Contemporary Mathematics

# Genetics of polynomials over local fields

Jordi Guàrdia and Enric Nart

Abstract. Let $(K, v)$ be a discrete valued field with valuation ring $\mathcal{O}$, and let $\mathcal{O}_v$ be the completion of $\mathcal{O}$ with respect to the $v$-adic topology. In this paper we discuss the advantages of manipulating polynomials in $\mathcal{O}_v[x]$ on a computer by means of OM representations of prime (monic and irreducible) polynomials. An OM representation supports discrete data characterizing the Okutsu equivalence class of the prime polynomial. These discrete parameters are a kind of DNA sequence common to all individuals in the same Okutsu class, and they contain relevant arithmetic information about the polynomial and the extension of $K_v$ that it determines.

## Introduction

Polynomials with $p$-adic coefficients arose in a purely algebraic context with Hensel's reinterpretation of the ideas of Kummer and Dedekind about factorization of algebraic integers. The prime polynomials in $\mathbb{Z}_p[x]$, whose roots in $\overline{\mathbb{Q}}_p$ are algebraic over $\mathbb{Q}$, parameterize prime ideals dividing the prime number $p$ in maximal orders of number fields.

More generally, let $A$ be a Dedekind domain with field of fractions $K$, let $f \in A[x]$ be a monic irreducible separable polynomial of degree $n$ and let $L = K[x]/(f)$ be the finite extension of $K$ determined by $f$. The prime ideals of the integral closure of $A$ in $L$ dividing a given prime ideal $\mathfrak{p}$ in $A$ are in 1-1 correspondence with the prime factors of $f$ in $\hat{A}_{\mathfrak{p}}[x]$, where $\hat{A}_{\mathfrak{p}}$ is the completion of $A$ with respect to the $\mathfrak{p}$-adic topology. This leads to a wide scope of arithmetic problems where prime polynomials over local fields play a significant role. For instance, the analysis of the ramification of a finite separable morphism between two algebraic curves is one of such problems.

In this paper, we deal with an arbitrary discrete valued field $(K, v)$ with valuation ring $\mathcal{O}$. Let $K_v$ be the completion of $K$ at $v$ and denote by $\mathcal{O}_v \subset K_v$ the valuation ring of $K_v$. Given a monic square-free polynomial $f \in \mathcal{O}[x]$, we are interested in the computation of the prime factors of $f$ in $\mathcal{O}_v[x]$.

---

2010 *Mathematics Subject Classification.* Primary 11Y40; Secondary 11Y05, 11R04, 11R27.
*Key words and phrases.* genomic tree, local field, Montes algorithm, Newton polygon, Okutsu equivalence, OM factorization, OM representation, type, valuation.
Partially supported by MTM2012-34611 from the Spanish MEC.

From a computational perspective, polynomials in $\mathcal{O}_v[x]$ are approximated by polynomials in $\mathcal{O}[x]$, following closely the paradigm of polynomials with real coefficients. However, prime polynomials in $\mathcal{O}_v[x]$ are much richer objects because they have an algebraic substrate containing relevant arithmetic information. This substrate is described by a sequence of discrete parameters, which are a kind of DNA sequence common to all prime polynomials which are sufficiently close one to each other. Thanks to their discrete nature, these genetic data admit an exact computation.

The aim of this paper is to give a precise description of this genetic information, and to explain how it may be computed. To this end, we present under a new framework our previous work on computational tools for $v$-adic factorization, in collaboration with other authors.

Consider the simplest extension of $v$ to a valuation $\mu_0$ on $K_v(x)$; that is, $\mu_0$ acts on polynomials as

$$\mu_0\left(a_0 + a_1x + \cdots + a_tx^t\right) = \operatorname{Min}\left\{v(a_0), \dots, v(a_t)\right\}.$$

Let $F \in \mathcal{O}_v[x]$ be a prime polynomial and $\theta \in \overline{K}_v$ one of its roots. The valuation $v$ admits a unique extension to $\overline{K}_v$ and we may consider the pseudo-valuation $\mu_{\infty,F}$ on $K_v[x]$ defined as $\mu_{\infty,F}(g) = v(g(\theta))$ for any $g \in K_v[x]$.

The *precision* of an approximation $\phi$ to $F$ is typically measured as $\mu_0(F - \phi)$, the distance with respect to the valuation $\mu_0$. A much finer measure of the distance between $\phi$ and $F$ is given by the rational number $\mu_{\infty,F}(F - \phi) = v(\phi(\theta))$, which we call the *quality* of the approximation.

In a pioneering paper, MacLane described an inductive structure on the set of all discrete valuations on $K(x)$ extending $v$ [**11, 12**]. He expressed the pseudo-valuation $\mu_{\infty,F}$ as a limit of such valuations and showed that in this approximation process there is a finite chain of valuations:

$$\mu_0 < \mu_1 < \cdots < \mu_r < \mu_{\infty,F}$$

intrinsically attached to $F$. Let us denote $\mu_F := \mu_r$. Most of the genetic information of $F$ is provided by certain invariants and operators attached to these valuations $\mu_0, \dots, \mu_r$. These genetic data provide a closed formula for the quality of an approximation to $F$ in $\mathcal{O}[x]$ (cf. equation (4.2)), and they yield a procedure to construct approximations with a prescribed quality (cf. section 6.1).

In 2007, Vaquié reviewed and generalized MacLane's work to arbitrary valued fields $(K, v)$ which are not necessarily discrete [**17, 18, 19**]. The use of the graded algebra $\mathcal{G}r(\mu)$ attached to a valuation $\mu$ on $K(x)$ led Vaquié to a more elegant presentation of the theory. A key role is played by the *residual ideals* in the degree-zero subring $\Delta(\mu)$ of $\mathcal{G}r(\mu)$. The residual ideal of a polynomial $g \in K[x]$ is defined as $\mathcal{R}_\mu(g) = H_\mu(g)\mathcal{G}r(\mu) \cap \Delta(\mu)$, where $\mathrm{H}_\mu(g)$ is the image of $g$ in the piece of degree $\mu(g)$ of the algebra.

In a recent paper [**3**], this approach of Vaquié was extended with a constructive treatment of the theory in the discrete case. On the set $\mathbb{P}$ of all prime polynomials in $\mathcal{O}_v[x]$, the following equivalence relation is considered in [**4**]: two prime polynomials $F, G \in \mathbb{P}$ of the same degree are *Okutsu equivalent*, and we write $F \approx G$, if the quality of $G$ as an approximation to $F$ is greater than certain *Okutsu bound* $\delta_0(F)$. The main result of [**3**] establishes a canonical bijection between the quotient set $\mathbb{P}/\approx$ and the *MacLane space* $\mathbb{M}$, defined as the set of all pairs $(\mu, \mathcal{L})$, where $\mu$

is an inductive valuation on $K(x)$ and $\mathcal{L}$ is a *strong* maximal ideal of $\Delta(\mu)$. The bijection sends the class of $F$ to the pair $(\mu_F, \mathcal{R}_{\mu_F}(F))$.

The point $(\mu, \mathcal{L})$ of the MacLane space which corresponds to the Okutsu class of a prime polynomal $F \in \mathbb{P}$ is, by definition, the *genetic code* of $F$. Thus, two prime polynomials have the same genetic code if and only if they are Okutsu equivalent.

Let us now be more precise about the contents of this paper, which is a natural continuation of [**3**]. In order to make the paper as self-contained as possible, we sketch in sections 1 and 2 the results of [**3**]; in this way, we collect all technical definitions and results which will be needed in the rest of the paper. In sections 3 and 4 we discuss *types* and *OM representations* as the computational objects which are able to support the genetic data of polynomials. The initials OM stand for Ore-MacLane or Okutsu-Montes indistinctly. We parameterize the MacLane space $\mathbb{M}$ by certain set $\mathbb{T}$ of equivalence classes of types and we introduce the *genomic tree* of a square-free polynomial $f \in \mathcal{O}[x]$ as a discrete object gathering the genetic information of all prime factors of $f$. In section 5 we present an adapted version of the Montes algorithm, aiming at the computation of the genomic tree of $f$, together with an approximation to each prime factor by an Okutsu equivalent polynomial in $\mathcal{O}[x]$. The knowledge of the genetic code of a prime polynomial facilitates the resolution of many computational tasks concerning this polynomial. Section 6 is devoted to the discussion of these algorithmic applications.

Suppose that $f \in \mathcal{O}[x]$ is monic irreducible and separable, and let $L$ be the finite extension of $K$ determined by $f$. It is well known that the computation of sufficiently good approximations to the prime factors of $f$ in $\mathcal{O}_v[x]$ leads to the design of routines for the computation of the integral closure of $\mathcal{O}$ in $L$, the $v$-part of the discriminant of $L/K$, and the resolution of similar arithmetic tasks concerning the extension $L/K$. Thus, the use of the Montes algorithm as a fast method to compute approximate $v$-adic factorizations leads to an improvement of many classical arithmetic algorithms. But this is not the spirit of the routines of section 6. Each of these routines addresses a concrete arithmetic problem by finding a tight link between the problem and the genetics of certain prime polynomials. This leads to an original design for the routine and to a much better practical performance.

The concept of a type and the Montes algorithm were introduced in [**13**] for $v$ a discrete valuation on a global field $K$. These results were reviewed in [**5, 6**] and their computational implications were developed in a series of papers [**2, 7, 8, 9, 14**]. The derivation of these tools from the modern presentation of MacLane's valuations in the spirit of Vaquié, leads to a more elegant treatment of the subject and to its generalization to arbitrary discrete valued fields $(K, v)$.

## 1. MacLane valuations

Let $K$ be a field equipped with a discrete valuation $v\colon K^* \to \mathbb{Z}$, normalized so that $v(K^*) = \mathbb{Z}$. Let $\mathcal{O}$ be the valuation ring of $K$, $\mathfrak{m}$ the maximal ideal, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$ and $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ the residue class field.

Let $K_v$ be the completion of $K$ and denote still by $v\colon \overline{K}_v^* \to \mathbb{Q}$ the canonical extension of $v$ to a fixed algebraic closure of $K_v$. Let $\mathcal{O}_v$ be the valuation ring of $K_v$, $\mathfrak{m}_v$ its maximal ideal and $\mathbb{F}_v = \mathcal{O}_v/\mathfrak{m}_v$ the residue class field. We consider the canonical isomorphism $\mathbb{F} \simeq \mathbb{F}_v$ as an identity and we indicate simply with a bar, $\overline{\phantom{x}}\colon \mathcal{O}_v[x] \longrightarrow \mathbb{F}[x]$, the homomorphism of reduction of polynomials modulo $\mathfrak{m}_v$.

Let $\mathbb{V}$ be the set of discrete valuations, $\mu\colon K(x)^* \to \mathbb{Q}$, such that $\mu_{|K} = v$ and $\mu(x) \ge 0$. From now on, the elements of $\mathbb{V}$ will be simply called *valuations*.

For any valuation $\mu \in \mathbb{V}$, we denote

- $\Gamma(\mu) = \mu\left(K(x)^*\right) \subset \mathbb{Q}$, the cyclic group of finite values of $\mu$.
- $e(\mu) > 0$, the ramification index of $\mu$, determined by $\Gamma(\mu) = e(\mu)^{-1}\mathbb{Z}$.

In the set $\mathbb{V}$ there is a natural partial ordering:

$$\mu \le \mu' \quad \text{ if } \quad \mu(g) \le \mu'(g),\ \forall\, g \in K[x].$$

We denote by $\mu_0 \in \mathbb{V}$ the valuation which acts on polynomials as

$$\mu_0\left(a_0 + a_1x + \cdots + a_tx^t\right) = \operatorname{Min}_{0\le s\le t}\left\{v(a_s)\right\}.$$

Clearly, $\mu_0 \le \mu$ for all $\mu \in \mathbb{V}$; in other words, $\mu_0$ is the minimum element in $\mathbb{V}$.

In this section we describe a certain subset $\mathbb{V}^{\mathrm{ind}} \subset \mathbb{V}$ introduced by MacLane [**11**], formed by the so-called *inductive valuations*. The modern presentation of this topic in the language of graded algebras is due to Vaquié [**17**]. We follow the development of [**3**] which included a constructive treatment of the subject.

**1.1. Key polynomials and augmented valuations.** Let $\mu \in \mathbb{V}$ be a valuation. For any $\alpha \in \Gamma(\mu)$ we consider the following $\mathcal{O}$-submodules in $K[x]$:

$$\mathcal{P}_\alpha = \mathcal{P}_\alpha(\mu) = \{g \in K[x] \mid \mu(g) \ge \alpha\} \supset \mathcal{P}_\alpha^+ = \mathcal{P}_\alpha^+(\mu) = \{g \in K[x] \mid \mu(g) > \alpha\}.$$

The *graded algebra of* $\mu$ is the integral domain:

$$\mathcal{G}r(\mu) := \bigoplus\nolimits_{\alpha\in\Gamma(\mu)} \mathcal{P}_\alpha/\mathcal{P}_\alpha^+.$$

Let $\Delta(\mu) = \mathcal{P}_0/\mathcal{P}_0^+$ be the piece of degree zero of this algebra. Clearly, $\mathcal{O} \subset \mathcal{P}_0$ and $\mathfrak{m} = \mathcal{P}_0^+ \cap \mathcal{O}$; thus, there is a canonical homomorphism $\mathbb{F} \to \Delta(\mu)$ equipping $\Delta(\mu)$ (and $\mathcal{G}r(\mu)$) with a canonical structure of $\mathbb{F}$-algebra.

There is a natural map $\mathrm{H}_\mu\colon K[x] \longrightarrow \mathcal{G}r(\mu)$, given by $\mathrm{H}_\mu(0) = 0$, and

$$\mathrm{H}_\mu(g) = g + \mathcal{P}^+_{\mu(g)} \in \mathcal{P}_{\mu(g)}/\mathcal{P}^+_{\mu(g)}, \ \text{ for } g \ne 0.$$

This map does not respect addition but it is multiplicative: $\mathrm{H}_\mu(gh) = \mathrm{H}_\mu(g)\,\mathrm{H}_\mu(h)$ for all $g, h \in K[x]$.

If $\mu \le \mu'$, then a canonical homomorphism of graded algebras $\mathcal{G}r(\mu) \to \mathcal{G}r(\mu')$ is determined by $g + \mathcal{P}_\alpha^+(\mu) \mapsto g + \mathcal{P}_\alpha^+(\mu')$ for all $g, \alpha$. Clearly, $\mathrm{H}_\mu(g)$ belongs to $\operatorname{Ker}(\mathcal{G}r(\mu) \to \mathcal{G}r(\mu'))$ if and only if $\mu(g) < \mu'(g)$.

Definition 1.1. Let $g, h, \phi \in K[x]$. We say that:
$g, h$ are *$\mu$-equivalent*, and we write $g \sim_\mu h$, if $\mathrm{H}_\mu(g) = \mathrm{H}_\mu(h)$.
$g$ is *$\mu$-divisible* by $h$, and we write $h \mid_\mu g$, if $\mathrm{H}_\mu(h) \mid \mathrm{H}_\mu(g)$ in $\mathcal{G}r(\mu)$.
$\phi$ is *$\mu$-irreducible* if $\mathrm{H}_\mu(\phi)\mathcal{G}r(\mu)$ is a non-zero prime ideal.
$\phi$ is *$\mu$-minimal* if $\deg\phi > 0$ and $\phi \nmid_\mu g$ for any non-zero $g$ with $\deg g < \deg\phi$.

A *key polynomial* for $\mu$ is a monic polynomial $\phi \in K[x]$ which is $\mu$-minimal and $\mu$-irreducible. We denote by $\mathrm{KP}(\mu)$ the set of all key polynomials for $\mu$.

For instance, $\mathrm{KP}(\mu_0)$ is the set of all monic polynomials $g \in \mathcal{O}[x]$ such that $\overline{g}$ is irreducible in $\mathbb{F}[x]$.

Lemma 1.2. *Every $\phi \in \mathrm{KP}(\mu)$ is irreducible in $K_v[x]$ and it belongs to $\mathcal{O}[x]$.*

Take $\phi \in \mathrm{KP}(\mu)$ and $\nu \in \mathbb{Q}_{>0}$. The *augmented valuation* of $\mu$ with respect to these data is the valuation $\mu'$ determined by the following action on $K[x]$:

$$\mu'(g) = \mathrm{Min}_{0\le s}\{\mu(a_s\phi^s) + s\nu\},$$

where $g = \sum_{0\le s} a_s\phi^s$ is the canonical $\phi$-expansion of $g$. We denote $\mu' = [\mu; \phi, \nu]$.

PROPOSITION 1.3.

(1) *The natural extension of $\mu'$ to $K(x)$ is a valuation on this field and $\mu \le \mu'$.*
(2) $\mathrm{Ker}\,(\mathcal{G}r(\mu) \to \mathcal{G}r(\mu')) = \mathrm{H}_\mu(\phi)\,\mathcal{G}r(\mu)$.
(3) *$\phi$ is a key polynomial for $\mu'$ too.*

Denote $\Delta = \Delta(\mu)$, and let $I(\Delta)$ be the set of ideals in $\Delta$. Consider the following *residual ideal operator*, which translates questions about $K[x]$ and $\mu$ into ideal-theoretic considerations in the ring $\Delta$:

$$\mathcal{R} = \mathcal{R}_\mu\colon K[x] \longrightarrow I(\Delta), \qquad g \mapsto \Delta \cap \mathrm{H}_\mu(g)\mathcal{G}r(\mu).$$

Let $\phi$ be a key polynomial for $\mu$. Choose a root $\theta \in \overline{K}_v$ of $\phi$ and denote $K_\phi = K_v(\theta)$ the finite extension of $K_v$ generated by $\theta$. Also, let $\mathcal{O}_\phi \subset K_\phi$ be the valuation ring of $K_\phi$, $\mathfrak{m}_\phi$ the maximal ideal and $\mathbb{F}_\phi = \mathcal{O}_\phi/\mathfrak{m}_\phi$ the residue class field.

PROPOSITION 1.4. *If $\phi$ is a key polynomial for $\mu$, then*

(1) $\mathcal{R}(\phi) = \mathrm{Ker}(\Delta \twoheadrightarrow \mathbb{F}_\phi)$ *for the onto homomorphism $\Delta \to \mathbb{F}_\phi$ determined by $g + \mathcal{P}_0^+ \mapsto g(\theta) + \mathfrak{m}_\phi$. In particular, $\mathcal{R}(\phi)$ is a maximal ideal of $\Delta$.*
(2) $\mathcal{R}(\phi) = \mathrm{Ker}(\Delta \to \Delta(\mu'))$ *for any augmented valuation $\mu' = [\mu; \phi, \nu]$. Thus, the image of $\Delta \to \Delta(\mu')$ is a field canonically isomorphic to $\mathbb{F}_\phi$.*

**1.2. Newton polygons.** The choice of a key polynomial $\phi$ for a valuation $\mu$ determines a *Newton polygon operator*

$$N_{\mu,\phi}\colon K[x] \longrightarrow 2^{\mathbb{R}^2},$$

where $2^{\mathbb{R}^2}$ is the set of subsets of the euclidean plane $\mathbb{R}^2$. The Newton polygon of the zero polynomial is the empty set. If $g = \sum_{0\le s} a_s\phi^s$ is the canonical $\phi$-expansion of a non-zero polynomial $g \in K[x]$, then $N_{\mu,\phi}(g)$ is the lower convex hull of the cloud of points $(s, \mu(a_s\phi^s))$ for all $0 \le s$. Figure 1 shows the typical shape of $N_{\mu,\phi}(g)$.

