Contact arithmetic*†

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

Laboratoire d'informatique de l'École polytechnique (LIX, UMR 7161)
CNRS, École polytechnique, Institut Polytechnique de Paris
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 June 19, 2025

The irreducible factorization of polynomials over power series is central to several problems in computer algebra: integral bases, genus of a curve, Jacobian of a curve, Riemann–Roch spaces. Well-known applications include cryptography and algebraic geometry error-correcting codes. Towards solving these problems with quasi-optimal complexity, recent algorithms make use of the so-called "contact representation". When carrying out the Newton polygon method, this allows intermediate objects to be represented in a compact way with respect to the required relative precision. In this paper, we focus on the complexity of the corresponding "contact arithmetic" and present quasi-optimal algorithms for multiplication and division in the contact representation.

KEYWORDS: contact factorization, approximate root, key polynomial, OM algorithm, algebraic curve, accelerated tower, computer algebra, algorithm, complexity

1. INTRODUCTION

Consider the valued field $\mathbb{L} = \mathbb{K}((z))$ of Laurent series over an effective field $\mathbb{K}$. Here "effective" means that algorithms are at our disposal for the arithmetic operations and the zero test in $\mathbb{K}$. We will write $v: \mathbb{L} \to \Gamma_{\mathbb{L}} \cup \{\infty\}$ for the valuation on $\mathbb{L}$, with value group $\Gamma_{\mathbb{L}} = \mathbb{Z}$.

Computing the irreducible factorization of polynomials over $\mathbb{L}$ is central for several problems in computer algebra: integral bases, genus of a curve, Jacobian of a curve, Riemann–Roch spaces. Well-known applications include cryptography and algebraic geometry error-correcting codes.

The standard way to factor polynomials over $\mathbb{L}$ is to use the Newton–Puiseux method. The mathematical description of this algorithm goes back to Newton and Puiseux [16, 21]. Analyzing its computational complexity turns out to be subtle, due to the infinite nature of Laurent series. In particular, we must first decide how to represent and truncate elements in algebraic extensions of $\mathbb{L}$.

∗. Grégoire Lecerf has been supported by the French ANR-22-CE48-0016 NODE project. Joris van der Hoeven has been supported by an ERC-2023-ADG grant for the ODELIX project (number 101142171).
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

†. This article has been written using GNU TEXMACS [6].

If $P \in \mathbb{L}[x]$ is an irreducible polynomial, then $\mathbb{E} := \mathbb{L}[x]/(P(x))$ is again a valued field and v extends uniquely to $\mathbb{E}$. The main goal of this paper is to device efficient algorithms for computations with suitably truncated elements in $\mathbb{E}$.

If $\mathbb{K}$ has characteristic zero, then the roots of P are conjugate Puiseux series whose coefficients lie in an algebraic extension of $\mathbb{K}$. Taking ξ to be one of these roots, one obvious plan for computations in $\mathbb{E}$ is to simply extend $\mathbb{L}$ by ξ and do all our computations with Puiseux series. However, this is non-trivial to implement with good complexity and the restriction to characteristic zero is an important drawback.

In order to factor polynomials over $\mathbb{L}$ with good complexity, modern algorithms [11, 18–20] are based on an alternate representation for elements in $\mathbb{E}$. This representation was used by Abhyankar and Moh in [1, 2] and is called the *contact representation* in [11]. The precise definition is somewhat technical and recalled in section 1.1 below. It has the advantage of providing a compact representation for truncations of elements of $\mathbb{E}$, in particular when the relative precision of such truncations is low.

Given an ordinary non-zero Laurent series $f = \sum_{k \geqslant \sigma} f_k z^k$ with $\sigma := v(f)$, its truncation with relative precision ρ is simply $f_\sigma z^\sigma + \cdots + f_{\sigma+\rho-1} z^{\sigma+\rho-1}$. Truncating elements of $\mathbb{E}$ depends on the basis we choose for $\mathbb{E}$ as a vector space over $\mathbb{L}$. Consider for instance the case when $P = (x^2 - 3z^{31})^2 - xz^{1001}$ and the element $f = x^2 - 3z^{31} \in \mathbb{E}$ with $v(f) = 2033/4$. It is more accurate and compact to represent approximations of f with respect to the basis $1, x, x^2 - 3z^{31}, x(x^2 - 3z^{31})$ than with respect to the canonical basis $1, x, x^2, x^3$. Although conversions between both bases are possible, such conversions involve a constant loss of precision, which is a problem when working with low relative precision.

In a nutshell, the contact representation is both compact and accurate for low relative precisions, whereas the usual representation with respect to the basis $1, x, \ldots, x^{\deg P - 1}$ is more straightforward and efficient from a computational point for high precisions. In the recent works [3, 11, 18–20], the subtleties of the contact representation were circumvented by keeping the precision sufficiently high; in this way, it remained acceptable to do all actual computations using the classical representation. However, in the case of [11], this could only be achieved at the price of several convolutions, making part of the algorithms less natural.

The present work is inspired by the idea that, in order to design efficient and elegant algorithms for high-level mathematical problems (e.g. factorization over $\mathbb{L}$), it is worthwhile to find the intrinsically best adapted representation for the underlying objects (the contact representation) and then to first develop efficient algorithms in order to work with this representation (contact arithmetic); see also [7].

In this paper, we present quasi-optimal algorithms for basic arithmetic operations when using the contact representation. The contact representation can be regarded as a hybrid one that mixes recursive p-adic expansions (at high relative precision) and towers of algebraic extensions (at low relative precision). Our complexity bounds are quasi-optimal, uniformly in the required precision. In order to achieve them, we will borrow techniques from [9] to accelerate computations in towers of algebraic extensions.

The contact representation is fairly subtle, which explains the length of this paper. But we believe that this makes it even more worthwhile to separate the "low-level" contact arithmetic that we develop here from high-level applications to factorization and other problems (which we intend to work out in upcoming work).

1.1. Main result

In order to present our main result we need several definitions for the contact representation of elements of $\mathbb{E}$.

DEFINITION 1.1. *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 $\gamma_1, \ldots, \gamma_{t+1}$, called* **contact slopes**.

These data are required to satisfy the following properties:

- *Regarded in $\mathbb{K}[[z]][\varphi_1, \ldots, \varphi_{i-1}][\varphi_i]$, the polynomial 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 $\mathbb{K}[[z, \varphi_1, \ldots, \varphi_{t+1}]]$ 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 $i = 1, \ldots, t$.*

The tower is said to be **almost reduced** *when $d_i \geqslant 2$ for $i = 2, \ldots, t$. We write $D_i := d_1 \cdots d_i$ for $i = 1, \ldots, t$.*

The above contact tower defines the following sequence of isomorphic $\mathbb{K}((z))$-algebras:

$$\mathbb{P}_i := \mathbb{K}((z))[\varphi_1, \ldots, \varphi_{i+1}] / (\Phi_1 - \varphi_2, \ldots, \Phi_i - \varphi_{i+1}), \text{ for } i = 1, \ldots, t;$$

see [11, Lemma 3.15]. Note that [11] defines $\mathbb{P}_i$ over $\mathbb{K}[[z]]$, but the results from there can naturally be restated over $\mathbb{K}((z))$ instead. An element a in $\mathbb{P}_i$ admits a unique representative, called **canonical**, in the form of a polynomial in $\mathbb{K}((z))[\varphi_1, \ldots, \varphi_{i+1}]$ whose partial degree in φ_j is $< d_j$ for $j = 1, \ldots, i$; see [11, section 3.5]. We write $(\mathbb{P}_t)_{<l}$ for the elements of $\mathbb{P}_t$ whose canonical representative has degree $< l$ in φ_{t+1}. We let

$$\Gamma_i := \mathbb{Z} + \mathbb{Z}\,\gamma_1 + \cdots + \mathbb{Z}\,\gamma_i.$$

Following [11, Proposition 3.22], the valuation $v : \mathbb{K}((z)) \to \mathbb{Z} \cup \{\infty\}$ extends to a semi-valuation $v(\cdot; \mathbb{P}_i) : \mathbb{P}_i \to \Gamma_{i+1} \cup \{\infty\}$ defined by $v(\varphi_j; \mathbb{P}_t) := \gamma_j$ for $j = 1, \ldots, i+1$, and such that $\mathbb{P}_i$ inherits the above weighted grading of $\mathbb{K}((z))[[\varphi_1, \ldots, \varphi_{i+1}]]$. Most of the valuations considered in this paper will be semi-valuations, so we will drop the prefix "semi" for convenience.

The **initial inverse** of $b \in \mathbb{P}_{t-1}$ is a homogeneous element $u \in \mathbb{P}_{t-1}$ such that:

- $v(u; \mathbb{P}_{t-1}) = -v(b; \mathbb{P}_{t-1})$,
- the homogeneous component of valuation 0 of $u\,b$, written $[u\,b; \mathbb{P}_{t-1}]_0$, equals 1.

Note that in [11, Definition 4.2 and Lemma 4.3] we forced a normalized form to represent initial inverses. This normalization is not needed in this paper because we perform computations in contact towers directly over $\mathbb{K}((z))$ instead of $\mathbb{K}[[z]]$.

DEFINITION 1.2. *A contact tower $(\mathbb{P}_i)_{i \leqslant t}$ as in Definition 1.1 is said to be* **separable** *when $\dfrac{\partial \Phi_i}{\partial \varphi_i}$ is initially invertible in $\mathbb{P}_i$, for $i = 1, \ldots, s$. It is said to be* **effectively separable** *if the initial inverse of the $\dfrac{\partial \Phi_i}{\partial \varphi_i}$ is known for algorithmic purposes, for $i = 1, \ldots, t$.*

DEFINITION 1.3. *With the notation of Definition 1.1, 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 initial inverse of $\Phi_i(\varphi_1,\ldots,\varphi_{i-1},0)$ is known for algorithmic purposes, for $i=1,\ldots,t$.*

We denote by $[\mathbb{P}_t]_{\sigma;\rho}$ the $\mathbb{K}$-vector space of the elements of $\mathbb{P}_t$ having valuation $\geqslant\sigma$ and (weighted) degree $<\sigma+\rho$. For $a\in\mathbb{P}_t$, we also write $[a;\mathbb{P}_t]_{\sigma;\rho}$ for the sum of the terms of a that belong to $[\mathbb{P}_t]_{\sigma;\rho}$. 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 [4, chapter 25, section 7] for technical details. An algebraic complexity model (*e.g.* straight-line programs) will be used for counting operations in $\mathbb{K}$.

For $i=1,\ldots,t+1$, there exists a unique integer $R_i\in\mathbb{N}$ such that Γ_i equals $R_i^{-1}\mathbb{Z}$; see [11, section 3.1]. The (logarithmic) height of a rational number a/b is defined by

$$\mathrm{ht}(a/b) := \log(\max(|a|,|b|)),$$

where log represents the natural logarithm. The number of bits for storing a/b in a dense fashion is asymptotically proportional to $\mathrm{ht}(a/b)$. Elements in a contact tower will be represented by the mixed dense-sparse representation described in section 2.3. A contact polynomial $P\in\mathbb{P}_t$ is said to be **clustered** if its canonical representative is monic in φ_{t+1} of degree $l\geqslant 1$ (that is $P_l\in\mathbb{K}$) and $v(P;\mathbb{P}_t)=l\,\gamma_{t+1}$. The definitions of the quotient and remainder of contact polynomials, written $\mathrm{quo}_{\varphi_{t+1}}$ and $\mathrm{rem}_{\varphi_{t+1}}$, are recalled in section 3.1. With these conventions, we are now able to state our main result.

THEOREM 1.4. *Let $\epsilon>0$ (thought to be arbitrarily small)* [*the ϵ notation is not so nice, because of the ϵ_i and because it used without warning as an arbirarily small positive constants at several places*]. *Given an almost reduced effectively separable and regular contact tower $(\mathbb{P}_i)_{i\leqslant t}$ and $\rho\in R_{t+1}^{-1}\mathbb{N}^{>0}$, we can compute auxiliary data (that only depend on the tower and ρ) using*

$$R_t^{-1}\tilde{O}(D_t^{1+\epsilon}r_{t+1}R_t(\rho+\mathrm{ht}\,\gamma_t))$$

operations in $\mathbb{K}$, such that, for any $l\in r_{t+1}\mathbb{N}^{>0}$, the following tasks can be performed using

$$R_{t+1}^{-1}\tilde{O}(D_t^{1+\epsilon}lR_{t+1}\rho)$$

operations in $\mathbb{K}$:

- *given $A\in[(\mathbb{P}_t)_{<l}]_{v(A;\mathbb{P}_t);\rho}$ and $B\in[(\mathbb{P}_t)_{<l}]_{v(B;\mathbb{P}_t);\rho}$, compute $[AB;\mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho}$,*
- *given $A\in[(\mathbb{P}_t)_{<2l}]_{v(A;\mathbb{P}_t);\rho}$ and $B\in[(\mathbb{P}_t)_{<l}]_{v(B;\mathbb{P}_t);\rho}$ clustered of degree l, compute $[A\,\mathrm{quo}_{\varphi_{t+1}}B;\mathbb{P}_t]_{v(A;\mathbb{P}_t)-v(B;\mathbb{P}_t);\rho}$ and $[A\,\mathrm{rem}_{\varphi_{t+1}}B;\mathbb{P}_t]_{v(A;\mathbb{P}_t);\rho}$.*

1.2. Related work

Theorem 1.4 contains the first nearly linear complexity bound for computing in contact towers. This result relies on our previous fast algorithms for algebraic towers [9, 10]. We are not aware of any other method with subquadratic complexity. Of course, when the relative precision is sufficiently large, a known fast strategy is to always work with respect to the plain coordinates z,x, modulo appropriate conversions; see [11, section 3.6].

Let P be irreducible in $\mathbb{K}((z))[x]$. In characteristic zero or $>\deg P$, rational Puiseux expansions can be computed efficiently [18], hence $\mathbb{E} = \mathbb{K}((z))[x]/(P(x))$ becomes explicitly isomorphic to $\mathbb{E}' := \mathbb{K}[\alpha]((z))[x]/(x^e - \alpha t)$, where α is algebraic over $\mathbb{K}$ of degree $s := (\deg P)/e$. In this way, arithmetic operations in $\mathbb{E}'$ can be achieved in softly linear time. The extension of this approach is tedious for small characteristic: Puiseux expansions do not exist any longer and uniformizing parameters are not known to be computable in quasi-linear time so far.

Contact towers (a term coined in [11]) constitute an alternate approach, that goes back to Mac Lane [15] and that has been independently popularized by Abhyankar and Moh [1, 2] in the seventies. In fact, the latter authors designed specific contact towers from so-called *approximate roots* of P, that can be computed easily. Poteaux and Weimann achieved a quasi-linear complexity bound for irreducibility testing [19]. Compared to Puiseux expansions, contact towers yield more convenient algorithmic and geometric views for germs of plane curves (the geometric counterpart of polynomials over power series).

Puiseux expansions and contact towers are central tools for computing local irreducible factorizations. Unless the characteristic is too small, fast algorithms have been recently presented in [3, 11, 19, 20], to which we also refer for further bibliographical references.

1.3. Overview of the paper

The paper divides into two parts: up to section 5 we gather definitions and design rather elementary (but new) algorithms for contact towers and sparse arithmetic, and from section 6 we focus on fast operations.

More precisely, the next section gathers notations and prerequisites about algorithms for multivariate polynomials and power series that are truncated with respect to a weighted valuation. In section 3 we design elementary algorithms for contact towers. We assume that algorithms are known for some $\mathbb{P}_h$ with $h < t$ and we reduce computations in $\mathbb{P}_t$ to operations in $\mathbb{P}_h$. Overall we achieve a product in $\mathbb{P}_t$ whose cost grows with 5^t times the square of the input of the multiplicands. The goal of the next sections is the construction of another tower that is isomorphic to $\mathbb{P}_t$ but with a sufficiently small height with respect to its degree D_t.

Let $\mathrm{in}(\Phi_i)$ represent the initial form of Φ_i, that is its homogenous component of lowest valuation. In section 4 we show how to compute a univariate representation of

$$\mathbb{K}((z))[\varphi_1, \ldots, \varphi_t]/(\mathrm{in}(\Phi_1), \ldots, \mathrm{in}(\Phi_t))$$

over

$$\mathbb{K}((z))[\varphi_1, \ldots, \varphi_h]/(\mathrm{in}(\Phi_1), \ldots, \mathrm{in}(\Phi_h))$$

in terms of an invertible primitive element of valuation R_t^{-1}. We will call this a *univariate-valued* representation in terms of a *primitive-valued* element[1.1]. In section 5 this representation is lifted at a prescribed relative precision ρ whenever

$$\rho \leqslant \min(\gamma_{h+1} - d_h\gamma_h, \gamma_{t+1} - d_t\gamma_t),$$

1.1. Such an element is sometimes called a uniformizing parameter or a local parameter. Our terminology tries to convey the idea that this is a primitive element both for the algebraic and valuative structures.

in order to obtain a univariate-valued representation of $\mathbb{P}_t$ over $\mathbb{P}_h$ at precision ρ.

We introduce flattenings in section 6: they consists in replacing consecutive levels of small degrees in a contact tower by a single level in a flattening. The problem is much more intricate than for algebraic towers [9]: a first type of flattening computes a univariate-valued representation, a second type is more straightforward to build but conversions to this representation induce a loss of precision. In addition we will design a specific fast flattened multiplication algorithm based on sparse arithmetic.

The different types of flattenings used in this article are presented in section 7. The first type will handle the case where $\rho \leqslant \gamma_{h+1} - d_h \gamma_h$ and $\rho \leqslant \gamma_{t+1} - d_t \gamma_t$ so $\Phi_h = 0$ and $\Phi_t = 0$ hold at relative precision ρ in $\mathbb{P}_t$. We will show that computing in $\mathbb{P}_t$ at relative precision ρ is equivalent to computing in $\mathbb{P}_t/(\varphi_{t+1})$. By means of the univariate-valued representation introduced in section 5, we will then construct an isomorphism between $\mathbb{P}_t/(\varphi_{t+1})$ and

$$(\mathbb{P}_h/(\varphi_{h+1}))[\tilde{\varphi}]/(\tilde{\Phi}(\varphi_1, \ldots, \varphi_h, \tilde{\varphi}))$$

where $\tilde{\varphi}$ is primitive-valued for $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$ and $\tilde{\Phi}$ is its minimal polynomial. It will be sufficient to perform these computations using a number of operations in $\mathbb{P}_h/(\varphi_{h+1})$ that remains polynomial in $D_h^{-1} D_t$. In fact $D_h^{-1} D_t$ represents the degree of the underlying flattening and it will be chosen of magnitude $O(D_t^{\epsilon})$, where ϵ can be fixed arbitrarily small. Conversions between $\mathbb{P}_t/(\varphi_{t+1})$ and $(\mathbb{P}_h/(\varphi_{h+1}))[\tilde{\varphi}]/(\tilde{\Phi}(\varphi_1, \ldots, \varphi_h, \tilde{\varphi}))$ will be performed without increasing the current precision ρ.

For the second type of flattening, we will replace $\mathbb{P}_t$ by $\mathbb{P}_h[\varphi_{t+1}]/(\tilde{\Phi}_t - \varphi_{t+1})$, where $\tilde{\Phi}_t$ is constructed as follows: $\tilde{\Phi}_{h+1} := \Phi_{h+1}$ and

$$\tilde{\Phi}_i(\varphi_1, \ldots, \varphi_{h+1}) := \Phi_i(\varphi_1, \ldots, \varphi_{h+1}, \tilde{\Phi}_{h+1}(\varphi_1, \ldots, \varphi_{h+1}), \ldots, \tilde{\Phi}_{i-1}(\varphi_1, \ldots, \varphi_{h+1})),$$

for $i = h+2, \ldots, t$. The conversions between $\mathbb{P}_t$ and $\mathbb{P}_h[\varphi_{t+1}]/(\tilde{\Phi}_t - \varphi_{t+1})$ will be done fast, but with a loss of precision of order $D_h^{-1} D_t \rho$. So, once again, this flattening will be used only when $D_h^{-1} D_t = O(D_t^{\epsilon})$. The special case where $h = 0$ was treated before in [11, section 3.5] and corresponds to conversions between contact and plain coordinates.

Finally, the top level algorithms are presented in section 8, where we describe a strategy to build efficient flattenings.

2. WEIGHTED POLYNOMIALS

In this section we first gather notations and known facts about weighted multivariate polynomials and series. Then we design fast algorithms for multiplying truncated weighted polynomials.

2.1. Notation

Let $\mathbb{L}$ be a commutative ring endowed with a (semi-)valuation v, whose valuation group is $R_0^{-1}\mathbb{Z}$ for some $R_0 \in \mathbb{N}^{>0}$. Let $\varphi_1, \ldots, \varphi_n$ be indeterminates. For any positive integers $l_1, \ldots, l_n$, we define

$$\mathbb{L}[\varphi_1, \ldots, \varphi_n]_{<(l_1, \ldots, l_n)} := \{P \in \mathbb{L}[\varphi_1, \ldots, \varphi_n] : \deg_{\varphi_1} P < l_1, \ldots, \deg_{\varphi_n} P < l_n\}.$$

For $i=1,\ldots,n$, we assign the weight $\gamma_i \in \mathbb{Q}^{>0}$ to φ_i and write val for the corresponding weighted valuation of $\mathbb{L}[\varphi_1,\ldots,\varphi_n]$, that is

$$\mathrm{val}(a\,\varphi_1^{e_1}\cdots\varphi_n^{e_n}) = v(a) + e_1\gamma_1 + \cdots + e_n\gamma_n,$$

for all $a \in \mathbb{L}$. As in the above context of contact towers (where $\mathbb{L}=\mathbb{K}((z))$ and $R_0=1$) we define

$$R_i^{-1}\mathbb{Z} := R_0^{-1}\mathbb{Z} + \gamma_1\mathbb{Z} + \cdots + \gamma_i\mathbb{Z}, \tag{2.1}$$

with $R_i \in \mathbb{N}$. Since R_{i-1} divides R_i we can set $r_i := R_i/R_{i-1} \in \mathbb{N}$ for $i=1,\ldots,n$. Given $\sigma \in \mathbb{Q}$ and $\rho \in \mathbb{Q}^{>0}$ we write

$$[\mathbb{L}[\varphi_1,\ldots,\varphi_n]]_{\sigma;\rho}$$

for the $\mathbb{L}$-module of polynomials of valuation $\geqslant\sigma$ that are defined up to valuation $\sigma+\rho$, which means that two polynomials coincide in $[\mathbb{L}[\varphi_1,\ldots,\varphi_n]]_{\sigma;\rho}$ whenever their difference has valuation $\geqslant\sigma+\rho$.

Since $d_i\gamma_i < \gamma_{i+1}$ for $i=1,\ldots,t$, we have $R_t\gamma_i \leqslant R_t\gamma_t$ and since the denominator of γ_i is R_i we have

$$\mathrm{ht}\,\gamma_i \leqslant \mathrm{ht}\,\gamma_t. \tag{2.2}$$

2.2. Sparse representation

A **sparse representation** of a polynomial P in $\mathbb{K}[\varphi_1,\ldots,\varphi_n]$ is a data structure that only stores the non-zero terms of P. The **support** of P is the set of its monomials having a non-zero coefficient. Each such term is a pair made of a coefficient and a degree vector. In an algebraic complexity model the bit size of the exponents counts for free, and the relevant size of such a polynomial is the cardinality of its support.

Consider two polynomials P and Q of $\mathbb{K}[\varphi_1,\ldots,\varphi_n]$ in sparse representation. An extensive literature exists about the general problem of multiplying P and Q; see [17] for a recent survey. In this paper, a superset $\mathcal{S}$ of the support of PQ will always be known and we will rely on the following classical result.

PROPOSITION 2.1. *Let $l_1,\ldots,l_n$ be positive integers and let $\theta \in \mathbb{K}$ be of multiplicative order $\geqslant l_1\cdots l_n$. Let $\mathcal{S}$ be a subset of $\{0,\ldots,l_1-1\}\times\cdots\times\{0,\ldots,l_n-1\}$, and let*

$$\Theta := (\theta, \theta^{l_1}, \theta^{l_1 l_2}, \ldots, \theta^{l_1\cdots l_{n-1}}).$$

1. *The value of Θ and the set $\mathcal{P}$ of all products $(\theta^{e_1}, \theta^{e_2 l_1}, \ldots, \theta^{e_n l_1\cdots l_{n-1}})$ for $(e_1,\ldots,e_n) \in \mathcal{S}$ can be computed using $O(|\mathcal{S}|\log(l_1\cdots l_n))$ operations in $\mathbb{K}$.*
2. *Assume that $\mathcal{P}$ has been precomputed. Let P be in $\mathbb{K}[\varphi_1,\ldots,\varphi_n]_{<(l_1,\ldots,l_n)}$, in sparse representation, and with a support included in $\mathcal{S}$. All the values of P at $\{\Theta^0,\Theta^1,\ldots,\Theta^{|\mathcal{S}|-1}\}$ can be computed using $\tilde{O}(|\mathcal{S}|)$ operations in $\mathbb{K}$.*
3. *Assume that $\mathcal{P}$ has been precomputed. Given $y_0,\ldots,y_{|\mathcal{S}|-1}$ in $\mathbb{K}$, there exists a unique polynomial P with support in $\mathcal{S}$ such that $P(\Theta^i)=y_i$, for $i=0,\ldots,|\mathcal{S}|-1$. This polynomial P can be computed using $\tilde{O}(|\mathcal{S}|)$ operations in $\mathbb{K}$.*

Proof. The first statement is straightforward by means of binary powering. The second and third ones are adapted from [8, section 5.2]. □

As said, handling supports of sparse polynomials does not matter from the algebraic complexity point of view. Nevertheless in the rest of this subsection we provide the reader with a few bit complexity bounds for building prescribed sparse supports but also for computing with sparse polynomials. The bit complexity is estimated for a RAM model over a fixed $\mathbb{Z}/N\mathbb{Z}$, as in [4]. These analyses aim at showing that the algebraic complexity bounds of this paper might be turned into bit complexity bounds. Yet a complete proof is out of the scope of this paper. We begin with the support of truncated polynomials in one variable.

LEMMA 2.2. *Let $\sigma \in R_1^{-1}\mathbb{Z}$, $\rho \in R_1^{-1}\mathbb{N}^{>0}$ and $l_1 \in r_1\mathbb{N}^{>0}$. Then there exists a subset*

$$\mathcal{S}_{\sigma,\rho,l_1} \subseteq \{0,\dots,l_1-1\}$$

of cardinality $\leqslant l_1 \min(R_0\rho, 1)$ such that for all polynomials

$$A = \sum_{0\leqslant i<l_1} A_i \varphi_1^i \in [\mathbb{L}[\varphi_1]_{<l_1}]_{\sigma;\rho}$$

we have $[A_i]_{\sigma-i\gamma_1;\rho} = 0$ whenever $i \notin \mathcal{S}_{\sigma,\rho,l_1}$. The set $\mathcal{S}_{\sigma,\rho,l_1}$ can be computed using

$$\tilde{O}(\log R_0 + \mathrm{ht}\,\sigma + \mathrm{ht}\,\rho + \mathrm{ht}\,\gamma_1) + \tilde{O}(l_1)\min(R_0\rho, 1)$$

bit operations.

Proof. If $R_0\rho \geqslant 1$ then we take $\mathcal{S} := \{0,\dots,l_1-1\}$. Otherwise there exists an integer $k \in \{1,\dots, r_1-1\}$ such that $\rho = k/R_1$. If $k = 1$, that is $\rho = 1/R_1$, then $[A_i]_{\sigma-i\gamma_1;\rho} = [A_i]_{\sigma-i\gamma_1}$ is zero whenever $\sigma - i\gamma_1 \notin R_0^{-1}\mathbb{Z}$, or equivalently whenever

$$R_1\sigma - iR_1\gamma_1 \notin r_1\mathbb{Z}. \tag{2.3}$$

By (2.1) we know that $R_1\gamma_1$ is coprime with r_1, so the condition (2.3) is further equivalent to $i \neq j \bmod r_1$, where

$$j := (R_1\gamma_1)^{-1} R_1\sigma \bmod r_1,$$

so we take

$$\mathcal{S}_{\sigma,\rho,l_1} := (j + r_1\mathbb{Z}) \cap \{0,\dots,l_1-1\}.$$

Since $l_1 \in r_1\mathbb{N}$ the cardinality of $\mathcal{S}_{\sigma,\rho,l_1}$ is $l_1/r_1 = R_0\rho\, l_1$. Computing the value of j takes $\tilde{O}(\log R_1 + \mathrm{ht}\,\sigma + \mathrm{ht}\,\gamma_1)$ bit operations. Then the construction of $\mathcal{S}_{\sigma,\rho,l_1}$ takes

$$O((l_1/r_1)\log l_1) = \tilde{O}(l_1)\min(R_0\rho, 1)$$

additional bit operations. If $k \geqslant 2$, then we take

$$\mathcal{S}_{\sigma,\rho,l_1} := \mathcal{S}_{\sigma,1/R_1,l_1} \cup \mathcal{S}_{\sigma+1/R_1,1/R_1,l_1} \cup \cdots \cup \mathcal{S}_{\sigma+(k-1)/R_1,1/R_1,l_1},$$

whose cardinality is $\leqslant kR_0 l_1/R_1 = R_0\rho\, l_1$. From the value of j computed for σ, we deduce the one for $\sigma + 1/R_1$ as $j + (R_1\gamma_1)^{-1} \bmod r_1$ using $O(\log r_1)$ bit operations, so the total time is as claimed. □

Here the support of a set of polynomials means the union of the supports of the polynomials in this set. So, Lemma 2.2 means that the support of $[\mathbb{L}[\varphi_1]_{<l_1}]_{\sigma;\rho}$ is a set of monomials in φ_1 of cardinality $\leqslant l_1 \min(R_0\rho, 1)$. We extend this result to several variables. Monomials in $\varphi_1,\dots,\varphi_n$ are represented by vectors in $\mathbb{N}^n$ and supports are sequences of monomials.

LEMMA 2.3. *Let $l_i \in r_i \mathbb{N}^{>0}$ for $i = 1, \ldots, n$, let $\sigma \in R_n^{-1} \mathbb{Z}$, and let $\rho \in R_n^{-1} \mathbb{N}^{>0}$. The support of $[\mathbb{L}[\varphi_1, \ldots, \varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma;\rho}$ has cardinality*

$$\leqslant l_1 \cdots l_n \min(R_0 \rho, 1)$$

and can be computed using

$$\tilde{O}(\operatorname{ht} \sigma + n \operatorname{ht} \gamma_n) + \tilde{O}(n l_1 \cdots l_n) \min(R_0 \rho, 1)$$

bit operations.

Proof. A homogeneous polynomial in $\mathbb{L}[\varphi_1]_{<l_1}$ has $\leqslant l_1 / r_1 = l_1 R_0 R_1^{-1}$ non-zero terms by Lemma 2.2. A straightforward induction on n yields that any homogeneous polynomial P in $\mathbb{L}[\varphi_1, \ldots, \varphi_n]_{<(l_1,\ldots,l_n)}$ has at most $\leqslant l_1 \cdots l_n R_0 R_n^{-1}$ non-zero terms.

If the polynomial P is not homogeneous and if $\rho = k / R_n < R_0^{-1}$, then the number of non-zero terms is $\leqslant l_1 \cdots l_n R_0 \rho$. If $R_0 \rho \geqslant 1$ then the bound on the number of monomials is clear.

In order to compute the support of $[\mathbb{L}[\varphi_1, \ldots, \varphi_n]_{<(l_1,\ldots,l_n)}]_\sigma$ we begin by computing $\Sigma := R_n \sigma \bmod R_n$, $s_i := l_i / r_i$, and $G_i = R_n \gamma_i \bmod R_n$, for $i = 1, \ldots, n$ using

$$\begin{aligned} & \tilde{O}(\operatorname{ht} \sigma + \operatorname{ht} \gamma_1 + \cdots + \operatorname{ht} \gamma_n + n \log R_n + \log(l_1 \cdots l_n)) \\ = \; & \tilde{O}(\operatorname{ht} \sigma + n \operatorname{ht} \gamma_n + n \log R_n + \log(l_1 \cdots l_n)) \end{aligned}$$

bit operations, by (2.2). Then $k_n := \operatorname{val}_{\varphi_n} P$ is the smallest nonnegative integer such that $\sigma - k_n \gamma_n \in R_{n-1}^{-1} \mathbb{Z}$ or equivalently that $\Sigma - G_n k_n \in r_n \mathbb{Z}$. By (2.1) we know that G_n is coprime with r_n, so we obtain

$$k_n := G_n^{-1} \Sigma \bmod r_n$$

in time $\tilde{O}(\log R_n)$. Without loss of generality we can replace σ by Σ / R_n and γ_i by G_i / R_n for computing supports. Let us write

$$P = \varphi_n^{k_n} (P_0 + P_1 \varphi_n^{r_n} + \cdots + P_{s_n - 1} \varphi_n^{(s_n - 1) r_n}),$$

where

$$P_i \in [\mathbb{L}[\varphi_1, \ldots, \varphi_{n-1}]_{<(l_1,\ldots,l_{n-1})}]_{\sigma - (i r_n + k_n)\gamma_n}.$$

Recursively we compute the support of P_i for $i = 0, \ldots, s_n - 1$, and deduce the support of P in time

$$O(s_n l_1 \cdots l_{n-1} R_0 R_{n-1}^{-1} \log(l_1 \cdots l_n)) = O(s_1 \cdots s_n R_0 \log(l_1 \cdots l_n)).$$

Let $\mathsf{C}(n)$ denote the cost for computing the support of a homogeneous polynomial in $\mathbb{L}[\varphi_1, \ldots, \varphi_n]_{<(l_1,\ldots,l_n)}$. We have shown that

$$\mathsf{C}(n) = s_n \mathsf{C}(n-1) + O(s_1 \cdots s_n R_0 \log(l_1 \cdots l_n)).$$

Unrolling this recurrence yields

$$\mathsf{C}(n) = O(n s_1 \cdots s_n R_0 \log(l_1 \cdots l_n)) = \tilde{O}(n l_1 \cdots l_n) R_0 R_n^{-1}.$$

For the next homogeneous component, of valuation $\sigma + R_n^{-1}$, we replace Σ by $(\Sigma + 1) \bmod R_n$ and restart the computation of the support. Consequently, for $\rho = k / R_n < R_0^{-1}$ we need to compute the support of k homogeneous polynomials. □

2.3. Truncated polynomials

For a truncated polynomial P in $[\mathbb{K}((z))[\varphi_1,...,\varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma;\rho}$ we use a mixed dense-sparse representation. Precisely, we store σ and the sequence of homogeneous components

$$([P]_{\sigma+i/R_n})_{i=0,\ldots,R_n\rho-1},$$

where each $[P]_{\sigma+i/R_n}$ is stored as the sparse representation of its specialization at $z=1$, that belongs to $\mathbb{K}[\varphi_1,\ldots,\varphi_n]_{<(l_1,\ldots,l_n)}$.

LEMMA 2.4. *Let $l_i \in r_i\,\mathbb{N}^{>0}$ for $i=1,\ldots,n$, let $\sigma \in R_n^{-1}\,\mathbb{Z}$, and let $\rho \in R_n^{-1}\,\mathbb{N}^{>0}$. The support with respect to $z,\varphi_1,\ldots,\varphi_n$ of $[\mathbb{K}((z))[\varphi_1,\ldots,\varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma;\rho}$ has cardinality $\leqslant l_1\cdots l_n\rho$ and can be computed using*

$$\tilde{O}(\operatorname{ht}\sigma + n\operatorname{ht}\gamma_n) + \tilde{O}(n\,l_1\cdots l_n)\,\rho$$

bit operations.

Proof. We adapt the proof of Lemma 2.3, with $R_0=1$. Let $P \in [\mathbb{K}((z))[\varphi_1,...,\varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma;\rho}$. Each homogeneous component of P has $\leqslant l_1\cdots l_n R_n^{-1}$ monomials in $\mathbb{K}[z,\varphi_1,\ldots,\varphi_n]$. A polynomial with relative precision ρ has $\leqslant R_n\rho$ homogeneous components. □

Given $\sigma \in R_n^{-1}\,\mathbb{Z}$ and $\rho \in R_n^{-1}\,\mathbb{N}^{>0}$, we will use the dense-sparse representation to multiply polynomials

$$A \in [\mathbb{K}((z))[\varphi_1,\ldots,\varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma_A;\rho} \text{ and } B \in [\mathbb{K}((z))[\varphi_1,\ldots,\varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma_B;\rho}$$

efficiently. Note that $AB \in [\mathbb{K}((z))[\varphi_1,\ldots,\varphi_n]_{<(2l_1-1,\ldots,2l_n-1)}]_{\sigma_A+\sigma_B;2\rho}$.

PROPOSITION 2.5. *Given $l_i \in r_i\,\mathbb{N}^{>0}$ for $i=1,\ldots,n$, two polynomials $A \in [\mathbb{K}((z))[\varphi_1,\ldots,\varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma_A;\rho}$ and $B \in [\mathbb{K}((z))[\varphi_1,\ldots,\varphi_n]_{<(l_1,\ldots,l_n)}]_{\sigma_B;\rho}$ can be multiplied using*

$$R_n^{-1}\,\tilde{O}(2^n l_1\cdots l_n R_n\rho)$$

operations in $\mathbb{K}$ and $\tilde{O}(\operatorname{ht}\sigma_A + \operatorname{ht}\sigma_B + \operatorname{ht}\gamma_n) + \tilde{O}(2^n l_1\cdots l_n)\,\rho$ bit operations.

Proof. Let $C := AB$, $\sigma_C := \sigma_A + \sigma_B$, and

$$\begin{aligned} I \;:=\; & \{\sigma_A, \sigma_A + R_n^{-1}, \ldots, \sigma_A + \rho - R_n^{-1}\} \cup \{\sigma_B, \sigma_B + R_n^{-1}, \ldots, \sigma_B + \rho - R_n^{-1}\} \\ & \cup \{\sigma_C, \sigma_C + R_n^{-1}, \ldots, \sigma_C + 2\rho - R_n^{-1}\}. \end{aligned}$$

For $i \in R_n^{-1}\,\mathbb{Z}$, we write $\mathcal{S}_i$ for the support of $[\mathbb{K}((z))[\varphi_1,...,\varphi_n]_{<(2l_1,\ldots,2l_n)}]_i$ where z is specialized at 1. Since $\mathcal{S}_i = \mathcal{S}_{i+1}$, it suffices to compute the $\mathcal{S}_i$ for $i \in I \bmod 1$. By Lemma 2.4, this takes

$$\begin{aligned} & \tilde{O}(\operatorname{ht}\sigma_A + \operatorname{ht}\sigma_B + \operatorname{ht}\gamma_1 + \cdots + \operatorname{ht}\gamma_n) + \tilde{O}(2^n l_1\cdots l_n)\,\rho \\ =\; & \tilde{O}(\operatorname{ht}\sigma_A + \operatorname{ht}\sigma_B + \operatorname{ht}\gamma_n) + \tilde{O}(2^n l_1\cdots l_n)\,\rho \qquad \text{(using (2.2))} \end{aligned}$$

bit operations, and we have $|\mathcal{S}_i| \leqslant 2^n l_1\cdots l_n R_n^{-1}$.

Assume that we are given an element $\theta \in \mathbb{K}$ of multiplicative order $\geqslant 2^n l_1\cdots l_n$, so we apply Proposition 2.1 with $2l_i$ instead of l_i. For each $i \in I \bmod 1$, we compute Θ and the set $\mathcal{D}_i$ corresponding to $\mathcal{S}_i$ using

$$O(2^n l_1\cdots l_n R_n^{-1}\log(2^n l_1\cdots l_n)) + \tilde{O}(2^n l_1\cdots l_n R_n^{-1}) = R_n^{-1}\,\tilde{O}(2^n l_1\cdots l_n)$$

operations in $\mathbb{K}$. Then we define

$$\bar{A}(t)(\varphi_1,\ldots,\varphi_n) = A(t, t^{\gamma_1}\varphi_1,\ldots,t^{\gamma_n}\varphi_n) = t^{\sigma_A} \sum_{0\leqslant i<R_n\rho} [A]_{\sigma_A+i/R_n}(1,\varphi_1,\ldots,\varphi_n)\, t^{i/R_n}$$

that belongs to $\mathbb{K}((t^{1/R_n}))[\varphi_1,\ldots,\varphi_n]$. We define $\bar{B}$ similarly. By Proposition 2.1 we compute $\bar{A}(t)(\Theta^j)$ and $\bar{B}(t)(\Theta^j)$ for $j=0,\ldots,|\mathcal{S}_i|-1$ using

$$\tilde{O}(2^n l_1\cdots l_n R_n^{-1})\, R_n\rho.$$

We compute $\bar{C}(t)(\Theta^j) = \bar{A}(t)(\Theta^j)\,\bar{B}(t)(\Theta^j)$ for $j=0,\ldots,|\mathcal{S}_i|-1$ at relative precision ρ using

$$O(2^n l_1\cdots l_n R_n^{-1})\,\tilde{O}(R_n\rho) = R_n^{-1}\tilde{O}(2^n l_1\cdots l_n R_n\rho)$$

operations in $\mathbb{K}$. Then we interpolate C from $\bar{C}$ using Proposition 2.1 again.

Finally, if we are not given an element $\theta\in\mathbb{K}$ of multiplicative order $\geqslant 2^n l_1\cdots l_n$, then we appeal to [12, Proposition A.2]: the overhead only induces logarithmic factors in the complexity bound. □

3. ELEMENTARY CONTACT ARITHMETIC

Given a contact tower as in Definition 1.1, we are interested in computing the product of two elements A and B in $\mathbb{P}_t$ with relative precision $\rho>0$. This section is devoted to relatively simple algorithms, on which the faster ones of section 7 will rely.

3.1. Generalized contact towers

As a first observation, since we are interested in computing with relative precision ρ in $\mathbb{P}_t$, we show that the defining polynomial $\Phi_i-\varphi_{i+1}$ can be replaced by Φ_i in the definition of $\mathbb{P}_t$ whenever $\gamma_{i+1}-d_i\gamma_i\geqslant\rho$ holds. For this purpose we introduce integers $\epsilon_1,\ldots,\epsilon_t$ in $\{0,1\}$ and the **generalized contact tower**

$$\mathbb{P}_i^\epsilon := \mathbb{K}((z))[\varphi_1,\ldots,\varphi_{i+1}]\,/\,(\Phi_1-\epsilon_1\varphi_2,\ldots,\Phi_i-\epsilon_i\varphi_{i+1}),\ \text{for } i=1,\ldots,t.$$

Generalized contact towers share many of the properties of contact towers. We gather the results needed in the sequel, along with brief proofs adapted from [11].

