathbb{K}$. If $\mathbb{K}$ has characteristic zero, then $\bar{\mathbb{K}}\langle\langle z\rangle\rangle$ is the algebraic closure of $\mathbb{K}((z))$. In other words, any polynomial P in $\mathbb{K}((z))[x]$ splits into linear factors in $\bar{\mathbb{K}}\langle\langle z\rangle\rangle[x]$.

Computations of Puiseux expansions of roots of P go back to Newton [62], and were rediscovered by Puiseux [75]; see [5, p. 198] and [82, 86]. The well known *Newton polygon method* turns out to be effective whenever $\bar{\mathbb{K}}$ is effective. When adopting a suitable algebraic complexity model (in which running times are measured in terms of the required number of arithmetic operations in $\mathbb{K}$ or $\bar{\mathbb{K}}$), the complexity is easily seen to be polynomial in the degree of P and in the required precision. However, at present time, we are not aware of an algorithm with a softly linear cost for any precision (especially below the valuation of discriminant of P).

For the design of such a quasi-optimal algorithm, it is important to carefully state the problem that needs to be solved. In particular, one has to pay attention to the ways in which algebraic numbers and fractional power series are represented. It turns out that the computation of Puiseux expansions is closely related to the computation of irreducible factorizations in $\mathbb{K}[[z]][x]$ and that representation issues are more straightforward for the latter problem.

In this paper, we therefore focus on the computation of irreducible factorizations. Our main goal is the design of an efficient algorithm for factoring a polynomial $P\in\mathbb{K}[[z]][x]$ that is given modulo $O(z^{\tau})$ for a finite precision $\tau\in\mathbb{N}$, assuming that we already have an algorithm for decomposing polynomials in $\mathbb{K}[x]$ into irreducible factors.

1.2. Notations and assumptions

For complexity analyses, we consider algebraic complexity models (such as computation trees). In other words we simply count numbers of arithmetic operations and zero tests in specified algebraic structures.

Until the end of the paper, $\epsilon>0$ is a fixed rational number that can be taken arbitrarily close to zero. For complexity estimates we often use the *soft-Oh* notation: $f(n)=\tilde{O}(g(n))$ means that$f(n)=g(n)\,(\log(g(n)))^{O(1)}$; see [26, chapter 25, section 7] for technical details. The least integer larger or equal to x is written $\lceil x\rceil$; the largest one smaller or equal to x is written $\lfloor x\rfloor$.

For randomized algorithms over a finite effective ring $\mathbb{A}$, we assume a special instruction that uniformly generates random elements in $\mathbb{A}$ with constant cost. For a given input, the cost of a randomized algorithm is thus a random variable. The *expected cost* for input size s is defined as the maximum of the averages of these random variables over all possible inputs of size $\leqslant s$.

For a finite field $\mathbb{F}_q$ of characteristic p and with q elements, the usual primitive element representation will be used, so elements in $\mathbb{F}_q$ will be regarded in $\mathbb{F}_p[z]/(\nu(z))$ where ν is an irreducible polynomial of degree $\log q/\log p$.

Polynomials We use $\mathsf{M}(d)$ as a notation for the cost of multiplying two polynomials of degree $<d$, in terms of the number of operations in the coefficient ring. We assume that $\mathsf{M}(d)/d$ is a non-decreasing function in d. It is known [11, 77] that one can take $\mathsf{M}(d)=O(d\log d\log\log d)$. For rings of positive characteristic, one even has $\mathsf{M}(d)=O(d\log d)$, modulo a plausible number-theoretic conjecture [34]. We will also denote

$$\mathbb{A}[x]_{<d}:=\{P\in\mathbb{A}[x]:\deg P<d\}.$$

Algebraic towers A *tower of algebraic extensions* of $\mathbb{K}$ of height t is a sequence $(\mathbb{A}_i)_{i\leqslant t}$ with $\mathbb{A}_0=\mathbb{K}$ and

$$\mathbb{A}_i=\mathbb{A}_{i-1}[x_i]/(\mu_i(x_i))$$

for a separable irreducible monic polynomial $\mu_i\in\mathbb{A}_{i-1}[x_{i-1}]$ and $i=1,\ldots,t$. We set

$$s_i:=\deg\mu_i.$$

Products and inversions in $\mathbb{A}_t$ take $\tilde{O}((s_1\cdots s_t)^{1+\epsilon})$ operations in $\mathbb{K}$. This was first proved in [45] in the case when $\mathbb{A}_t$ is a field and card $\mathbb{K}>\binom{s_1\cdots s_t}{2}$. The result was extended to more general algebraic towers in [46]. Whenever card $\mathbb{K}\leqslant\binom{s_1\cdots s_t}{2}$, we may work in an algebraic extension $\mathbb{L}$ of degree $n=O(\log(s_1\cdots s_t))$ such that $q^n=\text{card }\mathbb{L}>\binom{s_1\cdots s_t}{2}$. The computation of such an extension can be done using $\tilde{O}(p^{1/2}(n\log q)^{O(1)})=\tilde{O}(s_1\cdots s_t)$ operations in the prime subfield $\mathbb{F}_p$ of $\mathbb{K}$, thanks to [79, Theorem 4.1]. For a fixed field $\mathbb{K}$, this can be regarded as a precomputation, whereas computations with elements in $\mathbb{L}$ instead of $\mathbb{K}$ induce only a logarithmic overhead $\tilde{O}(\log(s_1\cdots s_t))$.

Factorization We define $\mathsf{F}_{\mathbb{K}}(n;s_1,\ldots,s_t)$ to be an upper bound for the cost (expected or not) of irreducible factorization of a polynomial in $\mathbb{A}_t[x]_{\leqslant n}$. It is convenient to introduce

$$\bar{\mathsf{F}}_{\mathbb{K}}(m):=m\max_{ns_1\cdots s_t\leqslant m}\frac{\mathsf{F}_{\mathbb{K}}(n;s_1,\ldots,s_t)}{ns_1\cdots s_t},$$

so $\bar{\mathsf{F}}_{\mathbb{K}}(m)/m$ is a non-decreasing function in m.

For example, if $\mathbb{K}$ is the finite field $\mathbb{F}_q$, then a well known probabilistic algorithm due to Cantor and Zassenhaus [12] factors univariate polynomials in $\mathbb{F}_q[x]_{\leqslant n}$ using an expected number of $\tilde{O}(n^2\log^2 q)$ bit operations.

The currently best known algorithm is obtained as a combination of results due to von zur Gathen, Kaltofen and Shoup [27, 48, 49], and Kedlaya and Umans [51]: it takes an expected number of

$$\mathsf{F}_{\mathbb{F}_q}(n)=O((n^{1.5}\log q\log p)^{1+\epsilon})$$

bit operations; see [47, Corollary 5.1].

The case of a tower $(\mathbb{A}_i)_{i\leqslant t}$ over $\mathbb{F}_q=\mathbb{A}_0$ (with the above notation) reduces to the case of $\mathbb{F}_{q^{s_1\cdots s_t}}$ by means of the fast change of representation of [70, Theorem 1.2], that applies whenever

$$p>s_1\cdots s_t\frac{\log q}{\log p}. \tag{1.1}$$

In terms of bit complexity, and for a "random access memory" computational model, this yields

$$\mathsf{F}_{\mathbb{K}}(n;s_1,\ldots,s_t)=O((n^{1.5}s_1\cdots s_t\log q\log p)^{1+\epsilon}).$$

Details can be found in [47, Corollary 5.3]. Whenever condition (1.1) is satisfied, we may then use the expected bit complexity bound

$$\bar{\mathsf{F}}_{\mathbb{F}_q}(m)=O((m^{1.5}\log q\log p)^{1+\epsilon}).$$

When the tower has small degrees s_i, optimized factorization procedures can be found in [44, 47, 48]. In particular, if $\log q/\log p$ is smooth, then polynomials of small degree can even be factored in quasi-optimal time. Note that these optimizations do not depend on Kedlaya–Umans' algorithm for modular composition.

For an abstract effective field $\mathbb{K}$, there does not exist a general algorithm to factor polynomials in $\mathbb{K}[x]$ into irreducible ones [24, 25]. Throughout this paper, we will therefore need to assume that such an algorithm is provided by the computational model:

K. Irreducible factorization in $\mathbb{K}[x]$ is available within the computational model.

In practice, this property holds whenever $\mathbb{K}$ is effectively finitely generated over its prime subfield. Once factorization is available in $\mathbb{K}[x]$, it is also available in $\mathbb{A}_t[x]$, with a complexity that depends on those of resultants and gcds [81].

1.3. Related work

Let $\mathbb{K}$ still denote an effective field, let $P(z,x) \in \mathbb{K}[[z]][x]$ be monic as a polynomial in x, and assume that $P(0,0)=0$. So $P(z,x)$ defines a germ of curve at the origin. In practice, we always truncate P at a finite order in z. For the discussion in the following paragraphs, we therefore take $P \in \mathbb{K}[z][x]$ and assume that P is monic, primitive, and separable in x, of total degree $\leqslant d$, and of partial degrees $\leqslant d_z$ in z and $\leqslant d_x$ in x.

Puiseux expansions If the characteristic of $\mathbb{K}$ is zero or sufficiently large, then Puiseux expansions to any given precision can be computed in polynomial time when considering an algebraic complexity model over $\bar{\mathbb{K}}$—this result belongs to the folklore.

Consider a Puiseux series $x(z)$ that is a root of P. The shortest truncation of this series which is different from any truncation of a distinct Puiseux series root of P is called the *singular part* of $x(z)$. In 1978, Kung and Traub [52] showed that the Puiseux expansion of $x(z)$ can be computed efficiently using Newton's method, once its singular part is known.

The complexity of the computation of singular parts started to be studied in the eighties. In [35], Henry and Merle showed that the embedded resolution of an irreducible germ of curve defined by $P(z,x)=0$ at the origin can be computed with $O(d^8)$ operations in $\bar{\mathbb{K}}$. In [19], Duval introduced the notion of *rational Puiseux expansions*, that allowed computations over $\bar{\mathbb{K}}$ to be replaced by computations over $\mathbb{K}$. She adapted the usual Newton polygon algorithm to such a rational representation, and made use of *dynamic evaluation* to handle algebraic extensions without polynomial factorization. She achieved a total cost of $O(d^8)$ operations in $\mathbb{K}$, whenever the characteristic is zero or sufficiently large. This analysis was based on slow arithmetic for polynomials and series.

In his PhD thesis [68], Poteaux showed that Duval's algorithm takes at most $O(d_x^6 d_z^2)$ operations in $\mathbb{K}$ in order to obtain all the singular parts of the Puiseux expansions. In [69], Poteaux and Rybowicz also proved that the singular parts of the rational Puiseux expansions centered at a single point can be computed using $\tilde{O}(d_x^3 d_z + d_x^2 \log q)$ operations in $\mathbb{K}$, in the case when $\mathbb{K} = \mathbb{F}_q$; this bound relies on fast polynomial arithmetic. In [72], Poteaux and Weimann finally gave a probabilistic algorithm that allows singular parts to be computed with $\tilde{O}(d_x(\operatorname{val}_z(\operatorname{Disc}_x P)+1))$ operations in $\mathbb{K}$, assuming that the characteristic of $\mathbb{K}$ is zero or sufficiently large. This bound is quasi-optimal in worst cases, when we need order about $\operatorname{val}_z(\operatorname{Disc}_x P)$ before root separation takes place [72, Example 8.1]. Their algorithm makes use of dynamic evaluation and the singular parts are represented by truncations of rational Puiseux expansions. These algorithms by Poteaux *et al.* also extend efficiently to obtain the collection of all singular parts at each of the singularities of the algebraic curve defined by $P(z,x)=0$. As a byproduct, Poteaux and Weimann proved the expected complexity bound $\tilde{O}(d_x(\operatorname{val}_z(\operatorname{Disc}_x P) + \tau)) + \mathsf{F}_{\mathbb{K}}(d_x)$ for the irreducible factors of P at precision $O(z^\tau)$, still under the assumption that the characteristic of $\mathbb{K}$ is $>d_x$; see [72, Theorem 1.6].

When $\mathbb{K}=\mathbb{Q}$, a polynomial bit complexity for Puiseux series was first achieved by Chistov [13]. The complexity bound for this case was subsequently detailed and improved by Walsh [83, 84]. Since the complexity exponents are rather large, multimodular approaches turn out to be of practical interest [68].

Once singular parts are known, we have already mentioned that Puiseux expansions can be extended by means of the Newton operator, as described in [52]; see also [39] for recent optimizations. For small and moderate expansion orders, it is often more efficient to use lazy or relaxed arithmetic to expand algebraic power series [38, 85]. For very large expansion orders, yet another method is to compute a differential operator that annihilates the expansions [15, 16]; see [8] for complexity bounds. It is also worth mentioning that individual terms of algebraic Puiseux series over a finite field can be computed even faster than with the Newton iteration [7].

Approximate roots In positive characteristic, the field of Puiseux series no longer coincides with the algebraic closure of $\mathbb{K}((z))$; see for instance [50]. Hamburger–Noether expansions constitute a natural extension of Puiseux series in positive characteristic [9].

In his 1989 article [1], Abhyankar addressed a question from Kuo about an algorithm to decide the irreducibility of a germ of curve, without using blowups or Puiseux series. In characteristic zero, Abhyankar gave a positive answer to this question, by using expansions of the defining polynomial of the germ with respect to so-called *approximate roots*. These approximate roots can be determined recursively by means of a generalized Newton polygon, previously introduced in [2, 3]. They generalize Tschirnhaus transforms [80]. Complexity analyses can be found in [71, 73]: in favorable cases irreducibility tests take softly linear time (plus a justifiable amount of irreducibility tests in $\mathbb{K}[x]$).

Abhyankar's work has been completed and extended to arbitrary characteristic by Cossart and Moreno-Socías in [18], where they present an alternative construction based on valuation theory. The mathematical relationship between approximate roots, Puiseux expansions, and Hamburger–Noether expansions can be found in [73, 76].

Local factorizations Whenever $\mathbb{L}$ is a local ring different from $\mathbb{K}[[z]]$, factorization in $\mathbb{L}[x]$ is a more difficult problem, for which Puiseux expansions cannot be used. The first interesting case is when $\mathbb{L}$ is the field $\mathbb{Q}_p$ of the p-adic numbers. Let F be a monic primitive square-free polynomial in $\mathbb{Z}[x]$. A first series of contributions concern the *Round Four* algorithm due to Zassenhaus, and dedicated to the construction of integral bases modulo F; see [17, 21, 22] for instance. The first polynomial time algorithm for factoring F over $\mathbb{Q}_p$ was given by Chistov [14], and then improved by Cantor and Gordon in [10].

After that, Pauli [67] designed a factorization algorithm over an algebraic extension of degree k of $\mathbb{Q}_p$ with bit complexity

$$(d^2 \operatorname{val}_p(\operatorname{disc} F)\, (d+\operatorname{val}_p(\operatorname{disc} F))\log p^k)^{1+o(1)}. \tag{1.2}$$

Since 1999, Montes has been designing different algorithms; his irreducibility test of [57] has been shown in [23] to have a complexity similar to (1.2).

The next improvements are due to Guàrdia, Montes, and Nart [29, 30]. They exploit previous ideas by MacLane and Okutsu in order to compute so-called *OM factorizations* (as a shorthand for "Okutsu–Montes factorizations"); see [61] for a survey. In [6], Bauch, Nart, and Stainsby proved the bit complexity bound

$$O((d^2 + d\operatorname{val}_p^2(\operatorname{disc} F) + d\operatorname{val}_p(\operatorname{disc} F)\log p^k)^{1+o(1)})$$

for an algebraic extension of degree k of $\mathbb{Q}_p$. Further refinements and applications, including the computation of integral closures, can be found in [20, 31, 32].

In [74] Poteaux and Weimann recently improved the latter complexity bound to

$$O((d\,\mathrm{val}_p(\mathrm{disc}\,F)\log p^k)^{1+o(1)})$$

(discarding factorization costs in $\mathbb{F}_p[x]$) whenever $p > d$: they made use of the natural "divide and conquer" extension of the generalized Hensel lifting of [33] and also applied the same "increase of precision" strategy as in [72].

Non-archimedean value groups Various other generalizations of Puiseux expansions have been investigated by van der Hoeven, starting in 1997 with his PhD thesis [37]. First of all, he developed a framework for the resolution of algebraic equations over a field $\mathbb{S}$ of generalized power series instead of $\mathbb{K}[[z]]$. One natural example is to take $\mathbb{S} = \mathbb{K}((z))$, where $\mathbb{K}$ is an effective subfield of another field of Laurent series $\Bbbk((u))$. In this case, the underlying value group of $\mathbb{S}$ becomes non-archimedean, and the issue arises how to conduct exact computations with truncated power series. This is easy if $\mathbb{K} = \Bbbk(u)$, but less trivial if $\mathbb{K}$ contains transcendental power series such as $\sin u$, because of the required zero test. We refer to [41, 42] for some recent perspectives on this type of computations.

The resolution of algebraic equations over fields $\mathbb{S}$ of generalized power series is still based on the Newton polygon method. However, the complexity can no longer be analyzed in terms of the truncation order in a non-archimedean context. Instead, one may consider the resolution of equations in Hensel position as a natural building block. In [37], van der Hoeven showed how to reduce the resolution of a general algebraic equation of degree d to at most $2d-1$ applications of Hensel's lemma. It would be interesting to analyze the complexity of this algorithm in the special cases that were considered above.

Non-archimedean value groups are not merely a theoretical curiosity. Until recently, effective counterparts of Hironaka's theory of standard bases for power series were only known in the case of algebraic power series [4, 58]. In [42], generalized Puiseux series have been put to develop elimination theories for more general power series, such as differentially algebraic power series. Non-archimedean value groups actually arise in a natural way when studying algebraic differential equations, and the Newton polygon method can be generalized to this context; see [5] for recent progress and further references.

1.4. Outline of the paper

The main purpose of this paper is to present a self-contained and quasi-optimal algorithm for approximate factorization over rings of formal power series. We show how to efficiently factor P into irreducible polynomials, and for each irreducible factor P_i we construct generators of the valuation group of $\mathbb{K}[[z]][x]/(P_i)$ in a form of a *contact tower*; see Definition 3.1. An *irreducible factorization* of P modulo $O(z^\tau)$ is a list of factors $P_1, \ldots, P_r$ of P modulo $O(z^\tau)$, along with their associated multiplicity and contact tower; see Definition 7.6. In particular the P_i are irreducible, pairwise coprime, and we have

$$P = P_1^{m_1} \cdots P_r^{m_r} + O(z^\tau),$$

for some integers $m_i \geqslant 1$. The contact tower associated to P_i allows the computation of the valuation in $\mathbb{K}[[z]][x]/(P_i)$ in softly linear time. The following main result will be proved at the end of section 8.2:

THEOREM 1.1. *Let ϵ be a fixed positive value, and assume* $\mathbf{K}$. *Let $P \in \mathbb{K}[[z]][x]$ be monic of degree n in x, known modulo $O(z^{\tau})$, and such that the characteristic of $\mathbb{K}$ is zero or $>n$. Then, an irreducible factorization of P modulo $O(z^{\tau})$ can be computed using*

$$\tilde{O}(n^{1+\epsilon}\tau) + 2\,\bar{\mathsf{F}}_{\mathbb{K}}(n)$$

operations in $\mathbb{K}$.

Example 1.2. Take $\mathbb{K} := \mathbb{Q}$, $\tau := 2$, and $P := x^2 + O(z^2)$. Then $r = 1$, $P_1 = x$, and $m_1 = 2$ is an irreducible factorization of P modulo $O(z^{\tau})$. Taking $r = 2$, $P_1 = x - z$, $P_2 = x + z$, $m_1 = m_2 = 1$, we obtain another such factorization. This shows that approximate factorizations are not unique in general.

Note that the term $2\,\bar{\mathsf{F}}(n)$ is negligible with respect to $n^{1+\epsilon}\tau$ as soon as the precision τ is sufficiently large. By using our approximate factorization algorithm with a sufficiently large precision, we deduce the following complexity bound for the actual irreducible factorization of P; see section 9.5.

THEOREM 1.3. *Let ϵ be a fixed positive value, and assume* $\mathbf{K}$. *Let $P \in \mathbb{K}[[z]][x]$ be monic and separable of degree n in x and known at precision* $\mathrm{val}_z(\mathrm{Disc}_x P) + \sigma$ *in z with $\sigma > 0$. Assume that the characteristic of $\mathbb{K}$ is zero or $>n$. Then, the irreducible factors of P can be computed modulo $O(z^{\sigma})$ using*

$$\tilde{O}(n^{1+\epsilon}(\mathrm{val}_z(\mathrm{Disc}_x P) + \sigma)) + 2\,\bar{\mathsf{F}}_{\mathbb{K}}(n)$$

operations in $\mathbb{K}$.

Theorem 1.3 considers $\mathrm{val}_z(\mathrm{Disc}_x P)$ as part of the input. This is not very restrictive in characteristic zero or $>\mathrm{val}_z(\mathrm{Disc}_x P)$ thanks to [60, Theorem 1]. On the other hand, if P belongs $\mathbb{K}[z][x]$ then $\mathrm{val}_z(\mathrm{Disc}_x P) \leqslant (2n-1)\deg_z P$ can be computed with $\tilde{O}(n^2 \deg_z P)$ operations in $\mathbb{K}$. Theorem 1.3 can be regarded as a deterministic counterpart of [72, Theorem 1.6] and is also similar to [74, Theorem 4], although the underlying algorithms are notably different. Our proofs are elaborated from scratch by taking special care of the precisions and the cost of all factorizations in $\mathbb{K}[x]$. We rely neither on Puiseux expansions (contrary to [72]), nor on *OM factorizations*, nor on approximate roots, nor on the "divide and conquer" strategy from [72, 74] on the precision. Instead, our algorithm is based on a natural cascade of factorizations driven by Newton polytopes and a new method to balance the depth of the recursive calls: namely our central shift algorithm of section 7.7. Note that approximate factorizations in the sense of Theorem 1.1 (especially below the valuation of the discriminant) are not assessed in [72, 74].

The algorithm behind Theorem 1.1 decomposes into several subtasks for which we design efficient solutions. The first subtask concerns the computation of so-called *distinct-slope* and *equal-slope factorizations*; see section 7. Distinct-slope factorizations separate the factors of P according to the slopes of its Newton polygons. Equal-slope factorizations serve a similar purpose for polynomials with a single slope. We achieve these computations in softly linear time by means of a generalized Hensel lifting, as explained in section 4.

The contact factorization algorithm performs a cascade of distinct-slope and equal-slope factorizations over increasing contact towers. When the tree modeling the successive splittings of P is not sufficiently well balanced, the total complexity moves away from quasi-linearity. Our *central shift* algorithm of section 7.7 circumvents this issue through tree-balancing. The top level algorithm is described in section 8.

Computing over contact towers involves two difficulties. First, as for towers of algebraic field extensions, we do not know how to perform arithmetic operations in softly linear time. We overcome this difficulty by doing most of the operations within the original ring $\mathbb{K}[[z]][x]$ using a sufficiently high precision. The second difficulty concerns zero tests and inversions in towers. In section 6, we introduce *initial expansions*, that can be computed fast thanks to accelerated tower arithmetic [45].

As said, the power series setting from this paper is simpler than the one of general local fields studied by Montes *et al.* Nevertheless, the main mathematical ideas are roughly the same and go back to the work of MacLane [55, 56] on *augmented valuations*: approximate roots, OM-factorizations, and contact towers share the same philosophy.

Compared to [55, 56], our contact towers represent a kind of a more general "augmented semi-valuations". Approximate roots can indeed be regarded as special cases of contact towers but also of so-called "tipos" in [57]. Our contact factorization algorithm does not rely on approximate roots: as explained in section 8.3, such roots may be useful in practice, but it is a drawback that they are not preserved during factorizations. In fact, our new central shift strategy behaves as an algorithmic improvement with respect to approximate roots; see section 2.6. While MacLane, and later Montes, focused on constructing augmented (semi-)valuations over polynomial rings, our down-to-earth and self-contained approach begins with designing efficient data structures in the vein of triangular sets and Hironaka's standard bases [36]. In addition, let us mention that, compared to [74], our multi-factor Hensel lifting of section 4 is based on a faster multi-remaindering strategy.

We would also like to insist on our novel strategy for approximate factorizations, that is behind Theorem 1.1. Roughly speaking, the problem here is similar to approximate factorization in $\mathbb{C}[x]$. The first quasi-optimal algorithms for the computation of the distinct roots were designed for the case when the required precision is sufficiently high [66, 78]; more recently, a different algorithm was proposed for small precisions [59]. Detailed comparisons between all known algorithms for local factorization would be too long and technical to be discussed here. Instead, we dedicate our next section to *introductory examples* that illustrate the computational difficulties that are common to all known approaches.

At the end of the paper, a glossary is dedicated to the specific mathematical notations, and an index gathers references to the main definitions.

2. INTRODUCTORY EXAMPLES

Before we give the formal definition of a *contact factorization*, we review a few motivating examples from the complexity perspective.

2.1. Graded rings and Newton polygons

Let $\bar{\Gamma}$ be a totally ordered abelian group and let $\Gamma \subseteq \bar{\Gamma}$ be a monoid embedded in $\bar{\Gamma}$. A *graded ring R* with respect to the *grading* Γ is a direct sum

$$\bigoplus_{e \in \Gamma} R_e,$$

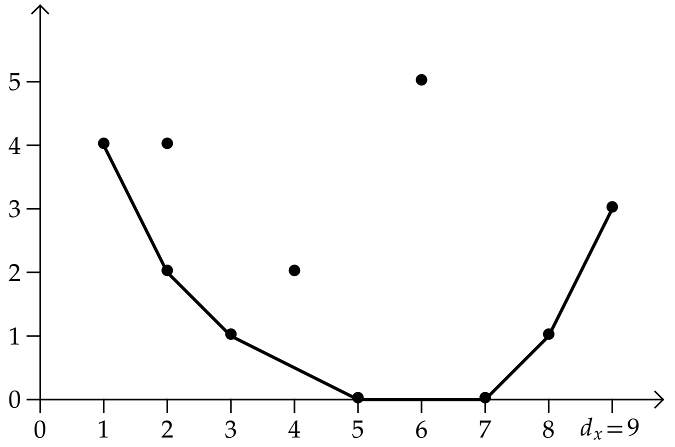

Figure 2.1. The Newton polygon of $P(z,x):=z^4x+(z^2+z^4)\,x^2+zx^3+z^2x^4+x^5+z^5x^6+x^7+zx^8+z^3x^9$. Each dot represents a monomial in P.

where the R_e are abelian groups such that $R_eR_f\subseteq R_{e+f}$ for all e and f in Γ. An element of R is said to be *homogeneous* if it belongs to one of the R_e. Any element a in R can be uniquely written $\sum_{e\in\Gamma}[a]_e$, where $[a]_e\in R_e$ is called the *homogeneous component* of degree e of a. If $e\in\Gamma$ and $\eta\in\bar{\Gamma}^>$, then we also denote

$$[a]_{e;\eta}:=\sum_{\substack{f\in\Gamma\\ e\leqslant f<e+\eta}}[a]_f.$$

The *initial form* of a non-zero element $a\in R$, written $\operatorname{in}(a)$, is the non-zero homogeneous component $[a]_e$ with the smallest index e. By convention we set $\operatorname{in}(0):=0$.

An ideal I of R is said to be *homogeneous* whenever it can be generated by homogeneous elements, or equivalently whenever the homogenous components of any element of I also belong to I.

To each non-zero element $a\in R$ we may associate the smallest index $e=:v(a)$ such that $[a]_e\neq 0$; we set $v(0):=\infty$. The map $v:R\rightarrow\Gamma\cup\{\infty\}$ is a *semi-valuation*, which means that it satisfies $v(a+b)\geqslant\min(v(a),v(b))$ and $v(ab)\geqslant v(a)+v(b)$ for all $a,b\in R$. Given $\eta\in\bar{\Gamma}^>$, we call $[a]_{e;\eta}$ the *truncation* of a at *relative precision* η.

The *Newton polygon* of a non-zero polynomial

$$P=P_0+P_1x+\cdots+P_{d_x}x^{d_x}\in R[x]$$

of degree d_x is the lower border of the convex hull in $\mathbb{R}_{\geqslant 0}\times(\Gamma\cup\{\infty\})$ of the set of points

$$\{(i,v(P_i)):0\leqslant i\leqslant d_x,P_i\neq 0\}.$$

Figure 2.1 illustrates this definition with $R=\mathbb{K}[[z]]$ and $\Gamma=\mathbb{N}$. The Newton polygon is thus a broken line with edges $(i_0,j_0),\ldots,(i_r,j_r)$, with $r\geqslant 0$, such that:

- $0=i_0<i_1<\cdots<i_r$,
- $j_k=v(P_{i_k})$ for $k=0,\ldots,r$,
- $v(P_i)\geqslant\frac{i-i_k}{i_{k+1}-i_k}v(P_{i_{k+1}})+\frac{i_{k+1}-i}{i_{k+1}-i_k}v(P_{i_k})$, for all k and $i_k<i<i_{k+1}$ with $P_i\neq 0$,
- $v(P_i)>\frac{i-i_k}{i_{k+1}-i_k}v(P_{i_{k+1}})+\frac{i_{k+1}-i}{i_{k+1}-i_k}v(P_{i_k})$, for all k and $i<i_k$ or $i>i_{k+1}$ with $P_i\neq 0$.

Intuitively speaking, these conditions mean that $(i, v(P_i))$ lies on or above the Newton polygon. If $P_0 = 0$, then we have $i_0 := 0$ and $j_0 := \infty$. Any $k = 1, \ldots, r$ determines an edge E_k with vertices (i_{k-1}, j_{k-1}) and (i_k, j_k). The *Newton polynomial* associated to E_k is

$$\sum_{i \in \mathbb{N}, (i,j) \in E_k} [P_i]_j x^{i - i_{k-1}} \in R[x].$$

Whenever $\Gamma \subseteq \mathbb{R}$, the *slope* of E_k is $(j_k - j_{k-1}) / (i_k - i_{k-1})$. The first slope is $-\infty$ whenever $P_0 = 0$. Two consecutive edges have different slopes.

2.2. Explicit solutions *versus* factorization

In order to illustrate computations in algebraic extensions of $\mathbb{K}$ or $\mathbb{K}[[z]]$, let us first consider applying the Newton polygon method to an input polynomial of the form

$$P(z, x) = P_0(x) + z P_1(z, x),$$

where $P_0(x) \in \mathbb{K}[x]$ is a monic separable irreducible polynomial of degree d_x and $P_1 \in \mathbb{K}[z, x]$ has degree $< d_x$ in x. We then consider

$$P(z, x) = 0 \tag{2.1}$$

as a polynomial equation in x. The Newton polygon of P consists of a single edge starting at $(0, 0)$ and ending at $(d_x, 0)$; its slope is 0.

Equation (2.1) has a solution in $\mathbb{E}[[z]]$, where $\mathbb{E} := \mathbb{K}[x] / (P_0(x))$. Indeed, let α be the class of x in $\mathbb{E}$. Replacing x by $\alpha + \tilde{x}$ in (2.1), we obtain the new equivalent equation

$$P_0'(\alpha)\, \tilde{x} + \tfrac{1}{2} P_0''(\alpha)\, \tilde{x} + \cdots + \tfrac{1}{d_x!} P_0^{(d_x)}(\alpha)\, \tilde{x}^{d_x} = z P_1(z, \alpha + \tilde{x}). \tag{2.2}$$

The separability of P_0 implies $P_0'(\alpha) \neq 0$, which allows us to apply Hensel's lemma: there exists a unique solution $\tilde{x} \in \mathbb{E}[[z]]$ with valuation $v(\tilde{x}) > 0$ in z. This is the point of view of factoring P in terms of Puiseux expansions.

In terms of space complexity, we note that computations in $\mathbb{E}$ typically require d_x times more space than in $\mathbb{K}$. Fortunately, this is compensated by the fact that the "unique" solution $\tilde{x}$ to (2.2) actually describes all d_x solutions to (2.1) in $\bar{\mathbb{K}}[[z]]$. Indeed, any solution in $\bar{\mathbb{K}}[[z]]$ is obtained by substituting a root $\zeta \in \bar{\mathbb{K}}$ of P_0 for α in the expression of $\tilde{x}$.

From a time complexity point of view, the resolution of (2.2) can be done efficiently by using Newton's method. However, this involves truncated power series evaluations of expressions such as $P_1(z, \alpha + \tilde{x})$, where $\tilde{x} \in \mathbb{E}[[z]]$. These give in turn rise to modular compositions (with modulus P_0). Over general coefficient fields $\mathbb{K}$, no quasi-optimal algorithm (of complexity $d_x^{1+o(1)}$) is currently known for this task, so it is preferable to avoid such operations whenever possible. In particular, it is better to avoid working over algebraic extensions of the field $\mathbb{K}$ of coefficients.

In order to avoid modular compositions, one idea is to consider that equation (2.1) does not require any explicit resolution. In other words, it is already in such a simple form that we may essentially consider it as "solved". More generally, later in this paper, we will consider an equation $P(z, x) = 0$ as "solved" if and only if the Newton polygon of P with respect to suitable "contact coordinates" has a single slope for which the associated Newton polynomial is separable (and technically, irreducible).

The problem of solving a general equation $P(z,x)=0$ with $P\in\mathbb{K}[z,x]$ then reduces to the problem of factoring P as a product of "solved" polynomials. From this perspective, expressing the solutions of $P(z,x)=0$ as Puiseux series becomes a rewriting problem for "solved" polynomials, which is independent from the main resolution of the equation $P(z,x)=0$ itself.

2.3. Contact coordinates

Consider the polynomial equation in x over $\mathbb{Q}[[z]]$ given by

$$P(z,x):=x^4-6x^2-5z^2x+9=0. \tag{2.3}$$

When solving this equation by means of the Newton polygon method, we see that the Newton polygon of P has a single slope with associated Newton polynomial

$$x^4-6x^2+9=(x^2-3)^2.$$

In other words, all solutions of (2.3) are of the form $x=\alpha_1+o(1)$, where $\alpha_1^2-3=0$. Usually, the Newton polygon method proceeds by performing a change of variable

$$x=\alpha_1+\tilde{x},$$

while imposing the constraint $v(\tilde{x})>0$. So we are reduced to solving

$$P(z,\alpha_1+\tilde{x})=\tilde{x}^4+4\alpha_1\tilde{x}^3+12\tilde{x}^2-5z^2\tilde{x}-5z^2\alpha_1=0.$$

The Newton polygon has two edges: $((0,2),(2,0))$ and $((2,0),(4,0))$. Therefore $v(\tilde{x})=1$ and we have $12\tilde{x}^2-5z^2\alpha_1=0+o(z^2)$, so $\tilde{x}=\alpha_2z+o(z)$, where $12\alpha_2^2-5\alpha_1=0$. We proceed with the change of variable

$$\tilde{x}=\alpha_2z+z\tilde{\tilde{x}},$$

while imposing the constraint $v(\tilde{\tilde{x}})>0$. So we are now led to solving

$$P(z,\alpha_1+\alpha_2z+z\tilde{\tilde{x}})/z^2=0=24\alpha_2\tilde{\tilde{x}}+O(x^2)+O(z).$$

The unique value of $\tilde{\tilde{x}}$ can therefore be computed efficiently by means of the Newton iteration as a regular root of $P(z,\alpha_1+\alpha_2z+z\tilde{\tilde{x}})/z^2$. However, this means that we have to work over the algebraic extension $\mathbb{Q}[\alpha_1,\alpha_2]$.

The idea behind contact calculus is to avoid computing over this type of algebraic extensions, by working with respect to so-called contact coordinates instead. In the present example, the idea is to rewrite (2.3) as

$$(x^2-3)^2-5z^2x=0.$$

We next reinterpret this equation as

$$\varphi_2^2-5z^2\varphi_1=0, \tag{2.4}$$

where φ_1 and φ_2 are two new variables that are subject to the following constraints:

- $\varphi_1=x$, $\varphi_2=\varphi_1^2-3$,
- $v(\varphi_1)=0$ and $v(\varphi_2)>0$.

The variables φ_1 and φ_2 can be regarded as unknowns, with values in the ring of Puiseux series in z. These unknowns satisfy the system of equations

$$\varphi_1=x,\ \varphi_2=\varphi_1^2-3,\ \varphi_2^2-5z^2\varphi_1=0.$$

In other words, computing Puiseux expansions of solutions to P is equivalent to computing Puiseux expansions of solutions to the latter system. We note that φ_1^2-3 is separable in φ_1 and that the solutions for φ_1 begin with $\pm\sqrt{3}+O(z)$. Then $\varphi_2^2-5z^2\varphi_1$ is separable in φ_2 for each solution φ_1, so the system admits the following solutions:

$$\begin{array}{rclrcl}
\varphi_1 &=& \sqrt{3}+O(z) & \varphi_2 &=& \sqrt{5\sqrt{3}}\,z+O(z^2)\\
\varphi_1 &=& \sqrt{3}+O(z) & \varphi_2 &=& -\sqrt{5\sqrt{3}}\,z+O(z^2)\\
\varphi_1 &=& -\sqrt{3}+O(z) & \varphi_2 &=& \sqrt{5\sqrt{3}}\,\mathrm{i}\,z+O(z^2)\\
\varphi_1 &=& -\sqrt{3}+O(z) & \varphi_2 &=& -\sqrt{5\sqrt{3}}\,\mathrm{i}\,z+O(z^2)
\end{array}$$

After the change of variable $\varphi_2=z\,\tilde{\varphi}_2$, these solutions are regular roots of the following map modulo $O(z)$:

$$(\varphi_1,\tilde{\varphi}_2)\;\mapsto\;\begin{pmatrix} z\,\tilde{\varphi}_2-(\varphi_1^2-3)\\ \tilde{\varphi}_2^2-5\,\varphi_1\end{pmatrix}.$$

By means of the Newton iteration, these roots may be lifted efficiently to any required precision, and so may the corresponding solutions of P.

The variables φ_1 and φ_2 are called contact coordinates. Note that

$$P=(\varphi_1^2-3)^2+O(z^2),$$

so the germ of the curve defined by $\varphi_1^2-3=0$ approximates the one defined by $P=0$. From a geometric point of view, the two germs are "in contact".

Informally speaking, the Newton polygon of equation (2.4) in φ_2 has a single edge of vertices $(0,2)$ and $(2,0)$, with associated Newton polynomial $\varphi_2^2-5z^2\varphi_1$, whence $v(\varphi_2)=1$. The precise meaning of this "generalized Newton polygon" will be the purpose of section 7. Since the polynomial $(\varphi_2/z)^2-5\varphi_1$ is separable in φ_2/z, we consider the polynomial $\varphi_2^2-5z^2\varphi_1$ to be "solved".

Working with contact coordinates is a little bit tricky, since φ_1 and φ_2 are related by the equation $\varphi_2=\varphi_1^2-3$. Basic arithmetic operations and the Newton polygon method therefore have to be adapted with care. It turns out that "contact calculus" with respect to contact coordinates has a double flavor. At small orders τ in z, it boils down to working in towers of algebraic extensions of $\mathbb{Q}[[z]]/(z^\tau)$. At large orders in z, we may convert between polynomials in $\mathbb{Q}[[z]][x]$ and $\mathbb{Q}[[z]][\varphi_1,\varphi_2]/(\varphi_2-\varphi_1^2+3)$ through the mechanism of (x^2-3)-adic expansions.

In this paper, we have chosen to do most actual computations in $\mathbb{Q}[[z]][x]$, since fast algorithms for basic arithmetic operations in this ring are well known. However, conversions between the "plain coordinates" (z,x) and the "contact coordinates" (z,φ_1,φ_2) incur some precision loss. Fortunately, this precision loss can be controlled for the applications in this paper. Of course, it would be interesting to design a genuine fast arithmetic for contact coordinates without precision loss.

2.4. Towards general contact coordinates

Example (2.3) has several variants that motivate the general definition of contact coordinates in the next section. First of all, consider the equation

$$P(z,x):=\left(x-\tfrac{1}{1-z}\right)^4-6\left(x-\tfrac{1}{1-z}\right)^2-5z^{20}\left(x-\tfrac{1}{1-z}\right)+9=0. \tag{2.5}$$

In that case, the contact coordinates would rather be $\varphi_1 = x - \frac{1}{1-z}$ and $\varphi_2 = \varphi_1^2 - 3$. This illustrates that we do not systematically take $\varphi_1 = x$, although we always do have $\varphi_1 - x \in \mathbb{K}[[z]]$ when working over $\mathbb{K}$.

Let us next consider the equation

$$P(z,x) := ((x^2-3)^2 - 5z^2x)^3 + z^7x = 0. \tag{2.6}$$

In this case, we start with the same contact coordinates $\varphi_1 = x$ and $\varphi_2 = \varphi_1^2 - 3$ as for (2.3), but also need to introduce a third one $\varphi_3 = \varphi_2^2 - 5z^2\varphi_1$, subject to $v(\varphi_3) > 2$. In general, we may need to introduce as many as $\lceil \log d_x / \log 2 \rceil$ contact coordinates.

Yet another variant of (2.3) is the equation

$$P(z,x) := x^4 - 6x^2 + 9 - z^2 = 0 \tag{2.7}$$

We again use the same contact coordinates $\varphi_1 = x$ and $\varphi_2 = \varphi_1^2 - 3$ as for (2.3), but this time $P(z,x)$ rewrites into $\varphi_2^2 - z^2$, that can be factored:

$$\varphi_2^2 - z^2 = (\varphi_2 + z)(\varphi_2 - z).$$

In general, these types of factorizations can be expensive to compute with respect to the original coordinates and become more transparent for the contact coordinates.