If the Newton polygon $N = N_{\mu,\phi}(g)$ is not a single point, we formally write $N = S_1 + \cdots + S_k$, where $S_i$ are the sides of $N$, ordered by their increasing slopes. The left and right end points of $N$ and the points joining two sides of different slopes are called the *vertices* of $N$.

Usually, we shall be interested only in the *principal Newton polygon* $N^-_{\mu,\phi}(g)$ formed by the sides of negative slope. If there are no sides of negative slope, then $N^-_{\mu,\phi}(g)$ is the left end point of $N_{\mu,\phi}(g)$.

The *length* $\ell(N)$ of a Newton polygon $N$ is the abscissa of its right end point.

LEMMA 1.5. *For every non-zero polynomial $g \in K[x]$, we have*

$$\ell(N^-_{\mu,\phi}(g)) = \mathrm{ord}_{\mu,\phi}(g),$$

*where* $\mathrm{ord}_{\mu,\phi}(g)$ *denotes the largest integer $s$ such that $\phi^s \mid_\mu g$.*

Let $\nu$ be a positive rational number and let $L_{-\nu}$ be the line of slope $-\nu$ which first touches the polygon $N_{\mu,\phi}(g)$ from below.

We define the *$\nu$-component* of $N = N_{\mu,\phi}(g)$ as the segment

$$S_\nu(g) := \{(x, y) \in N \mid y + \nu x \text{ is minimal}\} = N \cap L_{-\nu},$$

Figure 1. Newton polygon of a polynomial $g\in K[x]$

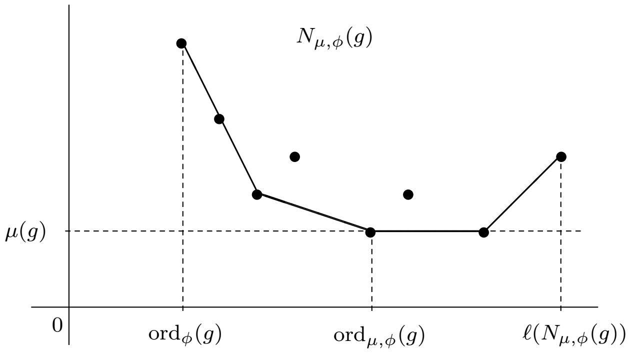
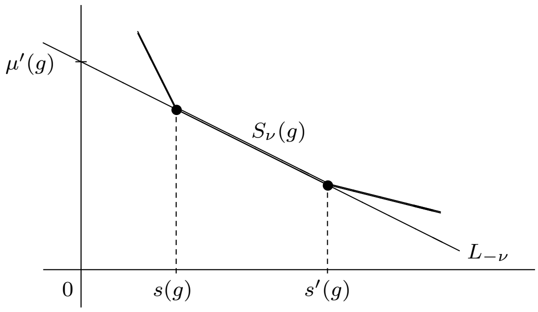



Figure 2. $\nu$-component of $N_{\mu,\phi}(g)$




and we denote by $s(g)\le s'(g)$ the abscissas of the end points of $S_\nu(g)$, where $\mu'=[\mu;\phi,\nu]$. If $N$ has a side $S$ of slope $-\nu$, then $S_\nu(g)=S$; otherwise, $S_\nu(g)$ is a vertex of $N$ and $s(g)=s'(g)$ (see Figure 2).

The next result facilitates the computation of the value $\mu'(g)$ from the Newton polygon $N_{\mu,\phi}(g)$.

Lemma 1.6. *With the above notation, the line $L_{-\nu}$ cuts the vertical axis at the point $(0,\mu'(g))$. Also, $s(g)=\operatorname{ord}_{\mu',\phi}(g)$.*

**1.3. Inductive valuations.** A valuation $\mu\in\mathbb{V}$ is called *inductive* if it is attained after a finite number of augmentation steps starting with $\mu_0$.

$$\mu_0 \xrightarrow{\ \phi_1,\nu_1\ } \mu_1 \xrightarrow{\ \phi_2,\nu_2\ } \cdots \xrightarrow{\ \phi_{r-1},\nu_{r-1}\ } \mu_{r-1} \xrightarrow{\ \phi_r,\nu_r\ } \mu_r=\mu. \tag{1.1}$$

We denote by $\mathbb{V}^{\mathrm{ind}}\subset\mathbb{V}$ the subset of all inductive valuations.

A chain of augmented valuations as in (1.1) is called a *MacLane chain of length* $r$ of $\mu$ if $\phi_{i+1}\not\sim_{\mu_i}\phi_i$ for all $1\le i<r$.

We say that (1.1) is an *optimal MacLane chain* of $\mu$ if $\deg\phi_1<\cdots<\deg\phi_r$.

An optimal MacLane chain is in particular a MacLane chain and every inductive valuation admits optimal MacLane chains [**3**, Sec. 3.1].

In every chain of augmented valuations we have

$$\deg\phi_1\mid\deg\phi_2\mid\cdots\mid\deg\phi_{r-1}\mid\deg\phi_r.$$

In a MacLane chain, we have moreover

$$\mathbb{Z}=\Gamma(\mu_0)\subset\Gamma(\mu_1)\subset\cdots\subset\Gamma(\mu_{r-1})\subset\Gamma(\mu_r)=\Gamma(\mu).$$

PROPOSITION 1.7. *Suppose the inductive valuation $\mu$ admits an optimal MacLane chain as in (1.1). Consider another optimal MacLane chain*

$$\mu_0 \xrightarrow{\phi_1',\nu_1'} \mu_1' \xrightarrow{\phi_2',\nu_2'} \cdots \xrightarrow{\phi_{r'-1}',\nu_{r'-1}} \mu_{r'-1}' \xrightarrow{\phi_{r'}',\nu_{r'}'} \mu_{r'}'=\mu'.$$

*Then, $\mu=\mu'$ if and only if $r=r'$ and:*

$$\deg\phi_i=\deg\phi_i',\quad \mu_i(\phi_i)=\mu_i(\phi_i'),\quad \nu_i=\nu_i',\quad \textit{for all }\ 1\le i\le r.$$

*In this case, we also have $\mu_i=\mu_i'$ and $\phi_i\sim_{\mu_{i-1}}\phi_i'$ for all $1\le i\le r$.*

Therefore, in any optimal MacLane chain of $\mu$, the intermediate valuations $\mu_1,\dots,\mu_{r-1}$, the positive rational numbers $\nu_1,\dots,\nu_r$, and the degrees of the key polynomials $\deg\phi_1,\dots,\deg\phi_r$ are intrinsic data of $\mu$, whereas the key polynomials $\phi_1,\dots,\phi_r$ admit different choices.

The *MacLane depth* of an inductive valuation $\mu$ is the length of any optimal MacLane chain of $\mu$.

A MacLane chain of $\mu$ determines an extension of $\mu$ to a valuation on $K_v(x)$. In fact, $\mu_0$ admits an obvious extension, and we may trivially extend to polynomials in $K_v[x]$ the definition of the successive augmentations.

PROPOSITION 1.8. *The restriction map $\mathbb{V}^{\mathrm{ind}}(K_v)\to\mathbb{V}^{\mathrm{ind}}(K)$ is bijective. The inverse map $\mathbb{V}^{\mathrm{ind}}(K)\to\mathbb{V}^{\mathrm{ind}}(K_v)$ sends an inductive valuation $\mu$ on $K(x)$ to the valuation on $K_v(x)$ determined by a MacLane chain of $\mu$.*

**1.4. Data and operators attached to a MacLane chain.** Consider an inductive valuation $\mu$ equipped with a Maclane chain of length $r$ as in (1.1). We may attach to this chain several data and operators.

Let us denote

$$\Gamma_i=\Gamma(\mu_i)=e(\mu_i)^{-1}\mathbb{Z},\quad \Delta_i=\Delta(\mu_i),\qquad 0\le i\le r.$$

$$\mathbb{F}_0:=\operatorname{Im}(\mathbb{F}\to\Delta_0);\quad \mathbb{F}_i:=\operatorname{Im}(\Delta_{i-1}\to\Delta_i),\quad 1\le i\le r.$$

By Proposition 1.4, $\mathbb{F}_i$ is a field canonically isomorphic to the residue class field $\mathbb{F}_{\phi_i}$ of the extension of $K_v$ determined by $\phi_i$; in particular, $\mathbb{F}_i$ is a finite extension of $\mathbb{F}$. We abuse of language and we identify $\mathbb{F}$ with $\mathbb{F}_0$ and each field $\mathbb{F}_i\subset\Delta_i$ with its image under the canonical map $\Delta_i\to\Delta_j$ for $j\ge i$. In other words, we consider as inclusions the canonical embeddings

$$\mathbb{F}=\mathbb{F}_0\subset\mathbb{F}_1\subset\cdots\subset\mathbb{F}_r.$$

Let us normalize the valuations $\mu_0,\dots,\mu_r$ by defining $v_i:=e(\mu_i)\mu_i$ for all $0\le i\le r$, so that $v_0,\dots,v_r$ have group of values equal to $\mathbb{Z}$.

Take $e_0=m_0=1$ and $\nu_0=\lambda_0=h_0=w_0=V_0=0$. For all $1\le i\le r$, we consider the following numerical data:

$$\begin{array}{lll}
m_i:=\deg\phi_i, & e_i:=e(\mu_i)/e(\mu_{i-1}), & f_{i-1}:=[\mathbb{F}_i\colon\mathbb{F}_{i-1}],\\
h_i:=e(\mu_i)\nu_i, & \lambda_i:=e(\mu_{i-1})\nu_i=h_i/e_i, & \\
w_i:=\mu_{i-1}(\phi_i), & V_i:=e(\mu_{i-1})w_i=v_{i-1}(\phi_i), &
\end{array}$$

It is easy to show that $\gcd(h_i, e_i) = 1$. All these data may be expressed in terms of the positive integers

$$e_0, \dots, e_r,\ f_0, \dots, f_{r-1},\ h_1, \dots, h_r. \tag{1.2}$$

For instance, for all $1 \le i \le r$ we have:

$$\begin{aligned}
&e(\phi_i) = e(\mu_{i-1}) = e_0 \cdots e_{i-1},\\
&f(\phi_i) = [\mathbb{F}_i \colon \mathbb{F}_0] = f_0 \cdots f_{i-1},\\
&\nu_i = h_i/e_1 \cdots e_i,\\
&m_i = e_{i-1}f_{i-1}m_{i-1} = (e_0 \cdots e_{i-1})(f_0 \cdots f_{i-1}),\\
&w_i = e_{i-1}f_{i-1}(w_{i-1} + \nu_{i-1}) = m_i \textstyle\sum_{1\le j<i} \nu_j/m_j,
\end{aligned}$$

Here, $e(\phi_i)$ and $f(\phi_i)$ are the ramification index and residual degree of the extension $K_{\phi_i}/K_v$, respectively. The recurrence satisfied by $m_i$, $w_i$ allows us to consider new data

$$m_{r+1} := e_r f_r m_r,\ w_{r+1} := e_r f_r (w_r + \nu_r),\ V_{r+1} := e(\mu_r) w_{r+1} = e_r f_r (e_r V_r + h_r).$$

If the MacLane chain is optimal, all these rational numbers are intrinsic data of $\mu$ by Proposition 1.7. In this case, we refer to them as $e_i(\mu)$, $f_i(\mu)$, $h_i(\mu)$, $\lambda_i(\mu)$, $\nu_i(\mu)$, $m_i(\mu)$, $w_i(\mu)$, $V_i(\mu)$, and the positive integers in (1.2) are called the *basic MacLane invariants* of $\mu$.

We consider as well some rational functions in $K(x)$ defined in a recursive way. For every $0 \le i \le r$, consider integers $\ell_i, \ell_i'$ uniquely determined by

$$\ell_i h_i + \ell_i' e_i = 1, \qquad 0 \le \ell_i < e_i. \tag{1.3}$$

Take $\pi_0 = \pi_1 = \pi$, $\Phi_0 = \phi_0 = \gamma_0 = x$, and define

$$\Phi_i = \phi_i\,(\pi_i)^{-V_i}, \quad \gamma_i = (\Phi_i)^{e_i}(\pi_i)^{-h_i}, \quad \pi_{i+1} = (\Phi_i)^{\ell_i}(\pi_i)^{\ell_i'}, \quad 1 \le i \le r. \tag{1.4}$$

It is easy to check by induction that

$$\mu_i(\pi_i) = 1/e(\mu_{i-1}), \quad \mu_i(\Phi_i) = \nu_i, \quad \mu_i(\gamma_i) = 0.$$

All polynomial factors dividing $\pi_i$, and those dividing $\Phi_i$ with a negative exponent lead to units in the graded algebra of $\mu$. Hence, it makes sense to define, for all $0 \le i \le r$:

$$x_i := H_{\mu_i}(\Phi_i) \in \mathcal{G}r(\mu_i),\ \ p_i := H_{\mu_i}(\pi_i) \in \mathcal{G}r(\mu_i)^*,\ \ y_i := H_{\mu_i}(\gamma_i) = x_i^{e_i} p_i^{-h_i} \in \Delta_i,$$

and for $0 \le i < r$:

$$\begin{aligned}
&z_i \in \mathbb{F}_{i+1},\ \text{the image of } y_i \text{ under } \Delta_i \to \Delta_{i+1},\\
&\psi_i \in \mathbb{F}_i[y],\ \text{minimal polynomial of } z_i \text{ over } \mathbb{F}_i.
\end{aligned}$$

We have $z_i \ne 0$ (and $\psi_i \ne y$) for $i > 0$. For $i = 0$ we have $z_0 = 0$ (and $\psi_0 = y$) if and only if $\overline{\phi}_1 = x$ in $\mathbb{F}[x]$. Moreover,

$$\mathbb{F}_{i+1} = \mathbb{F}_i[z_i] = \mathbb{F}_0[z_0, \dots, z_i], \quad \deg \psi_i = f_i.$$

Consider *Newton polygon operators*

$$N_i := N_{v_{i-1},\phi_i} \colon\ K[x] \longrightarrow 2^{\mathbb{R}^2}, \quad 1 \le i \le r.$$

Since we deal with normalized valuations, the vertices of $N_i(g)$ have integer coordinates for any $g \in K[x]$. Actually, the Newton polygon $N_i(g)$ is the image of $N_{\mu_{i-1},\phi_i}(g)$ under the affine transformation $(x, y) \mapsto (x, e(\mu_{i-1})y)$. Hence, the vertices of both polygons have the same abscissas and this affine map sends the

$\nu_i$-component of $N_{\mu_{i-1},\phi_i}(g)$ to the $\lambda_i$-component of $N_i(g)$. In particular, Lemma 1.6 shows that the line of slope $-\lambda_i$ containing the $\lambda_i$-component of $N_i(g)$ cuts the vertical axis at the ordinate $e(\mu_{i-1})\mu_i(g) = v_i(g)/e_i$ (see Figure 3).

Also, a MacLane chain supports *residual polynomial operators*:

$$R_i := R_{v_{i-1},\phi_i,\lambda_i}\colon K[x] \longrightarrow \mathbb{F}_i[y], \qquad 0 \le i \le r.$$

We have $R_i(0) = 0$ for all $i$. For a non-zero $g \in K[x]$ we define $R_0(g) = \overline{g/\pi^{\mu_0(g)}}$, whereas $R_i(g)$ for $i > 0$ is determined by the following result.

Theorem 1.9. *For $i > 0$ and a non-zero $g \in K[x]$ let $(s_i(g), u_i(g))$ be the left end point of the $\lambda_i$-component of $N_i(g)$. There exists a unique polynomial $R_i(g) \in \mathbb{F}_i[y]$ such that $\mathrm{H}_{\mu_i}(g) = x_i^{s_i(g)} p_i^{u_i(g)} R_i(g)(y_i)$.*

The degree of $R_i(g)$ is $(s_i'(g) - s_i(g))/e_i$, where $s_i'(g)$ is the abscissa of the right end point of the $\lambda_i$-component of $N_i(g)$.

In section 3 we shall show how to compute the operator $R_i$ in practice.

**1.5. Structure of the graded algebra.** The elements $x_r, p_r, y_r \in \mathcal{G}r(\mu)$ attached to a MacLane chain determine the structure of the graded algera of an inductive valuation.

Theorem 1.10. *The mapping $\mathbb{F}_r[y] \to \Delta$ determined by $y \mapsto y_r$ is an isomorphism of $\mathbb{F}_r$-algebras. The inverse mapping is given by*

$$g + \mathcal{P}_0^+(\mu) \mapsto y^{\lfloor s_r(g)/e_r \rfloor} R_r(g)(y),$$

*for any $g \in K[x]$ with $\mu(g) = 0$.*

Theorem 1.11. *The graded algebra of $\mu$ is*

$$\mathcal{G}r(\mu) = \mathbb{F}_r[y_r, p_r, p_r^{-1}][x_r] = \Delta[p_r, p_r^{-1}][x_r].$$

*The elements $y_r, p_r$ are algebraically independent over $\mathbb{F}_r$, and $x_r^{e_r} = p_r^{h_r} y_r$.*

From these results one may derive further properties of the residual polynomials. The most outstanding fact is that the element $R_r(g)(y_r) \in \Delta$ is, up to a power of $y_r$, a generator of the residual ideal $\mathcal{R}(g)$.

Corollary 1.12. *Take $0 \le i \le r$ and non-zero $g, h \in K[x]$. Then,*

1. *If $g \sim_{\mu_i} h$, then $R_i(g) = R_i(h)$.*
2. *If $i < r$, then $R_{i+1}(\phi_{i+1}) = 1$ and $R_i(\phi_{i+1}) = \psi_i$.*
3. *$R_i(gh) = R_i(g)R_i(h)$.*
4. *$\mathcal{R}(g) = y_r^{\lceil s_r(g)/e_r \rceil} R_r(g)(y_r)\,\Delta$, if we agree that $s_0(g) = 0$.*
5. *If $\phi$ is a key polynomial for $\mu$, then $\mathcal{R}(\phi) = R_r(\phi)(y_r)\,\Delta$ if $\phi \not\sim_\mu \phi_r$, and $\mathcal{R}(\phi) = y_r\Delta$ otherwise.*

The above results yield a strong connection between maximal ideals of $\Delta$ and residual ideals of key polynomials.