PROPOSITION 3.1. *For $i=1,\ldots,t$, any $P\in\mathbb{P}_i^\epsilon$ admits a unique representative of the form*

$$P = \sum_{k_1<d_1,\ldots,k_i<d_i,k_{i+1}\in\mathbb{N}} P_{k_1,\ldots,k_{i+1}}\varphi_1^{k_1}\cdots\varphi_{i+1}^{k_{i+1}} \in \mathbb{K}((z))[\varphi_1,\ldots,\varphi_i]_{<(d_1,\ldots,d_i)}[\varphi_{i+1}],$$

which we call the **canonical representative** *of P.*

Proof. Assume that the polynomial P, written as above, belongs to the ideal

$$I_i^\epsilon := (\Phi_1-\epsilon_1\varphi_2,\ldots,\Phi_i-\epsilon_i\varphi_{i+1}).$$

If P is not identically zero, then its initial form $\mathrm{in}(P;\mathbb{P}_i)$ is non-zero. The proof of [11, Lemma 3.7] extends to I_i^ϵ *mutatis mutandis* and gives us that

$$\mathrm{in}(I_i^\epsilon) = (\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_i)).$$

Finally [11, Lemma 3.4] implies that $\mathrm{in}(P;\mathbb{P}_i)$ must be zero, that is a contradiction. □

PROPOSITION 3.2. *For $i=1,\dots,t$ the map*

$$\begin{aligned} v(\cdot;\mathbb{P}_i^\epsilon):\quad \mathbb{P}_i^\epsilon &\to \mathbb{Z}+\mathbb{Z}\gamma_1+\cdots+\mathbb{Z}\gamma_{i+1}\cup\{\infty\}\\ P &\mapsto \min\{\mathrm{val}_z P_{k_1,\dots,k_{i+1}}+k_1\gamma_1+\cdots+k_{i+1}\gamma_{i+1} : k_1<d_1,\dots,k_i<d_i,k_{i+1}\in\mathbb{N}\}\end{aligned}$$

is a valuation of $\mathbb{P}_i^\epsilon$, that inherits the weighted grading of $\mathbb{K}((z))[[\varphi_1,\dots,\varphi_{t+1}]]$.

Proof. By routine adaptation of the proof of [11, Proposition 3.22]. □

The integer $R_i\in\mathbb{N}$ defined by

$$R_i^{-1}\mathbb{Z}=\mathbb{Z}+\gamma_1\mathbb{Z}+\cdots+\gamma_i\mathbb{Z}$$

is called the **ramification index** of $v(\cdot;\mathbb{P}_i)$ and $v(\cdot;\mathbb{P}_i^\epsilon)$, for $i=0,\dots,t+1$. From Definition 1.1 it is clear that R_i divides $d_1\cdots d_i$. By construction, R_{i-1} divides R_i, and

$$r_i := R_i/R_{i-1},$$

divides d_i, for $i=1,\dots,t$.

Elements in $\mathbb{P}_t^\epsilon$ will be called **generalized contact polynomials**. Such a polynomial P will be usually written

$$P=P_l\varphi_{t+1}^l+\cdots+P_1\varphi_{t+1}+P_0,$$

with $P_i\in\mathbb{K}((z))[\varphi_1,\dots,\varphi_t]_{<(d_1,\dots,d_t)}$ and $P_l\neq 0$. This is called the **contact representation** of P. The integer l is called the **degree** of P in φ_{t+1} and is written $\deg_{\varphi_{t+1}}P$. We will write $(\mathbb{P}_t^\epsilon)_{<l}$ for the set of contact polynomials of $\mathbb{P}_t^\epsilon$ of degree $<l$ in φ_{t+1}. A contact polynomial $P\in\mathbb{P}_t^\epsilon$ is said to be **clustered** if its canonical representative is monic in φ_{t+1} of degree $l\geqslant 1$ (that is $P_l\in\mathbb{K}$) and $v(P;\mathbb{P}_t^\epsilon)=l\gamma_{t+1}$. Note that Φ_i is clustered in $\mathbb{P}_{i-1}^\epsilon$.

Let A and B be contact polynomials in $\mathbb{P}_t^\epsilon$, if B is clustered of degree n, then there exist unique elements $Q_i\in(\mathbb{P}_t^\epsilon)_{<n}$ such that

$$A=\sum_{i\geqslant 0}Q_iB^i.$$

This decomposition is adapted from [11, Lemma 3.12] and yields a natural notion of division: there exists unique contact polynomials $R\in(\mathbb{P}_t^\epsilon)_{<n}$ and $Q\in\mathbb{P}_t^\epsilon$ such that

$$A=QB+R.$$

The **quotient** Q is written $A\,\mathrm{quo}_{\varphi_{t+1}}B$ and the **remainder** R is written $A\,\mathrm{rem}_{\varphi_{t+1}}B$.

Now let $A=\sum_{i\geqslant 0}A_i\varphi_{t+1}^i$ and $B=\sum_{i\geqslant 0}B_i\varphi_{t+1}^i$ be contact polynomials in $\mathbb{P}_t$ and let us compute their product $C=AB=\sum_{i\geqslant 0}C_i\varphi_{t+1}^i$, where

$$C_i := \sum_{k+l=i}A_kB_l\in(\mathbb{P}_t)_{<2}.$$

Each C_i writes canonically into $C_i=c_i+c_i'\Phi_t$ with c_i and c_i' in $\mathbb{P}_{t-1}$. Now if $\gamma_{t+1}-d_t\gamma_t\geqslant\rho$, then we have

$$[C_i;\mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)-i\gamma_{t+1};\rho}=[c_i;\mathbb{P}_{t-1}]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)-i\gamma_{t+1};\rho}.$$

In other words, computing $[AB;\mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho}$ in $\mathbb{P}_t$ is the same as in $\mathbb{P}_t^\epsilon$ when $\epsilon_1=\cdots=\epsilon_{t-1}=1$ and $\epsilon_t=0$. By decreasing induction on t, it follows that computing $[AB;\mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho}$ in $\mathbb{P}_t$ is the same as in $\mathbb{P}_t^\epsilon$ where we set $\epsilon_i:=0$ when $\gamma_{i+1}-d_i\gamma_i\geqslant\rho$, and $\epsilon_i:=1$ otherwise for $i=1,\dots,t$.

The rest of this section is devoted to rather elementary algorithms for multiplying elements in a generalized contact tower at a given relative precision ρ. In order to keep the notation simple, we drop the superscript ϵ for generalized contact towers. So, unless specified, contact towers will be of the generalized kind.

3.2. Cost functions

Given a clustered contact polynomial $F \in \mathbb{P}_t$ of degree $l \geqslant 1$ in φ_{t+1}, its **pre-inverse** will refer to the clustered contact polynomial $G \in \mathbb{P}_t$ of degree l in φ_{t+1} such that

$$FG \in \varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<l}.$$

Since $FH \notin \varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<l}$ holds for all $H \in (\mathbb{P}_t)_{<l}$, if a pre-inverse exists, then it is necessarily unique. The existence of pre-inverses is addressed in section 3.5. We introduce the following cost functions:

- $\mathsf{A}(d_1, \ldots, d_t, l; \rho)$ is a function that bounds the cost for adding two elements in $\mathbb{P}_t$ of degree $<l$ in φ_{t+1} with relative precision $\leqslant \rho$.
- $\mathsf{M}(d_1, \ldots, d_t, l; \rho)$ is a function that bounds the cost for multiplying two elements in $\mathbb{P}_t$ of degree $<l$ in φ_{t+1} with relative precision $\leqslant \rho$.
- $\mathsf{D}(d_1, \ldots, d_t, l; \rho)$ bounds the cost of a division in $\mathbb{P}_t$ of a contact polynomial of degree $<2l$ by a clustered contact polynomial of $\mathbb{P}_t$ of degree l with relative precision $\leqslant \rho$.
- $\mathsf{I}(d_1, \ldots, d_t, l; \rho)$ bounds the cost for computing the pre-inverse of a clustered contact polynomial in $\mathbb{P}_t$ of degree l in φ_{t+1} with relative precision $\leqslant \rho$.
- $\mathsf{B}(d_1, \ldots, d_t, l; \rho) := 2\,\mathsf{A}(d_1, \ldots, d_t, l; \rho) + \mathsf{M}(d_1, \ldots, d_t, l; \rho) + \mathsf{D}(d_1, \ldots, d_t, l; \rho)$.

LEMMA 3.3. *Without loss of generality, we may always assume that*

$$\mathsf{M}(d_1, \ldots, d_t, 1; \rho) \leqslant \mathsf{M}(d_1, \ldots, d_t; \rho) + \mathsf{D}(d_1, \ldots, d_t; \rho).$$

Proof. Let A and B be in $(\mathbb{P}_t)_{<1}$. Regarded in $(\mathbb{P}_{t-1})_{<d_t}$ their product $C = AB$ costs $\leqslant \mathsf{M}(d_1, \ldots, d_t; \rho)$. We divide C by Φ_t in $\mathbb{P}_{t-1}$ with $\leqslant \mathsf{D}(d_1, \ldots, d_t; \rho)$ operations. Let Q and R denote the resulting quotient Q and remainder, so $C = Q\Phi_t + R$. Since Q has valuation $v(A; \mathbb{P}_t) + v(B; \mathbb{P}_t) - d_t\gamma_t$, and since $\gamma_{t+1} > d_t\gamma_t$, we have

$$[AB; \mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho} = \epsilon_t\,[Q; \mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)-\gamma_{t+1};\rho}\,\varphi_{t+1} + [R; \mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho}. \qquad \square$$

LEMMA 3.4. *Let F be a clustered polynomial in $\mathbb{P}_t$ of degree l in φ_{t+1}, together with its pre-inverse G. For all $P \in (\mathbb{P}_t)_{<l}$ at relative precision $\rho > 0$, there exists a unique $U \in [(\mathbb{P}_t)_{<l}]_{v(P;\mathbb{P}_t);\rho}$ such that*

$$[P; \mathbb{P}_t]_{v(P;\mathbb{P}_t);\rho} = [(UF)\ \mathrm{quo}_{\varphi_{t+1}}\ \varphi_{t+1}^l; \mathbb{P}_t]_{v(P;\mathbb{P}_t);\rho}. \tag{3.1}$$

It is given by $U = [(GP)\ \mathrm{quo}_{\varphi_{t+1}}\ \varphi_{t+1}^l; \mathbb{P}_t]_{v(P;\mathbb{P}_t);\rho}$.

Proof. Equation (3.1) corresponds to searching for $U \in [(\mathbb{P}_t)_{<l}]_{v(P;\mathbb{P}_t);\rho}$ and $R \in [(\mathbb{P}_t)_{<l}]_{v(P;\mathbb{P}_t)+l\gamma_{t+1};\rho}$ such that

$$[UF; \mathbb{P}_t]_{v(P;\mathbb{P}_t)+l\gamma_{t+1};\rho} = [P\varphi_{t+1}^l + R; \mathbb{P}_t]_{v(P;\mathbb{P}_t)+l\gamma_{t+1};\rho},$$

which implies that

$$\begin{aligned} 0 &= [GP\varphi_{t+1}^l - UGF + GR; \mathbb{P}_t]_{v(P;\mathbb{P}_t)+2l\gamma_{t+1};\rho} \\ &\in [GP\varphi_{t+1}^l - U(\varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<l}) + GR; \mathbb{P}_t]_{v(P;\mathbb{P}_t)+2l\gamma_{t+1};\rho}, \end{aligned}$$

so $U = [(GP)\ \mathrm{quo}_{\varphi_{t+1}}\ \varphi_{t+1}^l; \mathbb{P}_t]_{v(P;\mathbb{P}_t);\rho}$ is the unique solution of Equation (3.1). □

3.3. Multiplication

The following simple multiplication algorithm in $\mathbb{P}_t$ makes use of operations in $\mathbb{P}_{t-1}$, whose cost functions are assumed to be as in section 3.2.

Algorithm 3.1

Input. $A = \sum_{i=0}^{l-1} A_i \varphi_{t+1}^i \in [\mathbb{P}_t]_{\sigma_A;\rho}$ and $B = \sum_{i=0}^{l-1} B_i \varphi_{t+1}^i \in [\mathbb{P}_t]_{\sigma_B;\rho}$ of degree $<l$ in φ_{t+1}.

Output. $[AB; \mathbb{P}_t]_{\sigma_A+\sigma_B;\rho}$.

1. For $i = 0, \ldots, 2l-2$
   compute $L_i + H_i \varphi_{t+1} := \sum_{k_A+k_B=i} [A_{k_A} B_{k_B}; \mathbb{P}_t]_{\sigma_A+\sigma_B-i\gamma_{t+1};\rho}$.
2. Return $L_0 + (H_0 + L_1)\varphi_{t+1} + \cdots + (H_{2l-3} + L_{2l-2})\varphi_{t+1}^{2l-2} + H_{2l-2}\varphi_{t+1}^{2l-1}$.

PROPOSITION 3.5. *Algorithm 3.1 is correct and performs*

$$\leqslant 2\,\mathsf{B}(d_1, \ldots, d_t; \max(R_t^{-1}, \rho))\ (\min(R_t\rho, 1)\, l)^2$$

operations in $\mathbb{K}$, *whenever* $\rho \in R_{t+1}^{-1}\mathbb{N}^{>0}$ *and* $l \in r_{t+1}\mathbb{N}^{>0}$.

Proof. The correctness is straightforward from the definitions. The number of non-zero terms in A is $\leqslant \min(R_t\rho, 1)\, l$ by Lemma 2.2. The number of non-zero products $A_{k_A} B_{k_B}$ performed in step 1 is therefore $\leqslant (\min(R_t\rho, 1)\, l)^2$, so this step costs

$$\leqslant (2\,\mathsf{A}(d_1, \ldots, d_t; \rho) + \mathsf{M}(d_1, \ldots, d_t; \rho) + \mathsf{D}(d_1, \ldots, d_t; \rho))\ (\min(R_t\rho, 1)\, l)^2$$

thanks to Lemma 3.3. Step 2 takes

$$\leqslant 2\,\mathsf{A}(d_1, \ldots, d_t; \rho)\min(R_t\rho, 1)\, l$$

operations in $\mathbb{K}$. Since $l \in r_{t+1}\mathbb{N}^{>0}$, we use $\min(R_t\rho, 1)\, l \geqslant 1$ in order to simply the final cost bound. □

3.4. Division

Let $F = \sum_{i=0}^{l} F_i \varphi_{t+1}^i \in \mathbb{P}_t$ be a clustered polynomial of degree l in φ_{t+1} and let $P \in (\mathbb{P}_t)_{<l}$. We address the computation of the quotient $P\ \mathrm{quo}_{\varphi_{t+1}} F$ and the remainder of $P\ \mathrm{rem}_{\varphi_{t+1}} F$ at relative precision $\rho \in R_{t+1}^{-1}\mathbb{N}^{>0}$. We assume that the pre-inverse $\varphi_{t+1} + g$ of $\varphi_{t+1} + F_{l-1}$ is at our disposal at relative precision ρ.

Algorithm 3.2

Input. A clustered polynomial $F \in [\mathbb{P}_t]_{l\gamma_{t+1};\rho}$ of degree l in φ_{t+1}, $P \in [(\mathbb{P}_t)_{<2l}]_{v(P;\mathbb{P}_t);\rho}$, and the pre-inverse $\varphi_{t+1} + g$ of $\varphi_{t+1} + F_{l-1}$ at relative precision ρ.

Output. $[P\ \mathrm{quo}_{\varphi_{t+1}} F; \mathbb{P}_t]_{v(P;\mathbb{P}_t)-l\gamma_{t+1};\rho}$ and $[P\ \mathrm{rem}_{\varphi_{t+1}} F; \mathbb{P}_t]_{v(P;\mathbb{P}_t);\rho}$.

1. Set $R := P$.

2. For i from $2l-1$ down to l do:
   a. Compute $Q_{i-l} := [((\varphi_{t+1}+g)\,R_i) \operatorname{quo} \varphi_{t+1}; \mathbb{P}_t]_{v(P;\mathbb{P}_t)-i\gamma_{t+1};\rho}$, where R_i represents the coefficient of φ_{t+1}^i in the contact representation of R;
   b. Replace R by $R - [Q_{i-l}\,\varphi_{t+1}^{i-l} F; \mathbb{P}_t]_{v(P;\mathbb{P}_t);\rho}$.
3. Return $\sum_{i=0}^{l-1} Q_i\,\varphi_{t+1}^i$ and R.

PROPOSITION 3.6. *Algorithm 3.2 is correct and performs*

$$\leqslant 2\,\mathsf{B}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))\,(\min(R_t\rho,1)\,l)^2$$

operations in $\mathbb{K}$ whenever $\rho \in R_{t+1}^{-1}\,\mathbb{N}^{>0}$ and $l \in r_{t+1}\,\mathbb{N}^{>0}$.

Proof. For a fixed value of i in step 2, by Lemma 3.4, we have

$$R_i = [Q_{i-l}\,(\varphi_{t+1}+F_{l-1}) \operatorname{quo} \varphi_{t+1}; \mathbb{P}_t]_{v(P;\mathbb{P}_t)-i\gamma_{t+1};\rho},$$

so the algorithm finishes with the expected quotient and remainder. The number of non-zero coefficients R_i encountered during step 2 is $\leqslant \min(R_t\rho,1)\,l$ by Lemma 2.2. According to Lemma 3.3, step 2.a costs $\leqslant \mathsf{B}(d_1,\ldots,d_t;\rho)$. Step 2.b costs

$$\leqslant \mathsf{B}(d_1,\ldots,d_t;\rho)\min(R_t\rho,1)\,l.$$

Finally we use $\min(R_t\rho,1)\,l \geqslant 1$. □

3.5. Pre-inverse

Given $F = \sum_{i=0}^{l} F_i\,\varphi_{t+1}^i \in \mathbb{P}_t$ clustered of degree l in φ_{t+1}, we wish to compute its pre-inverse G with relative precision ρ. We adapt the well-known method for power series inversion. The algorithm is recursive on the height t. If $t=0$ then the pre-inverse of φ_1+F_{l-1} is φ_1-F_{l-1} because $F_{l-1}\in\mathbb{K}((z))$.

LEMMA 3.7. *If g is the pre-inverse of Φ_t+F_{l-1} regarded as a clustered polynomial in $\mathbb{P}_{t-1}$ of degree d_t in φ_t and at relative precision ρ, then*

$$[\varphi_{t+1} - (g\,((F_{l-1}\Phi_t) \operatorname{quo}_{\varphi_t} \varphi_t^{d_t})) \operatorname{quo}_{\varphi_t} \varphi_t^{d_t}; \mathbb{P}_t]_{\gamma_{t+1};\rho}$$

is the pre-inverse of $\varphi_{t+1}+F_{l-1}$ at relative precision ρ.

Proof. Since $v(F_{l-1};\mathbb{P}_{t-1}) \geqslant \gamma_{t+1} > d_t\gamma_t$, Φ_t+F_{l-1} is clustered in $\mathbb{P}_{t-1}$, so g is well defined. Computing the pre-inverse of $\varphi_{t+1}+F_{l-1}$ means finding $u\in[(\mathbb{P}_t)_{<1}]_{\gamma_{t+1};\rho}$ such that

$$[(\varphi_{t+1}+u)\,(\varphi_{t+1}+F_{l-1}); \mathbb{P}_t]_{2\gamma_{t+1};\rho} \in \varphi_{t+1}^2 + (\mathbb{P}_t)_{<1}.$$

This condition is equivalent to

$$[\varphi_{t+1}\,(u+F_{l-1}) + u\,F_{l-1}; \mathbb{P}_t]_{2\gamma_{t+1};\rho} \in (\mathbb{P}_t)_{<1},$$

that is further equivalent to

$$[u+F_{l-1}; \mathbb{P}_{t-1}]_{\gamma_{t+1};\rho} = -[(u\,F_{l-1}) \operatorname{quo}_{\varphi_t} \Phi_t; \mathbb{P}_{t-1}]_{\gamma_{t+1};\rho},$$

in $\mathbb{P}_{t-1}$, then to

$$[F_{l-1}\,\Phi_t + u\,(\Phi_t+F_{l-1}); \mathbb{P}_{t-1}]_{\gamma_{t+1}+d_t\gamma_t;\rho} \in (\mathbb{P}_{t-1})_{<d_t},$$

and finally to

$$[(F_{l-1}\Phi_t)\ \mathrm{quo}_{\varphi_t}\varphi_t^{d_t};\mathbb{P}_{t-1}]_{\gamma_{t+1};\rho}=-[(u\,(\Phi_t+F_{l-1}))\ \mathrm{quo}_{\varphi_t}\varphi_t^{d_t};\mathbb{P}_{t-1}]_{\gamma_{t+1};\rho}.$$

From Lemma 3.4 we deduce that $u=-[(g\,((F_{l-1}\Phi_t)\ \mathrm{quo}_{\varphi_t}\varphi_t^{d_t}))\ \mathrm{quo}_{\varphi_t}\varphi_t^{d_t};\mathbb{P}_{t-1}]_{\gamma_{t+1};\rho}$. □

LEMMA 3.8. *Let $k\in\{1,\ldots,l-1\}$ and let $G\in\varphi_{t+1}^{l}+\varphi_{t+1}^{l-k}(\mathbb{P}_t)_{<k}$ be clustered of degree l in φ_{t+1} such that*

$$[FG;\mathbb{P}_t]_{2l\gamma_{t+1};\rho}\in\varphi_{t+1}^{2l}+(\mathbb{P}_t)_{<2l-k}.$$

There exists a unique $G_{l-(k+1)}\in[(\mathbb{P}_t)_{<1}]_{(k+1)\gamma_{t+1};\rho}$ such that

$$[F\,(G+G_{l-(k+1)}\varphi_{t+1}^{l-(k+1)});\mathbb{P}_t]_{2l\gamma_{t+1};\rho}\in\varphi_{t+1}^{2l}+(\mathbb{P}_t)_{<2l-(k+1)}.$$

It is given by

$$G_{l-(k+1)}:=-[(c\,(\varphi_{t+1}+G_{l-1}))\ \mathrm{quo}_{\varphi_{t+1}}\varphi_{t+1};\mathbb{P}_t]_{(k+1)\gamma_{t+1};\rho},$$

where G_{l-1} is the coefficient of φ_{t+1}^{l-1} in G and $c\in(\mathbb{P}_t)_{<1}$ is defined by

$$[FG;\mathbb{P}_t]_{2l\gamma_{t+1};\rho}=\varphi_{t+1}^{2l}+c\,\varphi_{t+1}^{2l-(k+1)}+(\mathbb{P}_t)_{<2l-(k+1)}.$$

Proof. From

$$F\,(G+G_{l-(k+1)}\varphi_{t+1}^{l-(k+1)})=FG+G_{l-(k+1)}\varphi_{t+1}^{l-(k+1)}F,$$

the condition for $G_{l-(k+1)}$ is equivalent to

$$[c+(G_{l-(k+1)}\,(\varphi_{t+1}+F_{l-1})\ \mathrm{quo}_{\varphi_{t+1}}\varphi_{t+1});\mathbb{P}_t]_{(k+1)\gamma_{t+1};\rho}\in(\mathbb{P}_t)_{<1}.$$

Since $\varphi_{t+1}+G_{l-1}$ is the pre-inverse of $\varphi_{t+1}+F_{l-1}$ at relative precision ρ, there exists a unique solution for $G_{l-(k+1)}$ given by Lemma 3.4. □

A straightforward induction based on the two latter lemmas shows that pre-inverses do exist.

PROPOSITION 3.9. *The pre-inverse of a clustered contact polynomial $F\in\mathbb{P}_t$ of degree $l\in r_{t+1}\,\mathbb{N}^{>0}$ in φ_{t+1} can be computed at relative precision $\rho\in R_{t+1}^{-1}\,\mathbb{N}^{>0}$ using*

$$\leqslant 4\,\mathsf{B}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))\,(\min(R_t\rho,1)\,l)^2+\mathsf{I}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))$$

operations in $\mathbb{K}$.

Proof. From Lemmas 3.7 and 3.3 we can compute the pre-inverse of

$$F\,\mathrm{quo}_{\varphi_{t+1}}\varphi_{t+1}^{l-1}=\varphi_{t+1}+F_{l-1}$$

at relative precision ρ using

$$\leqslant\mathsf{I}(d_1,\ldots,d_t;\rho)+2\,\mathsf{B}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))$$

operations in $\mathbb{K}$. By induction on k, suppose that the pre-inverse G of $F\,\mathrm{quo}_{\varphi_{t+1}}\varphi_{t+1}^{l-k}$ is known along with the product GF, for some $k\geqslant 1$ and still at relative precision ρ. Thanks to Lemma 3.8 we deduce the pre-inverse $\tilde{G}$ of $F\,\mathrm{quo}_{\varphi_{t+1}}\varphi_{t+1}^{l-(k+1)}$ in the form

$$\tilde{G}:=G\,\varphi_{t+1}+G_{l-(k+1)}$$

with a cost $\leqslant \mathsf{B}(d_1,\ldots,d_t;\rho)$. The product

$$\tilde{G}F = GF\varphi_{t+1} + G_{l-(k+1)}F$$

at relative precision ρ costs

$$\leqslant \mathsf{B}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))\min(R_t\rho,1)\,l.$$

By taking the sum of these costs for $k=1,\ldots,l-1$ and for when $G_{l-(k+1)}$ is known to be non-zero at relative precision ρ, we achieve the total bound

$$\begin{aligned}\leqslant\ & \mathsf{B}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))\,(\min(R_t\rho,1)\,l\,(\min(R_t\rho,1)\,l+1)+2)\\ &+\mathsf{I}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))\end{aligned}$$

for the pre-inverse of F. Finally we use $\min(R_t\rho,1)\,l\geqslant 1$ in order to simplify this bound. □

3.6. From height h to t

So far we have reduced operations in $\mathbb{P}_t$ to operations in $\mathbb{P}_{t-1}$. Now we proceed by induction in order to reduce operations in $\mathbb{P}_t$ to operations in $\mathbb{P}_h$ for any fixed $h<t$.

LEMMA 3.10. *For all $h\leqslant t$ and all $\rho>0$ we have*

$$\min(R_t\rho,1)\min(R_h\max(R_t^{-1},\rho),1)=\min(R_h\rho,1).$$

Proof. If $\rho<R_t^{-1}$ then

$$\min(R_t\rho,1)\min(R_h\max(R_t^{-1},\rho),1)=R_t\rho\min(R_t^{-1}R_h,1)=R_h\rho=\min(R_h\rho,1).$$

Otherwise we have $R_t^{-1}\leqslant\rho$, hence

$$\min(R_t\rho,1)\min(R_h\max(R_t^{-1},\rho),1)=\min(R_h\rho,1).$$ □

PROPOSITION 3.11. *Let $h\in\{0,\ldots,t\}$, $\rho\in R_{t+1}^{-1}\mathbb{N}^{>0}$, $l\in r_{t+1}\mathbb{N}^{>0}$, and let $F\in\mathbb{P}_t$ be a clustered polynomial of degree l in φ_{t+1}. Let $\Phi_{i,d_i-1}\in(\mathbb{P}_i)_{<1}$ denote the coefficient of $\varphi_{i+1}^{d_i-1}$ in Φ_i. Then the pre-inverses of $\varphi_{h+1}+\Phi_{h+1,d_{h+1}-1},\ldots,\varphi_t+\Phi_{t,d_t-1}$, $\varphi_{t+1}+F_{l-1}$ can be obtained with a cost*

$$\begin{aligned}\leqslant\ & 5^{t-h+1}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\ &+\mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(t-h+1).\end{aligned}$$

Once these pre-inverses are known, we may compute in $\mathbb{P}_t$ with the cost bound

$$\mathsf{B}(d_1,\ldots,d_t,l;\rho)\leqslant 5^{t-h+1}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\rho,1)\,d_{h+1}\cdots d_t\,l)^2,$$

where underlying divisions in φ_{t+1} are only allowed by F.

In addition, given the pre-inverses of $\varphi_{h+1}+\Phi_{h+1,d_{h+1}-1},\ldots,\varphi_t+\Phi_{t,d_t-1}$ we have

$$\begin{aligned}\mathsf{I}(d_1,\ldots,d_t,l;\rho)\ \leqslant\ & 5^{t-h+1}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\rho,1)\,d_{h+1}\cdots d_t\,l)^2\\ &+\mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho)).\end{aligned}$$

Proof. From Proposition 3.5 we may take

$$\mathsf{M}(d_1,\ldots,d_t,l;\rho)\leqslant 2\,\mathsf{B}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))\,(\min(R_t\rho,1)\,l)^2.$$

Assuming that the pre-inverse of $\varphi_{t+1}+F_{l-1}$ is known, thanks to Proposition 3.6, for divisions by F, we may take

$$\mathsf{D}(d_1,\dots,d_t,l;\rho)\leqslant 2\,\mathsf{B}(d_1,\dots,d_t;\max(R_t^{-1},\rho))\,(\min(R_t\rho,1)\,l)^2.$$

From Lemma 2.2 we straightforwardly obtain

$$\mathsf{A}(d_1,\dots,d_t,l;\rho)\leqslant \mathsf{A}(d_1,\dots,d_t;\max(R_t^{-1},\rho))\min(R_t\rho,1)\,l.$$

By summing these three inequalities and using $\min(R_t\rho,1)\,l\geqslant 1$, we deduce

$$\mathsf{B}(d_1,\dots,d_t,l;\rho)\leqslant 5\,\mathsf{B}(d_1,\dots,d_t;\max(R_t^{-1},\rho))\,(\min(R_t\rho,1)\,l)^2.$$

By unrolling the latter inequality and using Lemma 3.10, we obtain that

$$\begin{aligned}
&\mathsf{B}(d_1,\dots,d_t,l;\rho)\\
\leqslant\ & 5^2\,\mathsf{B}(d_1,\dots,d_{t-1};\max(R_{t-1}^{-1},\rho))\,(\min(R_{t-1}\max(R_t^{-1},\rho),1)\,d_t\min(R_t\rho,1)\,l)^2\\
\leqslant\ & 5^2\,\mathsf{B}(d_1,\dots,d_{t-1};\max(R_{t-1}^{-1},\rho))\,(\min(R_{t-1}\rho,1)\,d_t\,l)^2\\
\vdots\\
\leqslant\ & 5^{t-h+1}\,\mathsf{B}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\rho,1)\,d_{h+1}\cdots d_t\,l)^2,
\end{aligned}\tag{3.2}$$

whenever the pre-inverses of $\varphi_{h+1}+\Phi_{h+1,d_{h+1}-1}$, …, $\varphi_t+\Phi_{t,d_t-1}$, $\varphi_{t+1}+F_{l-1}$ are known.

From Proposition 3.9 we know that

$$\mathsf{I}(d_1,\dots,d_t,l;\rho)\leqslant 4\,\mathsf{B}(d_1,\dots,d_t;\max(R_t^{-1},\rho))\,(\min(R_t\rho,1)\,l)^2+\mathsf{I}(d_1,\dots,d_t;\max(R_t^{-1},\rho)).$$

By using (3.2) and Lemma 3.10 we deduce that

$$\begin{aligned}
&\mathsf{I}(d_1,\dots,d_t,l;\rho)\\
\leqslant\ & 4\times 5^{t-h}\,\mathsf{B}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\,(\min(R_t\rho,1)\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t\,l)^2\\
&\quad+\mathsf{I}(d_1,\dots,d_t;\max(R_t^{-1},\rho))\\
\leqslant\ & 4\times 5^{t-h}\,\mathsf{B}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\rho,1)\,d_{h+1}\cdots d_t\,l)^2\\
&\quad+\mathsf{I}(d_1,\dots,d_t;\max(R_t^{-1},\rho)).
\end{aligned}$$

Iterating the latter inequality yields

$$\begin{aligned}
&\mathsf{I}(d_1,\dots,d_t,l;\rho)\\
\leqslant\ & 4\,\mathsf{B}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\\
&\quad\times(5^{t-h}(\min(R_h\max(R_{t+1}^{-1},\rho),1)\,d_{h+1}\cdots d_t\,l)^2+\cdots+5\,(\min(R_h\max(R_{h+1}^{-1},\rho),1)\,d_{h+1})^2)\\
&\qquad+\mathsf{I}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\\
\leqslant\ & 4\,\mathsf{B}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\\
&\quad\times(5^{t-h}(\min(R_h\rho,1)\,d_{h+1}\cdots d_t\,l)^2+\cdots+5\,(\min(R_h\rho,1)\,d_{h+1}\cdots d_t\,l)^2)\\
&\qquad+\mathsf{I}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\\
\leqslant\ & 5^{t-h+1}\,\mathsf{B}(d_1,\dots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\rho,1)\,d_{h+1}\cdots d_t\,l)^2\\
&\quad+\mathsf{I}(d_1,\dots,d_h;\max(R_h^{-1},\rho)).
\end{aligned}\tag{3.3}$$

From Lemmas 3.3 and 3.7 the pre-inverse of $\varphi_{t+1}+F_{l-1}$ is obtained at relative precision ρ using

$$\leqslant\mathsf{I}(d_1,\dots,d_t;\max(R_t^{-1},\rho))+2\,\mathsf{B}(d_1,\dots,d_t;\max(R_t^{-1},\rho))$$

operations in $\mathbb{K}$. Consequently, the cost for obtaining the pre-inverses of $\varphi_{h+1} + \Phi_{h+1,d_{h+1}-1}, \ldots, \varphi_t + \Phi_{t,d_t-1}, \varphi_{t+1} + F_{l-1}$ is

$$
\begin{aligned}
&\leqslant \mathsf{I}(d_1,\ldots,d_t;\max(R_t^{-1},\rho)) + \cdots + \mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\quad + 2\,\mathsf{B}(d_1,\ldots,d_t;\max(R_t^{-1},\rho)) + \cdots + 2\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\leqslant 5^{t-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\
&\quad + \mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\quad \cdots\\
&\quad + 5\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_h^{-1},\rho),1)\,d_{h+1})^2\\
&\quad + \mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho)) \qquad \text{(by using (3.3))}\\
&\quad + \mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\quad + 2\times 5^{t-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\
&\quad \cdots\\
&\quad + 2\times 5\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_{h+1}^{-1},\rho),1)\,d_{h+1})^2\\
&\quad + 2\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho)) \qquad \text{(by using (3.2))}\\
&\leqslant 5^{t-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\
&\quad + \mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\quad \cdots\\
&\quad + 5\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\
&\quad + \mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\quad + \mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\quad + 2\times 5^{t-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\
&\quad \cdots\\
&\quad + 2\times 5\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\
&\quad + 2\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\\
&\leqslant 5^{t-h+1}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\max(R_t^{-1},\rho),1)\,d_{h+1}\cdots d_t)^2\\
&\quad + (t-h+1)\,\mathsf{I}(d_1,\ldots,d_h;\max(R_h^{-1},\rho)),
\end{aligned}
$$

which concludes the proof. □

3.7. Fast division

So far we have designed rather elementary algorithms for contact towers, that will be useful to section 7. Computing pre-inverses faster will be useful as well. The following lemma is adapted from the usual fast power series inversion method.

LEMMA 3.12. *Let F and G be clustered monic contact polynomials of $\mathbb{P}_t$ of degree l in φ_{t+1} and let $k \leqslant l$ be such that*

$$[FG;\mathbb{P}_t]_{2l\gamma_{t+1};\rho} \in \varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<2l-k}.$$

Then for any $e \leqslant k$, $G \operatorname{quo} \varphi_{t+1}^{l-e}$ is the pre-inverse of $F \operatorname{quo} \varphi_{t+1}^{l-e}$ at precision ρ.

Proof. Let $F_1 := F \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{l-e}$, $F_0 := F \operatorname{rem}_{\varphi_{t+1}} \varphi_{t+1}^{l-e}$, $G_1 := G \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{l-e}$, $G_0 := G \operatorname{rem}_{\varphi_{t+1}} \varphi_{t+1}^{l-e}$. From

$$[(F_1\varphi_{t+1}^{l-e} + F_0)\,(G_1\varphi_{t+1}^{l-e} + G_0);\mathbb{P}_t]_{2l\gamma_{t+1};\rho} \in \varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<2l-k},$$

we obtain

$$[F_1 G_1 \varphi_{t+1}^{2(l-e)} + (F_1 G_0 + F_0 G_1)\, \varphi_{t+1}^{l-e} + F_0 G_0; \mathbb{P}_t]_{2l\gamma_{t+1};\rho} \in \varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<2l-k}.$$

Since $\deg_{\varphi_{t+1}}(F_1 G_0 + F_0 G_1) < l$ and $\deg_{\varphi_{t+1}}(F_0 G_0) < 2\,(l-e)$, we deduce that

$$[F_1 G_1; \mathbb{P}_t]_{2e\gamma_{t+1};\rho} \in \varphi_{t+1}^{2e} + (\mathbb{P}_t)_{<2e-k}.$$

The conclusion follows from $2e - k \leqslant e$. □

LEMMA 3.13. *Let $k \in \{1, \ldots, l-1\}$, let $K := \min(2k, l)$, and let $G \in \mathbb{P}_t$ be clustered of degree l in φ_{t+1} such that*

$$[FG; \mathbb{P}_t]_{2l\gamma_{t+1};\rho} \in \varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<2l-k}.$$

There exists a unique $\tilde{G} \in [(\mathbb{P}_t)_{<K-k}]_{K\gamma_{t+1};\rho}$ such that

$$[F\,(G + \tilde{G}\,\varphi_{t+1}^{l-K}); \mathbb{P}_t]_{2l\gamma_{t+1};\rho} \in \varphi_{t+1}^{2l} + (\mathbb{P}_t)_{<2l-K}.$$

It is given by

$$\tilde{G} = [((G \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{l-(K-k)})\, C) \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{K-k}; \mathbb{P}_t]_{K\gamma_{t+1};\rho},$$

where $C \in (\mathbb{P}_t)_{<K-k}$ is defined by

$$[FG; \mathbb{P}_t]_{2l\gamma_{t+1};\rho} = \varphi_{t+1}^{2l} + C\,\varphi_{t+1}^{2l-K} + (\mathbb{P}_t)_{<2l-K}.$$

Proof. From

$$F\,(G + \tilde{G}\,\varphi_{t+1}^{l-K}) = FG + F\tilde{G}\,\varphi_{t+1}^{l-K},$$

the condition for $\tilde{G}$ becomes

$$[C\,\varphi_{t+1}^{l} + F\tilde{G}; \mathbb{P}_t]_{(l+K)\gamma_{t+1};\rho} \in (\mathbb{P}_t)_{<l}$$

and then

$$C = [((F \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{l-(K-k)})\, \tilde{G}) \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{K-k}; \mathbb{P}_t]_{K\gamma_{t+1};\rho}.$$

By Lemma 3.12, $G \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{l-(K-k)}$ is the pre-inverse of $F \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{l-(K-k)}$ at relative precision ρ. There exists a unique solution for $\tilde{G}$ given by Lemma 3.4. □

PROPOSITION 3.14. *The pre-inverse of a clustered contact polynomial $F \in \mathbb{P}_t$ of degree l in φ_{t+1} can be computed at relative precision $\rho \in R_{t+1}^{-1}\,\mathbb{N}^{>0}$ using*

$$O(\mathsf{M}(d_1, \ldots, d_t, l; \rho) \log l) + \mathsf{I}(d_1, \ldots, d_t; \max(R_t^{-1}, \rho))$$

operations in $\mathbb{K}$ whenever $l \in r_{t+1}\,\mathbb{N}^{>0}$.

Proof. From Lemma 3.7 we can compute the pre-inverse of

$$F \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{l-1} = \varphi_{t+1} + F_{l-1}$$

at relative precision ρ using

$$\leqslant \mathsf{I}(d_1, \ldots, d_t; \max(R_t^{-1}, \rho)) + O(\mathsf{M}(d_1, \ldots, d_t, l; \rho) + \mathsf{A}(d_1, \ldots, d_t, l; \rho))$$

operations in $\mathbb{K}$. This makes it possible to apply Lemma 3.13 $O(\log l)$ times, with $k = 1, 2, 4, \ldots$, in order to obtain the pre-inverse of F using

$$O(\mathsf{M}(d_1, \ldots, d_t, l; \rho) \log l)$$

operations in $\mathbb{K}$. □

As for usual polynomials, pre-inverses are used to reduce divisions to multiplications.

LEMMA 3.15. *Let F be a clustered monic contact polynomials of $\mathbb{P}_t$ of degree l in φ_{t+1}, let G be its pre-inverse, and let $A \in (\mathbb{P}_t)_{<2l}$. The quotient $Q := A \operatorname{quo}_{\varphi_{t+1}} F$ can be computed as*

$$Q = GA \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{2l}.$$

Proof. Let $W := GF - \varphi_{t+1}^{2l} \in (\mathbb{P}_t)_{<l}$, and let $R := A \operatorname{rem}_{\varphi_{t+1}} F$, so we have

$$A = QF + R.$$

By multiplying both sides of this equality by G we obtain

$$GA = QGF + GR = Q(\varphi_{t+1}^{2l} + W) + GR = Q\varphi_{t+1}^{2l} + QW + GR,$$

whence $Q = GA \operatorname{quo}_{\varphi_{t+1}} \varphi_{t+1}^{2l}$. □

PROPOSITION 3.16. *Let F be a clustered monic contact polynomial of $\mathbb{P}_t$ of degree $l \in r_{t+1}\mathbb{N}^{>0}$ in φ_{t+1} and given at precision $\rho \in R_{t+1}^{-1}\mathbb{N}^{>0}$. Given the pre-inverse G of F at precision ρ, the division of a contact polynomial of $(\mathbb{P}_t)_{<2l}$ at precision ρ costs*

$$O(\mathsf{M}(d_1, \ldots, d_t, l; \rho) + \mathsf{A}(d_1, \ldots, d_t, l; \rho)).$$

Proof. This follows from Lemma 3.15. □

4. INITIAL PRIMITIVE-VALUED REPRESENTATION

Throughout this section, $(\mathbb{P}_i)_{i \leqslant t}$ represents a generalized contact tower as in Definition 1.1 and $h < t$ is a fixed integer. We will assume that $\epsilon_h = \epsilon_t = 0$ so that $\mathbb{K}((z)) \subseteq \mathbb{P}_h/(\varphi_{h+1}) \subseteq \mathbb{P}_t/(\varphi_{t+1})$ is a tower of algebraic extensions. One important question is how to compute efficiently in $\mathbb{P}_t/(\varphi_{t+1})$, provided that we know how to compute efficiently in $\mathbb{P}_h/(\varphi_h)$. We will achieve this by representing elements in $\mathbb{P}_t/(\varphi_{t+1})$ as follows.