2.5. Tschirnhaus transforms and approximate roots

Let us first consider the equation

$$P(z,x) = x^2 - \frac{2}{1-z}x + \frac{1}{(1-z)^2} - z^{100} = 0. \tag{2.8}$$

When solving this equation using the usual Newton polygon method, we find that there is a single slope $v(\varphi_1) = 0$, with $\varphi_1 = x$, for which the associated Newton polynomial $\varphi_1^2 - 2\varphi_1 + 1$ has a single root $\alpha = 1$ of multiplicity 2. This means that the leading terms of the Puiseux expansions are 1 and that the remaining terms can be found by performing the change of variable $x = 1 + \tilde{x}$ and solving the resulting equation for $\tilde{x}$:

$$\tilde{x}^2 - \frac{2z}{1-z}\tilde{x} + \frac{z^2}{(1-z)^2} - z^{100} = 0.$$

In a similar way, we find the leading term z of $\tilde{x}$, which has again multiplicity 2. We have to go on like this for 50 steps until reaching the equation

$$\hat{x}^2 - \frac{2z^{50}}{1-z}\hat{x} + \frac{z^{100}}{(1-z)^2} - z^{100} = 0.$$

At this point there are two possible dominant terms for $\hat{x}$ (namely $2z^{50}$ and z^{51}), each of multiplicity one, and we consider that we essentially solved the equation (more terms can be obtained efficiently using Newton's method).

From the complexity point of view, the problem is that we need to recompute a new equation at every step where we discover one more term of the expansion, which is quite expensive. A well known trick to replace the 50 steps by a single one is to compute the solution $\xi = z/(1-z)$ to the derivative of the equation, that is

$$2\xi - \frac{2z}{1-z} = 0,$$

and directly set $x=\xi+\tilde{x}$ instead of $x=1+\tilde{x}$. The new equation in $\tilde{x}$ then becomes

$$\tilde{x}^2-z^{100}=0,$$

after which the resolution process directly splits into two branches $\tilde{x}=z^{50}$ and $\tilde{x}=-z^{50}$. In general, for a d-fold leading term, we need to consider a solution ξ to the $(d-1)$-fold derivative of the equation. In that case, the change of variables $x=\xi+\tilde{x}$ is called a *Tschirnhaus transform*.

For general contact coordinates, things become more technical, but similar strategies apply. In general, if $\mathbb{A}$ is a ring with unity, if f is a monic polynomial of degree d in $\mathbb{A}[x]$, if m divides d, and if m is invertible in $\mathbb{A}$, then there exists a unique monic polynomial $g\in\mathbb{A}[x]$ of degree d/m such that $f-g^m$ has degree $<d-d/m$; see section 8.3. The polynomial g is called the m-th *approximate root* of f. If $m=d$, then the d-th approximate root $g=x-\xi\in\mathbb{A}[x]$ corresponds to the Tschirnhaus transform $x=\xi+\tilde{x}$. In general, the g-adic expansion of f writes as $g^m+u_{m-1}g^{m-1}+\cdots+u_1g+u_0$ where the u_i are polynomials in $\mathbb{A}[x]$ of degree $<\deg g=d/m$, so g is the m-th *approximate root* of f if and only if $u_{m-1}=0$.

2.6. Central shifts

Let us now consider yet another type of equation with an almost d-fold multiple solution

$$P(z,x):=(x-1)\,(x-1-z)\cdots(x-1-z-\cdots-z^{d-1})=0. \tag{2.9}$$

When solving the equation naively with the Newton polygon method, we obtain a d-fold branch $x=1+O(z)$ at the first step, a single branch $x=1+O(z^2)$ and a $(d-1)$-fold branch $x=1+z+O(z^2)$ at the second step, a single branch $x=1+z+O(z^3)$ and a $(d-2)$-fold branch $x=1+z+z^2+O(z^3)$ at the third step, and so on. From the complexity point of view, factoring out a single branch at every step leads to a cost

$$O(d+(d-1)+(d-2)+\cdots+1)=O(d^2)$$

as a function of d, which is not quasi-linear in d.

Using Tschirnhaus transforms is not really of any help. For instance, the $(d-1)$-fold derivative of the equation yields

$$d!\,\xi-(d-1)!\,(d+(d-1)\,z+\cdots+z^{d-1})=0,$$

with solution $\xi=1+(1-{}^1\!/_d)\,z+\cdots$. After the change of variable $x=\xi+\tilde{x}$, we still obtain one single branch and one $(d-1)$-fold branch.

What really helps in this situation is a way to determine the series

$$\xi=1+z+\cdots+z^{d-1}. \tag{2.10}$$

This series has the property that, after the change of variable $x=\xi+\tilde{x}$, we obtain the equivalent equation

$$(\tilde{x}+z+\cdots+z^{d-1})\,(\tilde{x}+z^2+\cdots+z^{d-1})\cdots(\tilde{x}+z^{d-1})\,\tilde{x}=0,$$

whose Newton polygon has $d-1$ edges. In particular, the resolution process now branches into d distinct parts of multiplicity one.

Computing the series (2.10) is equivalent to "solving" P. But instead of peeling off factors of degree one from the left-hand side of (2.9), we rather compute ξ with precision about $d/2$ in a recursive manner. This allows to factor P as the product of two polynomials of degree close to $d/2$, and to repeat this process in a recursive manner. Series such as (2.10) will be called *central shifts*. For a general polynomial equation $P(z,x)=0$, even within contact coordinates, the central shift will allow us to guarantee a suitably balanced factorization $P=A\,B$ for which A and B can recursively be factored with good complexity.

3. CONTACT CALCULUS

This section formalizes the concept of contact towers. The effective ground field is written $\mathbb{K}$ and the contact coordinates will be denoted by $\varphi_1,\ldots,\varphi_t$.

3.1. Weighted valuations

We endow $\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]$ with the weighted valuation, simply written "val", defined by $\operatorname{val} z=1$ and $\operatorname{val}\varphi_i=\gamma_i\in\mathbb{Q}$ for $i=1,\ldots,t$. With

$$\Gamma_t=\mathbb{N}+\gamma_1\,\mathbb{N}+\cdots+\gamma_t\,\mathbb{N},$$

this valuation induces a grading

$$\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]=\bigoplus_{e\in\Gamma_t}\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]_e,$$

where $\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]_e$ is the set of polynomials made only of terms of valuation e; notice that $\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]_0=\mathbb{K}$. When no confusion is possible, we drop "weighted".

Let R_t be the least common multiple of the denominators of $\gamma_1,\ldots,\gamma_t$. Then, the Chinese remainder theorem implies the following identity for the group completion $\bar{\Gamma}_t$ of Γ_t:

$$\bar{\Gamma}_t=\mathbb{Z}+\sum_{i=1}^{t}\mathbb{Z}\,\gamma_i=\mathbb{Z}\,\frac{1}{R_t}.$$

The integer R_t is called the *ramification index* of the valuation.

3.2. Contact towers

The following definition is central for the rest of this paper.

DEFINITION 3.1. *A **contact tower** of height t consists of:*

- *Variables $\varphi_1,\ldots,\varphi_t$, called contact coordinates;*
- *Defining polynomials $\Phi_i\in\mathbb{K}[[z]][\varphi_1,\ldots,\varphi_i]$ for $i=1,\ldots,t$;*
- *Rational numbers $\gamma_1,\ldots,\gamma_t$, called weights.*

These data are required to satisfy the following properties:

- *Φ_i is monic in φ_i of degree $d_i\geqslant 1$;*
- *$\deg_{\varphi_j}\Phi_i<d_j$, for $i=2,\ldots,t$ and $j=1,\ldots,i-1$;*
- *$\gamma_1\geqslant 0$ and $d_i\,\gamma_i\geqslant 1$ for $i=2,\ldots,t$;*

- *We endow* $\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]$ *with the weighted valuation defined by* $\operatorname{val} z=1$ *and* $\operatorname{val}\varphi_i=\gamma_i$ *for* $i=1,\ldots,t$. *We demand that:*
  - $\operatorname{val}\Phi_i=d_i\gamma_i$, *for* $i=1,\ldots,t$;
  - $\gamma_{i+1}>d_i\gamma_i$, *for* $i=1,\ldots,t-1$.

The tower is said to be ***reduced*** *when* $d_i\geqslant 2$ *for* $i=2,\ldots,t$. *Unless explicitly stated, the towers in this paper will be* ***almost reduced*** *in the sense that* $d_i\geqslant 2$ *for* $i=2,\ldots,t-1$.

The weights $\gamma_1,\ldots,\gamma_t$ will also be called the *contact slopes*, in reference to the slopes of the corresponding Newton polygons; see section 7.3. When a contact tower is almost reduced then $t=O(\log(d_1\cdots d_t))$ holds. The *degree* of the tower is $d_1\cdots d_t$.

Example 3.2. $t=1$, $\Phi_1=\varphi_1^2-3$, $\gamma_1=0$ form a contact tower of height 1.

Example 3.3. Consider the example (2.6). It turns out that $t=2$, $\Phi_1=\varphi_1^2-3$ and $\Phi_2=\varphi_2^2-5z^2\varphi_1$ form a contact tower with contact slopes $\gamma_1=0$, $\gamma_2=1$. Here we got γ_1 and γ_2 from $2\gamma_1=\operatorname{val}(\varphi_1^2)=\operatorname{val}(-3)=0$ and $2\gamma_2=\operatorname{val}(\varphi_2^2)=\operatorname{val}(5z^2\varphi_1)=2$.

We introduce another independent variable φ_{t+1} of weight γ_{t+1} and subject to the constraint $\gamma_{t+1}>d_t\gamma_t$. We also define the ideal

$$I_t:=(\Phi_1-\varphi_2,\ldots,\Phi_{t-1}-\varphi_t,\Phi_t-\varphi_{t+1})\subseteq\mathbb{K}[[z,\varphi_1,\ldots,\varphi_{t+1}]],$$

and the corresponding quotient ring

$$\mathbb{S}_t:=\mathbb{K}[[z,\varphi_1,\ldots,\varphi_{t+1}]]/I_t.$$

3.3. Canonical representation

In the following paragraphs, we show that $\mathbb{S}_t$ is effective for computations with finite truncation orders in z and φ_{t+1}. For this, we adopt the point of view of standard bases, while doing the proofs from scratch for completeness. We recall that the *lexicographic ordering* $<_{\text{lex}}$ on $\mathbb{N}^n$ is defined as follows:

$$(a_1,\ldots,a_n)<_{\text{lex}}(b_1,\ldots,b_n)\Longleftrightarrow\exists j\in\{1,\ldots,n\}\text{ such that }a_1=b_1,\ldots,a_{j-1}=b_{j-1},a_j<b_j.$$

We also introduce a total ordering $\prec$ with

$$z\prec\varphi_{t+1}\prec\varphi_1\prec\cdots\prec\varphi_t\prec 1$$

on the group $z^{\mathbb{N}}\varphi_1^{\mathbb{N}}\cdots\varphi_{t+1}^{\mathbb{N}}:=\{z^{e_0}\varphi_1^{e_1}\cdots\varphi_{t+1}^{e_{t+1}}:e_0,\ldots,e_{t+1}\in\mathbb{N}\}$ by

$$\begin{gathered}z^{e_0}\varphi_1^{e_1}\cdots\varphi_{t+1}^{e_{t+1}}\succ z^{f_0}\varphi_1^{f_1}\cdots\varphi_{t+1}^{f_{t+1}}\\ \Longleftrightarrow\\ e_0+e_1\gamma_1+\cdots+e_{t+1}\gamma_{t+1}<f_0+f_1\gamma_1+\cdots+f_{t+1}\gamma_{t+1}\text{ or}\\ \begin{cases}e_0+e_1\gamma_1+\cdots+e_{t+1}\gamma_{t+1}=f_0+f_1\gamma_1+\cdots+f_{t+1}\gamma_{t+1}\text{ and}\\ (e_t,\ldots,e_1,e_{t+1},e_0)>_{\text{lex}}(f_t,\ldots,f_1,f_{t+1},f_0).\end{cases}\end{gathered}$$

The ordering $\prec$ is a *monomial ordering* in the sense that

$$z^{e_0}\varphi_1^{e_1}\cdots\varphi_{t+1}^{e_{t+1}}\prec z^{f_0}\varphi_1^{f_1}\cdots\varphi_{t+1}^{f_{t+1}}$$

implies

$$z^{e_0+g_0}\varphi_1^{e_1+g_1}\cdots\varphi_{t+1}^{e_{t+1}+g_{t+1}}\prec z^{f_0+g_0}\varphi_1^{f_1+g_1}\cdots\varphi_{t+1}^{f_{t+1}+g_{t+1}}$$

for all $(g_0, \ldots, g_{t+1}) \in \mathbb{N}^{t+2}$. The *leading monomial* $\operatorname{lm} P$ of $P \in \mathbb{K}[[z, \varphi_1, \ldots, \varphi_{t+1}]]$ with respect to this ordering is defined to be the largest monomial with a non-zero coefficient in P. The set of monomials spanned by the leading monomials of the elements of an ideal I is written $\operatorname{lm} I$. Note that $z^{\mathbb{N}} \varphi_1^{\mathbb{N}} \cdots \varphi_{t+1}^{\mathbb{N}} \operatorname{lm} I \subseteq \operatorname{lm} I$. With the terminology of [28], the ordering $\prec$ is called a *negative weighted degree lexicographic local ordering*.

A *standard basis* of an ideal $I \subseteq \mathbb{K}[[z, \varphi_1, \ldots, \varphi_{t+1}]]$ with respect to the monomial ordering $\prec$ is a set of generators $g_1, \ldots, g_s$ such that the leading monomial of any polynomial in I is a multiple of the leading monomial of at least one of the g_i. In other words, $\operatorname{lm} I$ is generated by $\operatorname{lm} g_1, \ldots, \operatorname{lm} g_s$. A standard basis is said to be *reduced* whenever none of the non-leading monomials in the g_i belong to $\operatorname{lm} I$.

For the completeness, we now prove two well known lemmas from the theory of standard bases.

LEMMA 3.4. $\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_t)$ *is a reduced standard basis of* $(\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_t))$ *for* $\prec$.

Proof. Since $\Phi_1, \ldots, \Phi_t$ are independent of φ_{t+1}, it suffices to prove the lemma in $\mathbb{K}[[z, \varphi_1, \ldots, \varphi_t]]$. According to the assumptions, $\operatorname{in}(\Phi_i) = [\Phi_i]_{d_i \gamma_i}$ is monic of degree d_i in φ_i, and $\deg_{\varphi_j} \Phi_i < d_j$ for all $i = 1, \ldots, t$ and $j = 1, \ldots, i-1$. Therefore,

$$\operatorname{lm}(\operatorname{in}(\Phi_i)) = \operatorname{lm} \Phi_i = \varphi_i^{d_i}$$

for $i = 1, \ldots, t$. The lemma follows from general standard basis theory since the leading monomials of the $\operatorname{in}(\Phi_i)$ share no variable. For completeness, we give a dedicated proof.

Let us prove by induction on $i \geqslant 1$ that $\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_i)$ is a standard basis for the ideal $(\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_i))$ in $\mathbb{K}[[z, \varphi_1, \ldots, \varphi_i]]$. This clearly holds for $i = 1$. Let us assume that the induction hypothesis holds for some $i \geqslant 1$ and consider $H \in (\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_i))$. If $\deg_{\varphi_i} H \geqslant d_i$, then $\operatorname{lm} H$ is a multiple of $\operatorname{lm} \Phi_i$. Otherwise, we write

$$H(z, \varphi_1, \ldots, \varphi_i) = H_0(z, \varphi_1, \ldots, \varphi_{i-1}) + H_1(z, \varphi_1, \ldots, \varphi_{i-1})\, \varphi_i + \cdots + H_k(z, \varphi_1, \ldots, \varphi_{i-1})\, \varphi_i^k,$$

with $k < d_i$ and $H_k \neq 0$. Then

$$\begin{aligned} 0 &= H \bmod (\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_i)) \\ &= H_0 \bmod (\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_{i-1})) + \cdots + (H_k \bmod (\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_{i-1})))\, \varphi_i^k, \end{aligned}$$

so H_k belongs to the ideal $(\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_{i-1}))$ of $\mathbb{K}[[z, \varphi_1, \ldots, \varphi_{i-1}]]$. By the induction hypothesis, $\operatorname{lm} H_k$ is a multiple of $\varphi_j^{d_j}$ for some $j < i$, whence so is $\operatorname{lm} H$. It follows that $\operatorname{in}(\Phi_1), \ldots, \operatorname{in}(\Phi_t)$ is a standard basis. The fact that it is reduced is clear from degree considerations. □

For $k < l$, we define

$$S_{k,l} := (0, \ldots, 0, -\Phi_l, 0, \ldots, 0, \Phi_k, 0, \ldots, 0)$$

where $-\Phi_l$ stands at position k and Φ_k at position l. Note that the dot product $S_{k,l} \cdot (\Phi_1, \ldots, \Phi_t)$ is identically zero. For $G := (G_1, \ldots, G_t)$, the initial form of G, still written $\operatorname{in}(G)$, is defined as $(\operatorname{in}(G_1), \ldots, \operatorname{in}(G_t))$.

LEMMA 3.5. *If* $H_1 \operatorname{in}(\Phi_1) + \cdots + H_t \operatorname{in}(\Phi_t) = 0$ *for homogeneous* $H_1, \ldots, H_t \in \mathbb{K}[[z, \varphi_1, \ldots, \varphi_t]]$, *then*

$$(H_1, \ldots, H_t) \in \sum_{1 \leqslant k < l \leqslant t} \mathbb{K}[[z, \varphi_1, \ldots, \varphi_t]] \operatorname{in}(S_{k,l}). \tag{3.1}$$

Proof. We prove the lemma by induction on t. For $t=0$, we have nothing to prove, so assume that $t\geqslant 1$. Extracting homogeneous components, we may assume without loss of generality that

$$\mathrm{val}(H_i\,\mathrm{in}(\Phi_i))=\mathrm{val}(H_j\,\mathrm{in}(\Phi_j))$$

whenever $H_i\neq 0$ and $H_j\neq 0$. By the induction hypothesis, we may also assume that $H_t\neq 0$. Long division of H_t by $\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_{t-1})$ yields

$$H_t=Q_1\,\mathrm{in}(\Phi_1)+\cdots+Q_{t-1}\,\mathrm{in}(\Phi_{t-1})+R$$

for homogeneous polynomials $Q_1,\ldots,Q_{t-1},R\in\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]$ with $\deg_{\varphi_i}R<d_i$, for $i=1,\ldots,t-1$.

Reducing the relation $H_1\,\mathrm{in}(\Phi_1)+\cdots+H_t\,\mathrm{in}(\Phi_t)=0$ modulo $(\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_{t-1}))$, we obtain

$$R\,\mathrm{in}(\Phi_t)=0\bmod(\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_{t-1})).$$

Since Φ_t is monic in φ_t, it follows that $R=0\bmod(\mathrm{in}(\Phi_1),...,\mathrm{in}(\Phi_{t-1}))$, and thus that $R=0$. Consequently, we obtain

$$(H_1,\ldots,H_t)=(H_1,\ldots,H_{t-1},Q_1\,\mathrm{in}(\Phi_1)+\cdots+Q_{t-1}\,\mathrm{in}(\Phi_{t-1})),$$

which implies

$$\begin{aligned}(\tilde H_1,\ldots,\tilde H_{t-1},0) &:= (H_1+Q_1\,\mathrm{in}(\Phi_t),\ldots,H_{t-1}+Q_{t-1}\,\mathrm{in}(\Phi_t),0)\\ &= (H_1,\ldots,H_t)-Q_1\,\mathrm{in}(S_{1,t})-\cdots-Q_{t-1}\,\mathrm{in}(S_{t-1,t}).\end{aligned}$$

Let $i=1,\ldots,t-1$. If $Q_i=0$, then $\tilde H_i=H_i$ is homogeneous. Otherwise, we have

$$\begin{aligned}\mathrm{val}(Q_i\,\mathrm{in}(\Phi_t)) &= \mathrm{val}\,H_t-\mathrm{val}\,\Phi_i+\mathrm{val}\,\Phi_t\\ &= \mathrm{val}(H_t\Phi_t)-\mathrm{val}\,\Phi_i\\ &= \mathrm{val}(H_i\Phi_i)-\mathrm{val}\,\Phi_i\\ &= \mathrm{val}\,H_i,\end{aligned}$$

so $\tilde H_i$ is also homogeneous. Each $\tilde H_i$ can be expanded with respect to φ_t:

$$\tilde H_i=\sum_{j\geqslant 0}\tilde H_{i,j}\,\varphi_t^j,$$

with $\tilde H_{i,j}\in\mathbb{K}[[z,\varphi_1,\ldots,\varphi_{t-1}]]$. Then we have

$$\begin{aligned}0 &= \left(\sum_{j\geqslant 0}\tilde H_{1,j}\varphi_t^j\right)\mathrm{in}(\Phi_1)+\cdots+\left(\sum_{j\geqslant 0}\tilde H_{t-1,j}\varphi_t^j\right)\mathrm{in}(\Phi_{t-1})\\ &= \sum_{j\geqslant 0}(\tilde H_{1,j}\,\mathrm{in}(\Phi_1)+\cdots+\tilde H_{t-1,j}\,\mathrm{in}(\Phi_{t-1}))\,\varphi_t^j,\end{aligned}$$

which implies $\tilde H_{1,j}\,\mathrm{in}(\Phi_1)+\cdots+\tilde H_{t-1,j}\,\mathrm{in}(\Phi_{t-1})=0$ for all $j\geqslant 0$. We conclude by applying the induction hypothesis. □

LEMMA 3.6. *If $H_1\,\mathrm{in}(\Phi_1)+\cdots+H_t\,\mathrm{in}(\Phi_t)=0$ holds with H_i homogeneous in $\mathbb{K}[[z,\varphi_1,...,\varphi_{t+1}]]$, then there exist $G_1,...,G_t$ in $\mathbb{K}[[z,\varphi_1,...,\varphi_{t+1}]]$ such that $G_1(\Phi_1-\varphi_2)+\cdots+G_t(\Phi_t-\varphi_{t+1})=0$ and $\mathrm{in}(G_i)=H_i$ for $i=1,\ldots,t$.*

Proof. We expand each H_i with respect to the variable φ_{t+1}:

$$H_i=\sum_{j\geqslant 0}H_{i,j}\,\varphi_{t+1}^j,\quad\text{where } H_{i,j}\in\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]].$$

For all $j \geqslant 0$, we get

$$H_{1,j}\,\mathrm{in}(\Phi_1) + \cdots + H_{t,j}\,\mathrm{in}(\Phi_t) = 0,$$

so Lemma 3.5 ensures the existence of homogeneous polynomials $Q_{k,l}^{\{j\}}$ in $\mathbb{K}[[z,\varphi_1,\ldots,\varphi_t]]$ such that

$$(H_{1,j},\ldots,H_{t,j}) = \sum_{1 \leqslant k < l \leqslant t} Q_{k,l}^{\{j\}}\,\mathrm{in}(S_{k,l}).$$

Letting $Q_{k,l} := \sum_{j \geqslant 0} Q_{k,l}^{\{j\}}\,\varphi_{t+1}^j$, we deduce that

$$(H_1,\ldots,H_t) = \sum_{1 \leqslant k < l \leqslant t} Q_{k,l}\,\mathrm{in}(S_{k,l}).$$

Since the H_i are homogeneous, up to replacing the $Q_{k,l}$ by their homogeneous components of suitable valuation, we may assume that

- the $Q_{k,l}$ are homogeneous,
- $\mathrm{val}\,H_k = \mathrm{val}(Q_{k,l}\,\mathrm{in}(\Phi_l))$ holds for all $k < l$ with $H_k \neq 0$ and $Q_{k,l} \neq 0$,
- $\mathrm{val}\,H_l = \mathrm{val}(Q_{k,l}\,\mathrm{in}(\Phi_k))$ holds for all $k < l$ with $H_l \neq 0$ and $Q_{k,l} \neq 0$.

For $k < l$, we introduce the vectors

$$\bar{S}_{k,l} := (0,\ldots,0,-(\Phi_l - \varphi_{l+1}),0,\ldots,0,\Phi_k - \varphi_{k+1},0,\ldots,0),$$

where $-(\Phi_l - \varphi_{l+1})$ stands at position k and $\Phi_k - \varphi_{k+1}$ at position l, so the dot product $\bar{S}_{k,l} \cdot (\Phi_1 - \varphi_2,\ldots,\Phi_t - \varphi_{t+1})$ is identically zero. We set

$$(G_1,\ldots,G_t) := \sum_{1 \leqslant k < l \leqslant t} Q_{k,l}\,\bar{S}_{k,l}.$$

Using the fact that $\gamma_{i+1} = \mathrm{val}\,\varphi_{i+1} > \mathrm{val}\,\Phi_i = d_i\,\gamma_i$, we conclude that

$$\mathrm{in}(G_1,\ldots,G_t) = \mathrm{in}\left(\sum_{1 \leqslant k < l \leqslant t} Q_{k,l}\,\bar{S}_{k,l}\right) = \sum_{1 \leqslant k < l \leqslant t} Q_{k,l}\,\mathrm{in}(S_{k,l}) = (H_1,\ldots,H_t). \qquad \square$$

LEMMA 3.7. *We have* $\mathrm{in}(I_t) = (\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_t))$.

Proof. Let $P \in I_t$, so there exist $P_1,\ldots,P_t \in \mathbb{K}[[z,\varphi_1,\ldots,\varphi_{t+1}]]$ with

$$P = P_1\,(\Phi_1 - \varphi_2) + \cdots + P_t\,(\Phi_t - \varphi_{t+1}).$$

We repeat the following operations:

1. Let $\eta := \min\,(\mathrm{val}\,P_i + \mathrm{val}\,\Phi_i : i = 1,\ldots,t)$. Since $\mathrm{val}\,\varphi_{i+1} > \mathrm{val}\,\Phi_i = d_i\,\gamma_i$, we always have $\eta \leqslant \mathrm{val}\,P$. If $\eta = \mathrm{val}\,P$, then we obtain a relation

$$\mathrm{in}(P) = \sum_{i \in \mathcal{S}} \mathrm{in}(P_i)\,\mathrm{in}(\Phi_i)$$

   where $\mathcal{S}$ is the non-empty subset of indices i such that $\mathrm{val}\,P_i = \eta - d_i\,\gamma_i$, so we are done.
2. Otherwise $\eta < \mathrm{val}\,P$, hence $\sum_{i \in \mathcal{S}} \mathrm{in}(P_i)\,\mathrm{in}(\Phi_i) = 0$. The latter relation can be lifted to $\sum_{i=1}^t G_i\,(\Phi_i - \varphi_{t+1}) = 0$ with $\mathrm{in}(G_i) = \mathrm{in}(P_i)$ for $i = 1,\ldots,t$, by Lemma 3.6.
3. Replace the vector $(P_1,\ldots,P_t)$ by $(P_1,\ldots,P_t) - (G_1,\ldots,G_t)$, and go to step 1.

Thanks again to the assumption $\mathrm{val}\,\varphi_{i+1} > \mathrm{val}\,\Phi_i = d_i\,\gamma_i$, the relation $P = P_1\,(\Phi_1 - \varphi_2) + \cdots + P_t\,(\Phi_t - \varphi_{t+1})$ holds after each iteration. Furthermore, the value of η strictly increases, so the process converges. We conclude that $\mathrm{in}(P) \in (\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_t))$. □

PROPOSITION 3.8. *$\Phi_1 - \varphi_2, \ldots, \Phi_t - \varphi_{t+1}$ is a standard basis of I_t for $\prec$. It is reduced whenever the contact tower is reduced.*

Proof. Assume that $P \neq 0$ belongs to I_t. Then $\operatorname{lm} P = \operatorname{lm}(\operatorname{in}(P))$, so Lemma 3.7 implies that $\operatorname{lm} \Phi_i = \operatorname{lm}(\operatorname{in}(\Phi_i)) \,|\, \operatorname{lm} P$ for some i. □

From Proposition 3.8, we know that an element a of $\mathbb{S}_t$ can be uniquely represented by a polynomial $A(\varphi_1, \ldots, \varphi_{t+1}) \in \mathbb{K}[[z, \varphi_{t+1}]][\varphi_1, \ldots, \varphi_t]$ of partial degree $<d_i$ in φ_i for $i = 1, \ldots, t$. We call A the *canonical representative* of a.

We introduce contact towers as a tool for the local resolution of polynomial equations. For this, we will often reduce to the case when all the roots of the polynomial are in the local region of interest. Such polynomials are said to be "clustered":

DEFINITION 3.9. *An element a in $\mathbb{S}_t$ is a **clustered polynomial** if its canonical representative is monic in φ_{t+1} of degree $l \geqslant 1$ and if $v(a) = l\,\gamma_{t+1}$.*

Example 3.10. For the contact tower of Definition 3.1, the polynomial Φ_i is a clustered polynomial regarded in $\mathbb{S}_i$ for $i = 1, \ldots, s$.

3.4. Arithmetic in contact towers

The theory of standard bases comes with algorithms to compute modulo ideals given by standard bases. We now detail how to perform such computations in the case of $\mathbb{S}_t$.

Additions, subtractions and scalar multiplications are straightforward, but other operations require an appropriate treatment of "carries" within Φ_i-adic expansions. For the contact coordinates of Example 3.3, let us briefly illustrate how carries occur during multiplications.

Example 3.11. In Example 3.3 the polynomials $\Phi_1 = \varphi_1^2 - 3$ and $\Phi_2 = \varphi_2^2 - 5\,z^2\,\varphi_1$ form a contact tower with contact slopes $\gamma_1 = 0$, $\gamma_2 = 1$.

Let us first illustrate the computation of a product modulo I_2:

$$a := (\varphi_3 + \varphi_1\,\varphi_2)\,(\varphi_1\,\varphi_3 - 3\,z\,\varphi_2 + \varphi_1) \bmod I_2.$$

Doing a direct polynomial multiplication, we obtain

$$a = \varphi_1\,\varphi_3^2 + (\varphi_1^2\,\varphi_2 - 3\,z\,\varphi_2 + \varphi_1)\,\varphi_3 - 3\,z\,\varphi_1\,\varphi_2^2 + \varphi_1^2\,\varphi_2 \bmod I_2,$$

which is not in canonical representation since the degrees in φ_1 and φ_2 are too high. We thus have to rewrite

$$\varphi_1^2\,\varphi_2 = (\varphi_2 + 3)\,\varphi_2 \bmod I_2 = \varphi_3 + 3\,\varphi_2 + 5\,z^2\,\varphi_1 \bmod I_2$$

and

$$\varphi_1\,\varphi_2^2 = \varphi_1\,\varphi_3 + 5\,z^2\,\varphi_1^2 \bmod I_2 = \varphi_1\,\varphi_3 + 5\,z^2\,\varphi_2 + 15\,z^2 \bmod I_2.$$

At the end, this leads to the following canonical representation for a modulo I_2:

$$a = (\varphi_1 + 1)\,\varphi_3^2 + ((3 - 3z)\,\varphi_2 + (1 - 3z + 5z^2)\,\varphi_1 + 1)\,\varphi_3 + (3 + 15z^3)\,\varphi_2 + 5z^2\varphi_1 + 45z^3 \bmod I_2.$$

The canonical representative A of an element a in $\mathbb{S}_t$ can uniquely be written as

$$A = \sum_{i \geqslant 0} A_i(\varphi_1, \ldots, \varphi_t)\,\varphi_{t+1}^i,$$

where $A_i \in \mathbb{K}[[z]][\varphi_1, \ldots, \varphi_t]$ satisfies $\deg_{\varphi_j} A_i < d_j$ for $j = 1, \ldots, t$. Similarly, the canonical representative B of another element $b \in \mathbb{S}_t$ can be written as

$$B = \sum_{i \geqslant 0} B_i(\varphi_1, \ldots, \varphi_t) \, \varphi_{t+1}^i.$$

Now assume that $B_i = 0$ for sufficiently large values of i. Then we may regard b as a univariate polynomial in φ_{t+1}: the "degree of b in φ_{t+1}", written $\deg_{\varphi_{t+1}} b$, is defined as the largest integer n such that $B_n \neq 0$. We say that b is "monic of degree n in φ_{t+1}" when $B_n = 1$ and $B_i = 0$ for $i > n$.

Now we ask whether we can define and compute a generalized Euclidean division of a by b. The answer is "yes" under suitable assumptions. More generally, the following lemma shows that there exists a unique b-adic expansion of a.

LEMMA 3.12. *With the above notation let us assume that b is clustered at $\mathbb{P}_t$ and has degree $n \geqslant 1$ in φ_{t+1}. Then, there exist unique elements q_i in $\mathbb{P}_t$ satisfying*

$$a = \sum_{i \geqslant 0} q_i b^i,$$

and such that $\deg_{\varphi_{t+1}} q_i < n$ *for all $i \geqslant 0$.*

Proof. This lemma is a reformulation of what we have already proved with contact coordinates. In fact, it suffices to increase the height of the tower by one, to set

$$\Phi_{t+1} := \sum_{i=0}^{n} B_i(\varphi_1, \ldots, \varphi_t) \, \varphi_{t+1}^i,$$

$d_{t+1} := n$, and to assign any weight $\gamma_{t+2} > d_{t+1} \gamma_{t+1}$ to the new variable φ_{t+2}. Therefore, the canonical representative of the image of a in $\mathbb{S}_{t+1}$ is given by

$$a = \sum_{i \geqslant 0} E_i(\varphi_1, \ldots, \varphi_{t+1}) \, \varphi_{t+2}^i,$$

where $\deg_{\varphi_j} E_i < d_i$ for $j = 1, \ldots, t+1$. Consequently the above b-adic expansion of a exists with $q_i := E_i(\varphi_1, \ldots, \varphi_{t+1})$.

As for uniqueness, let the q_i be as in the statement of the lemma, and let us write them

$$q_i = Q_i(\varphi_1, \ldots, \varphi_{t+1})$$

with $\deg_{\varphi_{t+1}} Q_i < d_{t+1}$. The Q_i must satisfy

$$\sum_{i \geqslant 0} A_i(\varphi_1, \ldots, \varphi_t) \, \varphi_{t+1}^i - \sum_{i \geqslant 0} Q_i(\varphi_1, \ldots, \varphi_{t+1}) \, \Phi_{t+1}^i(\varphi_1, \ldots, \varphi_t) \in I_t,$$

that implies

$$\sum_{i \geqslant 0} A_i(\varphi_1, \ldots, \varphi_t) \, \varphi_{t+1}^i - \sum_{i \geqslant 0} Q_i(\varphi_1, \ldots, \varphi_{t+1}) \, \varphi_{t+2}^i \in I_{t+1} = I_t + (\Phi_{t+1} - \varphi_{t+2}).$$

It follows that the Q_i do exist and are uniquely determined by the canonical representative of a in $\mathbb{S}_{t+1}$. □

DEFINITION 3.13. *With the notation of Lemma 3.12, $\sum_{i \geqslant 1} q_i b^{i-1}$ and q_0 are respectively called the* ***quotient*** *and* ***remainder*** *of the Euclidean division of a by b, and are written $\sum_{i \geqslant 1} q_i b^{i-1} = a \operatorname{quo} b$ and $q_0 = a \operatorname{rem} b$.*

Example 3.14. With the contact coordinates of Example 3.11, take

$$a := \varphi_2 \varphi_3 \text{ and } b := \varphi_3 - \varphi_2.$$

We have

$$\begin{aligned} a &= \varphi_2 b + \varphi_2^2 \bmod I_2 \\ &= \varphi_2 b + \varphi_3 + 5 z^2 \varphi_1 \bmod I_2 \\ &= (\varphi_2 + 1)\, b + \varphi_2 + 5 z^2 \varphi_1 \bmod I_2. \end{aligned}$$

Therefore the division of a by b writes $a = q b + r$ with $q := \varphi_2 + 1$ and $r := \varphi_2 + 5 z^2 \varphi_1$.

3.5. Plain coordinates

In what follows, we will restrict ourselves to computations with "polynomials" in

$$\mathbb{P}_t := \mathbb{K}[[z]][\varphi_1, \ldots, \varphi_{t+1}] / I_t$$

instead of "series" in $\mathbb{S}_t$. Elements a in $\mathbb{P}_t$ can be represented canonically by polynomials $A(\varphi_1, \ldots, \varphi_{t+1}) \in \mathbb{K}[[z]][\varphi_1, \ldots, \varphi_{t+1}]$ of partial degrees $< d_i$ in φ_i for $i = 1, \ldots, t$. In order to alleviate terminology, we call elements in $\mathbb{P}_t$ *contact polynomials*, in which case we always assume that a is represented canonically as a polynomial $c_l \varphi_{t+1}^l + \cdots + c_0$ in φ_{t+1} with $c_0, \ldots, c_l \in \mathbb{P}_{t-1}$; we will also call this the *contact representation*. At the same time, we will keep the terminology of "canonical representatives" whenever we need to carefully distinguish between a and its actual polynomial representative A.

By what precedes, we may recursively expand elements in $\mathbb{P}_t$ with respect to φ_{t+1}, φ_t,..., until φ_1. However, from a computational point of view such *recursive Φ-adic expansions* are expensive. Indeed such expansions are reminiscent of computations modulo triangular sets, so it would be interesting to examine whether the algorithms of [45] could be adapted or not. In this subsection we follow another direction that leads to efficient algorithms. The key idea is to rewrite elements in $\mathbb{P}_t$ with respect to the *plain coordinates z* and x. For this purpose, we introduce the following polynomials:

$$\begin{aligned} \Psi_0(x) &:= x, \\ \Psi_i(x) &:= \Phi_i(\Psi_0(x), \ldots, \Psi_{i-1}(x)), \qquad i = 1, \ldots, t. \end{aligned}$$

Note that Ψ_i is monic of degree $d_1 \cdots d_i$. The change of representation is presented in the following lemma:

LEMMA 3.15. *The following map is a $\mathbb{K}[[z]]$-algebra isomorphism:*

$$\begin{aligned} \Pi_t\colon\ \mathbb{P}_t &\cong \mathbb{K}[[z]][x] \\ \varphi_{i+1} &\longmapsto \Psi_i(x) \textit{ for } i = 0, \ldots, t. \end{aligned} \tag{3.2}$$

Proof. We introduce the following auxiliary evaluation morphism over $\mathbb{K}[[z]]$:

$$\begin{aligned} \tilde{\Pi}_t\colon\ \mathbb{K}[[z]][\varphi_1, \ldots, \varphi_{t+1}] &\longrightarrow \mathbb{K}[[z]][x] \\ \varphi_{i+1} &\longmapsto \Psi_i(x) \text{ for } i = 0, \ldots, t. \end{aligned}$$

For $i = 1, \ldots, t$, we have

$$\tilde{\Pi}_t(\Phi_i(\varphi_1, \ldots, \varphi_i) - \varphi_{i+1}) = \Phi_i(\Psi_0(x), \Psi_1(x), \ldots, \Psi_{i-1}(x)) - \Psi_i(x) = 0,$$

so $\Phi_i(\varphi_1, \ldots, \varphi_i) - \varphi_{i+1} \in \ker \tilde{\Pi}_t$ and Π_t is well defined.

Let us prove by induction on t that Π_t is bijective. This is clear when $t = 0$, so assume that $t \geqslant 1$. Let $P \in \mathbb{K}[[z]][x]$ be of degree $< l d$ for some integer $l \geqslant 0$. The Ψ_t-adic expansion of P yields a polynomial

$$Q_t(x, \psi_{t+1}) = Q_{t,0}(x) + \cdots + Q_{t,l-1}(x)\, \psi_{t+1}^{l-1} \in \mathbb{K}[[z]][x, \psi_{t+1}]$$

such that $Q_t(x, \Psi_t(x)) = P(x)$ and $Q_{t,i} \in \mathbb{K}[[z]][x]_{<d}$ for $i = 0, \ldots, l-1$. Next we recursively compute $\hat{Q}_{t,i}(\varphi_1, \ldots, \varphi_t) := \Pi_{t-1}^{-1}(Q_{t,i})$ for $i = 0, \ldots, l-1$. This yields

$$\hat{P}(\varphi_1, \ldots, \varphi_{t+1}) := \hat{Q}_{t,0}(\varphi_1, \ldots, \varphi_t) + \cdots + \hat{Q}_{t,l-1}(\varphi_1, \ldots, \varphi_t)\, \varphi_{t+1}^{l-1}$$

with $P = \Pi_t(\hat{P})$. This proves that Π_t is surjective.

Now let $\hat{P} \in \ker \Pi_t$ be non-zero. Since $\deg_x(\Pi_t(\hat{P})) \geqslant d_1 \cdots d_t \deg_{\varphi_{t+1}} \hat{P}$, we must have $\deg_{\varphi_{t+1}} \hat{P} \leqslant 0$, that is $\hat{P} \in \ker \Pi_{t-1}$. The induction hypothesis implies that $\hat{P} = 0$. □

3.6. Conversion costs

As seen in the proof of Lemma 3.15, the isomorphism Π_t corresponds to a cascade of Φ_i-adic expansions for $i = 1, \ldots, t$. We begin with recalling known costs for univariate expansions over an effective ring $\mathbb{A}$.