Theorem 1.13. *The mapping $\mathcal{R}\colon \mathrm{KP}(\mu) \longrightarrow \mathrm{Max}(\Delta)$ induces a bijection between $\mathrm{KP}(\mu)/\!\sim_\mu$ and $\mathrm{Max}(\Delta)$.*

Corollary 1.14. *Let $\phi$ be a key polynomial for $\mu$ such that $\phi_r \nmid_\mu \phi$ and denote $\psi = R_r(\phi)$. Then, $\mathrm{ord}_\psi(R_r(g)) = \mathrm{ord}_{\mu,\phi}(g)$ for any non-zero $g \in K[x]$.*

**1.6. Data comparison between optimal MacLane chains.** Suppose that the given MacLane chain (1.1) of the inductive valuation $\mu$ is optimal. By Proposition 1.7, any other optimal MacLane chain of $\mu$ is obtained by replacing the key polynomials $\phi_1, \dots, \phi_r$ with another family $\phi_1^*, \dots, \phi_r^*$ such that

$$\phi_i^* = \phi_i + a_i, \quad \deg a_i < m_i, \quad \mu_i(a_i) \ge \mu_i(\phi_i).$$

Take $\eta_0 := 0 \in \mathbb{F}$. For every $1 \le i \le r$ consider the following element $\eta_i \in \mathbb{F}_i$:

$$\eta_i := \begin{cases} 0, & \text{if } \mu_i(a_i) > \mu_i(\phi_i) \quad (\text{i.e. } \phi_i^* \sim_{\mu_i} \phi_i), \\ R_i(a_i) \in \mathbb{F}_i^*, & \text{if } \mu_i(a_i) = \mu_i(\phi_i) \quad (\text{i.e. } \phi_i^* \not\sim_{\mu_i} \phi_i). \end{cases} \tag{1.5}$$

Since $\deg a_i < \deg \phi_i$, we have $\mu_i(a_i) = \mu_{i-1}(a_i)$ by the definition of the augmentation of valuations. If $e_i > 1$, we have $\mu_i(\phi_i) = \mu_{i-1}(\phi_i) + \nu_i \notin \Gamma_{i-1}$. Hence, in this case we cannot have $\mu_i(a_i) = \mu_i(\phi_i)$. In other words,

$$e_i > 1 \implies \phi_i^* \sim_{\mu_i} \phi_i \implies \eta_i = 0.$$

The next result shows the relationship of the data $x_i, p_i, y_i, z_i, \psi_i$ attached to the optimal MacLane chain (1.1) with the analogous data $x_i^*, p_i^*, y_i^*, z_i^*, \psi_i^*$ attached to the optimal MacLane chain determined by the choice of $\phi_1^*, \dots, \phi_r^*$ as key polynomials.

LEMMA 1.15. *With the above notation, for all* $0 \le i \le r$ *we have*

$$p_i^* = p_i, \quad x_i^* = x_i + p_i^{h_i}\eta_i, \quad y_i^* = y_i + \eta_i,$$

*whereas for* $0 \le i < r$ *we have* $z_i^* = z_i + \eta_i, \quad \psi_i^*(y) = \psi_i(y - \eta_i)$.

## 2. Okutsu equivalence of prime polynomials

In this section, we show how inductive valuations parameterize certain sets of prime polynomials. All results are extracted from [**3**].

We shall apply inductive valuations $\mu$ on $K(x)$ to polynomials in $K_v[x]$, without any mention of the natural extension of $\mu$ to $K_v(x)$ described in Proposition 1.8.

Let $\mathbb{P} \subset \mathcal{O}_v[x]$ be the set of all monic irreducible polynomials in $\mathcal{O}_v[x]$. We say that an element in $\mathbb{P}$ is a *prime polynomial* (with respect to $v$).

Let $F \in \mathbb{P}$ and fix $\theta \in \overline{K}_v$ a root of $F$. Let $K_F = K_v(\theta)$ be the finite extension of $K_v$ generated by $\theta$, $\mathcal{O}_F$ the ring of integers of $K_F$, $\mathfrak{m}_F$ the maximal ideal and $\mathbb{F}_F$ the residue class field. We have $\deg F = e(F)f(F)$, where $e(F)$, $f(F)$ are the ramification index and residual degree of $K_F/K_v$, respectively.

Let $\mu_{\infty,F}$ be the pseudo-valuation on $K[x]$ obtained as the composition:

$$\mu_{\infty,F} \colon K[x] \longrightarrow K_v(\theta) \xrightarrow{v} \mathbb{Q} \cup \{\infty\},$$

the first mapping being determined by $x \mapsto \theta$. This pseudo-valuation does not depend on the choice of $\theta$ as a root of $F$.

Recall that a pseudo-valuation has the same properties as a valuation, except for the fact that the pre-image of $\infty$ is a prime ideal which is not necessarily zero.

We are interested in finding properties of prime polynomials leading to a certain comprehension of the structure of the set $\mathbb{P}$. An inductive valuation $\mu$ such that $\mu < \mu_{\infty,F}$ reveals many properties of $F$.

THEOREM 2.1. *Let* $F \in \mathbb{P}$ *be a prime polynomial. An inductive valuation* $\mu$ *satisfies* $\mu \le \mu_{\infty,F}$ *if and only if there exists* $\phi \in \mathrm{KP}(\mu)$ *such that* $\phi \mid_\mu F$. *In this case, for a non-zero polynomial* $g \in K[x]$, *we have*

$$\mu(g) = \mu_{\infty,F}(g) \quad \textit{if and only if} \quad \phi \nmid_\mu g.$$

THEOREM 2.2. *Let $F$ be a prime polynomial, $\mu$ an inductive valuation and $\phi$ a key polynomial for $\mu$. Then, $\phi \mid_\mu F$ if and only if $\mu_{\infty,F}(\phi) > \mu(\phi)$. Moreover, if this condition holds, then:*

(1) *Either $F = \phi$, or the Newton polygon $N_{\mu,\phi}(F)$ is one-sided of slope $-\nu$, where $\nu = \mu_{\infty,F}(\phi) - \mu(\phi) \in \mathbb{Q}_{>0}$.*
(2) *Let $\ell = \ell(N_{\mu,\phi}(F))$. Then, $F \sim_\mu \phi^\ell$ and $\deg F = \deg \phi^\ell$.*

Theorem 2.2 is a generalization of Hensel's lemma. The residual ideal $\mathcal{R}_\mu(F) = \mathcal{R}_\mu(\phi)^\ell$ is a power of the maximal ideal $\mathcal{R}_\mu(\phi)$. Thus, if for a certain polynomial $g \in K[x]$ the residual ideal $\mathcal{R}_\mu(g)$ factorizes as the product of two coprime proper ideals, we may conclude that $g$ factorizes in $K_v[x]$. This yields the fundamental result concerning factorization of polynomials over $K_v$.

THEOREM 2.3. *Let $\mu$ be an inductive valuation equipped with a MacLane chain of length $r$ as in (1.1). Let $\phi \in \mathrm{KP}(\mu)$ such that $\phi \not\sim_\mu \phi_r$. Then, every monic polynomial $g \in \mathcal{O}_v[x]$ factorizes into a product of monic polynomials in $\mathcal{O}_v[x]$:*

$$g = g_0\, \phi^{\mathrm{ord}_\phi(g)} \prod\nolimits_{(\lambda,\psi)} g_{\lambda,\psi},$$

*where $-\lambda$ runs on the slopes of $N^-_{r+1}(g) := N^-_{v_r,\phi}(g)$ and $\psi$ runs on the prime factors of $R_{r+1,\lambda}(g) := R_{v_r,\phi,\lambda}(g)$ in $\mathbb{F}_{r+1}[y]$, where $\mathbb{F}_{r+1} := \mathbb{F}_r[y]/(R_r(\phi))$. Moreover,*

$$\deg g_0 = \deg g - \ell(N^-_{r+1}(g)) \deg \phi, \quad \deg g_{\lambda,\psi} = e_\lambda \,\mathrm{ord}_\psi(R_{r+1,\lambda}(g)) \deg \psi \deg \phi,$$

*where $e_\lambda$ is the least positive denominator of $\lambda$. Further, if $\mathrm{ord}_\psi(R_{r+1,\lambda}(g)) = 1$, then $g_{\lambda,\psi}$ is irreducible in $\mathcal{O}_v[x]$.*

PROOF. Let $g = G_1 \cdots G_t$ be the prime factorization of $g$ in $\mathcal{O}_v[x]$. The factor $g_0$ is the product of all prime factors $G_j$ such that $\phi \nmid_\mu G_j$. The factor $\phi^{\mathrm{ord}_\phi(g)}$ is the product of all $G_j = \phi$. The factor $g_{\lambda,\psi}$ is the product of all $G_j$ such that $\phi \mid_\mu G_j$, $N^-_{r+1}(G_j)$ is one-sided of slope $-\lambda$ and $R_{r+1,\lambda}(G_j)$ is a power of $\psi$. □

The *Okutsu bound* of a prime polynomial $F \in \mathbb{P}$ is defined as

$$\delta_0(F) := \deg(F)\,\mathrm{Max}\,\{v(g(\theta))/\deg g \mid g \in \mathcal{O}[x],\ g \text{ monic},\ \deg g < \deg F\}\,.$$

We may attach to $F$ a valuation $\mu_F\colon K_v(x)^* \to \mathbb{Q}$, determined by the following action on polynomials:

$$\mu_F(g) = \mathrm{Min}_{0\le s}\{v(a_s(\theta)) + s\delta_0(F)\},$$

where $g = \sum_{0\le s} a_s F^s$ is the $F$-expansion of $g$.

DEFINITION 2.4. We say that a key polynomial $\phi$ for an inductive valuation $\mu$ of depth $r$ is *strong* if either $r = 0$ or $\deg \phi > m_r(\mu)$. We say that $\mathcal{L} \in \mathrm{Max}(\Delta(\mu))$ is *strong* if $\mathcal{L} = \mathcal{R}(\phi)$ for a strong $\phi \in \mathrm{KP}(\mu)$.

THEOREM 2.5. *The mapping $\mu_F$ is an inductive valuation on $K_v(x)$ and $F$ is a strong key polynomial for $\mu_F$.*

We denote by the same symbol $\mu_F$ the valuation on $K(x)$ obtained by restriction. The *Okutsu depth* of a prime polynomial $F$ (defined in [**4, 15**]) coincides with the MacLane depth of the canonical valuation $\mu_F$.

Let $F$ be a prime polynomial of Okutsu depth $r$, and define $f_r := \deg R_r(F)$ with respect to any optimal MacLane chain of $\mu_F$. An *Okutsu invariant* of $F$ is a rational number that depends only on $e_0,\dots,e_r,f_0,\dots,f_r,h_1,\dots,h_r$; that is, on the basic MacLane invariants of $\mu_F$ and the number $f_r$.

As examples of Okutsu invariants we may quote:

$$e(F)=e(\mu_F)=e_0\cdots e_r,\quad f(F)=f_0\cdots f_r,\quad \delta_0(F)=w_{r+1}. \tag{2.1}$$

In section 4.1 we exhibit some more Okutsu invariants of prime polynomials.

Definition 2.6. Let $F,G\in\mathbb{P}$ be two prime polynomials of the same degree, and let $\theta\in\overline{K}_v$ be a root of $F$. We say that $F$ and $G$ are *Okutsu equivalent*, and we write $F\approx G$, if $v(G(\theta))>\delta_0(F)$.

We denote by $[F]\subset\mathbb{P}$ the set of all prime polynomials which are Okutsu equivalent to $F$. The idea behind this concept is that $F$ and $G$ are close enough to share the same Okutsu invariants, as the next result shows.

Proposition 2.7. *Let $F,G\in\mathbb{P}$ be two prime polynomials of the same degree. The following conditions are equivalent:*

(1) $F\approx G$.
(2) $F\sim_{\mu_F}G$.
(3) $\mu_F=\mu_G$ *and* $\mathcal{R}(F)=\mathcal{R}(G)$*, where* $\mathcal{R}:=\mathcal{R}_{\mu_F}=\mathcal{R}_{\mu_G}$.

The symmetry of condition (3) shows that $\approx$ is an equivalence relation on the set $\mathbb{P}$ of prime polynomials. These conditions determine a parameterization of the quotient set $\mathbb{P}/\approx$ by a discrete space.

The *MacLane space* of the valued field $(K,v)$ is defined to be the set

$$\mathbb{M}=\left\{(\mu,\mathcal{L})\mid \mu\in\mathbb{V}^{\mathrm{ind}},\ \mathcal{L}\in\operatorname{Max}(\Delta(\mu)),\ \mathcal{L}\text{ strong}\right\}.$$

We may define the following "Okutsu map":

$$\mathrm{ok}\colon\mathbb{M}\longrightarrow\mathbb{P}/\approx,\qquad (\mu,\mathcal{L})\ \mapsto\ [\phi],$$

where $\phi$ is any key polynomial for $\mu$ such that $\mathcal{R}_\mu(\phi)=\mathcal{L}$.

Theorem 2.8. *The Okutsu map is bijective and the inverse map is determined by* $F\mapsto(\mu_F,\mathcal{R}_{\mu_F}(F))$.

A point $(\mu,\mathcal{L})\in\mathbb{M}$ is characterized by discrete invariants which may be considered as a kind of DNA sequence encoding arithmetic properties which are common to all prime polynomials in the Okutsu class $[F]=\mathrm{ok}(\mu,\mathcal{L})$.

## 3. Types over $(K,v)$

We keep dealing with a fixed discrete valued field $(K,v)$ with valuation ring $\mathcal{O}$.

**3.1. Types.** A *type* is a computational object which is able to represent a pair $(\mu,\mathcal{L})$, where $\mu$ is an inductive valuation on $K(x)$ and $\mathcal{L}$ is a maximal ideal in $\Delta(\mu)$. More precisely, a type collects discrete data determining a MacLane chain of $\mu$ and the maximal ideal $\mathcal{L}$.

Therefore, a type $\mathbf{t}$ supports some data structured into levels:

$$\mathbf{t}=(\psi_0;(\phi_1,\lambda_1,\psi_1);\cdots;(\phi_r,\lambda_r,\psi_r)).$$

The number $r$ of levels is called the *order* of the type.

A type $\mathbf{t}=(\psi_0)$ of order 0 is determined by the choice of an arbitrary monic irreducible polynomial $\psi_0\in\mathbb{F}[y]$. It supports the following data at level 0:

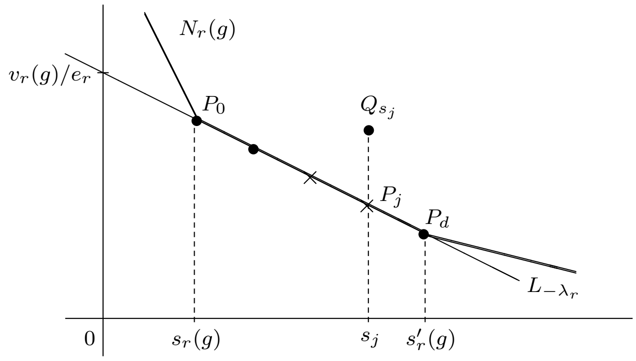
- The minimal valuation $\mu_0$ on $K(x)$ and its normalization $v_0=\mu_0$.

- Numerical data: $e_0 = m_0 = 1$, $\nu_0 = \lambda_0 = h_0 = 0$.
- $\psi_0 \in \mathbb{F}_0[y]$ a monic irreducible polynomial.
- $\mathbb{F}_1 = \mathbb{F}_0[y]/(\psi_0)$ a finite extension of $\mathbb{F}$ of degree $f_0 := \deg \psi_0$.
- $z_0 \in \mathbb{F}_1$ the class of $y$. Hence, $\mathbb{F}_1 = \mathbb{F}_0[z_0]$ and $\psi_0$ is the minimal polynomial of $z_0$ over $\mathbb{F}_0$.
- The residual polynomial operator $R_0\colon K[x] \to \mathbb{F}_0[y]$, where $\mathbb{F}_0 = \mathbb{F}$. It is defined as $R_0(g) = \overline{g(y)/\pi^{v_0(g)}}$ for any non-zero $g \in K[x]$.

If $\mathbf{t}_0 = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots ; (\phi_{r-1}, \lambda_{r-1}, \psi_{r-1}))$ is a type of order $r-1 \ge 0$, then a type $\mathbf{t} = (\mathbf{t}_0; (\phi_r, \lambda_r, \psi_r))$ of order $r$ may be obtained by adding the following data at the $r$-th level:

- A *representative* $\phi_r$ of $\mathbf{t}_0$. That is, a monic polynomial $\phi_r \in \mathcal{O}[x]$ of degree $m_r := e_{r-1}f_{r-1}m_{r-1}$ such that $R_{r-1}(\phi_r) = \psi_{r-1}$. Lemma 3.1 below shows that $\phi_r$ is a key polynomial for $\mu_{r-1}$.
- The Newton polygon operator $N_r = N_{v_{r-1},\phi_r}$.
- A positive rational number $\lambda_r = h_r/e_r$, with $h_r$, $e_r$ positive coprime integers. We say that $\lambda_r$ is the *slope* of $\mathbf{t}$ at level $r$.
- The non-normalized slope $\nu_r = \lambda_r/e(\mu_{r-1}) = h_r/e_1 \cdots e_r$.
- The augmented valuation $\mu_r = [\mu_{r-1}; \phi_r, \nu_r]$, together with its normalization $v_r = e(\mu_r)\mu_r = e_1 \cdots e_r \mu_r$.
- $\psi_r \in \mathbb{F}_r[y]$ a monic irreducible polynomial, $\psi_r \ne y$.
- $\mathbb{F}_{r+1} = \mathbb{F}_r[y]/(\psi_r)$ a finite extension of $\mathbb{F}_r$ of degree $f_r := \deg \psi_r$.
- $z_r \in \mathbb{F}_{r+1}$ the class of $y$. Hence, $\mathbb{F}_{r+1} = \mathbb{F}_r[z_r]$ and $\psi_r$ is the minimal polynomial of $z_r$ over $\mathbb{F}_r$.
- A residual polynomial operator $R_r\colon K[x] \to \mathbb{F}_r[y]$ described as follows.

FIGURE 3. Computation of $R_r(g)$ for a non-zero polynomial $g \in K[x]$. The line $L_{-\lambda_r}$ has slope $-\lambda_r$.