DEFINITION 4.1. *A* **univariate-valued representation** *of $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$ at precision $\rho \in R_t^{-1}\mathbb{N}^{>0}$ is made of the following data:*

- *a homogeneous primitive element ϖ of $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$ of valuation R_t^{-1},*
- *an initially separable monic polynomial $\chi(T) \in (\mathbb{P}_h/(\varphi_{h+1}))[T]$ of degree $D_h^{-1}D_t$, of valuation $(D_h^{-1}D_t)R_t^{-1}$ at relative precision ρ, where T has valuation R_t^{-1},*
- *polynomials $w_{h+1}(T), \ldots, w_t(T)$ in $(\mathbb{P}_h/(\varphi_{h+1}))[T]_{<D_h^{-1}D_t}$ of valuations $\gamma_{h+1}, \ldots, \gamma_t$ and at relative precision ρ.*

These data satisfy the following properties:

- $[(\varpi(\varphi_1, \ldots, \varphi_h, w_{h+1}(T), \ldots, w_t(T)) - T) \operatorname{rem} \chi(T)]_{R_t^{-1};\rho} = 0$,
- $[\chi(\varpi); \mathbb{P}_t]_{(D_h^{-1}D_t)R_t^{-1};\rho} = 0$,
- $[(\Phi_i(\varphi_1, \ldots, \varphi_h, w_{h+1}(T), \ldots, w_t(T)) - \epsilon_i w_{i+1}(T)) \operatorname{rem} \chi(T)]_{d_i\gamma_i;\rho} = 0$, *for* $i = h+1, \ldots, t$.

Any element of $\mathbb{P}_t/(\varphi_{t+1})$ can uniquely be represented as an element of $\mathbb{P}_h/(\varphi_{h+1})[T]/(\chi(T))$ via the following isomorphism:

$$\begin{aligned}\mathbb{P}_h/(\varphi_{h+1})[T]/(\chi(T)) &\cong \mathbb{P}_t/(\varphi_{t+1})\\ T &\mapsto \varpi\\ w_i(T) &\leftarrow \varphi_i \text{ for } i=h+1,\ldots,t.\end{aligned}$$

In this section, we focus on the computation of an *initial primitive-valued representation*, which is simply a univariate-valued representation of minimal precision $\rho = R_t^{-1}$. For this purpose, we define

$$\mathbb{I}_i := \mathbb{K}((z))[\varphi_1,\ldots,\varphi_i]/(\mathrm{in}(\Phi_1),\ldots,\mathrm{in}(\Phi_i)),$$

for $i=1,\ldots,t$. Computing an initial univariate-valued representation of $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$ essentially amounts to computing a homogeneous element ϖ in $\mathbb{I}_t$ of valuation R_t^{-1} such that the map

$$\begin{aligned}\mathbb{I}_h[T] &\to \mathbb{I}_t\\ T &\mapsto \varpi\end{aligned}$$

is surjective. We call such a ϖ a *primitive-valued element* of $\mathbb{I}_t$ over $\mathbb{I}_h$. Its minimal polynomial χ over $\mathbb{I}_h$ is the monic generator of the kernel of this map. It is homogeneous of degree $D_h^{-1}D_t$. The surjectivity further implies the existence of homogeneous polynomials $w_{h+1},\ldots,w_t$ in $\mathbb{I}_h[T]_{<D_h^{-1}D_t}$ such that $\varphi_i = w_i(\varpi)$ holds for $i=h+1,\ldots,t$. These polynomials are obtained as a byproduct of the computation of ϖ and, together with ϖ, give rise to the desired initial univariate-valued representation.

It is classical that $\mathbb{I}_t$ is isomorphic to an algebra of the form $\mathbb{A}_t((z))[T]/(T^{R_t}-\zeta T)$, where $\mathbb{A}_t$ is an algebraic extension of $\mathbb{K}$ and $\zeta\in\mathbb{A}_t$; see [11, section 6]. On the level of coefficients, we are therefore led to compute in so-called algebraic towers $(\mathbb{A}_i)_{i\leqslant t}$ over $\mathbb{K}$. Some relevant complexity results for such computations are recalled in section 4.1.

Now direct computations in $\mathbb{A}_t((z))[T]/(T^{R_t}-\zeta T)$ can become expensive for towers of large heights, since every next floor gives rise to a constant overhead. This explains the interest of doing relative computations of $\mathbb{I}_t$ over $\mathbb{I}_h$: using the univariate-valued representation, this will allow us to bundle all floors between level h and t into a single univariate extension, for which we can use fast univariate arithmetic, in the same spirit as the accelerated tower arithmetic from [9]. In section 4.2, we first construct an isomorphism Υ of the form $\mathbb{I}_t \cong \dot{\mathbb{A}}_t((z))[T_h,T_t]/\left(T_h^{R_h}-\rho_h z, T_t^{R_h^{-1}R_t}-\zeta_t T_h\right)$, where $\rho_h\in\mathbb{A}_h$ and $\rho_t\in\dot{\mathbb{A}}_t$. Here $\dot{\mathbb{A}}_t$ is a primitive algebraic extension of $\mathbb{A}_h$ that is isomorphic to $\mathbb{A}_t$ (in particular, computations in $\dot{\mathbb{A}}_t$ will be more efficient than computations in $\mathbb{A}_t$).

A natural candidate for a primitive-valued ϖ for $\mathbb{I}_t$ over $\mathbb{I}_h$ is $\Upsilon^{-1}(T_t)$. Although this element is not always primitive, as we shall show in section 4.3, it turns out that we may always take $\varpi := \Upsilon^{-1}(\theta T_t)$ for some suitable value of θ in $\dot{\mathbb{A}}_t$. In section 4.4 we show how to compute $\chi, w_{h+1},\ldots,w_t$, and derive the desired initial primitive-valued representation of $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$.

Remark 4.2. From a mathematical perspective, it is not essential that ϖ be homogeneous in Definition 4.1. Nonetheless, this is naturally the case for initial primitive-valued representations, and this property also simplifies computations. Furthermore, it turns out that we can keep the same primitive-valued element ϖ when lifting our representation to higher precisions, as we will show in section 5 below.

4.1. Separable algebraic towers

A **separable (algebraic) tower** over $\mathbb{K}$ is a sequence $(\mathbb{A}_i)_{i\leqslant t}$ with $\mathbb{A}_0 := \mathbb{K}$ and

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

where the $\mu_i(x_i) \in \mathbb{A}_{i-1}[x_i]$ are monic separable polynomials. We write α_i for the image of x_i in $\mathbb{A}_i$ and set $s_i := \deg \mu_i$ for $i=1,\ldots,t$. We will write

$$S_i := s_1 \cdots s_i$$

for the degree of $\mathbb{A}_i$ over $\mathbb{K}$. The tower is said to be **effectively separable** when we are further given u_i and v_i in $\mathbb{A}_{i-1}[x_i]$ of respective degree $<\deg \mu_i$ and $<\deg \mu_i - 1$ such that the Bézout relation

$$1 = u_i \mu_i' + v_i \mu_i$$

holds, for $i=1,\ldots,t$. Throughout the rest of this paper, without loss of generality, we will freely assume that such towers are simplified so that $s_i \geqslant 2$ holds for $i=1,\ldots,t$. The cardinality of $\mathbb{K}$ will be written card $\mathbb{K}$. We will rely on the following complexity bound.

PROPOSITION 4.3. *Let $\epsilon < 1/2$ be a fixed positive constant, that can be taken arbitrarily close to 0. Given an explicitly separable tower $(\mathbb{A}_i)_{i\leqslant t}$, one multiplication and one inversion (when the inverse exists) in $\mathbb{A}_t$ costs*

$$\tilde{O}(S_t^{1+\epsilon})$$

operations in $\mathbb{K}$.

Proof. If card $\mathbb{K} > \binom{S_t}{2}$, then the result directly follows from [10, Theorem 4]. Otherwise, with the notation of [10, section 7], we observe that the assumption on card $\mathbb{K}$ is only needed to build primitive tower representations of degree $<\delta = O(S_t^{\epsilon})$, so it is sufficient to assume card $\mathbb{K} > \binom{\delta}{2}$ instead. After that, if card $\mathbb{K} \leqslant \binom{\delta}{2} \leqslant S_t$, then we appeal to [12, Proposition A.2]: the overhead only induces logarithmic factors in the complexity bound. □

The next lemma addresses the complexity for obtaining a univariate representation of $\mathbb{A}_t$ over $\mathbb{A}_h$ for a given $h<t$. For the purpose of this paper, this complexity bound does not need to be sharp because $S_h^{-1} S_t$ will be taken relatively small.

LEMMA 4.4. *Let $h<t$ and assume* card $\mathbb{K} > \binom{S_h^{-1} S_t}{2}$. *There exist $\nu_{h+1},\ldots,\nu_t$ in $\mathbb{A}_h$, $\Xi \in \mathbb{A}_h[U]$ separable and monic of degree $S_h^{-1} S_t$, and $A_{h+1},\ldots,A_t \in \mathbb{A}_h[U]_{<S_h^{-1}S_t}$ such that*

$$\begin{aligned} \mathbb{A}_t &\to \dot{\mathbb{A}}_t := \mathbb{A}_h[U]/(\Xi(U)) \\ \alpha_i &\mapsto A_i(U) \text{ for } i=h+1,\ldots,t \end{aligned}$$

is an $\mathbb{A}_h$-algebra isomorphism and that

$$(\nu_{h+1} A_{h+1}(U) + \cdots + \nu_t A_t(U) - U) \operatorname{rem} \Xi(U) = 0.$$

In addition, if we are given $> \binom{S_h^{-1} S_t}{2}$ distinct elements in $\mathbb{K}$, then such a **univariate representation** *$\nu_{h+1},\ldots,\nu_t$, Ξ, $A_{h+1},\ldots,A_t$ of $\mathbb{A}_t$ over $\mathbb{A}_h$ can be computed using*

$$\tilde{O}(S_h^{1+\epsilon} (S_h^{-1} S_t)^3)$$

operations in $\mathbb{K}$. One conversion between $\mathbb{A}_t$ and $\dot{\mathbb{A}}_t$ costs $\tilde{O}(S_h^{1+\epsilon} (S_h^{-1} S_t)^2)$ operations in $\mathbb{K}$.

Proof. If $\mathbb{A}_h$ is a field, then [9, Corollary 1] allows us to compute the univariate representation $\dot{\mathbb{A}}_t$ of $\mathbb{A}_t$ over $\mathbb{A}_h$ using $\tilde{O}((S_h^{-1}S_t)^3)$ operations in $\mathbb{A}_h$. In general, $\mathbb{A}_h$ is not a field, but panoramic evaluation can be used to simulate field operations in it. Precisely we appeal to [10, Corollary 1] in order to run the algorithm underlying [9, Corollary 1]: using

$$\tilde{O}(S_h^{1+\epsilon}(S_h^{-1}S_t)^3)$$

operations in $\mathbb{K}$, we obtain a so-called panoramic splitting

$$\mathrm{P}: \quad \mathbb{A}_h \cong \mathbb{D}_1 \oplus \cdots \oplus \mathbb{D}_\ell$$

of $\mathbb{A}_h$ and univariate representations $\nu_{h+1}^{(j)}, \ldots, \nu_t^{(j)}$, $\Xi^{(j)}$, $A_{h+1}^{(j)}, \ldots, A_t^{(j)}$ for the restrictions of $\mathbb{A}_t$ over $\mathbb{D}_j$ for $j = 1, \ldots, \ell$. We further know from [10, Corollary 1] that one evaluation of P and P^{-1} takes $\tilde{O}(S_h^{1+\epsilon})$ operations in $\mathbb{K}$. Finally, we take $\nu_i := \mathrm{P}^{-1}(\nu_i^{(1)}, \ldots, \nu_i^{(\ell)})$ for $i = h+1, \ldots, t$. We extend P to $\mathbb{A}_h[T]$ coefficient-wise, and set $\Xi := \mathrm{P}^{-1}(\Xi^{(1)}, \ldots, \Xi^{(\ell)})$ and $A_i := \mathrm{P}^{-1}(A_i^{(1)}, \ldots, A_i^{(\ell)})$ for $i = h+1, \ldots, t$.

The cost of the conversions between $\mathbb{A}_t$ and $\dot{\mathbb{A}}_t$ is addressed in [9, Proposition 5], which simplifies to $\tilde{O}((S_h^{-1}S_t)^2)$ operations in $\mathbb{A}_h$: these conversions only involve ring operations in $\mathbb{A}_h$, so [9, Proposition 5] can be used even if $\mathbb{A}_h$ is not a field. □

4.2. Relative ramified and primitive constant extensions

It is known that $\mathbb{I}_i$ decomposes into a separable extension of $\mathbb{K}$ followed by purely ramified extensions; see for instance [11, section 6]. Given $h < t$, we use this decomposition in order to compute a univariate-valued representation of $\mathbb{I}_t$ over $\mathbb{I}_h$. We let

$$S_i := D_i / R_i \text{ and } s_i := S_{i-1}^{-1} S_i \text{ for } i = 1, \ldots, t.$$

We begin with a first technical rewriting of $\mathbb{I}_t$, summarized in the following lemma.

LEMMA 4.5. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be an almost reduced, effectively separable and regular contact tower, let $h < t$, and assume that we are given $> \binom{S_h^{-1}S_t}{2}$ distinct elements in $\mathbb{K}$. Using*

$$\tilde{O}(S_t^{1+\epsilon}(\mathrm{ht}\,\gamma_t \log^3 D_t + (S_h^{-1}S_t)^2 \log D_t))$$

operations in $\mathbb{K}$, we can compute the following data:

- *An effectively separable algebraic tower $(\mathbb{A}_i)_{i \leqslant t}$ as in section 4.1;*
- *A univariate representation $\nu_{h+1}, \ldots, \nu_t$, Ξ, $A_{h+1}, \ldots, A_t$ of $\mathbb{A}_t$ over $\mathbb{A}_h$, as in Lemma 4.4;*
- *$\rho_h, c_1, \ldots, c_h$ in $\mathbb{A}_h$, $\zeta_t, c_{h+1}, \ldots, c_t$ in $\dot{\mathbb{A}}_t$, $e_1, \ldots, e_t$ in $\mathbb{Z}$, $f_1, \ldots, f_t$ in $\{0, \ldots, R_h - 1\}$ and $g_{h+1}, \ldots, g_t$ in $\{0, \ldots, R_t - 1\}$ such that*

$$\begin{aligned} \mathrm{Y}: \quad \mathbb{I}_t &\cong \dot{\mathbb{A}}_t((z))[T_h, T_t] / \left(T_h^{R_h} - \rho_h z, T_t^{R_h^{-1}R_t} - \zeta_t T_h\right), \\ \varphi_i &\mapsto c_i z^{e_i} T_h^{f_i} \text{ for } i = 1, \ldots, h \\ \varphi_i &\mapsto c_i z^{e_i} T_h^{f_i} T_t^{g_i} \text{ for } i = h+1, \ldots, t \end{aligned}$$

is a $\mathbb{K}((z))$-algebra isomorphism, that preserves the valuation, when setting $v(T_h) := R_h^{-1}$ and $v(T_t) := R_t^{-1}$.

One evaluation of Y and Y^{-1} at a homogeneous element costs

$$\tilde{O}(S_t^{1+\epsilon}(\mathrm{ht}\,\gamma_t \log^2 D_t + S_h^{-1}S_t))$$

operations in $\mathbb{K}$.

Proof. By [11, Proposition 13] we can compute a so-called initial expansion [11, Definition 10] of $(\mathbb{P}_i)_{i\leqslant t}$, using

$$\tilde{O}(S_t^{1+\epsilon}\log(d_t\gamma_t D_t)\log^2 D_t) = \tilde{O}(S_t^{1+\epsilon}\operatorname{ht}\gamma_t\log^3 D_t) \tag{4.1}$$

operations in $\mathbb{K}$. In particular, combined with [11, Proposition 12], we obtain:

- 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 $\mathbb{A}_{i-1}[x_i]$. For $i=1,\ldots,t$, the class α_i of x_i in $\mathbb{A}_i$ is invertible and its inverse is known.
- For $i=1,\ldots,t$, an invertible $\rho_i\in\mathbb{A}_i$ and its inverse, along with a $\mathbb{K}((z))$-algebra isomorphism

  $$\mathrm{E}_i\colon\quad \mathbb{I}_i \;\cong\; \mathbb{A}_i((z))[T_i]/(T_i^{R_i}-\rho_i z)$$

  that preserves the valuation for the weight R_i^{-1} of T_i and such that one evaluation of E_i and E_i^{-1} in valuation $\sigma\in R_i^{-1}\mathbb{Z}$ with $|\sigma|<1$ costs

  $$\begin{aligned}\tilde{O}(S_i^{1+\epsilon}\log((|\sigma|+d_i\gamma_i)R_i)\log D_i) &= \tilde{O}(S_i^{1+\epsilon}\operatorname{ht}\gamma_i\log^2 D_i)\\ &= \tilde{O}(S_i^{1+\epsilon}\operatorname{ht}\gamma_t\log^2 D_t),\end{aligned} \tag{4.2}$$

  by (2.2). Note that this complexity bound further holds for any valuation, up to rescaling the arguments of E_i and E_i^{-1} by a suitable power of z.

Then, we compute $\theta_t\in\mathbb{A}_t$ invertible such that $\mathrm{E}_t(\mathrm{E}_h^{-1}(T_h)) = \theta_t^{-1}T_t^{R_h^{-1}R_t}$ holds, and define the $\mathbb{A}_t((z))$-algebra isomorphism

$$\begin{aligned}\mathrm{F}\colon\quad \mathbb{A}_t((z))[T_t]/(T_t^{R_t}-\rho_t z) &\;\cong\; \mathbb{A}_t((z))[T_h,T_t]/\left(T_h^{R_h}-\rho_h z, T_t^{R_h^{-1}R_t}-\theta_t T_h\right)\\ T_t &\;\mapsto\; T_t.\end{aligned}$$

Thanks to Lemma 4.4, we may compute a univariate representation of $\mathbb{A}_t$ over $\mathbb{A}_h$ using

$$\tilde{O}(S_h^{1+\epsilon}(S_h^{-1}S_t)^3) = \tilde{O}(S_t^{1+\epsilon}(S_h^{-1}S_t)^2) \tag{4.3}$$

operations in $\mathbb{K}$. Lemma 4.4 also ensures that one conversion between $\mathbb{A}_t$ and $\dot{\mathbb{A}}_t$ costs

$$\tilde{O}(S_h^{1+\epsilon}(S_h^{-1}S_t)^2) = \tilde{O}(S_t^{1+\epsilon}(S_h^{-1}S_t)). \tag{4.4}$$

In particular we compute $\zeta_t := \mathrm{A}(\theta_t)$ with this cost, and extend A coefficient-wise into $\bar{\mathrm{A}}$:

$$\begin{aligned}&\mathbb{A}_t((z))[T_h,T_t]/\left(T_h^{R_h}-\rho_h z, T_t^{R_h^{-1}R_t}-\theta_t T_h\right)\\ \cong\;&\dot{\mathbb{A}}_t((z))[T_h,T_t]/\left(T_h^{R_h}-\rho_h z, T_t^{R_h^{-1}R_t}-\zeta_t T_h\right).\end{aligned}$$

Finally, we set

$$\mathrm{Y} := \bar{\mathrm{A}}\circ\mathrm{F}\circ\mathrm{E}_t.$$

For $i=1,\ldots,h$, we take $e_i := (\gamma_i R_h) \operatorname{quo} R_h$, $f_i := (\gamma_i R_h) \operatorname{rem} R_h$, and $c_i\in\mathbb{A}_h$ such that

$$\mathrm{Y}(\varphi_i) = \mathrm{E}_h(\varphi_i) = c_i z^{e_i} T_h^{f_i}.$$

For $i=h+1,\ldots,t$, we compute ς_i invertible in $\mathbb{A}_t$ such that

$$\mathrm{E}_t(\varphi_i) = \varsigma_i z^{\tilde{e}_i} T_t^{\tilde{f}_i},$$

where $\tilde{e}_i := (R_t\,\gamma_i) \operatorname{quo} R_t$ and $\tilde{f}_i := (R_t\,\gamma_i) \operatorname{rem} R_t$. Writing $e'_i := \tilde{f}_i \operatorname{quo} (R_h^{-1} R_t)$ and $f'_i := \tilde{f}_i \operatorname{rem} (R_h^{-1} R_t)$, we obtain that

$$\begin{aligned}
\mathrm{F}\big(\varsigma_i z^{\tilde{e}_i} T_t^{\tilde{f}_i}\big) &= \varsigma_i z^{\tilde{e}_i} \big(T_t^{R_h^{-1}R_t}\big)^{e'_i} T_t^{f'_i} \bmod \big(T_t^{R_h^{-1}R_t} - \theta_t T_h\big) \\
&= \varsigma_i\, \theta_t^{e'_i} z^{\tilde{e}_i} T_h^{e'_i} T_t^{f'_i} \\
&= \varsigma_i\, \theta_t^{e'_i} z^{\tilde{e}_i} (\rho_h z)^{e'_i \operatorname{quo} R_h} T_h^{e'_i \operatorname{rem} R_h} T_t^{f'_i} \\
&= \varsigma_i\, \theta_t^{e'_i} \rho_h^{e'_i \operatorname{quo} R_h} z^{\tilde{e}_i + e'_i \operatorname{quo} R_h} T_h^{e'_i \operatorname{rem} R_h} T_t^{f'_i},
\end{aligned}$$

so we take

$$\sigma_i := \varsigma_i\, \theta_t^{e'_i} \rho_h^{e'_i \operatorname{quo} R_h}, \quad e_i := \tilde{e}_i + e'_i \operatorname{quo} R_h, \quad f_i := e'_i \operatorname{rem} R_h, \quad g_i := f'_i.$$

In this way, $O(\mathrm{ht}\,\gamma_i + \mathrm{ht}\,\gamma_t)$ products in $\mathbb{A}_t$ suffice to obtain σ_i from ς_i, that is $O(\mathrm{ht}\,\gamma_t)$ products thanks to (2.2).

The total cost of this construction of Y is the sum of (4.1), (4.3), $O(\log D_t)$ evaluations of E_h, E_h^{-1}, E_t of cost (4.2), $O(\log D_t)$ conversions from $\mathbb{A}_t$ to $\dot{\mathbb{A}}_t$ of cost (4.4), and $O(\mathrm{ht}\,\gamma_t)$ further products in $\mathbb{A}_t$.

When evaluating Y (resp. Y^{-1}) at a homogeneous element, the contribution of $\bar{\mathrm{A}}$ (resp. of $\bar{\mathrm{A}}^{-1}$) costs (4.4), since a homogeneous element of $\mathbb{A}_t((z))[T_h, T_t] / \big(T_h^{R_h} - \rho_h z, T_t^{R_h^{-1}R_t} - \theta_t T_h\big)$ is represented uniquely in the form $c z^e T_h^f T_t^g$, where $c \in \mathbb{A}_t$, $e \in \mathbb{Z}$, $0 \leqslant f < R_h$, $0 \leqslant g < R_h^{-1} R_t$. For such an element $c z^e T_h^f T_t^g$ we have

$$\mathrm{F}^{-1}\big(c z^e T_h^f T_t^g\big) = c\, \theta_t^{-f} z^e T_t^{g + f(R_h^{-1}R_t)}.$$

Therefore, one evaluation of F or F^{-1} costs

$$\tilde{O}(S_t^{1+\epsilon} \log R_h) = \tilde{O}(S_t^{1+\epsilon} \log D_t). \tag{4.5}$$

Finally, the cost of one evaluation of Y or Y^{-1} at a homogeneous element is bounded by the sum of (4.2), (4.4), and (4.5). □

Example 4.6. Let us consider the contact tower over $\mathbb{K} := \mathbb{F}_{11} = \mathbb{Z}/11\,\mathbb{Z}$ defined by $t := 3$, $\gamma_1 := 1/2$, $\gamma_2 := 5/4$, $\gamma_3 := 41/8$, and

$$\begin{aligned}
\Phi_1(\varphi_1) &:= \varphi_1^2 - z \\
\Phi_2(\varphi_1, \varphi_2) &:= \varphi_2^4 - z^5 + z^6 \\
\Phi_3(\varphi_1, \varphi_2, \varphi_3) &:= \varphi_3^4 - z^{18} \varphi_2^2.
\end{aligned}$$

At the first level of the contact tower, we have $r_1 = 2$, $s_1 = 1$, and we take $\mu_1(x_1) := x_1 - 1$, whence $\mathbb{A}_1 \cong \mathbb{K}$, $\alpha_1 = 1$, and

$$\mathbb{I}_1 \cong \mathbb{A}_1((z))[y_1] / (y_1^2 - z).$$

Since the image π_1 of y_1 in $\mathbb{I}_1$ is primitive-valued, we may define

$$\begin{aligned}
\mathrm{E}_1\colon \quad \mathbb{I}_1 &\cong \mathbb{A}_1((z))[T_1] / (T_1^2 - z) \\
\varphi_1 &\mapsto T_1.
\end{aligned}$$

At the second level, $\mathrm{in}(\Phi_2)$ is rewritten $\varphi_2^4 - \pi_1^{10}$ over $\mathbb{I}_1$, whence $r_2 = 2$ and $s_1 = 2$. We set $\mu_2(x_1, x_2) := x_2^2 - 1$, hence $\mathbb{A}_2 \cong \mathbb{K}[x_2] / (x_2^2 - 1)$, and obtain

$$\mathbb{I}_2 \cong \mathbb{A}_2((z))[y_1, y_2] / (y_1^2 - z, y_2^2 - \alpha_2 z^2 y_1),$$

where α_2 is the image of x_2 in $\mathbb{A}_2$. Taking the image π_2 of $z^{-1} y_2$ in $\mathbb{I}_2$ for a primitive-valued element, we define

$$\begin{aligned} \mathrm{E}_2\colon\quad \mathbb{I}_2 &\cong \mathbb{A}_2((z))[T_2]/(T_2^4 - z) \\ \varphi_1 &\mapsto \alpha_2 T_2^2 \\ \varphi_2 &\mapsto z\, T_2. \end{aligned}$$

For the third level of the contact tower, $\mathrm{in}(\Phi_3)$ is rewritten $\varphi_3^4 - z^{20}\pi_2^2$ over $\mathbb{I}_2$, whence $r_3 = 2$ and $s_2 = 2$. We set $\mu_3(x_1, x_2, x_3) := x_3^2 - 1$ and obtain

$$\mathbb{I}_3 \cong \mathbb{A}_3((z))[y_1, y_2, y_3]/(y_1^2 - z, y_2^2 - \alpha_2 z^2 y_1, y_3^2 - \alpha_3 z^9 y_2).$$

Taking the image π_3 of $\alpha_2 z^{-5} y_3$ in $\mathbb{I}_3$ for a primitive-valued element, we define

$$\begin{aligned} \mathrm{E}_3\colon\quad \mathbb{I}_3 &\cong \mathbb{A}_3((z))[T_3]/(T_3^8 - z) \\ \varphi_1 &\mapsto \alpha_2 T_3^4 \\ \varphi_2 &\mapsto \alpha_3 z\, T_3^2 \\ \varphi_3 &\mapsto \alpha_2 z^5 T_3. \end{aligned}$$

Now, let us build the map Υ of Lemma 4.5 for $h := 1$. For the univariate representation of $\mathbb{A}_3$ over $\mathbb{A}_1$, we use the primitive element $x_2 + 2x_3$, hence

$$\Xi(U) = (U-3)(U-1)(U+3)(U+1),$$

and obtain

$$\begin{aligned} \mathrm{A}\colon\quad \mathbb{A}_3 &\to \dot{\mathbb{A}}_3 := \mathbb{A}_1[U]/(\Xi(U)) \\ \alpha_2 &\mapsto A_2(U) := 2U^3 - 3U \\ \alpha_3 &\mapsto A_3(U) := -U^3 + 2U. \end{aligned}$$

We deduce the following expression for Υ:

$$\begin{aligned} \Upsilon\colon\quad \mathbb{I}_3 &\cong \dot{\mathbb{A}}_3((z))[T_1, T_3]/(T_1^2 - z, T_3^4 - A_2(U)\, T_1), \\ \varphi_1 &\mapsto T_1 \\ \varphi_2 &\mapsto A_3(U)\, z\, T_3^2 \\ \varphi_3 &\mapsto A_2(U)\, z^5 T_3. \end{aligned}$$

4.3. Construction of primitive-valued elements

A natural candidate for a primitive element of minimal valuation for $\mathbb{I}_t$ over $\mathbb{I}_h$ is $\Upsilon^{-1}(T_t)$. Unfortunately, it is not always primitive, as illustrated by the following example.

Example 4.7. (Continued from Example 4.6) The minimal polynomial of $\Upsilon^{-1}(T_3)$ over $\mathbb{I}_1$ is $\prod_{\Xi(\xi)=0} (T^4 - A_2(\xi)\, T_1) = (T^4 - T_1)^2 (T^4 + T_1)^2 = (T^8 - z)^2$, which is not separable. So $\Upsilon^{-1}(T_t)$ is not a primitive element of $\mathbb{I}_3$ over $\mathbb{I}_1$.

We will show in the proof of Proposition 4.10 that $\Upsilon^{-1}(\theta T_t)$ is indeed primitive for $\mathbb{I}_t$ over $\mathbb{I}_h$ for suitable values of θ in $\dot{\mathbb{A}}_t$. We begin with a technical lemma, where Λ stands for a new polynomial variable: in the context of Lemma 4.4, if U is a primitive element of $\mathbb{A}_t$ over $\mathbb{A}_h$, then $(U + \lambda)^{R_h^{-1} R_t} \zeta_t(U)$ is also primitive for almost all $\lambda \in \mathbb{K}$.

LEMMA 4.8. *Let the assumptions and the notation be as in Lemma 4.5, assume that we are given* $>(D_h^{-1}D_t)^2$ *elements in* $\mathbb{K}$, *and let*

$$\Psi(\tilde{U},\Lambda) := \mathrm{Res}_U\big(\Xi(U), \tilde{U} - (U+\Lambda)^{R_h^{-1}R_t}\zeta_t(U)\big) \in \mathbb{A}_h[\tilde{U},\Lambda],$$

where $\zeta_t(U)$ *represents the pre-image of* ζ_t *in* $\mathbb{A}_h[U]_{<S_h^{-1}S_h}$. *Using*

$$\tilde{O}(S_h^{1+\epsilon}(D_h^{-1}D_t)^6)$$

operations in $\mathbb{K}$, *we can compute* $\lambda \in \mathbb{A}_h$, $\tilde{\Xi}(\tilde{U}) := \Psi(\tilde{U},\lambda)$, *and* $V \in \mathbb{A}_h[\tilde{U}]_{<S_h^{-1}S_t}$ *such that:*

i. $U+\lambda$ *is invertible modulo* $\Xi(U)$,

ii. $\tilde{\Xi}(\tilde{U})$ *is separable,*

iii. $V\big((U+\lambda)^{R_h^{-1}R_t}\zeta_t(U)\big) - U = 0 \bmod \Xi(U)$.

Proof. Let us first assume that $\mathbb{A}_h$ is a field. Given $\lambda \in \mathbb{A}_h$, note that $\Xi(U-\lambda)$ is the minimal polynomial of $U+\lambda$ in $\mathbb{A}_h[U]/(\Xi(U))$. Therefore if ξ is a root of Ξ in a suitable algebraic closure, then $\xi+\lambda$ is invertible if and only if $\Xi(-\lambda)$ is non-zero. Consequently at most $S_h^{-1}S_t$ values of λ do not satisfy property (i). Letting

$$\Delta(\Lambda) := \mathrm{Disc}_{\tilde{U}}(\Psi(\tilde{U},\Lambda)) \in \mathbb{A}_h[\Lambda],$$

the multiplicativity of the resultant yields

$$\begin{aligned}\Psi(\tilde{U},\Lambda) &= \prod_{\Xi(\xi)=0}\big(\tilde{U} - (\xi+\Lambda)^{R_h^{-1}R_t}\zeta_t(\xi)\big)\\ \Delta(\Lambda) &= \pm\prod_{\substack{\Xi(\xi)=\Xi(\xi')=0\\ \xi\neq\xi'}}\Delta_{\xi,\xi'}(\Lambda),\end{aligned}$$

where

$$\Delta_{\xi,\xi'}(\Lambda) := (\xi+\Lambda)^{R_h^{-1}R_t}\zeta_t(\xi) - (\xi'+\Lambda)^{R_h^{-1}R_t}\zeta_t(\xi').$$

Since $\mathbb{I}_t$ is a separable extension of $\mathbb{K}((z))$, the polynomial $T_t^{R_t} - \rho_t z$ is separable in T_t, and therefore R_t is invertible in $\mathbb{K}$. Consequently, if $\zeta_h(\xi) = \zeta_h(\xi')$, then the leading term of $\Delta_{\xi,\xi'}(\Lambda)$ is

$$R_h^{-1}R_t\,(\xi-\xi')\,\zeta_t(\xi)\,\Lambda^{R_h^{-1}R_t-1}.$$

If $\zeta_h(\xi) \neq \zeta_h(\xi')$, then $\Delta_{\xi,\xi'}(\Lambda)$ clearly has degree $R_h^{-1}R_t$ in Λ. It follows that Δ is not the zero polynomial and that at most $(R_h^{-1}R_t)\binom{S_h^{-1}S_t}{2}$ values of λ do not satisfy property (ii).

Since

$$S_h^{-1}S_t + (R_h^{-1}R_t)\binom{S_h^{-1}S_t}{2} \leqslant (D_h^{-1}D_t)^2$$

there exists a suitable value for λ in any given set $\mathcal{L}$ of cardinality $(D_h^{-1}D_t)^2+1$. In order to find a suitable value, it suffices to evaluate $\Xi(-\Lambda)\,\Delta(\Lambda)$ at all the points of $\mathcal{L}$.

The polynomial $\Psi(\tilde{U},\Lambda)$ has degree $\leqslant S_h^{-1}S_t$ in $\tilde{U}$ and degree

$$\leqslant R_h^{-1}R_tS_h^{-1}S_t = \tilde{O}(D_h^{-1}D_t)$$

in Λ. So it can be computed using

$$\tilde{O}(D_h^{-1}D_tS_h^{-1}S_t\,(S_h^{-1}S_t)^4) = \tilde{O}((D_h^{-1}D_t)^6)$$

operations in $\mathbb{A}_h$ by means of the Berkowitz algorithm [22] applied to the Sylvester matrix of $T-(U+\Lambda)^{R_h^{-1}R_t}\zeta_h(U)$ rem $\Xi(U)$ and $\Xi(U)$. Since $\Delta(\Lambda)$ has degree

$$\leqslant (R_h^{-1}R_t)\,(S_h^{-1}S_t)^2=\tilde{O}((D_h^{-1}D_t)^2),$$

it can be computed using

$$\tilde{O}([(R_h^{-1}R_t)\,(S_h^{-1}S_t)^2]\,(S_h^{-1}S_t)^4)=\tilde{O}((D_h^{-1}D_t)^6)$$

operations in $\mathbb{A}_h$ by means of the Berkowitz algorithm.

The evaluation of $\Xi(-\Lambda)\,\Delta(\Lambda)$ at all the elements of $\mathcal{L}$ takes $\tilde{O}((D_h^{-1}D_t)^2)$ operations in $\mathbb{A}_h$; see [4, Chapter 10] for instance. From Proposition 4.3 we know that one operation in $\mathbb{A}_h$ reduces to $\tilde{O}(S_h^{1+\epsilon})$ operations in $\mathbb{K}$. Consequently we obtain a suitable value for λ using a total number of $\tilde{O}(S_h^{1+\epsilon}\,(D_h^{-1}D_t)^6)$ operations in $\mathbb{K}$.

In this way $(U+\lambda)^{R_h^{-1}R_t}\zeta_t(U)$ is a primitive element of $\dot{\mathbb{A}}_t$, of minimal polynomial $\tilde{\Xi}(\tilde{U})$. Therefore, there exists a unique $V(\tilde{U})\in\mathbb{A}_h[\tilde{U}]_{<S_h^{-1}S_t}$ satisfying property (iii). If ξ is a root of $\tilde{\Xi}(\tilde{U})$, then $\Xi(U)$ and $\xi-(U+\lambda)^{R_h^{-1}R_t}\zeta_t(U)$ share a proper gcd, that is $U-V(\xi)$. In this case, it is known that this gcd is proportional to the first subresultant of $\Xi(U)$ and $\xi-(U+\lambda)^{R_h^{-1}R_t}\zeta_t(U)$; see [14, Theorem 9]. Since the specialization at $\tilde{U}=\xi$ of the first subresultant $S_0(\tilde{U})\,U-S_1(\tilde{U})$ of $\Xi(U)$ and $\tilde{U}-(U+\lambda)^{R_h^{-1}R_t}\zeta_t(U)$ coincides with the first subresultant of $\Xi(U)$ and $\xi-(U+\lambda)^{R_h^{-1}R_t}\zeta_t(U)$, we deduce that $S_0(\tilde{U})$ is invertible modulo $\tilde{\Xi}(\tilde{U})$.

The polynomials S_0 and S_1 are minors of the Sylvester matrix of $\Xi(U)$ and $T-(U+\lambda)^{R_h^{-1}R_t}\zeta_h(U)$ rem $\Xi(U)$; see [14, section 2.1] for instance. They can thus be computed using $\tilde{O}((S_h^{-1}S_t)^4)$ operations in $\mathbb{A}_h$, again by means the Berkowitz algorithm. Computing $V(\tilde{U})=S_1(\tilde{U})/S_0(\tilde{U})$ mod $R(\tilde{U},\lambda)$ further needs $\tilde{O}(S_h^{-1}S_t)$ operations in $\mathbb{A}_h$.

It remains to handle the case where $\mathbb{A}_h$ is not a field. Panoramic evaluation can perform the above calculations [10, Corollary 1] still using $\tilde{O}(S_h^{1+\epsilon}\,(D_h^{-1}D_t)^6)$ operations in $\mathbb{K}$: we obtain a panoramic splitting

$$\mathrm{P}:\quad \mathbb{A}_h\cong\mathbb{D}_1\oplus\cdots\oplus\mathbb{D}_\ell$$

of $\mathbb{A}_h$ and suitable values $\lambda^{(1)},\ldots,\lambda^{(l)}$ in $\mathbb{K}$ for the restrictions of $\mathbb{A}_h$ over $\mathbb{D}_j$ for $j=1,\ldots,\ell$, along with the corresponding $\tilde{\Xi}^{(j)}$ and $V^{(j)}\in\mathbb{A}_h[\tilde{U}]_{<S_h^{-1}S_t}$. We further know from [10, Corollary 1] that one evaluation of P and P^{-1} takes $\tilde{O}(S_h^{1+\epsilon})$ operations in $\mathbb{K}$. Finally we take $\lambda:=\mathrm{P}^{-1}(\lambda^{(1)},\ldots,\lambda^{(\ell)})$, $\tilde{\Xi}:=\mathrm{P}^{-1}(\tilde{\Xi}^{(1)},\ldots,\tilde{\Xi}^{(\ell)})$, $V:=\mathrm{P}^{-1}(V^{(1)},\ldots,V^{(\ell)})$, where P is implicitly extended to $\mathbb{A}_h[\tilde{U}]$ coefficient-wise. □

Example 4.9. (Continued from Example 4.7) In Lemma 4.8, we can take $\lambda=4$ and

$$\begin{aligned}\tilde{\Xi}(\tilde{U}) &= \tilde{U}^4+5\tilde{U}^3+3\tilde{U}^2+4\tilde{U}+9\\ V(\tilde{U}) &= 9\tilde{U}^3+10\tilde{U}^2.\end{aligned}$$

4.4. Initial univariate-valued representation

We put Lemmas 4.5 and 4.8 together in order to construct an initial primitive-valued element of $\mathbb{I}_t$ over $\mathbb{I}_h$, written ϖ in the following proposition.

PROPOSITION 4.10. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an almost reduced effectively separable and regular contact tower, let $h<t$, and assume that we are given $>(D_h^{-1}D_t)^2$ distinct elements in $\mathbb{K}$. Using*

$$\tilde{O}(S_t^{1+\epsilon}(\mathrm{ht}\,\gamma_t+(D_h^{-1}D_t)^6))$$

operations in $\mathbb{K}$, we can compute:

- *a homogeneous polynomial ϖ in $\mathbb{I}_t$ of valuation R_t^{-1},*
- *a monic separable homogeneous polynomial $\chi\in\mathbb{I}_h[T]$ of degree $D_h^{-1}D_t$, where T has valuation R_t^{-1},*
- *homogeneous polynomials $w_{h+1},\dots,w_t$ in $\mathbb{I}_h[T]_{<D_h^{-1}D_t}$ of respective valuations $\gamma_{h+1},\dots,\gamma_t$,*

such that

$$(\varpi(\varphi_1,\dots,\varphi_h,w_{h+1}(T),\dots,w_t(T))-T)\ \mathrm{rem}\ \chi(T)=0,$$

and

$$\mathrm{in}(\Phi_i)(\varphi_1,\dots,\varphi_h,w_{h+1}(T),\dots,w_i(T))\ \mathrm{rem}\ \chi(T)=0,\ \textit{for } i=h+1,\dots,t.$$

In other words, the map

$$\begin{aligned} Z\colon\quad \mathbb{I}_t &\cong \mathbb{I}_h[T]/(\chi(T))\\ \varphi_i &\mapsto w_i(T)\ \textit{for } i=h+1,\dots,n\end{aligned}$$

is an isomorphism of $\mathbb{I}_h$-algebras. One evaluation of Z and Z^{-1} at a homogeneous element costs

$$\tilde{O}(S_t^{1+\epsilon}(\mathrm{ht}\,\gamma_t+D_h^{-1}D_t))$$

operations in $\mathbb{K}$.

Proof. We set

$$\mathbb{B}_h:=\mathbb{A}_h((z))[T_h]/(T_h^{R_h}-\rho_h z),$$

which is another $\mathbb{K}((z))$-algebra representation of $\mathbb{I}_h$ via the map $E_h\colon\mathbb{I}_h\cong\mathbb{B}_h$ introduced in the proof of Lemma 4.5. A homogeneous element of $\mathbb{B}_h$ can be written $cz^eT_h^f$, where $c\in\mathbb{A}_h$, $z\in\mathbb{Z}$, and $0\leqslant f<R_h$. Consequently, the product of two homogeneous elements of $\mathbb{B}_h$ costs $\leqslant 2$ operations in $\mathbb{A}_h$.