LEMMA 3.16. *Let $f \in \mathbb{A}[x]_{<n}$ and let $g \in \mathbb{A}[x]$ be monic of degree d. The g-adic expansion of f can be computed using $O(\mathsf{M}(n) \log(\lceil n/d \rceil + 1))$ operations in $\mathbb{A}$.*

Proof. Without loss of generality, we may assume that $n = 2^k d$ for some integer $k \geqslant 0$. We compute $g^2, g^4, \ldots, g^{2^{k-1}}$ using $O(\mathsf{M}(n))$ operations in $\mathbb{A}$. We divide f by $g^{2^{k-1}}$, so $f = f_0 + f_1 g^{2^{k-1}}$ with $\deg f_0 < 2^{k-1} d$ and $\deg f_1 < 2^{k-1} d$. Then we compute the g-adic expansion of f_0 and f_1 in a recursive manner so the expansion of f is obtained by merging those of f_0 and f_1. The depth of the recursive calls is $k = O(\log(\lceil n/d \rceil + 1))$. The sum of the costs of the operations at depth l is $O(\mathsf{M}(n))$, whence the claimed bound. □

LEMMA 3.17. *Let $f_0, \ldots, f_l$ be polynomials in $\mathbb{A}[x]_{<d}$ and let g be a monic polynomial of degree d in $\mathbb{A}[x]$. Then, $f_0 + f_1 g + \cdots + f_{l-1} g^{l-1}$ can be computed using $O(\mathsf{M}(n) \log(\lceil n/d \rceil + 1))$ operations in $\mathbb{A}$, where $n := d\,l$.*

Proof. Without loss of generality, we may assume that $l = 2^k$ for some integer $k \geqslant 0$. We compute $g^2, g^4, \ldots, g^{2^{k-1}}$ with $O(\mathsf{M}(n))$ operations in $\mathbb{K}$. In a recursive manner we compute $F_0 := f_0 + f_1 g + \cdots + f_{l/2-1} g^{l/2-1}$ and $F_1 := f_{l/2} + f_{l/2+1} g + \cdots + f_{l-1} g^{l/2-1}$, and finally we compute $F_0 + g^{l/2} F_1$ with $O(\mathsf{M}(n))$ operations in $\mathbb{A}$. The rest of the complexity analysis follows as in the proof of Lemma 3.16. □

Remark 3.18. When univariate polynomial multiplication is done using FFT techniques, we note that it is possible to save a factor $\log \log n$ in Lemmas 3.16 and 3.17; see [40].

PROPOSITION 3.19. *Let $d := d_1 \cdots d_t$, and write $n = d\,l$. One evaluation of Π_t modulo $O(z^\tau)$ at an element of degree $<l$ in φ_{t+1} (for the canonical representation), and one evaluation of Π_t^{-1} modulo $O(z^\tau)$ at a polynomial of degree $<n$ in x, both take $O(\mathsf{M}(n\,\tau) \log n)$ operations in $\mathbb{K}$.*

Proof. Let $P \in \mathbb{K}[[z]][x]$ be of degree $<n$. Its Ψ_t-adic expansion takes $O(\mathsf{M}(n\,\tau) \log l)$ operations in $\mathbb{K}$ by Lemma 3.16. Then, we perform $l = n/d$ calls to Π_{t-1} in degree $<d$. A straightforward induction gives a total complexity bound

$$\begin{aligned} & O(\mathsf{M}(n\,\tau) \log l + l\,\mathsf{M}(d\,\tau) \log d_t + l\,d_t\,\mathsf{M}((d/d_t)\,\tau) \log d_{t-1} + \cdots \\ & \quad + l\,d_t \cdots d_3\,\mathsf{M}(d_1 d_2\,\tau) \log d_2) \\ = \ & O(\mathsf{M}(n\,\tau) \log n). \end{aligned}$$

The backward conversion makes use of Lemma 3.17, and the complexity analysis is similar. □

PROPOSITION 3.20. *Let $d := d_1 \cdots d_t$, and let a and b be two contact polynomials in $\mathbb{P}_t$ of degree $<l$ in φ_{t+1} and given with precision $O(z^\tau)$. Then, the product $a\,b$ can be computed modulo $O(z^\tau)$ with $O(\mathsf{M}(n\,\tau)\log n)$ operations in $\mathbb{K}$, where $n := l\,d$.*

Proof. The product is computed via the following formula:

$$a\,b = \Pi_t^{-1}(\Pi_t(a)\,\Pi_t(b)) + O(z^\tau).$$

By Proposition 3.19 the cost of the conversions amounts to $O(\mathsf{M}(n\,\tau)\log n)$. Multiplying $\Pi_t(a)$ and $\Pi_t(b)$ modulo $O(z^\tau)$ incurs $O(\mathsf{M}(n\,\tau))$. □

For actual machine computations, we only work with truncated power series. The decision of whether it is more efficient to use contact representations or the plain representations in $\mathbb{K}[[z]][x]$ depends on the truncation order. For sufficiently small orders, the "carries" can be neglected, which makes it more efficient to conduct computations directly in the contact representation. For large orders, and thus for asymptotic complexity analyses, the overhead of the conversions using isomorphism (3.2) becomes small, and it is more efficient to perform arithmetic operations in $\mathbb{K}[[z]][x]$. Until the end of the paper we perform most of the computations directly in $\mathbb{K}[[z]][x]$, and thereby minimize the number of conversions.

The isomorphism (3.2) also allows for efficient Euclidean divisions in $\mathbb{P}_t$ with respect to φ_{t+1}, in the sense of Lemma 3.12. In fact, let a and b be as in the lemma, and compute the division of $\Pi_t(a)$ by $\Pi_t(b)$:

$$\Pi_t(a) = Q\,\Pi_t(b) + R,$$

where $\deg R < \deg(\Pi_t(b)) = d_1 \cdots d_t n$. The degree in φ_{t+1} of the canonical representative of $\Pi_t^{-1}(R)$ is therefore $<n$. It follows that $\Pi_t^{-1}(R)$ equals the remainder $r = q_0$ of Definition 3.13. Since both a and b have finite degree in φ_{t+1}, we note that this also yields an easier way to define the division in comparison to Lemma 3.12. In particular, the assumption that $\operatorname{val} B = n\,\gamma_{t+1}$ is not needed.

PROPOSITION 3.21. *Let $d := d_1 \cdots d_t$, and let a and b be two contact polynomials in $\mathbb{P}_t$ of degree $<l$ in φ_{t+1}, and given with precision $O(z^\tau)$. If b is monic in φ_{t+1}, then the division of a by b can be computed modulo $O(z^\tau)$ with $O(\mathsf{M}(n\,\tau)\log n)$ operations in $\mathbb{K}$, where $n := l\,d$.*

Proof. The division $a = q\,b + r$ is computed as above via

$$\Pi_t(a) = \Pi_t(q)\,\Pi_t(b) + \Pi_t(r).$$

By Proposition 3.19 the conversions take $O(\mathsf{M}(n\,\tau)\log n)$. Dividing $\Pi_t(a)$ by $\Pi_t(b)$ modulo $O(z^\tau)$ incurs $O(\mathsf{M}(n\,\tau))$. □

3.7. Semi-valuations in contact towers

Recall that Γ_{t+1} represents the valuation semi-group of the contact tower

$$\Gamma_{t+1} := \mathbb{N} + \mathbb{N}\,\gamma_1 + \cdots + \mathbb{N}\,\gamma_{t+1}.$$

PROPOSITION 3.22. *Let $\bar{\varphi}_i$ stand for the image of φ_i in $\mathbb{S}_t$. The valuation $v: \mathbb{K}[[z]] \rightarrow \mathbb{N} \cup \{\infty\}$ extends to a semi-valuation $\mathbb{S}_t \rightarrow \Gamma_{t+1} \cup \{\infty\}$ with $v(\bar{\varphi}_i) := \gamma_i$ for $i = 1, \ldots, t+1$, and such that $\mathbb{S}_t$ inherits the weighted grading of $\mathbb{K}[[z, \varphi_1, \ldots, \varphi_{t+1}]]$.*

Proof. For $a \in \mathbb{S}_t$ of canonical representative A, we set

$$v(a) := \operatorname{val} A.$$

We need to verify that v actually defines a semi-valuation in $\mathbb{S}_t$.

If b is another element of $\mathbb{S}_t$ of canonical representative B, then it is straightforward to verify that $v(a+b) \geqslant \min(v(a), v(b))$. As for the product, we compute the long division by the standard basis thanks to Proposition 3.8:

$$A B = Q_1 (\Phi_1 - \varphi_2) + \cdots + Q_t (\Phi_t - \varphi_{t+1}) + R,$$

where R is the canonical representative of $a b$, so $v(a b) = \operatorname{val} R$. The latter long division begins with setting $P := A B$ and then it successively subtracts polynomials of the form $G = c z^{e_0} \varphi_1^{e_1} \cdots \varphi_{t+1}^{e_{t+1}} (\Phi_i - \varphi_{i+1})$ from P where $i \leqslant t$, $c \in \mathbb{K}$, $e_i \in \mathbb{N}$, and $\operatorname{lm} P = \operatorname{lm} G$. Since the monomials in G have valuation $\geqslant \operatorname{val}(\operatorname{lm} G)$, it follows that

$$\operatorname{val}(P - G) \geqslant \min(\operatorname{val} P, \operatorname{val} G) = \operatorname{val} P.$$

This shows that $\operatorname{val} R \geqslant \operatorname{val}(A B)$. Since $\operatorname{val}(A B) = \operatorname{val} A + \operatorname{val} B$, we deduce that $v(a b) \geqslant v(a) + v(b)$. □

We write $\operatorname{val}_z A$ for the *partial valuation* in z of $A \in \mathbb{K}[[z, \varphi_1, \ldots, \varphi_{t+1}]]$. The valuation in z of an element of $\mathbb{P}_t$ will be the valuation in z of its canonical representative. In the canonical representation, the degrees of the φ_i being bounded, the valuation in z of an element in $\mathbb{P}_t$ can be related to $v(a)$ in terms of the γ_i. The following bounds will be useful when converting between the canonical and plain representations.

LEMMA 3.23. *Let $a \in \mathbb{S}_t$ be of canonical representative $A(\varphi_1, \ldots, \varphi_i)$ for some $i \leqslant t+1$. Then we have*

$$\operatorname{val} A - \gamma_i (1 + \deg_{\varphi_i} A) \;=\; v(a) - \gamma_i (1 + \deg_{\varphi_i} A) \;\leqslant\; \operatorname{val}_z A \;\leqslant\; v(a) \;=\; \operatorname{val} A.$$

Proof. Assume $a \neq 0$. There exists a monomial of the form $z^{\operatorname{val}_z A} \varphi_1^{e_1} \cdots \varphi_i^{e_i}$ in A. Using $\gamma_1 \geqslant 0$ and $\gamma_{i+1} > d_i \gamma_i$ for $i = 1, \ldots, t$, we verify that

$$\begin{aligned} 0 \;\leqslant\; v(a) - \operatorname{val}_z A \;&\leqslant\; e_1 \gamma_1 + \cdots + e_i \gamma_i \\ &\leqslant\; (d_1 - 1) \gamma_1 + (d_2 - 1) \gamma_2 + \cdots + (d_{i-1} - 1) \gamma_{i-1} + \gamma_i \deg_{\varphi_i} A \end{aligned} \tag{3.3}$$

and then that

$$\begin{aligned} 0 \;\leqslant\; v(a) - \operatorname{val}_z A \;&\leqslant\; d_1 \gamma_1 + (d_2 - 1) \gamma_2 + \cdots + (d_{i-1} - 1) \gamma_{i-1} + \gamma_i \deg_{\varphi_i} A \\ &\leqslant\; \gamma_2 + (d_2 - 1) \gamma_2 + \cdots + (d_{i-1} - 1) \gamma_{i-1} + \gamma_i \deg_{\varphi_i} A \\ &=\; d_2 \gamma_2 + (d_3 - 1) \gamma_3 + \cdots + (d_{i-1} - 1) \gamma_{i-1} + \gamma_i \deg_{\varphi_i} A \\ &\leqslant\; \gamma_3 + (d_3 - 1) \gamma_3 + \cdots + (d_{i-1} - 1) \gamma_{i-1} + \gamma_i \deg_{\varphi_i} A \\ &\quad\;\; \cdots \\ &\leqslant\; \gamma_i + \gamma_i \deg_{\varphi_i} A. \end{aligned}$$

□

The following lemma asserts that Π_t preserves the valuation in z.

LEMMA 3.24. *For all $a \in \mathbb{P}_t$ we have $\operatorname{val}_z(\Pi_t(a)) = \operatorname{val}_z a$. For all $A \in \mathbb{K}[[z]][x]$ we have $\operatorname{val}_z(\Pi_t^{-1}(A)) = \operatorname{val}_z A$.*

Proof. For any element $a \in \mathbb{P}_t$, the inequality $\mathrm{val}_z(\Pi_t(a)) \geqslant \mathrm{val}_z a$ clearly holds. Conversely, for any $A \in \mathbb{K}[[z]][x]$, we have $\mathrm{val}_z(\Pi_t^{-1}(A)) \geqslant \mathrm{val}_z A$. It follows that

$$\mathrm{val}_z(\Pi_t(a)) \geqslant \mathrm{val}_z a = \mathrm{val}_z(\Pi_t^{-1}(\Pi_t(a))) \geqslant \mathrm{val}_z(\Pi_t(a)),$$

whence the first assertion. The second assertion is a consequence of the fact that Π_t is a $\mathbb{K}[[z]]$-isomorphism; see Lemma 3.15. □

The next lemma relates valuations and precisions of approximations of a and $\Pi_t(a)$.

LEMMA 3.25. *Let α and $\eta > 0$ be rational numbers. For all $a \in \mathbb{P}_t$ we have*

$$[\Pi_t(a)]_{\alpha;\eta} = [\Pi_t([a]_{0;\alpha+\eta+l\gamma_{t+1}})]_{\alpha;\eta}, \text{ where } l := 1 + \deg_{\varphi_{t+1}} a.$$

For all $A \in \mathbb{K}[[z]][x]$ we have

$$[\Pi_t^{-1}(A)]_{\alpha;\eta} = [\Pi_t^{-1}([A]_{0;\alpha+\eta})]_{\alpha;\eta}.$$

Proof. Lemmas 3.23 and 3.24 give us

$$v(a) - l\gamma_{t+1} \leqslant \mathrm{val}_z(\Pi_t(a)) \leqslant v(a). \tag{3.4}$$

In particular, if $v(a) \geqslant \alpha + \eta + l\gamma_{t+1}$ then $\mathrm{val}_z(\Pi_t(a)) \geqslant \alpha + \eta$. As for the second assertion, the inequalities (3.4) are equivalent to

$$\mathrm{val}_z A \leqslant v(\Pi_t^{-1}(A)) \leqslant \mathrm{val}_z A + l\gamma_{t+1}.$$

In particular, if $\mathrm{val}_z A \geqslant \alpha + \eta$ then $v(\Pi_t^{-1}(A)) \geqslant \alpha + \eta$. □

Remark 3.26. Lemma 3.25 can be refined into

$$\begin{aligned}[\Pi_t(a)]_{\alpha;\eta} &= [\Pi_t([a]_{\alpha;\eta+l\gamma_{t+1}})]_{\alpha;\eta}, \text{ where } l := 1 + \deg_{\varphi_{t+1}} a.\\ [\Pi_t^{-1}(A)]_{\alpha;\eta} &= [\Pi_t^{-1}([A]_{\alpha-l\gamma_{t+1};l\gamma_{t+1}+\eta})]_{\alpha;\eta}, \text{ where } l := 1 + \deg_{\varphi_{t+1}}(\Pi_t^{-1}(A)).\end{aligned}$$

For simplicity we will not use this refinement in the sequel.

4. CONTACT HENSEL LIFTING

The usual Hensel lemma asserts that if a monic polynomial $A \in \mathbb{K}[[z]][x]$ factors into two monic coprime polynomials A_1 and A_2 modulo z, then there exist unique monic polynomials $\hat{A}_1$ and $\hat{A}_2$ in $\mathbb{K}[[z]][x]$ such that $A = \hat{A}_1 \hat{A}_2$, $A_1 = \hat{A}_1 \bmod z$, and $A_2 = \hat{A}_2 \bmod z$. In addition, $\hat{A}_1$ and $\hat{A}_2$ can be obtained with a softly linear cost in the output size.

A variant of Hensel lifting is the Weierstraß preparation theorem, in which case A and A_2 are no longer monic, but A_2 is invertible as a power series in x. We will generalize these two kinds of lifting to the contact coordinate framework.

Throughout this section, $a, a_1, \ldots, a_s$ are elements in $\mathbb{P}_t$, regarded informally as "polynomials" in the main variable φ_{t+1}. We will assume that $a = a_1 \cdots a_s$ holds for a "sufficient" initial precision, and that $a_1, \ldots, a_s$ are "pairwise coprime". We want to lift $a_1, \ldots, a_s$ into $\hat{a}_1, \ldots, \hat{a}_s$ so that $a = \hat{a}_1 \cdots \hat{a}_s$ holds up to a required precision. The case when a is monic and

$$\deg_{\varphi_{t+1}} a = \deg_{\varphi_{t+1}}(\mathrm{in}(a))$$

corresponds to the *multi-factor Hensel lifting*. The case when $s = 2$ and

$$\deg_{\varphi_{t+1}}(\mathrm{in}(a)) < \deg_{\varphi_{t+1}} a$$

is called the *Weierstraß normalization* of a.

Let $A \in \mathbb{K}[[z]][\varphi_1, \ldots, \varphi_{t+1}]$ be the canonical representative of a. We recall that $\deg_{\varphi_{t+1}} a = \deg_{\varphi_{t+1}} A$, $\operatorname{val}_z a = \operatorname{val}_z A$, and $\operatorname{in}(a)$ is the image of $\operatorname{in}(A)$ in $\mathbb{P}_t$. If b is a non-zero element in $\mathbb{P}_t$ that is monic in φ_{t+1}, then $a \operatorname{rem} b$ represents the remainder in the division of a by b, as specified in Definition 3.13.

4.1. Normalized inverses

Let a be clustered (see Definition 3.9) at $\mathbb{P}_t$ and of degree $l \geqslant 1$ in φ_{t+1}. Given $b \in \mathbb{P}_t$ with $\deg_{\varphi_{t+1}} b < l$, its inverse modulo a, whenever it exists, belongs to $z^{-\delta} \mathbb{P}_t$ for some $\delta \in \mathbb{N}$. In order to determine a bound for δ, consider $u \in \mathbb{P}_t$ satisfying

- $\deg_{\varphi_{t+1}} u < l$,
- $\delta := v(u) + v(b)$ is an integer $\geqslant 0$,
- $z^{\delta} = u\, b \operatorname{rem} a$.

Lemma 3.23 yields

$$\operatorname{val}_z u \geqslant v(u) - l\,\gamma_{t+1} = \delta - v(b) - l\,\gamma_{t+1}.$$

If $\delta > v(b) + l\,\gamma_{t+1}$, then setting $\tilde{\delta} := \lceil \delta - v(b) - l\,\gamma_{t+1} \rceil$ leads to

$$v(b) + l\,\gamma_{t+1} - 1 < \delta - \tilde{\delta} \leqslant v(b) + l\,\gamma_{t+1}.$$

So we may divide u by $z^{\tilde{\delta}}$ and subtract $\tilde{\delta}$ from δ in order to get a "simplified" modular inverse u of b that satisfies

$$v(b) + l\,\gamma_{t+1} - 1 < \delta \leqslant v(b) + l\,\gamma_{t+1}. \tag{4.1}$$

If $\delta \leqslant v(b) + l\,\gamma_{t+1} - 1$, so that $\tilde{\delta} := \lceil \delta - v(b) - l\,\gamma_{t+1} \rceil < 0$, then multiplication of u by $z^{-\tilde{\delta}}$ also reduces to the case when (4.1) holds. In general, this shows that modular inverses can always be normalized in the sense of the following definition:

DEFINITION 4.1. *Let a be clustered at $\mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1}, and let $b \in \mathbb{P}_t$ be of degree $<l$ in φ_{t+1}. A* ***normalized inverse*** *of b* ***modulo*** *a with relative precision $\eta > 0$ is an element $u / z^{\delta} \in z^{-\delta} \mathbb{P}_t$ with $u = [u]_{v(u);\eta}$ such that:*

- $\deg_{\varphi_{t+1}} u < l$,
- *$\delta := v(u) + v(b)$ satisfies $\delta = \lfloor v(b) + l\,\gamma_{t+1} \rfloor \in \mathbb{N}$,*
- $z^{\delta} = [u\, b \operatorname{rem} a]_{\delta;\eta}$.

If $\eta = \min(\Gamma_{t+1} \setminus \{0\})$, then we say that u / z^{δ} is the ***normalized initial inverse*** *of b* ***modulo*** *a.*

The existence and the computation of such inverses are postponed in section 7.1. The next definition concerns the special case when b belongs to $\mathbb{P}_{t-1}$.

DEFINITION 4.2. *Let $b \in \mathbb{P}_t$ be of degree 0 in φ_{t+1} (b is in $\mathbb{P}_{t-1}$). A* ***normalized initial inverse*** *of b is a homogeneous element $u / z^{\delta} \in z^{-\delta} \mathbb{P}_{t-1}$ such that:*

- *$\delta := v(u) + v(b)$ satisfies $\delta = \lfloor v(b) + d_t\,\gamma_t \rfloor \in \mathbb{N}$,*
- $z^{\delta} = [u\, b]_{\delta}$.

LEMMA 4.3. *If $b \in \mathbb{P}_{t-1}$ has a normalized initial inverse, then it is unique and $v(c\, b) = v(c) + v(b)$ holds for all $c \in \mathbb{P}_t$.*

Proof. We have $v(c b) \geqslant v(c) + v(b)$. Definition 4.2 also yields

$$\delta + v(c) = v(c b u) \geqslant v(c b) + v(u) = v(c b) + \delta - v(b).$$

Concerning the uniqueness, if u' / z^{δ} represents a normalized initial inverse of b then

$$v((u - u') b) > \delta$$

and therefore $v(u - u') > \delta - v(b)$, whence $u = u'$. □

LEMMA 4.4. *If b has a normalized inverse modulo a with relative precision $\eta > 0$, as in Definition 4.1, then it is unique and $v((c b) \operatorname{rem} a) = v(c \operatorname{rem} a) + v(b)$ holds for all $c \in \mathbb{P}_t$.*

Proof. We extend the contact tower with $\Phi_{t+1} := a$ and apply Lemma 4.3 in order to obtain the equality for the valuation. As for the uniqueness let u' / z^{δ} represent another normalized inverse modulo a. We have $v((u - u') b) \geqslant \delta + \eta$ and thus $v(u - u') \geqslant \delta + \eta - v(b)$, whence $u = u'$. □

4.2. Lifting modular inverses

We explain how to increase the relative precision of a normalized modular inverse, in terms of the contact coordinates.

PROPOSITION 4.5. *Let $b, a, u \in \mathbb{P}_t$, $\delta \in \mathbb{N}$ and $\eta > 0$, be such that*

- *a is clustered at $\mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1},*
- *$\deg b < l$,*
- *u / z^{δ} is a normalized inverse of b modulo a with relative precision $\eta > 0$.*

Then, there exists a unique normalized modular inverse $\hat{u} / z^{\delta}$ of b with relative precision 2η such that $[\hat{u}]_{v(u); \eta} = u$. More precisely, with $\delta := v(u) + v(b)$ and

$$c := u (z^{\delta} - u b) \operatorname{rem} a,$$

we have $\operatorname{val}_z c \geqslant \delta$ and

$$\hat{u} = u + [c]_{v(u) + \delta + \eta; \eta} / z^{\delta}.$$

Proof. Let $\tilde{u}$ represent an unknown in $[\mathbb{P}_t]_{v(u) + \eta; \eta}$ with $\deg_{\varphi_{t+1}} \tilde{u} < l$, and which satisfies

$$[z^{\delta} - (u + \tilde{u}) b \operatorname{rem} a]_{\delta; 2 \eta} = 0. \tag{4.2}$$

This equation is equivalent to

$$[z^{\delta} - u b \operatorname{rem} a]_{\delta + \eta; \eta} = [\tilde{u} b \operatorname{rem} a]_{\delta + \eta; \eta},$$

and, by Lemma 4.4, to

$$\begin{aligned} [u (z^{\delta} - u b) \operatorname{rem} a]_{v(u) + \delta + \eta; \eta} &= [\tilde{u} u b \operatorname{rem} a]_{v(u) + \delta + \eta; \eta} \\ &= [z^{\delta} \tilde{u} \operatorname{rem} a]_{v(u) + \delta + \eta; \eta} \\ &= [z^{\delta} \tilde{u}]_{v(u) + \delta + \eta; \eta}. \end{aligned}$$

Hence

$$z^{\delta} \tilde{u} = [c]_{v(u) + \delta + \eta; \eta}.$$

We have $v(z^{\delta} - u b) \geqslant \delta + \eta$, and therefore $v(c) \geqslant v(u) + \delta + \eta$. Lemma 3.23 implies that

$$\operatorname{val}_z c \geqslant v(u) + \delta + \eta - l \gamma_{t+1} = \delta - v(b) + \delta + \eta - l \gamma_{t+1} > \delta + \eta - 1,$$

so c can actually be divided by z^{δ}. We conclude that $\tilde{u} = c / z^{\delta}$ is the unique solution of (4.2), whence $\hat{u} = u + \tilde{u}$ fulfills all requirements. □

COROLLARY 4.6. *Let a be clustered at $\mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1}. If $b \in \mathbb{P}_t$ admits an initial inverse u / z^{δ} modulo a, then there exists a unique $u^{\infty} \in \mathbb{P}_t$ such that $\operatorname{in}(u^{\infty}) = u$ and $z^{\delta} = u^{\infty} b \operatorname{rem} a$.*

Proof. Thanks to repeated applications of Proposition 4.5 we can construct the initial inverse of b modulo a with any finite relative precision. The existence of u^{∞} follows from the completeness of $\mathbb{P}_t$. □

The next corollary addresses the precision loss of the initial inverse of b modulo a when a and b are truncated modulo $O(z^{\tau})$.

COROLLARY 4.7. *Let a be clustered at $\mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1}. If $b \in \mathbb{P}_t$ admits an initial inverse u / z^{δ} modulo a, then u^{∞} (as defined in Corollary 4.6) can be computed modulo $O(z^{\tau - \delta})$ from the truncations of a and b modulo $O(z^{\tau})$, whenever $\tau \geqslant \delta$.*

Proof. Let

$$\hat{a} := \Pi_t^{-1}([\Pi_t(a)]_{0;\tau}), \qquad \hat{b} := \Pi_t^{-1}([\Pi_t(b)]_{0;\tau})$$

represent the truncations of of a and b modulo $O(z^{\tau})$, and let η be the smallest element of Γ_t larger or equal to $\tau + v(a) - v(u) - \delta$. Thanks to repeated applications of Proposition 4.5 we can compute the initial inverse $\hat{u} / z^{\delta}$ of $\hat{b}$ modulo $\hat{a}$ with relative precision η.

Since $\delta = \lfloor v(b) + l \gamma_{t+1} \rfloor = v(u) + v(b)$ and $v(a) = l \gamma_{t+1}$, we have $v(a) \geqslant v(u)$ and therefore $\eta \geqslant 0$. From

$$[z^{\delta} - \hat{u} \hat{b} \operatorname{rem} \hat{a}]_{\delta;\eta} = 0,$$

we deduce that

$$[z^{\delta} - \hat{u} b \operatorname{rem} a]_{\delta;\eta} = 0 + O(z^{\tau}).$$

It follows that $[(\hat{u} - u^{\infty}) b \operatorname{rem} a]_{\delta;\eta} = 0 + O(z^{\tau})$ and then that

$$[u^{\infty} (\hat{u} - u^{\infty}) b \operatorname{rem} a]_{\delta + v(u);\eta} = 0 + O(z^{\tau}).$$

Using $u^{\infty} b \operatorname{rem} a = z^{\delta}$, we obtain that

$$[(\hat{u} - u^{\infty}) z^{\delta}]_{\delta + v(u);\eta} = 0 + O(z^{\tau}),$$

hence

$$[\hat{u} - u^{\infty}]_{v(u);\eta} = 0 + O(z^{\tau - \delta}).$$

Lemma 3.23 implies that

$$\operatorname{val}_z(\hat{u} - u^{\infty}) \geqslant \min (v(u) + \eta - v(a), \tau - \delta).$$

Thanks to the value taken for η it follows that

$$\operatorname{val}_z(\hat{u} - u^{\infty}) \geqslant \min (\tau + v(a) - v(u) - \delta + v(u) - v(a), \tau - \delta) = \tau - \delta,$$

whence $\hat{u} = u^{\infty} + O(z^{\tau - \delta})$. □

4.3. Weierstraß normalization

We now turn to the Weierstraß normalization of an element $a \in \mathbb{P}_t$. The following definition gathers the necessary technical conditions and data structures.

DEFINITION 4.8. *Let $a \in \mathbb{P}_t$ be of degree $l \geqslant 1$ in φ_{t+1}. A* ***Weierstraß context*** *for a with relative precision $\eta > 0$ consists of elements a_1, a_2, u_1 in $\mathbb{P}_t$ and $\delta_1 \in \mathbb{N}$ that satisfy the following properties:*

W₁. *a_1 is clustered at $\mathbb{P}_t$ of degree $l_1 \geqslant 1$ in φ_{t+1}, $a_1 = [a_1]_{v(a_1);\eta}$,*

W₂. $\deg_{\varphi_{t+1}}(\mathrm{in}(a_2)) = 0$*,* $v(a) = v(a_1) + v(a_2)$*,* $a_2 = [a_2]_{v(a_2);\eta}$*,*

W₃. $[a - a_1 a_2]_{v(a);\eta} = 0$*,*

W₄. *u_1 / z^{δ_1} represents the normalized inverse of a_2 with relative precision η.*

If $\eta = \min(\Gamma_t \setminus \{0\})$*, then we say that a_1, a_2, u_1, δ_1 is an* ***initial Weierstraß context*** *for a.*

The Weierstraß lifting step summarizes as follows.

PROPOSITION 4.9. *Let $a \in \mathbb{P}_t$ be monic of degree $l \geqslant 1$ in φ_{t+1} and let a_1, a_2, u_1, δ_1 denote a Weierstraß context for a with relative precision $\eta > 0$. Then, there exists a unique Weierstraß context $\hat{a}_1$, $\hat{a}_2, \hat{u}_1, \delta_1$ for a with relative precision 2η such that $[\hat{a}_1]_{v(a_1);\eta} = a_1$, $[\hat{a}_2]_{v(a_2);\eta} = a_2$, and $[\hat{u}_1]_{v(u_1);\eta} = u_1$. More precisely, with*

$$b_1 := u_1 a \,\mathrm{rem}\, a_1,$$

we have $\mathrm{val}_z\, b_1 \geqslant \delta_1$ *and*

$$\begin{aligned} \hat{a}_1 &= a_1 + [b_1]_{v(a_1)+\eta+\delta_1;\eta} / z^{\delta_1} \\ \hat{a}_2 &= [a \,\mathrm{quo}\, \hat{a}_1]_{v(a_2);2\eta}. \end{aligned}$$

Letting

$$c_1 := u_1 (z^{\delta_1} - u_1 \hat{a}_2) \,\mathrm{rem}\, \hat{a}_1,$$

we also have $\mathrm{val}_z\, c_1 \geqslant \delta_1$ *and*

$$\hat{u}_1 = u_1 + [c_1]_{v(u_1)+\delta_1+\eta;\eta} / z^{\delta_1}.$$

Proof. Consider the unknowns $\tilde{a}_1 \in [\mathbb{P}_t]_{v(a_1)+\eta;\eta}$ and $\tilde{a}_2 \in [\mathbb{P}_t]_{v(a_2)+\eta;\eta}$ such that $\deg_{\varphi_{t+1}} \tilde{a}_1 < l_1$ and

$$[a]_{v(a);2\eta} = [(a_1 + \tilde{a}_1)\,(a_2 + \tilde{a}_2)]_{v(a);2\eta} = [a_1 a_2 + a_1 \tilde{a}_2 + \tilde{a}_2 a_1]_{v(a);2\eta}.$$

It follows that

$$[a \,\mathrm{rem}\, a_1]_{v(a);2\eta} = [\tilde{a}_1 a_2 \,\mathrm{rem}\, a_1]_{v(a);2\eta}.$$

Lemma 4.4 and the constraints on valuations and precisions equivalently yield

$$\begin{aligned} [u_1 a \,\mathrm{rem}\, a_1]_{v(a)+v(u_1)+\eta;\eta} &= [u_1 a_2 \tilde{a}_1 \,\mathrm{rem}\, a_1]_{v(a)+v(u_1)+\eta;\eta} \\ &= [z^{\delta_1} \tilde{a}_1 \,\mathrm{rem}\, a_1]_{v(a)+\delta_1-v(a_2)+\eta;\eta} \\ &= [z^{\delta_1} \tilde{a}_1]_{v(a)+\delta_1-v(a_2)+\eta;\eta} \\ &= [z^{\delta_1} \tilde{a}_1]_{v(a_1)+\delta_1+\eta;\eta}, \end{aligned}$$

whence

$$z^{\delta_1} \tilde{a}_1 := [u_1 a \,\mathrm{rem}\, a_1]_{v(a_1)+\delta_1+\eta;\eta}.$$

Then Lemma 3.23 gives

$$\mathrm{val}_z(u_1 a \,\mathrm{rem}\, a_1) \geqslant v(u_1 a \,\mathrm{rem}\, a_1) - l_1 \gamma_{t+1} \geqslant v(a_1) + \delta_1 + \eta - v(a_1) = \delta_1 + \eta.$$

This shows that $\tilde{a}_1$ exists and is uniquely determined by

$$\tilde{a}_1 := [u_1 a \,\mathrm{rem}\, a_1]_{v(a_1)+\delta_1+\eta;\eta} / z^{\delta_1}.$$

The formula for $\hat{a}_2$ is straightforward and the one for $\hat{u}_1$ follows from Proposition 4.5. □

COROLLARY 4.10. *Let $a \in \mathbb{P}_t$ be monic of degree $l \geqslant 1$ in φ_{t+1} and let a_1, a_2, u_1, δ_1 denote an initial Weierstraß context for a. Then, there exist unique $a_1^{\infty}, a_2^{\infty} \in \mathbb{P}_t$ such that $[a_1^{\infty}]_{v(a_1)} = a_1$, $[a_2^{\infty}]_{v(a_2)} = a_2$, and $a = a_1^{\infty} a_2^{\infty}$. We call a_1^{∞} (that is clustered at $\mathbb{P}_t$) the* ***Weierstraß part*** *of a.*

Proof. This follows from Proposition 4.9 and the completeness of $\mathbb{P}_t$. □

COROLLARY 4.11. *Let $a \in \mathbb{P}_t$ be monic of degree $l \geqslant 1$ in φ_{t+1}. If there exists an initial Weierstraß context a_1, a_2, u_1, δ_1 for a, then a_1^{∞} and a_2^{∞} (as defined in Corollary 4.10) can be computed modulo $O(z^{\tau - \delta_1})$ from the truncation of a modulo $O(z^{\tau})$.*

Proof. We introduce the truncation $\hat{a} := \Pi_t^{-1}([\Pi_t(a)]_{0,\tau})$ of a modulo $O(z^{\tau})$, and set η to the smallest element of Γ_t larger or equal to $\tau - \delta_1$. The quadruple a_1, a_2, u_1, δ_1 is an initial Weierstraß context for $\hat{a}$. From Proposition 4.9 we know that we can compute the Weierstraß context $\hat{a}_1$, $\hat{a}_2$, $\hat{u}_1$, δ_1 for $\hat{a}$ with relative precision η, so that $[\hat{a} - \hat{a}_1 \hat{a}_2]_{v(a);\eta} = 0$ and

$$[a - \hat{a}_1 \hat{a}_2]_{v(a);\eta} = 0 + O(z^{\tau}).$$

According to Corollary 4.6 we may consider the modular inverse $\tilde{u}_1$ of $\hat{a}_2$ modulo a_1^{∞}, so that $\tilde{u}_1 \hat{a}_2 \operatorname{rem} a_1^{\infty} = z^{\delta_1}$. Hence

$$[\tilde{u}_1 a - \hat{a}_1 \tilde{u}_1 \hat{a}_2]_{v(a)+v(u_1);\eta} = 0 + O(z^{\tau})$$

and

$$[z^{\delta_1} \hat{a}_1 \operatorname{rem} a_1^{\infty}]_{v(a)+v(u_1);\eta} = 0 + O(z^{\tau}).$$

Lemma 3.23 implies that

$$\begin{aligned}
\operatorname{val}_z(\hat{a}_1 \operatorname{rem} a_1^{\infty}) &\geqslant \min(v(a) + v(u_1) - \delta_1 + \eta - l_1 \gamma_{t+1}, \tau - \delta_1)\\
&= \min(v(a) + v(u_1) - (v(u_1) + v(a_2)) + \eta - l_1 \gamma_{t+1}, \tau - \delta_1)\\
&= \min(v(a) - v(a_2) + \eta - v(a_1), \tau - \delta_1)\\
&= \min(\eta, \tau - \delta_1)\\
&= \tau - \delta_1.
\end{aligned}$$

Since $\hat{a}_1$ and a_1^{∞} are monic of the same degree in φ_{t+1} we deduce that $\hat{a}_1 = a_1^{\infty} + O(z^{\tau - \delta_1})$. □

4.4. Weierstraß normalization via plain coordinates

The above formulas for the Weierstraß lifting can be applied directly in $\mathbb{P}_t$, but for the sake of efficiency it is worth using plain coordinates. As a technical complication, conversions between contact and plain coordinates result in precision loss. Fortunately, this loss is sufficiently small so that it has no serious impact on the complexity of our top-level factorization algorithm. In the following algorithm, the input and output polynomials use plain coordinates. However, the relative precision η, to be doubled during a lifting step, refers to the contact coordinates.

Algorithm 4.1

Input. A contact tower of height t and degree d as above, a rational number $\eta > 0$. A monic polynomial $A \in \mathbb{K}[[z]][x]$ modulo $O(z^{v(a)+2\eta})$, where $a := \Pi_t^{-1}(A)$, and polynomials A_1, A_2, U_1 in $\mathbb{K}[[z]][x]$ modulo $O(z^{v(a)+\eta})$. The elements $a_i := [\Pi_t^{-1}(A_i)]_{v(\Pi_t^{-1}(A_i));\eta}$ for $i = 1, 2$, $u_1 := [\Pi_t^{-1}(U_1)]_{v(\Pi_t^{-1}(U_1));\eta}$, and δ_1 form a Weierstraß context for a with relative precision η, as in Definition 4.8.

Output. $\hat{A}_1, \hat{A}_2, \hat{U}_1$ in $\mathbb{K}[[z]][x]$ modulo $O(z^{v(a)+2\eta})$, such that the elements $\hat{a}_i := [\Pi_t^{-1}(\hat{A}_i)]_{v(a_i);2\eta}$ for $i=1,2$, $\hat{u}_1 := [\Pi_t^{-1}(\hat{U}_1)]_{v(u_1);2\eta}$, and δ_1 form a Weierstraß context for a with relative precision 2η such that $[\hat{a}_i]_{v(a_i);\eta} = [a_i]_{v(a_i);\eta}$ for $i=1,2$ and $[\hat{u}_1]_{v(u_1);\eta} = [u_1]_{v(u_1);\eta}$.

```
1. Set $\tau := v(a) + 2\eta$.
2. Compute $B_1 := U_1 A \operatorname{rem} A_1$ in $\mathbb{K}[[z]]/(z^{\tau+\delta_1})[x]$.
3. Compute $\tilde{A}_1 := B_1 / z^{\delta_i}$ and $\hat{A}_1 := A_1 + \tilde{A}_1$ in $\mathbb{K}[[z]]/(z^{\tau})[x]$.
4. Compute $\hat{A}_2 := A \operatorname{quo} \hat{A}_1$ in $\mathbb{K}[[z]]/(z^{\tau})[x]$.
5. Compute $C_1 := U_1 (z^{\delta_1} - U_1 \hat{A}_2) \operatorname{rem} \hat{A}_1$ in $\mathbb{K}[[z]]/(z^{\tau+\delta_1})[x]$.
6. Compute $\tilde{U}_1 := C_1 / z^{\delta_1}$ and $\hat{U}_1 := U_1 + \tilde{U}_1$ in $\mathbb{K}[[z]]/(z^{\tau})[x]$.
7. Return $\hat{A}_1, \hat{A}_2, \hat{U}_1$.
```

PROPOSITION 4.12. *Algorithm 4.1 is correct and takes*

$$O(\mathsf{M}(l d (v(a) + \eta)))$$

operations in $\mathbb{K}$*, where* $l := \deg_{\varphi_{t+1}} a$.