The operator $R_r$ maps 0 to 0. For a non-zero $g \in K[x]$ with $\phi_r$-expansion $g = \sum_{0 \le s} a_s \phi_r^s$, let us denote by $s_r(g) \le s'_r(g)$ the abscissas of the end points of the $\lambda_r$-component $S$ of $N_r(g)$ (cf. section 1.2). Let $d = (s'_r(g) - s_r(g))/e_r$ be the *degree* of $S$. There are $d+1$ points of integer coordinates $P_0, \dots, P_d$ lying on $S$, with abscissas $s_j := s_r(g) + je_r$ for $0 \le j \le d$ (see Figure 3). Denote by $Q_{s_j} = (s_j, v_{r-1}(a_{s_j}\phi_r^{s_j}))$ the point of abscissa $s_j$ in the cloud of points which is used to compute the Newton polygon $N_r(g)$. Consider the following residual coefficient:

$$c_j := \begin{cases} 0, & \text{if } Q_{s_j} \text{ lies above } N_r(g), \\ z_{r-1}^{t_{r-1}(a_{s_j})} R_{r-1}(a_{s_j})(z_{r-1}) \in \mathbb{F}_r^*, & \text{if } Q_{s_j} \text{ lies on } N_r(g), \end{cases} \tag{3.1}$$

where for any $a \in K[x]$ we define $t_0(a) = 0$ and $t_k(a) = (s_k(a) - \ell_k v_k(a))/e_k$ if $k > 0$. Then, we define

$$R_r(g)(y) := R_{v_{r-1},\phi_r,\lambda_r}(g) = c_0 + c_1 y + \cdots + c_d y^d \in \mathbb{F}_r[y],$$

Since $c_0 c_d \neq 0$, the polynomial $R_r(g)$ has degree $d$ and it is never divisible by $y$.

LEMMA 3.1. *Let* $\mathbf{t}$ *be a type of order* $r$ *and denote* $\mu := \mu_r$, $\Delta := \Delta(\mu)$.

(1) $\mu$ *is an inductive valuation and the chain of augmentations*

$$\mu_0 \xrightarrow{\phi_1,\nu_1} \mu_1 \xrightarrow{\phi_2,\nu_2} \cdots \xrightarrow{\phi_{r-1},\nu_{r-1}} \mu_{r-1} \xrightarrow{\phi_r,\nu_r} \mu_r = \mu$$

*is a MacLane chain of* $\mu$.

(2) *For* $1 \le i \le r$ *denote by* $\mathbb{F}_{i,\mu}$, $z_{i-1,\mu}$, $\psi_{i-1,\mu}$, $R_{i,\mu}$ *the data and operator attached to this MacLane chain of* $\mu$ *in section 1.4. The rule* $\iota_i(z_{i-1}) = z_{i-1,\mu}$ *determines a commutative diagram with vertical isomorphisms:*

$$\begin{array}{ccccccc} \mathbb{F} = \mathbb{F}_0 & \subset & \mathbb{F}_1 & \subset & \cdots & \subset & \mathbb{F}_r \\ \| & & \downarrow \iota_1 & & \cdots & & \downarrow \iota_r \\ \mathbb{F} = \mathbb{F}_{0,\mu} & \subset & \mathbb{F}_{1,\mu} & \subset & \cdots & \subset & \mathbb{F}_{r,\mu} \end{array}$$

*If we denote still by* $\iota_i$ *the isomorphism between* $\mathbb{F}_i[y]$ *and* $\mathbb{F}_{i,\mu}[y]$ *induced by* $\iota_i$, *we have* $R_{i,\mu} = \iota_i \circ R_i$ *for all* $i$. *Thus, up to considering these isomorphisms* $\iota_i$ *as identities, we may identify all data and operators supported by* $\mathbf{t}$ *with the analogous data and operators attached to* $\mu$*:*

$$\mathbb{F}_i = \mathbb{F}_{i,\mu}, \quad z_{i-1} = z_{i-1,\mu}, \quad \psi_{i-1} = \psi_{i-1,\mu}, \quad R_i = R_{i,\mu}.$$

(3) *A polynomial* $\phi \in K[x]$ *is a representative of* $\mathbf{t}$ *if and only if* $\phi$ *is a key polynomial for* $\mu$ *and* $\mathcal{R}(\phi) = \psi_r(y_r)\Delta$.[1]

PROOF. Let us prove all statements by induction on $r$. Suppose first that $\mathbf{t} = (\psi_0)$ is a type of order 0. In this case, $\mu = \mu_0$ and items (1) and (2) are trivial. Note that $R_0 = R_{0,\mu}$ by the definition of both operators. A representative of $\mathbf{t}$ is a monic polynomial $\phi \in \mathcal{O}[x]$ of degree $m_1 = f_0 = \deg \psi_0$ such that $\overline{\phi} = R_0(\phi) = \psi_0$. On the other hand, a key polynomial for $\mu_0$ is a monic polynomial $\phi \in \mathcal{O}[x]$ such that $\overline{\phi}$ is irreducible in $\mathbb{F}[x]$. Also, Corollary 1.12,(4) shows that $\mathcal{R}(\phi) = R_0(\phi)(y_0)\Delta$. Since $R_0(\phi)$ and $\psi_0$ are monic polynomials, the equality $R_0(\phi)(y_0)\Delta = \psi_0(y_0)\Delta$ is equivalent to $R_0(\phi) = \psi_0$, by Theorem 1.10. This proves item (3).

We assume from now on that $r > 0$ and all statements of the lemma are true for types of order $r-1$. In particular, $\mu_{r-1}$ is an inductive valuation and

$$\mu_0 \xrightarrow{\phi_1,\nu_1} \mu_1 \xrightarrow{\phi_2,\nu_2} \cdots \longrightarrow \mu_{r-2} \xrightarrow{\phi_{r-1},\nu_{r-1}} \mu_{r-1}$$

is a MacLane chain of $\mu_{r-1}$. For all $1 \le i < r$ we have isomorphisms:

$$\iota_i \colon \mathbb{F}_i \longrightarrow \mathbb{F}_{i,\mu}, \quad z_{i-1} \mapsto z_{i-1,\mu}$$

[1] In this equality we use the convention of item (2). The polynomial $\psi_r \in \mathbb{F}_r[y]$ is considered as a polynomial with coefficients in $\mathbb{F}_{r,\mu} \subset \Delta$ via the isomorphism $\iota_r \colon \mathbb{F}_r \to \mathbb{F}_{r,\mu}$.

such that $\iota_i$ restricted to $\mathbb{F}_{i-1}$ coincides with $\iota_{i-1}$. Since $\psi_{i-1}$, $\psi_{i-1,\mu}$ are the minimal polynomials of $z_{i-1}$, $z_{i-1,\mu}$ over $\mathbb{F}_{i-1}$, $\mathbb{F}_{i-1,\mu}$, respectively, we have $\psi_{i-1,\mu} = \iota_{i-1}(\psi_{i-1})$. Also, $\phi_r$ is a key polynomial for $\mu_{r-1}$ such that

$$\mathcal{R}_{\mu_{r-1}}(\phi_r) = \iota_{r-1}(\psi_{r-1})(y_{r-1})\Delta_{r-1}.$$

In order to prove item (1) we need only to show that $\phi_r \not\sim_{\mu_{r-1}} \phi_{r-1}$ if $r > 1$. In fact, if $r > 1$, then $\psi_{r-1} \neq y$; by Theorem 1.10, $\mathcal{R}_{\mu_{r-1}}(\phi_r) \neq y_{r-1}\Delta_{r-1}$, and this implies $\phi_r \not\sim_{\mu_{r-1}} \phi_{r-1}$ by Corollary 1.12,(5).

Let us prove item (2). We have $\mathbb{F}_r = \mathbb{F}_{r-1}[z_{r-1}]$ and $\psi_{r-1} = R_{r-1}(\phi_r)$ is the minimal polynomial of $z_{r-1}$ over $\mathbb{F}_{r-1}$. Also, $\mathbb{F}_{r,\mu} = \mathbb{F}_{r-1,\mu}[z_{r-1,\mu}]$ and $\psi_{r-1,\mu} = R_{r-1,\mu}(\phi_r)$ (Corollary 1.12) is the minimal polynomial of $z_{r-1,\mu}$ over $\mathbb{F}_{r-1,\mu}$. By the induction hypothesis, we have $R_{r-1,\mu} = \iota_{r-1} \circ R_{r-1}$, so that $\psi_{r-1,\mu} = \iota_{r-1}(\psi_{r-1})$, and this implies that $\iota_r$ is well-defined and is an isomorphism.

By [**3**, Def. 3.15 + Cor. 4.9], for any non-zero $g \in K[x]$ we have

$$R_{r,\mu}(g) = c'_0 + c'_1 y + \cdots + c'_d y^d,$$

where $d = (s'_r(g) - s_r(g))/e_r = \deg R_r(g)$ and the coefficients $c'_j \in \mathbb{F}_{r,\mu}$ satisfy:

$$c'_j = \begin{cases} 0, & \text{if } Q_{s_j} \text{ lies above } N_r(g), \\ z_{r-1,\mu}^{\ell'_{r-1}\mathfrak{s}_j - \ell_{r-1}\mathfrak{u}_j} z_{r-1,\mu}^{\lfloor s_{r-1}(a_{s_j})/e_{r-1}\rfloor} R_{r-1,\mu}(a_{s_j})(z_{r-1,\mu}), & \text{if } Q_{s_j} \text{ lies on } N_r(g), \end{cases}$$

where $a_{s_j}$, $Q_{s_j}$ are defined as in (3.1) and $\mathfrak{s}_j, \mathfrak{u}_j \in \mathbb{Z}$ are uniquely determined by:

$$h_{r-1}\mathfrak{s}_j + e_{r-1}\mathfrak{u}_j = v_{r-1}(a_{s_j}), \quad 0 \le \mathfrak{s}_j < e_{r-1}. \tag{3.2}$$

We want to prove that $R_{r,\mu} = \iota_r \circ R_r$, or equivalently $c'_j = \iota_r(c_j)$ for all $0 \le j \le d$, which is clearly equivalent to:

$$\ell'_{r-1}\mathfrak{s}_j - \ell_{r-1}\mathfrak{u}_j + \lfloor s_{r-1}(a_{s_j})/e_{r-1}\rfloor = (s_{r-1}(a_{s_j}) - \ell_{r-1}v_{r-1}(a_{s_j}))/e_{r-1}. \tag{3.3}$$

Let $L$ be the line of slope $-\lambda_{r-1}$ containing the $\lambda_{r-1}$-component of $N_{r-1}(a_{s_j})$. As shown in Figure 3, this line cuts the vertical axis at the point $(0, v_{r-1}(a_{s_j})/e_{r-1})$. Hence, (3.2) shows that $(\mathfrak{s}_j, \mathfrak{u}_j)$ is the point of least non-negative abscissa among all points on $L$ having integer coordinates. Since the point $(s_{r-1}(a_{s_j}), u_{r-1}(a_{s_j}))$ belongs to $L \cap (\mathbb{Z}_{\ge 0} \times \mathbb{Z})$, we have $\lfloor s_{r-1}(a_{s_j})/e_{r-1}\rfloor = (s_{r-1}(a_{s_j}) - \mathfrak{s}_j)/e_{r-1}$. Then, the equality (3.3) is easily deduced from (3.2) and the Bézout identity (1.3).

Let us prove item (3). After item (2), we may identify all data and operators supported by $\mathbf{t}$ with the analogous data and operators attached to the MacLane chain of $\mu$. Suppose that $\phi$ is a representative of $\mathbf{t}$, so that $\deg\phi = m_{r+1}$ and $\psi_r = R_r(\phi)$. By the definition of the operator $R_r$, we have

$$(s'_r(\phi) - s_r(\phi))m_r = e_r(\deg\psi_r)m_r = e_r f_r m_r = m_{r+1} = \deg\phi.$$

Since $\deg\phi \ge s'_r(\phi)m_r$, we deduce that $s_r(\phi) = 0$ and $s'_r(\phi) = e_r \deg\psi_r$. Thus, $\phi$ is a key polynomial for $\mu$ because it satisfies condition (2) of [**3**, Lem. 5.2]. By Corollary 1.12,(4), $\mathcal{R}(\phi) = R_r(\phi)(y_r)\Delta = \psi_r(y_r)\Delta$.

Conversely, suppose that $\phi \in \mathrm{KP}(\mu)$ satisfies $\mathcal{R}(\phi) = \psi_r(y_r)\Delta$. By Lemma 1.2, $\phi$ is a monic polynomial with coefficients in $\mathcal{O}$. Since $\psi_r \neq y$, Theorem 1.10 and Corollary 1.12,(5) show that $\phi \not\sim_\mu \phi_r$ and $\mathcal{R}(\phi) = R_r(\phi)(y_r)\Delta$. By [**3**, Lem. 5.2], $R_r(\phi)$ is monic irreducible and $\deg\phi = e_r \deg R_r(\phi)m_r$. By Theorem 1.10, the monic polynomials $\psi_r$ and $R_r(\phi)$ generate the same ideal in $\mathbb{F}_r[y]$; hence, $R_r(\phi) = \psi_r$ and $\deg\phi = m_{r+1}$. Thus, $\phi$ is a representative of $\mathbf{t}$. □

Note that a type $\mathbf{t}$ of order $r$ determines the numerical values $m_{r+1} := e_r f_r m_r$, $V_{r+1} := e_r f_r (e_r V_r + h_r)$ of any enlargement of $\mathbf{t}$ to a type of order $r+1$.

The data $\psi_r$, $\mathbb{F}_{r+1}$, $z_r$ at the $r$-th level of $\mathbf{t}$ do not correspond to data attached to the MacLane chain of $\mu = \mu_r$. Through the isomorphism $\mathbb{F}_r[y] \simeq \Delta$ of Theorem 1.10 the irreducible polynomial $\psi_r \in \mathbb{F}_r[y]$ determines a maximal ideal $\mathcal{L} = \psi_r(y_r)\Delta$ in $\Delta$. Hence, the type $\mathbf{t}$ singles out a pair $(\mu_{\mathbf{t}}, \mathcal{L}_{\mathbf{t}})$, where $\mu_{\mathbf{t}} = \mu$ is an inductive valuation and $\mathcal{L}_{\mathbf{t}} = \mathcal{L}$ is a maximal ideal in $\Delta$.

Remark 3.2. The definition of a type given in this paper has some slight differences with respect to the original definition in [**6**], where $K$ was a global field.

(1) In [**6**] we used negative slopes $\lambda_i = -h_i/e_i$.

(2) The valuations $v_0, \dots, v_r$ were denoted $v_1, \dots, v_{r+1}$ in [**6**].

(3) Instead of the Bézout identities $\ell_i h_i + \ell'_i e_i = 1$, in [**6**] we used the identities $\ell_i h_i - \ell'_i e_i = 1$. This amounts to a change of sign of the data $\ell'_i$.

(4) The residual operators $R_i$ have been normalized (by a slight change in the definition of the rational functions $\Phi_i$ from section 1.4) to satisfy $R_i(1) = 1$. In this way, if $g \in K[x]$ has leading coefficient one in its $\phi_i$-expansion, then $R_i(g)$ is monic.

Let $\mathbf{t}$ be a type of order $r$ over $(K, v)$. The *truncation* of $\mathbf{t}$ at level $j$, $\operatorname{Trunc}_j(\mathbf{t})$, is the type of order $j$ obtained from $\mathbf{t}$ by dropping all levels higher than $j$.

For any $g \in K[x]$ we define $\operatorname{ord}_{\mathbf{t}}(g) := \operatorname{ord}_{\psi_r} R_r(g)$ in $\mathbb{F}_r[y]$. If $\operatorname{ord}_{\mathbf{t}}(g) > 0$, we say that $\mathbf{t}$ *divides* $g$, and we write $\mathbf{t} \mid g$. By Corollary 1.14 and Lemma 3.1, we have $\operatorname{ord}_{\mathbf{t}} = \operatorname{ord}_{\mu_r,\phi}$ for any representative $\phi$ of $\mathbf{t}$. In particular, $\operatorname{ord}_{\mathbf{t}}(gh) = \operatorname{ord}_{\mathbf{t}}(g) + \operatorname{ord}_{\mathbf{t}}(h)$ for all $g, h \in K[x]$.

The next result is a consequence of Proposition 1.4 and Theorem 1.10.

Corollary 3.3. *Let* $\mathbf{t}$ *be a type of order* $r$, $\phi$ *a representative of* $\mathbf{t}$, *and* $\alpha \in \overline{K}_v$ *a root of* $\phi$. *Then, we have an isomorphism*

$$\mathbb{F}_{r+1} \xrightarrow{\sim} \mathbb{F}_\phi, \quad z_0 \mapsto \gamma_0(\alpha) + \mathfrak{m}_\phi, \dots, z_r \mapsto \gamma_r(\alpha) + \mathfrak{m}_\phi$$

*where the rational functions* $\gamma_0 \dots, \gamma_r \in K(x)$ *are those defined in (1.4).*

### 3.2. Construction of types.

Combined with Theorem 1.13, Lemma 3.1,(3) shows that any type admits infinitely many representatives. In this section we describe a concrete procedure to construct a representative of a type.

Proposition 3.4. *Let* $\mathbf{t}$ *be a type of order* $r \geq 1$. *Let* $\varphi \in \mathbb{F}_r[y]$ *be a non-zero polynomial of degree less than* $f_r$ *and let* $b \geq V_{r+1}$ *be an integer. Then, we may construct a polynomial* $g \in \mathcal{O}[x]$ *such that*

$$\deg g < m_{r+1}, \quad v_r(g) = b, \quad y^{\lfloor s_r(g)/e_r \rfloor} R_r(g) = \varphi.$$

Proof. Let $L$ be the line of slope $-\lambda_r$ cutting the vertical axis at the point $(0, b/e_r)$. Let $\mathfrak{s}$ be the least non-negative abscissa of a point of integer coordinates lying on $L$; this abscissa $\mathfrak{s}$ is uniquely determined by the conditions:

$$\mathfrak{s} h_r \equiv b \pmod{e_r}, \quad 0 \leq \mathfrak{s} < e_r.$$

Let $k = \operatorname{ord}_y(\varphi)$ and write $\varphi = y^k \sum_{0 \leq j < f_r - k} \zeta_j y^j$, with $\zeta_j \in \mathbb{F}_r$ and $\zeta_0 \neq 0$. For each $0 \leq j < f_r - k$ such that $\zeta_j \neq 0$ we denote

$$s_j = \mathfrak{s} + (j+k)e_r, \quad b_j = (b/e_r) - s_j(V_r + \lambda_r).$$

Clearly, $s_j < (j+k+1)e_r \leq e_r f_r$ and $b_j \geq (e_r f_r - s_j)(V_r + \lambda_r) > V_r + \lambda_r > V_r$, because $b/e_r \geq e_r f_r (V_r + \lambda_r)$ by hypothesis.