First, we build the isomorphism Y of Lemma 4.5 using

$$\tilde{O}(S_t^{1+\epsilon}(\mathrm{ht}\,\gamma_t\log^3 D_t+(S_h^{-1}S_t)^2\log D_t)) \tag{4.6}$$

operations in $\mathbb{K}$. Then, we compute $\lambda\in\mathbb{A}_h$, $\tilde{\Xi}$, and V as in Lemma 4.8, using

$$\tilde{O}(S_h^{1+\epsilon}(D_h^{-1}D_t)^6) \tag{4.7}$$

operations in $\mathbb{K}$. This yields the following isomorphism of $\mathbb{B}_h$-algebras:

$$\begin{aligned} \mathrm{M}_1\colon\quad \mathbb{B}_h[U,T_t]/\left(\Xi(U),T_t^{R_h^{-1}R_t}-\zeta_t(U)\,T_h\right) &\cong \mathbb{B}_h[\tilde{U},\tilde{T}_t]/\left(\tilde{\Xi}(\tilde{U}),\tilde{T}_t^{R_h^{-1}R_t}-\tilde{U}\,T_h\right)\\ U &\mapsto V(\tilde{U})\\ T_t &\mapsto (V(\tilde{U})+\lambda)^{-1}\tilde{T}_t\\ (U+\lambda)^{R_h^{-1}R_t}\zeta_t(U) &\leftarrow \tilde{U}.\end{aligned}$$

From Lemma 4.8, we know that $\Xi(-\lambda)$ is invertible. Since $\Xi(X-\lambda)$ is the minimal polynomial of $U+\lambda$ modulo $\Xi(U)$, the inverse of $U+\lambda$ modulo $\Xi(U)$ is given by

$$I(U):=\left(\frac{\Xi(X-\lambda)-\Xi(-\lambda)}{-\Xi(-\lambda)\,X}\right)(U+\lambda),$$

which can be obtained with $\tilde{O}(S_h^{-1} S_t)$ ring operations in $\mathbb{A}_h$ plus the inversion of $\Xi(-\lambda)$. The inverse of $V(\tilde{U}) + \lambda$ modulo $\tilde{\Xi}(\tilde{U})$ equals $I(V(\tilde{U}))$ rem $\tilde{\Xi}(\tilde{U})$, which can be computed using $\tilde{O}((S_h^{-1} S_t)^2)$ further operations in $\mathbb{A}_h$. On the other hand, computing $(U+\lambda)^{R_h^{-1} R_t} \zeta_t(U)$ modulo $\Xi(U)$ takes $\tilde{O}(S_h^{-1} S_t \log(R_h^{-1} R_t))$ operations in $\mathbb{A}_h$.

A homogeneous element of $\mathbb{B}_h[U, T_t] / \left(\Xi(U), T_t^{R_h^{-1} R_t} - \zeta_t(U)\, T_h\right)$ can be uniquely written $C(U)\, z^e\, T_h^f\, T_t^g$, where $C(U) \in \mathbb{A}_h[U]_{<S_h^{-1} S_t}$, $e \in \mathbb{Z}$, $0 \leqslant f < R_h$, and $0 \leqslant g < R_h^{-1} R_t$. Consequently, computing

$$\mathrm{M}_1\left(C(U)\, z^e\, T_h^f\, T_t^g\right) = C(V(\tilde{U}))\, (V(\tilde{U}) + \lambda)^{-g}\, z^e\, T_h^f\, \tilde{T}_t^g \bmod \tilde{\Xi}(\tilde{U})$$

takes

$$\tilde{O}((S_h^{-1} S_t)^2 + S_h^{-1} S_t \log(R_h^{-1} R_t)) \tag{4.8}$$

operations in $\mathbb{A}_h$. The same cost bound applies to M_1^{-1}.

The characteristic polynomial of $\tilde{T}_t$ over $\mathbb{B}_h$ is

$$\tilde{\chi}(T) := \mathrm{Res}_{\tilde{U}}\left(\tilde{\Xi}(\tilde{U}), T^{R_h^{-1} R_t} - \tilde{U} T_h\right) = T_h^{S_h^{-1} S_t}\, \tilde{\Xi}\left(T_h^{-1} T^{R_h^{-1} R_t}\right),$$

and its computation takes

$$O(S_h^{-1} S_t) \tag{4.9}$$

operations in $\mathbb{B}_h$. As seen in the proof of Lemma 4.8, the integer R_t is invertible in $\mathbb{K}$, so $\tilde{\chi}$ is separable, and the map

$$\begin{aligned} \mathrm{M}_2\colon \quad \mathbb{B}_h[\tilde{U}, \tilde{T}_t] / \left(\tilde{\Xi}(\tilde{U}), \tilde{T}_t^{R_h^{-1} R_t} - \tilde{U} T_h\right) &\cong \mathbb{B}_h[T] / (\tilde{\chi}(T)) \\ \tilde{U} &\mapsto T_h^{-1} T^{R_h^{-1} R_t} \\ \tilde{T}_t &\mapsto T \end{aligned}$$

is a $\mathbb{B}_h$-algebra isomorphism. Let us consider a homogeneous element of $\mathbb{B}_h[T] / (\tilde{\chi}(T))$, of the form

$$T^e \sum_{0 \leqslant i < S_h^{-1} S_t} c_i z^{e_i} T_h^{f_i} \left(T^{R_h^{-1} R_t}\right)^i,$$

where $0 \leqslant e < R_h^{-1} R_t$, $c_i \in \mathbb{A}_h$, $e_i \in \mathbb{Z}$, $0 \leqslant f_i < R_h$, and $g := e_i + R_h^{-1} (f_i + i)$ is independent of i. The computation of

$$\begin{aligned} & \mathrm{M}_2^{-1}\left(T^e \sum_{0 \leqslant i < S_h^{-1} S_t} c_i z^{e_i} T_h^{f_i} \left(T^{R_h^{-1} R_t}\right)^i\right) \\ = \; & \tilde{T}_t^e \sum_{0 \leqslant i < S_h^{-1} S_t} c_i z^{e_i} T_h^{f_i} \left(\tilde{T}_t^{R_h^{-1} R_t}\right)^i \bmod \left(\tilde{T}_t^{R_h^{-1} R_t} - \tilde{U} T_h\right) \\ = \; & \tilde{T}_t^e \sum_{0 \leqslant i < S_h^{-1} S_t} c_i z^{e_i} T_h^{f_i + i} \tilde{U}^i \\ = \; & \tilde{T}_t^e \sum_{0 \leqslant i < S_h^{-1} S_t} c_i \rho_h^{(f_i + i) \operatorname{quo} R_h} z^{e_i + (f_i + i) \operatorname{quo} R_h} T_h^{(f_i + i) \operatorname{rem} R_h} \tilde{U}^i \\ = \; & \left(\sum_{0 \leqslant i < S_h^{-1} S_t} c_i \rho_h^{(f_i + i) \operatorname{quo} R_h} \tilde{U}^i\right) z^{(g R_h) \operatorname{quo} R_h} T_h^{(g R_h) \operatorname{rem} R_h} \tilde{T}_t^e, \end{aligned}$$

takes

$$\tilde{O}(S_h^{-1} S_t) \tag{4.10}$$

operations in $\mathbb{A}_h$. By reverting these calculations, the same cost is achieved for one evaluation of M_2. We extend the map E_h to $\mathbb{I}_h[T]$ coefficientwise, and compute

$$\chi(T) := \mathrm{E}_h^{-1}(\tilde{\chi}(T)).$$

Composed with Y, we finally obtain the desired initial univariate-valued representation of $\mathbb{I}_t$ over $\mathbb{I}_h$:

$$\mathrm{E}_h \circ \mathrm{M}_2 \circ \mathrm{M}_1 \circ \mathrm{Y}: \quad \mathbb{I}_t \cong \mathbb{I}_h[T]/(\chi(T)).$$

The total cost of the construction of Y, E_h, M_1, and M_2 is bounded by the sum of (4.6) and (4.7), that is

$$\tilde{O}(S_t^{1+\epsilon}(\mathrm{ht}\,\gamma_t + (D_h^{-1} D_t)^6))$$

operations in $\mathbb{K}$. The cost of one evaluation of $\mathrm{E}_h \circ \mathrm{M}_2 \circ \mathrm{M}_1 \circ \mathrm{Y}$ or $(\mathrm{E}_h \circ \mathrm{M}_2 \circ \mathrm{M}_1 \circ \mathrm{Y})^{-1}$ is at most by the sum of (4.8), (4.10), and the costs for Y and E_h given in Lemma 4.5, that is bounded by

$$\tilde{O}(S_t^{1+\epsilon}(\mathrm{ht}\,\gamma_t + D_h^{-1} D_t))$$

operations in $\mathbb{K}$. Finally we take $\varpi := (\mathrm{E}_h \circ \mathrm{M}_2 \circ \mathrm{M}_1 \circ \mathrm{Y})^{-1}(T)$ and $w_i(T) := \mathrm{E}_h \circ \mathrm{M}_2 \circ \mathrm{M}_1 \circ \mathrm{Y}(\varphi_i)$, for $i = h+1, \ldots, t$. □

Example 4.11. (Continued from Example 4.9). We calculate the representation of $\mathbb{I}_t$ over $\mathbb{I}_h$ given in Proposition 4.10. The initial primitive-valued element is

$$\begin{aligned} \varpi &= \mathrm{Y}^{-1}((U+4)\,T_3) \\ &= 2z^{-17}\varphi_1\varphi_2^2\varphi_3^3 + (4z^{-8}\varphi_1\varphi_2^2 + z^{-5})\,\varphi_3 \end{aligned}$$

and the corresponding initial univariate-valued representation is

$$\begin{aligned} \chi(T) &= T^{16} + 3\varphi_1 T^{12} + 6zT^8 + 2z\varphi_1 T^4 + 9z^2 \\ w_2(T) &= 6z^{-1}\varphi_1 T^{14} + 8T^{10} + 5\varphi_1 T^6 + 2zT^2 \\ w_3(T) &= 7z^3\varphi_1 T^{13} + 9z^4 T^9 + 4z^4\varphi_1 T^5 + z^5 T. \end{aligned}$$

5. PRIMITIVE-VALUED REPRESENTATION

In this section we consider a generalized contact tower $(\mathbb{P}_i)_{i \leqslant t}$ as in section 3.1 and an index $h < t$ such that

$$\epsilon_h = \epsilon_t = 0.$$

It follows that $\mathbb{P}_t/(\varphi_{t+1})$ has dimension $D_h^{-1} D_t$ over $\mathbb{P}_h/(\varphi_{h+1})$, and that $\mathbb{P}_h/(\varphi_{h+1})$ has dimension D_h over $\mathbb{K}((z))$. We are interested in computing a primitive-valued element representation of $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$.

Using Proposition 4.10, we first compute an initial univariate-valued representation of $\mathbb{I}_t = \mathbb{K}((z))[\varphi_1,...,\varphi_t]/(\mathrm{in}(\Phi_1),...,\mathrm{in}(\Phi_t))$ over $\mathbb{I}_h = \mathbb{K}((z))[\varphi_1,...,\varphi_h]/(\mathrm{in}(\Phi_1),...,\mathrm{in}(\Phi_h))$. This yields a homogeneous polynomial ϖ in $\mathbb{I}_t$ of valuation R_t^{-1}, a monic separable homogeneous polynomial $\chi \in \mathbb{I}_h[T]$ of degree $D_h^{-1}D_t$, where T has valuation R_t^{-1}, and homogeneous polynomials $w_{h+1},\ldots,w_t$ in $\mathbb{I}_h[T]_{<D_h^{-1}D_t}$ of respective valuation $\gamma_{h+1},\ldots,\gamma_t$, such that

$$[(\varpi(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_t(T)) - T) \operatorname{rem} \chi(T)]_{R_t^{-1};R_t^{-1}} = 0,$$

and

$$[(\Phi_i(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_i(T)) - \epsilon_i w_{i+1}(T)) \operatorname{rem} \chi(T)]_{d_i\gamma_i;R_t^{-1}} = 0, \text{ for } i = h+1,\ldots,t.$$

Then, given a target precision $\rho \in R_t^{-1}\mathbb{N}^{>0}$, we will use a suitable Hensel lifting in order to obtain $\chi^{\{\rho\}} \in (\mathbb{P}_h/(\varphi_{h+1}))[T]$ monic of degree $D_h^{-1}D_t$, and polynomials $w_{h+1}^{\{\rho\}},\ldots,w_t^{\{\rho\}}$ in $(\mathbb{P}_h/(\varphi_{h+1}))[T]_{<D_h^{-1}D_t}$ such that:

- $\mathrm{in}(\chi^{\{\rho\}}) = \chi$, and $\mathrm{in}(w_i^{\{\rho\}}) = \mathrm{in}(w_i)$, for $i = h+1,\ldots,t$,
- $\big[\big(\varpi\big(\varphi_1,\ldots,\varphi_h,w_{h+1}^{\{\rho\}}(T),\ldots,w_t^{\{\rho\}}(T)\big) - T\big) \operatorname{rem} \chi^{\{\rho\}}(T)\big]_{R_t^{-1};\rho} = 0$,
- $\big[\big(\Phi_i\big(\varphi_1,\ldots,\varphi_h,w_{h+1}^{\{\rho\}}(T),\ldots,w_i^{\{\rho\}}(T)\big) - \epsilon_i w_i^{\{\rho\}}(T)\big) \operatorname{rem} \chi^{\{\rho\}}(T)\big]_{d_i\gamma_i;\rho} = 0$, for $i = h+1,\ldots,t$.

We begin by presenting our lifting strategy, which is naturally based on the Newton operator of the map $(\varphi_1,\ldots,\varphi_t) \mapsto (\Phi_1 - \epsilon_1\varphi_2,\ldots,\Phi_t - \epsilon_t\varphi_{t+1})$.

5.1. Hasse derivative and Taylor expansion

Let $\mathbb{A}$ denote a commutative ring, let $f \in \mathbb{A}[x_1,\ldots,x_n]$ and let $y_1,\ldots,y_n$ be independent variables. Expanding

$$f(x_1,\ldots,x_n) = f(y_1 + (x_1 - y_1),\ldots,y_n + (x_n - y_n))$$

in terms of the powers of $(x_j - y_j)$ in $\mathbb{A}[x_1,\ldots,x_n,y_1,\ldots,y_n]$ yields

$$f(x_1,\ldots,x_n) = \sum_{e_1\geqslant 0,\ldots,e_n\geqslant 0} (D^{(e_1,\ldots,e_n)}f)(y_1,\ldots,y_n)\,(x_1 - y_1)^{e_1}\cdots(x_n - y_n)^{e_n}, \tag{5.1}$$

where $D^{(e_1,\ldots,e_n)}f$ are polynomials in $\mathbb{A}[y_1,\ldots,y_n]$ of total degree $\leqslant \deg f - (e_1 + \cdots + e_n)$. This operator $D^{(e_1,\ldots,e_n)}$ is usually called the *Hasse derivative* of orders $(e_1,\ldots,e_n)$. Applied to a monomial $x_1^{k_1}\cdots x_n^{k_n}$, where $k_1 \geqslant 0,\ldots,k_n \geqslant 0$, we have

$$D^{(e_1,\ldots,e_n)}(x_1^{k_1}\cdots x_n^{k_n}) = \binom{k_1}{e_1}\cdots\binom{k_n}{e_n} x_1^{k_1-e_1}\cdots x_n^{k_n-e_n}.$$

Note that

$$e_1!\cdots e_n!\, D^{(e_1,\ldots,e_n)}f = \frac{\partial^{e_1+\cdots+e_n}f}{\partial x^{e_1}\cdots\partial x^{e_n}}.$$

For any $(a_1,\ldots,a_n) \in \mathbb{A}^n$, the following Taylor expansion holds after replacing y_j by a_j in (5.1):

$$f(x_1,\ldots,x_n) = \sum_{e_1\geqslant 0,\ldots,e_n\geqslant 0} (D^{(e_1,\ldots,e_n)}f)(a_1,\ldots,a_n)\,(x_1 - a_1)^{e_1}\cdots(x_n - a_n)^{e_n}. \tag{5.2}$$

5.2. Newton operator

Consider the map

$$\begin{aligned}\boldsymbol{\Phi}_t\colon\ \mathbb{K}((z))[\varphi_1,\dots,\varphi_t]^t &\to \mathbb{K}((z))[\varphi_1,\dots,\varphi_t]^t\\ \begin{pmatrix}\varphi_1\\ \vdots\\ \varphi_{t-1}\\ \varphi_t\end{pmatrix} &\mapsto \begin{pmatrix}\Phi_1(\varphi_1)-\epsilon_1\varphi_2\\ \vdots\\ \Phi_{t-1}(\varphi_1,\dots,\varphi_{t-1})-\epsilon_{t-1}\varphi_t\\ \Phi_t(\varphi_1,\dots,\varphi_t)\end{pmatrix},\end{aligned}$$

whose Jacobian matrix is

$$\boldsymbol{J}_t := \begin{pmatrix}\frac{\partial\Phi_1}{\partial\varphi_1} & -\epsilon_1 & & 0\\ \vdots & \ddots & \ddots & \\ \frac{\partial\Phi_{t-1}}{\partial\varphi_1} & \cdots & \frac{\partial\Phi_{t-1}}{\partial\varphi_{t-1}} & -\epsilon_{t-1}\\ \frac{\partial\Phi_t}{\partial\varphi_1} & & \cdots & \frac{\partial\Phi_t}{\partial\varphi_t}\end{pmatrix}.$$

The corresponding Newtor iterator is the map

$$\begin{pmatrix}\varphi_1\\ \vdots\\ \varphi_t\end{pmatrix}\mapsto\begin{pmatrix}\varphi_1\\ \vdots\\ \varphi_t\end{pmatrix}-\boldsymbol{J}_t^{-1}\cdot\boldsymbol{\Phi}_t(\varphi_1,\dots,\varphi_t).$$

In order to quantify the convergence of this operator, we begin by studying the valuations of the determinant and the adjunct matrix of $\boldsymbol{J}_t$.

LEMMA 5.1. *For all k,l with $1\leqslant k\leqslant l\leqslant t_j$ we have*

$$\operatorname{in}\begin{vmatrix}\frac{\partial\Phi_k}{\partial\varphi_k} & -\epsilon_1 & & 0\\ \vdots & \ddots & \ddots & \\ \frac{\partial\Phi_{l-1}}{\partial\varphi_k} & \cdots & \frac{\partial\Phi_{l-1}}{\partial\varphi_{l-1}} & -\epsilon_{l-1}\\ \frac{\partial\Phi_l}{\partial\varphi_k} & & \cdots & \frac{\partial\Phi_l}{\partial\varphi_l}\end{vmatrix}=\operatorname{in}\left(\frac{\partial\Phi_k}{\partial\varphi_k}\cdots\frac{\partial\Phi_l}{\partial\varphi_l}\right).$$

Proof. For simplicity, the proof is presented for $k=1$ and $l=t$. The general case only involves syntactic adjustments. The usual expansion of the determinant of J_t yields

$$\det\boldsymbol{J}_t=\sum_{\sigma\in\mathfrak{S}_t}(-1)^{\operatorname{sig}\sigma}\prod_{1\leqslant i\leqslant t}\boldsymbol{J}_{t;i,\sigma(i)},\tag{5.3}$$

where $\mathfrak{S}_t$ is the permutation group of $\{1,\dots,t\}$, sig represents the usual signature function, and $\boldsymbol{J}_{t;i,j}$ stands for the entry (i,j) in $\boldsymbol{J}_t$. Note that a product $\prod_{i=1}^t\boldsymbol{J}_{t;i,\sigma(i)}$ vanishes whenever $\sigma(i)>i+1$ for some i in $\{1,\dots,t-2\}$, and that the identity permutation id_t is the only element of $\mathfrak{S}_t$ that satisfies $\sigma(i)\leqslant i$ for all $i=1,\dots,t$.

Now let $\mathfrak{S}_t^{(k)}$ denote the subset of permutations σ that satisfy $\sigma(i)\leqslant i+1$ for all $i=1,\dots,t-1$ and such that the latter inequality is an equality for exactly k values of i. The expansion (5.3) of the determinant rewrites into

$$\det\boldsymbol{J}_t=\frac{\partial\Phi_1}{\partial\varphi_1}\cdots\frac{\partial\Phi_t}{\partial\varphi_t}+\sum_{1\leqslant k<t}\ \sum_{\sigma\in\mathfrak{S}_t^{(k)}}(-1)^{\operatorname{sig}\sigma}\prod_{\substack{1\leqslant i\leqslant t\\ \sigma(i)=i+1}}\epsilon_i\prod_{\substack{1\leqslant i\leqslant t\\ \sigma(i)\leqslant i}}^{t}\frac{\partial\Phi_i}{\partial\varphi_{\sigma(i)}}.$$

The valuation of the first term equals $\sum_{i=1}^{t} (d_i - 1)\,\gamma_i$. For $k \in \{1, \ldots, t-1\}$ and $\sigma \in \mathfrak{S}_t^{(k)}$, we have

$$\begin{aligned}
\operatorname{val}\left(\prod_{\substack{1 \leqslant i \leqslant t \\ \sigma(i) \leqslant i}} \frac{\partial \Phi_i}{\partial \varphi_{\sigma(i)}} \right) &\geqslant \sum_{\substack{1 \leqslant i \leqslant t \\ \sigma(i) \leqslant i}} d_i \gamma_i - \sum_{\substack{1 \leqslant i \leqslant t \\ \sigma(i) \leqslant i}} \gamma_{\sigma(i)} \\
&= \sum_{1 \leqslant i \leqslant t} d_i \gamma_i - \sum_{\substack{1 \leqslant i \leqslant t \\ \sigma(i) = i+1}} d_i \gamma_i - \sum_{1 \leqslant i \leqslant t} \gamma_{\sigma(i)} + \sum_{\substack{1 \leqslant i \leqslant t \\ \sigma(i) = i+1}} \gamma_{\sigma(i)} \\
&= \sum_{1 \leqslant i \leqslant t} (d_i - 1)\,\gamma_i + \sum_{\substack{1 \leqslant i \leqslant t \\ \sigma(i) = i+1}} (\gamma_{i+1} - d_i \gamma_i) \\
&> \operatorname{val}\left(\frac{\partial \Phi_1}{\partial \varphi_1} \cdots \frac{\partial \Phi_t}{\partial \varphi_t} \right),
\end{aligned}$$

which concludes the proof. □

LEMMA 5.2. *Let* $\operatorname{adj} \boldsymbol{J}_t$ *represent the adjunct matrix of* $\boldsymbol{J}_t$. *The entry* (k,l) *of* $\operatorname{adj} \boldsymbol{J}_t$ *has valuation*

$$\geqslant \operatorname{val}(\det \boldsymbol{J}_t) + \gamma_k - d_l \gamma_l.$$

Proof. The entry (k,l) of $\operatorname{adj} J_t$ is $(-1)^{k+l}$ times the (l,k)-minor $\boldsymbol{K}_{k,l}$ of $\boldsymbol{J}_t$. When $l \leqslant k$, we have

$$\boldsymbol{K}_{k,l} = \begin{vmatrix}
\frac{\partial \Phi_1}{\partial \varphi_1} & -\epsilon_1 & & & & & & \\
\vdots & \ddots & \ddots & & & & 0 & \\
\frac{\partial \Phi_{l-1}}{\partial \varphi_1} & \cdots & \frac{\partial \Phi_{l-1}}{\partial \varphi_{l-1}} & -\epsilon_{l-1} & & & & \\
\frac{\partial \Phi_{l+1}}{\partial \varphi_1} & \cdots & & \frac{\partial \Phi_{l+1}}{\partial \varphi_{l+1}} & -\epsilon_{l+1} & & & \\
\vdots & & & & \ddots & -\epsilon_{k-2} & & \\
\frac{\partial \Phi_{k-1}}{\partial \varphi_1} & & \cdots & & & \frac{\partial \Phi_{k-1}}{\partial \varphi_{k-1}} & & \\
\frac{\partial \Phi_k}{\partial \varphi_1} & & \cdots & & & \frac{\partial \Phi_k}{\partial \varphi_{k-1}} & -\epsilon_k & \\
\frac{\partial \Phi_{k+1}}{\partial \varphi_1} & & \cdots & & & & \frac{\partial \Phi_{k+1}}{\partial \varphi_{k+1}} & -\epsilon_{k+1} \\
\vdots & & & & & & \ddots & -\epsilon_{t-1} \\
\frac{\partial \Phi_t}{\partial \varphi_1} & & & & \cdots & & & \frac{\partial \Phi_t}{\partial \varphi_t}
\end{vmatrix}. \tag{5.4}$$

Let $\mathfrak{S}_t^{(\kappa_1,\kappa_2,\kappa_3)}$ denote the set of bijections

$$\sigma : \{1, \ldots, t\} \setminus \{l\} \to \{1, \ldots, t\} \setminus \{k\}$$

such that $\sigma(i) \leqslant i+1$, κ_1 (resp. κ_2, κ_3) is the number of indices $i \in \{1, \ldots, l-1\}$ (resp. $i \in \{l+1, \ldots, k-2\}$, $i \in \{k, \ldots, t-1\}$) such that $\sigma(i) = i+1$. We expand the determinant (5.4) as follows

$$\boldsymbol{K}_{k,l} = \sum_{\kappa_1+\kappa_2+\kappa_3 \leqslant t-1} \sum_{\sigma \in \mathfrak{S}_t^{(\kappa_1,\kappa_2,\kappa_3)}} (-1)^{\operatorname{sig}(\sigma)} \prod_{\substack{1 \leqslant i \leqslant t \\ i \neq k,l \\ \sigma(i) = i+1}} \epsilon_i \prod_{\substack{1 \leqslant i < l \\ \sigma(i) \leqslant i}} \frac{\partial \Phi_i}{\partial \varphi_{\sigma(i)}} \prod_{\substack{l+1 \leqslant i < k \\ \sigma(i) \leqslant i}} \frac{\partial \Phi_i}{\partial \varphi_{\sigma(i)}} \prod_{\substack{k \leqslant i \leqslant t \\ \sigma(i) \leqslant i}} \frac{\partial \Phi_i}{\partial \varphi_{\sigma(i)}}.$$

Then for all $\sigma \in \mathfrak{S}_t^{(\kappa_1,\kappa_2,\kappa_3)}$ we verify that

$$\begin{aligned}
&\operatorname{val}\left(\prod_{\substack{1\leqslant i<l\\ \sigma(i)\leqslant i}} \frac{\partial\Phi_i}{\partial\varphi_{\sigma(i)}} \prod_{\substack{l+1\leqslant i<k\\ \sigma(i)\leqslant i}} \frac{\partial\Phi_i}{\partial\varphi_{\sigma(i)}} \prod_{\substack{k\leqslant i\leqslant t\\ \sigma(i)\leqslant i}} \frac{\partial\Phi_i}{\partial\varphi_{\sigma(i)}}\right)\\
&\geqslant \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l\\ \sigma(i)\leqslant i}} d_i\gamma_i - \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l\\ \sigma(i)\leqslant i}} \gamma_{\sigma(i)}\\
&= \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l}} d_i\gamma_i - \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l\\ \sigma(i)=i+1}} d_i\gamma_i - \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l}} \gamma_{\sigma(i)} + \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l\\ \sigma(i)=i+1}} \gamma_{\sigma(i)}\\
&= \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l}} d_i\gamma_i - \sum_{\substack{1\leqslant i\leqslant t\\ i\neq k}} \gamma_i + \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l\\ \sigma(i)=i+1}} (\gamma_{i+1} - d_i\gamma_i)\\
&\geqslant \sum_{\substack{1\leqslant i\leqslant t\\ i\neq l}} d_i\gamma_i - \sum_{\substack{1\leqslant i\leqslant t\\ i\neq k}} \gamma_i\\
&= \left(\sum_{1\leqslant i\leqslant t} (d_i-1)\,\gamma_i\right) + \gamma_k - d_l\gamma_l.
\end{aligned}$$

Thanks to Lemma 5.1, this concludes the proof of the lemma when $l \leqslant k$. If $l \geqslant k$, then the determinant

$$\boldsymbol{K}_{k,l} = \begin{vmatrix}
\frac{\partial\Phi_1}{\partial\varphi_1} & -\epsilon_1 & & & & & & \\
\vdots & \ddots & -\epsilon_{k-2} & & & & & \\
\frac{\partial\Phi_{k-1}}{\partial\varphi_1} & \cdots & \frac{\partial\Phi_{k-1}}{\partial\varphi_{k-1}} & & & & 0 & \\
\frac{\partial\Phi_k}{\partial\varphi_1} & \cdots & \frac{\partial\Phi_k}{\partial\varphi_{k-1}} & -\epsilon_k & & & & \\
\frac{\partial\Phi_{k+1}}{\partial\varphi_1} & & \cdots & \frac{\partial\Phi_{k+1}}{\partial\varphi_{k+1}} & -\epsilon_{k+1} & & & \\
\vdots & & & & \ddots & \ddots & & \\
\frac{\partial\Phi_{l-1}}{\partial\varphi_1} & & & \cdots & & \frac{\partial\Phi_{l-1}}{\partial\varphi_{l-1}} & -\epsilon_{l-1} & \\
\frac{\partial\Phi_{l+1}}{\partial\varphi_1} & & & \cdots & & & \frac{\partial\Phi_{l+1}}{\partial\varphi_{l+1}} & -\epsilon_{l+1} \\
\vdots & & & & & & & \ddots \\
\frac{\partial\Phi_t}{\partial\varphi_t} & & & & & \cdots & & \frac{\partial\Phi_t}{\partial\varphi_t}
\end{vmatrix},$$

is block triangular (with three blocks). Applying Lemma 5.1 to the first and third blocks, we obtain

$$\operatorname{in}(\boldsymbol{K}_{k,l}) = (-1)^{l-k+1} \operatorname{in}\left(\frac{\partial\Phi_1}{\partial\varphi_1}\cdots\frac{\partial\Phi_{k-1}}{\partial\varphi_{k-1}}\frac{\partial\Phi_{l+1}}{\partial\varphi_{l+1}}\cdots\frac{\partial\Phi_t}{\partial\varphi_t}\right).$$

It follows that

$$\operatorname{val}\boldsymbol{K}_{k,l} = \sum_{1\leqslant i\leqslant t} (d_i-1)\,\gamma_i - \sum_{k\leqslant i\leqslant l} (d_i-1)\,\gamma_i \geqslant \sum_{1\leqslant i\leqslant t} (d_i-1)\,\gamma_i - d_l\gamma_l + \gamma_k,$$

since $\sum_{i=k}^{l} (d_i-1)\,\gamma_i = d_l\gamma_l - (\gamma_l - d_{l-1}\gamma_{l-1}) - \cdots - (\gamma_{k+1} - d_k\gamma_k) - \gamma_k \leqslant d_l\gamma_l - \gamma_k$. □

5.3. One lifting step

The above valuation estimates now allow us to study of the behavior of the Newton operator of $\boldsymbol{\Phi}_t$ from precision η to 2η. For this purpose, let $\mathbb{L}$ be a valued algebra over $\mathbb{K}((z))$. For $i=1,\ldots,t$, let $a_i \in [\mathbb{L}]_{\gamma_i;\eta}$ be such that

$$[\Phi_i(a_1,\ldots,a_i) - \epsilon_i a_{i+1}]_{d_i\gamma_i;\eta} \;=\; [\Phi_i(a_1,\ldots,a_i) - \epsilon_i a_{i+1}]_{0;d_i\gamma_i+\eta} \;=\; 0$$

and $\boldsymbol{J}_t(a_1,\ldots,a_t)$ is invertible of valuation $\mathrm{val}(\det \boldsymbol{J}_t)$. Still for $i=1,\ldots,t$, we are looking for $\hat{a}_i \in [\mathbb{L}]_{\gamma_i;2\eta}$ such that $[\hat{a}_i]_{\gamma_i;\eta} = a_i$ and

$$[\Phi_i(\hat{a}_1,\ldots,\hat{a}_i) - \epsilon_i \hat{a}_{i+1}]_{d_i\gamma_i;2\eta} \;=\; [\Phi_i(\hat{a}_1,\ldots,\hat{a}_i) - \epsilon_i \hat{a}_{i+1}]_{0;d_i\gamma_i+2\eta} \;=\; 0 \tag{5.5}$$

Setting $\tilde{a}_i := \hat{a}_i - a_i \in [\mathbb{L}]_{\gamma_i+\eta;\eta}$, the first order Taylor expansion of $\boldsymbol{\Phi}_t$ yields

$$\boldsymbol{\Phi}_t(\hat{a}_1,\ldots,\hat{a}_t) \;=\; \boldsymbol{\Phi}_t(a_1,\ldots,a_t) + \boldsymbol{J}_t(a_1,\ldots,a_t) \begin{pmatrix} \tilde{a}_1 \\ \vdots \\ \tilde{a}_t \end{pmatrix} + \begin{pmatrix} \varepsilon_1(a_1,\tilde{a}_1) \\ \vdots \\ \varepsilon_t(a_1,\ldots,a_t,\tilde{a}_1,\ldots,\tilde{a}_t) \end{pmatrix}, \tag{5.6}$$

where ε_i represents the sum of the terms of order at least 2:

$$\varepsilon_i(a_1,\ldots,a_i,\tilde{a}_1,\ldots,\tilde{a}_i) := \sum_{e_1+\cdots+e_i\geqslant 2} (D^{(e_1,\ldots,e_i)}\,\Phi_i)(a_1,\ldots,a_i)\,\tilde{a}_1^{e_1}\cdots\tilde{a}_i^{e_i}.$$

Since $v((D^{(e_1,\ldots,e_i)}\,\Phi_i)(a_1,\ldots,a_i)) \geqslant d_i\gamma_i - e_1\gamma_1 - \cdots - e_i\gamma_i$ and $v(\tilde{a}_i) \geqslant \gamma_i+\eta$, for $i=1,\ldots,t$, we have

$$\begin{aligned}
& v(\varepsilon_i(a_1,\ldots,a_i,\tilde{a}_1,\ldots,\tilde{a}_i)) \\
\geqslant\; & \min_{e_1+\cdots+e_i\geqslant 2} (d_i\gamma_i - e_1\gamma_1 - \cdots - e_i\gamma_i + e_1(\gamma_1+\eta_1) + \cdots + e_i(\gamma_i+\eta_i)) \\
=\; & \min_{e_1+\cdots+e_i\geqslant 2} (d_i\gamma_i + e_1\eta_1 + \cdots + e_i\eta_i) \\
\geqslant\; & d_i\gamma_i + 2\eta.
\end{aligned}$$

After left multiplying both sides of (5.6) by $\mathrm{adj}\, J_t(a_1,\ldots,a_t)$, we obtain that

$$\begin{aligned}
& \mathrm{adj}\,\boldsymbol{J}_t(a_1,\ldots,a_t)\,\boldsymbol{\Phi}_t(\hat{a}_1,\ldots,\hat{a}_t) \\
=\; & \mathrm{adj}\,\boldsymbol{J}_t(a_1,\ldots,a_t)\,\boldsymbol{\Phi}_t(a_1,\ldots,a_t) + \det \boldsymbol{J}_t(a_1,\ldots,a_t) \begin{pmatrix} \tilde{a}_1 \\ \vdots \\ \tilde{a}_t \end{pmatrix} \\
& + \mathrm{adj}\,\boldsymbol{J}_t(a_1,\ldots,a_t) \begin{pmatrix} \varepsilon_1(a_1,\tilde{a}_1) \\ \vdots \\ \varepsilon_t(a_1,\ldots,a_t,\tilde{a}_1,\ldots,\tilde{a}_t) \end{pmatrix}.
\end{aligned}$$

Regarding "v" and "$\geqslant$" component-wise, Lemma 5.2 yields

$$v(\mathrm{adj}\,\boldsymbol{J}_t(a_1,\ldots,a_t)\,\boldsymbol{\Phi}_t(\hat{a}_1,\ldots,\hat{a}_t)) \geqslant \begin{pmatrix} \mathrm{val}(\det \boldsymbol{J}_t) + \gamma_1 + 2\eta \\ \vdots \\ \mathrm{val}(\det \boldsymbol{J}_t) + \gamma_t + 2\eta \end{pmatrix},$$

and

$$v\left(\mathrm{adj}\,\boldsymbol{J}_t(a_1,\ldots,a_t) \begin{pmatrix} \varepsilon_1(a_1,\tilde{a}_1) \\ \vdots \\ \varepsilon_t(a_1,\ldots,a_t,\tilde{a}_1,\ldots,\tilde{a}_t) \end{pmatrix}\right) \geqslant \begin{pmatrix} \mathrm{val}(\det \boldsymbol{J}_t) + \gamma_1 + 2\eta \\ \vdots \\ \mathrm{val}(\det \boldsymbol{J}_t) + \gamma_t + 2\eta \end{pmatrix}.$$

It follows that

$$v\left(\mathrm{adj}\,\boldsymbol{J}_t(a_1,\ldots,a_t)\,\boldsymbol{\Phi}_t(a_1,\ldots,a_t) + \det \boldsymbol{J}_t(a_1,\ldots,a_t) \begin{pmatrix} \tilde{a}_1 \\ \vdots \\ \tilde{a}_t \end{pmatrix}\right) \;\geqslant\; \begin{pmatrix} \mathrm{val}(\det \boldsymbol{J}_t) + \gamma_1 + 2\eta \\ \vdots \\ \mathrm{val}(\det \boldsymbol{J}_t) + \gamma_t + 2\eta \end{pmatrix}.$$

Consequently, under the contraints on the valuations of the $\hat{a}_i$, equations (5.5) are equivalent to

$$\begin{pmatrix} b_1 \\ \vdots \\ b_t \end{pmatrix} := -\frac{\operatorname{adj} \boldsymbol{J}_t(a_1,\ldots,a_t)}{\det \boldsymbol{J}_t(a_1,\ldots,a_t)} \boldsymbol{\Phi}_t(a_1,\ldots,a_t). \tag{5.7}$$

Finally we have shown that the $\tilde{a}_i$ exist and are uniquely determined by

$$\begin{pmatrix} \tilde{a}_1 \\ \vdots \\ \tilde{a}_t \end{pmatrix} = \begin{pmatrix} [b_1]_{0;\gamma_1+2\eta} \\ \vdots \\ [b_t]_{0;\gamma_t+2\eta} \end{pmatrix} = \begin{pmatrix} [b_1]_{\gamma_1+\eta;\eta} \\ \vdots \\ [b_t]_{\gamma_t+\eta;\eta} \end{pmatrix}.$$

In other words

$$\begin{pmatrix} \hat{a}_1 \\ \vdots \\ \hat{a}_t \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix} + \begin{pmatrix} [b_1]_{\gamma_1+\eta;\eta} \\ \vdots \\ [b_t]_{\gamma_t+\eta;\eta} \end{pmatrix}.$$

is the unique solution of (5.5).

5.4. Complete lifting

We are now ready to extend Proposition 4.10 for the computation of univariate-valued representations at higher precisions. The following algorithm is adapted from [5, Section 4].

Algorithm 5.1

Input. An effectively separable and regular contact tower $(\mathbb{P}_i)_{i\leqslant t}$. An integer $h<t$, and a relative precision $\rho \in R_t^{-1}\mathbb{N}^{>0}$.

Output. A univariate-valued representation of $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$ at precision ρ.

Assumption. $\epsilon_h = \epsilon_t = 0$, and we are given $>(D_h^{-1}D_t)^2$ distinct elements in $\mathbb{K}$.

1. Compute $\varpi, \chi, w_{h+1}, \ldots, w_t$ as in Proposition 4.10 and let $\eta := R_t^{-1}$.
2. While $\eta < \rho$ do:
   a. Compute $(\tilde{w}_{h+1}(T),\ldots,\tilde{w}_t(T))^{\top}$ modulo $\chi(T)$ at relative precision 2η as $-\dfrac{\operatorname{adj} \boldsymbol{J}_t(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_t(T))}{\det \boldsymbol{J}_t(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_t(T))} \boldsymbol{\Phi}_t(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_t(T))$.
   b. Compute $\hat{w}_i(T) := [w_i(T) + \tilde{w}_i(T)]_{\gamma_i;2\eta}$, for $i = h+1,\ldots,t$.
   c. Compute $\Delta(T) := [(\varpi(\varphi_1,\ldots,\varphi_h,\hat{w}_{h+1}(T),\ldots,\hat{w}_t(T)) - T) \operatorname{rem} \chi(T)]_{R_t^{-1};2\eta}$.
   d. Compute $\bar{\chi}(T) := [\chi - (\Delta\chi') \operatorname{rem} \chi]_{(D_h^{-1}D_t)R_t^{-1};2\eta}$.
   e. For $i = h+1,\ldots,t$, compute $\bar{w}_i := [\hat{w}_i - (\Delta w_i') \operatorname{rem} \chi]_{\gamma_i;2\eta}$.
   f. Replace η by $\min(2\eta,\rho)$, χ by $\bar{\chi}$ and w_i by $\bar{w}_i$, for $i = h+1,\ldots,t$.
3. Return $\varpi, \chi, w_{h+1}, \ldots, w_t$.

PROPOSITION 5.3. *Algorithm 5.1 is correct. If $\mathbb{P}_t$ is almost reduced, then it performs*

$$\begin{aligned} &\tilde{O}(D_t^{1+\epsilon}(D_h^{-1}D_t)^6 \operatorname{ht}\gamma_t) \\ +\ &\tilde{O}(\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\rho,1)\,D_h^{-1}D_t)^2 D_h^{-1}D_t \operatorname{ht}\rho \log^4 D_t) \end{aligned}$$

operations in $\mathbb{K}$. In addition, the polynomials $\chi, w_{h+1}, \ldots, w_t$ of a univariate-valued representation are uniquely determined at precision ρ by the contact tower $\mathbb{P}_t$ and the choice of ϖ. The constant coefficient $\chi(0)$ is initially invertible in $\mathbb{P}_h$ of valuation $(D_h^{-1}D_t)\,R_t^{-1}$.

Proof. Let

$$\mathbb{L} := (\mathbb{P}_h/(\varphi_{t+1}))[T]/(\chi(T))$$

and let $v(\cdot;\mathbb{L})$ be the extension of $v(\cdot;\mathbb{P}_h)$ to $\mathbb{L}$, so $v(T;\mathbb{L}) = R_t^{-1}$. Proposition 4.10 gives us a univariate-valued representation at precision $\eta = R_t^{-1}$. Note that ϖ is homogeneous, and that χ and the w_i are uniquely determined by the choice of ϖ at this precision.