Proof. The hypotheses of Proposition 4.9 are satisfied. We let

$$b_1 := u_1 a \operatorname{rem} a_1 = \Pi_t^{-1}(B_1).$$

Lemma 3.25 implies

$$[b_1]_{0;\tau+\delta_1} = [\Pi_t^{-1}([B_1]_{0;\tau+\delta_1})]_{0;\tau+\delta_1}.$$

We have seen in Proposition 4.9 that $\operatorname{val}_z b_1 \geqslant \delta_1$, whence $\operatorname{val}_z B_1 \geqslant \delta_1$ by Lemma 3.24. Consequently $\tilde{A}_1$ is well defined. With the notation of Proposition 4.9 we verify that

$$\begin{aligned} \hat{a}_1 &= [a_1 + b_1 / z^{\delta_1}]_{0;v(a_1)+2\eta} \\ &= [\Pi_t^{-1}(\hat{A}_1)]_{0;v(a_1)+2\eta} \\ &= [\Pi_t^{-1}([\hat{A}_1]_{0;v(a_1)+2\eta})]_{0;v(a_1)+2\eta} \end{aligned}$$

and

$$\begin{aligned} [\Pi_t^{-1}([\hat{A}_2]_{0;\tau})]_{0;v(a_2)+2\eta} &= [\Pi_t^{-1}([A \operatorname{quo} \hat{A}_1]_{0;\tau})]_{0;v(a_2)+2\eta} \\ &= [[a]_{0;\tau} \operatorname{quo} [\hat{a}_1]_{0;\tau}]_{0;v(a_2)+2\eta} \\ &= [\hat{a}_2]_{0;v(a_2)+2\eta}. \end{aligned}$$

By Proposition 4.9, properties W_1, W_2, and W_3 of Definition 4.8 thus hold for $\hat{a}_1, \hat{a}_2$, and relative precision 2η.

In a similar fashion we verify that

$$[c_1]_{0;\tau+\delta_1} = [\Pi_t^{-1}(C_1)]_{0;\tau+\delta_1} = [\Pi_t^{-1}([C_1]_{0;\tau+\delta_1})]_{0;\tau+\delta_1},$$

so we have

$$[\hat{u}_1]_{0;v(u_1)+2\eta} = [u_1 + \Pi_t^{-1}(\tilde{U}_1)]_{0;v(u_1)+2\eta} = [u_1 + \Pi_t^{-1}([\tilde{U}_1]_{0;\tau})]_{0;v(u_1)+2\eta}.$$

By Proposition 4.5, property W_4 holds. We are done with the correctness. The cost analysis is obtained routinely by using $\delta_1 = \lfloor v(a_2) + d_t \gamma_t \rfloor \leqslant \lfloor v(a) \rfloor$. □

Applying successively Algorithm 4.1 several times enables us to lift any such initial context to any requested precision. The cost is summarized in the following corollaries.

COROLLARY 4.13. *Let $a \in \mathbb{P}_t$ be of degree $l \geqslant 1$ in φ_{t+1} and let a_1, a_2, u_1, δ_1 be an initial Weierstraß context for a. Then, given $\eta > 0$, we may compute a Weierstraß context $\hat{a}_1, \hat{a}_2, \hat{u}_1, \delta_1$ for a with relative precision η using*

$$O(\mathsf{M}(l d \tau) \log(l d R_{t+1} v(a)))$$

operations in $\mathbb{K}$, where $\tau = v(a) + \eta$ and $d = d_1 \cdots d_t$ is the degree of the contact tower.

Proof. We convert the input data into the plain representation modulo $O(z^\tau)$ using Proposition 3.19, with $O(\mathsf{M}(l d \tau) \log(l d))$ operations in $\mathbb{K}$.

We successively apply Algorithm 4.1 to increase the relative precision from $\frac{2^{k-1}}{R_{t+1}}$ to $\frac{2^k}{R_{t+1}}$, for $k = 1, \ldots, \lceil \log_2(R_{t+1} \eta) \rceil$. By Proposition 4.12, the total cost of the lifting contributes to

$$\begin{aligned} & O\left(\sum_{k=1}^{\lceil \log_2(R_{t+1}\eta) \rceil} \mathsf{M}\left(l d \left(v(a) + \frac{2^k}{R_{t+1}} \right) \right) \right) \\ = \; & O\left(\sum_{k=1}^{\lceil \log_2(R_{t+1} v(a)) \rceil} \mathsf{M}(l d v(a)) + \sum_{k=\lceil \log_2(R_{t+1} v(a)) \rceil + 1}^{\lceil \log_2(R_{t+1}\eta) \rceil} \mathsf{M}\left(l d \frac{2^k}{R_{t+1}} \right) \right) \\ = \; & O(\mathsf{M}(l d v(a)) \log(R_{t+1} v(a)) + \mathsf{M}(l d \eta)). \end{aligned}$$

At the end of the lifting, we convert the polynomials to contact coordinates modulo $O(z^\tau)$ via Proposition 3.19, again with $O(\mathsf{M}(l d \tau) \log(l d))$ operations in $\mathbb{K}$. □

COROLLARY 4.14. *Let $a \in \mathbb{P}_t$ be of degree $l \geqslant 1$ in φ_{t+1} and let a_1, a_2, u_1, δ_1 form an initial Weierstraß context for a. Then, given a with precision $O(z^\tau)$ with $\tau > \delta_1$, we can compute its Weierstraß part a_1^∞ (as defined in Corollary 4.10) with precision $O(z^{\tau - \delta_1})$ using*

$$O(\mathsf{M}(l d \tau) \log(l d v(a)))$$

operations in $\mathbb{K}$, where $d = d_1 \cdots d_t$ is the degree of the contact tower.

Proof. The truncation of a_1^∞ at precision $O(z^\tau)$ does not depend on γ_{t+1}, as long as the initial Weierstraß context properties are preserved. In particular we may set $-\gamma_{t+1}$ to the largest slope of a_1^∞ (which is $-\infty$ if a_1^∞ is a power of φ_{t+1}), so we have $-\gamma_{t+1} \in \frac{1}{l_1} \Gamma_t$ where $l_1 := \deg_{\varphi_{t+1}} a_1$, whence

$$R_{t+1} \leqslant R_t l_1 \leqslant d l. \tag{4.3}$$

We use Corollary 4.13 with relative precision $\eta := \tau - \delta_1$, as in the proof of Corollary 4.11. The running time is

$$O(\mathsf{M}(l d (v(a) + \eta)) \log(l d R_{t+1} v(a)))$$

which yields the claimed bound thanks to inequality (4.3) and

$$v(a) + \eta = v(a) + \tau - \delta_1 = v(a) + \tau - \lfloor v(a_2) + d_t \gamma_t \rfloor \leqslant v(a) + \tau - (v(a) - 1) = \tau + 1. \quad \square$$

4.5. Hensel lifting step

We now turn to the lifting of a factorization of an element $a \in \mathbb{P}_t$, assuming that suitable approximate modular inverses are known. The following definition gathers the necessary technical conditions and data structures.

DEFINITION 4.15. *Let a be clustered at $\mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1}. A* ***Hensel context*** *for a with relative precision $\eta > 0$ consists of elements $a_1, \ldots, a_s, u_1, \ldots, u_s$ in $\mathbb{P}_t$ and integers $\delta_1, \ldots, \delta_s$ that satisfy the following properties:*

H$_1$. *For $i = 1, \ldots, s$, a_i is clustered at $\mathbb{P}_t$ of degree $l_i \geqslant 1$, and has relative precision η,*

H$_2$. $v(a) = v(a_1) + \cdots + v(a_s)$*, and* $l = l_1 + \cdots + l_s$*,*

H$_3$. $[a - a_1 \cdots a_s]_{v(a);\eta} = 0$*,*

H$_4$. *For $i = 1, \ldots, s$, $v(\hat{a}_i) = v(\hat{a}_i \operatorname{rem} a_i)$ and u_i / z^{δ_i} is the normalized inverse of $\hat{a}_i$ modulo a_i with relative precision η, where $\hat{a}_i := a_1 \cdots a_{i-1} a_{i+1} \cdots a_s$.*

If $\eta = \min(\Gamma_t \setminus \{0\})$, then we say that $a_1, \ldots, a_s, u_1, \ldots, u_s, \delta_1, \ldots, \delta_s$ is an ***initial Hensel context*** *for a.*

Informally speaking, the assumption that $\hat{a}_i$ admits a normalized initial inverse modulo a_i for $i = 1, \ldots, s$ corresponds to the idea that $a_1, \ldots, a_s$ are "initially coprime". We revisit the classical Chinese theorem in this context.

LEMMA 4.16. *Given a Hensel context as in Definition 4.15, the following formula holds in $\mathbb{P}_t[z^{-1}]$:*

$$1 = [u_1 \hat{a}_1 / z^{\delta_1} + \cdots + u_s \hat{a}_s / z^{\delta_s}]_{0;\eta}.$$

Proof. Let us write

$$c := u_1 \hat{a}_1 / z^{\delta_1} + \cdots + u_s \hat{a}_s / z^{\delta_s} \in \mathbb{P}_t[z^{-1}].$$

By construction this yields

$$1 = [u_i \hat{a}_i / z^{\delta_i} \operatorname{rem} a_i]_{0;\eta} = [c \operatorname{rem} a_i]_{0;\eta} \tag{4.4}$$

for $i = 1, \ldots, s$. Assume by induction that there exists $q_i \in \mathbb{P}_t[z^{-1}]$ such that

$$1 = [c - q_i a_1 \cdots a_i]_{0;\eta}. \tag{4.5}$$

holds for some $i \geqslant 1$, which is indeed the case for $i = 1$ by (4.4). Combined with (4.4) for $i + 1$, there exists $\tilde{q}_{i+1} \in \mathbb{P}_t[z^{-1}]$ such that

$$0 = [q_i a_1 \cdots a_i - \tilde{q}_{i+1} a_{i+1}]_{0;\eta}. \tag{4.6}$$

Since $a_1 \cdots a_i$ is initially invertible modulo a_{i+1}, Corollary 4.6 yields the existence of the initial inverse $v_i / z^{\sigma_i} \in \mathbb{P}_t[z^{-1}]$ of $a_1 \cdots a_i$ modulo a_{i+1}, so there exists $\tilde{q}_{i+1} \in \mathbb{P}_t[z^{-1}]$ such that

$$1 = v_i a_1 \cdots a_i / z^{\sigma_i} - \tilde{q}_{i+1} a_{i+1}.$$

Combining the latter equality to (4.6) gives

$$0 = [q_i - (q_i - v_i / z^{\sigma_i}) \tilde{q}_{i+1} a_{i+1}]_{-v(a_1 \cdots a_i);\eta},$$

thanks to Lemma 4.4 and H$_4$. In this way, equality (4.5) holds for $i + 1$ with $q_{i+1} := (q_i - v_i / z^{\sigma_i}) \tilde{q}_{i+1}$. At the end of the induction equality (4.5) holds for s, and since $\deg_{\varphi_{t+1}} c < \deg_{\varphi_{t+1}} a$, we finally deduce that $[q_s]_{-v(a_1 \cdots a_s);\eta} = 0$. □

Given a clustered at $\mathbb{P}_t$, we can increase $(\mathbb{P})_{i \leqslant t}$ with $\Phi_{t+1} := a$ and $\gamma_{t+2} := \infty$. The contact tower $(\mathbb{P})_{i \leqslant t+1}$ obtained in this way corresponds to the quotient ring $\mathbb{P}_t / (a)$: in the sequel $\mathbb{P}_t / (a)$ is endowed with the semi-valuation induced by $\mathbb{P}_{t+1}$.

PROPOSITION 4.17. *Given a Hensel context as in Definition 4.15, the map*

$$\begin{array}{rrcl}\Omega: & [\mathbb{P}_t/(a_1\cdots a_s)]_{v(a);\eta} & \longrightarrow & [\mathbb{P}_t/(a_1)]_{v(a);\eta}\times\cdots\times[\mathbb{P}_t/(a_s)]_{v(a);\eta}\\ & b & \longmapsto & ([b\operatorname{rem}a_1]_{v(a);\eta},\ldots,[b\operatorname{rem}a_s]_{v(a);\eta})\end{array}$$

is a $\mathbb{K}$*-linear isomorphism and we have* $\Omega^{-1}(c_1,\ldots,c_s):=[c]_{v(a);\eta}$*, where*

$$c:=(u_1c_1/z^{\delta_1}\operatorname{rem}a_1)\,\hat{a}_1+\cdots+(u_sc_s/z^{\delta_s}\operatorname{rem}a_s)\,\hat{a}_s.$$

Proof. It is clear from the assumptions that the map is well defined and $\mathbb{K}$-linear. Let

$$(c_1,\ldots,c_s)\in(\mathbb{P}_t/(a_1))_{v(a);\eta}\times\cdots\times(\mathbb{P}_t/(a_s))_{v(a);\eta}.$$

From Lemma 4.4 we have

$$v(u_ic_i\operatorname{rem}a_i)=v(u_i)+v(c_i)\geqslant\delta_i-v(\hat{a}_i\operatorname{rem}a_i)+v(a)=\delta_i-v(\hat{a}_i)+v(a)=v(a_i)+\delta_i,$$

so Lemma 3.23 implies

$$\operatorname{val}_z(u_ic_i\operatorname{rem}a_i)\geqslant\delta_i.$$

If follows that $(u_ic_i\operatorname{rem}a_i)/z^{\delta_i}$ belongs to $\mathbb{P}_t$ and that $v((u_ic_i/z^{\delta_i}\operatorname{rem}a_i)\,\hat{a}_i)\geqslant v(a)$. By construction we have

$$\Omega([c]_{v(a);\eta})=([c_1]_{v(a);\eta},\ldots,[c_s]_{v(a);\eta})=(c_1,\ldots,c_s),$$

that proves that Ω is surjective.

Let $b\in(\mathbb{P}_t/(a_1\cdots a_s))_{v(a);\eta}$ be in the kernel of Ω. There exists $q_i\in\mathbb{P}_t$ such that $b=[q_ia_i]_{v(a);\eta}$ for $i=1,\ldots,s$. By Lemma 4.16 we deduce that

$$b=[u_1\hat{a}_1q_1a_1/z^{\delta_1}+\cdots+u_s\hat{a}_sq_sa_s/z^{\delta_s}]_{v(a);\eta},$$

whence $[b\operatorname{rem}a]_{v(a);\eta}=0$. Consequently Ω is injective. □

The Hensel lifting step goes as follows.

PROPOSITION 4.18. *Let a be clustered at* $\mathbb{P}_t$ *of degree* $l\geqslant1$ *in* φ_{t+1}*. Let* $a_1,\ldots,a_s,u_1,\ldots,u_s,\delta_1,\ldots,\delta_s$ *represent a Hensel context for a with relative precision* $\eta>0$*. Then, there exists a unique Hensel context* $\hat{a}_1,\ldots,\hat{a}_s,\hat{u}_1,\ldots,\hat{u}_s,\delta_1,\ldots,\delta_s$ *for a with relative precision* 2η *such that* $[\hat{a}_i]_{v(a_i);\eta}=a_i$ *and* $[\hat{u}_i]_{v(u_i);\eta}=u_i$ *for* $i=1,\ldots,s$*. More precisely, letting*

$$b_i:=u_ia\operatorname{rem}a_i,$$

for $i=1,\ldots,s$*, we have* $\operatorname{val}_z b_i\geqslant\delta_i$*,*

$$\hat{a}_i=a_i+[b_i]_{v(a_i)+\eta+\delta_i;\eta}/z^{\delta_i}.$$

Letting $e:=\sum_{i=1}^s\prod_{j=1,j\neq i}^s\hat{a}_j$ *and*

$$c_i:=u_i\,(z^{\delta_i}-u_ie)\operatorname{rem}\hat{a}_i,\quad \textit{for } i=1,\ldots,s,$$

we also have $\operatorname{val}_z c_i\geqslant\delta_i$ *and*

$$\hat{u}_i=u_i+[c_i]_{v(u_i)+\delta_i+\eta;\eta}/z^{\delta_i}.$$

Proof. For $i=1,\ldots,s$, let us consider unknowns $\tilde{a}_i$ in $[\mathbb{P}_t]_{v(a_i)+\eta;\eta}$ such that $\deg_{\varphi_{t+1}}\tilde{a}_i<l_i$ and

$$[a]_{v(a);2\eta}=[(a_1+\tilde{a}_1)\cdots(a_s+\tilde{a}_s)]_{v(a);2\eta}.$$

After expanding the right-hand side of the latter equation, we obtain equivalently that

$$[a - a_1 \cdots a_s]_{v(a)+\eta;\eta} = [\hat{a}_1 \tilde{a}_1 + \cdots + \hat{a}_s \tilde{a}_s]_{v(a)+\eta;\eta}. \tag{4.7}$$

By Proposition 4.17, equality (4.7) is in turn equivalent to

$$[a \operatorname{rem} a_i]_{v(a)+\eta;\eta} = [(\hat{a}_i \tilde{a}_i) \operatorname{rem} a_i]_{v(a)+\eta;\eta} \quad \text{for } i = 1, \ldots, s.$$

For $i = 1, \ldots, s$, Lemma 4.4 and the constraints on valuations and precisions then yield

$$\begin{aligned}
[u_i a \operatorname{rem} a_i]_{v(a)+v(u_i)+\eta;\eta} &= [u_i \hat{a}_i \tilde{a}_i \operatorname{rem} a_i]_{v(a)+v(u_i)+\eta;\eta} \\
&= [z^{\delta_i} \tilde{a}_i \operatorname{rem} a_i]_{v(a)+\delta_i - v(\hat{a}_i)+\eta;\eta} \\
&= [z^{\delta_i} \tilde{a}_i]_{v(a)+\delta_i - v(\hat{a}_i)+\eta;\eta} \\
&= [z^{\delta_i} \tilde{a}_i]_{v(a_i)+\delta_i+\eta;\eta},
\end{aligned}$$

whence

$$z^{\delta_i} \tilde{a}_i := [u_i a \operatorname{rem} a_i]_{v(a_i)+\delta_i+\eta;\eta}.$$

Then Lemma 3.23 gives

$$\operatorname{val}_z(u_i a \operatorname{rem} a_i) \geqslant v(u_i a \operatorname{rem} a_i) - l_i \gamma_{t+1} \geqslant v(a_i) + \delta_i + \eta - l_i \gamma_{t+1} = \delta_i + \eta.$$

For $i = 1, \ldots, s$, this shows that $\tilde{a}_i$ is uniquely determined by

$$\tilde{a}_i := [u_i a \operatorname{rem} a_i]_{v(a_i)+\delta_i+\eta;\eta} / z^{\delta_i},$$

whence $\hat{a}_1, \ldots, \hat{a}_s$ satisfy the required properties. We finally remark that

$$e \operatorname{rem} \hat{a}_i = \hat{a}_1 \cdots \hat{a}_{i-1} \hat{a}_{i+1} \cdots \hat{a}_s \operatorname{rem} \hat{a}_i$$

for $i = 1, \ldots, s$, so the formulas for the $\hat{u}_i$ follow from Proposition 4.5. □

COROLLARY 4.19. *Let a be clustered at $\mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1} and let $a_1, \ldots, a_s, u_1, \ldots, u_s$, $\delta_1, \ldots, \delta_s$ represent an initial Hensel context for a. Then, there exist unique $a_1^\infty, \ldots, a_s^\infty \in \mathbb{P}_t$ such that $[a_i^\infty]_{v(a_i)} = a_i$, for $i = 1, \ldots, s$, and $a = a_1^\infty \cdots a_s^\infty$.*

Proof. This follows from a repeated use of Proposition 4.18 with increasing precision. □

COROLLARY 4.20. *Let a be clustered at $\mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1} and let $a_1, \ldots, a_s, u_1, \ldots, u_s$, $\delta_1, \ldots, \delta_s$ represent an initial Hensel context for a. Then a_i^∞ (as defined in Corollary 4.19) can be computed modulo $O(z^{\tau - \delta_i})$ for $i = 1, \ldots, s$ from the truncation of a modulo $O(z^\tau)$.*

Proof. We introduce the truncation $\hat{a} := \Pi_t^{-1}([\Pi_t(a)]_{0,\tau})$ of a modulo $O(z^\tau)$ and let η be the smallest element of Γ_{t+1} larger or equal to $\tau - \min_{i=1,\ldots,s}(\delta_i)$. By assumption, $a_1, \ldots$, $a_s, u_1, \ldots, u_s, \delta_1, \ldots, \delta_s$ form an initial Hensel context for $\hat{a}$. From Proposition 4.18 we know that we can compute the Hensel context $\hat{a}_1, \ldots, \hat{a}_s, \hat{u}_1, \ldots, \hat{u}_s, \delta_1, \ldots, \delta_s$ for $\hat{a}$ with relative precision η, so that $[\hat{a} - \hat{a}_1 \cdots \hat{a}_s]_{v(a);\eta} = 0$ and

$$[a - \hat{a}_1 \cdots \hat{a}_s]_{v(a);\eta} = 0 + O(z^\tau).$$

Since u_i / z^{δ_i} is the initial inverse of $\hat{a}_1 \cdots \hat{a}_{i-1} \hat{a}_{i+1} \cdots \hat{a}_s$ modulo a_i, Corollary 4.6 ensures the existence of the modular inverse $\tilde{u}_i$ of $\hat{a}_1 \cdots \hat{a}_{i-1} \hat{a}_{i+1} \cdots \hat{a}_s$ modulo a_i^∞, which satisfies

$$\tilde{u}_i \hat{a}_1 \cdots \hat{a}_{i-1} \hat{a}_{i+1} \cdots \hat{a}_s \operatorname{rem} a_i^\infty = z^{\delta_i}.$$

It follows that

$$[\tilde{u}_i a - \tilde{u}_i \hat{a}_1 \cdots \hat{a}_s]_{v(a)+v(u_i);\eta} = 0 + O(z^\tau),$$

whence

$$[z^{\delta_i} \hat{a}_i \operatorname{rem} a_i^{\infty}]_{v(a)+v(u_i);\eta} = 0 + O(z^{\tau}).$$

Lemma 3.23 implies that

$$\begin{aligned}
\operatorname{val}_z(\hat{a}_i \operatorname{rem} a_i^{\infty}) &\geqslant \min(v(a) + v(u_i) - \delta_i + \eta - l_i \gamma_{t+1}, \tau - \delta_i) \\
&= \min(v(a) + v(u_i) - (v(u_i) + v(a) - v(a_i)) + \eta - v(a_i), \tau - \delta_i) \\
&= \min(\eta, \tau - \delta_i) \\
&\geqslant \tau - \delta_i.
\end{aligned}$$

Since $\hat{a}_i$ and a_i^{∞} are monic of the same degree in φ_{t+1} we deduce that $\hat{a}_i = a_i^{\infty} + O(z^{\tau - \delta_i})$. □

4.6. Hensel lifting via plain coordinates

Hensel lifting is performed by the following algorithm that is dedicated to doubling the relative precision of a Hensel context.

Algorithm 4.2

Input. A contact tower of height t and degree d as above, a rational number $\eta > 0$. A monic polynomial $A \in \mathbb{K}[[z]][x]$ modulo $O(z^{v(a)+2\eta})$, where $a := \Pi_t^{-1}(A)$, and polynomials $A_1, \ldots, A_s, U_1, \ldots, U_s$ in $\mathbb{K}[[z]][x]$ modulo $O(z^{v(a)+\eta})$. Integers $\delta_1, \ldots, \delta_s$ in $\mathbb{N}$. The elements $a_i := \Pi_t^{-1}(A_i)$, $u_i := \Pi_t^{-1}(U_i)$, and δ_i for $i = 1, \ldots, s$ form a Hensel context for a with relative precision η as in Definition 4.15.

Output. $\hat{A}_1, \ldots, \hat{A}_s, \hat{U}_1, \ldots, \hat{U}_s$ in $\mathbb{K}[[z]][x]$ modulo $O(z^{v(a)+2\eta})$, such that the elements $\hat{a}_i := \Pi_t^{-1}(\hat{A}_i)$, $\hat{u}_i := \Pi_t^{-1}(\hat{U}_i)$, and δ_i for $i = 1, \ldots, s$ form a Hensel context for a with relative precision 2η.

```
1. Set $\tau := v(a) + 2\eta$, and $\bar{\delta} := \max(\delta_1, \ldots, \delta_s)$.
2. Compute $R_i := A \operatorname{rem} A_i$ in $\mathbb{K}[[z]]/(z^{\tau+\bar{\delta}})[x]$, for $i = 1, \ldots, s$.
3. For $i = 1, \ldots, s$:
   a. Compute $B_i := U_i R_i \operatorname{rem} A_i$ in $\mathbb{K}[[z]]/(z^{\tau+\delta_i})[x]$,
   b. Compute $\tilde{A}_i := B_i / z^{\delta_i}$ and $\hat{A}_i := A_i + \tilde{A}_i$ in $\mathbb{K}[[z]]/(z^{\tau})[x]$.
4. Compute $E := \sum_{i=1}^{s} \prod_{j=1, j \neq i}^{s} \hat{A}_j$ in $\mathbb{K}[[z]]/(z^{\tau+\bar{\delta}})[x]$.
5. Compute $S_i := E \operatorname{rem} \hat{A}_i$ in $\mathbb{K}[[z]]/(z^{\tau+\bar{\delta}})[x]$ for $i = 1, \ldots, s$.
6. For $i = 1, \ldots, s$, compute $C_i := U_i (z^{\delta_i} - U_i S_i) \operatorname{rem} \hat{A}_i$ in $\mathbb{K}[[z]]/(z^{\tau+\delta_i})[x]$.
7. For $i = 1, \ldots, s$, compute $\tilde{U}_i := C_i / z^{\delta_i}$ and $\hat{U}_i := U_i + \tilde{U}_i$ in $\mathbb{K}[[z]]/(z^{\tau})[x]$.
8. Return $\hat{A}_1, \ldots, \hat{A}_s, \hat{U}_1, \ldots, \hat{U}_s$.
```

PROPOSITION 4.21. *Algorithm 4.2 is correct and takes*

$$O(\mathsf{M}(l d (v(a) + \eta)) \log s)$$

operations in $\mathbb{K}$*, where* $l := \deg_{\varphi_{t+1}} a$.

Proof. The hypotheses of Proposition 4.18 are satisfied. We let

$$b_i := u_i a \operatorname{rem} a_i = \Pi_t^{-1}(B_i).$$

Lemma 3.25 implies

$$[b_i]_{0;\tau+\delta_i} = [\Pi_t^{-1}([B_i]_{0;\tau+\delta_i})]_{0;\tau+\delta_i}.$$

We have seen in Proposition 4.18 that $\mathrm{val}_z\, b_i \geqslant \delta_i$, whence $\mathrm{val}_z\, B_i \geqslant \delta_i$ by Lemma 3.24. Consequently $\tilde{A}_i$ is well defined for $i = 1, \ldots, s$. With the notation of Proposition 4.18 we verify that

$$\begin{aligned}\hat{a}_i &= [a_i + b_i / z^{\delta_i}]_{0;v(a_i)+2\eta}\\ &= [\Pi_t^{-1}(\hat{A}_i)]_{0;v(a_i)+2\eta}\\ &= [\Pi_t^{-1}([\hat{A}_i]_{0;v(a_i)+2\eta})]_{0;v(a_i)+2\eta}.\end{aligned}$$

By Proposition 4.18, properties H_1, H_2, and H_3 of Definition 4.15 thus hold for $\hat{a}_1, \ldots, \hat{a}_s$ and relative precision $2\,\eta$.

In a similar fashion we verify that

$$[c_i]_{0;\tau+\delta_i} = [\Pi_t^{-1}(C_i)]_{0;\tau+\delta_i} = [\Pi_t^{-1}([C_i]_{0;\tau+\delta_i})]_{0;\tau+\delta_i}.$$

From Proposition 4.18 we know that z^{δ_i} divides c_i, so it divides C_i. Consequently $\tilde{U}_i$ is well defined for $i = 1, \ldots, s$, and we have

$$[\hat{u}_i]_{0;v(u_i)+2\eta} = [u_i + \Pi_t^{-1}(\tilde{U}_i)]_{0;v(u_i)+2\eta} = [u_i + \Pi_t^{-1}([\tilde{U}_i]_{0;\tau})]_{0;v(u_i)+2\eta}.$$

By Proposition 4.5, property H_4 holds. We are done with the correctness.

Concerning complexities, from Definition 4.2 we first observe that

$$\delta_i \leqslant v(\hat{a}_i) + \gamma_{t+1} \deg_{\varphi_{t+1}} a_i = v(\hat{a}_i) + v(a_i) = v(a) \text{ and } v(u_i) \leqslant v(a_i),$$

for $i = 1, \ldots, s$. Consequently steps 2, 4, and 5 take

$$O(\mathsf{M}(l\,d\,(v(a) + \eta)) \log s)$$

operations in $\mathbb{K}$ using the sub-product tree technique; see [26, chapter 10, Theorems 10.6 and 10.10], for instance. The other steps require $O(\mathsf{M}(l\,d\,(v(a) + \eta)))$ further operations in $\mathbb{K}$. □

Applying successively Algorithm 4.2 several times enables us to lift an initial Hensel context to any requested precision. The cost is summarized in the following corollary.

COROLLARY 4.22. *Let a be clustered at $\mathbb{P}_t$ of degree l in φ_{t+1}, and let $a_1, \ldots, a_s, u_1, \ldots, u_s, \delta_1, \ldots, \delta_s$ be an initial Hensel context for a. Then, given $\eta > 0$ and $\tau := v(a) + \eta$, we may compute a Hensel context $\hat{a}_1, \ldots, \hat{a}_s, \hat{u}_1, \ldots, \hat{u}_s, \delta_1, \ldots, \delta_s$ for a with relative precision η using*

$$O(\mathsf{M}(l\,d\,\tau) \log(l\,d\,R_{t+1}\, v(a)) \log s)$$

operations in $\mathbb{K}$, where $d = d_1 \cdots d_t$ is the degree of the contact tower.

Proof. We convert the input data into the plain representation modulo $O(z^\tau)$ using Proposition 3.19, with $O(\mathsf{M}(l\,d\,\tau) \log(l\,d))$ operations in $\mathbb{K}$.

We successively apply Algorithm 4.2 to increase the relative precision from $\frac{2^{k-1}}{R_{t+1}}$ to $\frac{2^k}{R_{t+1}}$, for $k = 1, \ldots, \lceil \log_2(R_{t+1}\,\eta) \rceil$. By Proposition 4.21, the total cost of the lifting contributes to

$$\begin{aligned} & O\left(\sum_{k=1}^{\lceil \log_2(R_{t+1}\eta) \rceil} \mathsf{M}\left(l\,d\left(v(a) + \frac{2^k}{R_{t+1}}\right)\right) \log s\right)\\ = {} & O\left(\sum_{k=1}^{\lceil \log_2(R_{t+1} v(a)) \rceil} \mathsf{M}(l\,d\,v(a)) \log s + \sum_{k=\lceil \log_2(R_{t+1} v(a)) \rceil + 1}^{\lceil \log_2(R_{t+1}\eta) \rceil} \mathsf{M}\left(l\,d\,\frac{2^k}{R_{t+1}}\right) \log s\right)\\ = {} & O(\mathsf{M}(l\,d\,v(a)) \log(R_{t+1}\, v(a)) \log s + \mathsf{M}(l\,d\,\eta) \log s)\\ = {} & O(\mathsf{M}(l\,d\,\tau) \log(R_{t+1}\, v(a)) \log s).\end{aligned}$$

At the end of the lifting, we convert the polynomials to contact coordinates modulo $O(z^\tau)$ using Proposition 3.19, again with $O(\mathsf{M}(l\,d\,\tau)\log(l\,d))$ operations in $\mathbb{K}$. □

COROLLARY 4.23. *Let a be clustered at $\mathbb{P}_t$ of degree l in φ_{t+1}, and let $a_1,\ldots,a_s,u_1,\ldots,u_s,\delta_1,\ldots,\delta_s$ be an initial Hensel context for a. Then, given a at precision $O(z^\tau)$ we can compute a_i^∞ (as defined in Corollary 4.20) at precision $O(z^{\tau-\delta_i})$ for $i=1,\ldots s$, using*

$$O(\mathsf{M}(l\,d\,\tau)\log(l\,d\,v(a))\log s)$$

operations in $\mathbb{K}$, where $d=d_1\cdots d_t$ is the degree of the contact tower.

Proof. We use Corollary 4.22 with the relative precision $\eta:=\tau-\min_{i=1,\ldots,s}(\delta_i)$ as in the proof of Corollary 4.20. The running time is

$$O(\mathsf{M}(l\,d\,(v(a)+\eta))\log(l\,d\,R_{t+1}\,v(a))\log s).$$

Then we verify that

$$v(a)+\tau-\delta_i=v(a)+\tau-\lfloor v(\hat{a}_i)+l_i\,\gamma_{t+1}\rfloor\leqslant v(a)+\tau-(v(a)-1)=\tau+1.$$

Using $R_{t+1}\leqslant R_t\,l\leqslant l\,d$ the cost of the lifting simplifies to $O(\mathsf{M}(l\,d\,\tau)\log(l\,d\,v(a))\log s)$. □

5. SEPARABLE TOWERS

In this section we introduce the notion of "separability" for contact towers. This will allow the construction of derivations on contact towers, which will be the key ingredient of the central shift algorithm in section 7.7.

5.1. Definition

Informally speaking, a contact tower is said to be separable when the initial forms of the its defining polynomials Φ_i are separable. The precise definition is as follows.

DEFINITION 5.1. *A tower $(\mathbb{P}_i)_{i\leqslant t}$ of contact coordinates as in Definition 3.1 is said to be* ***separable*** *when $\frac{\partial\Phi_i}{\partial\varphi_i}$ is initially invertible in $\mathbb{P}_i$, for $i=1,\ldots,s$. It is said to be* ***effectively separable*** *if the normalized initial inverses of the $\frac{\partial\Phi_i}{\partial\varphi_i}$ are known for algorithmic purpose.*

Throughout this section, we assume that $(\mathbb{P}_i)_{i\leqslant t}$ is effectively separable. For $i=1,\ldots,t$, $\Theta_i\in\mathbb{K}[z,\varphi_1,\ldots,\varphi_i]$ represents the initial inverse of $\frac{\partial\Phi_i}{\partial\varphi_i}$ modulo Φ_i. More precisely, we assume that Θ_i is homogeneous and satisfies $\mathrm{in}\left(\Theta_i\frac{\partial\Phi_i}{\partial\varphi_i}\right)=z^{\kappa_i}$, where $\kappa_i\in\mathbb{N}$. From Definition 4.1 we know that

$$0\leqslant\kappa_i\leqslant(2\,d_i-1)\,\gamma_i,$$

since $\mathrm{val}\left(\frac{\partial\Phi_i}{\partial\varphi_i}\right)=(d_i-1)\,\gamma_i$.

Example 5.2. We define an effectively separable contact tower of height 1 by taking $t=1$, $\Phi_1=\varphi_1^2-3$, $\gamma_1=0$, $\kappa_1=0$, and $\Theta_1=\varphi_1/6$. Indeed,

$$\mathrm{in}\left(\Theta_1\frac{\partial\Phi_1}{\partial\varphi_1}\,\mathrm{rem}_{\varphi_1}\,\Phi_1\right)=\mathrm{in}\left(\frac{\varphi_1^2}{3}\,\mathrm{rem}_{\varphi_1}\,\Phi_1\right)=1,$$

where rem_{φ_1} stands for remainder with respect to the variable φ_1.

Example 5.3. Consider Example (2.6): $\Phi_1 = \varphi_1^2 - 3$ and $\Phi_2 = \varphi_2^2 - 5\, z^2\, \varphi_1$ form a contact tower of height $t = 2$ with contact slopes $\gamma_1 = 0$, $\gamma_2 = 1$. We get γ_1 and γ_2 from $2\,\gamma_1 = \mathrm{val}(\varphi_1^2) = \mathrm{val}(-3) = 0$ and $2\,\gamma_2 = \mathrm{val}(\varphi_2^2) = \mathrm{val}(5\, z^2\, \varphi_1) = 2$. As for the modular inverses we may take $\kappa_1 = 0$, $\kappa_2 = 2$,

$$\Theta_1 = \frac{\varphi_1}{6}, \text{ and } \Theta_2 = \frac{\varphi_1\, \varphi_2}{30}.$$

Indeed, we verify that

$$\begin{aligned} \mathrm{in}\left(\Theta_2 \frac{\partial \Phi_2}{\partial \varphi_2} \mathrm{rem}_{\varphi_2} \Phi_2 \right) &= \mathrm{in}\left(\frac{\varphi_1\, \varphi_2^2}{15} \mathrm{rem}_{\varphi_2} \Phi_2 \right) \\ &= \mathrm{in}\left(\frac{\varphi_1\, (5\, z^2\, \varphi_1 + \varphi_3)}{15} \mathrm{rem}_{\varphi_2} \Phi_2 \right) \\ &= \mathrm{in}(z^2). \end{aligned}$$

5.2. First derivatives

Since the map $\Pi_t \colon \mathbb{P}_t \rightarrow \mathbb{K}[[z]][x]$ is a $\mathbb{K}[[z]]$-isomorphism, from Lemma 3.15, the derivation $\frac{\mathrm{d}}{\mathrm{d}x}$ on $\mathbb{K}[[z]][x]$ induces a derivation on $\mathbb{P}_t$ (that is still denoted by $\frac{\mathrm{d}}{\mathrm{d}x}$ for simplicity):

$$\frac{\mathrm{d}a}{\mathrm{d}x} := \Pi_t^{-1}\left(\frac{\mathrm{d}}{\mathrm{d}x} (\Pi_t(a)) \right).$$

The separability assumption ensures that this derivation satisfies several convenient properties.

LEMMA 5.4. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be a separable contact tower. For $i = 1, \ldots, t$ we have*

$$\mathrm{in}\left(\frac{\mathrm{d}\varphi_{i+1}}{\mathrm{d}x} \right) = \mathrm{in}\left(\frac{\partial \Phi_i}{\partial \varphi_i} \frac{\mathrm{d}\varphi_i}{\mathrm{d}x} \right)$$

and

$$v\left(\frac{\mathrm{d}\varphi_{i+1}}{\mathrm{d}x} \right) = (d_i - 1)\, \gamma_i + (d_{i-1} - 1)\, \gamma_{i-1} + \cdots + (d_1 - 1)\, \gamma_1.$$

Proof. We prove the result by induction on i. For $i = 1$ we have

$$\frac{\mathrm{d}\varphi_2}{\mathrm{d}x} = \frac{\partial \Phi_1}{\partial \varphi_1}$$

and

$$v\left(\frac{\mathrm{d}\varphi_2}{\mathrm{d}x} \right) = \mathrm{val}\left(\frac{\partial \Phi_1}{\partial \varphi_1} \right) = (d_1 - 1)\, \gamma_1.$$

For $i = 2, \ldots, t$ we have

$$\frac{\mathrm{d}\varphi_{i+1}}{\mathrm{d}x} = \frac{\partial \Phi_i}{\partial \varphi_1} + \frac{\partial \Phi_i}{\partial \varphi_2} \frac{\mathrm{d}\varphi_2}{\mathrm{d}x} + \cdots + \frac{\partial \Phi_i}{\partial \varphi_i} \frac{\mathrm{d}\varphi_i}{\mathrm{d}x}.$$

By Lemma 4.3, the separability assumption yields

$$v\left(\frac{\partial \Phi_i}{\partial \varphi_i} \frac{\mathrm{d}\varphi_i}{\mathrm{d}x} \right) = v\left(\frac{\partial \Phi_i}{\partial \varphi_i} \right) + v\left(\frac{\mathrm{d}\varphi_i}{\mathrm{d}x} \right).$$

Combined with the induction hypothesis we deduce

$$v\left(\frac{\partial \Phi_i}{\partial \varphi_i} \frac{\mathrm{d}\varphi_i}{\mathrm{d}x} \right) = (d_i - 1)\, \gamma_i + (d_{i-1} - 1)\, \gamma_{i-1} + \cdots + (d_1 - 1)\, \gamma_1.$$

On the other hand, for $j < i$ we have

$$v\left(\frac{\partial \Phi_i}{\partial \varphi_j} \frac{\mathrm{d}\varphi_j}{\mathrm{d}x} \right) \geqslant d_i\, \gamma_i - \gamma_j + (d_{j-1} - 1)\, \gamma_{j-1} + \cdots + (d_1 - 1)\, \gamma_1,$$

and therefore

$$\begin{aligned}
&v\left(\frac{\partial \Phi_i}{\partial \varphi_j}\frac{\mathrm{d}\varphi_j}{\mathrm{d}x}\right)-v\left(\frac{\partial \Phi_i}{\partial \varphi_i}\frac{\mathrm{d}\varphi_i}{\mathrm{d}x}\right)\\
\geqslant\ & d_i\gamma_i-\gamma_j-(d_i-1)\,\gamma_i-(d_{i-1}-1)\,\gamma_{i-1}-\cdots-(d_j-1)\,\gamma_j\\
=\ & \gamma_i-(d_{i-1}-1)\,\gamma_{i-1}-\cdots-(d_j-1)\,\gamma_j-\gamma_j\\
=\ & (\gamma_i-d_{i-1}\gamma_{i-1})+\cdots+(\gamma_{j+1}-d_j\gamma_j)\\
>\ & 0.
\end{aligned}$$

□

5.3. Higher derivatives

We now study the effect of several consecutive differentiations in x.