Also, for each such $j$ we consider an analogous abscissa $\mathfrak{s}_j$ determined by

$$\mathfrak{s}_j h_{r-1} \equiv b_j \pmod{e_{r-1}}, \quad 0 \le \mathfrak{s}_j < e_{r-1},$$

and we let $\varphi_j \in \mathbb{F}_{r-1}[y]$ be the unique polynomial such that

$$\deg \varphi_j < f_{r-1}, \quad \varphi_j(z_{r-1}) = \zeta_j\, z_{r-1}^{(\ell_{r-1}b_j-\mathfrak{s}_j)/e_{r-1}} \in \mathbb{F}_r^*. \tag{3.4}$$

For $r=1$ we have $\ell_0 = 0$, $\mathfrak{s}_j = 0$ and $\varphi_j(z_{r-1}) = \zeta_j$.

Consider $g = \phi_r^{s_0}\left(\sum_{0\le j<f_r-k} a_{s_j}\phi_r^{je_r}\right)$, where $a_{s_j} = 0$ if $\zeta_j = 0$, whereas for $\zeta_j \ne 0$ we take $a_{s_j} \in \mathcal{O}[x]$ satisfying

$$\deg a_{s_j} < m_r, \quad v_{r-1}(a_{s_j}) = b_j, \quad y^{\lfloor s_{r-1}(a_{s_j})/e_{r-1}\rfloor} R_{r-1}(a_{s_j}) = \varphi_j. \tag{3.5}$$

Clearly, $\deg g < e_r f_r m_r$. Since $v_{r-1}(a_{s_j}) = b_j$, the point $(s_j, v_{r-1}(a_{s_j}\phi_r^{s_j}))$ lies on $L$, and this guarantees that $v_r(g) = b$ by Lemma 1.6. By construction, $s_r(g) = s_0 = \mathfrak{s} + ke_r$, so that $\lfloor s_r(g)/e_r \rfloor = k$. Thus, the condition $y^{\lfloor s_r(g)/e_r\rfloor} R_r(g) = \varphi$ is equivalent to $R_r(g) = \sum_{0\le j<f_r-k} \zeta_j y^j$; by the definition (3.1) of the coefficients of the residual polynomial, this amounts to

$$z_{r-1}^{\left(s_{r-1}(a_{s_j})-\ell_{r-1}b_j\right)/e_{r-1}} R_{r-1}(a_{s_j})(z_{r-1}) = \zeta_j$$

for all $0 \le j < f_r - k$ such that $\zeta_j \ne 0$. This equality is a consequence of (3.4) and (3.5), having in mind that $\lfloor s_{r-1}(a_{s_j})/e_{r-1}\rfloor = (s_{r-1}(a_{s_j}) - \mathfrak{s}_j)/e_{r-1}$ if $r > 1$, whereas for $r = 1$ we have $s_0(a_{s_j}) = 0$.

Therefore, we may construct $g$ by a recurrent procedure leading to the solution of the same problem for types of lower order. Thus, it suffices to solve the problem for types of order one, which is quite easy. In fact, if $r = 1$ and $\zeta_j \ne 0$, we may take $a_{s_j} = \pi^{b_j} a'_{s_j}$, where $a'_{s_j}$ is an arbitrary lifting of $\varphi_j \in \mathbb{F}[y]$ to $\mathcal{O}[x]$; since $v_0(a'_{s_j}) = 0$, we have $v_0(a_{s_j}) = b_j \ge V_1 = 0$, so that $a_{s_j}$ belongs to $\mathcal{O}[x]$ as well. $\square$

In order to construct a representative $\phi$ of $\mathbf{t}$ we may apply the procedure of Proposition 3.4 to construct a polynomial $g \in \mathcal{O}[x]$ such that $R_r(g) = \psi_r - y^{f_r}$, and take $\phi = \phi_r^{e_r f_r} + g$. This justifies the following statement.

Theorem 3.5. *We may efficiently construct representatives of types.*

Since the level data $\lambda_i$, $\psi_i$ are arbitrarily chosen, Theorem 3.5 shows that we may construct types of prescribed order $r$ and prescribed numerical data $h_i, e_i, f_i$ for $1 \le i \le r$. In other words, we may construct inductive valuations of prescribed depth and prescribed MacLane invariants. This facilitates the construction of local extensions with prescribed arithmetic properties (cf. sections 4.1 and 6.8).

Example 3.6. Take $K = \mathbb{Q}$ and $v$ the 2-adic valuation, so that $\mathbb{F}$ is the field with 2 elements. Let $z \in \overline{\mathbb{F}}$ be a generator of the field with 4 elements.

The type of order one $(y; (x, 1/2, y+1))$ admits $\phi_2 := x^2 + 2$ as a representative. We may enlarge this type to the following higher order types:

$$\mathbf{t} = (y; (x, \tfrac{1}{2}, y+1); (x^2+2, 1, y^2+y+1); (\phi_3, 164, y+z+1)),$$
$$\mathbf{t}^* = (y; (x, \tfrac{1}{2}, y+1); (x^2+2, \tfrac{3}{2}, y+1); (\phi_3^*, \tfrac{1}{2}, y+1); (\phi_4^*, 646, y+1)),$$

where

$$\phi_3 = x^4 + 2x^3 + 4x^2 + 4x + 12,$$
$$\phi_3^* = x^4 + 4x^2 + 8x + 4,$$
$$\phi_4^* = x^8 + 8x^6 + 16x^5 + 24x^4 + 96x^3 + 96x^2 + 128x + 16,$$

have been computed with the procedure of Proposition 3.4 and the slopes and $\psi$-polynomials have been arbitrarily chosen.

**3.3. Equivalence of types.** Let $\mathbf{t}$ be a type of order $r \ge 0$. We saw in section 3.1 that $\mathbf{t}$ determines an inductive valuation $\mu_{\mathbf{t}}$ and a maximal ideal $\mathcal{L}_{\mathbf{t}}$ in $\Delta := \Delta(\mu_{\mathbf{t}})$.

We say that $\mathbf{t}$ is *optimal* if $m_1 < \cdots < m_r$. We say that $\mathbf{t}$ is *strongly optimal* if $m_1 < \cdots < m_r < m_{r+1}$. We agree that a type of order zero is strongly optimal.

LEMMA 3.7. *The type* $\mathbf{t}$ *is optimal if and only if the MacLane chain of* $\mu_{\mathbf{t}}$ *attached to* $\mathbf{t}$ *is optimal. In this case, the order of* $\mathbf{t}$ *coincides with the depth of* $\mu_{\mathbf{t}}$.

*The type* $\mathbf{t}$ *is strongly optimal if and only if* $\mathbf{t}$ *is optimal and* $\mathcal{L}_{\mathbf{t}}$ *is a strong maximal ideal of* $\Delta$.

PROOF. The first statement is an immediate consequence of the definitions.

Let $\mathbf{t}$ be an optimal type with representative $\phi$. By Lemma 3.1, $\phi$ is a key polynomial for $\mu_{\mathbf{t}}$ and $\mathcal{R}(\phi) = \mathcal{L}_{\mathbf{t}}$. Both conditions, $\mathbf{t}$ strongly optimal, and $\mathcal{L}_{\mathbf{t}}$ strong (Definition 2.4), are equivalent to $\deg \phi > m_r(\mu_{\mathbf{t}})$. ☐

The aim of this section is to extend the correspondence $\mathbf{t} \mapsto (\mu_{\mathbf{t}}, \mathcal{L}_{\mathbf{t}})$ to an identification of the MacLane space $\mathbb{M}$ of $(K, v)$ with a quotient set of strongly optimal types classified by a certain equivalence relation.

Denote by $\mathcal{T}$ the set of all types over $(K, v)$ and let $\mathcal{T}^{\mathrm{str}} \subset \mathcal{T}$ be the subset of all strongly optimal types. By Lemma 3.7, we have a well-defined "MacLane map" from $\mathcal{T}^{\mathrm{str}}$ to the MacLane space of $(K, v)$:

$$\mathrm{ml}\colon \mathcal{T}^{\mathrm{str}} \longrightarrow \mathbb{M}, \qquad \mathbf{t} \mapsto (\mu_{\mathbf{t}}, \mathcal{L}_{\mathbf{t}}).$$

This mapping is clearly onto. In fact, for any point $(\mu, \mathcal{L})$ in the MacLane space $\mathbb{M}$ we may consider an optimal MacLane chain of $\mu$:

$$\mu_0 \xrightarrow{\phi_1,\nu_1} \mu_1 \xrightarrow{\phi_2,\nu_2} \cdots \xrightarrow{\phi_{r-1},\nu_{r-1}} \mu_{r-1} \xrightarrow{\phi_r,\nu_r} \mu_r = \mu.$$

Then, with the natural identifications described in Lemma 3.1, this MacLane chain determines almost all data of an optimal type of order $r$:

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_r, \lambda_r, -)),$$

such that $\mu_{\mathbf{t}} = \mu$. Also, the MacLane chain induces the isomorphism $\mathbb{F}_r[y] \simeq \Delta$ of Theorem 1.10, so that $\mathcal{L} = \psi_r(y_r)\Delta$ for some (unique) monic irreducible polynomial $\psi_r \in \mathbb{F}_r[y]$. Hence, the optimal type $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_r, \lambda_r, \psi_r))$ satisfies $\mu_t = \mu$ and $\mathcal{L}_{\mathbf{t}} = \mathcal{L}$. Since $\mathcal{L}$ is a strong maximal ideal, the type $\mathbf{t}$ is strongly optimal by Lemma 3.7.

Our next aim is to describe the fibers of the MacLane map. To this end we consider an equivalence relation on the set $\mathcal{T}^{\mathrm{str}}$ of strongly optimal types.

DEFINITION 3.8. Consider two strongly optimal types of the same order $r$:

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_r, \lambda_r, \psi_r)), \quad \mathbf{t}^* = (\psi_0^*; (\phi_1^*, \lambda_1^*, \psi_1^*); \dots; (\phi_r^*, \lambda_r^*, \psi_r^*)).$$

We say that $\mathbf{t}$ and $\mathbf{t}^*$ are equivalent if they satisfy the following conditions:

(i) $\phi_i^* = \phi_i + a_i$, $\deg a_i < m_i$, $\mu_i(a_i) \ge \mu_i(\phi_i)$, for all $1 \le i \le r$.

(ii) $\lambda_i^* = \lambda_i$ for all $1 \le i \le r$.

(iii) $\psi_i^*(y) = \psi_i(y - \eta_i)$ with $\eta_i$ defined as in (1.5), for all $0 \le i \le r$.

We write $\mathbf{t} \equiv \mathbf{t}^*$ in this case. We denote by $\mathbb{T} = \mathcal{T}^{\mathrm{str}}/\equiv$ the quotient set and we write $[\mathbf{t}] \subset \mathcal{T}^{\mathrm{str}}$ for the class of all types equivalent to $\mathbf{t}$.

Proposition 3.9. *Two strongly optimal types* $\mathbf{t},\mathbf{t}^*$ *are equivalent if and only if* $\mathrm{ml}(\mathbf{t})=\mathrm{ml}(\mathbf{t}^*)$.

Proof. If $\mathbf{t}\equiv\mathbf{t}^*$, then $\mu_{\mathbf{t}}=\mu_{\mathbf{t}^*}$ by Proposition 1.7. Also,

$$\mathcal{L}_{\mathbf{t}^*}=\psi_r^*(y_r^*)\Delta=\psi_r(y_r^*-\eta_r)\Delta=\psi_r(y_r)\Delta=\mathcal{L}_{\mathbf{t}},$$

by Lemma 1.15. Hence, $\mathrm{ml}(\mathbf{t})=\mathrm{ml}(\mathbf{t}^*)$.

Conversely, assume that $\mathrm{ml}(\mathbf{t})=\mathrm{ml}(\mathbf{t}^*)$. From $\mu_{\mathbf{t}}=\mu_{\mathbf{t}^*}$ we deduce by Proposition 1.7 that conditions (i), (ii) from Definition 3.8 hold, and condition (iii) holds for $i<r$. By Lemma 1.15, we have moreover $y_r^*=y_r+\eta_r$. Hence,

$$\psi_r^*(y_r+\eta_r)\Delta=\psi_r^*(y_r^*)\Delta=\mathcal{L}_{\mathbf{t}^*}=\mathcal{L}_{\mathbf{t}}=\psi_r(y_r)\Delta.$$

Since these polynomials are monic, Theorem 1.10 shows that $\psi_r^*(y+\eta_r)=\psi_r(y)$. $\square$

In combination with Theorem 2.8, we get the following result.

Theorem 3.10. *The MacLane and Okutsu maps induce a canonical bijection between the set of equivalence classes of strongly optimal types and the set of Okutsu equivalence classes of prime polynomials:*

$$\mathbb{T}\stackrel{\mathrm{ml}}{\longrightarrow}\mathbb{M}\stackrel{\mathrm{ok}}{\longrightarrow}(\mathbb{P}/\approx).$$

Corollary 3.11. *If* $\phi$ *is a representative of* $\mathbf{t}\in\mathcal{T}^{\mathrm{str}}$*, then* $(\mathrm{ok}\circ\mathrm{ml})([\mathbf{t}])=[\phi]$ *and* $[\phi]\cap\mathcal{O}[x]$ *coincides with the set* $\mathrm{Rep}(\mathbf{t})$ *of all representatives of* $\mathbf{t}$.

Proof. An immediate consequence of Proposition 2.7 and Lemma 3.1,(3). $\square$

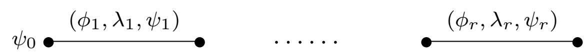
**3.4. Tree structure on the set of types.** Let us introduce a tree structure on the set $\mathcal{T}$ of types. Given two types $\mathbf{t},\mathbf{t}'\in\mathcal{T}$, there is an oriented edge $\mathbf{t}'\to\mathbf{t}$ if and only if $\mathbf{t}'=\mathrm{Trunc}_{r-1}(\mathbf{t})$, where $r$ is the order of $\mathbf{t}$. Thus, we have a unique path of length equal to the order of $\mathbf{t}$:

$$\mathrm{Trunc}_0(\mathbf{t})\longrightarrow\mathrm{Trunc}_1(\mathbf{t})\longrightarrow\cdots\longrightarrow\mathrm{Trunc}_{r-1}(\mathbf{t})\longrightarrow\mathbf{t}. \tag{3.6}$$

The root nodes are the types of order zero. Thus, the connected components of $\mathcal{T}$ are the subtrees $\mathcal{T}_\varphi$ of all types $\mathbf{t}$ with $\mathrm{Trunc}_0(\mathbf{t})=(\varphi)$, for $\varphi$ running on the set $\mathbb{P}(\mathbb{F})$ of all monic irreducible poynomials in $\mathbb{F}[y]$.

The branches of a type $\mathbf{t}$ of order $r$ are parametrized by triples $(\phi,\lambda,\psi)$, where $\phi$ is a representative of $\mathbf{t}$, $\lambda$ is a positive rational number and $\psi\in\mathbb{F}_{r+1}[y]$ is a monic irreducible polynomial such that $\psi\ne y$. Such a triple determines an edge $\mathbf{t}\to\mathbf{t}^*$, where $\mathbf{t}^*=(\mathbf{t};(\phi,\lambda,\psi))$ is the type obtained by enlarging $\mathbf{t}$ with data $(\phi,\lambda,\psi)$ at the $(r+1)$-th level.

Suppose $\mathbf{t}=(\psi_0;(\phi_1,\lambda_1,\psi_1);\dots;(\phi_r,\lambda_r,\psi_r))$. In practice, when we represent a path like (3.6) we omit the labels of the vertices which are not root nodes and we label the edges with the level data.

(3.7)



Also, since the sense of the edges is self-evident, we draw them as lines instead of vectors. We recover the real path (3.6) from its practical representation (3.7) by attaching to each vertex of the path the type obtained by gathering all level data from the previous edges.

All truncates of a strongly optimal type $\mathbf{t}$ are strongly optimal, hence the subset $\mathcal{T}^{\mathrm{str}}\subset\mathcal{T}$ is a full subtree of $\mathcal{T}$. Also, if $\mathbf{t}\equiv\mathbf{t}^*$ are strongly optimal, then

$\mathrm{Trunc}_i(\mathbf{t}) \equiv \mathrm{Trunc}_i(\mathbf{t}^*)$ for all $0 \le i \le r$. Therefore, the tree structure on $\mathcal{T}^{\rm str}$ induces a natural tree structure on the quotient set $\mathbb{T} = \mathcal{T}^{\rm str}/\equiv$.

Since the equivalence relation $\equiv$ only identifies vertices of the same order, a path of length $r$ in $\mathcal{T}^{\rm str}$ determines a path of length $r$ in $\mathbb{T}$.

For types of order zero, $\mathbf{t} \equiv \mathbf{t}^*$ holds only for $\mathbf{t} = \mathbf{t}^*$; thus, the root nodes of $\mathbb{T}$ are in 1-1 correspondence with the set $\mathbb{P}(\mathbb{F})$ too.

The branches of $[\mathbf{t}] \in \mathbb{T}$ are determined by triples $(\phi, \lambda, \psi)$ as above such that $e_\lambda \deg\psi > 1$, where $e_\lambda$ is the least positive denominator of $\lambda$. Two such triples $(\phi, \lambda, \psi)$, $(\phi^*, \lambda^*, \psi^*)$ yield the same branch if and only if $(\mathbf{t}; (\phi, \lambda, \psi)) \equiv (\mathbf{t}; (\phi^*, \lambda^*, \psi^*))$; by Definition 3.8 this is equivalent to

$$\lambda^* = \lambda, \quad \mu_{\mathbf{t}}(\phi - \phi^*) \ge \mu_{\mathbf{t}}(\phi) + \lambda/(e_1 \cdots e_{r-1}), \quad \psi^*(y) = \psi(y - \eta),$$

with $\eta = \eta_{r+1}$ defined as in (1.5) with respect to $\phi_{r+1} = \phi$ and $\phi^*_{r+1} = \phi^*$.

Of course, through the bijective mappings ml and ok we obtain a tree structure on the sets $\mathbb{M}$ and $\mathbb{P}/\approx$ as well.

## 4. OM representations of square-free polynomials

**4.1. OM representations of prime polynomials.** Consider a prime polynomial $F \in \mathbb{P}$ and let $(\mu, \mathcal{L}) \in \mathbb{M}$ be the point in the MacLane space corresponding to the Okutsu equivalence class of $F$; that is, $\mathrm{ok}(\mu, \mathcal{L}) = [F]$.

For any polynomial $\phi \in [F] \cap \mathcal{O}[x]$ the pair $[(\mu, \mathcal{L}), \phi]$ is called an *OM representation* of $F$. If $\phi = F$ we say that the OM representation is *exact*.