In step 2.a, the Newton iteration (5.7) is applied to

$$\begin{aligned} a_i &:= \varphi_i, \text{ for } i = 1, \ldots, h \\ a_i &:= w_i(T), \text{ for } i = h+1, \ldots, t. \end{aligned}$$

Note that $\tilde{w}_i = 0$, for $i = 1,...,h$. At the end of step 2.b, we obtain $[\hat{w}_i(T)]_{\gamma_i;\eta} = [w_i(T)]_{\gamma_i;\eta}$ and

$$[(\Phi_i(\varphi_1, \ldots, \varphi_h, \hat{w}_{h+1}(T), \ldots, \hat{w}_i(T)) - \epsilon_i \hat{w}_{i+1}(T)) \operatorname{rem} \chi(T)]_{d_i\gamma_i;2\eta} = 0,$$

for $i = h+1, \ldots, t$. The $\hat{w}_i$ are uniquely determined by these properties, under the constraints on the valuation of the $\hat{w}_i(T)$.

By construction, $\Delta(T)$ has valuation $\geqslant R_t^{-1} + \eta$ and therefore $\bar{\chi}, \bar{w}_{h+1}, \ldots, \bar{w}_t$ coincide with $\chi, w_{h+1}, \ldots, w_t$ at precision η. It follows that

$$\begin{aligned} [\bar{\chi}(T+\Delta) \operatorname{rem} \chi]_{(D_h^{-1}D_t)R_t^{-1};2\eta} &= [(\bar{\chi} + (\Delta\bar{\chi}')) \operatorname{rem} \chi]_{(D_h^{-1}D_t)R_t^{-1};2\eta} \\ &= [(\chi - \Delta(\chi' - \bar{\chi}')) \operatorname{rem} \chi]_{(D_h^{-1}D_t)R_t^{-1};2\eta} \\ &= 0, \end{aligned}$$

and that

$$\begin{aligned} [\bar{w}_i(T+\Delta) \operatorname{rem} \chi]_{\gamma_i;2\eta} &= [(\bar{w}_i + (\Delta\bar{w}_i')) \operatorname{rem} \chi]_{\gamma_i;2\eta} \\ &= [\hat{w}_i - \Delta(w_i' - \bar{w}_i') \operatorname{rem} \chi]_{\gamma_i;2\eta} \\ &= \hat{w}_i, \end{aligned}$$

for $i = h+1, \ldots, t$. It follows that

$$\begin{aligned} & [(\Phi_i(\varphi_1, \ldots, \varphi_h, \bar{w}_{h+1}(T), \ldots, \bar{w}_i(T)) - \epsilon_i \bar{w}_{i+1}(T)) \operatorname{rem} \bar{\chi}(T)]_{d_i\gamma_i;2\eta} \\ = \; & [(\Phi_i(\varphi_1, \ldots, \varphi_h, \hat{w}_{h+1}(T-\Delta), \ldots, \hat{w}_i(T-\Delta)) - \epsilon_i \hat{w}_{i+1}(T-\Delta)) \operatorname{rem} \chi(T-\Delta)]_{d_i\gamma_i;2\eta} \\ = \; & [((\Phi_i(\varphi_1, \ldots, \varphi_h, \hat{w}_{h+1}(T), \ldots, \hat{w}_i(T)) - \epsilon_i \hat{w}_{i+1}(T)) \operatorname{rem} \chi(T))(T-\Delta)]_{d_i\gamma_i;2\eta} \\ = \; & 0 \end{aligned}$$

holds for $i = h+1, \ldots, t$, and similarly that

$$\begin{aligned} & [(\varpi(\varphi_1, \ldots, \varphi_h, \bar{w}_{h+1}(T), \ldots, \bar{w}_t(T)) - T) \operatorname{rem} \bar{\chi}(T)]_{R_t^{-1};2\eta} \\ = \; & [((\varpi(\varphi_1, \ldots, \varphi_h, \hat{w}_{h+1}(T), \ldots, \hat{w}_t(T)) - (T+\Delta)) \operatorname{rem} \chi(T))(T-\Delta)]_{R_t^{-1};2\eta} \\ = \; & 0. \end{aligned}$$

This proves that the values for $\varpi, \chi, w_{h+1}, \ldots, w_t$ returned by the algorithm actually constitute a univariate-valued representation of $\mathbb{P}_t/(\varphi_{t+1})$ over $\mathbb{P}_h/(\varphi_{h+1})$ at precision ρ. We are done with the correctness. The latter calculations further show that such a univariate-valued representation $\bar{\chi}, \bar{w}_{h+1}, \ldots, \bar{w}_t$ in terms of ϖ is unique.

Let us now assess the complexity. By Proposition 4.10 we compute $\varpi, \chi, w_{h+1}, \ldots, w_t$ at precision R_t^{-1} in time

$$\tilde{O}(D_t^{1+\epsilon}(D_h^{-1}D_t)^6 \operatorname{ht}\gamma_t). \tag{5.8}$$

Assuming that operations in $\mathbb{P}_h/(\varphi_{h+1})$ with relative precision ρ can be done using $\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))$ operations in $\mathbb{K}$, one operation in $\mathbb{P}_h[T]/(\varphi_{h+1},\chi(T))$ at relative precision ρ does not exceed

$$O(\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho))\,(\min(R_h\rho,1)\,(D_h^{-1}D_t))^2),$$

by using the schoolbook methods, thanks to Lemma 2.2.

For $i=h+1,\ldots,t$, the evaluation of all the Φ_i and of the Jacobian $\boldsymbol{J}_t$ at $(\varphi_1,\ldots,\varphi_h, w_{h+1}(T),\ldots,w_t(T))$ modulo $\chi(T)$ at relative precision ρ costs

$$\tilde{O}((\min(R_h\rho,1)\,D_h^{-1}D_t)^2 D_h^{-1}D_t t^2) \tag{5.9}$$

operations in $\mathbb{P}_h/(\varphi_{h+1})$. The determinant and the adjunct matrix of $\boldsymbol{J}_t(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots, w_t(T))$ modulo $\chi(T)$ can be obtained using

$$\tilde{O}((\min(R_h\rho,1)\,D_h^{-1}D_t)^2 t^4) \tag{5.10}$$

operations in $\mathbb{P}_h/(\varphi_{h+1})$ by using the Berkowitz algorithm. By Lemma 5.1 the initial inverse of

$$\det(\boldsymbol{J}_t(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_t(T)))$$

can be computed as the initial of

$$(\Delta_1(\varphi_1)\cdots\Delta_t(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_t(T)))\operatorname{rem}\chi(T),$$

in time bounded by (5.9), where Δ_i represents the initial inverse of $\frac{\partial\Phi_i}{\partial\varphi_i}$.

The inverse of $\det\boldsymbol{J}_t(\varphi_1,\ldots,\varphi_h,w_{h+1}(T),\ldots,w_t(T))$ at precision ρ can be lifted efficiently via the usual Newton iteration, using $O(\log(R_t\rho))=O(\mathrm{ht}\,\rho)$ operations in $\mathbb{P}_h[T]/(\varphi_{h+1},\chi(T))$.

Since ϖ is homogeneous in $\mathbb{K}((z))[\varphi_1,\ldots,\varphi_t]_{<(d_1,\ldots,d_t)}$, its evaluation in step 2.c does not exceed (5.9). Computing $\bar{\chi}$ and $\bar{w}_{h+1},\ldots,\bar{w}_t$ takes $\tilde{O}((\min(R_h\rho,1)\,D_h^{-1}D_t)^2 t)$ further operations in $\mathbb{P}_h/(\varphi_{h+1})$. We conclude by adding the costs of all these intermediate tasks. □

Example 5.4. (Continued from Example 4.11) We are interested in lifting the univariate-valued representation of Example 4.11 with $\epsilon_1=\epsilon_3=0$, $\epsilon_2=1$, and precision $\rho=1/4$. We enter the lifting at precision $1/8$ with

$$\begin{aligned}
\varpi &= 2z^{-17}\varphi_1\varphi_2^2\varphi_3^3+(4z^{-8}\varphi_1\varphi_2^2+z^{-5})\,\varphi_3\\
\chi(T) &= T^{16}+3\varphi_1T^{12}+6zT^8+2z\varphi_1T^4+9z^2\\
w_2(T) &= 6z^{-1}\varphi_1T^{14}+8T^{10}+5\varphi_1T^6+2zT^2\\
w_3(T) &= 7z^3\varphi_1T^{13}+9z^4T^9+4z^4\varphi_1T^5+z^5T.
\end{aligned}$$

We have

$$\begin{aligned}
\Phi_2(\varphi_1,w_2(T))-w_3(T)\operatorname{rem}\chi(T) &= -w_3(T)\\
\Phi_3(\varphi_1,w_2(T),w_3(T))\operatorname{rem}\chi(T) &= 0.
\end{aligned}$$

With the notation of Algorithm 5.1, we perform following Newton iteration at relative precision $2\eta=1/4$:

$$\begin{aligned}
\begin{pmatrix}\tilde{w}_2(T)\\ \tilde{w}_3(T)\end{pmatrix} &= -\begin{pmatrix}4w_2(T)^3 & 0\\ -2z^{18}w_2(T) & 4w_3(T)^3\end{pmatrix}^{-1}\begin{pmatrix}\Phi_2(\varphi_1,w_2(T))-w_3(T)\\ \Phi_3(\varphi_1,w_2(T),w_3(T))\end{pmatrix}\bmod\chi(T)\\
&= \begin{pmatrix}5z^{-1}\varphi_1T^{15}+7T^{11}+7\varphi_1T^7+8zT^3\\ 7T^{10}\end{pmatrix}.
\end{aligned}$$

Then, we obtain

$$\Delta(T) = 3\varphi_1 T^{14} + T^{10} + 8\varphi_1 T^6 + 2T^2,$$

and deduce the univariate-valued representation at relative precision $2\eta = 1/4$:

$$\begin{aligned}
\bar{\chi}(T) &= T^{16} + \varphi_1 T^{13} + 3\varphi_1 T^{12} + 7zT^9 + 6zT^8 + 2z\varphi_1 T^4 + 9z^2 \\
\bar{w}_2(T) &= z^{-1}\varphi_1 T^{15} + 6z^{-1}\varphi_1 T^{14} + 8T^{10} + 7\varphi_1 T^7 + 5\varphi_1 T^6 + 2zT^3 + 2zT^2 \\
\bar{w}_3(T) &= 7z^3\varphi_1 T^{14} + 7z^3\varphi_1 T^{13} + 7z^4 T^{10} + 9z^4 T^9 + 6z^4\varphi_1 T^6 + 4z^4\varphi_1 T^5 + z^5 T^2 + z^5 T.
\end{aligned}$$

6. FLATTENED REPRESENTATION

For this section we are given a generalized contact tower $(\mathbb{P}_i)_{i\leqslant t}$, of the form

$$\mathbb{P}_i := \mathbb{K}((z))[\varphi_1, \ldots, \varphi_{i+1}] / (\Phi_1(\varphi_1) - \epsilon_1\varphi_2, \Phi_2(\varphi_1, \varphi_2) - \epsilon_2\varphi_3, \ldots, \Phi_i(\varphi_1, \ldots, \varphi_i) - \epsilon_i\varphi_{i+1}).$$

We wish to compute in $\mathbb{P}_t$ at relative precision $\rho > 0$, which leads us to assume that $\epsilon_i = 1$ if $\gamma_{i+1} - d_i\gamma_i < \rho$ and $\epsilon_i = 0$ otherwise, for $i = 1, \ldots, t$.

6.1. Flattenings

The complexity bounds of section 3 for computing with contact polynomials grow exponentially with the height t of the tower. In order to circumvent this dependency on t, we will replace consecutive levels of the tower of low degree by a single level. This tactic was used before in the simpler context of towers of algebraic extension and gave rise to so-called accelerated tower arithmetic [9].

Unfortunately, when compressing several levels in a contact tower, the resulting "flattened" tower will not be of contact type. There will be two main types of flattenings. The first type introduces an algebraic extension which violates the condition that $\gamma_{i+1} > d_i\gamma_i$ for all i. The second type of flattening gives rise to a defining polynomial that is not initially separable and that will necessitate increasing the relative precision.

In order to cover these two types of flattenings, plus a trivial third one, we need the following technical definition. For simplicity the tower will be assumed almost reduced, and the first level (that was allowed to be of degree one) is left unchanged.

DEFINITION 6.1. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an almost reduced generalized contact tower such that $\epsilon_i := 1$ if $\gamma_{i+1} - d_i\gamma_i < \rho$ and $\epsilon_i := 0$ otherwise, for $i = 1, \ldots, t$. A tower $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ of the form*

$$\tilde{\mathbb{P}}_j := \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{j+1}] / (\tilde{\Phi}_1(\tilde{\varphi}_1) - \tilde{\epsilon}_1\tilde{\varphi}_2, \tilde{\Phi}_2(\tilde{\varphi}_1, \tilde{\varphi}_2) - \tilde{\epsilon}_2\tilde{\varphi}_3, \ldots, \tilde{\Phi}_j(\tilde{\varphi}_1, \ldots, \tilde{\varphi}_j) - \tilde{\epsilon}_j\tilde{\varphi}_{j+1}),$$

for $j = 1, \ldots, \tilde{t}$ is a **flattening** *for $(\mathbb{P}_i)_{i\leqslant t}$ at relative precision ρ if*

1. *$\tilde{\Phi}_j \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{j-1}]_{<(\tilde{d}_1, \ldots, \tilde{d}_{j-1})}[\tilde{\varphi}_j]$ is monic of degree in $\tilde{\varphi}_j$ written $\tilde{d}_j$, for $j = 1, \ldots, \tilde{t}$, with $\tilde{\Phi}_1(\tilde{\varphi}_1) = \Phi_1(\tilde{\varphi}_1)$.*
2. *There exists an integer sequence*

$$0 = i_0 < i_1 < \cdots < i_{\tilde{t}} = t,$$

with $i_1 = 1$, and a sequence of $\mathbb{K}((z))$-algebra isomorphisms

$$\xi_j: \quad \mathbb{P}_{i_j} \to \tilde{\mathbb{P}}_j$$

with the following properties for $j = 1, \ldots, \tilde{t}$:

F1. *$\tilde{\epsilon}_j = \epsilon_{i_j}$;*

F₂. *The restriction of* ξ_j *to* $(\mathbb{P}_{i_{j-1}})_{<1}$ *coincides with* ξ_{j-1};

F₃. *The projection of* $\mathbb{K}((z))[\tilde\varphi_1,\dots,\tilde\varphi_j]_{<(\tilde d_1,\dots,\tilde d_j)}$ *to* $\tilde{\mathbb{P}}_j$ *is injective and equals* $\xi_j((\mathbb{P}_{i_j})_{<1})$;

F₄. $\xi_j(\varphi_{i_j+1})=\tilde\varphi_{j+1}$;

F₅. *If* $j<\tilde t$ *and* $\epsilon_{i_j}=1$ *then* $\xi_{j+1}(\varphi_{i_j+1})=\tilde\varphi_{j+1}$;

F₆. $v\Big(\xi_j^{-1}\Big(\tilde\Phi_j-\tilde\varphi_j^{\tilde d_j}\Big);\mathbb{P}_{i_{j-1}}\Big)\geqslant \tilde d_j v(\xi_j^{-1}(\tilde\varphi_j);\mathbb{P}_{i_j})$

3. *For* $j=1,\dots,\tilde t$, *there exists* $\tilde\Omega_j\in\mathbb{K}((z))[\tilde\varphi_1,\dots,\tilde\varphi_{j-1}]_{<(\tilde d_1,\dots,\tilde d_{j-1})}[\tilde\varphi_j]$ *monic of degree* $\tilde d_j$ *in* $\tilde\varphi_j$ *such that the image of* $\tilde\Omega_j\tilde\Phi_j$ *in* $\tilde{\mathbb{P}}_{j-1}$ *belongs to the image of*

$$\tilde\varphi_j^{2\tilde d_j}+\mathbb{K}((z))[\tilde\varphi_1,\dots,\tilde\varphi_j]_{<(\tilde d_1,\dots,\tilde d_j)}$$

in $\tilde{\mathbb{P}}_{j-1}$, *and that* $v\Big(\xi_j^{-1}\Big(\tilde\Omega_j-\tilde\varphi_j^{\tilde d_j}\Big);\mathbb{P}_{i_{j-1}}\Big)\geqslant\tilde d_j v(\xi_j^{-1}(\tilde\varphi_j);\mathbb{P}_{i_j})$.

Property **F₄** imposes the natural image $\xi_j(\varphi_{i_j+1})=\tilde\varphi_{j+1}$. If $\epsilon_{i_j}=\tilde\epsilon_j=1$, then **F₅** naturally extends this requirement to ξ_{j+1}; the image $\xi_{j+1}(\varphi_{i_j+1})$ might have been chosen more arbitrarily if $\epsilon_{i_j}=\tilde\epsilon_j=0$. Property **F₆** ensures that the defining polynomial $\tilde\Phi_j$ is clustered as an element of $\mathbb{P}_{i_{j-1}}$. The polynomial $\tilde\Omega_j$ is required to be the clustered pre-inverse of $\tilde\Phi_j$ in $\mathbb{P}_{i_{j-1}}$.

As a consequence of the definition, the pre-image $\xi_j^{-1}(A)$ of an element $A\in\tilde{\mathbb{P}}_j$ can be written

$$\xi_j^{-1}(A)=\sum_{k\geqslant 0} b_k\varphi_{i_j+1}^k,$$

where $b_k\in(\mathbb{P}_{i_j})_{<1}$. The representation of A in the form

$$A=\sum_{k\geqslant 0} a_k\tilde\varphi_{j+1}^k,$$

where $a_k=\xi_j(b_k)\in\mathbb{K}((z))[\tilde\varphi_1,\dots,\tilde\varphi_j]_{<(\tilde d_1,\dots,\tilde d_j)}$, will be said **canonical**. In particular we note that $\tilde d_j=d_{i_{j-1}+1}\cdots d_{i_j}$, for $j=1,\dots,\tilde t$, that $\tilde d_1=d_1$ may be equal to one, and that $\tilde d_j\geqslant 2$ for $j=2,\dots,\tilde t$.

In the rest of the paper, the canonical representation of an element A of $\tilde{\mathbb{P}}_j$ will be written $\mathrm{red}_j A$. We will also write $\deg_{\tilde\varphi_{j+1}}(\mathrm{red}_j A)$ for its degree in $\tilde\varphi_{j+1}$ and $(\tilde{\mathbb{P}}_j)_{<l}$ for the elements whose canonical representative has degree $<l$ in $\tilde\varphi_{j+1}$.

For $k=0,\dots,\tilde t$, we endow $\mathbb{K}((z))[\tilde\varphi_1,\dots,\tilde\varphi_{k+1}]$ with the weighted valuation, written val_k, defined by

$$\begin{aligned}\mathrm{val}_k\,\tilde\varphi_1 &:= \gamma_1\\ \mathrm{val}_k\,\tilde\varphi_j &:= v(\xi_k^{-1}(\tilde\varphi_j);\mathbb{P}_{i_k}),\ \text{for } j=2,\dots,k+1.\end{aligned}\tag{6.1}$$

In particular **F₄** implies $\mathrm{val}_k\,\tilde\varphi_{k+1}=\gamma_{i_k+1}$. For $2\leqslant j\leqslant k$, by **F₃** we have $\xi_k^{-1}(\tilde\varphi_j)\in(\mathbb{P}_{i_k})_{<1}$, while $\xi_{\tilde t}^{-1}$ coincides with ξ_k^{-1} on $(\mathbb{P}_{i_k})_{<1}$ by **F₂**. Consequently,

$$\mathrm{val}_{\tilde t}\,\tilde\varphi_j=v(\xi_{\tilde t}^{-1}(\tilde\varphi_j);\mathbb{P}_t)=v(\xi_k^{-1}(\tilde\varphi_j);\mathbb{P}_{i_k})=\mathrm{val}_k\,\tilde\varphi_j,\ \text{whenever } j\leqslant k\leqslant\tilde t.\tag{6.2}$$

We set $\tilde\gamma_1:=\gamma_1$ and $\tilde\gamma_j:=\mathrm{val}_j\,\tilde\varphi_j$ for $j=2,\dots,\tilde t$. If $j<\tilde t$, note that **F₅** implies

$$\tilde\gamma_{j+1}=\mathrm{val}_{j+1}\,\tilde\varphi_{j+1}=v(\xi_{j+1}^{-1}(\tilde\varphi_{j+1});\mathbb{P}_{i_{j+1}})=\gamma_{i_j+1},\ \text{whenever } \epsilon_{i_j}=1.\tag{6.3}$$

Given $\tilde P\in\mathbb{K}((z))[\tilde\varphi_1,\dots,\tilde\varphi_{\tilde t+1}]$ the notation $[\tilde P;\mathbb{K}((z))[\tilde\varphi_1,\dots,\tilde\varphi_{\tilde t+1}]]_{\sigma;\rho}$ will stand for the truncation of $\tilde P$ from valuation σ and precision ρ with respect to $\mathrm{val}_{\tilde t}$.

Example 6.2. Let us consider the following contact tower of height $t := 4$ over $\mathbb{K} := \mathbb{Q}$:

$$\begin{aligned}\Phi_1(\varphi_1) &= \varphi_1 - 1 - z\\ \Phi_2(\varphi_1,\varphi_2) &= \varphi_2^2 - z\\ \Phi_3(\varphi_1,\varphi_2,\varphi_3) &= \varphi_3^2 - z^2\varphi_2\\ \Phi_4(\varphi_1,\varphi_2,\varphi_3,\varphi_4) &= \varphi_4^2 - z^4\varphi_3,\end{aligned}$$

with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 1$, so $d_1 = 1$, $d_2 = d_3 = d_4 = 2$, $\gamma_1 = 0$, $\gamma_2 = 1/2$, $\gamma_3 = 5/4$, $\gamma_4 = 21/8$, $\gamma_5 := +\infty$. By definition, the first level of the flattening is "trivial", with $\tilde\Phi_1(\tilde\varphi_1) := \Phi_1(\tilde\varphi_1)$:

$$\begin{aligned}\xi_1\colon\quad \mathbb{P}_1 &\to \tilde{\mathbb{P}}_1\\ \varphi_1 &\mapsto \tilde\varphi_1\\ \varphi_2 &\mapsto \tilde\varphi_2.\end{aligned}$$

Then, we build a second level, that will be called of "second type" in section 7.3, with $i_1 = 1$, $i_2 := 3$,

$$\tilde\Phi_2(\tilde\varphi_1,\tilde\varphi_2) := \Phi_3(\tilde\varphi_1,\tilde\varphi_2,\Phi_2(\tilde\varphi_1,\tilde\varphi_2)),$$

and

$$\begin{aligned}\xi_2\colon\quad \mathbb{P}_3 &\to \tilde{\mathbb{P}}_2\\ \varphi_1 &\mapsto \tilde\varphi_1\\ \varphi_2 &\mapsto \tilde\varphi_2\\ \varphi_3 &\mapsto \tilde\Phi_2(\tilde\varphi_1,\tilde\varphi_2)\\ \varphi_4 &\mapsto \tilde\varphi_3 = \Phi_3(\tilde\varphi_1,\tilde\varphi_2,\Phi_2(\tilde\varphi_1,\tilde\varphi_2))\end{aligned}$$

The third level of the flattening is "trivial", that is $i_3 := 4$,

$$\tilde\Phi_3(\tilde\varphi_1,\tilde\varphi_2,\tilde\varphi_3) := \Phi_4(\tilde\varphi_1,\tilde\varphi_2,\Phi_2(\tilde\varphi_1,\tilde\varphi_2),\tilde\varphi_3),$$

and

$$\begin{aligned}\xi_3\colon\quad \mathbb{P}_4 &\to \tilde{\mathbb{P}}_3\\ \varphi_1 &\mapsto \tilde\varphi_1\\ \varphi_2 &\mapsto \tilde\varphi_2\\ \varphi_3 &\mapsto \tilde\Phi_2(\tilde\varphi_1,\tilde\varphi_2)\\ \varphi_4 &\mapsto \tilde\varphi_3 = \Phi_3(\tilde\varphi_1,\tilde\varphi_2,\Phi_2(\tilde\varphi_1,\tilde\varphi_2))\\ \varphi_5 &\mapsto \tilde\varphi_4 = \tilde\Phi_3(\tilde\varphi_1,\tilde\varphi_2,\tilde\varphi_3).\end{aligned}$$

We have $\tilde\gamma_1 = \gamma_1$, $\tilde\gamma_2 = \gamma_2$, $\tilde\gamma_3 = \gamma_4$.

Assume that $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde t}$ is a flattening for $(\mathbb{P}_i)_{i\leqslant t}$ at precision ρ. For any $j = 1,\ldots,\tilde t$, we note that $(\tilde{\mathbb{P}}_{j'})_{j'\leqslant j}$ is again a flattening for $(\mathbb{P}_{i'})_{i'\leqslant i_j}$ at precision ρ. Flattenings will be built by induction on the height, so it will be useful to keep in mind that

$$\begin{aligned}\mathbb{P}_{i_j} &= \mathbb{P}_{i_{j-1}}[\varphi_{i_{j-1}+2},\ldots,\varphi_{i_j+1}]/(\Phi_{i_{j-1}+1}(\varphi_1,\ldots,\varphi_{i_{j-1}+1}) - \epsilon_{i_{j-1}+1}\varphi_{i_j+2},\ldots,\\ &\qquad\qquad \Phi_{i_j}(\varphi_1,\ldots,\varphi_{i_j}) - \epsilon_{i_j}\varphi_{i_j+1})\\ \tilde{\mathbb{P}}_j &= \tilde{\mathbb{P}}_{j-1}[\tilde\varphi_{j+1}]/(\tilde\Phi_j(\tilde\varphi_1,\ldots,\tilde\varphi_j) - \tilde\epsilon_j\tilde\varphi_{j+1}).\end{aligned}$$

LEMMA 6.3. *The canonical representative $\tilde A$ of an element of $\tilde{\mathbb{P}}_{\tilde t}$ satisfies*

$$\operatorname{val}_{\tilde t}\tilde A \leqslant v(\xi_{\tilde t}^{-1}(\tilde A);\mathbb{P}_t).$$

Proof. We first handle the case where $\tilde{A} \in (\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$. Let us write

$$\tilde{A} = \sum_{0 \leqslant k < \tilde{d}_{\tilde{t}}} \tilde{a}_k \tilde{\varphi}_{\tilde{t}}^k,$$

where $\tilde{a}_0, \ldots, \tilde{a}_{\tilde{d}_{\tilde{t}}-1}$ are in $(\tilde{\mathbb{P}}_{\tilde{t}-1})_{<1}$. The proof is done by induction on $\tilde{t}$. The case $\tilde{t} = 0$ is clear. Let us assume that the lemma holds for $\tilde{t} - 1 \geqslant 0$. We verify that

$$\begin{aligned}
v(\xi_{\tilde{t}}^{-1}(\tilde{A}); \mathbb{P}_t) &= v\left(\sum_{0 \leqslant k < \tilde{d}_{\tilde{t}}} \xi_{\tilde{t}-1}^{-1}(\tilde{a}_k)\, \xi_{\tilde{t}}^{-1}(\tilde{\varphi}_{\tilde{t}})^k; \mathbb{P}_t \right) && \text{(by } \mathbf{F_2}\text{)} \\
&\geqslant \min_{0 \leqslant k < \tilde{d}_{\tilde{t}}} \left(v(\xi_{\tilde{t}-1}^{-1}(\tilde{a}_k); \mathbb{P}_{i_{\tilde{t}-1}}) + v(\xi_{\tilde{t}}^{-1}(\tilde{\varphi}_{\tilde{t}})^k; \mathbb{P}_t) \right) \\
&\geqslant \min_{0 \leqslant k < \tilde{d}_{\tilde{t}}} \left(\mathrm{val}_{\tilde{t}-1} \tilde{a}_k + k \,\mathrm{val}_{\tilde{t}}\, \tilde{\varphi}_{\tilde{t}} \right) && \text{(by induction)} \\
&= \min_{0 \leqslant k < \tilde{d}_{\tilde{t}}} \left(\mathrm{val}_{\tilde{t}} \tilde{a}_k + k \,\mathrm{val}_{\tilde{t}}\, \tilde{\varphi}_{\tilde{t}} \right) && \text{(by (6.2))} \\
&= \mathrm{val}_{\tilde{t}} \tilde{A}. && (6.4)
\end{aligned}$$

Now consider a general $\tilde{A} = \sum_{k \geqslant 0} \tilde{a}_k \tilde{\varphi}_{\tilde{t}+1}^k$, written canonically:

$$\begin{aligned}
v(\xi_{\tilde{t}}^{-1}(\tilde{A}); \mathbb{P}_t) &= v\left(\sum_{k \geqslant 0} \xi_{\tilde{t}}^{-1}(\tilde{a}_k)\, \varphi_{t+1}^k; \mathbb{P}_t \right) && \text{(by } \mathbf{F_4}\text{)} \\
&\geqslant \min_{k \geqslant 0} \left(v(\xi_{\tilde{t}}^{-1}(\tilde{a}_k); \mathbb{P}_t) + k\, v(\varphi_{t+1}; \mathbb{P}_t) \right) && \text{(by (6.4))} \\
&\geqslant \min_{k \geqslant 0} \left(\mathrm{val}_{\tilde{t}} \tilde{a}_k + k \,\mathrm{val}_{\tilde{t}}\, \tilde{\varphi}_{\tilde{t}+1} \right) && \text{(by } \mathbf{F_4} \text{ and (6.1))} \\
&= \mathrm{val}_{\tilde{t}} \tilde{A}. && \square
\end{aligned}$$

We define the following important quantity, called the **defect** of ξ_j, that measures the loss of precision when converting contact polynomials via ξ_j:

$$\mathrm{dct}\, \xi_j := \max_{A \in (\mathbb{P}_{i_j})_{<1}} \left(v(A; \mathbb{P}_{i_j}) - \mathrm{val}_j(\mathrm{red}_j(\xi_j(A))) \right). \tag{6.5}$$

By Lemma 6.3 the backward conversion does not cause any precision loss. If A is in $\mathbb{P}_t$ and if $\tilde{A} = \sum_{k \geqslant 0} \tilde{a}_k \tilde{\varphi}_{\tilde{t}+1}^k$ is the canonical representative of $\xi_{\tilde{t}}(A)$, then we have

$$\begin{aligned}
\mathrm{val}_{\tilde{t}} \tilde{A} &= \min_{k \geqslant 0} \left(\mathrm{val}_{\tilde{t}} \tilde{a}_k + k \gamma_{t+1} \right) \\
&\geqslant \min_{k \geqslant 0} \left(v(\xi_{\tilde{t}}^{-1}(\tilde{a}_k); \mathbb{P}_t) - \mathrm{dct}\, \xi_{\tilde{t}} + k \gamma_{t+1} \right) \\
&= v(A; \mathbb{P}_t) - \mathrm{dct}\, \xi_{\tilde{t}}. && (6.6)
\end{aligned}$$

In order to multiply two elements of $(\mathbb{P}_t)_{<1}$, we shall first convert them into their canonical representations in $(\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$, then compute their product in $\mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_t]$, next reduce this product into its canonical representative in $\tilde{\mathbb{P}}_{\tilde{t}}$, and finally convert the result back into $(\mathbb{P}_t)_{<2}$. The following proposition details the extra precision needed for this approach.

PROPOSITION 6.4. *Let A and B be in $(\mathbb{P}_t)_{<1}$ at relative precision ρ, let $\tilde{A}$ and $\tilde{B}$ be the canonical representatives of $\xi_{\tilde{t}}(A)$ and $\xi_{\tilde{t}}(B)$, let $\tilde{P} := \tilde{A}\,\tilde{B}$, and let $\eta \geqslant \mathrm{dct}\, \xi_{\tilde{t}}$. Then the product AB at relative precision ρ can be computed using*

$$\begin{aligned}
&[AB; \mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho} \\
&= [\xi_{\tilde{t}}^{-1}([\mathrm{red}_{\tilde{t}} \tilde{P}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)-\eta;\rho+\eta})]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho}.
\end{aligned}$$

Proof. By (6.6) we have $\mathrm{val}_{\tilde{t}}\,\tilde{A} \geqslant v(A;\mathbb{P}_t) - \eta$ and $\mathrm{val}_{\tilde{t}}\,\tilde{B} \geqslant v(B;\mathbb{P}_t) - \eta$. By Lemma 6.3, the terms of $\mathrm{val}_{\tilde{t}}\,\tilde{A}$ (resp. of $\mathrm{val}_{\tilde{t}}\,\tilde{B}$) have valuation $< v(A;\mathbb{P}_t) + \rho$ (resp. $< v(B;\mathbb{P}_t) + \rho$). In other words, we have

$$\begin{aligned}\tilde{A} &= [\tilde{A}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{v(A;\mathbb{P}_t)-\eta;\rho+\eta}\\ \tilde{B} &= [\tilde{B}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{v(B;\mathbb{P}_t)-\eta;\rho+\eta},\end{aligned}$$

hence

$$\tilde{P} = [\tilde{P}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)-2\eta;2\rho+2\eta}.$$

Since $\tilde{P}$ equals $\xi_{\tilde{t}}(A\,B)$ in $\tilde{\mathbb{P}}_{\tilde{t}}$, we have

$$\mathrm{val}_{\tilde{t}}(\mathrm{red}_{\tilde{t}}\,\tilde{P}) \geqslant v(A\,B;\mathbb{P}_t) - \eta \geqslant v(A;\mathbb{P}_t) + v(B;\mathbb{P}_t) - \eta.$$

On the other hand, from Lemma 6.3, we know that if $\tilde{C}$ is the canonical representative of an element of $\tilde{\mathbb{P}}_{\tilde{t}}$ of valuation $\mathrm{val}_{\tilde{t}}\,\tilde{C} \geqslant v(A;\mathbb{P}_t) + v(B;\mathbb{P}_t) + \rho$ then

$$v(\xi_t^{-1}(\tilde{C});\mathbb{P}_t) \geqslant v(A;\mathbb{P}_t) + v(B;\mathbb{P}_t) + \rho.$$

Consequently, we may recover

$$[A\,B;\mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho},$$

from $\mathrm{red}_t\,\tilde{P}$ at precision $\rho+\eta$. □

The rest of this section is dedicated to speed up multiplication and Euclidean division using flattenings.

6.2. Reduction in the flattened representation

Given $\tilde{P} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]$, we define its **nested valuation** $\mathrm{nval}_{\tilde{t}}\,P$ by

$$\mathrm{nval}_{\tilde{t}}\,P \;:=\; \min_{1 \leqslant j \leqslant \tilde{t}, k_{j+1}, \ldots, k_{\tilde{t}}} (v(\xi_j^{-1}(\tilde{P}_{k_{j+1}, \ldots, k_{\tilde{t}}});\mathbb{P}_{i_j}) + k_{j+1}\,\mathrm{val}_{\tilde{t}}\,\tilde{\varphi}_{j+1} + \cdots + k_{\tilde{t}}\,\mathrm{val}_{\tilde{t}}\,\tilde{\varphi}_{\tilde{t}}),$$

where for every $j = 1, \ldots, \tilde{t}$, the $\tilde{P}_{k_{j+1}, \ldots, k_{\tilde{t}}}$ are the coefficients of the canonical expansion

$$\tilde{P} = \sum_{k_{j+1}, \ldots, k_{\tilde{t}}} \tilde{P}_{k_{j+1}, \ldots, k_{\tilde{t}}}\, \tilde{\varphi}_{j+1}^{k_{j+1}} \cdots \tilde{\varphi}_{\tilde{t}}^{k_{\tilde{t}}}.$$

If $\tilde{P} \in (\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$ is reduced, then we have

$$\mathrm{nval}_{\tilde{t}}\,\tilde{P} = v(\xi_{\tilde{t}}^{-1}(\tilde{P});\mathbb{P}_t).$$

Using (6.2) we also note that

$$\mathrm{nval}_{\tilde{t}}\,\tilde{P}_{k_{j+1}, \ldots, k_{\tilde{t}}} \geqslant \mathrm{nval}_{\tilde{t}}\,P - k_{j+1}\,\mathrm{val}_{\tilde{t}}\,\tilde{\varphi}_{j+1} - \cdots - k_{\tilde{t}}\,\mathrm{val}_{\tilde{t}}\,\tilde{\varphi}_{\tilde{t}},$$

for all $j, k_{j+1}, \ldots, k_{\tilde{t}}$.

LEMMA 6.5. *Let $\tilde{A}$ and $\tilde{B}$ be the canonical representatives of two elements of $(\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$. Then*

$$\tilde{P} := \tilde{A}\,\tilde{B} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]_{<(2\tilde{d}_1-1, \ldots, 2\tilde{d}_{\tilde{t}}-1)}$$

has nested valuation

$$\mathrm{nval}_{\tilde{t}}\,\tilde{P} \geqslant \mathrm{nval}_{\tilde{t}}\,\tilde{A} + \mathrm{nval}_{\tilde{t}}\,\tilde{B}.$$

Proof. Consider the canonical representations

$$\begin{aligned}\tilde{A} &= \sum_{k_{j+1}<\tilde{d}_{j+1},\ldots,k_{\tilde{t}}<\tilde{d}_{\tilde{t}}} \tilde{A}_{k_{j+1},\ldots,k_{\tilde{t}}} \tilde{\varphi}_{j+1}^{k_{j+1}} \cdots \tilde{\varphi}_{\tilde{t}}^{k_{\tilde{t}}} \\ \tilde{B} &= \sum_{k_{j+1}<\tilde{d}_{j+1},\ldots,k_{\tilde{t}}<\tilde{d}_{\tilde{t}}} \tilde{B}_{k_{j+1},\ldots,k_{\tilde{t}}} \tilde{\varphi}_{j+1}^{k_{j+1}} \cdots \tilde{\varphi}_{\tilde{t}}^{k_{\tilde{t}}}.\end{aligned}$$

Given in $j, k_{j+1}, \ldots, k_{\tilde{t}}$, we have

$$v(\xi_{\tilde{t}}^{-1}(\tilde{A}_{k_{j+1},\ldots,k_{\tilde{t}}}); \mathbb{P}_t) \geqslant v(\xi_{\tilde{t}}^{-1}(\tilde{A}); \mathbb{P}_t) - k_{j+1}\operatorname{val}_{\tilde{t}} \tilde{\varphi}_{j+1} - \cdots - k_{\tilde{t}}\operatorname{val}_{\tilde{t}} \tilde{\varphi}_{\tilde{t}}.$$

Since $\tilde{A}_{k_{j+1},\ldots,k_{\tilde{t}}} \in \mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_j]_{<(\tilde{d}_1,\ldots,\tilde{d}_j)}$ the pre-image $\xi_{\tilde{t}}^{-1}(\tilde{A}_{k_{j+1},\ldots,k_{\tilde{t}}})$ belongs to $(\mathbb{P}_{i_j})_{<1}$, so

$$v(\xi_{\tilde{t}}^{-1}(\tilde{A}_{k_{j+1},\ldots,k_{\tilde{t}}}); \mathbb{P}_t) = v(\xi_j^{-1}(\tilde{A}_{k_{j+1},\ldots,k_{\tilde{t}}}); \mathbb{P}_{i_j}).$$

Similar properties hold for $\tilde{B}$. From

$$\tilde{P}_{k_{j+1},\ldots,k_{\tilde{t}}} = \sum_{e_{j+1}+f_{j+1}=k_{j+1},\ldots,e_{\tilde{t}}+f_{\tilde{t}}=k_{\tilde{t}}} \tilde{A}_{e_{j+1},\ldots,e_{\tilde{t}}} \tilde{B}_{f_{j+1},\ldots,f_{\tilde{t}}},$$

we deduce that

$$\begin{aligned}& v(\xi_j^{-1}(\tilde{P}_{k_{j+1},\ldots,k_{\tilde{t}}}); \mathbb{P}_{i_j}) \\ \geqslant\ & \min_{e_{j+1}+f_{j+1}=k_{j+1},\ldots,e_{\tilde{t}}+f_{\tilde{t}}=k_{\tilde{t}}} v(\xi_j^{-1}(\tilde{A}_{e_{j+1},\ldots,e_{\tilde{t}}}); \mathbb{P}_{i_j}) + v(\xi_j^{-1}(\tilde{B}_{f_{j+1},\ldots,j_{\tilde{t}}}); \mathbb{P}_{i_j}) \\ \geqslant\ & v(\xi_{\tilde{t}}^{-1}(\tilde{A}); \mathbb{P}_t) + v(\xi_{\tilde{t}}^{-1}(\tilde{B}); \mathbb{P}_t) - k_{j+1}\operatorname{val}_{\tilde{t}} \tilde{\varphi}_{j+1} - \cdots - k_{\tilde{t}}\operatorname{val}_{\tilde{t}} \tilde{\varphi}_{\tilde{t}},\end{aligned}$$

which concludes the proof. □

The goal of this subsection is an algorithm to compute $\operatorname{red}_{\tilde{t}} \tilde{P}$ efficiently. It is adapted from Lebreton's method for algebraic towers [13]. We say that a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ for $(\mathbb{P}_i)_{i\leqslant t}$ is given at relative precision $\rho \in R_t^{-1}\,\mathbb{N}^{>0}$ and defect bound $\eta \geqslant \operatorname{dct} \tilde{\xi}_{\tilde{t}}$ when the following data are known:

- $[\tilde{\Phi}_1; \mathbb{K}((z))[\tilde{\varphi}_1, \tilde{\varphi}_2]]_{\tilde{d}_1\tilde{\gamma}_1-\eta;\rho+\eta'}, \ldots, [\tilde{\Phi}_{\tilde{t}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{\tilde{d}_{\tilde{t}}\tilde{\gamma}_{\tilde{t}}-\eta;\rho+\eta'}$
- $[\tilde{\Omega}_1; \mathbb{K}((z))[\tilde{\varphi}_1, \tilde{\varphi}_2]]_{\tilde{d}_1\tilde{\gamma}_1-\eta;\rho+\eta'}, \ldots, [\tilde{\Omega}_{\tilde{t}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{\tilde{d}_{\tilde{t}}\tilde{\gamma}_{\tilde{t}}-\eta;\rho+\eta}$.

Since $\operatorname{val}_{j+1} \tilde{\Phi}_j \geqslant \tilde{d}_j\tilde{\gamma}_j - \eta$ we have

$$[\tilde{\Phi}_j; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{j+1}]]_{0;\tilde{d}_j\tilde{\gamma}_j+\rho} = [\tilde{\Phi}_j; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{j+1}]]_{\tilde{d}_j\tilde{\gamma}_j-\eta;\rho+\eta'}$$

for $j = 1, \ldots, \tilde{t}$. The same property holds for the truncations of the $\tilde{\Omega}_j$.