LEMMA 5.5. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be a separable contact tower. For any $c\in\mathbb{P}_{t-1}$ we have*

$$\begin{aligned}
v\left(\frac{\mathrm{d}c}{\mathrm{d}x}\right) &\geqslant v(c)+(d_{t-1}\gamma_{t-1}-\gamma_t)+\cdots+(d_1\gamma_1-\gamma_2)-\gamma_1\\
&= v(c)-\gamma_t+v\left(\frac{\mathrm{d}\varphi_t}{\mathrm{d}x}\right).
\end{aligned}$$

Proof. The inequality follows from

$$\frac{\mathrm{d}c}{\mathrm{d}x}=\sum_{i=1}^{t}\frac{\partial c}{\partial\varphi_i}\frac{\mathrm{d}\varphi_i}{\mathrm{d}x},$$

Lemma 5.4, and the inequality

$$-\gamma_i+(d_{i-1}-1)\,\gamma_{i-1}+\cdots+(d_1-1)\,\gamma_1\geqslant-\gamma_{i+1}+(d_i-1)\,\gamma_i+\cdots+(d_1-1)\,\gamma_1$$

for $i=1,\ldots,t-1$. □

LEMMA 5.6. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be a separable contact tower and let $a\in\mathbb{P}_{t+1}$ be such that*

$$v\left(\frac{\partial a}{\partial\varphi_{t+1}}\right)=v(a)-\gamma_{t+1}.$$

Then we have

$$\mathrm{in}\left(\frac{\mathrm{d}a}{\mathrm{d}x}\right)=\mathrm{in}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\frac{\partial a}{\partial\varphi_{t+1}}\right).$$

Proof. Writing $a=c_l\varphi_{t+1}^l+\cdots+c_0$, we have

$$\frac{\mathrm{d}a}{\mathrm{d}x}=\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\frac{\partial a}{\partial\varphi_{t+1}}+\sum_{j=0}^{l}\frac{\mathrm{d}c_j}{\mathrm{d}x}\varphi_{t+1}^j.$$

Then, for $j=0,\ldots,l$, we have $v(c_j)\geqslant v(a)-j\gamma_{t+1}$ so Lemma 5.5 yields

$$v\left(\frac{\mathrm{d}c_j}{\mathrm{d}x}\varphi_{t+1}^j\right)\geqslant v(a)-\gamma_t+v\left(\frac{\mathrm{d}\varphi_t}{\mathrm{d}x}\right).$$

On the other hand,

$$v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\frac{\partial a}{\partial\varphi_{t+1}}\right)=v(a)-\gamma_{t+1}+v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right), \tag{5.1}$$

so Lemma 5.4 implies

$$v\left(\frac{\mathrm{d}c_j}{\mathrm{d}x}\varphi_{t+1}^j\right)-v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\frac{\partial a}{\partial\varphi_{t+1}}\right)\ \geqslant\ \gamma_{t+1}-d_t\gamma_t\ >\ 0$$

and

$$\operatorname{in}\left(\frac{\mathrm{d}a}{\mathrm{d}x}\right)=\operatorname{in}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\frac{\partial a}{\partial\varphi_{t+1}}\right).$$ □

LEMMA 5.7. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be a separable contact tower. Given $a\in\mathbb{P}_t$ and $k\geqslant 0$ such that*

$$v\left(\frac{\partial^k a}{\partial\varphi_{t+1}^k}\right)=v(a)-k\gamma_{t+1},$$

we have

$$\operatorname{in}\left(\frac{\mathrm{d}^k a}{\mathrm{d}x^k}\right)=\operatorname{in}\left(\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^k\frac{\partial^k a}{\partial\varphi_{t+1}^k}\right).$$

Proof. First note that

$$v\left(\frac{\partial^j a}{\partial\varphi_{t+1}^j}\right)=v(a)-j\gamma_{t+1}$$

holds for all $j\leqslant k$. We prove the lemma by induction on k. The result is clear for $k=0$, so assume that $k\geqslant 1$. The induction hypothesis implies that

$$\frac{\mathrm{d}^{k-1}a}{\mathrm{d}x^{k-1}}=\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\frac{\partial^{k-1}a}{\partial\varphi_{t+1}^{k-1}}+R \tag{5.2}$$

for some R such that

$$v(R)>v\left(\frac{\mathrm{d}^{k-1}a}{\mathrm{d}x^{k-1}}\right).$$

Differentiating (5.2) with respect to φ_{t+1} yields

$$\frac{\partial}{\partial\varphi_{t+1}}\frac{\mathrm{d}^{k-1}a}{\mathrm{d}x^{k-1}}=\frac{\partial}{\partial\varphi_{t+1}}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\frac{\partial^{k-1}a}{\partial\varphi_{t+1}^{k-1}}+\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\frac{\partial^k a}{\partial\varphi_{t+1}^k}+\frac{\partial R}{\partial\varphi_{t+1}}. \tag{5.3}$$

Since $\operatorname{in}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)$ does not depend on φ_{t+1}, the initial form of $\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}$ also does not depend on φ_{t+1}. It follows that

$$v\left(\frac{\partial}{\partial\varphi_{t+1}}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\right)>v\left(\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\right)-\gamma_{t+1},$$

whence

$$v\left(\frac{\partial}{\partial\varphi_{t+1}}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\frac{\partial^{k-1}a}{\partial\varphi_{t+1}^{k-1}}\right)>v\left(\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\frac{\partial^k a}{\partial\varphi_{t+1}^k}\right). \tag{5.4}$$

Equation (5.2), the assumption on a, and the definition of R imply that

$$v\left(\frac{\partial R}{\partial\varphi_{t+1}}\right)\geqslant v(R)-\gamma_{t+1}>v\left(\frac{\mathrm{d}^{k-1}a}{\mathrm{d}x^{k-1}}\right)-\gamma_{t+1}=v\left(\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\frac{\partial^k a}{\partial\varphi_{t+1}^k}\right). \tag{5.5}$$

By combining (5.3), (5.4), and (5.5) we deduce

$$\operatorname{in}\left(\frac{\partial}{\partial\varphi_{t+1}}\frac{\mathrm{d}^{k-1}a}{\mathrm{d}x^{k-1}}\right)=\operatorname{in}\left(\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)^{k-1}\frac{\partial^k a}{\partial\varphi_{t+1}^k}\right). \tag{5.6}$$

On the other hand Lemma 5.6 gives us

$$\operatorname{in}\left(\frac{\mathrm{d}^k a}{\mathrm{d}x^k}\right)=\operatorname{in}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\frac{\partial}{\partial\varphi_{t+1}}\frac{\mathrm{d}^{k-1}a}{\mathrm{d}x^{k-1}}\right). \tag{5.7}$$

We conclude the proof by combining equations (5.6) and (5.7). □

6. INITIAL EXPANSIONS

Canonical representations are not always the most efficient ones for computations with initial forms. This can be already observed in the case when $t=1$. Indeed, let us write

$$\mathrm{in}(\Phi_1)=\varphi_1^{d_1}+c_{d_1-1}z^{e_{d_1-1}}\varphi_1^{d_1-1}+\cdots+c_0z^{e_0},$$

with $c_i\in\mathbb{K}$ and $e_i\in\mathbb{N}$ for $i=0,\ldots,d_1-1$. Let f_1 and $r_1\geqslant 1$ be coprime integers such that

$$\gamma_1=\frac{f_1}{r_1}=\frac{e_0}{d_1}.$$

Then, the coefficient c_j is zero whenever j is not a multiple of r_1. This shows that $\mathrm{in}(\Phi_1)$ is sparse in the sense that it contains at most $s_1:=d_1/r_1$ non-zero terms besides $\varphi_1^{d_1}$. In particular, computations that use the dense representation are deemed to be suboptimal.

Assume for instance that we need to compute the valuation and the initial inverse of $a\in\mathbb{P}_1$. We first extract the initial part of its canonical representative A; there exist $k\in\{0,\ldots,r_1-1\}$ and $a_0,\ldots,a_{s_1-1}\in\mathbb{K}$ such that

$$\mathrm{in}(A)=a_{s_1-1}z^{\sigma-(s_1-1)f_1-k\frac{f_1}{r_1}}\varphi_1^{(s_1-1)r_1+k}+\cdots+a_0z^{\sigma-k\frac{f_1}{r_1}}\varphi_1^k,$$

where $\sigma:=\mathrm{val}\,A$. Note that $\mathrm{in}(A)$ is again sparse. We now have to compute the Bézout relation of the specializations at $z=1$ of $\mathrm{in}(A)$ and $\mathrm{in}(\Phi_1)$ in $\mathbb{K}[\varphi_1]$. Without exploiting the sparsity, this computation takes $O(\mathsf{M}(d_1)\log d_1)$ operations in $\mathbb{K}$. In this particular case, the remedy is to compute with respect to $\varphi_1^{r_1}$ instead of φ_1, while exploiting the fact that $\mathrm{in}(A)\,\varphi_1^{-k}$ and $\mathrm{in}(\Phi_1)$ are dense polynomials in $\varphi_1^{r_1}$.

In order to generalize this remedy to the case when $t>1$, we show in this section how to rewrite sparse homogeneous polynomials in $\mathbb{K}[[z]][\varphi_1,\ldots,\varphi_t]$ into suitable products of coefficients in "algebraic towers" $(\mathbb{A}_i)_{i\leqslant t}$ over $\mathbb{K}$ and "monomials".

In all computations below, $(\mathbb{P}_i)_{i\leqslant t}$ will be an effectively separable contact tower (as in Definition 5.1) that satisfies the following additional property.

DEFINITION 6.1. *With the notation of Definition 3.1, a contact tower of height t is said to be* ***regular*** *when $\Phi_i(\varphi_1,\ldots,\varphi_{i-1},0)$ has valuation $d_i\gamma_i$ and is initially invertible, for $i=1,\ldots,s$. It is said to be* ***effectively regular*** *if the normalized initial inverse of $\Phi_i(\varphi_1,\ldots,\varphi_{i-1},0)$ is known for algorithm purpose, for $i=1,\ldots,s$.*

This regularity assumption implies that γ_i is determined by

$$\gamma_i=\frac{1}{d_i}\mathrm{val}(\Phi_i(\varphi_1,\ldots,\varphi_{i-1},0)).$$

6.1. Definition

An *algebraic tower* over $\mathbb{K}$ is a sequence $(\mathbb{A}_i)_{i\leqslant t}$ with $\mathbb{A}_0:=\mathbb{K}$ and $\mathbb{A}_i:=\mathbb{A}_{i-1}[x_i]/(\mu_i(x_i))$, for $i=1,\ldots,t$ and monic polynomials $\mu_i(x_i)\in\mathbb{A}_{i-1}[x_i]$. We will write α_i for the image of x_i in $\mathbb{A}_i$ and set $s_i:=\deg\mu_i$ for $i=1,\ldots,t$. The tower is said to be *effectively separable* when we are given u and v in $\mathbb{A}_{i-1}[x_i]$ of respective degree $<\deg\mu_i$ and $<\deg\mu_i-1$ such that the Bézout relation

$$1=u\,\mu_i'+v\,\mu_i$$

holds, for $i=1,\ldots,t$. The next definition concerns the alternative representation of homogeneous polynomials modulo $(\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_t))$.

DEFINITION 6.2. *An* ***initial expansion*** *consists of the following data:*

- *An effectively separable tower*

  $$\mathbb{A}_0 := \mathbb{K} \text{ and } \mathbb{A}_i := \mathbb{A}_{i-1}[x_i] / (\mu_i(x_i)), \text{ for } i = 1, \ldots, t,$$

  where μ_i is monic of degree $s_i > 0$ in $\mathbb{A}_{i-1}[x_i]$. The class of x_i in $\mathbb{A}_i$ is written α_i. For $i=1,...,t$ the inverse of α_i exists and is known.

- *A tower of purely ramified extensions of $\mathbb{B}_0 := \mathbb{K}[[z]]$, written*

  $$\mathbb{B}_i := \mathbb{A}_i[y_1, \ldots, y_i] / \left(y_1^{r_1} - b_0 \alpha_1 z^{f_{1,0}}, \ldots, y_i^{r_i} - b_{i-1} \alpha_i z^{f_{i,0}} y_1^{f_{i,1}} \cdots y_{i-1}^{f_{i,i-1}}\right),$$

  where $r_1, \ldots, r_t$ are positive integers called ***ramification indices****,*

  $$(f_{i,0}, \ldots, f_{i,i-1}) \in \mathbb{N} \times \{0, \ldots, r_1 - 1\} \times \cdots \times \{0, \ldots, r_{i-1} - 1\},$$

  for $i = 1, \ldots, t$, and b_j is invertible in $\mathbb{A}_j$ for $j = 0, \ldots, t-1$. The class of y_i in $\mathbb{B}_i$ is written β_i.

- *$\rho_i \in \mathbb{A}_i$ and a uniformizing parameter $\pi_i \in \mathbb{B}_i$ such that $\pi_i^{R_i} = \rho_i z$, where $R_i := r_1 \cdots r_i$, for $i = 1, \ldots, t$.*

- *$f_i \in \mathbb{N}^>$ coprime with r_i along with integers u_i and v_i such that $\pi_i^{f_i} = \alpha_i^{-u_i} \beta_i$ and $u_i r_i + v_i f_i = 1$, for $i = 1, \ldots, t$.*

6.2. Initial expansions for towers of height $t = 1$

The construction of an initial expansion associated to a contact tower is achieved by induction on t. This subsection is devoted to the case when $t = 1$. As in the introduction of this section, we write

$$\operatorname{in}(\Phi_1) = \varphi_1^{d_1} + c_{d_1-1} z^{e_{d_1-1}} \varphi_1^{d_1-1} + \cdots + c_0 z^{e_0},$$

with $c_i \in \mathbb{K}$ and $e_i \in \mathbb{N}$ for $i = 0, \ldots, d_1 - 1$. Note that $c_0 \neq 0$ because the tower is regular. As before, we let f_1 and $r_1 \geqslant 1$ be coprime integers such that

$$\gamma_1 = \frac{e_0}{d_1} = \frac{f_1}{r_1}.$$

We define

$$\mu_1(x_1) := x_1^{s_1} + c_{d_1 - r_1} x_1^{s_1 - 1} + \cdots + c_{r_1} x_1 + c_0,$$

where $s_1 := d_1 / r_1$. Note that $c_j = 0$ whenever j is not a multiple of r_1. The inverse of α_1 is:

$$\alpha_1^{-1} = \left(\frac{\mu_1(x_1) - \mu_1(0)}{-\mu_1(0)\, x_1}\right)(\alpha_1).$$

With $f_{1,0} := f_1$ and $b_0 := 1$, the map

$$\begin{array}{rrcl} \mathrm{T}_1\colon & \mathbb{K}((z))[\varphi_1] / (\operatorname{in}(I_1)) & \cong & \mathbb{B}_1[z^{-1}] \\ & \varphi_1 & \longmapsto & \beta_1, \end{array}$$

is well defined because

$$\begin{aligned} (\operatorname{in}(\Phi_1))(\beta_1) &= \beta_1^{d_1} + c_{d_1 - r_1} z^{f_1} \beta_1^{d_1 - r_1} + \cdots + c_0 z^{d_1 f_1 / r_1} \\ &= (\beta_1^{r_1})^{s_1} + c_{d_1 - r_1} z^{f_1} (\beta_1^{r_1})^{s_1 - 1} + \cdots + c_0 z^{f_1 s_1} \\ &= (\alpha_1 z^{f_1})^{s_1} + c_{d_1 - r_1} z^{f_1} (\alpha_1 z^{f_1})^{s_1 - 1} + \cdots + c_0 z^{f_1 s_1} \\ &= \mu_1(\alpha_1)\, z^{f_1 s_1} \\ &= 0. \end{aligned}$$

Let us now show how to compute conversions *via* T_1. Let $A \in \mathbb{K}[z][\varphi_1]_{<d_1}$ be homogeneous of valuation σ and write

$$A = a_{s_1-1} z^{\sigma-(s_1-1)f_1-k\frac{f_1}{r_1}} \varphi_1^{(s_1-1)r_1+k} + \cdots + a_0 z^{\sigma-k\frac{f_1}{r_1}} \varphi_1^k$$

with $k \in \{0,\ldots,r_1-1\}$. Then the formula

$$\mathrm{T}_1(A) = z^{\sigma-k\frac{f_1}{r_1}} \beta_1^k (a_{s_1-1} \alpha_1^{s_1-1} + \cdots + a_1 \alpha_1 + a_0)$$

allows for the computation of $\mathrm{T}_1(A)$ without any arithmetic operations or zero tests. This also shows that T_1 is an isomorphism.

Assume that two elements $z^{\varepsilon_0} \beta_1^{\varepsilon_1}$ and $z^{\varepsilon_0'} \beta_1^{\varepsilon_1'}$ in $\mathbb{B}_1[z^{-1}]$ with $0 \leqslant \varepsilon_1' \leqslant \varepsilon_1 < r_1$ have the same valuation, that is

$$\varepsilon_0 + \varepsilon_1 \frac{f_1}{r_1} = \varepsilon_0' + \varepsilon_1' \frac{f_1}{r_1}.$$

If $f_1 = 0$ (that corresponds to $e_0 = 0$), then $r_1 = 1$ so $\varepsilon_1 = \varepsilon_1' = 0$ and therefore $\varepsilon_0 = \varepsilon_0'$. Otherwise we have

$$(\varepsilon_1' - \varepsilon_1) f_1 = (\varepsilon_0 - \varepsilon_0') r_1,$$

and r_1 and f_1 are coprime. So r_1 divides $\varepsilon_1' - \varepsilon_1$, whence $\varepsilon_1' = \varepsilon_1$ and $\varepsilon_0' = \varepsilon_0$. In other words, any homogeneous element in $\mathbb{B}_1[[z^{-1}]]$ can be written in a unique way as $c z^{\varepsilon_0} \beta_1^{\varepsilon_1}$ with $c \in \mathbb{A}_1$, $\varepsilon_0 \in \mathbb{Z}$, and $0 \leqslant \varepsilon_1 < r_1$.

Now consider the Bézout relation $u_1 r_1 + v_1 f_1 = 1$ between r_1 and f_1, with $|u_1| < f_1$ and $|v_1| < r_1$. The element

$$\pi_1 := z^{u_1} \beta_1^{v_1} \in \mathbb{B}_1[z^{-1}]$$

has valuation $1/r_1$. From

$$\pi_1^{r_1} = z^{u_1 r_1} \beta_1^{v_1 r_1} = z^{1-v_1 f_1} \beta_1^{v_1 r_1} = z^{1-v_1 f_1} (\alpha_1 z^{f_1})^{v_1} = \alpha_1^{v_1} z$$

and

$$\pi_1^{f_1} = z^{u_1 f_1} \beta_1^{v_1 f_1} = z^{u_1 f_1} \beta_1^{1-u_1 r_1} = z^{u_1 f_1} \beta_1 (\alpha_1 z^{f_1})^{-u_1} = \alpha_1^{-u_1} \beta_1,$$

we obtain formulas to rewrite z and β_1 in terms of π_1:

$$z = \alpha_1^{-v_1} \pi_1^{r_1}, \quad \beta_1 = \alpha_1^{u_1} \pi_1^{f_1}.$$

Consequently π_1 is a *uniformizing parameter* of $\mathbb{B}_1[z^{-1}]$, whose valuation group is

$$\bar{\Gamma}_1 = \frac{1}{r_1} \mathbb{Z},$$

and $\rho_1 := \alpha_1^{u_1}$. In particular, $\mathbb{B}_1$ is a purely ramified extension of $\mathbb{B}_0$. It remains to make $(\mathbb{A}_i)_{i \leqslant 1}$ effectively separable. To this end, we first compute

$$\begin{aligned}
\mathrm{T}_1\left(\mathrm{in}\left(\frac{\partial \Phi_1}{\partial \varphi_1}\right)\right) &= \mathrm{T}_1\left(\frac{\partial}{\partial \varphi_1} (\varphi_1^{r_1 s_1} + c_{d_1-r_1} z^{f_1} \varphi_1^{r_1(s_1-1)} + \cdots + c_0 z^{f_1 s_1})\right) \\
&= \mathrm{T}_1((s_1 \varphi_1^{r_1(s_1-1)} + (s_1-1) c_{d_1-r_1} z^{f_1} \varphi_1^{r_1(s_1-2)} + \cdots + c_{r_1} z^{f_1(s_1-1)}) r_1 \varphi_1^{r_1-1}) \\
&= (s_1 \alpha_1^{s_1-1} z^{f_1(s_1-1)} + (s_1-1) c_{d_1-r_1} \alpha_1^{s_1-2} z^{f_1(s_1-1)} + \cdots + c_{r_1} z^{f_1(s_1-1)}) r_1 \beta_1^{r_1-1} \\
&= r_1 \mu_1'(\alpha_1) z^{f_1(s_1-1)} \beta_1^{r_1-1}.
\end{aligned}$$

Let Θ_1 and κ_1 be such that $\mathrm{in}\left(\Theta_1 \frac{\partial \Phi_1}{\partial \varphi_1}\right) = z^{\kappa_1}$ and let $\theta_1(\alpha_1)\, z^{\varepsilon_0} \beta_1^{\varepsilon_1} := \mathrm{T}_1(\mathrm{in}(\Theta_1))$ be such that $0 \leqslant \varepsilon_1 \leqslant r_1 - 1$. Then we have

$$\begin{aligned} z^{\kappa_1} &= \theta_1(\alpha_1)\, z^{\varepsilon_0} \beta_1^{\varepsilon_1} r_1 \mu_1'(\alpha_1)\, z^{f_1(s_1-1)} \beta_1^{r_1-1} \\ &= r_1 \theta_1(\alpha_1)\, \mu_1'(\alpha_1)\, z^{\varepsilon_0 + f_1(s_1-1)} \beta_1^{\varepsilon_1 + r_1 - 1}. \end{aligned}$$

Necessarily $\varepsilon_1 = 1$ and $r_1 \alpha_1 \theta_1(\alpha_1)$ is the inverse of $\mu_1'(\alpha_1)$. From this inverse we easily recover the Bézout relation of μ_1' and μ_1, that makes the tower $(\mathbb{A}_i)_{i \leqslant 1}$ effectively separable.

6.3. Initial expansions for towers of height $t \geqslant 2$

The next lemma deals with the construction of an initial expansion associated to a contact tower. We extend the above construction for $t = 1$.

LEMMA 6.3. *Given an effectively separable and regular contact tower $(\mathbb{P}_i)_{i \leqslant t}$, there exists an initial expansion such that each r_i divides d_i, and*

$$\begin{aligned} \mathrm{T}_i\colon \quad \mathbb{K}((z))[\varphi_1, \ldots, \varphi_i] / (\mathrm{in}(I_i)) &\cong \mathbb{B}_i[z^{-1}] \\ \varphi_j &\longmapsto \beta_j \quad \textit{for } j = 1, \ldots, i, \end{aligned} \tag{6.1}$$

is a $\mathbb{K}((z))$-algebra isomorphism, for $i = 1, \ldots, t$. We set $s_i := d_i / r_i$. In addition, with $R_i := r_1 \cdots r_i$, $\mathbb{B}_i[z^{-1}]$ has valuation group

$$\bar{\Gamma}_i = \frac{1}{R_i} \mathbb{Z}.$$

The algebra $\mathbb{B}_i[z^{-1}]$ inherits the grading of $\mathbb{K}((z))[\varphi_1, \ldots, \varphi_i]$. We still write v for the semi-valuation induced over $\mathbb{B}_i[z^{-1}]$, so $v(z) = 1$ and $v(\beta_i) = \gamma_i$ for $i = 1, \ldots, t$. Any homogeneous element of $\mathbb{B}_i[z^{-1}]$ can uniquely be written as $c z^{\varepsilon_0} \beta_1^{\varepsilon_1} \cdots \beta_i^{\varepsilon_i}$, where $c \in \mathbb{A}_i$ and

$$(\varepsilon_0, \ldots, \varepsilon_i) \in \mathbb{Z} \times \{0, \ldots, r_1 - 1\} \times \cdots \times \{0, \ldots, r_i - 1\}.$$

Proof. We prove the lemma by induction on t. The case $t = 1$ has been addressed in the previous subsection, so we assume that $t \geqslant 2$ and recall that π_{t-1} is a uniformizing parameter of $\mathbb{B}_{t-1}[z^{-1}]$. We write

$$\mathrm{in}(\Phi_t) = \varphi_t^{d_t} + C_{d_t - 1} \varphi_t^{d_t - 1} + \cdots + C_0,$$

where $C_j \in \mathbb{K}[z][\varphi_1, \ldots, \varphi_{t-1}]$ is homogeneous for $j = 0, \ldots, d_{t-1}$. Then we define

$$c_j \pi_{t-1}^{e_j} := \mathrm{T}_{t-1}(C_j),$$

where $c_j \in \mathbb{A}_{t-1}$ and $e_j \in \mathbb{N}$, for $j = 0, \ldots, d_t - 1$. We introduce

$$s_t := \gcd(d_t, e_0), \; r_t := \frac{d_t}{s_t}, \; f_t := \frac{e_0}{s_t},$$

so we have

$$\gamma_t = \frac{e_0}{d_t R_{t-1}} = \frac{f_t}{r_t R_{t-1}}. \tag{6.2}$$

Since the tower is regular, c_0 is invertible. Since $\mathrm{in}(\Phi_t)$ is homogeneous, we have $c_j = 0$ whenever j is not a multiple of r_t and

$$e_{d_t - j r_t} + (d_t - j r_t) \frac{f_t}{r_t} = d_t \frac{f_t}{r_t}$$

for $j=1,\ldots,s_t$. The latter equation is equivalent to

$$e_{d_t-jr_t}=jf_t.$$

We define μ_t as

$$\mu_t(x_t):=x_t^{s_t}+c_{d_t-r_t}x_t^{s_t-1}+\cdots+c_{r_t}x_t+c_0$$

and

$$\beta_t^{r_t}=\alpha_t\pi_{t-1}^{f_t}. \tag{6.3}$$

The inverse of α_t is then given by

$$\alpha_t^{-1}=\left(\frac{\mu_t(x_t)-\mu_t(0)}{-\mu_t(0)\,x_t}\right)(\alpha_t). \tag{6.4}$$

From the induction hypothesis, $\pi_{t-1}^{f_t}$ can uniquely be rewritten as

$$\pi_{t-1}^{f_t}=b_{t-1}z^{f_{t,0}}\beta_1^{f_{t,1}}\cdots\beta_{t-1}^{f_{t,t-1}},$$

where b_{t-1} is invertible in $\mathbb{A}_{t-1}$ and $(f_{t,0},\ldots,f_{t,t-1})\in\mathbb{Z}\times\{0,\ldots,r_1-1\}\times\cdots\times\{0,\ldots,r_{t-1}-1\}$. We also have

$$v(\beta_t^{r_t})=r_tv(\beta_t)=r_t\gamma_t>r_td_{t-1}\gamma_{t-1},$$

so Lemma 3.23 further yields

$$\begin{aligned}f_{t,0}=\operatorname{val}_z\big(z^{f_{t,0}}\varphi_1^{f_{t,1}}\cdots\varphi_{t-1}^{f_{t,t-1}}\big) &\geqslant v(\beta_t^{r_t})-r_{t-1}\gamma_{t-1}\\ &\geqslant r_td_{t-1}\gamma_{t-1}-r_{t-1}\gamma_{t-1}\\ &\geqslant 0.\end{aligned}$$

Inside $\mathbb{B}_t$, the following equalities hold:

$$\begin{aligned}\beta_t^{d_t}+c_{d_t-r_t}\pi_{t-1}^{f_t}\beta_t^{d_t-r_t}+\cdots+c_0\pi_{t-1}^{s_tf_t} &= (\beta_t^{r_t})^{s_t}+c_{d_t-r_t}\pi_{t-1}^{f_t}(\beta_t^{r_t})^{s_t-1}+\cdots+c_0\pi_{t-1}^{s_tf_t}\\ &= \big(\alpha_t\pi_{t-1}^{f_t}\big)^{s_t}+c_{d_t-r_t}\pi_{t-1}^{f_t}\big(\alpha_t\pi_{t-1}^{f_t}\big)^{s_t-1}+\cdots+c_0\pi_{t-1}^{s_tf_t}\\ &= \mu_t(\alpha_t)\,\pi_{t-1}^{s_tf_t}\\ &= 0,\end{aligned}$$

which shows that T_t is well defined.

Let $A\in\mathbb{K}[z][\varphi_1,\ldots,\varphi_t]$ be homogeneous of valuation σ, such that $\deg_{\varphi_i}A<d_i$ for $i=1,\ldots,t$, and let us write it in the form

$$A=A_{s_t-1}\varphi_t^{(s_t-1)r_t+k}+\cdots+A_1\varphi_t^{r_t+k}+A_0\varphi_t^k,$$

with A_j homogeneous in $\mathbb{K}[z][\varphi_1,\ldots,\varphi_{t-1}]$ and $k\in\{0,\ldots,r_t-1\}$. Then

$$\begin{aligned}\mathrm{T}_t(A) &= \mathrm{T}_{t-1}(A_{s_t-1})\,\beta_t^{(s_t-1)r_t+k}+\cdots+\mathrm{T}_{t-1}(A_1)\,\beta_t^{r_t+k}+\mathrm{T}_{t-1}(A_0)\,\beta_t^k\\ &= \big(\mathrm{T}_{t-1}(A_{s_t-1})\,\big(\alpha_t\pi_{t-1}^{f_t}\big)^{s_t-1}+\cdots+\mathrm{T}_{t-1}(A_1)\,\alpha_t\pi_{t-1}^{f_t}+\mathrm{T}_{t-1}(A_0)\big)\,\beta_t^k\end{aligned}$$

shows that it is straightforward to compute T_t recursively, and that T_t is a $\mathbb{K}((z))$-algebra isomorphism; an explicit recursive formula for T_t^{-1} will be given in the proof of Proposition 6.4 below.

Now assume that two elements $\pi_{t-1}^{\varepsilon_{t-1}}\beta_t^{\varepsilon_t}$ and $\pi_{t-1}^{\varepsilon'_{t-1}}\beta_t^{\varepsilon'_t}$, with $0\leqslant\varepsilon_t\leqslant\varepsilon'_t<r_t$, have the same valuation, that is

$$\frac{\varepsilon_{t-1}}{r_1\cdots r_{t-1}}+\varepsilon_t\frac{f_t}{r_1\cdots r_t}=\frac{\varepsilon'_{t-1}}{r_1\cdots r_{t-1}}+\varepsilon'_t\frac{f_t}{r_1\cdots r_t},$$

or, equivalently

$$(\varepsilon_t' - \varepsilon_t)\, f_t = (\varepsilon_{t-1} - \varepsilon_{t-1}')\, r_t.$$

Since $t \geqslant 2$, from Definition 3.1, $f_t \neq 0$, and since r_t and f_t are coprime, r_t divides $\varepsilon_t' - \varepsilon_t$, whence $\varepsilon_t' = \varepsilon_t$ and $\varepsilon_{t-1}' = \varepsilon_{t-1}$. In other words, any homogeneous element in $\mathbb{B}_t[z^{-1}]$ can be uniquely written $b\, \pi_{t-1}^{\varepsilon_{t-1}} \beta_t^{\varepsilon_t}$ with $b \in \mathbb{A}_{t-1}$, $\varepsilon_{t-1} \in \mathbb{Z}$ and $0 \leqslant \varepsilon_t < r_t$.

Let

$$1 = u_t r_t + v_t f_t$$

be the Bézout relation of r_t and f_t, with $|u_t| < f_t$ and $|v_t| < r_t$. The element

$$\pi_t := \pi_{t-1}^{u_t} \beta_t^{v_t} \in \mathbb{B}_t[z^{-1}]$$

has valuation

$$\frac{u_t}{r_1 \cdots r_{t-1}} + \frac{v_t f_t}{r_1 \cdots r_t} = \frac{u_t r_t + v_t f_t}{r_1 \cdots r_t} = \frac{1}{r_1 \cdots r_t}.$$

On the other hand we verify that

$$\pi_t^{r_t} = \pi_{t-1}^{u_t r_t} \beta_t^{v_t r_t} = \pi_{t-1}^{1 - v_t f_t} \left(\alpha_t\, \pi_{t-1}^{f_{t+1}}\right)^{v_{t+1}} = \alpha_t^{v_t}\, \pi_{t-1} \tag{6.5}$$

and

$$\pi_t^{f_t} = \pi_{t-1}^{u_t f_t} \beta_t^{v_t f_t} = \pi_{t-1}^{u_t f_t} \beta_t^{1 - u_t r_t} = \pi_{t-1}^{u_t f_t} \left(\alpha_t \pi_{t-1}^{f_t}\right)^{-u_t} \beta_t \;=\; \alpha_t^{-u_t} \beta_t. \tag{6.6}$$

Consequently, the valuation group of $\mathbb{B}_t[z^{-1}]$ is

$$\bar{\Gamma}_t = \frac{1}{r_1 \cdots r_t} \mathbb{Z},$$

and π_t is a uniformizing parameter. In addition we have

$$\pi_t^{R_t} = (\alpha_t^{v_t}\, \pi_{t-1})^{R_{t-1}} = \alpha_t^{v_t R_{t-1}}\, \rho_{t-1}\, z,$$

whence

$$\rho_t = \alpha_t^{v_t R_{t-1}}\, \rho_{t-1}. \tag{6.7}$$

In order to show that $(\mathbb{A}_i)_{i \leqslant t}$ is separable, we verify that

$$\begin{aligned}
\mathrm{T}_t\!\left(\mathrm{in}\!\left(\frac{\partial \Phi_t}{\partial \varphi_t}\right)\right) &= \mathrm{T}_t\!\left(\frac{\partial}{\partial \varphi_t}\big(\varphi_t^{r_t s_t} + c_{d_t - r_t}\, \pi_{t-1}^{f_t}\, \varphi_t^{r_t(s_t-1)} + \cdots + c_0\, z^{d_t f_t / r_t}\big)\right)\\
&= \mathrm{T}_t\big(\big(s_t\, \varphi_t^{r_t(s_t-1)} + (s_t - 1)\, c_{d_t - r_t}\, \pi_{t-1}^{f_t}\, \varphi_t^{r_t(s_t-2)} + \cdots + c_{r_t}\, z^{f_t(s_t-1)}\big)\, r_t\, \varphi_t^{r_t - 1}\big)\\
&= \big(s_t\, \alpha_t^{s_t-1}\, \pi_{t-1}^{f_t(s_t-1)} + (s_t-1)\, c_{d_t - r_t}\, \alpha_t^{s_t-2}\, \pi_{t-1}^{f_t(s_t-1)} + \cdots + c_{r_t}\, \pi_{t-1}^{f_t(s_t-1)}\big)\, r_t\, \beta_t^{r_t-1}\\
&= r_t\, \mu_t'(\alpha_t)\, \pi_{t-1}^{f_t(s_t-1)}\, \beta_t^{r_t-1}.
\end{aligned}$$

Let Θ_t and κ_t be such that $\mathrm{in}\!\left(\Theta_t \frac{\partial \Phi_t}{\partial \varphi_t}\right) = z^{\kappa_t}$ and let $\theta_t(\alpha_t)\, \pi_{t-1}^{\varepsilon_{t-1}} \beta_t^{\varepsilon_t} := \mathrm{T}_t(\mathrm{in}(\Theta_t))$ be such that $0 \leqslant \varepsilon_t < r_t$. Then we have

$$\begin{aligned}
z^{\kappa_t} &= \theta_t(\alpha_t)\, \pi_{t-1}^{\varepsilon_{t-1}} \beta_t^{\varepsilon_t}\, r_t\, \mu_t'(\alpha_t)\, \pi_{t-1}^{f_t(s_t-1)}\, \beta_t^{r_t-1}\\
&= r_t\, \theta_t(\alpha_t)\, \mu_t'(\alpha_t)\, \pi_{t-1}^{\varepsilon_{t-1} + f_t(s_t-1)}\, \beta_t^{\varepsilon_t + r_t - 1}.
\end{aligned}$$

It follows that $\varepsilon_t = 1$ and

$$\begin{aligned}
z^{\kappa_t} &= r_t\, \theta_t(\alpha_t)\, \mu_t'(\alpha_t)\, \alpha_t\, \pi_{t-1}^{\varepsilon_{t-1} + f_t s_t}\\
&= r_t\, \theta_t(\alpha_t)\, \mu_t'(\alpha_t)\, \alpha_t\, \rho_{t-1}^{\kappa_t},
\end{aligned}$$

whence

$$(\mu_t'(\alpha_t))^{-1} = r_t\, \alpha_t\, \theta_t(\alpha_t)\, \rho_{t-1}^{\kappa_t}. \tag{6.8}$$

From this inverse we easily recover the Bézout relation of μ_t' and μ_t so the tower $(\mathbb{A}_i)_{i\leqslant t}$ is effectively separable. □

6.4. Conversion costs

Before turning the above construction of the initial expansion into an algorithm, we study the costs of the conversions T_t and T_t^{-1}. We recall from section 1.2 that products in $\mathbb{A}_t$ take $\tilde{O}((s_1\cdots s_t)^{1+\epsilon})$ operations in $\mathbb{K}$.

PROPOSITION 6.4. *Assume that we are given an initial expansion of a contact tower, and let a be homogeneous of valuation $\sigma\geqslant 0$ in $\mathbb{K}[[z]][\varphi_1,\ldots,\varphi_t]/(\mathrm{in}(I_t))$. Recall that $R_t:=r_1\cdots r_t$. Then we can compute $\mathrm{T}_t(a)$ in the form $c\,\pi_t^{\sigma R_t}$ with $c\in\mathbb{A}_t$ using*

$$\tilde{O}(s_t\,(s_1\cdots s_{t-1})^{1+\epsilon}\log(\sigma R_t)\,t)$$

operations in $\mathbb{K}$. Conversely, given $c\,\pi_t^{\sigma R_t}$ with $c\in\mathbb{A}_t$, we can compute

$$\mathrm{T}_t^{-1}(c\,\pi_t^{\sigma R_t})\in\mathbb{K}((z))[\varphi_1,\ldots,\varphi_t]/(\mathrm{in}(I_t))$$

with the same cost bound. In addition, if $c\in\mathbb{A}_t$ has degree $<l$ in α_t and if r_t divides σR_t, then we can compute $\mathrm{T}_t^{-1}(c\,\pi_{t-1}^{\sigma R_{t-1}})$ using

$$\tilde{O}(l\,(s_1\cdots s_{t-1})^{1+\epsilon}\log(\sigma R_{t-1})\,t)$$

operations in $\mathbb{K}$.

Proof. Let A denote the canonical representative of a. There exists k such that $0\leqslant k\leqslant r_t-1$ and

$$A=\varphi_t^k\sum_{j=0}^{s_t-1}C_{r_tj+k}\,\varphi_t^{r_tj}.$$

For $j=0,\ldots,s_t-1$ we recursively compute $c_j\,\pi_{t-1}^{(\sigma-(r_tj+k)\gamma_t)R_{t-1}}:=\mathrm{T}_{t-1}(C_{r_tj+k})$ with $c_j\in\mathbb{A}_{t-1}$. Then we verify

$$\begin{aligned}
\mathrm{T}_t(A) &= \beta_t^k\sum_{j=0}^{s_t-1}\mathrm{T}_{t-1}(C_{r_tj+k})\,\beta_t^{r_tj}\\
&= \beta_t^k\sum_{j=0}^{s_t-1}c_j\,\pi_{t-1}^{(\sigma-(r_tj+k)\gamma_t)R_{t-1}}\,\beta_t^{r_tj}\\
&= \beta_t^k\sum_{j=0}^{s_t-1}c_j\,\pi_{t-1}^{(\sigma-(r_tj+k)\gamma_t)R_{t-1}}\,\alpha_t^j\,\pi_{t-1}^{f_tj} && \text{(using (6.3))}\\
&= \left(\sum_{j=0}^{s_t-1}c_j\,\alpha_t^j\right)\pi_{t-1}^{(\sigma-k\gamma_t)R_{t-1}}\,\beta_t^k && \text{(using (6.2))}\\
&= \left(\sum_{j=0}^{s_t-1}c_j\,\alpha_t^j\right)\alpha_t^{-v_t(\sigma-k\gamma_t)R_{t-1}+u_tk}\,\pi_t^{\sigma R_t}. && \text{(using (6.2), (6.5), and (6.6))}
\end{aligned}$$

Recall that the inverse of α_t is at our disposal and that the c_j belong to $\mathbb{A}_{t-1}$. So we need to compute $\alpha_t^{-v_t(\sigma-k\gamma_t)R_{t-1}+u_tk}$ using binary powering and fast tower arithmetic. Then, we multiply this quantity by $\sum_{j=0}^{s_t-1}c_j\,\alpha_t^j$. These products require

$$\tilde{O}(s_t\,(s_1\cdots s_{t-1})^{1+\epsilon}\,(\log(|v_t|\,(\sigma-k\,\gamma_t)\,R_{t-1}+|u_t|k)+1))$$

operations in $\mathbb{K}$. Since $|v_t| < r_t$ and $|u_t| < f_t = \gamma_t R_t$, we may simplify

$$\log(|v_t|\,(\sigma - k\gamma_t)\,R_{t-1} + |u_t| k) \leqslant \log((\sigma - k\gamma_t)\,R_t + k\gamma_t R_t) = \log(\sigma R_t).$$

Let $\mathsf{C}_t(\sigma)$ be the cost of evaluating T_t at any valuation $\leqslant \sigma$. We have shown that

$$\mathsf{C}_t(\sigma) = s_t\,\mathsf{C}_{t-1}(\sigma) + \tilde{O}(s_t\,(s_1 \cdots s_{t-1})^{1+\epsilon} \log(\sigma R_t)),$$

whence

$$\mathsf{C}_t(\sigma) = O(s_t\,(s_1 \cdots s_{t-1})^{1+\epsilon} \log(\sigma R_t)\,t).$$

The above formulas can be read in reverse order for performing a backward conversion T_t^{-1}, with a similar cost; note that $k = f_t^{-1}\,\sigma R_t \bmod r_t$.