By Theorem 3.10 and Corollary 3.11, an OM representation may be handled in a computer as a pair

$$[(\mu, \mathcal{L}), \phi] \quad \leftrightarrow \quad [\mathbf{t}, \phi],$$

where $\mathbf{t}$ is a strongly optimal type of order $r$ such that $\mathrm{ml}([\mathbf{t}]) = (\mu, \mathcal{L})$, and $\phi$ is a representative of $\mathbf{t}$. Note that

$$\mu = \mu_{\mathbf{t}} = \mu_F = \mu_\phi, \qquad \mathcal{L} = \mathcal{L}_{\mathbf{t}} = \mathcal{R}(F) = \mathcal{R}(\phi).$$

The polynomial $\phi$ is a "sufficiently good" approximation to $F$ for many purposes. In a computational context, we propose to manipulate prime polynomials via OM representations $[\mathbf{t}, \phi]$ instead of dealing barely with approximations with a given precision. The discrete data contained in the type $\mathbf{t}$ is a kind of DNA sequence common to all individuals in the Okutsu class $[F]$, and many properties of $F$ and the extension $K_F/K_v$ are described by this genetic data.

This approach has many advantages. It allows to measure the distance between $F$ and $\phi$ by the *quality* of the aproximation instead of the precision (see Lemma 4.1 below). Also, the genetic data of $F$ provide arithmetic information on $F$ and $K_F$ which in the classical approach has to be derived from the approximation $\phi$ by means of extra routines that may have a heavy cost. Further, the genetic information of $F$ is helpful in the construction of approximations with a prescribed quality (section 6.1) and more generally, it leads to a new design of fast routines carrying out basic arithmetic tasks in number fields and function fields (sections 6.6, 6.7). Finally, the constructive procedure of section 3.2 may be used to efficiently construct prime polynomials with prescribed genetic data, or equivalently, with prescribed arithmetic properties.

The algorithmic applications of these ideas are discussed in section 6. Let us now mention a few concrete facts that illustrate some of these advantages. Let $r$ be the Okutsu depth of $F$, $n$ the degree of $F$ and let us fix $\theta \in \overline{K}_v$ a root of $F$.

**Maximal tamely ramified subextensions.** If the residue class field $\mathbb{F}$ is a perfect field and $F$ is a separable polynomial, then the extensions $K_\phi/K_v$ and $K_F/K_v$ have isomorphic maximal tamely ramified subextensions [**4, 15**]. In particular, if $K_\phi/K_v$ is tamely ramified then $K_\phi$ and $K_F$ are isomorphic.

**Okutsu bases.** The ring $\mathcal{O}_F$ is a free $\mathcal{O}_v$-module of rank $n$ and a basis is determined by the genetic information [**15**].

We may express any integer $0 \le m < n$ in a unique way as:

$$m = j_0 + j_1 m_1 + \cdots + j_r m_r, \quad 0 \le j_i < e_i f_i.$$

Consider the following integer $d_m$ and polynomial $g_m$ of degree $m$:

$$d_m = \lfloor j_1(w_1+\nu_1) + \cdots + j_r(w_r+\nu_r)\rfloor, \quad g_m(x) = \phi_0(x)^{j_0}\phi_1(x)^{j_1}\cdots\phi_r(x)^{j_r}.$$

Then, the following family is an $\mathcal{O}_v$-basis of $\mathcal{O}_F$:

$$1,\ \pi^{-d_1}g_1(\theta),\ \dots,\ \pi^{-d_{n-1}}g_{n-1}(\theta).$$

**Okutsu invariants.** All Okutsu invariants of $F$ may be deduced from an OM representation of $F$ by closed formulas. For instance, let us exhibit some more Okutsu invariants, taken from [**14**, Sec. 1], besides $e(F)$, $f(F)$ and $\delta_0(F)$ already mentioned in (2.1).

$$\begin{aligned} &\operatorname{cap}(F) := \operatorname{Max}\{v(g(\theta)) \mid g\in\mathcal{O}[x] \text{ monic, } \deg g < n\} = w_{r+1} - \textstyle\sum_{j=1}^r \nu_j,\\ &\exp(F) := \operatorname{Min}\left\{\delta\in\mathbb{Z}_{\ge 0} \mid \mathfrak{m}^\delta\mathcal{O}_F \subset \mathcal{O}_v[\theta]\right\} = \lfloor \operatorname{cap}(F)\rfloor,\\ &\operatorname{ind}(F) := \operatorname{length}_{\mathcal{O}_v}(\mathcal{O}_F/\mathcal{O}_v[\theta]) = n\left(\operatorname{cap}(F) - 1 + f(F)\right)/2,\\ &\mathfrak{f}(F) := \operatorname{Min}\left\{\delta\in\mathbb{Z}_{\ge 0} \mid (\mathfrak{m}_F)^\delta \subset \mathcal{O}_v[\theta]\right\} = 2\operatorname{ind}(F)/f(F).\end{aligned} \tag{4.1}$$

These numbers are called the *capacity*, *exponent*, *index* and *conductor* of $F$, respectively. The notation $\operatorname{length}_{\mathcal{O}_v}$ indicates length as an $\mathcal{O}_v$-module.

**Quality of an approximation.** There are two typical measures of the distance between $\phi$ and $F$:

$$\nu = \mu_0(F-\phi), \quad \nu' = v(\phi(\theta)) = \mu_{\infty,F}(F-\phi),$$

called the *precision* and the *quality* of the approximation, respectively. The precision is the largest positive integer $\nu$ such that $F \equiv \phi \pmod{\mathfrak{m}^\nu}$, whereas the *quality* is a positive rational number

Usually, $F$ is a prime factor of some given polynomial $f\in\mathcal{O}[x]$. We shall see in section 4.2 that in this case

$$\nu' = w_{r+1} + \nu_{r+1} = \delta_0(F) + \lambda_{r+1}/e(F), \tag{4.2}$$

where $\lambda_{r+1}$ is a positive integer which may be read in $N^-_{r+1}(f) := N^-_{v_r,\phi}(f)$.

The two measures are related by the following inequalities. The first one is obvious and the second one was derived in [**4**, Lem. 4.5].

Lemma 4.1. *For any OM representation* $[\mathbf{t},\phi]$ *of* $F$*, we have*

$$\nu' \ge \nu \ge \nu' - \operatorname{cap}(F) = \nu_1 + \cdots + \nu_r + \nu_{r+1}.$$

Let us exhibit some examples showing that both inequalities are sharp and illustrating that $\nu'$ is a better measure than $\nu$ of the distance between $F$ and $\phi$.

**Examples.** If $\phi = F + \pi^m$, then $\nu = m = \nu'$ and the first inequality of Lemma 4.1 is sharp. If the Okutsu depth of $F$ is $r \ge 1$ and we take $\phi = F + \pi^m \phi_1^{(n/m_1)-1}$, then $\nu = m$, whereas the quality

$$\nu' = m + ((n/m_1) - 1)v(\phi_1(\theta)) = \nu + ((n/m_1) - 1)\nu_1$$

can be much larger than $\nu$ if $n/m_1$ and/or $\nu_1$ are large.

For instance, the prime polynomial $F = x^2 + \pi$ is a representative of the type $\mathbf{t} = (y; (x, 1/2, y + 1))$; hence, it has invariants $m_1 = 1$, $e_1 = 2$, $f_1 = h_1 = 1 = w_2$ and $\operatorname{cap}(F) = w_2 - \nu_1 = 1/2$. For the approximation $\phi = x^2 + \pi^m x + \pi$ we have $\nu' = m + \nu_1 = \nu + (1/2)$, so that the second inequality of Lemma 4.1 is sharp. We deduce that $\nu_2 = m - (1/2)$ and $\lambda_2 = 2m - 1$.

**4.2. OM representation of a square-free polynomial.** Let $f = F_1 \cdots F_t$ be the prime factorization in $\mathcal{O}_v[x]$ of a square-free monic polynomial $f \in \mathcal{O}[x]$. For each $1 \le j \le t$, let $r_j$ be the Okutsu depth of $F_j$ and $\theta_j \in \overline{K}_v$ a root of $F_j$.

For a prime polynomial $F \in \mathbb{P}$, we denote by $\mathbf{t}_F$ any strongly optimal type whose equivalence class corresponds to the Okutsu class of $F$ under the mapping $\mathrm{ok} \circ \mathrm{ml}$ of Theorem 3.10. That is,

$$[\mathbf{t}_F] = (\mathrm{ok} \circ \mathrm{ml})^{-1}([F]) \in \mathbb{T}.$$

Definition 4.2. We denote by $\mathbb{T}(F) \subset \mathbb{T}$ the unibranch tree determined by the path joining $[\mathbf{t}_F]$ with its root node in $\mathbb{T}$. The *genomic tree* of $f$ is the finite tree $\mathbb{T}(f) := \mathbb{T}(F_1) \cup \cdots \cup \mathbb{T}(F_t) \subset \mathbb{T}$.

An OM representation of $f$ is an object which gathers the information provided by a family of OM representations of the prime factors. The approximations to the prime factors contained in all these OM representations constitute an approximate factorization of $f$ in $\mathcal{O}_v[x]$. Since we are only interested in approximate factorizations which are able to distinguish the different prime factors of $f$, we are led to consider the so-called *OM factorizations* of $f$.

Definition 4.3. Let $g, h \in \mathcal{O}[x]$ be monic polynomials with prime factorizations $g = G_1 \cdots G_s$, $h = H_1 \cdots H_{s'}$ in $\mathcal{O}_v[x]$. We say that $g$ and $h$ are *Okutsu equivalent*, and we write $g \approx h$, if $s = s'$ and $G_j \approx H_j$ for all $1 \le j \le s$, up to ordering.

An expression of the form, $g \approx P_1 \cdots P_s$, with $P_1, \dots, P_s \in \mathbb{P} \cap \mathcal{O}[x]$ is called an *Okutsu factorization* of $g$.

Clearly, every $g \in \mathcal{O}[x]$ admits a unique (up to $\approx$) Okutsu factorization. However, we need a stronger concept for our purposes. For instance, if all factors of $g$ are Okutsu equivalent to $P$, then $g \approx P^t$ is an Okutsu factorization of $g$ which is unable to distinguish the true prime factors of $g$.

Definition 4.4. We say that $P_j \in [F_j]$ is a *Montes approximation to $F_j$ as a factor of $f$* if $v(P_j(\theta_j)) > v(P_j(\theta_k))$ for all $k \ne j$.

An *OM factorization* of $f$ is an Okutsu factorization $f \approx P_1 \cdots P_t$ such that each approximate factor $P_j$ is a Montes approximation to $F_j$ as a factor of $f$.

Let $f \approx P_1 \cdots P_t$ be an OM factorization of $f$. By Corollary 3.11, $P_j$ is a representative of $\mathbf{t}_{F_j}$ and $[\mathbf{t}_{F_j}, P_j]$ is an OM representation of $F_j$ for all $j$.

In [**2**, Sec. 3.1] it is shown that the types $\mathbf{t}_{F_j}$ may be extended to types

$$\mathbf{t}_j := \left(\mathbf{t}_{F_j}; (P_j, \lambda_{r_j+1,j}, \psi_{r_j+1,j})\right) \quad \text{or} \quad \mathbf{t}_j := \left(\mathbf{t}_{F_j}; (P_j, \infty, -)\right),$$

according to $P_j \ne F_j$ or $P_j = F_j$, respectively. These types of order $r_j+1$ satisfy

$$\operatorname{ord}_{\mathbf{t}_j}(F_j)=1, \quad \mathbf{t}_j \nmid F_k, \quad \text{for all } 1\le k\ne j\le t.$$

The quality of the approximations $P_j \approx F_j$ is given by the formula:

$$v(P_j(\theta_j)) = \delta_0(F_j) + \lambda_{r_j+1,j}/e(F_j).$$

If $P_j \nmid f$, the slope $\lambda_{r_j+1,j}$ is an integer which may be computed as the largest slope (in absolute value) of $N^-_{r_j+1}(f) = N^-_{v_{r_j},P_j}(f)$. This slope corresponds to a side whose end points have abscissas 0 and 1 (see Figure 4). Hence, $R_{r_j+1}(f) := R_{v_{r_j},P_j,\lambda_{r_j+1}}(f)$ has degree one and $\psi_{r_j+1,j}$ is equal to $R_{r_j+1}(f)$ divided by its leading coefficient.

The types $\mathbf{t}_j$ are optimal, but not strongly optimal because $e_{r_j+1} = f_{r_j+1} = 1$, so that $m_{r_j+2} = m_{r_j+1} = \deg F_j$.

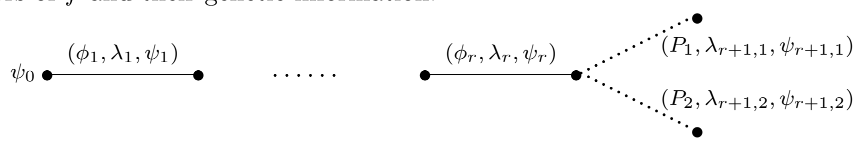
Definition 4.5. Let $T(f) \subset \mathcal{T}^{\rm str}$ be a faithful preimage of the genomic tree of $f$; that is, $T(f)$ maps to $\mathbb{T}(f)$ under the quotient map $\mathcal{T}^{\rm str} \to \mathbb{T}$, and the vertices of $T(f)$ are pairwise inequivalent.

An *OM representation* of $f$ is the tree obtained by enlarging $T(f)$ with the $t$ new vertices $\mathbf{t}_j$ and edges $\mathbf{t}_{F_j} \to \mathbf{t}_j$ determined by some OM factorization of $f$.

The leaves of an OM representation of $f$ are in 1-1 correspondence with the prime factors of $f$, whereas the root nodes are in 1-1 correspondence with the monic irreducible factors of $\overline{f}$ in $\mathbb{F}[y]$. Let us see some examples where $\overline{f}$ is supposed to be a power of an irreducible polynomial in $\mathbb{F}[y]$, so that the OM representation of $f$ is a connected tree.

Let $f = F_1F_2$ be a polynomial with two Okutsu equivalent prime factors. Then, $[\mathbf{t}_{F_1}] = [\mathbf{t}_{F_2}]$ and the genomic tree $\mathbb{T}(f) = \mathbb{T}(F_1) = \mathbb{T}(F_2)$ is a unibranch tree as in (3.7). It contains the genetic information of all prime factors of $f$, but it does not make apparent how to distinguish these factors.

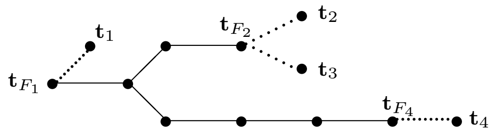
An OM representation of $f$ gives a more precise view of the different prime factors of $f$ and their genetic information:




We represent the edges $\mathbf{t}_{F_j} \to \mathbf{t}_j$ with dotted lines to emphasize that the leaves $\mathbf{t}_j$ are not strongly optimal types.

In general, the vertices $\mathbf{t}_{F_i}$ are not necessarily leaves of the tree $T(f)$. It may happen that $\mathbf{t}_{F_i}$ concides with a vertex in the path joining $\mathbf{t}_{F_j}$ with its root node for some $j \ne i$. Thus, the leaves of an OM representation of $f$ may sprout from arbitrary vertices in $T(f)$. For instance, in the next example $f$ has four prime factors; the vertex $\mathbf{t}_{F_1}$ has order 0, $\mathbf{t}_{F_2} = \mathbf{t}_{F_3}$ have order 3 and $\mathbf{t}_{F_4}$ has order 5.

(4.3)




We define the *index of coincidence* $i([\mathbf{t}], [\mathbf{t}'])$ between two vertices $[\mathbf{t}], [\mathbf{t}'] \in \mathbb{T}$, as follows. If they have different root nodes we agree that $i([\mathbf{t}], [\mathbf{t}']) = 0$; otherwise, we take $i([\mathbf{t}],[\mathbf{t}'])=1+\ell$, where $\ell$ is the length of the intersection of the two paths joining $[\mathbf{t}]$ and $[\mathbf{t}']$ with their common root node.

We may extend this notion to prime polynomials. If $F,G\in\mathbb{P}$, we define $i(F,G)$ as the index of coincidence of $[\mathbf{t}_F]$ and $[\mathbf{t}_G]$ as vertices of $\mathbb{T}$. For instance, in (4.3) we have $i(F_1,F_1)=i(F_1,F_2)=i(F_1,F_3)=i(F_1,F_4)=1$, $i(F_2,F_2)=i(F_2,F_3)=i(F_3,F_3)=4$, $i(F_2,F_4)=i(F_3,F_4)=2$, and $i(F_4,F_4)=6$.

We say that a leaf of an OM representation of $f$ is *isolated* if the previous node has only one branch. For instance, in (4.3) the leaf corresponding to $F_4$ is isolated and the other three leaves are not isolated.

## 5. Computation of the genetics of a polynomial: the Montes algorithm

In this section, we describe the OM factorization algorithm developed by Montes in 1999, inspired by the ideas of Ore and MacLane [**13**]. It was first published in [**5**], based on the theoretical background developed in [**6**]. In the context of this paper, the aim of the Montes algorithm is the computation of an OM representation of a given square-free polynomial $f\in\mathcal{O}[x]$.

Let $\mathcal{P}=\{F_1,\dots,F_t\}$ be the set of prime factors of $f$ in $\mathcal{O}_v[x]$. For any type $\mathbf{t}$ we denote

$$\mathcal{P}_{\mathbf{t}}=\{F\in\mathcal{P}\mid \mathbf{t}\mid F\}\subset\mathcal{P}.$$

Since $\operatorname{ord}_{\mathbf{t}}(f)=\sum_{1\le j\le t}\operatorname{ord}_{\mathbf{t}}(F_j)$, the set $\mathcal{P}_{\mathbf{t}}$ is empty if and only if $\mathbf{t}\nmid f$. Also, if $\operatorname{ord}_{\mathbf{t}}(f)=1$, then there is an index $j$ such that $\operatorname{ord}_{\mathbf{t}}(F_j)=1$ and $\operatorname{ord}_{\mathbf{t}}(F_k)=0$ for all $k\ne j$; thus, $\mathcal{P}_{\mathbf{t}}=\{F_j\}$ is a one-element subset in this case.

The Montes algorithm is based on Theorem 2.3. The idea is to detect successive dissections of the set $\mathcal{P}$ by subsets of the form $\mathcal{P}_{\mathbf{t}}$ for adequate types. The first dissection is derived from the factorization $\overline{f}=\prod_\varphi\varphi^{\omega_\varphi}$ into the product of powers of pairwise different irreducible factors in $\mathbb{F}[y]$. Each irreducible factor $\varphi$ determines a type of order zero $\mathbf{t}_\varphi=(\varphi)$ and the subset $\mathcal{P}_{\mathbf{t}_\varphi}$ contains all prime factors of $f$ whose reduction modulo $\mathfrak{m}$ is a power of $\varphi$. By Hensel's lemma, we obtain a partition $\mathcal{P}=\bigcup_\varphi\mathcal{P}_{\mathbf{t}_\varphi}$.