Algorithm 6.1

Input. An almost reduced generalized contact tower $(\mathbb{P}_i)_{i\leqslant t}$ at relative precision $\rho \in R_t^{-1}\,\mathbb{N}^{>0}$, a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ for $(\mathbb{P}_i)_{i\leqslant t}$ at relative precision ρ and defect bound $\eta \geqslant \operatorname{dct} \tilde{\xi}_{\tilde{t}}$, $\tilde{P} \in [\mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]_{<(2\tilde{d}_1-1,\ldots,2\tilde{d}_{\tilde{t}}-1,1)}]_{\sigma-2\eta;\rho+2\eta}$ with $\operatorname{nval}_{\tilde{t}} \tilde{P} \geqslant \sigma$.

Output. $[\operatorname{red}_{\tilde{t}} \tilde{P}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{\sigma-\eta;\rho+\eta} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]_{<(\tilde{d}_1,\ldots,\tilde{d}_{\tilde{t}},2)}$.

1. If $\tilde{t} = 0$ then return $[\tilde{P}; \mathbb{K}((z))]_{\sigma-\eta;\rho+\eta}$.
2. Write $\tilde{P} = \tilde{P}_0 + \tilde{P}_1\,\tilde{\varphi}_{\tilde{t}} + \cdots + \tilde{P}_{2\tilde{d}_{\tilde{t}}-2}\,\tilde{\varphi}_{\tilde{t}}^{2\tilde{d}_{\tilde{t}}-2}$ with

$$\tilde{P}_0, \ldots, \tilde{P}_{2\tilde{d}_{\tilde{t}}-2} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}-1}]_{<(2\tilde{d}_1-1,\ldots,2\tilde{d}_{\tilde{t}-1}-1)}.$$

For $i = -1, \ldots, \tilde{d}_{\tilde{t}} - 2$, recursively compute

$$\tilde{L}_i + \tilde{\epsilon}_{\tilde{t}-1}\tilde{H}_i\,\tilde{\varphi}_{\tilde{t}} := [\mathrm{red}_{\tilde{t}-1}\,\tilde{P}_{\tilde{d}_{\tilde{t}}+i}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]]_{\sigma-(\tilde{d}_{\tilde{t}}+i)\tilde{\gamma}_{\tilde{t}}-\eta;\rho+\eta}$$

and then $\tilde{P}^{\mathrm{hi}}$ as

$$(\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}_{-1} + \tilde{L}_0) + (\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}_0 + \tilde{L}_1)\,\tilde{\varphi}_{\tilde{t}} + \cdots + (\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}_{\tilde{d}_{\tilde{t}}-3} + \tilde{L}_{\tilde{d}_{\tilde{t}}-2})\,\tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}-2} + \tilde{\epsilon}_{\tilde{t}-1}\tilde{H}_{\tilde{d}_{\tilde{t}}-2}\tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}-1}.$$

3. Compute $\tilde{A} := \tilde{P}^{\mathrm{hi}}[\tilde{\Omega}_{\tilde{t}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{\tilde{d}_{\tilde{t}}\tilde{\gamma}_{\tilde{t}}-\eta;\rho+\eta}$ as

$$\tilde{P}^{\mathrm{hi}}\,\tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}} + \tilde{P}^{\mathrm{hi}}\Big([\tilde{\Omega}_{\tilde{t}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{\tilde{d}_{\tilde{t}}\tilde{\gamma}_{\tilde{t}}-\eta;\rho+\eta} - \tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}}\Big).$$

4. Write $\tilde{A} = \tilde{A}_0 + \tilde{A}_1\,\tilde{\varphi}_{\tilde{t}} + \cdots + \tilde{A}_{2\tilde{d}_{\tilde{t}}-1}\tilde{\varphi}_{\tilde{t}}^{2\tilde{d}_{\tilde{t}}-1}$ with

$$\tilde{A}_0, \ldots, \tilde{A}_{2\tilde{d}_{\tilde{t}}-1} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}-1}]_{<(2\tilde{d}_1-1, \ldots, 2\tilde{d}_{\tilde{t}-1}-1)}.$$

For $i = 0, \ldots, \tilde{d}_{\tilde{t}} - 1$, recursively compute

$$\tilde{L}'_i + \tilde{\epsilon}_{\tilde{t}-1}\tilde{H}'_i\,\tilde{\varphi}_t := [\mathrm{red}_{\tilde{t}-1}(\tilde{A}_{\tilde{d}_{\tilde{t}}+i}); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]]_{\sigma-(\tilde{d}_{\tilde{t}}+i)\gamma_{\tilde{t}}-\eta;\rho+\eta},$$

and $\tilde{A}^{\mathrm{hi}} \in [\mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]_{<(\tilde{d}_1, \ldots, \tilde{d}_{\tilde{t}})}]_{\sigma-\tilde{d}_{\tilde{t}}\tilde{\gamma}_t-\eta;\rho+\eta}$ as

$$(\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}'_0 + \tilde{L}'_1) + (\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}'_1 + \tilde{L}'_2)\,\tilde{\varphi}_{\tilde{t}} + \cdots + (\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}'_{\tilde{d}_{\tilde{t}}-2} + \tilde{L}'_{\tilde{d}_{\tilde{t}}-1})\,\tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}-2} + \tilde{\epsilon}_{\tilde{t}-1}\tilde{H}'_{\tilde{d}_{\tilde{t}}-1}\tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}-1}.$$

5. Compute $\tilde{B} := \tilde{P} - \tilde{A}^{\mathrm{hi}}[\tilde{\Phi}_{\tilde{t}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{\tilde{d}_{\tilde{t}}\tilde{\gamma}_{\tilde{t}}-\eta;\rho+\eta}$ as

$$\tilde{P} - \tilde{A}^{\mathrm{hi}}\,\tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}} - \tilde{A}^{\mathrm{hi}}\Big([\tilde{\Phi}_{\tilde{t}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}+1}]]_{\tilde{d}_{\tilde{t}}\tilde{\gamma}_{\tilde{t}}-\eta;\rho+\eta} - \tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}}\Big).$$

6. Write $\tilde{B} = \tilde{B}_0 + \tilde{B}_1\,\tilde{\varphi}_{\tilde{t}} + \cdots + \tilde{B}_{2\tilde{d}_{\tilde{t}}-1}\tilde{\varphi}_{\tilde{t}}^{2\tilde{d}_{\tilde{t}}-1}$ with

$$\tilde{B}_0, \ldots, \tilde{B}_{2\tilde{d}_{\tilde{t}}-1} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}-1}]_{<(2\tilde{d}_1-1, \ldots, 2\tilde{d}_{\tilde{t}-1}-1)}.$$

For $i = 0, \ldots, \tilde{d}_{\tilde{t}} - 1$, recursively compute

$$\tilde{L}''_i + \tilde{\epsilon}_{\tilde{t}-1}\tilde{H}''_i\,\tilde{\varphi}_t := [\mathrm{red}_{\tilde{t}-1}\,\tilde{B}_i; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]]_{\sigma-i\tilde{\gamma}_t-\eta;\rho+\eta},$$

and $\tilde{B}^{\mathrm{lo}} \in [\mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]_{<(\tilde{d}_1, \ldots, \tilde{d}_{\tilde{t}})}]_{\sigma-\eta;\rho+\eta}$ as

$$\tilde{L}''_0 + (\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}''_0 + \tilde{L}''_1)\,\tilde{\varphi}_{\tilde{t}} + \cdots + (\tilde{\epsilon}_{\tilde{t}-1}\tilde{H}''_{\tilde{d}_{\tilde{t}}-2} + \tilde{L}''_{\tilde{d}_{\tilde{t}}-1})\,\tilde{\varphi}_{\tilde{t}}^{\tilde{d}_{\tilde{t}}-1}.$$

7. Return $\tilde{\epsilon}_{\tilde{t}}\tilde{A}^{\mathrm{hi}}\,\tilde{\varphi}_{\tilde{t}+1} + \tilde{B}^{\mathrm{lo}}$.

PROPOSITION 6.6. *Algorithm 6.1 is correct and performs*

$$R_t^{-1}\,\tilde{O}\big(3^{\tilde{t}} D_t R_t\,(\rho+\eta)\big)$$

operations in $\mathbb{K}$.

Proof. If $\tilde{t} = 0$ then $\tilde{P} \in \mathbb{K}((z))$, so step 1 returns the correct value. Otherwise the nested valuation property ensures that $v(\xi_{\tilde{t}}^{-1}(\tilde{P}); \mathbb{P}_t) \geqslant \sigma$, so (6.6) yields

$$\mathrm{val}_{\tilde{t}}(\mathrm{red}_{\tilde{t}}\,\tilde{P})) \geqslant \sigma - \eta.$$

On the other hand,

$$\tilde{P}_i \in [\mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}]_{<(2\tilde{d}_1-1, \ldots, 2\tilde{d}_{\tilde{t}-1}-1, 1)}]_{\sigma-i\tilde{\gamma}_{\tilde{t}}-2\eta;\rho+2\eta}$$

has nested valuation $\geqslant \sigma - i\,\tilde{\gamma}_{\tilde{\imath}}$, for $i = 0, \ldots, 2\,\tilde{d}_{\tilde{\imath}} - 2$, so the recursive calls in step 2 are valid. It follows that $\mathrm{val}_{\tilde{\imath}-1}(\mathrm{red}_{\tilde{\imath}-1}\,\tilde{P}_i) \geqslant \sigma - i\,\tilde{\gamma}_{\tilde{\imath}} - \eta$, and that $\tilde{L}'_i + \tilde{\epsilon}_{\tilde{\imath}-1}\tilde{H}'_i\,\tilde{\varphi}_{\tilde{\imath}}$ approximates $\mathrm{red}_{\tilde{\imath}-1}\,\tilde{P}_i$ at precision $\geqslant \rho + \eta$.

If $\epsilon_{\tilde{\imath}-1} = 1$ then $\tilde{\gamma}_{\tilde{\imath}} = \mathrm{val}_{\tilde{\imath}}\,\tilde{\varphi}_{\tilde{\imath}} = \gamma_{i_{\tilde{\imath}-1}+1} = \mathrm{val}_{\tilde{\imath}-1}\,\tilde{\varphi}_{\tilde{\imath}}$ by (6.3), whence

$$\tilde{P}^{\mathrm{hi}} = \Big[\mathrm{red}_{\tilde{\imath}-1}\,\tilde{P}\,\mathrm{quo}_{\tilde{\varphi}_{\tilde{\imath}}}\,\tilde{\varphi}_{\tilde{\imath}}^{\tilde{d}_{\tilde{\imath}}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]\Big]_{\sigma-\eta;\rho+\eta}.$$

If $\epsilon_{\tilde{\imath}-1} = 0$, then the latter equality trivially holds. By construction of $\tilde{P}^{\mathrm{hi}}$ there exists

$$\tilde{P}^{\mathrm{lo}} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}}]_{<(\tilde{d}_1, \ldots, \tilde{d}_{\tilde{\imath}})}$$

such that

$$[\mathrm{red}_{\tilde{\imath}-1}\,\tilde{P}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{\sigma-\eta;\rho+\eta} = \tilde{P}^{\mathrm{lo}} + \tilde{P}^{\mathrm{hi}}\,\tilde{\varphi}_{\tilde{\imath}}^{\tilde{d}_{\tilde{\imath}}}.$$

In step 3, the polynomial $\tilde{A}$ belongs to $[\mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]_{<(2\tilde{d}_1-1, \ldots, 2\tilde{d}_{\tilde{\imath}}-1, 1)}]_{\sigma-2\eta;\rho+2\eta}$ and $\mathrm{nval}_{\tilde{\imath}}\,\tilde{A} \geqslant \sigma + \tilde{d}_{\tilde{\imath}}\,\tilde{\gamma}_{\tilde{\imath}}$ by Lemma 6.5 and Property $\mathbf{F_6}$ of Definition 6.1. The correctness of step 4 is thus similar to step 2. There exists $\tilde{A}^{\mathrm{lo}} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}}]_{<(\tilde{d}_1, \ldots, \tilde{d}_{\tilde{\imath}})}$ such that

$$[\mathrm{red}_{\tilde{\imath}-1}\,\tilde{A}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{\sigma+\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-\eta;\rho+\eta} = \tilde{A}^{\mathrm{lo}} + \tilde{A}^{\mathrm{hi}}\,\tilde{\varphi}_{\tilde{\imath}}^{\tilde{d}_{\tilde{\imath}}}.$$

Using Property 3 of Definition 6.1, let $\tilde{W} \in \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}}]_{<(\tilde{d}_1, \ldots, \tilde{d}_{\tilde{\imath}})}$ be such that

$$\begin{aligned}
&\tilde{\varphi}_{\tilde{\imath}}^{2\tilde{d}_{\tilde{\imath}}} + \tilde{W} \\
&= [\mathrm{red}_{\tilde{\imath}-1}([\tilde{\Omega}_{\tilde{\imath}}\,\tilde{\Phi}_{\tilde{\imath}}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{2\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-2\eta;2\rho+2\eta}); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{2\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-\eta;\rho+\eta}.
\end{aligned}$$

By Lemma 6.5 we have $\mathrm{val}_{\tilde{\imath}}(\mathrm{red}_{\tilde{\imath}-1}(\tilde{P}\,\tilde{\Omega}_{\tilde{\imath}}\,\tilde{\Phi}_{\tilde{\imath}})) \geqslant \sigma + 2\,\tilde{d}_{\tilde{\imath}}\,\tilde{\gamma}_{\tilde{\imath}}$. Then we verify that

$$\begin{aligned}
&[\mathrm{red}_{\tilde{\imath}-1}((\tilde{P}\,\tilde{\Omega}_{\tilde{\imath}})\,\tilde{\Phi}_{\tilde{\imath}}); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{\sigma+2\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-\eta;\rho+\eta} \\
&= \Big[\mathrm{red}_{\tilde{\imath}-1}\Big(\Big(\tilde{A}^{\mathrm{hi}}\,\tilde{\varphi}_{\tilde{\imath}}^{\tilde{d}_{\tilde{\imath}}} + \tilde{A}^{\mathrm{lo}}\Big)\,\tilde{\Phi}_{\tilde{\imath}}\,\tilde{\varphi}_{\tilde{\imath}}^{\tilde{d}_{\tilde{\imath}}} + \tilde{P}^{\mathrm{lo}}\,\tilde{\Omega}_{\tilde{\imath}}\,\tilde{\Phi}_{\tilde{\imath}}\Big); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]\Big]_{\sigma+2\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-\eta;\rho+\eta} \\
&= \Big[\mathrm{red}_{\tilde{\imath}-1}\Big(\tilde{A}^{\mathrm{hi}}\,\tilde{\Phi}_{\tilde{\imath}}\,\tilde{\varphi}_{\tilde{\imath}}^{2\tilde{d}_{\tilde{\imath}}} + \Big(\tilde{A}^{\mathrm{lo}}\,\tilde{\varphi}_{\tilde{\imath}}^{\tilde{d}_{\tilde{\imath}}} + \tilde{P}^{\mathrm{lo}}\,\tilde{\Omega}_{\tilde{\imath}}\Big)\,\tilde{\Phi}_{\tilde{\imath}}\Big); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]\Big]_{\sigma+2\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-\eta;\rho+\eta} \qquad (6.7)
\end{aligned}$$

and also that

$$\begin{aligned}
&[\mathrm{red}_{\tilde{\imath}-1}(\tilde{P}\,(\tilde{\Omega}_{\tilde{\imath}}\,\tilde{\Phi}_{\tilde{\imath}})); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{\sigma+2\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-\eta;\rho+\eta} \\
&= \Big[\mathrm{red}_{\tilde{\imath}-1}\Big(\tilde{P}\,\tilde{\varphi}_{\tilde{\imath}}^{2\tilde{d}_{\tilde{\imath}}} + \tilde{P}\,\tilde{W}\Big); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]\Big]_{\sigma+2\tilde{d}_{\tilde{\imath}}\tilde{\gamma}_{\tilde{\imath}}-\eta;\rho+\eta}. \qquad (6.8)
\end{aligned}$$

Since $\deg_{\tilde{\varphi}_{\tilde{\imath}}}\Big(\mathrm{red}_{\tilde{\imath}-1}\Big(\Big(\tilde{A}^{\mathrm{lo}}\,\tilde{\varphi}_{\tilde{\imath}}^{\tilde{d}_{\tilde{\imath}}} + \tilde{P}^{\mathrm{lo}}\,\tilde{\Omega}_{\tilde{\imath}}\Big)\,\tilde{\Phi}_{\tilde{\imath}}\Big)\Big) < 3\,\tilde{d}_{\tilde{\imath}}$, equating (6.7) with (6.8) leads to

$$\begin{aligned}
&[\mathrm{red}_{\tilde{\imath}}\,\tilde{P}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{\sigma-\eta;\rho+\eta} \\
&= [\mathrm{red}_{\tilde{\imath}}(\tilde{A}^{\mathrm{hi}}\,\tilde{\Phi}_{\tilde{\imath}} + \tilde{R}); \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{\sigma-\eta;\rho+\eta} \\
&= \tilde{\epsilon}_{\tilde{\imath}}\tilde{A}^{\mathrm{hi}}\,\tilde{\varphi}_{\tilde{\imath}+1} + \tilde{R},
\end{aligned}$$

for some $\tilde{R} \in (\tilde{\mathbb{P}}_{\tilde{\imath}})_{<1}$. From $\mathrm{val}_{\tilde{\imath}}(\tilde{\epsilon}_{\tilde{\imath}}\,\tilde{\varphi}_{\tilde{\imath}+1}) \geqslant \mathrm{val}_{\tilde{\imath}}(\tilde{\epsilon}_{\tilde{\imath}}\,\tilde{\Phi}_{\tilde{\imath}})$ and $\mathrm{val}_{\tilde{\imath}}(\mathrm{red}_{\tilde{\imath}}\,\tilde{P}) \geqslant \sigma - \eta$, it follows that the algorithm actually returns $[\mathrm{red}_{\tilde{\imath}}\,\tilde{P}; \mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}+1}]]_{\sigma-\eta;\rho+\eta}$.

As for the complexity analysis, note that $\tilde{A}$ and $\tilde{A}^{\mathrm{hi}}\,\tilde{\Phi}_{\tilde{\imath}}$ belong to

$$\mathbb{K}((z))[\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{\imath}}]_{<(2\tilde{d}_1-1, \ldots, 2\tilde{d}_{\tilde{\imath}-1}-1, 2\tilde{d}_{\tilde{\imath}})}.$$

By Proposition 2.5, the products in steps 3 and 5 take

$$R_{i_{\tilde{\imath}}}^{-1}\,\tilde{O}\big(2^{\tilde{\imath}}\,\tilde{D}_{\tilde{\imath}}\,R_{i_{\tilde{\imath}}}(\rho+\eta)\big)$$

operations in $\mathbb{K}$. Let $\mathsf{R}(\tilde{d}_1,\ldots,\tilde{d}_{\tilde{t}};\rho)$ denote the cost function of Algorithm 6.1. By Lemma 2.3, the recursive calls to Algorithm 6.1 take

$$3\min\left(R_{i_{\tilde{t}-1}}(2\rho+2\eta),1\right)\tilde{d}_{\tilde{t}}\,\mathsf{R}(\tilde{d}_1,\ldots,\tilde{d}_{\tilde{t}-1};\max\left(R^{-1}_{i_{\tilde{t}-1}},\rho\right))$$

operations in $\mathbb{K}$. It follows that

$$\begin{aligned}
&\mathsf{R}(\tilde{d}_1,\ldots,\tilde{d}_{\tilde{t}};\rho)\\
\leqslant\ & 3\,\mathsf{R}(\tilde{d}_1,\ldots,\tilde{d}_{\tilde{t}-1};\max\left(R^{-1}_{i_{\tilde{t}-1}},\rho\right))\min\left(R_{i_{\tilde{t}-1}}(2\rho+2\eta),1\right)\tilde{d}_{\tilde{t}}\\
&\quad+R^{-1}_{i_{\tilde{t}}}\tilde{O}\big(2^{\tilde{t}}\tilde{D}_{\tilde{t}}R_{i_{\tilde{t}}}\max\left(R^{-1}_{i_{\tilde{t}}},\rho+\eta\right)\big)\\
\leqslant\ & 3^2\mathsf{R}(\tilde{d}_1,\ldots,\tilde{d}_{\tilde{t}-2};\max\left(R^{-1}_{i_{\tilde{t}-2}},\rho\right))\\
&\quad\times\min\left(R_{i_{\tilde{t}-1}}(2\rho+2\eta),1\right)\min\left(R_{i_{\tilde{t}-2}}\max\left(R^{-1}_{i_{\tilde{t}-1}},2\rho+2\eta\right),1\right)\tilde{d}_{\tilde{t}-1}\tilde{d}_{\tilde{t}}\\
&\quad+3\min\left(R_{i_{\tilde{t}-1}}(2\rho+2\eta),1\right)\tilde{d}_{\tilde{t}}R^{-1}_{i_{\tilde{t}-1}}\tilde{O}\big(2^{\tilde{t}-1}\tilde{D}_{\tilde{t}-1}R_{i_{\tilde{t}-1}}\max\left(R^{-1}_{i_{\tilde{t}-1}},\rho+\eta\right)\big)\\
&\quad+R^{-1}_{i_{\tilde{t}}}\tilde{O}\big(2^{\tilde{t}}\tilde{D}_{\tilde{t}}R_{i_{\tilde{t}}}(\rho+\eta)\big)\\
\leqslant\ & 3^2\mathsf{R}(\tilde{d}_1,\ldots,\tilde{d}_{\tilde{t}-2};\max\left(R^{-1}_{i_{\tilde{t}-2}},\rho\right))\min\left(R_{i_{\tilde{t}-2}}(2\rho+2\eta),1\right)\tilde{d}_{\tilde{t}-1}\tilde{d}_{\tilde{t}}\qquad\text{(by Lemma 3.10)}\\
&\quad+\frac{3}{2}R^{-1}_{i_{\tilde{t}}}\tilde{O}\big(2^{\tilde{t}}\tilde{D}_{\tilde{t}}R_{i_{\tilde{t}}}(\rho+\eta)\big)+R^{-1}_{i_{\tilde{t}}}\tilde{O}\big(2^{\tilde{t}}\tilde{D}_{\tilde{t}}R_{i_{\tilde{t}}}(\rho+\eta)\big)\\
&\ \vdots\\
=\ & R^{-1}_{i_{\tilde{t}}}\tilde{O}\big(3^{\tilde{t}}\tilde{D}_{\tilde{t}}R_{i_{\tilde{t}}}(\rho+\eta)\big).
\end{aligned}$$

□

6.3. Flattened multiplication and division

As a direct application of Algorithm 6.1, we obtain the following multiplication method, which benefits from flattenings.

Algorithm 6.2

Input. An almost reduced generalized contact tower $(\mathbb{P}_i)_{i\leqslant t}$ at relative precision $\rho\in R^{-1}_{t+1}\,\mathbb{N}^{>0}$, a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ for $(\mathbb{P}_i)_{i\leqslant t}$ at relative precision ρ and defect bound $\eta\geqslant\operatorname{dct}\tilde{\xi}_{\tilde{t}}$, $\tilde{A}=[\operatorname{red}_{\tilde{t}}(\xi_{\tilde{t}}(A));\mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]]_{v(A;\mathbb{P}_t)-\eta;\rho+\eta}$, and $\tilde{B}=[\operatorname{red}_{\tilde{t}}(\xi_{\tilde{t}}(B);\mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}])]_{v(B;\mathbb{P}_t)-\eta;\rho+\eta}$, where A and B are in $(\mathbb{P}_t)_{<l}$.

Output. $[\operatorname{red}_{\tilde{t}}(\tilde{A}\,\tilde{B});\mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)-\eta;\rho+\eta}$.

1. Compute $\tilde{C}:=\tilde{A}\,\tilde{B}$ in $\mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]$.
2. Write $\tilde{C}=\tilde{C}_0+\tilde{C}_1\tilde{\varphi}_{\tilde{t}+1}+\cdots+\tilde{C}_{2l-2}\tilde{\varphi}^{2l-2}_{\tilde{t}+1}$
   with $\tilde{C}_0,\ldots,\tilde{C}_{2l-2}\in\mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}}]_{<(2\tilde{d}_1-1,\ldots,2\tilde{d}_{\tilde{t}}-1)}$.
   For $i=0,\ldots,2l-2$, compute $\tilde{L}_i+\epsilon_t\tilde{H}_i\,\tilde{\varphi}_{\tilde{t}+1}:=[\operatorname{red}_{\tilde{t}}(\tilde{C}_i)]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)-i\tilde{\gamma}_{\tilde{t}+1}-\eta;\rho+\eta}$ by using Algorithm 6.1.
3. Return $\tilde{L}_0+(\epsilon_t\tilde{H}_0+\tilde{L}_1)\,\tilde{\varphi}_{\tilde{t}+1}+\cdots+(\epsilon_t\tilde{H}_{2l-3}+\tilde{L}_{2l-2})\,\tilde{\varphi}^{2l-2}_{\tilde{t}+1}+\epsilon_t\tilde{H}_{2l-2}\,\tilde{\varphi}^{2l-1}_{\tilde{t}+1}$.

PROPOSITION 6.7. *Algorithm 6.2 is correct and performs*

$$R^{-1}_{t+1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}(\rho+\eta)\big)$$

operations in $\mathbb{K}$, *whenever* $l\in r_{t+1}\,\mathbb{N}^{>0}$.

Proof. By Lemma 6.5, we have $\operatorname{nval}_{\tilde{t}}\tilde{C}\geqslant v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t)$. So the correctness follows as in the proof of Proposition 6.6. The cost of step 1 is given in Proposition 2.5, that is

$$R^{-1}_{t+1}\tilde{O}\big(2^{\tilde{t}+1}D_t\,l\,R_{t+1}(\rho+\eta)\big)$$

The cost of step 2 follows from Proposition 6.6 and Lemma 2.2:

$$\begin{aligned} & R_t^{-1}\tilde{O}\big(3^{\tilde{t}} D_t l \min(R_t\rho, 1)\, R_t \max(R_t^{-1}, \rho+\eta)\big) \\ = \;& R_t^{-1}\tilde{O}\big(3^{\tilde{t}} D_t l \min(R_t(\rho+\eta), 1) \max(R_t(\rho+\eta), 1)\big) \\ = \;& R_t^{-1}\tilde{O}\big(3^{\tilde{t}} D_t l R_t(\rho+\eta)\big) \\ = \;& R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}} D_t l R_{t+1}(\rho+\eta)\big). \end{aligned}$$

The cost of step 3 is negligible. □

In short, $\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(A))$ will be called the **flattened representation** of $A \in \mathbb{P}_t$. Proposition 6.7 shows that fast products can be achieved using flattened representations, in the sense that $\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(AB))$ is obtained from $\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(A))$ and $\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(B))$. This approach extends to divisions as follows.

PROPOSITION 6.8. *Let $F \in \mathbb{P}_t$ be a clustered monic contact polynomial of degree $l \in r_{t+1}\mathbb{N}^{>0}$ in φ_{t+1} and given at precision $\rho \in R_{t+1}^{-1}\mathbb{N}^{>0}$. Let G be the pre-inverse of F at relative precision ρ, and let A be a contact polynomial of $(\mathbb{P}_t)_{<2l}$ of valuation $\geqslant\sigma$ at precision ρ. Given $[\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(F)); \mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]]_{l\gamma_{t+1}-\eta;\rho+\eta}$, $[\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(G)); \mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]]_{l\gamma_{t+1}-\eta;\rho+\eta}$, and $[\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(A)); \mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]]_{\sigma-\eta;\rho+\eta}$, we can compute*

$$\begin{aligned} & [\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(A \operatorname{quo} \varphi_{t+1} F); \mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}])]_{\sigma-l\gamma_{t+1}-\eta;\rho+\eta} \\ \text{and } & [\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(A \operatorname{rem} \varphi_{t+1} F)); \mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]]_{\sigma-\eta;\rho+\eta} \end{aligned}$$

using

$$R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}} D_t l R_{t+1}(\rho+\eta)\big)$$

operations in $\mathbb{K}$.

Proof. This follows from Propositions 3.16 and 6.7. □

7. THREE TYPES OF FLATTENING

In this section, we present three types of flattening along with conversion algorithms. The given generalized contact tower is still written $(\mathbb{P}_i)_{i\leqslant t}$ and is assumed to be almost reduced, effectively separable and regular. The relative precision we want to compute with is $\rho \in R_{t+1}^{-1}\mathbb{N}^{>0}$.

When a flattening for $(\mathbb{P}_i)_{i\leqslant t}$ is given as in Definition 6.1, we know from Lemma 6.3 and Equation (6.5) that an element $A \in \mathbb{P}_t$ can be recovered at precision ρ from

$$[\mathrm{red}_{\tilde{t}}(\xi_{\tilde{t}}(A)); \mathbb{K}((z))[\tilde{\varphi}_1,\ldots,\tilde{\varphi}_{\tilde{t}+1}]]_{v(A;\mathbb{P}_t)-\eta;\rho+\eta}$$

whenever $\eta \geqslant \mathrm{dct}\,\xi_{\tilde{t}}$. In the rest of the paper the notation

$$\mathsf{C}(\mathbb{P}_{i_{\tilde{t}},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t},<1;\rho+\eta})$$

will represent a complexity bound for the following tasks:

- compute $\xi_{\tilde{t}}(A)$ at relative precision $\rho+\eta$, for any $A \in (\mathbb{P}_{i_{\tilde{t}}})_{<1}$ given at relative precision ρ,
- compute $\xi_{\tilde{t}}^{-1}(\tilde{A})$ at relative precision ρ, from the canonical representative $\tilde{A} \in (\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$ at relative precision $\rho+\eta$.

Each type of flattening will involve precomputed **auxiliary data** for the sake of efficiency. In fact, at level j of a flattening, data in $\mathbb{P}_{i_{j-1}}$ at precision ρ shall be converted to $\tilde{\mathbb{P}}_{j-1}$ at relative precision $\geqslant \rho + \operatorname{dct} \xi_j$ in order to benefit from the flattened products and divisions of section 6.3. The pre-inverse of $\varphi_i + \Phi_{i,d_i-1}$ in $\mathbb{P}_i$ will be written Ψ_i.

7.1. Trivial flattening

We say that a flattening is **trivial** at level j when $i_j = i_{j-1} + 1$, $\tilde{\Phi}_j = \xi_{j-1}(\Phi_{i_j})$, and $\xi_j(\varphi_{i_j}) := \tilde{\varphi}_j$. Without loss of generality we may assume that $j = \tilde{t}$ for the sake of the presentation.

LEMMA 7.1. *Assume that $i_{\tilde{t}-1} = t-1$ and that $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}-1}$ is a flattening for $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}-1}}$. Then there exists a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ of $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}}}$, trivial at level $\tilde{t}$, with $i_{\tilde{t}} := i_{\tilde{t}-1} + 1 = t$, $\tilde{\epsilon}_{\tilde{t}} := \epsilon_{i_{\tilde{t}}}$,*

$$\tilde{\Phi}_{\tilde{t}}(\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{\tilde{t}}) := \xi_{\tilde{t}-1}(\Phi_{i_{\tilde{t}}}),$$

$$\begin{aligned} \xi_{\tilde{t}}\colon \quad \mathbb{P}_t &\to \tilde{\mathbb{P}}_{\tilde{t}} \\ \varphi_k &\mapsto \xi_{\tilde{t}-1}(\varphi_k) \text{ for } k = 1, \ldots, i_{\tilde{t}} \\ \varphi_{i_{\tilde{t}}+1} &\mapsto \tilde{\varphi}_{\tilde{t}+1}. \end{aligned}$$

We take $\tilde{\Omega}_{\tilde{t}} := \xi_{\tilde{t}-1}(\Omega_t)$, where Ω_t is the pre-inverse of Φ_t in $\mathbb{P}_{t-1}$. In addition we have $\operatorname{dct} \xi_{\tilde{t}} = \operatorname{dct} \xi_{\tilde{t}-1}$.

Proof. The proof is straightforward from Definition 6.1. □

The next proposition concerns the complexity for building a trivial flattening at level $\tilde{t}$. We recall that a flattening as in Definition 6.1 is said to be given at precision ρ and defect $\eta \geqslant \operatorname{dct} \xi_{\tilde{t}}$ when the $\tilde{\Phi}_j$ and the $\tilde{\Omega}_j$ are known at precision $\rho + \eta$, for $j = 1, \ldots, \tilde{t}$.

PROPOSITION 7.2. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an almost reduced, effectively separable and regular contact tower at precision $\rho \in R_t^{-1}\,\mathbb{N}^{>0}$, and let $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}-1}$ be a flattening for $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}-1}}$ with $i_{\tilde{t}-1} = t-1$ at precision ρ and defect $\eta \geqslant \operatorname{dct} \xi_{\tilde{t}}$. Then we can compute a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ of $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}}}$ trivial at level $\tilde{t}$ at precision ρ and defect η using*

$$\begin{aligned} & O(\mathsf{M}(d_1, \ldots, d_t; \rho) \log d_t) \\ + \ & \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta})\, O(\min(R_{t-1}\rho, 1)\, d_t) \\ + \ & \mathsf{I}(d_1, \ldots, d_{t-1}; \max(R_{t-1}^{-1}, \rho)) \end{aligned}$$

operations in $\mathbb{K}$.

Proof. We compute the pre-inverse Ω_t of Φ_t at precision ρ using

$$O(\mathsf{M}(d_1, \ldots, d_t; \rho) \log d_t) + \mathsf{I}(d_1, \ldots, d_{t-1}; \max(R_{t-1}^{-1}, \rho))$$

operations in $\mathbb{K}$ thanks to Proposition 3.14. By Lemma 2.2 we need $O(\min(R_{t-1}\rho, 1)\, d_t)$ evaluations of $\xi_{\tilde{t}-1}$ at elements of $(\mathbb{P}_{t-1})_{<d_t}$ in order to obtain $\xi_{\tilde{t}-1}(\Phi_t)$ and $\xi_{\tilde{t}-1}(\Omega_t)$ at relative precision $\rho + \eta$. □

PROPOSITION 7.3. *With the notation and assumptions of Proposition 7.2, one conversion between $(\mathbb{P}_t)_{<1}$ at precision $\rho \in R_t^{-1}\,\mathbb{N}^{>0}$ and $(\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$ at precision $\rho + \eta$ costs*

$$\mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta})\, O(\min(R_{t-1}\rho, 1)\, d_t).$$

Proof. For an element A in $(\mathbb{P}_t)_{<1}$, we consider its contact representation $\sum_{i=0}^{d_{t-1}} A_i \varphi_t^i$ and compute $\xi_{t-1}(A_i)$. The number of non-zero A_i is $O(\min(R_{t-1}\rho, 1), d_t)$ by Lemma 2.2. □

7.2. First type of flattening

We say that the level j of a flattening is of **first type** whenever

$$\epsilon_{i_{j-1}} = \epsilon_{i_j} = 0.$$

For the sake of the presentation, as previously we focus on the case where $j = \tilde{t}$, that is $\epsilon_{i_{\tilde{t}-1}} = \epsilon_{i_{\tilde{t}}} = 0$. In other words, $\mathbb{P}_{i_{\tilde{t}-1}}$ (resp. $\mathbb{P}_{i_{\tilde{t}}}$) is of the form $\mathbb{E}_{i_{\tilde{t}-1}}[\varphi_{i_{\tilde{t}-1}+1}]$ (resp. $\mathbb{E}_{i_{\tilde{t}}}[\varphi_{i_{\tilde{t}}+1}]$) where $\mathbb{E}_{i_{\tilde{t}-1}} := \mathbb{P}_{i_{\tilde{t}-1}}/(\varphi_{i_{\tilde{t}-1}+1})$ (resp. $\mathbb{E}_{i_{\tilde{t}}} := \mathbb{P}_{i_{\tilde{t}}}/(\varphi_{i_{\tilde{t}}+1})$) has finite dimension over $\mathbb{K}((z))$.

By Proposition 5.3 (with $h = i_{\tilde{t}-1}$ and $\rho = +\infty$ [we assumed $\rho < \infty$ in our definitions]), if card $\mathbb{K} > (D_h^{-1} D_t)^2$, then there exists a univariate-valued representation

$$\chi, w_{i_{\tilde{t}-1}+1}, \dots, w_{i_{\tilde{t}}}$$

of $\mathbb{E}_{i_{\tilde{t}}}$ over $\mathbb{E}_{i_{\tilde{t}-1}}$ in terms of a primitive-valued ϖ, hence

$$\chi(\varpi) = 0,$$

and $\varphi_k = w_k(\varpi)$ for $k = i_{\tilde{t}-1}+1, \dots, i_{\tilde{t}}$. In the proof of Proposition 7.5 below [not very kind], we shall see that there exists an $\Omega \in \mathbb{E}_{i_{\tilde{t}-1}}[T]$ with

$$\Omega(T)\,\chi(T) \in T^{2\tilde{d}_{\tilde{t}}} + \mathbb{E}_{i_{\tilde{t}-1}}[T]_{<\tilde{d}_{\tilde{t}}}. \tag{7.1}$$

In the following lemma, we extend $\xi_{\tilde{t}-1}$ coefficientwise to $\mathbb{P}_{i_{\tilde{t}-1}}[T]$, and $\xi_{\tilde{t}-1}(\chi)$ stands for the application of this extended map to χ.

LEMMA 7.4. *Assume that $(\tilde{\mathbb{P}}_j)_{j\leqslant \tilde{t}-1}$ is a flattening of $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}-1}}$ and that $\epsilon_{i_{\tilde{t}-1}} = \epsilon_{i_{\tilde{t}}} = 0$. Then there exists a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant \tilde{t}}$ of $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}}}$ of first type at level $\tilde{t}$, with $i_{\tilde{t}} := t$, $\tilde{\epsilon}_{\tilde{t}} := 0$,*

$$\tilde{\Phi}_{\tilde{t}}(\tilde{\varphi}_1, \dots, \tilde{\varphi}_{\tilde{t}}) := \xi_{\tilde{t}-1}(\chi)(\tilde{\varphi}_{\tilde{t}}),$$

$$\begin{aligned} \xi_{\tilde{t}}\colon \quad \mathbb{P}_t &\to \tilde{\mathbb{P}}_{\tilde{t}} \\ \varphi_k &\mapsto \xi_{\tilde{t}-1}(\varphi_k) \text{ for } k = 1, \dots, i_{\tilde{t}-1} \\ \varphi_k &\mapsto \xi_{\tilde{t}-1}(w_k)(\tilde{\varphi}_{\tilde{t}}) \text{ for } k = i_{\tilde{t}-1}+1, \dots, i_{\tilde{t}} \\ \varphi_{i_{\tilde{t}}+1} &\mapsto \tilde{\varphi}_{\tilde{t}+1} \end{aligned}$$

and $\tilde{\Omega}_{\tilde{t}} := \xi_{\tilde{t}-1}(\Omega)(\tilde{\varphi}_{\tilde{t}})$. In addition we have $\operatorname{dct} \xi_{\tilde{t}} = \operatorname{dct} \xi_{\tilde{t}-1}$.

Proof. By construction, Definition 6.1 holds. Only a brief explanation is necessary for **F3**: the $\mathbb{K}((z))$-vector space isomorphism

$$\begin{aligned} \mathbb{K}((z))[\tilde{\varphi}_1, \dots, \tilde{\varphi}_{\tilde{t}}]_{<(\tilde{d}_1, \dots, \tilde{d}_{\tilde{t}})} &\cong \mathbb{E}_{i_{\tilde{t}}} \\ \sum_{0\leqslant k<\tilde{d}_{\tilde{t}}} \tilde{A}_k \tilde{\varphi}_{\tilde{t}}^k &\mapsto \sum_{0\leqslant k<\tilde{d}_{\tilde{t}}} \xi_{\tilde{t}-1}^{-1}(\tilde{A}_k)\, \varpi^k \end{aligned}$$

shows that the projection $\mathbb{K}((z))[\tilde{\varphi}_1, \dots, \tilde{\varphi}_{\tilde{t}}]_{<(\tilde{d}_1, \dots, \tilde{d}_{\tilde{t}})} \to \tilde{\mathbb{P}}_{\tilde{t}}$ is injective, with image $\xi_{\tilde{t}}((\mathbb{P}_t)_{<1})$.

Given $\tilde{A} \in (\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$, let us write

$$\xi_{\tilde{t}}^{-1}(\tilde{A}) = \sum_{0\leqslant k<\tilde{d}_{i_{\tilde{t}}}} b_k \varpi^k$$

canonically in terms of ϖ, where $b_k \in (\mathbb{P}_{i_{\tilde{\imath}-1}})_{<1}$. Hence,

$$\tilde{A} = \sum_{0 \leqslant k < \tilde{d}_{\tilde{\imath}}} \xi_{\tilde{\imath}-1}(b_k)\, \tilde{\varphi}_{\tilde{\imath}}^k.$$

Definition (6.5) gives

$$\operatorname{val}_{\tilde{\imath}-1}(\xi_{\tilde{\imath}-1}(b_k)) \geqslant v(b_k; \mathbb{P}_{i_{\tilde{\imath}-1}}) - \operatorname{dct} \xi_{\tilde{\imath}-1},$$

hence

$$\begin{aligned}
\operatorname{val}_{\tilde{\imath}}(\tilde{A}) &= \min_{0 \leqslant k < \tilde{d}_{\tilde{\imath}}} (\operatorname{val}_{\tilde{\imath}-1}(\xi_{\tilde{\imath}-1}(b_k)) + \operatorname{val}_{\tilde{\imath}}(\tilde{\varphi}_{\tilde{\imath}}^k)) \\
&\geqslant \min_{0 \leqslant k < \tilde{d}_{\tilde{\imath}}} (v(b_k; \mathbb{P}_{i_{\tilde{\imath}-1}}) - \operatorname{dct} \xi_{\tilde{\imath}-1} + \operatorname{val}_{\tilde{\imath}}(\tilde{\varphi}_{\tilde{\imath}}^k)) \\
&= \left(\min_{0 \leqslant k < \tilde{d}_{\tilde{\imath}}} (v(b_k; \mathbb{P}_{i_{\tilde{\imath}-1}}) + v(\varpi^k; \mathbb{P}_t)) \right) - \operatorname{dct} \xi_{\tilde{\imath}-1} \\
&= v(\xi_{\tilde{\imath}}^{-1}(\tilde{A}); \mathbb{P}_t) - \operatorname{dct} \xi_{\tilde{\imath}-1},
\end{aligned}$$

and $\operatorname{dct} \xi_{\tilde{\imath}} \leqslant \operatorname{dct} \xi_{\tilde{\imath}-1}$. □

Let us now investigate flattenings of the first type from a complexity perspective. We still assume that a flattening is already at our disposal for $\mathbb{P}_{i_{\tilde{\imath}-1}}$.