The second assertion of the proposition corresponds to the special case where $k = 0$, which leads to the cost $l\,\mathsf{C}_{t-1}(\sigma)$ via the following formulas:

$$\begin{aligned}
\mathrm{T}_t^{-1}\left(\left(\sum_{j=0}^{l} c_j \alpha_t^j\right) \pi_{t-1}^{\sigma R_{t-1}}\right) &= \mathrm{T}_t^{-1}\left(\sum_{j=0}^{l} c_j\,\pi_{t-1}^{(\sigma - r_t j \gamma_t) R_{t-1}} \alpha_t^j\,\pi_{t-1}^{f_t j}\right)\\
&= \sum_{j=0}^{l} \mathrm{T}_t^{-1}\big(c_j\,\pi_{t-1}^{(\sigma - r_t j \gamma_t) R_{t-1}} \beta_t^j\big)\\
&= \sum_{j=0}^{l} \mathrm{T}_{t-1}^{-1}\big(c_j\,\pi_{t-1}^{(\sigma - r_t j \gamma_t) R_{t-1}}\big)\,\varphi_t^j. \qquad \square
\end{aligned}$$

6.5. Cost of initial expansions

Having shown how the conversions T_t and T_t^{-1} can be computed efficiently, let us now turn to the incremental construction of an initial expansion. We keep the same notation as in section 6.3.

PROPOSITION 6.5. *Given the initial forms* $\mathrm{in}(\Phi_1), \ldots, \mathrm{in}(\Phi_s)$ *of an effectively separable and regular contact tower, an initial expansion can be computed using*

$$\tilde{O}(s_t\,(s_1 \cdots s_{t-1})^{1+\epsilon} \log(d_t \gamma_t d)\,t^2)$$

operations in $\mathbb{K}$.

Proof. The case $t = 1$ has been detailed in section 6.1: it takes

$$\tilde{O}(s_1 \log(|u_1 v_1|)) = \tilde{O}(s_1 \log(f_1 r_1)) = \tilde{O}(s_1 \log(d_1 \gamma_1 r_1))$$

arithmetic operations in $\mathbb{K}$. By induction on t we may assume that the initial expansion has been computed up to height $t - 1$. We write

$$\mathrm{in}(\Phi_t) = \varphi_t^{d_t} + C_{d_t - 1}\,\varphi_t^{d_t - 1} + \cdots + C_0,$$

with the C_j homogeneous in $\mathbb{K}[z][\varphi_1, \ldots, \varphi_{t-1}]$. Since $\sigma = d_t \gamma_t$ and $R_t \leqslant d$, Proposition 6.4 allows us to compute $\mathrm{T}_{t-1}(C_{j r_t})$ for $j = 0, \ldots, s_t - 1$ using

$$\tilde{O}(s_t\,(s_1 \cdots s_{t-1})^{1+\epsilon} \log(d_t \gamma_t d)\,t) \tag{6.9}$$

operations in $\mathbb{K}$. This is sufficient to obtain μ_t.

If C_0' / z^{δ_0} stands for the normalized initial inverse of C_0, then we can compute $c_0'\,\pi_{t-1}^{e_0'} = T_{t-1}(C_0')$. Hence

$$z^{\delta_0} = T_{t-1}(C_0')\,T_{t-1}(C_0) = c_0'\,\pi_{t-1}^{e_0'} c_0\,\pi_{t-1}^{e_0} = c_0' c_0\,\rho_{t-1}^{\delta_0} z^{\delta_0},$$

so the computation of the inverse of $\mu_t(0)$ requires one evaluation of T_{t-1} at C_0' and $O(\log \delta_0) = O(\log(d_t \gamma_t))$ products in $\mathbb{A}_{t-1}$. The inverse of α_t is then obtained via (6.4) with $O(s_t)$ operations in $\mathbb{A}_{t-1}$. The cost of these two tasks does not exceed the bound (6.9).

The computation of the inverse u of μ_t' modulo μ_t then requires one evaluation of T_t at the initial inverse of $\frac{\partial \Phi_t}{\partial \varphi_t}$, then $O(\log \kappa_t) = O(\log(d_t \gamma_t))$ products in $\mathbb{A}_{t-1}$, and $O(1)$ products in $\mathbb{A}_t$, by using formula (6.8). The second cofactor of the Bézout relation of μ_t' and μ_t, namely $(1 - u\,\mu_t') / \mu_t$, requires $O(\mathsf{M}(s_t)) = \tilde{O}(s_t)$ further operations in $\mathbb{A}_{t-1}$.

By using formula (6.7), the computation of ρ_t from ρ_{t-1} takes

$$O(\log(|v_t|\, R_{t-1})) = O(\log R_t))$$

operations in $\mathbb{A}_t$, that is $\tilde{O}(s_t\,(s_1 \cdots s_{t-1})^{1+\epsilon} \log d)$ operations in $\mathbb{K}$. The sum of the costs for all levels of the tower is bounded by

$$\begin{aligned} & \tilde{O}\left(\sum_{i=1}^{t} s_i\,(s_1 \cdots s_{i-1})^{1+\epsilon} \log(d_1 \cdots d_i d_i \gamma_i)\, t\right) \\ = \; & \tilde{O}(s_t\,(s_1 \cdots s_{t-1})^{1+\epsilon} \log(d_t \gamma_t d)\, t^2). \end{aligned}$$ □

7. NEWTON FACTORIZATIONS

In this section we apply the lifting algorithms of section 4 in order to compute so-called *Newton factorizations* of a polynomial a that is clustered at $\mathbb{P}_t$ (Definition 3.9). These are partial factorizations that are related to the *contact Newton polygon* of a with respect to the current contact coordinates (Definition 7.7).

Until the end of the paper, contact towers will be effectively separable (Definition 5.1) and regular (Definition 6.1). Since we occasionally will have to manipulate multiple contact towers at multiple levels, it is convenient to

- regard an element $a \in \mathbb{P}_t$ as an element in any other $\mathbb{P}_i$ via the natural isomorphism $\Pi_i^{-1} \circ \Pi_t$;
- write

  $$\mathrm{in}(a; \mathbb{P}_i), v(a; \mathbb{P}_i), \text{ and } [a; \mathbb{P}_i]_{\alpha;\eta}$$

  for the initial form, the valuation, and the truncation of a, when regarded as an element in $\mathbb{P}_i$;
- given $A \in \mathbb{K}[[z]][\varphi_1, \ldots, \varphi_{i+1}]$, write

  $$\mathrm{in}(A; \mathbb{P}_i) \text{ and } v(A; \mathbb{P}_i)$$

  for the initial form and the valuation of $A(\varphi_1, \ldots, \varphi_{i+1})$ in $\mathbb{P}_i$.

7.1. Irreducible contact towers

Since we assumed from the outset that we have an algorithm or oracle for factoring univariate polynomials over $\mathbb{K}$, we are interested in factoring elements of $\mathbb{K}[[z]][x]$ into irreducible factors. There is a corresponding notion of irreducible contact towers and, thanks to our oracle, all contact towers that we will need for our main factoring algorithm can be forced to be of this type.

DEFINITION 7.1. *A homogeneous contact polynomial $a \in \mathbb{P}_i$ is said to be* ***initially reducible*** *if there exists a_1 and a_2 homogeneous in $\mathbb{P}_i \setminus \mathbb{P}_{i-1}$ such that $\operatorname{in}(a; \mathbb{P}_i) = \operatorname{in}(a_1 a_2; \mathbb{P}_i)$. A contact tower $(\mathbb{P}_i)_{i \leqslant t}$ is* ***irreducible*** *if $\operatorname{in}(\Phi_i; \mathbb{P}_{i-1})$ is initially irreducible for $i = 1, \ldots, t$.*

In view of the initial expansion $(\mathbb{A}_i)_{i \leqslant t}$ and $(\mathbb{B}_i)_{i \leqslant t}$ of a contact tower $(\mathbb{P}_i)_{i \leqslant t}$, we observe from Lemma 6.3 that $(\mathbb{P}_i)_{i \leqslant t}$ is irreducible if and only if $\mathbb{A}_t$ is a field. Equivalently, $(\mathbb{A}_i)_{i \leqslant t}$ is a tower of field extensions. In this case, any non-zero element in $\mathbb{P}_{t-1}$ admits a unique normalized initial inverse.

PROPOSITION 7.2. *A separable contact tower $(\mathbb{P}_i)_{i \leqslant t}$ is irreducible if and only if $\Pi_t(\varphi_{t+1}; \mathbb{P}_t)$ is irreducible.*

Proof. If $(\mathbb{P}_i)_{i \leqslant t}$ is reducible then their exists a smallest index i such that Φ_i admits an initial factorization regarded in $\mathbb{P}_{i-1}$. This initial factorization yields an initial Hensel context that can be lifted into a non trivial factorization of $\Pi_t(\varphi_{t+1}; \mathbb{P}_t)$ by Corollary 4.19.

Conversely assume that $(\mathbb{P}_i)_{i \leqslant t}$ is irreducible and let b be a factor of $\Pi_t(\varphi_{t+1}; \mathbb{P}_t)$. Then, $\operatorname{in}(b; \mathbb{P}_{i-1})$ initially divides $\operatorname{in}(\Phi_i; \mathbb{P}_{i-1})$, hence b cannot be a non trivial factor of $\Pi_t(\varphi_{t+1}; \mathbb{P}_t)$. □

The next lemmas are devoted to the complexity of initial inversions.

LEMMA 7.3. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be an effectively separable, regular, and irreducible contact tower, and assume that its initial expansion has been precomputed. Let $b \in \mathbb{P}_{t-1}$ be homogeneous and of valuation 0 in z. Then, b admits a unique normalized initial inverse, that can be computed with*

$$\tilde{O}(d_t (d_1 \cdots d_{t-1})^{1+\epsilon} \log(d_t \gamma_t)) = \tilde{O}(d^{1+\epsilon} \log(d_t \gamma_t))$$

operations in $\mathbb{K}$.

Proof. From Lemma 3.23 we know that $v(b) \leqslant d_t \gamma_t$. The computation of

$$\mathrm{T}_t(b) = c\, \pi_t^{v(b) R_t}$$

takes

$$\begin{aligned} \tilde{O}(s_t (s_1 \cdots s_{t-1})^{1+\epsilon} \log(v(b) R_t)\, t) &= \tilde{O}(s_t (s_1 \cdots s_{t-1})^{1+\epsilon} \log(d_t \gamma_t R_t)\, t) \\ &= \tilde{O}(d_t (d_1 \cdots d_{t-1})^{1+\epsilon} \log(d_t \gamma_t)) \end{aligned}$$

operations in $\mathbb{K}$ by Proposition 6.4. Then we compute $c^{-1} \rho_t^{-\lceil v(b) \rceil}$ in time

$$O(s_t (s_1 \cdots s_{t-1})^{1+\epsilon} \log(d_t \gamma_t)) = O(d^{1+\epsilon} \log(d_t \gamma_t)).$$

Proposition 6.4 allows us to obtain

$$u := \mathrm{T}_t^{-1}(c^{-1} \rho_t^{-\lceil v(b) \rceil} \pi_t^{R_t(\lceil v(b) \rceil - v(b))}) \in \mathbb{P}_t[z^{-1}]$$

with $\tilde{O}(d_t (d_1 \cdots d_{t-1})^{1+\epsilon})$ further operations. Since $v(u) \geqslant 0$, Lemma 3.23 implies $\operatorname{val}_z u \geqslant -d_t \gamma_t$. We verify that

$$\begin{aligned} \mathrm{T}_t(\operatorname{in}(u b)) &= c^{-1} \rho_t^{-\lceil v(b) \rceil} \pi_t^{R_t(\lceil v(b) \rceil - v(b))} c\, \pi_t^{R_t v(b)} \\ &= \rho_t^{-\lceil v(b) \rceil} \pi_t^{R_t \lceil v(b) \rceil} \\ &= z^{\lceil v(b) \rceil}, \end{aligned}$$

by using identity $\pi_t^{R_t} = \rho_t z$ stated in Definition 6.2. It follows that $\operatorname{in}(u b) = z^{\lceil v(b) \rceil}$. After multiplying or dividing u by a suitable power of z we obtain the normalized initial inverse of b. □

LEMMA 7.4. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an effectively separable, regular, and irreducible contact tower, and assume that its initial expansion has been precomputed. Let a be clustered at $\mathbb{P}_t$ of degree $l\geqslant 1$ in φ_{t+1} such that φ_{t+1} does not divide* $\operatorname{in}(a)$*, and let $b\in\mathbb{P}_t$ be homogeneous of degree $<l$ in φ_{t+1} and of valuation 0 in z. We can test whether b admits a normalized initial inverse modulo a or not, and if so compute this initial inverse with $\tilde{O}(l\,d^{1+\epsilon}\log(l\,\gamma_{t+1}))$ operations in $\mathbb{K}$.*

Proof. We increment the tower $(\mathbb{P}_i)_{i\leqslant t}$ with $\Phi_{t+1}=\operatorname{in}(a)$. The extended tower is not necessarily separable or irreducible because of its top level, but this does not prevent from building the corresponding incremented initial expansion with the difference that $\mathbb{A}_{t+1}$ is not a field extension of $\mathbb{A}_t$, that is not even necessarily separable. By Proposition 6.5 this "almost initial expansion" incurs $\tilde{O}(l\,d^{1+\epsilon}\log(l\,\gamma_{t+1}))$ operations in $\mathbb{K}$. The conclusion follows from Lemma 7.3: still writing $\mathrm{T}_{t+1}(b)=c\,\pi_{t+1}^{R_{t+1}v(b)}$, the required initial modular inverse exists if and only if c is invertible in $\mathbb{A}_{t+1}$. □

7.2. Contact factors

The following lemma asserts that a is clustered at any $\mathbb{P}_i$ for $i\leqslant t-1$ as soon as it is clustered at $\mathbb{P}_t$.

LEMMA 7.5. *Let $a\in\mathbb{P}_t$ be clustered as in Definition 3.9, of degree l in φ_{t+1}. Then, for $i=1,\ldots,t$, the polynomial a is clustered at $\mathbb{P}_i$, and we have $v(a;\mathbb{P}_i)=m_{i+1}\gamma_{i+1}$ where $m_{i+1}:=d_{i+1}\cdots d_t l$.*

Proof. Note that $\Pi_t(a)$ is monic in x of degree $d\,m_{t+1}$. Therefore a is monic in φ_{i+1} of degree m_{i+1} when regarded in $\mathbb{P}_i$, for $i=0,\ldots,t$. The rest of the proof is done by induction on i from t down to 1. The case $i=t$ corresponds to the hypothesis of the lemma. Now let us assume that $v(a;\mathbb{P}_i)=m_{i+1}\gamma_{i+1}$ holds for some $i\leqslant t$, and consider the contact representation

$$a=\varphi_{i+1}^{m_{i+1}}+c_{m_{i+1}-1}\varphi_{i+1}^{m_{i+1}-1}+\cdots+c_0$$

in $\mathbb{P}_i$, with

$$v(c_j;\mathbb{P}_{i-1})=v(c_j;\mathbb{P}_i)\geqslant(m_{i+1}-j)\,\gamma_{i+1}$$

for $j=0,\ldots,m_{i+1}-1$. It follows that

$$\begin{aligned} v(c_j\Phi_i^j;\mathbb{P}_{i-1}) &\geqslant (m_{i+1}-j)\,\gamma_{i+1}+j\,d_i\gamma_i\\ &\geqslant (m_{i+1}-j)\,d_i\gamma_i+j\,d_i\gamma_i\\ &= d_i m_{i+1}\gamma_i,\end{aligned}$$

where the second inequality is strict for $j<m_{i+1}$. Consequently, $v(a;\mathbb{P}_{i-1})=m_i\gamma_i$. □

DEFINITION 7.6. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an effectively separable, regular, and irreducible contact tower and let $a\in\mathbb{P}_t$ be clustered at $(\mathbb{P}_i)_{i\leqslant t}$. An **irreducible contact factorization** of a at precision $O(z^\tau)$ is a sequence of pairs $(a^{(j)},(\mathbb{P}_i^{(j)})_{i\leqslant t^{(j)}})$ modulo $O(z^\tau)$ for $j=1,\ldots,n$, such that:*

- *$(\mathbb{P}_i^{(j)})_{i\leqslant t^{(j)}}$ is an effectively separable, regular, and irreducible contact tower for $j=1,\ldots,n$;*
- *$t_j\geqslant t$ and $(\mathbb{P}_i^{(j)})_{i\leqslant t}=(\mathbb{P}_i)_{i\leqslant t}$ for $j=1,\ldots,n$;*
- *$a^{(j)}\in\mathbb{P}_{t^{(j)}}$ is a power of the last contact coordinate $\varphi_{t^{(j)}+1}$ of $\mathbb{P}_{t^{(j)}}$ for $j=1,\ldots,n$;*
- *$a=a^{(1)}\cdots a^{(n)}+O(z^\tau)$ (this equality can be regarded equivalently in any $\mathbb{P}_i$ for $i\leqslant t$).*

7.3. Contact Newton polygons

Consider a contact polynomial

$$a=c_l\varphi_{t+1}^l+c_{l-1}\varphi_{t+1}^{l-1}+\cdots+c_0\in\mathbb{P}_t,$$

with $c_i \in \mathbb{P}_{t-1}$ for $i=0,\ldots,l$ and $c_l \neq 0$. The *Newton polygon* $\mathcal{N} \subseteq \mathbb{R} \times (\mathbb{R} \cup \{+\infty\})$ of a is the lower border of the convex hull of the set of pairs (i,j) with $0 \leqslant i \leqslant l$ and $j \geqslant v(c_i)$. More precisely, $\mathcal{N}$ is a broken line with vertices $(i_0,j_0),\ldots,(i_r,j_r)$, where

- $0 = i_0 < \cdots < i_r = l$,
- $j_k = v(c_{i_k})$ for $k=0,\ldots,r$,
- for all $i=0,\ldots,l$ such that $c_i \neq 0$, the point $(i,v(c_i))$ is on or above the Newton polygon.

Any $k=1,\ldots,r$ determines an edge $\mathcal{E}_k$ between the vertices (i_{k-1},j_{k-1}) and (i_k,j_k), of slope $(j_k - j_{k-1})\,/\,(i_k - i_{k-1})$. The set of points above the Newton polygon is convex. When $c_0 = 0$ we have $j_0 = +\infty$, so the slope of the first edge is $-\infty$. In order to establish the usual relationship between $\mathcal{N}$ and the Newton polygons of the factors of a, we introduce the following definition.

DEFINITION 7.7. *With the above notation, the Newton polygon $(i_0,j_0),\ldots,(i_r,j_r)$ of $a \in \mathbb{P}_t$ is said to be **effectively regular** when the elements c_{i_k} are initially invertible in $\mathbb{P}_t$, and we are given the normalized initial inverses w_k / z^{κ_k} of c_{i_k} for $k=0,\ldots,r$. If $c_0=0$ then we set $w_k := 0$ by convention.*

The following lemma extends a special case of a classical result about Minkowski sums of polytopes due to Ostrowski [63] (translated in [65], and revisited later in [64]). In our variant we need to take care of "carries" involved by the contact arithmetic.

LEMMA 7.8. *Let $a = \sum_{k=0}^{l_a} c_k^a \, \varphi_{t+1}^k$ and $b = \sum_{k=0}^{l_b} c_k^b \, \varphi_{t+1}^k$ be contact polynomials in $\mathbb{P}_t$. Their respective Newton polygons $\mathcal{N}_a = ((i_0^a, j_0^a),\ldots,(i_{r_a}^a, j_{r_a}^a))$ and $\mathcal{N}_b = ((i_0^b, j_0^b),\ldots,(i_{r_b}^b, j_{r_b}^b))$ are assumed to be regular, the slopes of $\mathcal{N}_a$ are strictly smaller than the ones of $\mathcal{N}_b$, and all slopes are $\leqslant -\gamma_{t+1}$. If $c_0^a \neq 0$, $c_{l_a}^a = 1$, $c_0^b \neq 0$, and $c_{l_b}^b = 1$, then the Newton polygon $\mathcal{N}_{ab}$ of $a\,b$ equals*

$$\mathcal{N}_{ab} = ((i_0^a, j_0^a) + (i_0^b, j_0^b), \ldots, (i_{r_a}^a, j_{r_a}^a) + (i_0^b, j_0^b), \ldots, (i_{r_a}^a, j_{r_a}^a) + (i_{r_b}^b, j_{r_b}^b)).$$

In addition, the contact polynomial

$$a\,b = \sum_{k=0}^{l_a + l_b} c_k^{ab} \, \varphi_{t+1}^k$$

satisfies $\operatorname{in}(c^{ab}_{i_k^a + i_0^b}) = \operatorname{in}(c^a_{i_k^a} c^b_{i_0^b})$ *for* $k=0,\ldots,r_a$ *and* $\operatorname{in}\left(c^{ab}_{i_{r_a}^a + i_k^b}\right) = \operatorname{in}\left(c^a_{i_{r_a}^a} \, c^b_{i_k^b}\right)$ *for* $k=0,\ldots,r_b$.

Proof. First of all, note that the hypothesis on the slopes guarantees that the region of the plane above the Newton polygon

$$\mathcal{P} := ((i_0^a, j_0^a) + (i_0^b, j_0^b), \ldots, (i_{r_a}^a, j_{r_a}^a) + (i_0^b, j_0^b), \ldots, (i_{r_a}^a, j_{r_a}^a) + (i_{r_b}^b, j_{r_b}^b))$$

is actually convex.

Let (i^a, j^a) be a point above $\mathcal{N}_a$. For all $k=1,\ldots,r_a$, we have

$$j^a - j_{k-1}^a \geqslant \frac{j_k^a - j_{k-1}^a}{i_k^a - i_{k-1}^a} (i^a - i_{k-1}^a). \tag{7.1}$$

Similarly, for any point (i^b, j^b) above $\mathcal{N}_b$ and for all $k=1,\ldots,r_b$ we have

$$j^b - j_{k-1}^b \geqslant \frac{j_k^b - j_{k-1}^b}{i_k^b - i_{k-1}^b} (i^b - i_{k-1}^b). \tag{7.2}$$

Since the slope of the edge $((i_{k-1}^a, j_{k-1}^a), (i_k^a, j_k^a))$ is smaller than the slope of $((i_0^b, j_0^b), (i_1^b, j_1^b))$, for $k=1,\ldots,r_a$, we obtain

$$j^b - j_0^b \geqslant \frac{j_1^b - j_0^b}{i_1^b - i_0^b} (i^b - i_0^b) \geqslant \frac{j_k^a - j_{k-1}^a}{i_k^a - i_{k-1}^a} (i^b - i_0^b), \text{ since } i^b \geqslant i_0^b.$$

Combining the latter inequality with (7.1) leads to

$$j^a + j^b - j^a_{k-1} - j^b_0 \geqslant \frac{(j^a_k + j^b_0) - (j^a_{k-1} + j^b_0)}{(i^a_k + i^b_0) - (i^a_{k-1} + i^b_0)} (i^a + i^b - i^a_{k-1} - i^b_0),$$

which means that $(i^a + i^b, j^a + j^b)$ is above the line spanned by $(i^a_{k-1}, j^a_{k-1}) + (i^b_0, j^b_0)$ and $(i^a_k, j^a_k) + (i^b_0, j^b_0)$. Similarly, since $i^a \leqslant i^a_{r_a}$ and since the slope of the edge $((i^a_{r_a-1}, j^a_{r_a-1}), (i^a_{r_a}, j^a_{r_a}))$ is smaller than the one of $((i^b_{k-1}, j^b_{k-1}), (i^b_k, j^b_k))$, we obtain

$$j^a - j^a_{r_a} \geqslant \frac{j^a_{r_a} - j^a_{r_a-1}}{i^a_{r_a} - i^a_{r_a-1}} (i^a - i^a_{r_a}) \geqslant \frac{j^b_k - j^b_{k-1}}{i^b_k - i^b_{k-1}} (i^a - i^a_{r_a}),$$

for $k = 1, \ldots, r_b$. In combination with (7.2), this yields

$$j^a + j^b - j^a_{r_a} - j^b_{k-1} \geqslant \frac{(j^b_k + j^a_{r_a}) - (j^b_{k-1} + j^a_{r_a})}{(i^b_k + i^a_{r_a}) - (i^b_{k-1} + i^a_{r_a})} (i^a + i^b - i^a_{r_a} - i^b_{k-1}),$$

so $(i^a + i^b, j^a + j^b)$ is above the line spanned by $(i^a_{r_a}, j^a_{r_a}) + (i^b_{k-1}, j^b_{k-1})$ and $(i^a_{r_a}, j^a_{r_a}) + (i^b_k, j^b_k)$. So far, we have proved that $(i^a + i^b, v(c^a_{i^a}) + v(c^b_{i^a}))$ is above $\mathcal{P}$, for all $i_a = 0, \ldots, r_a$ and $i_b = 0, \ldots, r_b$.

Since $c^a_{i^a_k}$ and $c^b_{i^b_0}$ are invertible, for k in $i^a_0, \ldots, i^a_{r_a} - 1$, Lemma 4.3 yields

$$v(c^a_{i^a_k} c^b_{i^b_0}) = v(c^a_{i^a_k}) + v(c^b_{i^b_0}).$$

Now consider the contact polynomial $c^a_{i^a_k} c^b_{i^b_0} = e_0 + e_1 \varphi_{t+1} \in \mathbb{P}_t$ with $e_0, e_1 \in \mathbb{P}_{t-1}$, so we have $v(c^a_{i^a_k} c^b_{i^b_0}) = v(e_0)$ and $v(e_1) \geqslant v(c^a_{i^a_k} c^b_{i^b_0}) - \gamma_{t+1}$. Because the slopes of $\mathcal{P}$ are $< -\gamma_{t+1}$, the point $(i^a_k + 1, v(e_1))$ is strictly above $\mathcal{P}$.

Let us fix $-\gamma'_{t+1} < -\gamma_{t+1}$ to a value different from the slopes of $\mathcal{N}_a$ and $\mathcal{N}_b$. Let us assume first that $-\gamma'_{t+1}$ is less than the smallest slope of $\mathcal{N}_b$. If $-\gamma'_{t+1}$ is less than the largest slope of $\mathcal{N}_a$ we let k to be the largest integer such that $-\gamma'_{t+1}$ is less than the slope of $((i^a_{k-1}, j^a_{k-1}), (i^a_k, j^a_k))$, otherwise we let $k = r_a$. Let v' be the corresponding valuation induced in $\mathbb{P}_t$: $v'(\varphi_i) = \gamma_i$ for $i \leqslant t$ and $v'(\varphi_{t+1}) = \gamma'_{t+1}$; we write in$'$ for the corresponding initial part. We verify that

$$\begin{aligned} v'(a) &= v(c^a_{i^a_k}) + \gamma'_{t+1} i^a_k \quad \text{and} \quad \mathrm{in}'(a) = (\mathrm{in}(c^a_{i^a_k}))\, \varphi_{t+1}^{i^a_k}, \\ v'(b) &= v(c^b_{i^b_0}) + \gamma'_{t+1} i^b_0 \quad \text{and} \quad \mathrm{in}'(b) = (\mathrm{in}(c^b_{i^b_0}))\, \varphi_{t+1}^{i^b_0}, \\ v'(a b) &= v(c^a_{i^a_k}) + v(c^b_{i^b_0}) + \gamma'_{t+1} (i^a_k + i^b_0) \quad \text{and} \quad \mathrm{in}'(a b) = \mathrm{in}(c^a_{i^a_k} c^b_{i^b_0})\, \varphi_{t+1}^{i^a_k + i^b_0}. \end{aligned}$$

Consequently, Lemma 4.3 implies

$$(i^a_k + i^b_0, v(c^a_{i^a_k}) + v(c^b_{i^b_0})) = (i^a_k + i^b_0, j^a_k + j^b_0)$$

belongs to the Newton polygon of $a b$, and $\mathrm{in}\big(c^{ab}_{i^a_k + i^b_0}\big) = \mathrm{in}(c^a_{i^a_k} c^b_{i^b_0})$.

Assume now that $-\gamma'_{t+1}$ is greater than the smallest slope of $\mathcal{N}_b$ then we let k to be the first integer such that $-\gamma'_{t+1}$ is greater than the slope of $((i^b_{k-1}, j^b_{k-1}), (i^b_k, j^b_k))$. Using a similar argument as above, we may prove that

$$\big(i^a_{r_a} + i^b_k, v(c^a_{r_a}) + v\big(c^b_{i^b_k}\big)\big) = (i^a_{r_a} + i^b_k, j^a_{r_a} + j^b_k) \tag{7.3}$$

belongs to the Newton polygon of $a b$, and that $\mathrm{in}\big(c^{ab}_{i^a_{r_a} + i^b_k}\big) = \mathrm{in}\big(c^a_{r_a} c^b_{i^b_k}\big)$. This concludes the proof. □

LEMMA 7.9. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an effectively separable, regular, and irreducible contact tower and let*

$$a = c_l\,\varphi_{t+1}^l + c_{l-1}\,\varphi_{t+1}^{l-1} + \cdots + c_0$$

be a contact polynomial with the $c_i \in \mathbb{P}_{t-1}$ and truncated modulo $O(z^\tau)$ with $\tau > d_t\gamma_t$. Then, the effectively regular Newton polygon of a can be computed using

$$\tilde{O}(l\,d^{1+\epsilon}\,\tau)$$

operations in $\mathbb{K}$.

Proof. We first compute the initial expansion of $\mathbb{P}_t$, that contributes to $\tilde{O}(d^{1+\epsilon}\log(d_t\gamma_t))$ from Proposition 6.5. Set i in $0,\ldots,l$. In order to compute the valuation of c_i we run over all its homogeneous components in $\mathbb{P}_{t-1}$ in increasing valuation order. Up to precision τ, the number of such components is $\leqslant \tau r_1 \cdots r_t$. Each such component has $\leqslant s_1 \cdots s_t$ terms. Overall the number of zero tests in $\mathbb{K}$ is $O(l\,d\,\tau)$.

From the valuations of the c_i, the computation of the Newton polygon $\mathcal{N}$ does not involve arithmetic operations in $\mathbb{K}$, but $\tilde{O}(l\log(\tau r_1 \cdots r_t))$ bit operations (with the usual "divide and conquer" algorithm). Finally, for a vertex of abscissa i of the Newton polygon we need to compute the initial inverse of c_i. For this purpose we extract $b := \operatorname{in}(c_i; \mathbb{P}_{t-1}) / z^{\operatorname{val}_z c_i}$ and appeal to Lemma 7.3. □

7.4. Distinct-slope factorization

Let $a \in \mathbb{P}_t$ be clustered at $(\mathbb{P}_i)_{i\leqslant t}$ given with its effectively regular Newton polygon $\mathcal{N}$. We are to show that each edge of $\mathcal{N}$ gives rise to a factor of a.

Algorithm 7.1

Input. An effectively separable, regular, and irreducible contact tower $(\mathbb{P}_i)_{i\leqslant t}$ along with its initial expansion; a contact polynomial $a = \varphi_{t+1}^l + c_{l-1}\,\varphi_{t+1}^{l-1} + \cdots + c_0 \in \mathbb{P}_t$ given modulo $O(z^\tau)$ with $\tau > d_t\gamma_t$ and clustered at $\mathbb{P}_t$; the effectively regular Newton polygon of a (whose slopes are all $< -d_t\gamma_t$).

Let $0 = i_0 < i_1 < \cdots < i_{r-1} < i_r = l$ be the abscissas of the vertices of the Newton polygon, as in Definition 7.7. The normalized initial inverse w_k / z^{κ_k} of c_{i_k} is part of the input for $k = 0,\ldots,r$.

Output. Contact polynomials $a_1,\ldots,a_r$ modulo $O(z^\tau)$, clustered at $\mathbb{P}_t$, such that $a = a_1 \cdots a_r + O(z^\tau)$, $c_{i_j} a_j$ admits a single Newton polynomial that coincides with the j-th one of a, for $j = 1,\ldots,r$.

1. If $r = 1$ then return a.
2. Let $h := \lceil r/2 \rceil$ and set $\gamma_{t+1} := -\sigma_h$, where σ_h is the slope of the edge between abscissas i_{h-1} and i_h.
3. Compute $a_1 := \operatorname{in}(a\,w_h / z^{\kappa_h}; \mathbb{P}_t)$, $a_2 := [c_{i_h}]_{v(c_{i_h})}$, $u_1 := w_h$, $\delta_1 := \kappa_h$.
4. Via Corollary 4.14 called with precision $O(z^{\tau+\delta_1})$, compute contact polynomials $\hat{a}_1$ and $\hat{a}_2$ in $\mathbb{P}_t$ modulo $O(z^\tau)$ such that $a = \hat{a}_1 \hat{a}_2 + O(z^\tau)$, $\hat{a}_1$ is clustered at $\mathbb{P}_t$, $\operatorname{in}(\hat{a}_1; \mathbb{P}_t) = \operatorname{in}(a_1; \mathbb{P}_t)$, and $\operatorname{in}(\hat{a}_2; \mathbb{P}_t) = \operatorname{in}(a_2; \mathbb{P}_t)$.
5. Recursively call the algorithm with input $\hat{a}_1$: the vertices of the Newton polygon of $\hat{a}_1$ are $(i_0, j_0 - j_h), (i_1, j_1 - j_h), \ldots, (i_h, 0)$ and the normalized initial inverses are $\operatorname{in}(c_{i_h} w_0; \mathbb{P}_{t-1}), \ldots, \operatorname{in}(c_{i_h} w_{i_{h-1}}; \mathbb{P}_{t-1})$ rescaled by suitable powers of z.

6. Recursively call the algorithm with input $\hat{a}_2$: the vertices of the Newton polygon of $\hat{a}_2$ are $(0, j_h), (i_{h+1} - i_h, j_{h+1}), \ldots, (i_r - i_h, j_r)$, with normalized initial inverses $w_{i_h}, \ldots, w_{i_{r-1}}$.
7. Return the union of the sets of factors returned by the above recursive calls.

PROPOSITION 7.10. *Algorithm 7.1 is correct and takes*

$$O(\mathsf{M}(l\,d\,\tau)\log(l\,d\,\tau)\log r) = \tilde{O}(l\,d\,\tau)$$

operations in $\mathbb{K}$.

Proof. If $r = 1$ then the algorithm is clearly correct. From now assume $r \geqslant 2$. By definition of the effectively regular Newton polygon, the value of $\operatorname{in}(a; \mathbb{P}_t)$ occurring in step 3 writes as

$$\operatorname{in}(a; \mathbb{P}_t) = [c_{i_h}; \mathbb{P}_{t-1}]_{v(a) - i_h \gamma_{t+1}} \varphi_{t+1}^{i_h} + \cdots + [c_0; \mathbb{P}_{t-1}]_{v(a)}.$$

From $\operatorname{in}(w_h c_{i_h} / z^{\kappa_h}) = 1$ and $v(c_j) \geqslant v(a) + (i_h - j)\,\gamma_{t+1} \geqslant v(c_{i_h}) + \gamma_{t+1}$ for $j < i_h$, Lemma 4.3 yields

$$v(w_h c_j) = v(w_h) + v(c_j) = \kappa_h - v(c_{i_h}) + v(c_j) \geqslant \kappa_h + \gamma_{t+1}.$$

Then Lemma 3.23 implies $\operatorname{val}_z(w_h c_j) \geqslant v(w_h c_j) - d_t \gamma_t \geqslant \kappa_h$, hence step 3 computes an initial Weierstraß context for a.

Let a_1^∞ and a_2^∞ be as in Corollary 4.14: $a = a_1^\infty a_2^\infty$, $\hat{a}_1 = a_1^\infty + O(z^\tau)$, and $\hat{a}_2 = a_2^\infty + O(z^\tau)$ hold in step 4. From Lemma 7.8 we know that the Newton polygon of a is the Minkowski sum of those of a_1^∞ and a_2^∞ (up to the occasional vertex at infinity of a_1^∞ and a). Since the vertices of the Newton polygon of a have valuation in $z < \tau$ (or infinity), so are those of the polygons of a_1^∞ and a_2^∞.

Let $k \in \{0, 1\}$ be the first index such that $c_{i_k} \neq 0$. From $\operatorname{val}_z c_{i_k} < \tau$, Lemma 3.23 implies $v(c_{i_k}; \mathbb{P}_{t-1}) < \tau + d_t \gamma_t$, whence

$$\operatorname{val}_z(w_h c_{i_k} / z^{\kappa_h}) \leqslant v(w_h c_{i_k} / z^{\kappa_h}; \mathbb{P}_t) < \tau + d_t \gamma_t - v(c_{i_h}; \mathbb{P}_{t-1}) \leqslant \tau. \tag{7.4}$$

It follows that the Newton polygon of $\hat{a}_i$ coincides with the one of a_i^∞ for $i = 1, 2$, and that these polygons are effectively regular, with the initial inverses as in steps 4 and 5.

In step 3, for $j = 0, \ldots, h - 1$, we compute $\operatorname{in}(c_{i_j} w_h / z^{\kappa_h}; \mathbb{P}_{t-1})$ with $O(\mathsf{M}(d\,\tau)\log d)$ operations in $\mathbb{K}$ thanks to Proposition 3.20. The same cost applies to the computation of $\operatorname{in}(c_{i_h} w_j; \mathbb{P}_{t-1})$ in step 5. By Corollary 4.14, and since $\delta_1 \leqslant v(c_{i_h}) + d\,\gamma_t \leqslant 2\,\tau$, the cost of the lifting in step 4 is

$$O(\mathsf{M}(l\,d\,\tau)\log(l\,d\,\tau)).$$

The depth of the recursive calls is $O(\log r)$, so the complexity bound follows from a standard induction. □

DEFINITION 7.11. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be a contact tower, and let a be a contact polynomial clustered at $\mathbb{P}_t$. The* ***distinct-slope factorization*** *of a is made of contact polynomials $a_1, \ldots, a_r$ clustered at $\mathbb{P}_t$ such that $a = a_1 \cdots a_r$, the Newton polygon of a_i admits a single edge for $i = 1, \ldots, r$ and the sequence of the slopes of these edges is strictly increasing.*

COROLLARY 7.12. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be an effectively separable, regular, and irreducible contact tower, and let a be a contact polynomial clustered at $\mathbb{P}_t$. Then, there exists a unique distinct-slope factorization of a.*

Proof. Since the tower is irreducible, the Newton polygon of a can be made effectively regular, thanks to Lemma 7.3. Consequently the existence of the distinct-slope factorization of a follows from Proposition 7.10.

Given a distinct-slope factorization $a_1, \ldots, a_r$, by Lemma 7.8 the slopes of the a_i are those of the Newton polygon of a. If γ_{t+1} is set to the opposite of the slope of a_i then $\mathrm{in}(a_i; \mathbb{P}_t)$ is a Newton polynomial of a of slope $-\gamma_{t+1}$ (up to a power of φ_{t+1} and up to a factor in $\mathbb{P}_{t-1}$). The uniqueness of the a_i thus follows from the uniqueness of the lifting of the distinct slope factors. □

7.5. Equal-slope factorization

Consider the factorization of an element $a \in \mathbb{P}_t$ whose Newton polygon has a single edge with finite slope. We have already seen that an initial factorization into pairwise coprime factors of $\mathrm{in}(a; \mathbb{P}_t)$ lifts into a factorization of a. We now explain how to obtain this initial factorization. The contact polynomial a is assumed to be truncated modulo $O(z^\tau)$ with $\tau > d_t \gamma_t$.

We assume that the initial expansion of the contact tower has already been computed. We extend the map T_t (defined in Lemma 6.3) as follows:

$$\begin{array}{rrcl} \tilde{\mathrm{T}}_t\colon & \mathbb{K}((z))[\varphi_1, \ldots, \varphi_{t+1}] / (\mathrm{in}(I_t; \mathbb{P}_t)) & \longrightarrow & \mathbb{B}_i[z^{-1}, y_{t+1}] \\ & \varphi_i & \longmapsto & \beta_i = \mathrm{T}_t(\varphi_i) \text{ for } i \leqslant t \\ & \varphi_{t+1} & \longmapsto & y_{t+1}. \end{array}$$

We set γ_{t+1} to be the opposite of the unique slope of the Newton polygon of

$$a = \varphi_{t+1}^l + c_{l-1} \varphi_{t+1}^{l-1} + \cdots + c_0.$$

Note that $c_0 \neq 0$. Let

$$\frac{f_{t+1}}{r_{t+1}} := \frac{v(c_0; \mathbb{P}_{t-1}) \, R_t}{l} = R_t \gamma_{t+1} \tag{7.5}$$

with f_{t+1} prime to $r_{t+1} \geqslant 1$ and let $\ell := l / r_{t+1}$. Note that $v(c_0) \, R_t$ is an integer. In the next subsection we shall see that the notation is consistent since r_{t+1} will be the "next ramification index".

We compute $\varsigma_i \pi_t^{f_{t+1} i} := \mathrm{T}_t(c_{r_{t+1} i})$ with $\varsigma_i \in \mathbb{A}_t$, for $i = 0, \ldots, \ell - 1$, and construct

$$\chi(x_{t+1}) := x_{t+1}^\ell + \varsigma_{\ell-1} x_{t+1}^{\ell-1} + \cdots + \varsigma_0 \in \mathbb{A}_t[x_{t+1}],$$

so we have

$$\tilde{\mathrm{T}}_t(\mathrm{in}(a; \mathbb{P}_t)) = \pi_t^{f_{t+1} \ell} \chi\big(y_{t+1} / \pi_t^{f_{t+1}}\big). \tag{7.6}$$

We factor

$$\chi = \chi_1 \cdots \chi_s,$$

where each χ_j is a power of a monic irreducible factor and the χ_j are pairwise coprime. For $j = 1, \ldots, s$, we let $\ell_j := \deg \chi_j$ and

$$a_j := \tilde{\mathrm{T}}_t^{-1}\big(\pi_t^{f_{t+1} \ell_j} \chi_j\big(y_{t+1} / \pi_t^{f_{t+1}}\big)\big). \tag{7.7}$$

We compute a_j using

$$a_j = \varphi_{t+1}^{r_{t+1} \ell_j} + \mathrm{T}_t^{-1}\big(\chi_{j, \ell_j - 1} \pi_t^{f_{t+1} (\ell_j - 1)}\big) \, \varphi_{t+1}^{r_{t+1} (\ell_j - 1)} + \cdots + \mathrm{T}_t^{-1}(\chi_{j,0}),$$

where $\chi_{j,k}$ stands for the coefficient of x_{t+1}^k in χ_j.