In order to dissect $\mathcal{P}_{\mathbf{t}_\varphi}$, we choose a representative $\phi$ of $\mathbf{t}_\varphi$; that is, a monic lifting of $\varphi$ to $\mathcal{O}[x]$. By Lemma 1.5 and Corollary 1.14, $\omega_\varphi=\operatorname{ord}_{\mathbf{t}_\varphi}(f)$ is the length of the principal Newton polygon $N^-_{v_0,\phi}(f)$; thus, in order to compute this polygon we need only to compute the first $\omega_\varphi+1$ coefficients of the $\phi$-expansion of $f$. Then, for each slope $-\lambda$ of a side of $N^-_{v_0,\phi}(f)$ we compute the residual polynomial $R_{v_0,\phi,\lambda}(f)\in\mathbb{F}_1[y]=\mathbb{F}/(\varphi)[y]$. Finally, for each monic irreducible factor $\psi$ of $R_{v_0,\phi,\lambda}(f)$ in $\mathbb{F}_1[y]$ we consider the type of order one $\mathbf{t}_{\lambda,\psi}=(\varphi;(\phi,\lambda,\psi))$. By definition, $\operatorname{ord}_{\mathbf{t}_{\lambda,\psi}}(f)=\operatorname{ord}_\psi(R_{v_0,\phi,\lambda}(f))>0$, so that the subsets $\mathcal{P}_{\mathbf{t}_{\lambda,\psi}}$ are not empty. By Theorem 2.3, $\mathcal{P}_{\mathbf{t}_\varphi}=\bigcup_{\lambda,\psi}\mathcal{P}_{\mathbf{t}_{\lambda,\psi}}$ is a partition.

Each subset $\mathcal{P}_{\mathbf{t}_{\lambda,\psi}}$ is furtherly dissected by types obtained as enlargements of $\mathbf{t}_{\lambda,\psi}$ with a similar procedure. By a certain process of *refinement*, the algorithm is able to perform all these dissections dealing only with strongly optimal types.

As mentioned above, when we reach a type $\mathbf{t}$ with $\operatorname{ord}_{\mathbf{t}}(f)=1$, then $\mathcal{P}_{\mathbf{t}}=\{F_j\}$ singles out a prime factor of $f$.

Let us briefly review the relevant subroutines which are used.

`Factorization(`$\mathcal{F}$`,` $\varphi$`)`

Factorization of $\varphi\in\mathcal{F}[y]$ into a product of irreducible polynomials in $\mathcal{F}[y]$.

`Newton(`$\mathbf{t}$`,` $\omega$`,` $g$`)`

The type $\mathbf{t}$ of order $i$ is equipped with a representative $\phi$. The routine computes the first $\omega+1$ coefficients $a_0,\dots,a_\omega$ of the canonical $\phi$-expansion $g=\sum_{0\le s} a_s\phi^s$, and the Newton polygon of the set of points $(s, v_i(a_s\phi^s))$ for $0\le s\le\omega$.

`ResidualPolynomial(`$\mathbf{t}$`,` $\lambda$`,` $g$`)`
The type $\mathbf{t}$ of order $i-1$ is equipped with a representative $\phi$. The routine computes the residual polynomial $R_{v_{i-1},\phi,\lambda}(g)\in\mathbb{F}_i[y]$.

`Representative(`$\mathbf{t}$`)`
Computation of a representative of $\mathbf{t}$ by the procedure described in section 3.2.

We now describe the Montes algorithm in pseudocode. Along the process of enlarging types by adding new level data, the order of a type $\mathbf{t}$ is the largest level $i$ for which all three fundamental invariants $(\phi_i,\lambda_i,\psi_i)$ are assigned. We emphasize the type to which a certain level data belongs as a superindex: $\phi_i^{\mathbf{t}}$, $\lambda_i^{\mathbf{t}}$, $\psi_i^{\mathbf{t}}$, etc.

**MONTES' ALGORITHM**

INPUT:

– A discrete valued field $(K,v)$ with valuation ring $\mathcal{O}$.
– A monic square-free polynomial $f\in\mathcal{O}[x]$.

**1** Initialize an empty list `Forest`

**2** `Factorization(`$\mathbb{F}$`,`$\overline{f}$`)`

**3** FOR each monic irreducible factor $\varphi$ of $\overline{f}$ DO

**4** Take a monic lifting $\phi\in\mathcal{O}[x]$ of $\varphi$ and create a type $\mathbf{t}$ of order zero with
$\psi_0^{\mathbf{t}}\leftarrow\varphi,\quad \omega_1^{\mathbf{t}}\leftarrow\operatorname{ord}_\varphi\overline{f},\quad \phi_1^{\mathbf{t}}\leftarrow\phi,\quad \mathbb{F}_1^{\mathbf{t}}\leftarrow\mathbb{F}[y]/(\varphi)$

**5** Initialize a tree of types $T_\varphi$ having $\mathbf{t}$ as the unique vertex
Initialize a stack `BranchNodes`$=[\mathbf{t}]$
**WHILE** #`BranchNodes` $>0$ **DO**

**6** Extract a type $\mathbf{t}_0$ from `BranchNodes`. Let $i-1$ be its order

**7** IF $\phi_i^{\mathbf{t}_0}\mid f$ THEN $f\leftarrow f/\phi_i^{\mathbf{t}_0}$ and add the leaf $(\mathbf{t}_0;(\phi_i^{\mathbf{t}_0},\infty,-))$ to $T_\varphi$

**8** $N\leftarrow$ `Newton(`$\mathbf{t}_0$`,` $\omega_i^{\mathbf{t}_0}$`,` $f$`)`

**9** FOR every side $S$ of $N$ DO

**10** $\lambda_i^{\mathbf{t}_0}\leftarrow -$slope of $S$, $R_i(f)\leftarrow$ `ResidualPolynomial(`$\mathbf{t}_0$`,` $\lambda_i^{\mathbf{t}_0}$`,` $f$`)`

**11** `Factorization(`$\mathbb{F}_i^{\mathbf{t}_0}$`,` $R_i(f)$`)`

**12** FOR every monic irreducible factor $\psi$ of $R_i(f)$ DO

(a) Set $\mathbf{t}\leftarrow\mathbf{t}_0$ and extend $\mathbf{t}$ to an order $i$ type by setting
$\psi_i^{\mathbf{t}}\leftarrow\psi,\quad \mathbb{F}_{i+1}^{\mathbf{t}}\leftarrow\mathbb{F}_i^{\mathbf{t}}[y]/(\psi)$

(b) IF $\omega_i^{\mathbf{t}_0}=1$ THEN add the leaf $\mathbf{t}=\left(\mathbf{t}_0;(\phi_i^{\mathbf{t}},\lambda_i^{\mathbf{t}},\psi_i^{\mathbf{t}})\right)$ to $T_\varphi$
and go to step **6**

(c) $\omega_{i+1}^{\mathbf{t}}\leftarrow\operatorname{ord}_\psi R_i(f)$, $\phi_{i+1}^{\mathbf{t}}\leftarrow$ `Representative(`$\mathbf{t}$`)`

(d) IF $\deg\phi_{i+1}^{\mathbf{t}}>\deg\phi_i^{\mathbf{t}}$ THEN
add the vertex $\mathbf{t}=\left(\mathbf{t}_0;(\phi_i^{\mathbf{t}},\lambda_i^{\mathbf{t}},\psi_i^{\mathbf{t}})\right)$ to $T_\varphi$
ELSE $\phi_i^{\mathbf{t}}\leftarrow\phi_{i+1}^{\mathbf{t}},\quad \omega_i^{\mathbf{t}}\leftarrow\omega_{i+1}^{\mathbf{t}}$
and delete the $(i+1)$-th level of $\mathbf{t}$

(e) Add $\mathbf{t}$ to `BranchNodes`

**END WHILE**

**13** Add the tree $T_\varphi$ to the list `Forest`

OUTPUT:

− The list `Forest` of connected trees is an OM representation of $f$.

The arguments of [**5**] show that the algorithm terminates and has the right output. In that paper it was assumed that $K$ was a number field, but the arguments are valid for an arbitrary discrete valued field $(K, v)$. However, the design of the algorithm we present here has some changes with respect to the original design. Therefore, it may be worth clarifying some aspects on the flow and the output of the algorithm.

Let $T$ be the output OM representation of $f$. The forest $T$ is the disjoint union of connected trees $T_\varphi$ attached to the different irreducible factors $\varphi$ of $\overline{f}$ in $\mathbb{F}[y]$.

Remark 5.1. (1) An element in the list `BranchNodes` is a vertex of $T_\varphi$, represented by a strongly optimal type $\mathbf{t}_0$ of order $i-1$, together with attached data $\phi_i^{\mathbf{t}_0}$ and $\omega_i^{\mathbf{t}_0}$ at the $i$-th level. It may happen that different elements in `BranchNodes` have the same underlying vertex $\mathbf{t}_0$ of $T_\varphi$.

In step **12** we construct a type $\mathbf{t}_{\lambda,\psi} := \mathbf{t} = (\mathbf{t}_0; (\phi, \lambda, \psi))$ of order $i$ and we compute $\omega_{\lambda,\psi} := \omega_{i+1}^{\mathbf{t}} = \operatorname{ord}_{\mathbf{t}}(f)$ and a representative $\phi_{\lambda,\psi} := \phi_{i+1}^{\mathbf{t}}$. By Theorem 2.3, we have a partition $\mathcal{P}_{\mathbf{t}_0} = \bigcup_{\lambda,\psi} \mathcal{P}_{\mathbf{t}_{\lambda,\psi}}$.

If $\deg \phi_{\lambda,\psi} > \deg \phi$, then $\mathbf{t}_{\lambda,\psi}$ yields a new vertex of $T_\varphi$ with previous node $\mathbf{t}_0$. If $\deg \phi_{\lambda,\psi} = \deg \phi$, then $\mathbf{t}_{\lambda,\psi}$ is not strongly optimal and it cannot be a vertex of $T_\varphi$. However, the subset $\mathcal{P}_{\mathbf{t}_{\lambda,\psi}} \subset \mathcal{P}$ cannot be neglected. The algorithm adds to the list `BranchNodes` the vertex corresponding to the type $\mathbf{t}_0$ of order $i-1$ with data $\phi_{\lambda,\psi}$, $\omega_{\lambda,\psi}$ at the $i$-th level. This is called a *refinement step*. In a future iteration of the WHILE loop the branches of this node will determine a partition of the old set $\mathcal{P}_{\mathbf{t}_{\lambda,\psi}}$ [**5**, Sec. 3.2].

Note that a vertex $\mathbf{t}_0$ may sprout some branches of $T_\varphi$ in a WHILE loop and then sprout some other branches in a future iteration of the WHILE loop, derived from a refinement step. These new branches of $\mathbf{t}_0$ may again either lead to new vertices of $T_\varphi$ or to further refinement steps.

(2) In the original design of the algorithm in [**5**], all leaves of $T$ were isolated, at the price of admitting leaves represented by types of order $r+2$, where $r$ is the Okutsu depth of the corresponding prime factor of $f$ [**4**, Thm. 4.2].

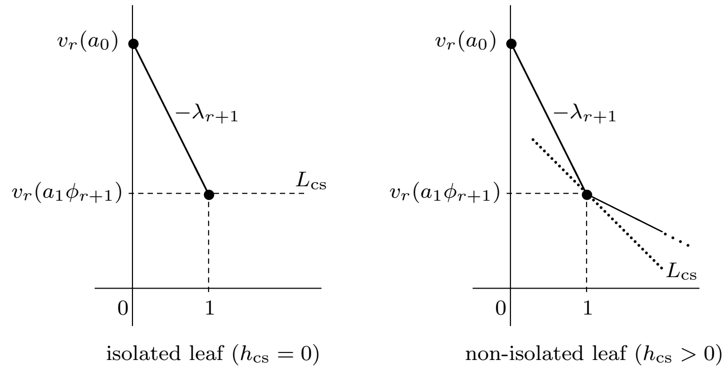
Since we want all leaves to have order $r+1$, we must admit non-isolated leaves. The algorithm stores a *cutting slope* $h_{\rm cs}$ as a "secondary datum" of each type $\mathbf{t}$ representing a leaf. This is a non-negative integer which vanishes if and only if the leaf is isolated. The Newton polygon $N_{r+1}^-(f)$ determined by $\mathbf{t}$ has a first side of slope $-\lambda_{r+1} < -h_{\rm cs}$ whose end points have abscissas 0 and 1. All other sides of the polygon have slope greater than or equal to $-h_{\rm cs}$ (see Figure 4).

In [**7**, Sec. 1.3] a description may be found of some more secondary data stored in the types of an OM representation of $f$, which have been ignored in the pseudocode description of the algorithm.

(3) For any type $\mathbf{t} \in T$ the prime factors of $f$ in $\mathcal{P}_{\mathbf{t}}$ correspond to the leaves of $T$ for which $\mathbf{t}$ is one of the vertices in the path joining the leaf with its root node.

The only algorithmic assumptions on the fields $K$, $\mathbb{F}$ for the algorithm to work properly are the existence of efficient routines for the division with remainder of

FIGURE 4. Newton polygon $N^-_{r+1}(f)$ determined by a leaf of $T$. The line $L_{\rm cs}$ has slope $-h_{\rm cs}$ and $f=\sum_{0\le s} a_s\phi_{r+1}^s$.




polynomials in $\mathcal{O}[x]$ and the factorization of polynomials over finite extensions of the residue class field $\mathbb{F}$. The performance will depend as well on the efficiency of these two tasks. We have not yet analyzed the complexity of the algorithm in the general case, but for $\mathbb{F}$ a finite field, the following complexity estimation was obtained in [**2**, Thm. 5.14].

THEOREM 5.2. *If $\mathbb{F}$ is a finite field, the complexity of the Montes algorithm, measured in number of operations in $\mathbb{F}$ is*

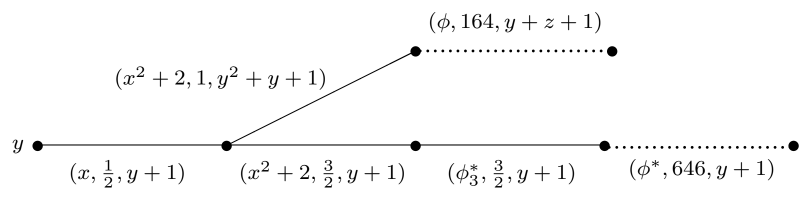
$$O\left(n^{2+\epsilon}+n^{1+\epsilon}(1+\delta)\log(q)+n^{1+\epsilon}\delta^{2+\epsilon}\right),$$

*where $q=\#\mathbb{F}$, $n=\deg f$ and $\delta:=v(\mathrm{Disc}(f))$.*

EXAMPLE 5.3. Take $K=\mathbb{Q}$ and $v$ the 2-adic valuation. Let $\phi:=\phi_3$ and $\phi^*:=\phi_4^*$ be the polynomials introduced in Example 3.6. Consider the polynomial

$$\begin{aligned} f=\phi\phi^*+2^{50}= \;& x^{12}+2x^{11}+12x^{10}+36x^9+100x^8+240x^7+544x^6+992x^5\\ &+1328x^4+2080x^3+1728x^2+1600x+1125899906842816. \end{aligned}$$

The Montes algorithm computes the following OM representation of $f$:




The polynomial $f$ has two prime factors in $\mathbb{Z}_2[x]$, say $f=FF^*$, with Okutsu depths $2,3$. The types $\mathbf{t}$, $\mathbf{t}^*$ of Example 3.6 are OM representations of $F$, $F^*$, respectively.

The numerical MacLane-Okutsu invariants of $F$ are:

$$\begin{array}{llllll} m_1=1, & e_1=2, & h_1=1, & f_1=1, & w_1=0, & \nu_1=1/2,\\ m_2=2, & e_2=1, & h_2=1, & f_2=2, & w_2=1, & \nu_2=1/2. \end{array}$$

The numerical MacLane-Okutsu invariants of $F^*$ are:

$$\begin{array}{llllll} m_1^*=1, & e_1^*=2, & h_1^*=1, & f_1^*=1, & w_1^*=0, & \nu_1^*=1/2,\\ m_2^*=2, & e_2^*=2, & h_2^*=3, & f_2^*=1, & w_2^*=1, & \nu_2^*=3/4,\\ m_3^*=4, & e_3^*=2, & h_3^*=1, & f_3^*=1, & w_3^*=7/2, & \nu_3^*=1/8. \end{array}$$

The formulas (4.1) allow us to compute the Okutsu invariants of both factors from these data. For instance,

$$\begin{array}{lllll} e(F)=2, & f(F)=2, & \delta_0(F)=3, & \operatorname{cap}(F)=2, & \operatorname{ind}(F)=3,\\ e(F^*)=8, & f(F^*)=1, & \delta_0(F^*)=29/4, & \operatorname{cap}(F^*)=47/8, & \operatorname{ind}(F^*)=20. \end{array}$$

We know that $f\approx\phi\phi^*$ is an OM factorization of $f$. The qualities of the approximations $\phi\approx F$, $\phi*\approx F^*$ are given by the formula (4.2). The slopes of the last levels of the OM representations are $\lambda_3=164$ and $\lambda_4^*=646$. We obtain:

$$\mu_{\infty,F}(\phi)=44, \qquad \mu_{\infty,F^*}(\phi^*)=47.$$

The estimation of Lemma 4.1 gives in both cases that the precision is at least 42.

## 6. Algorithmic applications of polynomial genetics

We proceed to illustrate how to use the genetic data to solve some typical problems related to polynomials over local fields. The algorithms exploit the connection of some concrete problem with the genetics of certain polynomials over local fields. This leads to an excellent practical performance.

**6.1. Single-factor lifting and $v$-adic factorization.** Let $f\in\mathcal{O}[x]$ be a monic square-free polynomial and let $f=F_1\cdots F_t$ be its factorization into a product of prime polynomials in $\mathcal{O}_v[x]$.

A *$v$-adic factorization* of $f$ is an approximate factorization with a prescribed precision; that is, a family of monic polynomials $P_1,\dots,P_t\in\mathcal{O}[x]$ such that $P_j\equiv F_j \pmod{\mathfrak{m}^\nu}$ for all $0\le j\le t$, for a prescribed positive integer $\nu$.

For many purposes, one needs sometimes to find an approximation with a prescribed quality to a single prime factor $F$ of $f$. This is the aim of the *single-factor lifting algorithm* [**9**], abbreviated as SFL in what follows. The algorithm of [**9**] was based on the original design of the Montes algorithm in which all trees of the output tree were isolated. Therefore, we review the design of SFL in some detail in order to show its adaptation to the present version of the Montes algorithm.