PROPOSITION 7.5. *Let $(\mathbb{P}_i)_{i \leqslant t}$ be an almost reduced, effectively separable and regular contact tower at precision $\rho \in R_t^{-1}\mathbb{N}^{>0}$, and let $(\tilde{\mathbb{P}}_j)_{j \leqslant \tilde{\imath}-1}$ be a flattening for $(\mathbb{P}_i)_{i \leqslant i_{\tilde{\imath}-1}}$ at precision ρ and defect $\leqslant \eta$. If we are given $> \tilde{d}_{\tilde{\imath}}^2$ distinct elements in $\mathbb{K}$, then we can compute a flattening $(\tilde{\mathbb{P}}_j)_{j \leqslant \tilde{\imath}}$ of $(\mathbb{P}_i)_{i \leqslant t}$ as in Lemma 7.4, using*

$$\begin{aligned}
&\tilde{O}(D_t^{1+\epsilon} \tilde{d}_t^6 \operatorname{ht} \gamma_t) \\
+\ &\tilde{O}(\mathsf{B}(d_1, \ldots, d_{i_{\tilde{\imath}-1}}; \max(R_{i_{\tilde{\imath}-1}}^{-1}, \rho))\, (\min(R_{i_{\tilde{\imath}-1}}\rho, 1)\, \tilde{d}_{\tilde{\imath}})^2 \tilde{d}_{\tilde{\imath}} \operatorname{ht} \rho \log^4 D_t) \\
+\ &O(\mathsf{C}(\mathbb{P}_{i_{\tilde{\imath}-1}, <1; \rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{\imath}-1, <1; \rho+\eta})\, \min(R_{i_{\tilde{\imath}-1}}\rho, 1)\, \tilde{d}_{\tilde{\imath}} \log D_t)
\end{aligned}$$

operations in $\mathbb{K}$.

Proof. This proposition mostly rephrases Proposition 5.3 for $h = i_{\tilde{\imath}-1}$ by taking into account the computation of $\tilde{\Omega}_{\tilde{\imath}}$. Let us first describe the computation of Ω from (7.1). Since $\mathbb{E}_{i_{\tilde{\imath}-1}}$ is a finite dimensional vector space over $\mathbb{K}((z))$ [finite $\mathbb{K}((z))$-algebra], a classical Newton iteration can be used as follows. We let

$$\hat{\chi}(T) = T^{\tilde{d}_{\tilde{\imath}}} \chi(T^{-1})$$

and we compute its inverse $\hat{\Omega}$ of degree $\leqslant \tilde{d}_{\tilde{\imath}}$ in $\mathbb{E}_{i_{\tilde{\imath}-1}}[[T]] / \left(T^{\tilde{d}_{\tilde{\imath}}+1}\right)$. By Lemma 2.2, a polynomial in $\mathbb{E}_{i_{\tilde{\imath}-1}}[[T]] / \left(T^{\tilde{d}_{\tilde{\imath}}+1}\right)$ has $O(\min(R_{i_{\tilde{\imath}-1}}\rho, 1)\, \tilde{d}_{\tilde{\imath}})$ non-zero terms. Therefore two such polynomials can be multiplied by the schoolbook method using $O((\min(R_{i_{\tilde{\imath}-1}}\rho, 1) \deg \chi)^2)$ operations in $\mathbb{E}_{i_{\tilde{\imath}-1}}$. In total the Newton iteration performs $O(\log \tilde{d}_{\tilde{\imath}})$ such products, hence

$$\tilde{O}(\mathsf{B}(d_1, \ldots, d_{i_{\tilde{\imath}-1}}; \max(R_{i_{\tilde{\imath}-1}}^{-1}, \rho))\, (\min(R_{i_{\tilde{\imath}-1}}\rho, 1) \deg \chi)^2 \log \tilde{d}_{\tilde{\imath}}) \tag{7.2}$$

operations in $\mathbb{K}$. Then we have

$$\hat{\Omega}(T)\, \hat{\chi}(T) = 1 + T^{\tilde{d}_{\tilde{\imath}}+1} \hat{Q}(T),$$

for some $\hat{Q} \in \mathbb{E}_{i_{\tilde{\imath}-1}}[T]_{<\tilde{d}_{\tilde{\imath}}}$, so we define

$$\Omega(T) := T^{\tilde{d}_{\tilde{\imath}}} \hat{\Omega}(T^{-1}) \quad \text{and} \quad Q(T) := T^{\tilde{d}_{\tilde{\imath}}-1} \hat{Q}(T^{-1}),$$

and obtain

$$\Omega(T)\,\chi(T) = T^{2\tilde{d}_{\tilde{t}}} + Q(T).$$

Deducing $\tilde{\Phi}_{\tilde{t}} = \xi_{\tilde{t}-1}(\chi)$, $\tilde{\Omega}_{\tilde{t}} = \xi_{\tilde{t}-1}(\Omega)$, and $\xi_{\tilde{t}-1}(w_k)$ for $k = i_{\tilde{t}-1}+1, \ldots, i_{\tilde{t}}$ costs

$$O((i_{\tilde{t}} - i_{\tilde{t}-1})\,\mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta})\min(R_{i_{\tilde{t}-1}}\rho, 1)\deg\chi). \tag{7.3}$$

The total cost is the sum of (7.2), (7.3), and the cost stated in Proposition 5.3 for $h = i_{\tilde{t}-1}$. □

For efficiency reasons, conversions between $(\mathbb{P}_t)_{<1}$ and $(\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$ will benefit from precomputations: the precomputed data will be called "auxiliary" in the sequel. [Where is the complexity of the precomputations analyzed?]

PROPOSITION 7.6. *With the notation of Proposition 7.5, assume that the following auxiliary data are given at precision $\rho+\eta$:*

- $\xi_{\tilde{t}-1}(\Phi_{i_{\tilde{t}-1}+1}), \ldots, \xi_{\tilde{t}-1}(\Phi_t)$,
- $\xi_{\tilde{t}-1}(\Psi_{i_{\tilde{t}-1}+1}), \ldots, \xi_{\tilde{t}-1}(\Psi_t)$,
- $\tilde{\varpi} = \xi_{\tilde{t}-1}(\varpi)$,
- $\tilde{\chi} := \xi_{\tilde{t}-1}(\chi)$, $\tilde{w}_{i_{\tilde{t}-1}+1} := \xi_{\tilde{t}-1}(w_{i_{\tilde{t}-1}+1}), \ldots, \tilde{w}_{i_{\tilde{t}}} := \xi_{\tilde{t}-1}(w_{i_{\tilde{t}}})$.

Then we have

$$\begin{aligned}
&\mathsf{C}(\mathbb{P}_{i_{\tilde{t}},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t},<1;\rho+\eta}) \\
=\ & R_t^{-1}\tilde{O}\big(3^{\tilde{t}} D_t R_t (\rho+\eta)\,\tilde{d}_{\tilde{t}}^5\big) + \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta})\min(R_{i_{\tilde{t}-1}}\rho, 1)\,\tilde{d}_{\tilde{t}}.
\end{aligned}$$

Proof. Each polynomial in T at precision ρ of degree $<\tilde{d}_{\tilde{t}}$ has at most $\min(R_{i_{\tilde{t}-1}}\rho, 1)\,\tilde{d}_{\tilde{t}}$ non-zero terms by Lemma 2.3. By means of binary powering and schoolbook products and divisions with respect to T one sum or product modulo χ takes

$$O((\min(R_{i_{\tilde{t}-1}}\rho, 1)\,\tilde{d}_{\tilde{t}})^2)$$

operations in $\mathbb{E}_{i_{\tilde{t}-1}}$. Let $A \in (\mathbb{P}_t)_{<1}$ be written canonically

$$A = \sum_{k_{i_{\tilde{t}-1}+1} < d_{i_{\tilde{t}-1}+1}, \ldots, k_{i_{\tilde{t}}} < d_{i_{\tilde{t}}}} a_{k_{i_{\tilde{t}-1}+1}, \ldots, k_{i_{\tilde{t}}}} \varphi_{i_{\tilde{t}-1}+1}^{k_{i_{\tilde{t}-1}+1}} \cdots \varphi_{i_{\tilde{t}}}^{k_{i_{\tilde{t}}}}.$$

In order to convert A into $(\tilde{\mathbb{P}}_{\tilde{t}})_{<1}$, we compute $w_{i_{\tilde{t}-1}+1}^{k_{i_{\tilde{t}-1}+1}} \cdots w_{i_{\tilde{t}}}^{k_{i_{\tilde{t}}}} \operatorname{rem} \chi$ at precision ρ for all $0 \leqslant k_{i_{\tilde{t}-1}+1} < d_{i_{\tilde{t}-1}+1}, \ldots, 0 \leqslant k_{i_{\tilde{t}}} < d_{i_{\tilde{t}}}$ with $a_{k_{i_{\tilde{t}-1}+1}, \ldots, k_{i_{\tilde{t}}}} \neq 0$, via flattened arithmetic. By Lemma 2.3, at most $\min(R_{i_{\tilde{t}-1}}\rho, 1)\,\tilde{d}_{\tilde{t}}$ terms of A are non-zero. So we compute the flattened representative $\tilde{a}_{k_{i_{\tilde{t}-1}+1}, \ldots, k_{i_{\tilde{t}}}}$ of the non-zero $a_{k_{i_{\tilde{t}-1}+1}, \ldots, k_{i_{\tilde{t}}}}$, then $\tilde{w}_{i_{\tilde{t}-1}+1}^{k_{i_{\tilde{t}-1}+1}} \cdots \tilde{w}_{i_{\tilde{t}}}^{k_{i_{\tilde{t}}}} \operatorname{rem} \tilde{\chi}$ at precision $\rho+\eta$, so

$$\sum_{k_{i_{\tilde{t}-1}+1} < d_{i_{\tilde{t}-1}+1}, \ldots, k_{i_{\tilde{t}}} < d_{i_{\tilde{t}}}} \tilde{a}_{k_{i_{\tilde{t}-1}+1}, \ldots, k_{i_{\tilde{t}}}} \tilde{w}_{i_{\tilde{t}-1}+1}^{k_{i_{\tilde{t}-1}+1}} \cdots \tilde{w}_{i_{\tilde{t}}}^{k_{i_{\tilde{t}}}} \operatorname{rem} \tilde{\chi}$$

is obtained using

$$O((\min(R_{i_{\tilde{t}-1}}(\rho+\eta), 1)\,\tilde{d}_{\tilde{t}})^3 \log D_t)$$

flattened operations in $\mathbb{E}_{i_{\tilde{t}-1}}$, which corresponds to

$$\begin{aligned}
&R_{i_{\tilde{t}-1}}^{-1}\tilde{O}\big(3^{\tilde{t}-1}\tilde{D}_{\tilde{t}-1} R_{i_{\tilde{t}-1}} \max(R_{i_{\tilde{t}-1}}^{-1}, \rho+\eta)\big)\,(\min(R_{i_{\tilde{t}-1}}(\rho+\eta), 1)\,\tilde{d}_{\tilde{t}})^3 \log D_t \\
=\ & R_{i_{\tilde{t}-1}}^{-1}\tilde{O}\big(3^{\tilde{t}} D_t R_{i_{\tilde{t}-1}} (\rho+\eta)\,\tilde{d}_{\tilde{t}}^2\big) \\
=\ & R_t^{-1}\tilde{O}\big(3^{\tilde{t}} D_t R_t (\rho+\eta)\,\tilde{d}_{\tilde{t}}^2\big)
\end{aligned}$$

operations in $\mathbb{K}$, by Proposition 6.7 with $t+1=i_{\tilde{\imath}-1}$ and $D_t l=\tilde{D}_{\tilde{\imath}-1}$.

Conversely, given

$$\tilde{A}=\sum_{0\leqslant k<\tilde{d}_{\tilde{\imath}}}\tilde{a}_k\tilde{\varphi}_{\tilde{\imath}}^k$$

there are $\leqslant\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}$ non-zero $\tilde{a}_k$, by Lemma 2.3, so the computation of

$$\sum_{0\leqslant k<\tilde{d}_{\tilde{\imath}}}\tilde{a}_k\tilde{\omega}^k$$

takes $O(\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}\log\tilde{d}_{\tilde{\imath}})$ flattened operations in $(\mathbb{P}_t)_{<1}$. By taking advantage of the auxiliary data $\xi_{\tilde{\imath}-1}(\Phi_{i_{\tilde{\imath}-1}+1}),\ldots,\xi_{\tilde{\imath}-1}(\Phi_t)$ and $\xi_{\tilde{\imath}-1}(\Psi_{i_{\tilde{\imath}-1}+1}),\ldots,\xi_{\tilde{\imath}-1}(\Psi_t)$, each such flattened operation reduces to

$$\begin{aligned}
&O(5^{i_{\tilde{\imath}}-i_{\tilde{\imath}-1}}\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho))\,(\min(R_{i_{\tilde{\imath}-1}}\rho,1)\,d_{i_{\tilde{\imath}-1}+1}\cdots d_t)^2)\\
=\;&O(5^{i_{\tilde{\imath}}-i_{\tilde{\imath}-1}}\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho))\,(\min(R_{i_{\tilde{\imath}-1}}\rho,1)\,\tilde{d}_{\tilde{\imath}})^2)\\
=\;&O(\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho))\min(R_{i_{\tilde{\imath}-1}}\rho,1)\,\tilde{d}_{\tilde{\imath}}^5)\qquad(\text{using } 2^{i_{\tilde{\imath}}-i_{\tilde{\imath}-1}}\leqslant\tilde{d}_{\tilde{\imath}})
\end{aligned}$$

operations in $\mathbb{K}$ by Proposition 3.11 (with $h=i_{\tilde{\imath}-1}$). Thanks to Proposition 6.7 (with $t+1=i_{\tilde{\imath}-1}$ and $D_t l=\tilde{D}_{\tilde{\imath}-1}$), and still for the flattened representation, we may take

$$\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\eta))=R_{i_{\tilde{\imath}-1}}^{-1}\tilde{O}\big(3^{\tilde{\imath}-1}\tilde{D}_{\tilde{\imath}-1}R_{i_{\tilde{\imath}-1}}\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\eta)\big).$$

Overall, the flattened representation of $\sum_{0\leqslant k<\tilde{d}_{\tilde{\imath}}}\tilde{a}_k\tilde{\omega}^k$ totalizes

$$\begin{aligned}
&O(\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho))\min(R_{i_{\tilde{\imath}-1}}\rho,1)\,\tilde{d}_{\tilde{\imath}}^5\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}\log\tilde{d}_{\tilde{\imath}})\\
=\;&R_{i_{\tilde{\imath}-1}}^{-1}\tilde{O}\big(3^{\tilde{\imath}-1}\tilde{D}_{\tilde{\imath}-1}R_{i_{\tilde{\imath}-1}}\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\eta)\big)\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}^6\log\tilde{d}_{\tilde{\imath}}\\
=\;&R_{i_{\tilde{\imath}-1}}^{-1}\tilde{O}\big(3^{\tilde{\imath}}\tilde{D}_{\tilde{\imath}}R_{i_{\tilde{\imath}-1}}(\rho+\eta)\,\tilde{d}_{\tilde{\imath}}^5\big)\\
=\;&R_t^{-1}\tilde{O}\big(3^{\tilde{\imath}}D_tR_t(\rho+\eta)\,\tilde{d}_{\tilde{\imath}}^5\big)
\end{aligned}$$

operations in $\mathbb{K}$, which concludes the proof. □

Example 7.7. (Continued from Example 5.4) We take $\tilde{t}:=2$, $i_1=1$ and $i_2=3$ and relative precision $\rho=1/4$ and defect $\eta=0$. The first level of the flattening is trivial:

$$\tilde{\Phi}_1(\tilde{\varphi}_1):=\Phi_1(\tilde{\varphi}_1).$$

For the second level we add the following flattened level of first type:

$$\tilde{\Phi}_2(\tilde{\varphi}_1,\tilde{\varphi}_2):=\tilde{\varphi}_2^{16}+\tilde{\varphi}_1\tilde{\varphi}_2^{13}+3\,\tilde{\varphi}_1\tilde{\varphi}_2^{12}+7z\,\tilde{\varphi}_2^9+6z\,\tilde{\varphi}_2^8+2z\,\tilde{\varphi}_1\tilde{\varphi}_2^4+9z^2$$

and

$$\begin{aligned}
\xi_2(\varphi_1)&:=\tilde{\varphi}_1\\
\xi_2(\varphi_2)&:=z^{-1}\tilde{\varphi}_1\tilde{\varphi}_2^{15}+6z^{-1}\tilde{\varphi}_1\tilde{\varphi}_2^{14}+8\,\tilde{\varphi}_2^{10}+7\,\tilde{\varphi}_1\tilde{\varphi}_2^7+5\,\tilde{\varphi}_1\tilde{\varphi}_2^6+2z\,\tilde{\varphi}_2^3+2z\,\tilde{\varphi}_2^2\\
\xi_2(\varphi_3)&:=7z^3\tilde{\varphi}_1\tilde{\varphi}_2^{14}+7z^3\tilde{\varphi}_1\tilde{\varphi}_2^{13}+7z^4\tilde{\varphi}_2^{10}+9z^4\tilde{\varphi}_2^9+6z^4\tilde{\varphi}_1\tilde{\varphi}_2^6+4z^4\tilde{\varphi}_1\tilde{\varphi}_2^5+z^5\tilde{\varphi}_2^2+z^5\tilde{\varphi}_2.
\end{aligned}$$

7.3. Second type of flattening

The second type of flattening concerns the case where

$$\epsilon_{i_{j-1}+1}=\epsilon_{i_{j-1}+2}=\cdots=\epsilon_{i_j-2}=\epsilon_{i_j-1}=1.\tag{7.4}$$

For all $k \leqslant l$ we define the following polynomials by induction:

$$\Phi_{k\rightsquigarrow l}(\varphi_1,\dots,\varphi_k) := \Phi_l(\varphi_1,\dots,\varphi_k,\Phi_{k\rightsquigarrow k}(\varphi_1,\dots,\varphi_k),\dots,\Phi_{k\rightsquigarrow l-1}(\varphi_1,\dots,\varphi_k)).$$

Note that $\Phi_{k\rightsquigarrow k}(\varphi_1,\dots,\varphi_k) = \Phi_k(\varphi_1,\dots,\varphi_k)$.

Example 7.8. $\Phi_{1\rightsquigarrow 2}(\varphi_1) = \Phi_2(\varphi_1,\Phi_1(\varphi_1))$ and $\Phi_{1\rightsquigarrow 3}(\varphi_1) = \Phi_3(\varphi_1,\Phi_1(\varphi_1),\Phi_{1\rightsquigarrow 2}(\varphi_1))$.

Again, in order to keep the notation simple, and without loss of generality, we focus on the case where $j = \tilde{t}$.

LEMMA 7.9. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an almost reduced, effectively separable, and regular contact tower at precision $\rho \in R_t^{-1}\mathbb{N}^{>0}$, let $(\tilde{\mathbb{P}}_j)_{j\leqslant \tilde{t}-1}$ be a flattening for $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}-1}}$ and assume that $\epsilon_{i_{\tilde{t}-1}+1} = \cdots = \epsilon_{i_{\tilde{t}}-1} = 1$. Then there exists a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant \tilde{t}}$ for $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}}}$ with $i_{\tilde{t}} := t$, $\tilde{\epsilon}_{\tilde{t}} = \epsilon_{i_{\tilde{t}}}$,*

$$\tilde{\Phi}_{\tilde{t}}(\tilde{\varphi}_1,\dots,\tilde{\varphi}_{\tilde{t}}) := \xi_{\tilde{t}-1}(\Phi_{i_{\tilde{t}-1}+1\rightsquigarrow i_{\tilde{t}}}),$$

$$\begin{aligned}
\xi_{\tilde{t}}\colon \quad \mathbb{P}_t &\to \tilde{\mathbb{P}}_{\tilde{t}}\\
\varphi_k &\mapsto \xi_{\tilde{t}-1}(\varphi_k) \text{ for } k = 1,\dots,i_{\tilde{t}-1}+1\\
\varphi_k &\mapsto \xi_{\tilde{t}-1}(\Phi_{i_{\tilde{t}-1}+1\rightsquigarrow k-1}(\varphi_1,\dots,\varphi_{i_{\tilde{t}-1}+1})) \text{ for } k = i_{\tilde{t}-1}+2,\dots,i_{\tilde{t}}\\
\varphi_{i_{\tilde{t}}+1} &\mapsto \tilde{\varphi}_{\tilde{t}+1},
\end{aligned}$$

$\tilde{\Omega}_{\tilde{t}} := \xi_{\tilde{t}-1}(\Omega)$, *where Ω stands for the pre-inverse of $\Phi_{i_{\tilde{t}-1}+1\rightsquigarrow i_{\tilde{t}}}$ in $\mathbb{P}_{i_{\tilde{t}-1}}$ at precision $\rho+\kappa_{\tilde{t}}$, where*

$$\kappa_{\tilde{t}} := \sum_{i_{\tilde{t}-1}+1<k\leqslant i_{\tilde{t}}} (d_k\cdots d_{i_{\tilde{t}}}-1)\,(\gamma_k - d_{k-1}\gamma_{k-1})$$

satisfies

$$\operatorname{dct}\xi_{\tilde{t}} \leqslant \operatorname{dct}\xi_{\tilde{t}-1} + \kappa_{\tilde{t}} \quad \text{and} \quad \kappa_{\tilde{t}} \leqslant \tilde{d}_{\tilde{t}}\rho.$$

Proof. For $k = i_{\tilde{t}-1}+2,\dots,i_{\tilde{t}}$ the polynomial $\Phi_{i_{\tilde{t}-1}+1\rightsquigarrow k}(\varphi_1,\dots,\varphi_{i_{\tilde{t}-1}+1})$ is monic in $\varphi_{i_{\tilde{t}-1}+1}$ and its initial in $\mathbb{P}_{i_{\tilde{t}-1}}$ is

$$\operatorname{in}\Big(\Phi_{i_{\tilde{t}-1}+1}^{d_{i_{\tilde{t}-1}+2}\cdots d_k};\mathbb{P}_{i_{\tilde{t}-1}}\Big).$$

It follows that $\Phi_{i_{\tilde{t}-1}+1\rightsquigarrow i_{\tilde{t}}}$ is clustered in $\mathbb{P}_{i_{\tilde{t}-1}}$ and that

$$v(\Phi_{i_{\tilde{t}-1}+1\rightsquigarrow i_{\tilde{t}}};\mathbb{P}_{i_{\tilde{t}-1}}) = \tilde{d}_{\tilde{t}}\gamma_{i_{\tilde{t}-1}+1}.$$

By [11, Lemma 15] the map

$$\begin{aligned}
\mathbb{K}((z))[\tilde{\varphi}_1,\dots,\tilde{\varphi}_{\tilde{t}-1}]_{<(\tilde{d}_1,\dots,\tilde{d}_{\tilde{t}-1})}[\tilde{\varphi}_{\tilde{t}}]_{<\tilde{d}_{\tilde{t}}} &\cong (\mathbb{P}_t)_{<1}\\
\sum_{k=0}^{\tilde{d}_{\tilde{t}}-1} \tilde{A}_k\tilde{\varphi}_{\tilde{t}}^k &\mapsto \sum_{k=0}^{\tilde{d}_{\tilde{t}}-1} \xi_{\tilde{t}-1}^{-1}(\tilde{A}_k)\,\varphi_{i_{\tilde{t}-1}+1}^k,
\end{aligned}$$

where $\tilde{A}_k \in \mathbb{K}((z))[\tilde{\varphi}_1,\dots,\tilde{\varphi}_{\tilde{t}-1}]_{<(\tilde{d}_1,\dots,\tilde{d}_{\tilde{t}-1})}$, is a $\mathbb{K}((z))$-vector space isomorphism, so Property $\mathbf{F_3}$ of Definition 6.1 holds. Other properties of Definition 6.1 hold by construction. For

$$A = \sum_{k_{i_{\tilde{t}-1}+1}<d_{i_{\tilde{t}-1}+1},\dots,k_{i_{\tilde{t}}}<d_{i_{\tilde{t}}}} a_{k_{i_{\tilde{t}-1}+1},\dots,k_{i_{\tilde{t}}}} \varphi_{i_{\tilde{t}-1}+1}^{k_{i_{\tilde{t}-1}+1}}\cdots\varphi_{i_{\tilde{t}}}^{k_{i_{\tilde{t}}}} \in (\mathbb{P}_t)_{<1},$$

where $a_{k_{i_{\tilde{t}-1}+1},\dots,k_{i_{\tilde{t}}}} \in (\mathbb{P}_{i_{\tilde{t}-1}})_{<1}$, we have

$$v(A;\mathbb{P}_t) = \min_{k_{i_{\tilde{t}-1}+1}<d_{i_{\tilde{t}-1}+1},\dots,k_{i_{\tilde{t}}}<d_{i_{\tilde{t}}}} \big(v\big(a_{k_{i_{\tilde{t}-1}+1},\dots,k_{i_{\tilde{t}}}};\mathbb{P}_{i_{\tilde{t}-1}}\big) + k_{i_{\tilde{t}-1}+1}\gamma_{i_{\tilde{t}-1}+1} + \cdots + k_{i_{\tilde{t}}}\gamma_{i_{\tilde{t}}}\big).$$

Since $\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}}}$ is clustered in $\mathbb{P}_{i_{\tilde{\imath}-1}}$ of valuation $d_{i_{\tilde{\imath}-1}+1}\cdots d_{i_{\tilde{\imath}}}\gamma_{i_{\tilde{\imath}-1}+1}$, the contact polynomial $\varphi_{i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+1}}\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+2}}\cdots\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}}-1}^{k_{i_{\tilde{\imath}}}}$ is clustered in $\mathbb{P}_{i_{\tilde{\imath}-1}}$ of degree

$$\Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}} := k_{i_{\tilde{\imath}-1}+1} + d_{i_{\tilde{\imath}-1}+1}k_{i_{\tilde{\imath}-1}+2} + \cdots + d_{i_{\tilde{\imath}-1}+1}\cdots d_{i_{\tilde{\imath}}-1}k_{i_{\tilde{\imath}}}$$

in $\varphi_{i_{\tilde{\imath}-1}+1}$ and of valuation

$$v\Big(\varphi_{i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+1}}\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+2}}\cdots\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}}-1}^{k_{i_{\tilde{\imath}}}};\mathbb{P}_{i_{\tilde{\imath}-1}}\Big) = \Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\gamma_{i_{\tilde{\imath}-1}+1}.$$

It follows that

$$\begin{aligned}
& v\Big(a_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\varphi_{i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+1}}\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+2}}\cdots\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}}-1}^{k_{i_{\tilde{\imath}}}};\mathbb{P}_{i_{\tilde{\imath}-1}}\Big)\\
\geqslant\ & v\big(a_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}};\mathbb{P}_{i_{\tilde{\imath}-1}}\big) + v\Big(\varphi_{i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+1}}\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+2}}\cdots\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}}-1}^{k_{i_{\tilde{\imath}}}};\mathbb{P}_{i_{\tilde{\imath}-1}}\Big)\\
\geqslant\ & v(A;\mathbb{P}_{i_{\tilde{\imath}}}) - (k_{i_{\tilde{\imath}-1}+1}\gamma_{i_{\tilde{\imath}-1}+1} + \cdots + k_{i_{\tilde{\imath}}}\gamma_{i_{\tilde{\imath}}}) + \Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\gamma_{i_{\tilde{\imath}-1}+1},
\end{aligned}$$

hence

$$v(A;\mathbb{P}_{i_{\tilde{\imath}-1}}) \geqslant v(A;\mathbb{P}_{i_{\tilde{\imath}}}) - \eta, \tag{7.5}$$

where

$$\eta := \max_{k_{i_{\tilde{\imath}-1}+1}<d_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}<d_{i_{\tilde{\imath}}}} \big(k_{i_{\tilde{\imath}-1}+1}\gamma_{i_{\tilde{\imath}-1}+1} + \cdots + k_{i_{\tilde{\imath}}}\gamma_{i_{\tilde{\imath}}} - \Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\gamma_{i_{\tilde{\imath}-1}+1}\big).$$

Note that

$$\gamma_l \geqslant d_{i_{\tilde{\imath}-1}+1}\cdots d_{l-1}\gamma_{i_{\tilde{\imath}-1}+1}$$

for $l = i_{\tilde{\imath}-1}+1,\ldots,i_{\tilde{\imath}}$, so $\eta\geqslant 0$. Consequently [where do you need $\eta\geqslant 0$?], the canonical representative of A in $\mathbb{P}_{i_{\tilde{\imath}-1}}$ can be written in the canonical form

$$A = \sum_{k_{i_{\tilde{\imath}-1}+1}<d_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}<d_{i_{\tilde{\imath}}}} b_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\varphi_{i_{\tilde{\imath}-1}+1}^{\Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}},$$

with

$$\begin{aligned}
v\big(b_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}};\mathbb{P}_{i_{\tilde{\imath}-1}}\big) &\geqslant v(A;\mathbb{P}_{i_{\tilde{\imath}-1}}) - \Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\gamma_{i_{\tilde{\imath}-1}+1}\\
&\geqslant v(A;\mathbb{P}_{i_{\tilde{\imath}}}) - \eta - \Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\gamma_{i_{\tilde{\imath}-1}+1},
\end{aligned} \tag{7.6}$$

using (7.5). Therefore

$$\xi_{\tilde{\imath}}(A) = \sum_{k_{i_{\tilde{\imath}-1}+1}<d_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}<d_{i_{\tilde{\imath}}}} \xi_{\tilde{\imath}-1}\big(b_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\big)\,\tilde{\varphi}_{\tilde{\imath}}^{\Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}}.$$

is the canonical representative of $\xi_{\tilde{\imath}}(A)$ and

$$\operatorname{val}_{\tilde{\imath}}(\xi_{\tilde{\imath}}(A)) = \min_{k_{i_{\tilde{\imath}-1}+1}<d_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}<d_{i_{\tilde{\imath}}}} \big(\operatorname{val}_{\tilde{\imath}-1}\big(\xi_{\tilde{\imath}-1}\big(b_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\big)\big) + \Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\gamma_{i_{\tilde{\imath}-1}+1}\big),$$

since $\gamma_{i_{\tilde{\imath}-1}+1} = \operatorname{val}_{\tilde{\imath}}\tilde{\varphi}_{\tilde{\imath}}$. Then, combining (7.6) with

$$v\big(b_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}};\mathbb{P}_{i_{\tilde{\imath}-1}}\big) - \operatorname{dct}\xi_{\tilde{\imath}-1} \leqslant \operatorname{val}_{\tilde{\imath}-1}\big(\xi_{\tilde{\imath}-1}\big(b_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\big)\big)$$

yields

$$v(A;\mathbb{P}_{i_{\tilde{\imath}}}) - \eta - \operatorname{dct}\xi_{\tilde{\imath}-1} \leqslant \operatorname{val}_{\tilde{\imath}-1}\big(\xi_{\tilde{\imath}-1}\big(b_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\big)\big) + \Delta_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\gamma_{i_{\tilde{\imath}-1}+1},$$

whence

$$\operatorname{val}_{\tilde{\imath}}(\xi_{\tilde{\imath}}(A)) \geqslant v(A;\mathbb{P}_{i_{\tilde{\imath}}}) - \eta - \operatorname{dct}\xi_{\tilde{\imath}-1}.$$

Next, we verify that

$$\begin{aligned}
\eta &= \max_{k_{i_{\tilde{\imath}-1}+1}<d_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}<d_{i_{\tilde{\imath}}}} \sum_{i_{\tilde{\imath}-1}+1<l\leqslant i_{\tilde{\imath}}} k_l\,(\gamma_l - d_{i_{\tilde{\imath}-1}+1}\cdots d_{l-1}\gamma_{i_{\tilde{\imath}-1}+1}) \\
&= \sum_{i_{\tilde{\imath}-1}+1<l\leqslant i_{\tilde{\imath}}} (d_l-1)\,(\gamma_l - d_{i_{\tilde{\imath}-1}+1}\cdots d_{l-1}\gamma_{i_{\tilde{\imath}-1}+1}) \\
&= \sum_{i_{\tilde{\imath}-1}+1<l\leqslant i_{\tilde{\imath}}} (d_l-1) \sum_{i_{\tilde{\imath}-1}+1<k\leqslant l} d_k\cdots d_{l-1}\,(\gamma_k - d_{k-1}\gamma_{k-1}) \\
&= \sum_{i_{\tilde{\imath}-1}+1<k\leqslant i_{\tilde{\imath}}} (\gamma_k - d_{k-1}\gamma_{k-1}) \sum_{k\leqslant l\leqslant i_{\tilde{\imath}}} d_k\cdots d_{l-1}\,(d_l-1) \\
&= \sum_{i_{\tilde{\imath}-1}+1<k\leqslant i_{\tilde{\imath}}} (d_k\cdots d_{i_{\tilde{\imath}}}-1)\,(\gamma_k - d_{k-1}\gamma_{k-1}) \\
&= \kappa_{\tilde{\imath}}.
\end{aligned}$$

In our setting, we recall that $\epsilon_{i-1}=1$ holds whenever $\gamma_i - d_{i-1}\gamma_{i-1}\leqslant\rho$. Therefore (7.4) implies that $\gamma_k - d_{k-1}\gamma_{k-1}\leqslant\rho$ for all $i_{\tilde{\imath}-1}+1<k\leqslant i_{\tilde{\imath}}$. By using $d_k\geqslant 2$ for $k\geqslant i_{\tilde{\imath}-1}+1$, we obtain $\tilde{d}_{\tilde{\imath}}\geqslant 2^{k-(i_{\tilde{\imath}-1}+1)}\,d_k\cdots d_{i_{\tilde{\imath}}}$, hence the bound

$$\begin{aligned}
\kappa_{\tilde{\imath}} &\leqslant \sum_{i_{\tilde{\imath}-1}+1<k\leqslant i_{\tilde{\imath}}} (d_k\cdots d_{i_{\tilde{\imath}}}-1)\,\rho \\
&< \sum_{i_{\tilde{\imath}-1}+1<k\leqslant i_{\tilde{\imath}}} \frac{1}{2^{k-(i_{\tilde{\imath}-1}+1)}}\,\tilde{d}_{\tilde{\imath}}\rho \\
&\leqslant \tilde{d}_{\tilde{\imath}}\rho.
\end{aligned}$$

□

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

$$\begin{aligned}
\Pi_i:\quad \mathbb{P}_i &\to \mathbb{P}_{i-1} \\
A &\mapsto A(\varphi_1,\ldots,\varphi_i,\Phi_i).
\end{aligned}$$

For $k'\geqslant k$, we also define

$$\Pi_{k'\rightsquigarrow k} = \Pi_k\circ\cdots\circ\Pi_{k'}.$$

Let us now study flattenings of the second type from a complexity perspective. We will not optimize the complexity of our algorithms as a function $\tilde{d}_{\tilde{\imath}}$, because $\tilde{d}_{\tilde{\imath}}$ will always be taken relatively small in the next section.

LEMMA 7.10. *Let $l\in r_{t+1}\,\mathbb{N}^{>0}$, let $A\in(\mathbb{P}_t)_{<l}$ be given at relative precision $\rho\in R_{t+1}^{-1}\,\mathbb{N}^{>0}$, and let $\eta\geqslant(l-1)\,(\gamma_{t+1}-d_t\gamma_t)$. Then*

$$[\Pi_t(A);\mathbb{P}_{t-1}]_{v(A;\mathbb{P}_t)-\eta;\rho+\eta} = [\Pi_t(A);\mathbb{P}_{t-1}]_{0;v(A;\mathbb{P}_t)+\rho}$$

can be computed using

$$O(\mathsf{B}(d_1,\ldots,d_{t-1};\max(R_{t-1}^{-1},\rho+\eta))\,(\min(R_{t-1}\,(\rho+\eta),1)\,d_t\,l)^2\,l)$$

operations in $\mathbb{K}$.

Proof. Let $\sum_{j<l} A_j\,\varphi_{t+1}^j$ denote the contact representation of A. We obtain

$$[A_j\,\Phi_t^j;\mathbb{P}_{t-1}]_{v(A;\mathbb{P}_t)-\eta;\rho+\eta}$$

for all $j=0,\ldots,l-1$, using

$$O(\mathsf{B}(d_1,\ldots,d_{t-1};\max(R_{t-1}^{-1},\rho+\eta))\,(\min(R_{t-1}(\rho+\eta),1)\,d_t\,l)^2\,l)$$

operations in $\mathbb{K}$ by Proposition 3.5, whence the claimed cost. □

LEMMA 7.11. *Let $l\in r_{t+1}\,\mathbb{N}^{>0}$, let $F\in\mathbb{P}_t$ be monic of degree l in φ_{t+1} and given in contact representation $\sum_{i\leqslant l}F_i\,\varphi_{t+1}^i$, and let $\varphi_{t+1}+G$ denote the pre-inverse of $\varphi_{t+1}+F_{l-1}$. Then, $(\varphi_{t+1}+G)^j\,\mathrm{quo}_{\varphi_{t+1}}\,\varphi_{t+1}^{j-1}$ is the pre-inverse of $F^j\,\mathrm{quo}_{\varphi_{t+1}}\,\varphi_{t+1}^{jl-1}$ for all $j\geqslant 1$.*

Proof. Expanding the terms of highest degrees of the product of two monic contact polynomials F and H yields

$$\begin{aligned}&(\varphi_{t+1}^l+F_{l-1}\,\varphi_{t+1}^{l-1}+F_{l-2}\,\varphi_{t+1}^{l-2}+\cdots)\,(\varphi_{t+1}^m+H_{m-1}\,\varphi_{t+1}^{m-1}+H_{m-2}\,\varphi_{t+1}^{m-2}+\cdots)\\ =\;&\varphi_{t+1}^{l+m}+(F_{l-1}+H_{m-1})\,\varphi_{t+1}^{l+m-1}+(F_{l-1}H_{m-1}+F_{l-2}+H_{m-2})\,\varphi_{t+1}^{l+m-2}+\cdots\end{aligned}$$

Consequently, the sub-dominant coefficient $F_{l-1}+H_{m-1}+F_{l-1}H_{m-1}\,\mathrm{quo}_{\varphi_t}\,\Phi_t$ in this product only depend on the sub-dominant coefficients F_{l-1} and H_{m-1} of F and H. [Not clear how this yields the desired result. The change from $\square\,\mathrm{quo}_{\varphi_{t+1}}\,\varphi_{t+1}^{j-1}$ to $\square\,\mathrm{quo}_{\varphi_t}\,\Phi_t$ is also confusing.] □

LEMMA 7.12. *Let $l\in r_{t+1}\,\mathbb{N}^{>0}$, let $A\in(\mathbb{P}_t)_{<l}$ be of valuation $\geqslant\sigma$, let $\rho\in R_{t+1}^{-1}\,\mathbb{N}^{>0}$, and let $\eta\geqslant(l-1)\,(\gamma_{t+1}-d_t\,\gamma_t)$. Given $B:=[\Pi_t(A);\mathbb{P}_{t-1}]_{\sigma-\eta;\rho+\eta}$ and $[\Psi_t;\mathbb{P}_{t-1}]_{\gamma_t;\rho+\eta}$, we can compute $[A;\mathbb{P}_t]_{\sigma;\rho}$ using*

$$O(\mathsf{B}(d_1,\ldots,d_{t-1};\max(R_{t-1}^{-1},\rho+\eta))\,(\min(R_{t-1}(\rho+\eta),1)\,d_t\,l)^2\,l)$$

operations in $\mathbb{K}$.

Proof. Let $A=\sum_{j<l}A_j\,\varphi_{t+1}^j$ and $B=\sum_{k<d_t l}B_k\,\varphi_t^k$ denote the contact representations of A and B. We compute $C_j:=[\Phi_t^j;\mathbb{P}_{t-1}]_{jd_t\gamma_t;\rho+\eta}$ and $[\Psi_t^j\,\mathrm{quo}_{\varphi_t}\,\varphi_t^{j-1};\mathbb{P}_{t-1}]_{\gamma_t;\rho+\eta}$ for $j=0,\ldots,l-1$, using

$$O(\mathsf{B}(d_1,\ldots,d_{t-1};\max(R_{t-1}^{-1},\rho+\eta))\,(\min(R_{t-1}(\rho+\eta),1)\,d_t\,l)^2\,l)$$

operations in $\mathbb{K}$ by Proposition 3.5. Then, we set $H_{l-1}:=B$ and for j from $l-1$ down to 0, we recursively compute

$$\begin{aligned}D_j&:=[H_j\,\mathrm{quo}_{\varphi_t}\,C_j;\mathbb{P}_{t-1}]_{\sigma-\eta-jd_t\gamma_t;\rho+\eta}\\ H_{j-1}&:=[H_j\,\mathrm{rem}_{\varphi_t}\,C_j;\mathbb{P}_{t-1}]_{\sigma-\eta;\rho+\eta}.\end{aligned}$$

In this way, we obtain the following approximation of the Φ_t-adic expansion of B:

$$B=\left[\sum_{j<l}D_j\,\Phi_t^j;\mathbb{P}_{t-1}\right]_{\sigma-\eta;\rho+\eta}.$$

Since

$$\sigma-\eta-jd_t\gamma_t+\rho+\eta=\sigma-jd_t\gamma_t+\rho\geqslant\sigma+\rho-j\gamma_{t+1},$$

we can read off $[A_j;\mathbb{P}_{t-1}]_{\sigma;\rho}$ from D_j. From Lemma 7.11, we know that $\Psi_t^j\,\mathrm{quo}_{\varphi_t}\,\varphi_t^{j-1}$ is the pre-inverse of $\Phi_t^j\,\mathrm{quo}_{\varphi_t}\,\varphi_t^{d_tj-1}$. Taking advantage of these pre-inverses, this sequence of divisions costs

$$O(\mathsf{B}(d_1,\ldots,d_{t-1};\max(R_{t-1}^{-1},\rho+\eta))\,(\min(R_{t-1}(\rho+\eta),1)\,d_t\,l)^2\,l),$$

in total, thanks to Proposition 3.6. □

LEMMA 7.13. *Let $h<t$, let $\rho\in R_{t+1}^{-1}\,\mathbb{N}^{>0}$, let*

$$\eta\geqslant (l-1)\,(\gamma_{t+1}-d_t\gamma_t)+(d_tl-1)\,(\gamma_t-d_{t-1}\gamma_{t-1})+\cdots+(d_{h+2}\cdots d_tl-1)\,(\gamma_{h+2}-d_{h+1}\gamma_{h+1}),$$

and assume that $\Psi_h,\ldots,\Psi_t$ are known at precision $\rho+\eta$. One evaluation of $\Pi_{t\rightsquigarrow h+1}$ with relative precision ρ at an element of degree $<l\in r_{t+1}\,\mathbb{N}^{>0}$ in φ_{t+1} at precision $\rho+\eta$, and one evaluation of $\Pi_{t\rightsquigarrow h+1}^{-1}$ with relative precision $\rho+\eta$ at a polynomial of degree $<d_{h+1}\cdots d_tl$ in φ_{h+1}, both cost

$$\tilde{O}(5^{t-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho+\eta))\min(R_h(\rho+\eta),1)\,(d_h\cdots d_tl)^4)$$

operations in $\mathbb{K}$.