LEMMA 7.13. *For $j=1,\ldots,s$, the polynomial a_j defined in (7.7) is homogeneous, monic in φ_{t+1}, and of valuation $f_{t+1}\,\ell_j/R_t=\ell_j\,v(a)/\ell$. In addition, we have*

$$\operatorname{in}(a;\mathbb{P}_t)=\operatorname{in}(a_1\cdots a_s;\mathbb{P}_t).$$

Proof. The first assertion is clear by construction. The second assertion follows from the fact that T_t is a ring isomorphism that preserves the valuation. □

We next compute the modular inverses

$$\xi_j:=\left(\frac{\chi}{\chi_j}\right)^{-1}\operatorname{mod}\chi_j$$

for $j=1,\ldots,s$. Let us write the expansion of ξ_j as follows

$$\xi_j(x_{t+1})=:\xi_{j,\ell_j-1}\,x_{t+1}^{\ell_j-1}+\cdots+\xi_{j,0}\in\mathbb{A}_t[x_{t+1}]_{<\ell_j},$$

let $\hat{\ell}\geqslant 0$ be the smallest integer such that $f_{t+1}\,\ell+\hat{\ell}$ is a multiple of R_t and set

$$\check{\ell}:=\frac{f_{t+1}\,\ell+\hat{\ell}}{R_t}.$$

From (7.5), we deduce

$$f_{t+1}\,\ell+\hat{\ell}\leqslant v(c_0)\,R_t+R_t\leqslant(\tau+d_t\,\gamma_t+1)\,R_t\leqslant(2\,\tau+1)\,R_t.$$

Recall from Definition 6.2 that $\pi_t^{R_t}=\rho_t\,z$. We further set

$$\begin{aligned}u_j\;:=\;&\mathrm{T}_t^{-1}\Big(\rho_t^{-\check{\ell}}\,\xi_{j,\ell_{j-1}}\,\pi_t^{f_{t+1}+\hat{\ell}}\Big)\,\varphi_{t+1}^{r_{t+1}(\ell_j-1)}+\cdots\\&+\mathrm{T}_t^{-1}\Big(\rho_t^{-\check{\ell}}\,\xi_{j,1}\,\pi_t^{f_{t+1}(\ell_j-1)+\hat{\ell}}\Big)\,\varphi_{t+1}^{r_{t+1}}+\mathrm{T}_t^{-1}\Big(\rho_t^{-\check{\ell}}\,\xi_{j,0}\,\pi_t^{f_{t+1}\ell_j+\hat{\ell}}\Big)\end{aligned}\tag{7.8}$$

so we have

$$\begin{aligned}\tilde{\mathrm{T}}_t(u_j)\;&=\;\rho_t^{-\check{\ell}}\,\xi_{j,\ell_{j-1}}\,\pi_t^{f_{t+1}+\hat{\ell}}\,y_{t+1}^{r_{t+1}(\ell_j-1)}+\cdots+\rho_t^{-\check{\ell}}\,\xi_{j,0}\,\pi_t^{f_{t+1}\ell_j+\hat{\ell}}\\&=\;\rho_t^{-\check{\ell}}\,\pi_t^{f_{t+1}\ell_j+\hat{\ell}}\,\xi_j\!\left(\frac{y_{t+1}^{r_{t+1}}}{\pi_t^{f_{t+1}}}\right).\end{aligned}$$

From

$$\xi_j(x_{t+1})\,\frac{\chi(x_{t+1})}{\chi_j(x_{t+1})}=1\operatorname{mod}\chi_j(x_{t+1})$$

we deduce that

$$\begin{aligned}&\tilde{\mathrm{T}}_t\!\left(\operatorname{in}\!\left(u_j\,\frac{a}{a_j}\operatorname{rem}_{\varphi_{t+1}}a_j;\mathbb{P}_t\right)\right)\\=\;&\tilde{\mathrm{T}}_t(u_j)\,\frac{\tilde{\mathrm{T}}_t(a)}{\tilde{\mathrm{T}}_t(a_j)}\operatorname{rem}\pi_t^{f_{t+1}\ell_j}\,\chi_j\!\left(\frac{y_{t+1}}{\pi_t^{f_{t+1}}}\right)\\=\;&\rho_t^{-\check{\ell}}\,\pi_t^{f_{t+1}\ell_j+\hat{\ell}}\,\xi_j\!\left(\frac{y_{t+1}^{r_{t+1}}}{\pi_t^{f_{t+1}}}\right)\frac{\pi_t^{f_{t+1}\ell}\,\chi\!\left(\frac{y_{t+1}}{\pi_t^{f_{t+1}}}\right)}{\pi_t^{f_{t+1}\ell_j}\,\chi_j\!\left(\frac{y_{t+1}}{\pi_t^{f_{t+1}}}\right)}\operatorname{rem}\pi_t^{f_{t+1}\ell_j}\,\chi_j\!\left(\frac{y_{t+1}}{\pi_t^{f_{t+1}}}\right)\\=\;&\rho_t^{-\check{\ell}}\,\pi_t^{f_{t+1}\ell+\hat{\ell}}\\=\;&\rho_t^{-\check{\ell}}\,\pi_t^{\check{\ell}R_t}\\=\;&z^{\check{\ell}},\end{aligned}$$

whence

$$\mathrm{in}\left(u_j \frac{a}{a_j} \mathrm{rem}_{\varphi_{t+1}} a_j; \mathbb{P}_t\right) = \mathrm{in}(\mathrm{T}_t^{-1}(z^{\check{\ell}}); \mathbb{P}_t) = z^{\check{\ell}}.$$

After a division by a suitable power of z, we deduce the normalized initial inverse of a/a_j modulo a_j for $j = 1, \ldots, s$.

The following algorithm makes use of the separable factorization of univariate polynomials: see [54]. In the case of characteristic zero or sufficiently large, that holds in the present paper, the separable factorization coincides with the squarefree factorization.

Algorithm 7.2

Input. An effectively separable, regular, and irreducible contact tower $(\mathbb{P}_i)_{i \leqslant t}$ along with its initial expansion; a contact polynomial $a = \varphi_{t+1}^l + c_{l-1} \varphi_{t+1}^{l-1} + \cdots + c_0 \in \mathbb{P}_t$ modulo $O(z^\tau)$ clustered at $(\mathbb{P}_i)_{i \leqslant t}$, with $\tau > d_t \gamma_t$; the Newton polygon of a, with a single edge of finite slope $-\gamma_{t+1}$.

Output. A factorization of a into clustered polynomials a_j at $(\mathbb{P}_i)_{i \leqslant t}$ modulo $O(z^\tau)$, each a_j has a single edge of slope $-\gamma_{t+1}$ in its Newton polygon and the associated Newton polygon is the initial power of an irreducible polynomial.

Assumption. The characteristic of $\mathbb{K}$ is zero or $>l$.

1. Compute $\tilde{\mathrm{T}}_{t+1}(a)$ and $\chi \in \mathbb{A}_t[x_{t+1}]$ such that $\tilde{\mathrm{T}}_{t+1}(a) = \pi_t^{f_{t+1}\ell} \chi(y_{t+1} / \pi_t^{f_{t+1}\ell})$.
2. Factor $\chi = \chi_1 \cdots \chi_s$, where $\chi_1, \ldots, \chi_s$ are pairwise coprime powers of irreducible factors of χ: this can be done by computing the separable factorization of χ and then the irreducible factors of the separable ones.
3. For $j = 1, \ldots, s$ compute $\zeta_j := \left(\frac{\chi}{\chi_j}\right)^{-1} \bmod \chi_j$.
4. For $j = 1, \ldots, s$ compute a_j as defined in (7.7).
5. For $j = 1, \ldots, s$ compute u_j as defined in (7.8), and set $\delta_j := \lfloor v(a/a_j) + l_j \gamma_{t+1} \rfloor = \lfloor v(a) \rfloor$.
6. Lift the initial factorization of $\mathrm{in}(a; \mathbb{P}_t) = \mathrm{in}(a_1 \cdots a_s; \mathbb{P}_t)$ into $a = \hat{a}_1 \cdots \hat{a}_s$ to precision $O(z^\tau)$ by using Corollary 4.23 at precision $O(z^{\tau + \lfloor v(a) \rfloor})$.
7. Return $\hat{a}_1, \ldots, \hat{a}_s$ modulo $O(z^\tau)$.

PROPOSITION 7.14. *Assume that* **K** *holds. Algorithm 7.2 is correct and takes*

$$\tilde{O}(l d^{1+\epsilon} \tau) + \bar{\mathsf{F}}_{\mathbb{K}}(\tilde{\ell} d)$$

operations in $\mathbb{K}$, where $\tilde{\ell}$ is the degree of the separable part of χ.

Proof. From the above discussion the required initial Hensel context is known when entering step 6, so lifting is possible thanks to Corollary 4.23. Using Lemma 3.23 we verify that

$$\begin{aligned} \mathrm{val}_z([\varphi_{t+1}^0] a_j) &\leqslant v([\varphi_{t+1}^0] a_j; \mathbb{P}_{t-1}) \\ &= v(a; \mathbb{P}_{t-1}) - v(a/a_j; \mathbb{P}_{t-1}) \\ &\leqslant \tau + d_t \gamma_t - \gamma_{t+1} \\ &< \tau. \end{aligned} \tag{7.9}$$

It follows that the Newton polygon of a_j modulo $O(z^\tau)$ has a single edge of slope $-\gamma_{t+1}$. We are done with the correctness of the algorithm.

Let $\frac{1}{R_{t+1}} \mathbb{Z} := \bar{\Gamma}_{t+1}$. Steps 1, 4, and 5 take

$$\tilde{O}(l (s_1 \cdots s_t)^{1+\epsilon} \log(d \tau)\, t) = \tilde{O}(l d^{1+\epsilon} \log \tau)$$

by Proposition 6.4. For the factorization of χ in step 2, as indicated we first compute the separable factorization $\chi = \tilde{\chi}_1^1 \tilde{\chi}_2^2 \cdots \tilde{\chi}_k^k$ using $\tilde{O}(\ell d^{1+\epsilon})$ operations in $\mathbb{K}$ by [54], and then factor $\tilde{\chi}_1, \ldots, \tilde{\chi}_k$ (which are pairwise coprime). Consequently the cost of factoring over $\mathbb{A}_t$ is

$$\mathsf{F}_{\mathbb{A}_t}(\deg \tilde{\chi}_1) + \cdots + \mathsf{F}_{\mathbb{A}_t}(\deg \tilde{\chi}_k) \leqslant \bar{\mathsf{F}}_{\mathbb{K}}(\tilde{\ell} d).$$

Step 3 contributes to

$$O((s_1 \cdots s_t)^{1+\epsilon} \mathsf{M}(\ell) \log \ell)$$

operations in $\mathbb{K}$: this includes the computation of $\sum_{j=1}^{s} \frac{\chi}{\chi_j}$ via [26, chapter 10, Theorem 10.10], the remainders by the χ_j via [26, chapter 10, Theorem 10.6], and $s \leqslant \ell$ modular inversions. Finally, the cost of step 6 follows from Corollary 4.23 and $\max_{j=1,\ldots,s}(\delta_j) \leqslant \tau$. □

DEFINITION 7.15. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be an effectively separable, regular, and irreducible contact tower, and let a be a contact polynomial clustered at $\mathbb{P}_t$ having a single edge in its Newton polygon. The* ***equal-slope factorization*** *of a is made of contact polynomials $a_1, \ldots, a_r$ clustered at $\mathbb{P}_t$ such that $a = a_1 \cdots a_r$, the Newton polygon of a_i admits a single edge of the same slope as a and its Newton polynomial is the initial of a power of an irreducible homogeneous polynomial for $i = 1, \ldots, r$. These irreducible homogeneous polynomials are pairwise distinct.*

COROLLARY 7.16. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be an effectively separable, regular, and irreducible contact tower, and let a be a contact polynomial clustered at $\mathbb{P}_t$ having a single edge in its Newton polygon. Then, there exists a unique equal-slope factorization of a, up to a permutation of the factors.*

Proof. The existence follows from Proposition 7.14. As for the uniqueness, assume that $a_1, \ldots, a_r$ is an equal-slope factorization of a. In the same way as we constructed χ from a in equation (7.6), we define the polynomial $\chi_i \in \mathbb{A}_t[x_{t+1}]$ of degree ℓ_i by

$$\tilde{\mathrm{T}}_t(\mathrm{in}(a_i; \mathbb{P}_t)) = \pi_t^{f_{t+1} \ell_i} \chi_i(y_{t+1} / \pi_t^{f_{t+1}}),$$

for $i = 1, \ldots, r$. The χ_i are powers of pairwise distinct irreducible polynomials, so they coincide with those computed in Algorithm 7.2. □

7.6. Incrementing the contact tower

After distinct-slope and equal-slope factorizations, we have reduced the general situation to the case where the Newton polygon of a has a single edge and the associated Newton polynomial is an initial power of an irreducible homogeneous polynomial. This allows us to increment the underlying contact tower with a new contact coordinate at level $t+1$ and then to pursue the factorization of a with respect to the extended tower. In order to ensure that the extended contact tower is separable, we assume from now on that the characteristic of $\mathbb{K}$ is zero or sufficiently large.

Algorithm 7.3

Input. An effectively separable, regular, and irreducible contact tower $(\mathbb{P}_i)_{i \leqslant t}$ along with its initial expansion; a contact polynomial $a = \varphi_{t+1}^l + c_{l-1} \varphi_{t+1}^{l-1} + \cdots + c_0$ clustered at $\mathbb{P}_t$ modulo $O(z^\tau)$ with $\tau > d_t \gamma_t$, whose Newton polygon has a single edge of finite slope $-\gamma_{t+1}$, and such that the associated Newton polynomial is the initial power of an irreducible homogeneous polynomial.

Output. An extended tower $(\mathbb{P}_i)_{i\leqslant t+1}$ modulo $O(z^\tau)$, still effectively separable, regular, and irreducible, and such that a is clustered at it of degree l/d_{t+1} in φ_{t+2}.

Assumption. The characteristic of $\mathbb{K}$ is zero or $>l$.

1. Compute $\tilde{\mathrm{T}}_t(a)$ into the form $\pi_t^{f_{t+1}\ell}\chi(y_{t+1}/\pi_t^{f_{t+1}})$, with $\chi\in\mathbb{A}_t[x_{t+1}]$.
2. Compute the separable factorization $\chi=\mu^{m_{t+1}}$, where μ is irreducible and separable, according to the assumptions.
3. Set $s_{t+1}:=\deg\mu=\ell/m_{t+1}$, $d_{t+1}:=r_{t+1}s_{t+1}$ as above, and compute
$$\Phi_{t+1}:=\tilde{\mathrm{T}}_t^{-1}(\pi_t^{f_{t+1}s_{t+1}}\mu(y_{t+1}/\pi_t^{f_{t+1}})).$$
4. Extend the contact tower with Φ_{t+1} and extend the initial expansion accordingly.
5. Make level $t+1$ of the tower effectively separable by computing the inverse of $\frac{\partial\Phi_{t+1}}{\partial\varphi_{t+1}}$ modulo Φ_{t+1}.

PROPOSITION 7.17. *Algorithm 7.3 is correct and takes*
$$\tilde{O}(l\,d^{1+\epsilon}\tau)$$
operations in $\mathbb{K}$.

Proof. By construction, Φ_{t+1} is homogeneous of valuation $f_{t+1}s_{t+1}R_t$ in $\mathbb{K}[z,\varphi_1,\ldots,\varphi_{t+1}]$, and $(\mathbb{P}_i)_{i\leqslant t+1}$ satisfies all the requirements of Definition 3.1. The incremented tower remains effectively regular, since the known initial inverse of c_0 straightforwardly yields an initial inverse of $\Phi_{t+1}(\varphi_1,\ldots,\varphi_t,0)$. We extend the initial expansion at level $t+1$ accordingly. The initial inverse in step 5 does exist because μ is separable.

Steps 1 and 3 contribute to
$$\tilde{O}(\ell\,(s_1\cdots s_t)^{1+\epsilon}\log(d\,\tau)\,t)=\tilde{O}(l\,d^{1+\epsilon}\log\tau)$$
by Proposition 6.4. Step 2 takes $O(\mathsf{M}(\ell)\log\ell)$ operations in $\mathbb{A}_t$ by [54]. The cost of step 5 is $\tilde{O}(l\,d^{1+\epsilon}\log(l\,\gamma_{t+1}))=\tilde{O}(l\,d^{1+\epsilon}\log\tau)$ by Lemma 7.4. Finally, a is initially equal to $\Phi_{t+1}^{m_{t+1}}$ whenever $\gamma_{t+2}>d_{t+1}\gamma_{t+1}$, which means that a is clustered at $\mathbb{P}_{t+1}$. □

7.7. The central shift algorithm

In principle, Algorithm 7.3 might introduce a new contact coordinate Φ_{t+1} of degree one in φ_{t+1}. For complexity reasons it is better to avoid this from happening. As outlined in the introductory sections 2.5 and 2.6, we now work out the central shift algorithm.

Let $(\mathbb{P}_i)_{i\leqslant t}$ be an effectively separable, regular, and irreducible contact tower. Let $a=c_l\varphi_{t+1}^l+c_{l-1}\varphi_{t+1}^{l-1}+\cdots+c_0$ be clustered at $\mathbb{P}_t$. An *initial root* of a is an element $f\in\mathbb{P}_{t-1}$ such that
$$[c_lf^l+c_{l-1}f^{l-1}+\cdots+c_0]_{v(a;\mathbb{P}_t)}=0.$$

If $b=c'_h\varphi_{t+1}^h+c'_{h-1}\varphi_{t+1}^{h-1}+\cdots+c'_0$ is a Newton polynomial of a, then an *initial root* of b is an initial root of a regarded with γ_{t+1} set to the opposite of the slope of b. One key idea behind the central shift algorithm is the following lemma, that will be used in a "divide and conquer" fashion in the subsequent algorithm.

LEMMA 7.18. *Let a be a contact polynomial clustered at $\mathbb{P}_t$, and let f be a non-zero initial root of* $\operatorname{in}(a;\mathbb{P}_t)$ *of multiplicity $l \geqslant 1$. If the characteristic of $\mathbb{K}$ is zero or $>l$, then f is an initial root of $\frac{\mathrm{d}^h a}{\mathrm{d}\varphi_1^h}$ of multiplicity $l-h$, for $h=0,\ldots,l$.*

Proof. Set $\gamma_{t+1} := v(f;\mathbb{P}_t)$. Lemma 5.7 implies

$$\operatorname{in}\left(\frac{\mathrm{d}^h a}{\mathrm{d}\varphi_1^h};\mathbb{P}_t\right) = \operatorname{in}\left(\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}\varphi_1}\right)^h \frac{\partial^h a}{\partial\varphi_{t+1}^h};\mathbb{P}_t\right). \tag{7.10}$$

Since the tower is separable, we know from Lemma 5.4 that $\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}\varphi_1}$ is initially invertible, hence f is an initial root of $\operatorname{in}\left(\frac{\mathrm{d}^h a}{\mathrm{d}\varphi_1^h};\mathbb{P}_t\right)$ of multiplicity h. □

Algorithm 7.4

Input. An effectively separable, regular, and irreducible tower $(\mathbb{P}_i)_{i\leqslant t}$; a contact polynomial $a\in\mathbb{P}_t$ clustered at $\mathbb{P}_t$ and of degree $l\geqslant 1$ in φ_{t+1} modulo $O(z^\tau)$, with $\tau > d_t\gamma_t$; we assume that $\operatorname{in}(a;\mathbb{P}_t) = \operatorname{in}((\varphi_{t+1}-f)^l;\mathbb{P}_t)$, where f is initially invertible in $\mathbb{P}_{t-1}$.

Output. An effectively separable, regular, and irreducible tower $(\hat{\mathbb{P}}_i)_{i\leqslant t}$ such that $\hat{\mathbb{P}}_i = \mathbb{P}_i$ for $i=1,\ldots,t-1$, and the non-zero initial roots of the Newton polynomials of a have multiplicity $\leqslant l/2$.

1. If $l=1$ then replace Φ_t by $\Phi_t - f$ and return $(\mathbb{P}_i)_{i\leqslant t}$.
2. Let $h := \lfloor l/2 \rfloor$ and compute the Weierstraß normalization b of $\frac{\mathrm{d}^h a}{\mathrm{d}\varphi_1^h}$ modulo $O(z^\tau)$ via Corollary 4.14. The initial context is made of

   $$a_1 := \operatorname{in}((\varphi_{t+1}-f)^{l-h};\mathbb{P}_t), \quad a_2 := \operatorname{in}\left(\frac{l!}{(l-h)!}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}\varphi_1}\right)^h;\mathbb{P}_{t-1}\right),$$

   and the normalized initial inverse u_1/z^{δ_1} of a_2 in $\mathbb{P}_{t-1}$.
3. Call the algorithm recursively with input $(\mathbb{P}_i)_{i\leqslant t}$ and b modulo $O(z^\tau)$. Let $(\tilde{\mathbb{P}}_i)_{i\leqslant t}$ be the tower obtained in return.
4. Compute the effectively regular Newton polygon of a in $\tilde{\mathbb{P}}_t$ modulo $O(z^\tau)$ via Lemma 7.9.
5. Compute the distinct-slope factorization of a in $\tilde{\mathbb{P}}_t$ modulo $O(z^\tau)$ with Algorithm 7.1.
6. If all the non-zero initial roots of the Newton polynomials of a have multiplicity $\leqslant l/2$, then return $(\tilde{\mathbb{P}}_i)_{i\leqslant t}$ modulo $O(z^\tau)$.
7. Otherwise, compute the factor $\tilde{a}$ modulo $O(z^\tau)$ of a of degree $\tilde{l}$ in φ_{t+1} whose initial is the $\tilde{l}$-th power of a linear factor $\tilde{\varphi}_{t+1}-\tilde{f}$ with $\tilde{l}>l/2$, $\tilde{f}$ non-zero, and where $\tilde{\gamma}_{t+1}$ is set to $v(\tilde{f};\mathbb{P}_{t-1})$.
8. Let $\tilde{h} := \tilde{l} - (l-h)$ and compute the Weierstraß normalization $\tilde{b}$ of $\frac{\mathrm{d}^{\tilde{h}}\tilde{a}}{\mathrm{d}\tilde{\varphi}_1^{\tilde{h}}}$ modulo $O(z^\tau)$ via Corollary 4.14. The initial context is made of

   $$\tilde{a}_1 := \operatorname{in}\big((\tilde{\varphi}_{t+1}-\tilde{f})^{\tilde{l}-\tilde{h}};\mathbb{P}_t\big), \quad \tilde{a}_2 := \operatorname{in}\left(\frac{\tilde{l}!}{(\tilde{l}-\tilde{h})!}\left(\frac{\mathrm{d}\tilde{\varphi}_{t+1}}{\mathrm{d}\varphi_1}\right)^{\tilde{h}};\mathbb{P}_{t-1}\right),$$

   and the normalized initial inverse $\tilde{u}_1/z^{\tilde{\delta}_1}$ of $\tilde{a}_2$ in $\mathbb{P}_{t-1}$.
9. Call the algorithm recursively with input $(\tilde{\mathbb{P}}_i)_{i\leqslant t}$ and $\tilde{b}$ modulo $O(z^\tau)$. Return the tower $(\hat{\mathbb{P}}_i)_{i\leqslant t}$ obtained in the output.

PROPOSITION 7.19. *Algorithm 7.4 is correct and takes*

$$\tilde{O}(l d^{1+\epsilon} \tau)$$

operations in $\mathbb{K}$.

Proof. If the algorithm exits at step 1, then $a = \varphi_{t+1}$ when regarded in the returned tower. Since $v(f; \mathbb{P}_{t-1}) > v(\Phi_t; \mathbb{P}_{t-1})$ the initial form of the returned Φ_t is the same as the initial form of the input value of Φ_t, hence the returned tower is effectively separable, regular, and irreducible. The Newton polynomial of a cannot have non-zero initial roots with respect to the returned contact tower, so the output is correct.

The initial Weierstraß context in step 2 follows from equation (7.10). If the algorithm exits at step 6, then the output is clearly correct. Let us now examine the situation when the algorithm does not exit at step 6.

In step 7, Lemma 7.18 ensures that $\tilde{f}$ is a non-zero initial root of a Newton polynomial of $\frac{\mathrm{d}^h a}{\mathrm{d}\varphi_1^h}$ of multiplicity $\tilde{l} - h$, regarded in $\tilde{\mathbb{P}}_t$. Since $\hat{\gamma}_{t+1} > \gamma_{t+1}$, $\tilde{f}$ is a non-zero initial root of a Newton polynomial of b of multiplicity $\tilde{l} - h$. As a non-zero initial root of a Newton polynomial of a modulo $O(z^\tau)$ we necessarily have $\operatorname{val}_z(\tilde{f}^{\tilde{l}} a_2) < \tau$, hence

$$v(\tilde{f}^{\tilde{l}} a_2; \mathbb{P}_{t-1}) < \tau + d_t \gamma_t$$

by Lemma 3.23. From Lemma 4.3, we deduce that

$$v(\tilde{f}^{\tilde{l}}; \mathbb{P}_{t-1}) < \tau + d_t \gamma_t - v(a_2) \leqslant \tau,$$

and consequently that

$$\operatorname{val}_z(\tilde{f}^{\tilde{l}-h}) \leqslant v(\tilde{f}^{\tilde{l}-h}; \mathbb{P}_{t-1}) < \tau.$$

It follows that $\tilde{f}$ is a non-zero initial root of a Newton polynomial of b of multiplicity $\tilde{l} - h$ modulo $O(z^\tau)$, hence that $\tilde{l} - h \leqslant (l-h)/2$. Consequently,

$$\tilde{l} \leqslant (l+h)/2. \tag{7.11}$$

We verify that $\tilde{h} = \tilde{l} - (l-h) > l/2 - (l-h) = h - l/2 > -1$, so $\tilde{h} \geqslant 0$. In step 8, the contact polynomial $\tilde{b}$ has degree $\tilde{l} - \tilde{h} = l - h$ in $\tilde{\varphi}_{t+1}$. By Lemma 7.18, inequality (7.11), and by following the same reasoning as for b, a non-zero initial root of a Newton polynomial of $\tilde{a}$ in $\hat{\mathbb{P}}_t$ has multiplicity

$$\leqslant (\tilde{l} - \tilde{h})/2 + \tilde{h} = (\tilde{l} + \tilde{h})/2 = \tilde{l} - (l-h)/2 \leqslant (l+h)/2 - (l-h)/2 = h \leqslant l/2.$$

Let us now examine the Newton polynomials of a in $\tilde{\mathbb{P}}_t$. For this purpose, by means of Corollaries 7.12 and 7.16, we may decompose a into

$$a = a_- a_= \tilde{a} a_+,$$

where a_- has Newton polynomials with slopes $< -\tilde{\gamma}_{t+1}$, where a_+ has Newton polynomials with slope $> -\tilde{\gamma}_{t+1}$, and where $a_=$ has a single Newton polynomial of slope $-\tilde{\gamma}_{t+1}$ but that does not admit $\tilde{f}$ for initial root.

The initial of $\Theta := \hat{\Phi}_t - \Phi_t$ is $\tilde{f}$, so its valuation is $\tilde{\gamma}_{t+1}$. Therefore the Newton polygon of a_- in $\hat{\mathbb{P}}_t$ has a single edge of slope $-\tilde{\gamma}_{t+1}$. We also verify that the Newton polygon of $a_=$ in $\hat{\mathbb{P}}_t$ admits a single edge of slope $-\tilde{\gamma}_{t+1}$. Then, the Newton polygon of a_+ in $\hat{\mathbb{P}}_t$ is the same as in $\tilde{\mathbb{P}}_t$. Finally the Newton polygon of $\tilde{a}$ in $\hat{\mathbb{P}}_t$ has slopes $< -\tilde{\gamma}_{t+1}$. Consequently the non-zero initial roots of the Newton polynomials of a in $\hat{\mathbb{P}}_t$ cannot have multiplicities $> l/2$. We are done with the proof of the correctness.

From Lemma 5.4 we have

$$\mathrm{in}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}\varphi_1}\right)=\mathrm{in}\left(\frac{\partial\Phi_t}{\partial\varphi_t}\cdots\frac{\partial\Phi_1}{\partial\varphi_1}\right).$$

Therefore, by using Proposition 3.20, the initial inverse of $\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}\varphi_1}$ can be obtained with $\tilde{O}(d\,\tau)$ operations in $\mathbb{K}$ from the precomputations attached to $(\mathbb{P}_i)_{i\leqslant t}$. The needed initial Weierstraß contexts in steps 2 and 8 can be obtained with $\tilde{O}(l\,d\,\tau)$ operations in $\mathbb{K}$ thanks to Proposition 3.20 again. The corresponding Weierstraß normalizations take further $\tilde{O}(l\,d\,\tau)$ operations in $\mathbb{K}$ by Corollary 4.14.

Let $\mathsf{C}(l)$ represent the cost of the algorithm with input a of degree l. In step 1, the cost is $\mathsf{C}(1)=O(d\,\tau)$. In step 4 the effectively regular Newton polygon can be determined with cost $\tilde{O}(l\,d^{1+\epsilon}\tau)$ by Lemma 7.9. Step 5 amounts to $\tilde{O}(l\,d\,\tau)$ by using distinct-slope factorization and Proposition 7.10. In step 6, we appeal to the equal-slope factorization but discarding the irreducible factorizations: in fact, having a root of multiplicity $>l/2$ is equivalent to having a separable factor of multiplicity $>l/2$, that can thus be read off from the separable factorization. So Proposition 7.14 provides us with a cost $\tilde{O}(l\,d^{1+\epsilon}\tau)$ for steps 6 and 7. Consequently the cost $\mathsf{C}(l)$ of the algorithm in degree l in φ_{t+1} satisfies

$$\mathsf{C}(l)=\mathsf{C}(l-h)+\mathsf{C}(h)+\tilde{O}(l\,d^{1+\epsilon}\tau).$$

We conclude by a standard induction. □

8. CONTACT FACTORIZATION

We are now in a position to present our top level algorithm for contact factorization. The distinct-slope and equal-slope factorizations are intertwined in order to increase the current contact tower and split the input polynomials. The process finishes once the polynomial to be factored is a power of the top level contact coordinate, up to the input precision. The central shift algorithm ensures that the “divide and conquer” approach only incurs a logarithmic complexity overhead.

8.1. Recentered Newton steps

The main step of the contact factorization is summarized in the following algorithm.

Algorithm 8.1

Input. $(\mathbb{P}_i)_{i\leqslant t}$ effectively separable, regular, and irreducible; a contact polynomial $a=\varphi_{t+1}^l+c_{l-1}\varphi_{t+1}^{l-1}+\cdots+c_0\in\mathbb{P}_t$ modulo $O(z^\tau)$ clustered at $\mathbb{P}_t$, with $\tau>d_t\gamma_t$.

Output. A set $\mathcal{R}$ of contact factors $(a^{(j)},(\mathbb{P}_i^{(j)})_{i\leqslant t})$ with precision $O(z^\tau)$ for $j=1,\ldots,n$ such that:

a) $(\mathbb{P}_i^{(j)})_{i\leqslant t-1}=(\mathbb{P}_i)_{i\leqslant t-1}$, for $j=1,\ldots,n$;

b) $a=a^{(1)}\cdots a^{(n)}+O(z^\tau)$;

c) $a^{(j)}$ is clustered at $\mathbb{P}_t^{(j)}$, for $j=1,\ldots,n$;

d) The Newton polygon of $a^{(j)}$ with respect to $(\mathbb{P}_i^{(j)})_{i\leqslant t}$ has a single edge whose Newton polynomial is an initial power of an homogeneous polynomial of degree ℓ_i in φ_{t+1};

e) If the Newton polygon of $a^{(j)}$ has a non-zero initial root, then its multiplicity is $\leqslant \max(l/2,1)$.

Assumption. The characteristic of $\mathbb{K}$ is zero or $>l$.

1. Initialize $\mathcal{R}$ with the empty set.
2. Compute the effectively regular Newton polygon of a modulo $O(z^\tau)$ via Lemma 7.9, and then the distinct-slope factorization of a modulo $O(z^\tau)$ by using Algorithm 7.1. Let $\mathcal{A}$ be the set of factors obtained in return.
3. For each b in $\mathcal{A}$, compute the equal-slope factorization of b over $(\mathbb{P}_i)_{i\leqslant t}$ by using Algorithm 7.2. Let $\mathcal{B}$ be the set of all resulting factors along with their multiplicities.
4. For each b in $\mathcal{B}$ of multiplicity written m:
   a. If $m \leqslant l/2$, then insert $(b, (\mathbb{P}_i)_{i\leqslant t})$ in $\mathcal{R}$.
   b. If $m > l/2$ (so b is an initial power of a polynomial of degree one in φ_{t+1}), then call Algorithm 7.4 and append the resulting factorization to $\mathcal{R}$.
5. Return $\mathcal{R}$.

PROPOSITION 8.1. *Assume that* **K** *holds. Algorithm 8.1 is correct and takes at most*

$$\tilde{O}(l d^{1+\epsilon} \tau) + \bar{\mathsf{F}}_{\mathbb{K}}((\ell_1 + \cdots + \ell_n)\, d)$$

operations in $\mathbb{K}$.

Proof. Properties (a) to (e) are satisfied by construction. Step 2 takes $\tilde{O}(l d^{1+\epsilon}\tau)$ by Lemma 7.9 and Proposition 7.10. Step 3 totalizes $\tilde{O}(l d^{1+\epsilon}\tau) + \bar{\mathsf{F}}_{\mathbb{K}}((\ell_1 + \cdots + \ell_n)\, d)$ by Proposition 7.14. Step 4 contributes to $\tilde{O}(l d^{1+\epsilon}\tau)$ by Proposition 7.19. □

8.2. Main algorithm

Our top level algorithm finally makes a repeated use of Algorithm 8.1.

Algorithm 8.2

Input. $(\mathbb{P}_i)_{i\leqslant t}$ effectively separable, regular, and irreducible; $a \in \mathbb{P}_t$ clustered at $\mathbb{P}_t$ modulo $O(z^\tau)$, of degree l in φ_{t+1}, with $\tau > d_t \gamma_t$.

Output. An irreducible contact factorization of a modulo $O(z^\tau)$.

Assumption. The characteristic of $\mathbb{K}$ is zero or $>l$.

1. Initialize $\mathcal{R}$ and $\mathcal{S}$ with the empty set.
2. Call Algorithm 8.1 and let $(a^{(j)}, (\mathbb{P}_i^{(j)})_{i\leqslant t})$ denote the returned contact factors for $j = 1, \ldots, n$.
3. For $j = 1, \ldots, n$:
   - If $a^{(j)}$ is a power of $\varphi_{t+1}^{(j)}$ then insert $(a^{(j)}, (\mathbb{P}_i^{(j)})_{i\leqslant t})$ into $\mathcal{S}$.
   - Otherwise, call Algorithm 7.3 with $a^{(j)}$ and $(\mathbb{P}_i^{(j)})_{i\leqslant t}$ and let $(\mathbb{P}_i^{(j)})_{i\leqslant t+1}$ be the returned tower.
   - If $a^{(j)}$ equals $\Phi_{t+1}^{(j)}$ then insert $(a^{(j)}, (\mathbb{P}_i^{(j)})_{i\leqslant t+1})$ into $\mathcal{S}$.
   - If $\Phi_{t+1}^{(j)}$ has degree 1 in φ_{t+1} and writes $\Phi_{t+1}^{(j)} = \varphi_{t+1} - f$, then replace $\Phi_t^{(j)}$ by $\Phi_t^{(j)} - f$ and insert the pair $(a^{(j)}, (\mathbb{P}_i^{(j)})_{i\leqslant t})$ into $\mathcal{R}$.

- Otherwise insert the pair $(a^{(j)},(\mathbb{P}_i^{(j)})_{i\leqslant t+1})$ into $\mathcal{R}$.

4. Call the algorithm recursively for each element of $\mathcal{R}$. Include the returned factors into $\mathcal{S}$.
5. Return $\mathcal{S}$.

PROPOSITION 8.2. *Assume that* **K** *holds. Algorithm 8.2 is correct and takes at most*

$$\tilde{O}((ld)^{1+\epsilon}\tau)+2\,\bar{\mathsf{F}}_{\mathbb{K}}(ld)$$

operations in $\mathbb{K}$*.*

Proof. On the one hand, if the initial of $a^{(j)}$ is a power of a degree one polynomial, then according to the specification of Algorithm 8.1 we have

$$\deg_{\varphi_{t+1}} a^{(j)} \leqslant \max(l/2,1).$$

On the other hand, if $a^{(j)}$ is an initial power of a polynomial $\Phi_{t+1}^{(j)}$ of degree $\geqslant 2$, then

$$\deg_{\varphi_{t+2}} a^{(j)} = \frac{\deg_{\varphi_{t+1}} a^{(j)}}{\deg_{\varphi_{t+1}} \Phi_{t+1}^{(j)}} \leqslant l/2.$$

Consequently the depth of the recursive calls is $O(\log l)$. Let us analyze the valuation of $v(\Phi_{t+1}^{(j)};\mathbb{P}_t)$. If $\Phi_{t+1}^{(j)}$ comes from a proper distinct-slope factor or a proper equal-slope factor of a then inequalities (7.4) and (7.9) ensure that

$$d_{t+1}\gamma_{t+1} = v(\Phi_{t+1}^{(j)};\mathbb{P}_t) < \tau.$$

Otherwise a has a single slope and its initial is separable, so $n=1$, $\Phi_{t+1}^{(1)}=a$ and this case does not yield a recursive call. We conclude that the algorithm behaves as specified.

Discarding factorization costs, step 2 takes $\tilde{O}(l\,d^{1+\epsilon}\tau)$ operations in $\mathbb{K}$, by Proposition 8.1. In step 3, by Proposition 6.5, for each $j=1,\ldots,n$ the initial expansion of $(\mathbb{P}_i^{(j)})_{i\leqslant t^{(j)}}$ takes $\tilde{O}((d^{(j)})^{1+\epsilon})$, where $d^{(j)}$ represents the degree of $(\mathbb{P}_i^{(j)})_{i\leqslant t^{(j)}}$. By Proposition 7.17, the cost of Algorithm 7.3 is $\tilde{O}(l^{(j)}\,(d^{(j)})^{1+\epsilon}\tau)$, where $l^{(j)}$ denotes the degree of $a^{(j)}$ in its main variable $\varphi_{t^{(j)}+1}^{(j)}$. The total cost of steps 3 is

$$\tilde{O}\left(\sum_{j=1}^{n} l^{(j)}\,(d^{(j)})^{1+\epsilon}\tau\right) = \tilde{O}((ld)^{1+\epsilon}\tau).$$

Let $(b^{(j)},(\mathbb{P}_i^{(j)})_{i\leqslant t^{(j)}})$ for $j=1,\ldots,m$ denote the elements of $\mathcal{R}$ when entering step 4. By construction we have

$$\sum_{j=1}^{m} \deg_{\varphi_{t^{(j)}+1}} b^{(j)} \deg \mathbb{P}_{t^{(j)}}^{(j)} \leqslant ld.$$

If $\mathsf{T}(l,d)$ represents the cost function of the algorithm (still discarding factorizations), we have shown that

$$\mathsf{T}(d,l) = \tilde{O}((ld)^{1+\epsilon}\tau) + \sum_{1\leqslant j\leqslant m} \mathsf{T}\big(\deg_{\varphi_{t^{(j)}+1}} b^{(j)}, \deg \mathbb{P}_{t^{(j)}}^{(j)}\big),$$

and that $\mathsf{T}(1,d)=\tilde{O}(d^{1+\epsilon}\tau)$. Unrolling the recursion $O(\log l)$ times leads to

$$\mathsf{T}(l,d) = \tilde{O}((ld)^{1+\epsilon}\tau\log l) = \tilde{O}((ld)^{1+\epsilon}\tau).$$

Let us now turn to the cumulated cost $\Phi(l,d)$ of factoring separable polynomials over algebraic extensions of $\mathbb{K}$ during the execution of Algorithm 8.2. Let us show by induction on d and $l\geqslant 2$ that

$$\Phi(l,d)\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}((l-2)\,d). \tag{8.1}$$

This is easy if $l=2$, so assume that $l>2$. We recall that

$$\bar{\mathsf{F}}_{\mathbb{K}}(l_1)+\cdots+\bar{\mathsf{F}}_{\mathbb{K}}(l_k)\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l_1+\cdots+l_k)$$

holds for any positive integers $l_1,\ldots,l_k$. Assume first that a has a non-trivial distinct-slope factorization $a=a_1\cdots a_k$ during Algorithm 8.1 and let $l_1,\ldots,l_k$ be the degrees of $a_1,\ldots,a_k$ in φ_{t+1}. Then the induction hypothesis implies

$$\begin{aligned}
\Phi(l,d) &\leqslant \Phi(l_1,d)+\cdots+\Phi(l_k,d)\\
&\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l_1 d)+\bar{\mathsf{F}}_{\mathbb{K}}(d\,(l_1-2))+\cdots+\bar{\mathsf{F}}_{\mathbb{K}}(d\,l_k)+\bar{\mathsf{F}}_{\mathbb{K}}(d\,(l_k-2))\\
&\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l_1 d+\cdots+l_k d)+\bar{\mathsf{F}}_{\mathbb{K}}((l_1-2+\cdots+l_k-2)\,d)\\
&= \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}(l d-2 k d)\\
&\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}(l d-2).
\end{aligned}$$

Assume next that the Newton polygon of a has a unique slope and that the associated Newton polynomial is the m-th power of an irreducible polynomial of degree $\geqslant$2, for some $m\geqslant 2$. Then the induction hypothesis yields

$$\begin{aligned}
\Phi(l,d) &= \Phi(l/m,m d)\\
&\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}((l-2m)\,d)\\
&\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}((l-2)\,d).
\end{aligned}$$

Assume finally that the Newton polygon of a has a unique slope and that the associated Newton polynomial χ has at least two distinct prime factors. Consider the separable factorization

$$\chi=\chi_1^1\chi_2^2\cdots\chi_k^k$$

and let $l_1,\ldots,l_k$ be the degrees of $\chi_1,\ldots,\chi_k$ in φ_{t+1}. Note that $l_1+\cdots+l_k\geqslant 2$ and

$$\Phi(l,d)\leqslant \sum_{1\leqslant j\leqslant k}\bar{\mathsf{F}}_{\mathbb{K}}(l_j d)+\sum_{2\leqslant j\leqslant k}\Phi(l_j d,j).$$

Applying the induction hypothesis, this again yields

$$\begin{aligned}
\Phi(l,d) &\leqslant \sum_{1\leqslant j\leqslant k}\bar{\mathsf{F}}_{\mathbb{K}}(l_j d)+\sum_{2\leqslant j\leqslant k}(\bar{\mathsf{F}}_{\mathbb{K}}(l_j j d)+\bar{\mathsf{F}}_{\mathbb{K}}(l_j\,(j-2)\,d))\\
&\leqslant \bar{\mathsf{F}}_{\mathbb{K}}\left(\sum_{1\leqslant j\leqslant k} l_j j d\right)+\bar{\mathsf{F}}_{\mathbb{K}}\left(\sum_{2\leqslant j\leqslant k}(l_j d+l_j\,(j-2)\,d)\right)\\
&= \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}\left(\sum_{1\leqslant j\leqslant k}(l_j j-l_j)\,d\right)\\
&= \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}\left(\left(l-\sum_{1\leqslant j\leqslant k} l_j\right)d\right)\\
&\leqslant \bar{\mathsf{F}}_{\mathbb{K}}(l d)+\bar{\mathsf{F}}_{\mathbb{K}}((l-2)\,d).
\end{aligned}$$

We conclude by induction that (8.1) indeed holds. □

Proof of Theorem 1.1. Theorem 1.1 is a consequence of Proposition 8.2 by applying Algorithm 8.2 with input $a = P$ and the trivial contact tower of height zero. □

8.3. Approximate roots

We explain how Abhyankar's approximate roots theory could improve our contact factorization algorithm in some cases. If $f \in \mathbb{K}[x]$ is a monic polynomial of degree l and if m is a divisor of l that is invertible in $\mathbb{K}$, then there exists a unique polynomial g of degree l/m such that

$$\deg(f - g^m) < \frac{l}{m}(m-1) = l - \frac{l}{m}. \tag{8.2}$$

This polynomial g is called the m-th approximate root of f. In particular, g is monic and the g-adic expansion of f is of the form

$$f = g^m + f_{m-2} g^{m-2} + \cdots + f_0,$$

where $f_i \in \mathbb{K}[x]_{<l/m}$. Let $\tilde{f}(x) := x^l f(1/x)$, that is the *reverse* of f, and $\tilde{g}(x) := x^{l/m} g(1/x)$. Condition (8.2) is equivalent to

$$\tilde{f}(x) = \tilde{g}(x)^m + O\left(x^{\frac{l}{m}+1}\right),$$

which means that g is uniquely determined by $\tilde{g}(x) := [\tilde{f}(x)^{1/m}]_{0;l/m+1}$, whenever $\mathbb{K}$ is a perfect field. The computation of the m-th approximate root of $\tilde{f}$ can be done using the Newton operator if m is not 0 in $\mathbb{K}$: we define the sequence $(h_i)_{i \geqslant 0}$

$$h_0 := \tilde{f}(0) = 1, \quad h_{i+1} := h_i + h_i f (1 - f h_i^m) / m + O(x^{2^{i+1}}).$$

A standard computation shows that this sequence converges quadratically to $f^{-1/m}$. The computation of $\tilde{g}$ by this method takes $O(\mathsf{M}(l/m) \log m)$ operations in $\mathbb{K}$. Let us now extend this construction to contact coordinates.

LEMMA 8.3. *Let $a \in \mathbb{P}_t$ be monic of degree l in φ_{t+1}, and let m be a divisor of l that is invertible in $\mathbb{K}$. Then, there exists a unique $b \in \mathbb{P}_t$ monic of degree l/m in φ_{t+1} such that*

$$\deg_{\varphi_{t+1}}(a - b^m) < l - l/m.$$

Proof. The condition rewrites

$$\deg(\Pi_t(a) - \Pi_t(b)^m) < d(l - l/m),$$

and we have $\deg(\Pi_t(a)) = d\,l$, $\deg(\Pi_t(b)) = d\,l/m$. Therefore $\Pi_t(b)$ is uniquely determined as the m-th approximate root of $\Pi_t(a)$. □

In the context of Lemma 8.3, the b-adic expansion of a has the form

$$a = b^m + a_{m-2} b^{m-2} + \cdots + a_0.$$

The algorithmic purpose of approximate roots is as follows. Suppose that

$$\operatorname{in}(a) = \operatorname{in}(b^m)$$

for some $b \in \mathbb{P}_t$ monic in φ_{t+1}. We can add one level to $\mathbb{P}_t$ with

$$\Phi_{t+1} := b \text{ and } \gamma_{t+1} := v(b) / \deg_{\varphi_{t+1}} b.$$

We write a' for the image of a in $\mathbb{P}_{t+1}$ and examine the Newton polygon of a'. If we had

$$\operatorname{in}(a') = \operatorname{in}((\varphi_{t+2} + c)^m),$$

with some $c \in \mathbb{P}_t$, this would mean that

$$[a']_{0;mv(c)+\epsilon} = [(b+c)^m]_{0;mv(c)+\epsilon} = [a]_{0;mv(c)+\epsilon},$$

for some sufficiently small positive value of ϵ. In particular, the b-adic expansion of a would be

$$[a]_{0;mv(c)+\epsilon} = \left[\sum_{i=0}^{m} \binom{m}{i} c^{m-i} b^i\right]_{0;mv(c)+\epsilon}$$

whence

$$[a]_{0;(m-1)v(b)+v(c)+\epsilon} = [b^m + m\,c\,b^{m-1}]_{0;(m-1)v(b)+v(c)+\epsilon}.$$

The latter equality is not possible since it contradicts the fact that b is an approximate root of a.

Consequently, the Newton polygon of a' cannot have a single edge with a Newton polynomial of the form $\operatorname{in}((\varphi_{t+2} + c)^m)$. Either it has at least two edges, or a single edge but the initial factors of the Newton polynomial have multiplicity $<m$. For the situations similar to the one of section 2.5 these computations are expected to be faster and easier than the central shift method.

9. IRREDUCIBLE FACTORIZATION

In this section we consider a monic and separable polynomial $A \in \mathbb{K}[[z]][x]$. We are interested in computing the irreducible factorization of A modulo $O(z^\sigma)$ for some requested precision σ. Our strategy naturally relies on computing a contact factorization of A for a sufficiently large precision. We begin with analyzing the precision loss induced by the distinct slope and equal-slope factorizations.

9.1. Roots and contact representation

Let $A \in \mathbb{K}[[z]][x]$ be monic and separable, and let $(\mathbb{P}_i)_{i \leqslant t}$ be a contact tower. Let $\overline{\mathbb{K}((z))}$ denote an algebraic closure of $\mathbb{K}((z))$, we still write val_z for the extended valuation.

LEMMA 9.1. *Assume that $\Pi_t^{-1}(A)$ is clustered at $\mathbb{P}_t$. If $\psi \in \overline{\mathbb{K}((z))}$ is a root of A, then*

$$\operatorname{val}_z(\Psi_i(\psi)) \geqslant \gamma_{i+1},$$

for $i = 0, \ldots, t$. In addition, for all $B \in \mathbb{K}[[z]][x]$ we have

$$\operatorname{val}_z(B(\psi)) \geqslant v(\Pi_t^{-1}(B); \mathbb{P}_t).$$

Proof. From Lemma 7.5 we know that $\Pi_0^{-1}(A)$ is clustered at $\mathbb{P}_0$, hence

$$v(\Pi_0^{-1}(A); \mathbb{P}_0) = d_1 \cdots d_t m_{t+1} \gamma_1,$$

where $m_{t+1} := \deg_{\varphi_{t+1}}(\Pi_t^{-1}(A))$. Since $A(\psi) = 0$, necessarily $\operatorname{val}_z(\Psi_0(\psi)) \geqslant \gamma_1$ holds.

Assume that the lemma holds up to some index $i \in \{0, \ldots, t-1\}$. From Lemma 7.5, the contact polynomial $\Pi_i^{-1}(A)$ is clustered at $\mathbb{P}_i$. Let us canonically write

$$\Pi_i^{-1}(A) = \varphi_{i+1}^{l_i} + c_{l_i-1} \varphi_{i+1}^{l_i-1} + \cdots + c_0,$$

where $l_i := d_{i+1} \cdots d_t m_{t+1}$ and $c_j \in \mathbb{P}_{i-1}$. By induction we have

$$\mathrm{val}_z(\Pi_{i-1}(c_j)(\psi)) \geqslant v(c_j; \mathbb{P}_{i-1}) \geqslant (l_i - j)\, \gamma_{i+1},$$

for $j = 0, \ldots, l_i - 1$. Since

$$A(\psi) = \Psi_i(\psi)^{l_i} + \Pi_{i-1}(c_{l_i-1})(\psi)\, \Psi_i(\psi)^{l_i-1} + \cdots + \Pi_{i-1}(c_0)(\psi) = 0,$$

necessarily $\mathrm{val}_z(\Psi_i(\psi)) \geqslant \gamma_{i+1}$ holds. Let $B \in \mathbb{K}[[z]][x]$ be canonically written

$$\Pi_i^{-1}(B) = c'_n \varphi_{i+1}^n + c'_{n-1} \varphi_{i+1}^{n-1} + \cdots + c'_0,$$

with $c'_j \in \mathbb{P}_{i-1}$. Thanks to the induction hypothesis, we verify that

$$\begin{aligned}
\mathrm{val}_z(B(\psi)) &= \mathrm{val}_z(\Pi_{i-1}(c'_n)(\psi)\, \Psi_i(\psi)^n + \Pi_{i-1}(c'_{n-1})(\psi)\, \Psi_i(\psi)^{n-1} + \cdots + \Pi_{i-1}(c'_0)(\psi)) \\
&\geqslant \min(v(c'_n; \mathbb{P}_{i-1}) + n\, \gamma_{i+1}, v(c'_{n-1}; \mathbb{P}_{i-1}) + (n-1)\, \gamma_{i+1}, \ldots, v(c'_0; \mathbb{P}_{i-1})) \\
&= v(\Pi_i^{-1}(B); \mathbb{P}_i).
\end{aligned}$$

Finally the lemma holds for index $i+1$. □

If $(\mathbb{P}_i)_{i \leqslant t}$ is a separable, regular, and irreducible contact tower, then Lemmas 4.3 and 7.3 imply that v is a valuation of $\mathbb{K}((z))[x]$ that extends val_z.

PROPOSITION 9.2. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be a separable, regular, and irreducible contact tower and let $F := \Pi_t(\varphi_{t+1})$. Then v is the unique valuation of $\mathbb{K}((z))[x]/(F)$ that extends val_z and we have*

$$v(A) = \frac{\mathrm{val}_z(\mathrm{Res}_x(A, F))}{\deg_x F},$$

for all A in $\mathbb{K}((z))[x]/(F)$.

Proof. Proposition 7.2 ensures that F is irreducible. By setting γ_{t+1} to infinity we obtain that v is a valuation of $\mathbb{P}_t/(\varphi_{t+1})$. The uniqueness and the resultant-based expression are well known; for instance, see [53, chapter XII, Corollary 6.2]. □

9.2. Discriminants

Let A be monic in $\mathbb{K}[[z]][x]$ and clustered at an effectively separable, regular, and irreducible contact tower $(\mathbb{P}_i)_{i \leqslant t}$. We assume that $-\gamma_{t+1}$ is larger than or equal to the smallest slope of the Newton polygon of A. As before, a stands for the image $\Pi_t^{-1}(A)$ of A in $\mathbb{P}_t$, whose degree in φ_{t+1} is written l.

LEMMA 9.3. *With the above notation, the following inequality holds:*

$$\mathrm{val}_z(\mathrm{Disc}_x A) \geqslant l\, d \left(v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x} \right) + v(a) - \gamma_{t+1} \right).$$

Proof. Poisson's formula for resultants yields

$$\mathrm{Res}_x\left(A(x), \frac{\partial A}{\partial x}(x) \right) = \prod_{A(\psi)=0} \frac{\partial A}{\partial x}(\psi).$$

Thanks to Lemma 5.7, we deduce:

$$\begin{aligned}
&\mathrm{val}_z\left(\mathrm{Res}_x\left(A(x), \frac{\partial A}{\partial x}(x)\right)\right)\\
\geqslant\ & \mathrm{val}_z\left(\prod_{A(\psi)=0}\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\frac{\partial a}{\partial \varphi_{t+1}}\right)(\Psi_0(\psi),\ldots,\Psi_t(\psi))\right)\\
\geqslant\ & \sum_{A(\psi)=0}\left(v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)+v\left(\frac{\partial a}{\partial\varphi_{t+1}}\right)\right) && \text{(by Lemma 9.1)}\\
\geqslant\ & \sum_{A(\psi)=0}\left(v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)+v(a)-\gamma_{t+1}\right)\\
\geqslant\ & l\,d\left(v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right)+v(a)-\gamma_{t+1}\right). && \square
\end{aligned}$$

Next, we consider A_1 and A_2 monic in $\mathbb{K}[[z]][x]$. Let a_1 and a_2 stand for the canonical representatives of A_1 and A_2 in $\mathbb{P}_t$, of respective degrees l_1 and l_2 in φ_{t+1}. In the sequel, we define $[\varphi_{t+1}^0]\,a_2$ to be the constant coefficient of a_2, when regarded as a univariate polynomial in φ_{t+1}.

LEMMA 9.4. *With the above notation, if the slopes of the Newton polygon of a_1 are $\leqslant -\gamma_{t+1}$ and the slopes of the Newton polygon of a_2 are $\geqslant -\gamma_{t+1}$, then we have*

$$\mathrm{val}_z(\mathrm{Res}_x(A_1(x), A_2(x))) \geqslant l_1\, d\, v([\varphi_{t+1}^0]\,a_2).$$

Proof. Again, we use Poisson's formula for the resultants:

$$\mathrm{Res}_x(A_1(x), A_2(x)) = (-1)^{\deg_x A_1 \deg_x A_2}\prod_{A_2(\psi)=0} A_1(\psi).$$

It follows that

$$\mathrm{Res}_x(A_1(x), A_2(x)) = (-1)^{\deg_x A_1 \deg_x A_2}\prod_{A_2(\psi)=0} a_1(\Psi_0(\psi),\ldots,\Psi_t(\psi)).$$

Let $A_{2,1},\ldots,A_{2,k}$ be the distinct-slope factors of A_2 (as in Definition 7.11) and let $a_{2,1},\ldots, a_{2,k}$ stand for their image in $\mathbb{P}_t$. We verify that:

$$\begin{aligned}
\mathrm{val}_z(\mathrm{Res}_x(A_1(x), A_2(x))) &= \mathrm{val}_z\left(\prod_{A_2(\psi)=0} a_1(\Psi_0(\psi),\ldots,\Psi_t(\psi))\right)\\
&\geqslant \sum_{A_2(\psi)=0}\mathrm{val}_z(a_1(\Psi_0(\psi),\ldots,\Psi_t(\psi)))\\
&= \sum_{j=1}^{k}\sum_{A_{2,j}(\psi)=0}\mathrm{val}_z(a_1(\Psi_0(\psi),\ldots,\Psi_t(\psi)))\\
&\geqslant \sum_{j=1}^{k}\sum_{A_{2,j}(\psi)=0}\mathrm{val}_z(\Psi_t(\psi)^{l_1})\\
&\geqslant l_1\sum_{j=1}^{k}\sum_{A_{2,j}(\psi)=0}\mathrm{val}_z(\Psi_t(\psi)).
\end{aligned}$$

By Lemma 9.1, if ψ is a root of $A_{2,j}$ then $\mathrm{val}_z(\Psi_t(\psi))$ is larger or equal to the opposite of the slope of the single edge of the Newton polygon of $a_{2,j}$, that is

$$\mathrm{val}_z(\Psi_t(\psi)) \geqslant \frac{v([\varphi_{t+1}^0]\, a_{2,j})}{\deg_{\varphi_{t+1}} a_{2,j}}.$$

It follows that

$$\begin{aligned}\mathrm{val}_z(\mathrm{Res}_x(A_1(x),A_2(x))) &\geqslant l_1 \sum_{j=1}^{k} \deg_x A_{2,j} \frac{v([\varphi_{t+1}^0]\, a_{2,j})}{\deg_{\varphi_{t+1}} a_{2,j}} \\ &= l_1 d \sum_{j=1}^{k} v([\varphi_{t+1}^0]\, a_{2,j}) \\ &= l_1 d\, v([\varphi_{t+1}^0]\, a_2). \qquad \text{(by Lemma 4.3)} \qquad \square\end{aligned}$$

In the rest of the section, we study the precision loss encountered in each Newton factorization. For a partial factorization $A = A_1 A_2$ with monic A_1 and A_2, the following well known formula will be used several times:

$$\mathrm{Disc}_x(A_1 A_2) = \mathrm{Disc}_x(A_1)\, \mathrm{Disc}_x(A_2)\, \mathrm{Res}_x(A_1, A_2)^2. \tag{9.1}$$

9.3. Precision loss during distinct-slope factorization

In the sequel σ represents the precision at which the irreducible factors of the input polynomial are required. Let a in $\mathbb{P}_t$ be given modulo $O(z^\tau)$ with

$$\tau \geqslant \mathrm{val}_z(\mathrm{Disc}_x(A)) + \sigma,$$

where $A := \Pi_t(a)$. We assume that the Newton polygon of a has been computed. Following Definition 7.11, we let a_1 stand for the product of factors of a with slopes $\leqslant -\gamma_{t+1}$ and let a_2 stand for the product of factors of a with slopes $> -\gamma_{t+1}$, hence $a = a_1 a_2$. Let $l_1 := \deg_{\varphi_{t+1}} a_1 \geqslant 1$ and $l_2 := \deg_{\varphi_{t+1}} a_2 \geqslant 1$, let u_1 / z^{δ_1} represent the normalized initial inverse of a_2.

According to Corollary 4.11, we may obtain a_1 with precision $O(z^{\tau_1})$, where

$$\tau_1 := \tau - \delta_1 = \tau - \lfloor v(a_2) + d_t \gamma_t \rfloor.$$

Setting $A_i := \Pi_t(a_i)$ for $i = 1, 2$, equation (9.1) and Lemma 9.4 imply

$$\begin{aligned}\mathrm{val}_z(\mathrm{Disc}_x A_1) &= \mathrm{val}_z(\mathrm{Disc}_x(A_1 A_2)) - \mathrm{val}_z(\mathrm{Disc}_x A_2) - 2\,\mathrm{val}_z(\mathrm{Res}_x(A_1, A_2)) \\ &\leqslant \mathrm{val}_z(\mathrm{Disc}_x(A_1 A_2)) - 2\,\mathrm{val}_z(\mathrm{Res}_x(A_1, A_2)) \\ &\leqslant \tau - \sigma - 2 d l_1 v(a_2) \\ &= \tau_1 + \lfloor v(a_2) + d_t \gamma_t \rfloor - \sigma - 2 d l_1 v(a_2) \\ &\leqslant \tau_1 - \sigma + (v(a_2) + d_t \gamma_t - 2 l_1 v(a_2)).\end{aligned}$$

Since $l_2 \geqslant 1$ we have $v(a_2) = v([\varphi_{t+1}^0]\, a_2) \geqslant d_t \gamma_t$, that yields

$$\tau_1 \geqslant \mathrm{val}_z(\mathrm{Disc}_x(A_1)) + \sigma.$$

We also compute a_2 with precision $O(z^{\tau_2})$, where $\tau_2 := \tau_1$, and the same calculation yields

$$\tau_2 \geqslant \mathrm{val}_z(\mathrm{Disc}_x(A_2)) + \sigma.$$

LEMMA 9.5. *With the above notation, let $a \in \mathbb{P}_t$ be given with precision $O(z^{\tau})$ such that*

$$\tau \geqslant \mathrm{val}_z(\mathrm{Disc}_x(\Pi_t(a))) + \sigma.$$

Then, Algorithm 7.1 computes truncations of the distinct slope factors $a_1, \ldots, a_r$ of a modulo some $O(z^{\tau_i})$ such that

$$\tau \geqslant \tau_i \geqslant \mathrm{val}_z(\mathrm{Disc}_x(\Pi_t(a_i))) + \sigma,$$

for $i = 1, \ldots, r$.

Proof. We apply the above precision analysis in the "divide and conquer" fashion used in Algorithm 7.1. □

9.4. Precision loss during equal-slope factorization

Now we examine the precision loss during the equal-slope factorization. The input is a polynomial a clustered at $\mathbb{P}_t$ and which has a single slope $-\gamma_{t+1}$ and known with precision $O(z^{\tau})$ such that

$$\tau \geqslant \mathrm{val}_z(\mathrm{Disc}_x A) + \sigma.$$

Let $a_1, \ldots, a_r$ represent the equal slope factors of a as in Definition 7.15, and set $l_i := \deg_{\varphi_{t+1}} a_i$. By Corollary 4.23 the contact polynomial a_i can be computed with relative precision $O(z^{\tau_i})$ where

$$\tau_i := \tau - \delta_i \quad \text{and} \quad \delta_i := \lfloor v(a) - v(a_i) + l_i \gamma_{t+1} \rfloor = \lfloor v(a) \rfloor$$

for $i = 1, \ldots, r$. Setting $A := \Pi_t^{-1}(a)$ and $A_i := \Pi_t^{-1}(a_i)$ for $i = 1, \ldots, r$, Lemma 9.4 implies that

$$\begin{aligned} \mathrm{val}_z(\mathrm{Res}_x(A / A_i(x), A_i(x))) &\geqslant (l - l_i)\, d\, v(a_i) \\ &= (l - l_i)\, d\, l_i \gamma_{t+1}. \end{aligned}$$

Since

$$2\,(l - l_i)\, l_i - l = ((l - l_i)\, l_i - (l - l_i)) + ((l - l_i)\, l_i - l_i) = (l - l_i)(l_i - 1) + l_i\,(l - (l_i + 1)) \geqslant 0$$

and $\delta_i \leqslant v(a)$, we obtain that

$$\tau_i \geqslant \mathrm{val}_z(\mathrm{Disc}_x A_i) + \sigma,$$

for $i = 1, \ldots, r$.

LEMMA 9.6. *With the above notation, let $a \in \mathbb{P}_t$ be given with precision*

$$\tau \geqslant \mathrm{val}_z(\mathrm{Disc}_x(A)) + \sigma.$$

Then Algorithm 7.2 computes the equal-slope factors $a_1, \ldots, a_s$ modulo $O(z^{\tau_i})$ such that

$$\tau_i \geqslant \mathrm{val}_z(\mathrm{Disc}_x(A_i)) + \sigma.$$

Proof. In fact Algorithm 7.2 computes the equal-slope factors of a with a precision higher than the one requested here, but the above discussion leads to the lower bounds. □

9.5. Approximate irreducible factorization

We are now ready to prove Theorem 1.3. We assume that $P \in \mathbb{K}[[z]][x]$ is monic and separable of degree n in x and known modulo $O(z^{\tau})$ where $\tau := \mathrm{val}_z(\mathrm{Disc}_x P) + \sigma$. We combine Theorem 1.1 with the above precision analyses.

Proof of Theorem 1.3. We apply Algorithm 8.2 with entry $P \in \mathbb{K}[[z]][x]$ modulo $O(z^{\tau})$, and with the trivial contact tower of height zero. The above precision analyses for the intermediate steps of the contact factorization algorithm, namely Lemmas 9.5 and 9.6, show by induction that all intermediate factors A of P occurring in the top level algorithm are computed along with a contact tower $(\mathbb{P}_i)_{i \leqslant t}$ of degree d with precision $O(z^{\tau})$ such that

$$\tau \geqslant \operatorname{val}_z(\operatorname{Disc}_x A) + \sigma.$$

Such a factor is proved to be irreducible when it has degree one in φ_{t+1}. In this case, by inequality (3.3), the coefficients of A are uniquely determined up to precision in z at least

$$\operatorname{val}_z(\operatorname{Disc}_x A) + \sigma - (d_1 - 1)\,\gamma_1 - \cdots - (d_t - 1)\,\gamma_t,$$

which equals

$$\operatorname{val}_z(\operatorname{Disc}_x A) + \sigma - v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right),$$

by Lemma 5.4. On the other hand, Lemma 9.3 yields

$$\operatorname{val}_z(\operatorname{Disc}_x A) \geqslant v\left(\frac{\mathrm{d}\varphi_{t+1}}{\mathrm{d}x}\right),$$

so the precision of A is at least $O(z^{\sigma})$ as claimed. Note that the central shift algorithm does not produce factors, so it does not involve any loss of precision. □

10. CONCLUSION

The contact factorization presented in this paper is subject to further improvements. A first research direction concerns the design of a contact factorization algorithm that would not rely on univariate irreducible factorization, by using the *directed evaluation* paradigm of [46] instead; so the computed contact towers would not be necessarily irreducible any longer. Another research direction concerns the design of fast algorithms for the contact coordinates in the vein of [45, 46]: we could avoid the conversions to plain coordinates and their precision loss. Another research direction concerns fields of small positive characteristic $p > 0$.

BIBLIOGRAPHY

[1] S. S. Abhyankar. Irreducibility criterion for germs of analytic functions of two complex variables. *Adv. Math.*, 74(2):190–257, 1989.

[2] S. S. Abhyankar and T. Moh. Newton–Puiseux expansion and generalized Tschirnhausen transformation. I. *J. Reine Angew. Math.*, 260:47–83, 1973.

[3] S. S. Abhyankar and T. Moh. Newton–Puiseux expansion and generalized Tschrinhausen transformation. II. *J. Reine Angew. Math.*, 261:29–54, 1973.

[4] M. E. Alonso, F. J. Castro-Jiménez, and H. Hauser. Encoding algebraic power series. *J. Found. Comput. Math.*, 18(3):789–833, 2018.

[5] M. Aschenbrenner, L. van den Dries, and J. van der Hoeven. *Asymptotic Differential Algebra and Model Theory of Transseries*. Number 195 in Annals of Mathematics studies. Princeton University Press, 2017.

[6] J.-D. Bauch, E. Nart, and H. D. Stainsby. Complexity of OM factorizations of polynomials over local fields. *LMS J. Comput. Math.*, 16:139–171, 2013.

[7] A. Bostan, G. Christol, and Ph. Dumas. Fast computation of the Nth term of an algebraic series over a finite prime field. In M. Rosenkranz, editor, *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 119–126. New York, NY, USA, 2016. ACM.

[8] A. Bostan, F. Chyzak, G. Lecerf, B. Salvy, and É. Schost. Differential equations for algebraic functions. In C. W. Brown, editor, *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*, ISSAC '07. New York, NY, USA, 2007. ACM.

[9] A. Campillo and J. I. Farrán. Symbolic Hamburger–Noether expressions of plane curves and applications to AG codes. *Math. Comp.*, 71(240):1759–1780, 2002.

[10] D. G. Cantor and D. M. Gordon. Factoring polynomials over p-adic fields. In W. Bosma, editor, *Algorithmic Number Theory. 4th International Symposium, ANTS-IV Leiden, The Netherlands, July 2-7, 2000. Proceedings*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 185–208. Springer-Verlag, 2000.

[11] D. G. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28:693–701, 1991.

[12] D. G. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 36(154):587–592, 1981.

[13] A. L. Chistov. Polynomial complexity of the Newton–Puiseux algorithm. In *Mathematical Foundations of Computer Science 1986. Proceedings of the 12th Symposium Bratislava, Czechoslovakia August 25–29, 1986*, volume 233 of *Lecture Notes in Comput. Sci.*, pages 247–255. Springer-Verlag, 1986.

[14] A. L. Chistov. Efficient factoring polynomials over local fields and its applications. In *Proceedings of the International Congress of Mathematicians, Kyoto, Japan, 1990*, volume 1, pages 1509–1519. Springer-Verlag, 1991.

[15] D. V. Chudnovsky and G. V. Chudnovsky. On expansion of algebraic functions in power and Puiseux series, I. *J. Complexity*, 2(4):271–294, 1986.

[16] D. V. Chudnovsky and G. V. Chudnovsky. On expansion of algebraic functions in power and Puiseux series, II. *J. Complexity*, 3(1):1–25, 1987.

[17] H. Cohen. *A course in computational algebraic number theory*. Graduate Texts in Mathematics. Springer, Berlin, Heidelberg, 1993.

[18] V. Cossart and G. Moreno-Socías. Racines approchées, suites génératrices, suffisance des jets. *Annales de la Faculté des sciences de Toulouse 6^{e} série*, 14(3):353–394, 2005.

[19] D. Duval. Rational Puiseux expansions. *Compos. Math.*, 70(2):119–154, 1989.

[20] J. Fernández, J. Guàrdia, J. Montes, and E. Nart. Residual ideals of MacLane valuations. *J. Algebra*, 427:30–75, 2015.

[21] D. Ford and P. Letard. Implementing the Round Four maximal order algorithm. *J. Théor. Nombres Bordeaux*, 6(1):39–80, 1994.

[22] D. Ford, S. Pauli, and X.-F. Roblot. A fast algorithm for polynomial factorization over $\mathbb{Q}_p$. *J. Théor. Nombres Bordeaux*, 14(1):151–169, 2002.

[23] D. Ford and O. Veres. On the complexity of the Montes ideal factorization algorithm. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory. 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 174–185. Springer-Verlag, 2010.

[24] A. Fröhlich and J. C. Shepherdson. On the factorisation of polynomials in a finite number of steps. *Math. Z.*, 62:331–334, 1955.

[25] A. Fröhlich and J. C. Shepherdson. Effective procedures in field theory. *Philos. Trans. Roy. Soc. London. Ser. A.*, 248:407–432, 1956.

[26] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 3rd edition, 2013.

[27] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Comput. Complexity*, 2(3):187–224, 1992.

[28] G.-M. Greuel and G. Pfister. *A Singular introduction to commutative algebra*. Springer-Verlag Berlin Heidelberg, 2002.

[29] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. Théor. Nombres Bordeaux*, 23(3):667–696, 2011.

[30] J. Guàrdia, J. Montes, and E. Nart. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.*, 364(1):361–416, 2012.

[31] J. Guàrdia, J. Montes, and E. Nart. A new computational approach to ideal theory in number fields. *Found. Comput. Math.*, 13(5):729–762, 2013.

[32] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons and integral bases. *J. Number Theory*, 147:549–589, 2015.

[33] J. Guàrdia, E. Nart, and S. Pauli. Single-factor lifting and factorization of polynomials over local fields. *J. Symbolic Comput.*, 47(11):1318–1346, 2012.

[34] D. Harvey and J. van der Hoeven. Polynomial multiplication over finite fields in time $O(n \log n)$. *J. ACM*, 69(2):1–40, 2022. Article No.: 12.

[35] J. P. G. Henry and M. Merle. Complexity of computation of embedded resolution of algebraic curves. In J. H. Davenport, editor, *Eurocal '87. European Conference on Computer Algebra. Leipzig, GDR, June 2–5, 1987. Proceedings*, volume 378 of *Lect. Notes Comput. Sci.*, pages 381–390. Springer Berlin Heidelberg, 1989.

[36] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. *Annals of Math.*, 79:109–326, 1964.

[37] J. van der Hoeven. *Automatic asymptotics*. PhD thesis, École polytechnique, Palaiseau, France, 1997.

[38] J. van der Hoeven. Relax, but don't be too lazy. *J. Symbolic Comput.*, 34:479–542, 2002.

[39] J. van der Hoeven. Newton's method and FFT trading. *J. Symbolic Comput.*, 45(8):857–878, 2010.

[40] J. van der Hoeven. Faster Chinese remaindering. Technical Report, HAL, 2016. https://hal.archives-ouvertes.fr/hal-01403810.

[41] J. van der Hoeven. Computing with D-algebraic power series. *Appl. Algebra Engrg. Comm. Comput.*, 30(1):17–49, 2019.

[42] J. van der Hoeven. Effective power series computations. *Found. Comput. Math.*, 19(3):623–651, 2019.

[43] J. van der Hoeven. *The Jolly Writer. Your Guide to GNU TeXmacs*. Scypress, 2020.

[44] J. van der Hoeven and G. Lecerf. Modular composition via factorization. *J. Complexity*, 48:36–68, 2018.

[45] J. van der Hoeven and G. Lecerf. Accelerated tower arithmetic. *J. Complexity*, 55:101402, 2019.

[46] J. van der Hoeven and G. Lecerf. Directed evaluation. *J. Complexity*, 60:101498, 2020.

[47] J. van der Hoeven and G. Lecerf. Univariate polynomial factorization over finite fields with large extension degree. *Appl. Algebra Eng. Commun. Comput.*, 2022. https://doi.org/10.1007/s00200-021-00536-1.

[48] E. Kaltofen and V. Shoup. Fast polynomial factorization over high algebraic extensions of finite fields. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC '97, pages 184–188. New York, NY, USA, 1997. ACM.

[49] E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. *Math. Comput.*, 67(223):1179–1197, 1998.

[50] K. S. Kedlaya. On the algebraicity of generalized power series. *Beitr. Algebra Geom.*, 58:499–527, 2017.

[51] K. S. Kedlaya and C. Umans. Fast polynomial factorization and modular composition. *SIAM J. Comput.*, 40(6):1767–1802, 2011.

[52] H. T. Kung and J. F. Traub. All algebraic functions can be computed fast. *J. ACM*, 25(2):245–260, 1979.

[53] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 3rd edition, 2002.

[54] G. Lecerf. Fast separable factorization and applications. *Appl. Algebra Engrg. Comm. Comput.*, 19(2):135–160, 2008.

[55] S. MacLane. A construction for absolute values in polynomial rings. *Trans. Am. Math. Soc.*, 40(3):363–395, 1936.

[56] S. MacLane. A construction for prime ideals as absolute values of an algebraic field. *Duke Math. J.*, 2(3):492–510, 1936.

[57] J. Montes. *Polígonos de Newton de orden superior y aplicaciones aritméticas*. PhD thesis, Universitat de Barcelona, Spain, 1999.

[58] F. Mora. An algorithm to compute the equations of tangent cones. In J. Calmet, editor, *Computer Algebra. EUROCAM '82, European Computer Algebra Conference, Marseilles, France, April 5-7, 1982*, volume 144 of *Lect. Notes in Computer Sc.*, pages 158–165. Springer-Verlag Berlin Heidelberg, 1982.

[59] G. Moroz. New data structure for univariate polynomial approximation and applications to root isolation, numerical multipoint evaluation, and other problems. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1090–1099. Los Alamitos, CA, USA, 2022. IEEE.

[60] G. Moroz and É. Schost. A fast algorithm for computing the truncated resultant. In M. Rosenkranz, editor, *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 341–348. New York, NY, USA, 2016. ACM.

[61] E. Nart. Okutsu–Montes representations of prime ideals of one-dimensional integral closures. *Publicacions Matemàtiques*, 55(2):261–294, 2011.

[62] I. Newton. *De methodis serierum et Fluxionum*. Manuscript, 1671.

[63] A. M. Ostrowski. Über die Bedeutung der Theorie der konvexen Polyeder für die formale Algebra. *Jahresber. Deutsch. Math.-Verein.*, 30(2):98–99, 1921. Talk given at *Der Deutsche Mathematikertag vom 18–24 September 1921 in Jena*.

[64] A. M. Ostrowski. On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms. *Aequationes Math.*, 13(3):201–228, 1975.

[65] A. M. Ostrowski. On the significance of the theory of convex polyhedra for formal algebra. *SIGSAM Bull.*, 33(1):5, 1999. Translated from [63].

[66] V. Y. Pan. Univariate polynomials: nearly optimal algorithms for numerical factorization and root-finding. *J. Symbolic Comput.*, 33(5):701–733, 2002.

[67] S. Pauli. Factoring polynomials over local fields. *J. Symbolic Comput.*, 32(5):533–547, 2001.

[68] A. Poteaux. *Calcul de développements de Puiseux et application au calcul de groupe de monodromie d'une courbe algébrique plane*. PhD thesis, Université de Limoges, France, 2008.

[69] A. Poteaux and M. Rybowicz. Improving complexity bounds for the computation of Puiseux series over finite fields. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC'15, pages 299–306. New York, NY, USA, 2015. ACM.

[70] A. Poteaux and É. Schost. Modular composition modulo triangular sets and applications. *Comput. Complex.*, 22(3):463–516, 2013.

[71] A. Poteaux and M. Weimann. Using approximate roots for irreducibility and equi-singularity issues in $K[[x]][y]$. Technical Report, arXiv:1904.00286, 2019.

[72] A. Poteaux and M. Weimann. Computing Puiseux series: a fast divide and conquer algorithm. *Ann. Henri Lebesgue*, 5:1061–1102, 2021.

[73] A. Poteaux and M. Weimann. A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$. *Comput. Complex.*, 31:6, 2022.

[74] A. Poteaux and M. Weimann. Local polynomial factorisation: improving the Montes algorithm. In A. Hashemi, editor, *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22, pages 149–157. New York, NY, USA, 2022. ACM.

[75] M. V. Puiseux. Recherches sur les fonctions algébriques. *J. Math. Pures et Appliquées*, 15:365–480, 1850.

[76] P. Russell. Hamburger–Noether expansions and approximate roots of polynomials. *Manuscripta Math.*, 31:25–95, 1980.

[77] A. Schönhage. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inform.*, 7:395–398, 1977.

[78] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. Technical Report, Math. Inst. Univ. of Tübingen, 1982.

[79] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Math. Comp.*, 54(189):435–447, 1990.

[80] S. Smith. On the higher singularities of plane curves. *Prod. London Math. Soc.*, 6:153–182, 1875.

[81] B. L. van der Waerden. *Algebra*. Springer, 7th edition, 1991. Based in part on lectures by E. Artin and E. Noether.

[82] R. J. Walker. *Algebraic Curves*, volume 13 of *Princeton mathematical series*. Princeton University Press, 1950.

[83] P. Walsh. A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function. *Math. Comp.*, 69(231):1167–1182, 2000.

[84] P. G. Walsh. On the complexity of rational Puiseux expansions. *Pacific J. Math.*, 188(2):369–387, 1999.

[85] S. M. Watt. A fixed point method for power series computation. In P. Gianni, editor, *Symbolic and Algebraic Computation. International Symposium ISSAC' 88, Rome, Italy, July 4-8, 1988. Proceedings*, volume 358 of *Lect. Notes in Computer Sc.*, pages 206–217. Springer-Verlag, 1989.

[86] O. Zariski. *Le problème des modules pour les branches planes*. Hermann, Paris, 1986.

GLOSSARY

$\mathbb{A}[x]_{<d}$	polynomials in $\mathbb{A}[x]$ of degree $<d$	2
$\bar{\mathsf{F}}_{\mathbb{K}}$	cost function for univariate polynomial factorization	3
K	assumption that irreducible factorization is available in $\mathbb{K}[x]$	4
$[a]_e$	homogeneous component of a of degree e	9

$[a]_{e;\eta}$	homogeneous components of a from degree e to $<e+\eta$	9
$\mathrm{in}(a)$	initial form of a	9
Γ_t	valuation semi-group of the t-th level of a contact tower	15
$\bar{\Gamma}_t$	group generated by Γ_t	15
R_t	ramification index of $\bar{\Gamma}_t$	15
Φ_i	i-th defining polynomial of a contact tower	15
I_t	defining ideal of a contact tower of height t	16
$\mathbb{S}_t$	level t of a contact tower	16
$\deg_{\varphi_{t+1}} b$	degree of b with respect to the contact variable φ_{t+1}	21
$\mathbb{P}_t$	polynomials at the level t of a contact tower	22
Ψ_i	expression of Φ_i in terms of the plain coordinates	22
Π_t	conversion to plain coordinates	22
$\mathrm{val}_z A$	valuation of A with respect to z	25
$\frac{\mathrm{d}a}{\mathrm{d}x}$	derivative of a with respect to x	40
$\mathrm{in}(a;\mathbb{P}_i)$	initial form of a regarded in $\mathbb{P}_i$	51
$v(a;\mathbb{P}_i)$	valuation of a regarded in $\mathbb{P}_i$	51
$[a;\mathbb{P}_i]_{\alpha;\eta}$	homogeneous components of a regarded in $\mathbb{P}_i$	51

INDEX