Proof. Recall that $\Pi_{t\rightsquigarrow h+1}=\Pi_{h+1}\circ\cdots\circ\Pi_t$. We apply Lemma 7.10 for Π_i (resp. Lemma 7.12 for Π_i^{-1}) recursively for i from t down to $h+1$. The total cost is

$$O\left(\sum_{h\leqslant i<t}\mathsf{B}(d_1,\ldots,d_i;\max(R_i^{-1},\rho+\eta))\,(\min(R_i\max(R_{i+2}^{-1},\rho+\eta),1)\,d_{i+1}\cdots d_tl)^2d_{i+2}\cdots d_tl\right),$$

which is bounded by

$$O\left(\sum_{h\leqslant i<t}\mathsf{B}(d_1,\ldots,d_i;\max(R_i^{-1},\rho+\eta))\,(\min(R_i(\rho+\eta),1)\,d_{i+1}\cdots d_tl)^2\,(d_{i+2}\cdots d_tl)^2\right),$$

For $i=h,\ldots,t-1$, Proposition 3.11 gives us

$$\begin{aligned}&\mathsf{B}(d_1,\ldots,d_i;\max(R_i^{-1},\rho+\eta))\\ \leqslant\;&5^{i-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho+\eta))\,(\min(R_h\max(R_i^{-1},\rho+\eta),1)\,d_{h+1}\cdots d_i)^2.\end{aligned}$$

Consequently,

$$\begin{aligned}&O(\mathsf{B}(d_1,\ldots,d_i;\max(R_i^{-1},\rho+\eta))\,(\min(R_i(\rho+\eta),1)\,d_{i+1}\cdots d_tl)^2\,(d_{i+2}\cdots d_tl)^2)\\ \leqslant\;&5^{i-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho+\eta))\min(R_i(\rho+\eta),1)\\ &\quad\times\min(R_h\max(R_i^{-1},\rho+\eta),1)\,(d_{h+1}\cdots d_tl)^4\\ \leqslant\;&5^{i-h}\,\mathsf{B}(d_1,\ldots,d_h;\max(R_h^{-1},\rho+\eta))\min(R_h(\rho+\eta),1)\,(d_h\cdots d_tl)^4,\end{aligned}$$

using Lemma 3.10. The total cost for $\Pi_{t\rightsquigarrow h+1}$ and $\Pi_{t\rightsquigarrow h+1}^{-1}$ directly follows by taking the sum of the latter bound for $i=h,\ldots,t-1$. □

PROPOSITION 7.14. *Given an almost reduced effectively separable and regular contact tower $(\mathbb{P}_i)_{i\leqslant t}$, given $\rho\in R_t^{-1}\,\mathbb{N}^{>0}$, and a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}-1}$ for $(\mathbb{P}_i)_{i\leqslant i_{\tilde{t}-1}}$ at precision ρ and defect $\leqslant\eta'$. Assume that $\epsilon_{i_{\tilde{t}-1}+1}=\cdots=\epsilon_{i_{\tilde{t}}-1}=1$ and that $\Psi_{i_{\tilde{t}-1}+1},\ldots,\Psi_t$ are known at precision $\rho+\kappa_{\tilde{t}}$. Then we can compute a flattening $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ for $(\mathbb{P}_i)_{i\leqslant t}$ of second type at level $\tilde{t}$, precision ρ, and defect $\leqslant\eta:=\eta'+\kappa_{\tilde{t}}$ using*

$$\begin{aligned}&\tilde{O}(5^{t-i_{\tilde{t}-1}}\,\mathsf{B}(d_1,\ldots,d_{i_{\tilde{t}-1}};\max(R_{i_{\tilde{t}-1}}^{-1},\rho+\eta))\min(R_{i_{\tilde{t}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{t}}^4)\\ +\;&\mathsf{I}(d_1,\ldots,d_{i_{\tilde{t}-1}};\max(R_{i_{\tilde{t}-1}}^{-1},\rho+\eta))\\ +\;&O(\mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho+\kappa_{\tilde{t}}}\leftrightarrow\tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta})\min(R_{i_{\tilde{t}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{t}})\end{aligned}$$

operations in $\mathbb{K}$.

Proof. We use Lemma 7.13 with $h = i_{\tilde{\imath}-1}$ in conjunction with Lemma 7.9 in order to compute $\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow k} = \Pi_{k-1\rightsquigarrow i_{\tilde{\imath}-1}+1}(\Phi_k)$ at precision $\rho+\eta$ for $k = i_{\tilde{\imath}-1}+1, \ldots, i_{\tilde{\imath}}$. This costs

$$\tilde{O}(5^{t-i_{\tilde{\imath}-1}}\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\eta))\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}^4).$$

We compute the pre-inverse $\Omega_{\tilde{\imath}}$ of $\Phi_{i_{\tilde{\imath}-1}+1\rightsquigarrow i_{\tilde{\imath}}}$ at relative precision $\rho+\kappa_{\tilde{\imath}}$, using

$$O(\mathsf{M}(d_1,\ldots,d_{i_{\tilde{\imath}-1}},\tilde{d}_{\tilde{\imath}};\max(R_{i_{\tilde{\imath}-1}+1}^{-1},\rho+\eta))\log\tilde{d}_{\tilde{\imath}}) + \mathsf{I}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\eta))$$

operations in $\mathbb{K}$, thanks to Proposition 3.14. By Proposition 3.11 we have

$$\begin{aligned}
&\mathsf{M}(d_1,\ldots,d_{i_{\tilde{\imath}-1}},\tilde{d}_{\tilde{\imath}};\max(R_{i_{\tilde{\imath}-1}+1}^{-1},\rho+\eta))\\
=\;& O(\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},(\rho+\eta)))\,(\min(R_{i_{\tilde{\imath}-1}}\max(R_{i_{\tilde{\imath}-1}+1}^{-1},\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}})^2)\\
=\;& O(\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},(\rho+\eta)))\min(R_{i_{\tilde{\imath}-1}}\max(R_{i_{\tilde{\imath}-1}+1}^{-1},\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}^2)\\
=\;& O(\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},(\rho+\eta)))\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}^3).
\end{aligned}$$

We deduce $\tilde{\Phi}_{\tilde{\imath}}$ and $\tilde{\Omega}_{\tilde{\imath}}$ using $O(\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}})$ evaluations of $\xi_{\tilde{\imath}-1}$ by Lemma 2.3. □

[Where is the complexity of the precomputations analyzed?]

PROPOSITION 7.15. *With the notation of Proposition 7.14, assume that the following auxiliary data are given at precision $\rho+\eta$:*

- $\xi_{\tilde{\imath}-1}(\Phi_{i_{\tilde{\imath}-1}+1}),\ldots,\xi_{\tilde{\imath}-1}(\Phi_t)$ *(here $\xi_{\tilde{\imath}-1}$ is applied coefficient-wise),*
- $\xi_{\tilde{\imath}-1}(\Psi_{i_{\tilde{\imath}-1}+1}),\ldots,\xi_{\tilde{\imath}-1}(\Psi_t)$*, where Ψ_j still denotes the pre-inverse of $\varphi_j+\Phi_{j,d_j-1}$ at precision $\rho+\kappa_{\tilde{\imath}}$.*

Then we have

$$\begin{aligned}
&\mathsf{C}(\mathbb{P}_{i_{\tilde{\imath}},<1;\rho}\leftrightarrow\tilde{\mathbb{P}}_{\tilde{\imath},<1;\rho+\eta})\\
=\;& R_t^{-1}\tilde{O}\big(3^{\tilde{\imath}}D_tR_t(\rho+\eta)\big)\,\tilde{d}_{\tilde{\imath}}^6\\
&+\mathsf{C}(\mathbb{P}_{i_{\tilde{\imath}-1},<1;\rho+\kappa_{\tilde{\imath}}}\leftrightarrow\tilde{\mathbb{P}}_{\tilde{\imath}-1,<1;\rho+\eta})\min(R_{i_{\tilde{\imath}-1}}(\rho+\kappa_{\tilde{\imath}}),1)\,\tilde{d}_{\tilde{\imath}}.
\end{aligned}$$

Proof. Let $A\in(\mathbb{P}_{i_{\tilde{\imath}}})_{<1}$ be written canonically

$$A=\sum_{k_{i_{\tilde{\imath}-1}+1}<d_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}<d_{i_{\tilde{\imath}}}} A_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}\varphi_{i_{\tilde{\imath}-1}+1}^{k_{i_{\tilde{\imath}-1}+1}}\cdots\varphi_{i_{\tilde{\imath}}}^{k_{i_{\tilde{\imath}}}}.$$

At relative precision ρ, the number of non-zero $A_{k_{i_{\tilde{\imath}-1}+1},\ldots,k_{i_{\tilde{\imath}}}}$ is

$$\leqslant\min(R_{i_{\tilde{\imath}-1}}\rho,1)\,\tilde{d}_{\tilde{\imath}}$$

by Lemma 2.3. We first convert these non-zero coefficients into $(\tilde{\mathbb{P}}_{\tilde{\imath}-1})_{<1}$ at relative precision $\rho+\eta$. For the arithmetic operations in $(\mathbb{P}_{i_{\tilde{\imath}-1}})_{<1}$ we then use the flattened representation, so Proposition 6.7 allows us to take

$$\mathsf{B}(d_1,\ldots,d_{i_{\tilde{\imath}-1}};\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\kappa_{\tilde{\imath}}))=R_{i_{\tilde{\imath}-1}}^{-1}\tilde{O}\big(3^{\tilde{\imath}}\tilde{D}_{\tilde{\imath}-1}R_{i_{\tilde{\imath}-1}}\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\eta)\big).$$

Using $2^{i_{\tilde{\imath}}-i_{\tilde{\imath}-1}}\leqslant\tilde{d}_{\tilde{\imath}}$, we have $5^{i_{\tilde{\imath}}-i_{\tilde{\imath}-1}}\leqslant\tilde{d}_{\tilde{\imath}}^3$, so the cost bound given in Lemma 7.13 becomes

$$\begin{aligned}
&R_{i_{\tilde{\imath}-1}}^{-1}\tilde{O}\big(3^{\tilde{\imath}}\tilde{D}_{\tilde{\imath}-1}R_{i_{\tilde{\imath}-1}}^{-1}\max(R_{i_{\tilde{\imath}-1}}^{-1},\rho+\eta)\min(R_{i_{\tilde{\imath}-1}}(\rho+\eta),1)\,\tilde{d}_{\tilde{\imath}}^7\big)\\
=\;& R_t^{-1}\tilde{O}\big(3^{\tilde{\imath}}\tilde{D}_{\tilde{\imath}}R_t(\rho+\eta)\big)\,\tilde{d}_{\tilde{\imath}}^6.
\end{aligned}$$

For the reverse conversion from $(\tilde{\mathbb{P}}_{\tilde{\imath}})_{<1}$ to $(\mathbb{P}_{i_{\tilde{\imath}}})_{<1}$ the complexity is the same, again by Lemma 7.13. □

8. ACCELERATED TOWER ARITHMETIC

We carry on with the notation of Definition 6.1 for flattenings and we recall that $\tilde{d}_j := d_{i_{j-1}+1} \cdots d_{i_j}$. We aim at constructing flattenings of sufficiently small height in order to obtain a fast product in the given contact tower: this will be achieved by merging consecutive levels of small degree. All contact towers in this section will be almost reduced, effectively separable, and regular.

8.1. δ-flattening

Given $\delta \leqslant D_t$, we can construct a sequence $\tilde{\imath}_k$ for $k = 0, \ldots, s$ with $\tilde{\imath}_0 = 0$, $\tilde{\imath}_0 = 1$, and

$$s \leqslant 3\frac{\log D_t}{\log \delta} + 2 \tag{8.1}$$

such that if $\tilde{\imath}_k > \tilde{\imath}_{k-1} + 1$, then $d_k < \delta$. We originally developed this construction for algebraic towers [9, section 4.2]. In this section we will refine it for contact towers. For a slice between $\tilde{\imath}_k$ and $\tilde{\imath}_{k+1} - 1$, we will construct at most four consecutive flattening steps, either trivial, or of first or second types.

We define $(i_j)_{j=0,\ldots,\tilde{t}}$ recursively from $i_0 := 0$ to $i_{\tilde{t}} = t$. We recall that the first level must be trivial, so $i_1 := 1$. For $j \geqslant 2$, assume that i_{j-1} has been defined and that $i_{j-1} = \tilde{\imath}_{k-1}$ for some $k \in \{1, \ldots, s\}$. If $\tilde{\imath}_k = \tilde{\imath}_{k-1} + 1$ then we set $i_j := \tilde{\imath}_k$ and introduce a trivial flattening step at level i_j. Otherwise, we distinguish the following cases.

Case 1. If $\epsilon_{\tilde{\imath}_{k-1}+1} = 1$, then we distinguish the following sub-cases.

- **a.** If $\epsilon_{\tilde{\imath}_{k-1}+1} = \cdots = \epsilon_{\tilde{\imath}_k - 1} = 1$, then we set $i_j := \tilde{\imath}_k$ and introduce a single flattening of second type between i_{j-1} and i_j.
- **b.** Otherwise, there exists a largest integer $i_j \leqslant \tilde{\imath}_k$ such that $\epsilon_{i_{j-1}+1} = \cdots = \epsilon_{i_j - 1} = 1$. By construction $i_j < \tilde{\imath}_k$ and $\epsilon_{i_j} = 0$, so we still use a flattening of second type between i_{j-1} and i_j, but beyond i_j, we distinguish two cases:
  - **i.** If $\epsilon_{\tilde{\imath}_k} = 0$ then we set $i_{j+1} := \tilde{\imath}_k$ and a flattening of first type is used between i_j and i_{j+1}.
  - **ii.** Otherwise, $\epsilon_{\tilde{\imath}_k} = 1$ and there exists a smallest integer $i_{j+1} \leqslant \tilde{\imath}_k$ such that $\epsilon_{i_{j+1}+1} = \cdots = \epsilon_{\tilde{\imath}_k} = 1$. Between i_j and i_{j+1} a flattening of first type is used. Between i_{j+1} and $i_{j+2} := \tilde{\imath}_k$ a flattening of second type is used.

Case 2. If $\epsilon_{\tilde{\imath}_{k-1}+1} = 0$, then we distinguish the following sub-cases.

- **a.** If $\epsilon_{\tilde{\imath}_{k-1}} = 0$, then we set i_j to the largest integer $\leqslant \tilde{\imath}_k$ such that $\epsilon_{i_j} = 0$, so we use a flattening of first type between i_{j-1} and i_j. If $i_j < \tilde{\imath}_k$ then we add another flattening of second type between i_j and $i_{j+1} := \tilde{\imath}_k$.
- **b.** Otherwise $\epsilon_{\tilde{\imath}_{k-1}} = 1$, and we set $i_j := i_{j-1} + 1 = \tilde{\imath}_{k-1} + 1$. Then we repeat the construction from case 1 at position $\tilde{\imath}_{k-1} + 1$ instead of $\tilde{\imath}_{k-1}$.

A flattening constructed in this way will be called a **δ-flattening** for the contact tower $(\mathbb{P}_i)_{i \leqslant t}$. The maximum length of a subsequence of $(i_j)_{j \leqslant \tilde{t}}$ between $\tilde{\imath}_{k-1}$ and $\tilde{\imath}_k$ is at most 4. This maximum is reached in case 2b, when the recursive construction falls in case 1bii, as illustrated below (where '$*$' stands for 0 or 1):

i	$i_{j-1} := \tilde{\imath}_{k-1}$	$i_j = i_{j-1} + 1$	$i_{j+1} := i_j + 1$	$\cdots$	$i_{j+2} - 1$	i_{j+2}	$i_{j+2} + 1$	$\cdots$	i_{j+3}	$i_{j+3} + 1$	$\cdots$	$i_{j+4} = \tilde{\imath}_{k+1}$
ϵ_i	1	0	1	$\cdots$	1	0	$*$	$*$	0	1	$\cdots$	1

LEMMA 8.1. *There exists a δ-flattening with the following properties:*

- $\tilde{t} \leqslant 12 \frac{\log D_t}{\log \delta} + 8$,
- *if $i_{j+1} > i_j + 1$ then $\tilde{d}_j \leqslant \delta$, for $j = 1, \ldots, \tilde{t}$,*
- $\operatorname{dct} \xi_j \leqslant \delta \rho j$, *for $j = 1, \ldots, \tilde{t}$.*

Proof. The existence of the flattening and the bound on $\operatorname{dct} \xi_j$ is a consequence of the above construction, Lemmas 7.1, 7.4, and 7.9. The first bound follows from (8.1) and $\tilde{t} \leqslant 4s$. □

8.2. Conversion cost

Now we assume that a δ-flattening is at our disposal and we study the cost of the conversions between $(\mathbb{P}_{i_{\tilde{i}}})_{<1}$ and $(\tilde{\mathbb{P}}_{\tilde{i}})_{<1}$. By definition of $\operatorname{dct} \xi_{\tilde{i}}$, any element A in $(\mathbb{P}_{i_{\tilde{i}}})_{<1}$ can be recovered at precision ρ from its image $\xi_{\tilde{i}}(A)$ at relative precision $\rho + \eta$ whenever $\eta \geqslant \operatorname{dct} \xi_{\tilde{i}}$.

LEMMA 8.2. *Given an almost reduced effectively separable and regular contact tower $(\mathbb{P}_i)_{i \leqslant t}$, and*

- *$\rho \in R_t^{-1} \mathbb{N}^{>0}$, $\eta \geqslant \delta \rho \tilde{t}$, a δ-flattening $(\tilde{\mathbb{P}}_j)_{j \leqslant \tilde{t}}$ of $(\mathbb{P}_i)_{i \leqslant t}$ at precision ρ,*
- *the auxiliary data of Proposition 7.3 (resp. 7.6 and 7.15), if the flattening at level j is trivial (resp. of first and second type), for $j = 1, \ldots, \tilde{t}$.*

Then we have

$$\mathsf{C}(\mathbb{P}_{i_{\tilde{i}},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t},<1;\rho+\eta}) = R_t^{-1} \tilde{O}\big(3^{\tilde{t}} D_t R_t (\rho + \eta)\, \delta^6\big).$$

Proof. If the flattening at level $\tilde{t}$ is trivial or of first type, then we set $\kappa_{\tilde{t}} := 0$. The upper bound $\eta = \delta \rho \tilde{t}$ on the defect comes from Lemma 8.1. In case of a non-trivial flattening at level $\tilde{t}$, we have $\tilde{d}_{\tilde{t}} \leqslant \delta$, and Propositions 7.6 and 7.15 yield

$$\begin{aligned}
&\mathsf{C}(\mathbb{P}_{i_{\tilde{i}},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t},<1;\rho+\eta}) \\
&= R_t^{-1} \tilde{O}\big(3^{\tilde{t}} D_t R_t (\rho + \eta)\, \tilde{d}_{\tilde{t}}^6\big) + \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho+\kappa_{\tilde{t}}} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta}) \min\big(R_{i_{\tilde{t}-1}} (\rho + \eta), 1\big)\, \tilde{d}_{\tilde{t}} \\
&= R_t^{-1} \tilde{O}\big(3^{\tilde{t}} D_t R_t (\rho + \eta)\, \delta^6\big) + \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho+\kappa_{\tilde{t}}} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta}) \min\big(R_{i_{\tilde{t}-1}} (\rho + \eta), 1\big)\, \tilde{d}_{\tilde{t}}.
\end{aligned}$$

Otherwise, in case of a trivial flattening, we have $i_{\tilde{t}} = i_{\tilde{t}-1} + 1$ and Proposition 7.3 gives

$$\mathsf{C}(\mathbb{P}_{i_{\tilde{i}},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t},<1;\rho+\eta}) = \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta}) \min\big(R_{i_{\tilde{t}-1}} \rho, 1\big)\, \tilde{d}_{\tilde{t}}.$$

It follows that

$$\begin{aligned}
&\mathsf{C}(\mathbb{P}_{i_{\tilde{i}},<1;\rho} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t},<1;\rho+\eta}) \\
&= R_t^{-1} \tilde{O}\big(3^{\tilde{t}} D_t R_t (\rho + \eta)\, \delta^6\big) + \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-1},<1;\rho+\kappa_{\tilde{t}}} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-1,<1;\rho+\eta}) \min\big(R_{i_{\tilde{t}-1}} \rho, 1\big)\, \tilde{d}_{\tilde{t}} \\
&= R_t^{-1} \tilde{O}\big(3^{\tilde{t}} D_t R_t (\rho + \eta)\, \delta^6\big) \\
&\qquad + R_{i_{\tilde{t}-1}}^{-1} \tilde{O}\big(3^{\tilde{t}-1} \tilde{D}_{\tilde{t}-1} R_{i_{\tilde{t}-1}} \max\big(R_{i_{\tilde{t}-1}}^{-1}, \rho + \eta\big)\, \delta^6\big) \min\big(R_{i_{\tilde{t}-1}} \rho, 1\big)\, \tilde{d}_{\tilde{t}} \\
&\qquad + \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-2},<1;\rho+\kappa_{\tilde{t}}+\kappa_{\tilde{t}-1}} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-2,<1;\rho+\eta}) \min\big(R_{i_{\tilde{t}-2}} \max\big(R_{i_{\tilde{t}-1}}^{-1}, \rho\big), 1\big) \min\big(R_{i_{\tilde{t}-1}} \rho, 1\big)\, \tilde{d}_{\tilde{t}-1} \tilde{d}_{\tilde{t}} \\
&= R_t^{-1} \tilde{O}\big((3^{\tilde{t}} + 3^{\tilde{t}-1})\, D_t R_t (\rho + \eta)\, \delta^6\big) \\
&\qquad + \mathsf{C}(\mathbb{P}_{i_{\tilde{t}-2},<1;\rho+\kappa_{\tilde{t}}+\kappa_{\tilde{t}-1}} \leftrightarrow \tilde{\mathbb{P}}_{\tilde{t}-2,<1;\rho+\eta}) \min\big(R_{i_{\tilde{t}-2}} \rho, 1\big)\, \tilde{d}_{\tilde{t}-1} \tilde{d}_{\tilde{t}} \qquad \text{(by Lemma 3.10)} \\
&\ \ \vdots \\
&= R_t^{-1} \tilde{O}\big(3^{\tilde{t}} \tilde{D}_{\tilde{t}} R_t (\rho + \eta)\, \delta^6\big),
\end{aligned}$$

which concludes the proof. □

8.3. Fast product and division

We still assume that a δ-flattening is at our disposal. Now we assess the cost of the multiplications and divisions in $\mathbb{P}_t$.

LEMMA 8.3. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an almost reduced effectively separable and regular contact tower. Let $1\leqslant\delta\leqslant d$, $l\in r_{t+1}\,\mathbb{N}^{>0}$, $\rho\in R_{t+1}^{-1}\,\mathbb{N}^{>0}$, and $\eta\geqslant\delta\,\rho\,\tilde{t}$. Given a δ-flattening for $(\mathbb{P}_i)_{\leqslant t}$ at precision ρ and defect $\leqslant\eta$, together with the auxiliary data needed in Lemma 8.2, we have*

$$\begin{aligned}\mathsf{B}(d_1\cdots d_t,l;\rho) &= R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big)\\ \mathsf{I}(d_1,\ldots,d_t,l;\rho) &= R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big).\end{aligned}$$

Proof. In order to multiply two elements of $(\mathbb{P}_i)_{i\leqslant t}$, we convert them into the flattened representation, multiply them, and convert them back. The number of the conversions is given by Lemma 2.2, their cost by Lemma 8.2, whereas the cost of the products is stated in Proposition 6.7, whence

$$\begin{aligned}&\mathsf{M}(d_1,\ldots,d_t,l;\rho)\\ =\;& O(\mathsf{C}(\mathbb{P}_{i_i,<1;\rho}\leftrightarrow\tilde{\mathbb{P}}_{\tilde{t},<1;\rho+\eta})\min(R_t\rho,1)\,l)+R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\big)\\ =\;& R_t^{-1}\tilde{O}\big(3^{\tilde{t}}D_tR_t\max(R_t^{-1},\rho+\eta)\,\delta^6\min(R_t\rho,1)\,l\big)+R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\big)\\ =\;& R_t^{-1}\tilde{O}\big(3^{\tilde{t}}D_tR_t\,(\rho+\eta)\,\delta^6\,l\big)+R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\big)\\ =\;& R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big).\end{aligned}$$

For computing a pre-inverse in degree l we apply Proposition 3.14 with the latter bound for M and achieve

$$R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big)+\mathsf{I}(d_1,\ldots,d_t;\max(R_t^{-1},\rho)).$$

Thanks to Proposition 3.16 we deduce

$$\mathsf{D}(d_1,\ldots,d_t,l;\rho)=R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big)+\mathsf{I}(d_1,\ldots,d_t;\max(R_t^{-1},\rho)).$$

Finally, Proposition 3.14 leads to

$$\begin{aligned}&\mathsf{I}(d_1,\ldots,d_t,l;\rho)\\ =\;& R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big)+\mathsf{I}(d_1,\ldots,d_t;\max(R_t^{-1},\rho))\\ =\;& R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big)+R_t^{-1}\tilde{O}\big(3^{\tilde{t}-1}D_tR_t\max(R_t^{-1},\rho+\eta)\,\delta^6\big)\\ &\quad+\mathsf{I}(d_1,\ldots,d_{t-1};\max(R_{t-1}^{-1},\rho))\\ =\;& R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big)+R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}-1}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big)\\ &\quad+\mathsf{I}(d_1,\ldots,d_{t-1};\max(R_{t-1}^{-1},\rho))\qquad(\text{since }\max(R_t^{-1},\rho+\eta)<r_{t+1}\,(\rho+\eta))\\ &\vdots\\ =\;& R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_t\,l\,R_{t+1}\,(\rho+\eta)\,\delta^6\big).\end{aligned}$$

□

8.4. Fast δ-flattening

It remains to compute δ-flattenings. For level j, we recursively use the preceding fast conversions, multiplications and divisions over $\tilde{\mathbb{P}}_{j-1}$. In case of a trivial flattening, or one of first type, at level j, recall that we set $\kappa_j:=0$. For the second type κ_j is defined in Lemma 7.9. Let us now show how to compute the auxiliary data for each level.

Algorithm 8.1

Input. An almost reduced effectively separable and regular contact tower $(\mathbb{P}_i)_{i\leqslant t}$ over $\mathbb{K}((z))$ at precision $\rho\in R_t^{-1}\,\mathbb{N}^{>0}$ a positive integer $\delta<d$.

Output. A δ-flattening for $(\mathbb{P}_i)_{i\leqslant t}$ at precision ρ and defect $\leqslant\delta\rho\tilde{t}$, along with the auxiliary data needed in Lemma 8.2.

Assumption. We are given $>\delta^2$ distinct elements in $\mathbb{K}$.

1. Determine the integer sequence $0=i_0<\cdots<i_{\tilde{t}}=t$ described before Lemma 8.1, along with the flattening types for each level. Let $\eta:=\delta\rho\tilde{t}$.
2. For $j=1,\ldots,\tilde{t}$ do:
   a. According to the type of the flattening at level j, use Proposition 7.2, 7.5, or 7.14 to increase the flattening for $\mathbb{P}_{i_j}$ over $\tilde{\mathbb{P}}_{j-1}$.
   b. Compute $\Psi_{i_{j-1}+1},\ldots,\Psi_{i_j}$ at precision $\rho+\kappa_j$ for a non-trival flattening. If the flattening at level j is of first or second type, then compute the auxiliary data needed in Proposition 7.6 or 7.15.
3. Return $(\tilde{\mathbb{P}}_j)_{j\leqslant\tilde{t}}$ along with the auxiliary data.

PROPOSITION 8.4. *Algorithm 8.1 is correct and performs*

$$\tilde{O}(D_t^{1+\epsilon}\,\delta^6\,\mathrm{ht}\,\gamma_t)+R_t^{-1}\,\tilde{O}\big(3^{\tilde{t}}D_tR_t\rho\,\delta^{12}\big)$$

operations in $\mathbb{K}$.

Proof. The correctness of Algorithm 8.1 is ensured by Lemmas 7.1, 7.4 and 7.9. We begin with the following technical upper bound:

$$\begin{aligned}
&R_{i_j}^{-1}\,\tilde{O}(3^j\tilde{D}_jR_{i_j}\max(R_{i_j}^{-1},\rho+\eta))\\
=\;&R_{i_j}^{-1}\,\tilde{O}(3^j\tilde{D}_jR_{i_j}R_{i_j}^{-1}R_t(\rho+\eta)) && (\text{since } \max(R_{i_j}^{-1},\rho+\eta)\leqslant R_{i_j}^{-1}R_t(\rho+\eta))\\
=\;&R_{i_j}^{-1}\,\tilde{O}(3^jD_tR_{i_j}(\rho+\eta))\\
=\;&R_t^{-1}\,\tilde{O}(3^jD_tR_t\rho\,\delta). && (8.2)
\end{aligned}$$

From Lemma 8.3 and (8.2), we obtain

$$\begin{aligned}
&\mathsf{B}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho+\eta))\\
=\;&R_{i_{j-1}}^{-1}\,\tilde{O}(3^{j-1}\tilde{D}_{j-1}R_{i_{j-1}}\max(R_{i_{j-1}}^{-1},\rho+\eta)\,\delta^6)\\
=\;&R_t^{-1}\,\tilde{O}(3^jD_tR_t\rho\,\delta^7), && (8.3)
\end{aligned}$$

and

$$\mathsf{I}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho+\eta))=R_t^{-1}\,\tilde{O}(3^jD_tR_t\rho\,\delta^7). \qquad (8.4)$$

For a trivial flattening, Proposition 7.2 gives the following cost for step 2.a:

$$\begin{aligned}
&O(\mathsf{M}(d_1,\ldots,d_{i_j};\max(R_{i_j}^{-1},\rho))\log d_{i_j})\\
&\quad+\mathsf{C}(\mathbb{P}_{i_{j-1},<1;\rho}\leftrightarrow\tilde{\mathbb{P}}_{j-1,<1;\rho+\eta})\,O(\min(R_{i_{j-1}}\max(R_{i_j}^{-1},\rho),1)\,d_{i_j})\\
&\quad+\mathsf{I}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho))\\
=\;&R_{i_j}^{-1}\,\tilde{O}(3^jD_{i_j}R_{i_j}\max(R_{i_j}^{-1},\rho+\eta)\,\delta^6) && (\text{by Lemma 8.3})\\
&\quad+R_{i_{j-1}}^{-1}\,\tilde{O}(3^j\tilde{D}_{j-1}R_{i_{j-1}}\max(R_{i_{j-1}}^{-1},\rho+\eta)\,\delta^6)\,O(\min(R_{i_{j-1}}\max(R_{i_j}^{-1},\rho),1)\,d_{i_j})\\
&&& (\text{by Lemma 8.2})\\
=\;&R_t^{-1}\,\tilde{O}(3^jD_tR_t\rho\,\delta^8). && (\text{using (8.2)})
\end{aligned}$$

For a flattening of first type, Proposition 7.5 gives the following cost for step 2.a:

$$\begin{aligned}
&\tilde{O}(D_j^{1+\epsilon}\delta^6 \mathrm{ht}\,\gamma_j)\\
&\quad + \tilde{O}(\mathsf{B}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho))\,(\min(R_{i_{j-1}}\max(R_{i_j}^{-1},\rho),1)\,\delta)^2\,\delta\,\mathrm{ht}\,\rho\log^4 D_j)\\
&\quad + O(\mathsf{C}(\mathbb{P}_{i_{j-1},<1;\rho}\leftrightarrow\tilde{\mathbb{P}}_{j-1,<1;\rho+\eta})\min(R_{i_{j-1}}\max(R_{i_j}^{-1},\rho),1)\,\delta\log D_j)\\
=\ &\tilde{O}(D_j^{1+\epsilon}\delta^6 \mathrm{ht}\,\gamma_j)\\
&\quad + R_t^{-1}\tilde{O}(3^{j-1}D_tR_t\rho\,\delta^{10}) && \text{(using (8.3))}\\
&\quad + R_t^{-1}\tilde{O}(3^{j-1}D_tR_t\rho\,\delta^{6}) && \text{(by Lemma 8.2)}\\
=\ &\tilde{O}(D_j^{1+\epsilon}\delta^6 \mathrm{ht}\,\gamma_j) + R_t^{-1}\tilde{O}(3^{j}D_tR_t\rho\,\delta^{10}).
\end{aligned}$$

For a flattening of second type, Proposition 7.14 gives the following cost for step 2.a:

$$\begin{aligned}
&\tilde{O}(5^{i_j-i_{j-1}}\mathsf{B}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho+\eta))\min(R_{i_{j-1}}\max(R_{i_j}^{-1},\rho+\eta),1)\,\delta^4)\\
&\quad + \mathsf{I}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho))\\
&\quad + O(\mathsf{C}(\mathbb{P}_{i_{j-1},<1;\rho}\leftrightarrow\tilde{\mathbb{P}}_{j-1,<1;\rho+\eta})\min(R_{i_{j-1}}\rho,1)\,\tilde{d}_j)\\
=\ &R_t^{-1}\tilde{O}(3^{j-1}D_tR_t\rho\,\delta^{11}) && \text{(using (8.3))}\\
&\quad + R_t^{-1}\tilde{O}(3^{j-1}D_tR_t\rho\,\delta^{7}) && \text{(using (8.4))}\\
&\quad + R_t^{-1}\tilde{O}(3^{j-1}D_tR_t(\rho+\eta)\,\delta^{6}) && \text{(by Lemma 8.2)}\\
=\ &R_t^{-1}\tilde{O}(3^{j-1}D_tR_t\rho\,\delta^{11}).
\end{aligned}$$

If the flattening at level j is non-trivial, then Proposition 3.11 applied to $h=i_{j-1}$ and $t=i_j$ gives the following cost bound for step 2.b:

$$\begin{aligned}
\leqslant\ &5^{i_j-i_{j-1}+1}\mathsf{B}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho+\kappa_j))\,(\min(R_{i_{j-1}}\max(R_{i_j}^{-1},\rho+\kappa_j),1)\,\delta)^2\\
&\quad + \mathsf{I}(d_1,\ldots,d_{i_{j-1}};\max(R_{i_{j-1}}^{-1},\rho+\kappa_j))\,(i_j-i_{j-1})\\
=\ &5^{i_j-i_{j-1}+1}R_t^{-1}\tilde{O}(3^{j-1}D_tR_t\rho\,\delta^{9}) && \text{(using (8.3) and (8.4))}\\
=\ &R_t^{-1}\tilde{O}(3^{j-1}D_tR_t\rho\,\delta^{12}). && \text{(using } 5^{i_j-i_{j-1}}\leqslant\delta^3\text{)}
\end{aligned}$$

The rest of step 2.b reduces to $\tilde{O}(\tilde{d}_j)=\tilde{O}(\delta)$ evaluations of ξ_{j-1}, which totalize

$$\mathsf{C}(\mathbb{P}_{i_{j-1},<1;\rho}\leftrightarrow\tilde{\mathbb{P}}_{j-1,<1;\rho+\eta})\,\tilde{O}(\delta) \;=\; R_t^{-1}\tilde{O}(3^jD_tR_t(\rho+\eta)\,\delta^6)$$

by Lemma 8.2. We conclude by summing the costs of steps 2.a and 2.b for $j=1,\ldots,\tilde{t}$, simplifying with (2.2). □

8.5. Proof of Theorem 1.4

We finally combine the preceding algorithms in order to prove our main result, first in terms of the parameter δ, and then only in terms of D_t.

THEOREM 8.5. *Let $(\mathbb{P}_i)_{i\leqslant t}$ be an almost reduced effectively separable and regular contact tower, $l\in r_{t+1}\mathbb{N}^{>0}$, and let $\delta\leqslant D_t$. For all $\rho\in R_{t+1}^{-1}\mathbb{N}^{>0}$, after precomputations (that only depend on the tower and ρ) of cost*

$$R_t^{-1}\tilde{O}\big(3^{\tilde{t}}D_tr_{t+1}R_t\rho\,\delta^{12}\big)+\tilde{O}(D_t^{1+\epsilon}\delta^6\,\mathrm{ht}\,\gamma_t),$$

the following holds:

- *Given $A\in[\mathbb{P}_{t,<l}]_{v(A;\mathbb{P}_t);\rho}$, and $B\in[\mathbb{P}_{t,<l}]_{v(B;\mathbb{P}_t);\rho}$, we can compute the truncated product $[AB;\mathbb{P}_t]_{v(A;\mathbb{P}_t)+v(B;\mathbb{P}_t);\rho}$ using*

$$R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}}D_tlR_{t+1}\rho\,\delta^6\big)$$

operations in $\mathbb{K}$.

- *Given $A \in [\mathbb{P}_{t,<2l}]_{v(A;\mathbb{P}_t);\rho}$, and $B \in [\mathbb{P}_{t,\leqslant l}]_{v(B;\mathbb{P}_t);\rho}$ monic of degree l, we can compute the truncated quotient and remainder $[A \operatorname{quo}_{\varphi_{t+1}} B; \mathbb{P}_t]_{v(A;\mathbb{P}_t)-v(B;\mathbb{P}_t);\rho}$ and $[A \operatorname{rem}_{\varphi_{t+1}} B; \mathbb{P}_t]_{v(A;\mathbb{P}_t);\rho}$ using*

$$R_{t+1}^{-1}\tilde{O}\big(3^{\tilde{t}} D_t l R_{t+1} \rho \delta^6\big)$$

operations in $\mathbb{K}$.

Proof. First we assume that we are given $>\delta^2$ distinct elements in $\mathbb{K}$. The cost for obtaining a δ-accelerated tower representation of $(\mathbb{P}_i)_{i\leqslant t}$ is given in Proposition 8.4. Then in order to multiply two elements in $(\mathbb{P}_i)_{i\leqslant t}$, we convert them into the flattening, multiply them, and convert them back. The cost of the conversions is given in Lemma 8.2, and the costs of the product and the division are stated in Propositions 6.7 and 6.8.

Finally if we are not given sufficiently many elements in $\mathbb{K}$, we appeal to [12, Proposition A.2]: the overhead only induces logarithmic factors in the complexity bound. □

Proof of Theorem 1.4. It is important to notice that constants hidden in the "O" of Theorem 8.5 are independent of the value for δ, so we may freely choose δ in terms of D_t. From Lemma 8.1 we know that

$$\tilde{t} \leqslant 12\frac{\log D_t}{\log \delta} + 8$$

In order to balance the contributions of $3^{\tilde{t}}$ and δ^6 in the complexity bound of Theorem 8.5, we take δ [hmm, recall that δ was assumed to be an integer in [9]] such that

$$6\log\delta = \left(12\frac{\log D_t}{\log\delta} + 8\right)\log 3,$$

so $\tilde{t} = O(\log^{1/2} D_t)$, $\frac{\log\delta}{\log D_t} = O\left(\frac{1}{\log^{1/2} D_t}\right)$, and $\delta = D_t^{o(1)}$. □

[In the references, it should be Mac Lane.]

BIBLIOGRAPHY

[1] S. S. Abhyankar and T. Moh. Newton–Puiseux expansion and generalized Tschirnhausen transformation. I. *J. Reine Angew. Math.*, 260:47–83, 1973.

[2] S. S. Abhyankar and T. Moh. Newton–Puiseux expansion and generalized Tschrinhausen transformation. II. *J. Reine Angew. Math.*, 261:29–54, 1973.

[3] M. Alberich-Carramiñana, J. Guàrdia, E. Nart, A. Poteaux, J. Roé, and M. Weimann. Polynomial factorization over Henselian fields. *Found. Comput. Math.*, 25:631–681, 2025.

[4] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 3rd edition, 2013.

[5] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[6] J. van der Hoeven. *The Jolly Writer. Your Guide to GNU TeXmacs*. Scypress, 2020.

[7] J. van der Hoeven. On the complexity of symbolic computation. In A. Hashemi, editor, *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22, pages 3–12. New York, NY, USA, 2022. ACM.

[8] J. van der Hoeven and G. Lecerf. On the bit-complexity of sparse polynomial multiplication. *J. Symbolic Comput.*, 50:227–254, 2013.

[9] J. van der Hoeven and G. Lecerf. Accelerated tower arithmetic. *J. Complexity*, 55:101402, 2019.

[10] J. van der Hoeven and G. Lecerf. Directed evaluation. *J. Complexity*, 60:101498, 2020.

[11] J. van der Hoeven and G. Lecerf. Approximate contact factorization of germs of plane curves. Technical Report, HAL, 2022. https://hal.archives-ouvertes.fr/hal-03745581.
[12] J. van der Hoeven and G. Lecerf. Faster multi-point evaluation over any field. Technical Report, HAL, 2024. https://hal.science/hal-04774026.
[13] R. Lebreton. Relaxed Hensel lifting of triangular sets. *J. Symbolic Comput.*, 68(2):230–258, 2015.
[14] G. Lecerf. On the complexity of the Lickteig–Roy subresultant algorithm. *J. Symbolic Comput.*, 92:243–268, 2019.
[15] S. MacLane. A construction for absolute values in polynomial rings. *Trans. Am. Math. Soc.*, 40(3):363–395, 1936.
[16] I. Newton. *De methodis serierum et Fluxionum*. Manuscript, 1671.
[17] A. Perret du Cray. *Algorithmes pour les polynômes creux : interpolation, arithmétique, test d'identité*. PhD thesis, Université de Montpellier (France), 2023.
[18] A. Poteaux and M. Weimann. Computing Puiseux series: a fast divide and conquer algorithm. *Ann. Henri Lebesgue*, 5:1061–1102, 2021.
[19] A. Poteaux and M. Weimann. A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$. *Comput. Complex.*, 31:6, 2022.
[20] 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.
[21] M. V. Puiseux. Recherches sur les fonctions algébriques. *J. Math. Pures et Appliquées*, 15:365–480, 1850.
[22] S. J. Berkowitz . On computing the determinant in small parallel time using a small number of processors. *Inform. Process. Lett.*, 18:147–150, 1984.