The starting point of SFL is a leaf $\mathbf{t}$ of an OM representation of $f$

$$\mathbf{t}=(\psi_0;(\phi_1,\lambda_1,\psi_1);\dots;(\phi_r,\lambda_r,\psi_r);(\phi_{r+1},\lambda_{r+1},\psi_{r+1})) \tag{6.1}$$

computed by the Montes algorithm. Let $F$ be the prime factor of $f$ singled out by $\mathbf{t}$, and let $\theta\in\overline{K}_v$ be a root of $F$. We denote

$$V:=V_{r+1},\quad \phi:=\phi_{r+1},\quad h_\phi:=\lambda_{r+1}=h_{r+1},\quad e:=e(F)=e_1\cdots e_r.$$

The polynomial $\phi$ is a Montes approximation to $F$ as a factor of $f$. By (4.2), the quality of the approximation is:

$$v(\phi(\theta))=(V+h_\phi)/e=\delta_0(F)+h_\phi/e.$$

The main loop of SFL computes a new Montes approximation $\Phi$ such that

$$h_\Phi\ge 2h_\phi-h_{\rm cs}.$$

The Newton polygon $N^-_{v_r,\Phi}(f)$ coincides with $N^-_{v_r,\phi}(f)$ except for the side of largest slope (in absolute value) $-h_\Phi$, whose end points have abscissas 0 and 1 (see Figure

4). In particular, the cutting slope $h_{\rm cs}$ of $\mathbf{t}$ separates again this initial side from the rest of the sides. Therefore, we may apply the SFL loop to $\Phi$ and iterate the procedure until we get a Montes approximation $\Phi$ with $h_\Phi$ large enough. By Lemma 4.1, if $h_\Phi \ge e(\nu+\operatorname{cap}(F)-\delta_0(F))$, then $\Phi\equiv F \pmod{\mathfrak{m}^\nu}$.

After $k$ iterations of the SFL loop we get a Montes approximation $\Phi_k$ with

$$h_{\Phi_k} \ge h_\phi + (2^k-1)(h_\phi - h_{\rm cs}).$$

Hence, for a given positive integer $H$, the number of iterations of the SFL loop that are needed to get $h_{\Phi_k}\ge H$ is $\lceil \log_2((H-h_{\rm cs})/(h_\phi-h_{\rm cs}))\rceil$.

Let us briefly explain how to construct $\Phi$ from $\phi$. Consider the first two coefficients $a_0$, $a_1$ of the $\phi$-expansion of $f$:

$$f = q\phi + a_0, \quad a_1 = q \pmod{\phi}.$$

A look at Figure 4 shows that $v_r(a_0)=v_r(a_1)+V+h_\phi$. Let $\alpha\in\overline{K}_v$ be a root of $\phi$ and let $K_\phi=K_v(\alpha)$, $\mathcal{O}_\phi$ the valuation ring of $K_\phi$ and $\mathfrak{m}_\phi$ the maximal ideal. Since $\deg a_0, \deg a_1 < \deg\phi$, we have $\phi\nmid_{\mu_r} a_0$, $\phi\nmid_{\mu_r} a_1$, and Theorem 2.1 shows that $v(a_0(\alpha))=v_r(a_0)/e$, $v(a_1(\alpha))=v_r(a_1)/e$.

The following theorem is a slight variation of [**9**, Thm. 5.1], where it was supposed that the leaf $\mathbf{t}$ was isolated and $h_{\rm cs}=0$.

Theorem 6.1. *Let $a\in\mathcal{O}[x]$ be a polynomial with $\deg a<\deg\phi$ and consider an integer $h_{\rm cs}<h\le h_\phi$. Then, $\Phi:=\phi+a$ is a Montes approximation to $F$ with $h_\Phi\ge 2h-h_{\rm cs}$ if and only if $a(\alpha)\equiv a_0(\alpha)/a_1(\alpha)$ $\left(\bmod\ \mathfrak{m}_\phi^{V+2h-h_{\rm cs}}\right)$.*

Let us show how to find a polynomial $a\in\mathcal{O}[x]$ satisfying the condition of Theorem 6.1. Compute a polynomial $\Psi\in K[x]$ with $\deg\Psi<n_F=\deg F=\deg\phi$ and $v_r(\Psi)=-v_r(a_1)$ [**9**, Lem. 4.8]. Multiply then,

$$A_0 := a_0\Psi \pmod{\phi}, \quad A_1 := a_1\Psi \pmod{\phi}.$$

Clearly, $a_0(\alpha)/a_1(\alpha)=A_0(\alpha)/A_1(\alpha)$, $v(A_0(\alpha))=(V+h_\phi)/e$ and $v(A_1(\alpha))=0$, so that $A_1(\alpha)$ is invertible in $\mathcal{O}_\phi$. In order to compute $a\in\mathcal{O}[x]$, it suffices to find an element $A_1^{-1}(\alpha)\in K_\phi$ with $A_1^{-1}(\alpha)A_1(\alpha)\equiv 1 \mod (\mathfrak{m}_\phi)^{h_\phi-h_{\rm cs}}$ and then take $a(x)\in K[x]$ to be the unique polynomial of degree less than $n_F$ satisfying $a(\alpha)=A_0(\alpha)A_1^{-1}(\alpha)$. By the formulas in (4.1) we have $v(a(\alpha))>\exp(F)=\exp(\phi)$, so that $a(x)\in\mathcal{O}[x]$.

In order to avoid inversions in $K_\phi$, we may compute the approximation $A_1^{-1}(\alpha)$ to $A_1(\alpha)^{-1}$ by the classical Newton iteration:

$$x_{k+1}=x_k(2-A_1(\alpha)x_k),$$

starting with a lift $x_0\in\mathcal{O}_\phi$ of the inverse of $A_1(\alpha)+\mathfrak{m}_\phi$ in the residue field $\mathcal{O}_\phi/\mathfrak{m}_\phi$. In [**7**, Sec. 4.2] it is explained how to compute $x_0$.

**SINGLE-FACTOR LIFTING**

INPUT:

– A discrete valued field $(K,v)$ with valuation ring $\mathcal{O}$.
– A monic square-free polynomial $f\in\mathcal{O}[x]$.
– A leaf $\mathbf{t}$ of order $r+1$, as in (6.1), of an OM representation of $f$.
– A positive integer $H$.

**1** $\phi\leftarrow\phi_{r+1}$, $q,a_0\leftarrow \operatorname{quotrem}(f,\phi)$, $a_1\leftarrow q \pmod{\phi}$

**2** $h_\phi\leftarrow v_r(a_0)-v_r(a_1\phi)$

**3** Find $\Psi \in K[x]$ with $\deg \Psi < \deg \phi$ and $v_r(\Psi) = -v_r(a_1)$ [**9**, Lem. 4.8]

**4** $A_0 \leftarrow \Psi a_0 \pmod{\phi}$, $A_1 \leftarrow \Psi a_1 \pmod{\phi}$

**5** Find $A_1^{-1} \in \mathcal{O}[x]$ with $A_1^{-1}(\alpha) A_1(\alpha) \equiv 1 \pmod{\mathfrak{m}_\phi}$ [**7**, Sec. 4.2]

**6** FOR $i = 1$ TO $\lceil \log_2(h_\phi - h_{\rm cs}) \rceil$ DO

$A_1^{-1} \leftarrow A_1^{-1}(2 - A_1 A_1^{-1}) \pmod{\phi}$

**7** $a \leftarrow A_0 A_1^{-1} \pmod{\phi}$, $\Phi \leftarrow \phi + a$

**8** FOR $i = 1$ TO $\lceil \log_2((H - h_{\rm cs})/(h_\phi - h_{\rm cs})) \rceil - 1$ DO

(a) $q, a_0 \leftarrow \operatorname{quotrem}(f, \Phi)$, $a_1 \leftarrow q \pmod{\Phi}$

(b) $A_0 \leftarrow \Psi a_0 \pmod{\Phi}$, $A_1 \leftarrow \Psi a_1 \pmod{\Phi}$

(c) $A_1^{-1} \leftarrow A_1^{-1}(2 - A_1 A_1^{-1}) \pmod{\Phi}$

(d) $a \leftarrow A_0 A_1^{-1} \pmod{\Phi}$, $\Phi \leftarrow \Phi + a$

OUTPUT:

– A Montes approximation $\Phi$ to the prime factor $F$ of $f$ attached to $\mathbf{t}$, such that $h_\Phi \ge H$.

Note that step **7** terminates a first iteration of the SFL loop. The rest of iterations are performed by the loop described in step **8**. For these iterations it is not necessary to start over the inversion loop of step **6**. In fact, let $\alpha_k \in \overline{K}_v$ be a root of $\Phi_k$ and denote by $A_{1,k}$ the $k$-th polynomial $A_1$. Then, for $h_{\rm cs} < h \le h_{\Phi_k}$, the inversion of $A_{1,k}(\alpha_k)$ modulo $\mathfrak{m}_{\Phi_k}^{h-h_{\rm cs}}$ is also an inversion of $A_{1,k+1}(\alpha_{k+1})$ modulo $\mathfrak{m}_{\Phi_{k+1}}^{h-h_{\rm cs}}$ [**9**, Prop. 5.5]; hence, we get the desired inversion of $A_{1,k+1}(\alpha_{k+1})$ modulo $\mathfrak{m}_{\Phi_{k+1}}^{2h-h_{\rm cs}}$ just by one iteration of the Newton inversion procedure in step **8**(c).

The complexity of the SFL routine was analyzed in [**9**, Lem. 6.5] and [**2**, Thm. 5.16]. In the next result we denote $n = \deg f$, $n_F = \deg F$ and $\delta_F = v(\operatorname{Disc}(F))$.

Theorem 6.2. *The SFL routine requires* $O\left(n n_F \nu^{1+\epsilon} + n \delta_F^{1+\epsilon}\right)$ *operations in* $\mathbb{F}$ *to compute a Montes approximation* $\Phi$ *to* $F$ *as a factor of* $f$*, with precision* $\nu$.

By applying the SFL routine to each leaf of an OM representation of $f$, we get an OM factorization $f \approx P_1 \cdots P_t$ such that $P_j \equiv F_j \pmod{\mathfrak{m}^\nu}$ for all $j$.

Theorem 6.3. *If* $\mathbb{F}$ *is a finite field, a combined application of the Montes and SFL algorithms, computes an OM factorization of* $f$ *with precision* $\nu$*, at the cost of*

$$O\left(n^{2+\epsilon} + n^{1+\epsilon}(1+\delta)\log q + n^{1+\epsilon}\delta^{2+\epsilon} + n^2\nu^{1+\epsilon}\right)$$

*operations in* $\mathbb{F}$.

Example 6.4. Recall the OM factorization $f \approx \phi\phi^*$ of Example 5.3. A single iteration of the main loop of SFL for each approximation of the true factors $f = FF^*$ yields the following improvements:

$$\begin{aligned}\Phi = \;& x^4 - 869643860553342248938373118x^3 + 895292343076575293699260420x^2 \\ & -358277240246400736326320124x - 615563580557575482075250676\end{aligned}$$

$$\begin{aligned}\Phi^* = \;& x^8 - 368296178732038025960751104x^7 - 158699985612499241777758200x^6 \\ & +440432535828627390937956368x^5 - 709340844783185197206077 20x^4 \\ & +468084806048993171281543264x^3 + 345452998984777616876109920x^2 \\ & -244862856588991367554793344x - 417188598541852473806553072.\end{aligned}$$

The qualities of these new approximations are:

$$\mu_{\infty,F}(\Phi)=85,\qquad \mu_{\infty,F^*}(\Phi^*)=88.$$

By Lemma 4.1, the precision is at least 83 in both cases.

**6.2. Computation of the pseudo-valuation $\mu_{\infty,F}$.** Let $F$ be a prime factor in $\mathcal{O}_v[x]$ of an irreducible polynomial $f\in\mathcal{O}[x]$. Let $\theta\in\overline{K}_v$ be a root of $F$.

We present an algorithm for the computation of $\mu_{\infty,F}(g)=v(g(\theta))$ for a given polynomial $g\in\mathcal{O}[x]$. The basic idea is that this value should be deduced from a comparison of the genomic trees of $F$ and $g$. More precisely, if we find an inductive valuation $\mu$ and a key polynomial $\phi$ for $\mu$ such that $\phi\mid_\mu F$ and $\phi\nmid_\mu g$, then $\mu_{\infty,F}(g)=\mu(g)$ by Theorem 2.1. From a computational perspective this amounts to finding a type $\mathbf{t}$ such that $\mathbf{t}\mid F$, $\mathbf{t}\nmid g$, leading to $\mu_{\infty,F}(g)=\mu_i(g)$, where $i$ is the order of $\mathbf{t}$.

Let $r$ be the Okutsu depth of $F$ and let $\mathbf{t}$ be the leaf of an OM representation of $f$, as in (6.1), corresponding to $F$. Since $\mathbf{t}\mid F$, we may check if $\operatorname{Trunc}_i(\mathbf{t})\nmid g$ holds for some $0\le i\le r+1$, leading to $v(g(\theta))=\mu_i(g)$. This fails if $\mathbf{t}\mid g$ (for instance, if $\phi_{r+1}\mid g$). In this case, we improve the Okutsu approximation $\phi_{r+1}$ by applying one loop of the SFL routine; then, we replace the $(r+1)$-th level of $\mathbf{t}$ by the data $(\phi,\lambda,\psi)$ determined by the new choice of $\phi_{r+1}$, and we test again if the new $\mathbf{t}$ divides $g$.

If $\mathbf{t}\mid g$, then $\phi_{r+1}$ is simultaneously close to a prime factor of $f$ and to a prime factor of $g$; hence, if $f$ and $g$ do not have a common prime factor in $\mathcal{O}_v[x]$, after a finite number of steps the renewed type $\mathbf{t}$ will not divide $g$. On the other hand, if $f$ and $g$ have a common prime factor, they must have a common irreducible factor in $\mathcal{O}[x]$ too; since $f$ is irreducible, necessarily $f$ divides $g$ and $g(\theta)=0$.

**$v$-VALUE ROUTINE**

INPUT:

- A discrete valued field $(K,v)$ with valuation ring $\mathcal{O}$.
- A monic irreducible polynomial $f\in\mathcal{O}[x]$.
- A leaf $\mathbf{t}$ of order $r+1$, as in (6.1), of an OM representation of $f$.
- A polynomial $g\in\mathcal{O}[x]$.

**1** $g\leftarrow g \pmod{f}$

**2** IF $g=0$ THEN RETURN $\infty$ ELSE $\nu\leftarrow v_0(g)$, $\quad g\leftarrow g/\pi^\nu$

**3** IF $\psi_0\nmid\overline{g}$ THEN RETURN $\nu$

**4** FOR $i=1$ to $r+1$ DO

(a) Compute $N_i^-(g)$ and the left end point $(s,u)$ of $S_{\lambda_i}(g)$ (section 1.2)

(b) Compute $R_i(g)$

(c) IF $\psi_i\nmid R_i(g)$ then RETURN $\nu+(u+s\lambda_i)/e_1\cdots e_{i-1}$

**5** WHILE $\psi_{r+1}\mid R_{r+1}(g)$ DO

(a) Apply one loop of SFL to improve $\phi_{r+1}$

(b) Set $\lambda_{r+1}$ as the largest slope in absolute value of the new $N_{r+1}^-(f)$

(c) $\psi_{r+1}\leftarrow R_{r+1}(f)$

(d) Compute the new $N_{r+1}^-(g)$ and the left end point $(s,u)$ of $S_{\lambda_{r+1}}(g)$

(e) Compute $R_{r+1}(g)$

**6** RETURN $\nu + (u + s\lambda_{r+1})/e(F)$

OUTPUT:

– $v(g(\theta))$, where $\theta \in \overline{K}_v$ is a root of the prime factor $F$ of $f$ attached to $\mathbf{t}$.

In step **4**(c) we use $v(g(\theta)) = \mu_i(g) = (u + s\lambda_i)/e_1 \cdots e_{i-1}$, by Lemma 1.6.

Let $\alpha \in \overline{K}$ be a root of $f$ and $L = K(\alpha)$ the finite extension of $K$ generated by $\alpha$. Every $\beta \in L$ is of the form $\beta = g(\alpha)$ for some $g \in K[x]$; hence, the $v$-routine computes $v(\iota(\beta))$, where $\iota\colon L \to \overline{K}_v$ is the embedding determined by $\alpha \mapsto \theta$.

Suppose $K$ is a number field and $v = v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation attached to a prime ideal $\mathfrak{p}$ of $K$. Then, the prime factor $F$ of $f$ corresponds to a prime ideal $\mathfrak{P}$ of $L$ dividing $\mathfrak{p}$. As explained in [**7**], the $v$-routine may be used to compute the $\mathfrak{P}$-adic valuation mapping $v_{\mathfrak{P}}\colon L \longrightarrow \mathbb{Z}$ by the formula

$$v_{\mathfrak{P}}(\beta) = e(\mathfrak{P}/\mathfrak{p})v(\iota(\beta)) = e(F)v(\iota(\beta)).$$

This routine is a crucial tool for the applications of polynomial genetics to ideal arithmetic in number fields and divisor arithmetic in function fields. In a number field, it computes the $\mathfrak{P}$-adic valuation with respect to a prime ideal $\mathfrak{P}$; in an algebraic curve, it determines the order of a function at a given point.

**6.3. Index of a square-free polynomial.** Index of a square-free polynomial Let $F \in \mathbb{P}$ be a prime polynomial and $\theta \in \overline{K}_v$ a root of $F$. The Dedekind domain $\mathcal{O}_F$ is a free $\mathcal{O}_v$-module of rank $n_F = \deg F$. Since $\mathcal{O}_v[\theta] \subset \mathcal{O}_F$ is also a free $\mathcal{O}_v$-module of the same rank, the quotient $\mathcal{O}_F/\mathcal{O}_v[\theta]$ is an $\mathcal{O}_v$-module of finite length. This length is the *index* of $F$ and we denote it by $\operatorname{ind}(F)$.

Now, let $f$ be a square-free polynomial in $\mathcal{O}[x]$ with prime factorization $f = F_1 \cdots F_t$ in $\mathcal{O}_v[x]$. We define the *index* of $f$ as

$$\operatorname{ind}(f) := \sum_{1\le i\le t} \operatorname{ind}(F_i) + \sum_{0\le i<j\le t} v(\operatorname{Res}(F_i, F_j)). \tag{6.2}$$

By using a formula of [**6**, Thm. 4.18], in [**5**] it was shown how to compute $\operatorname{ind}(f)$ as the accumulation of the number of points of integer coordinates lying below all Newton polygons that occur along the flow of the Montes algorithm.

Alternatively, we may compute $\operatorname{ind}(f)$ by a closed formula in terms of the data stored in a OM-representation of $f$. By either method, we obtain the value of $\operatorname{ind}(f)$ as a by-product of the Montes algorithm at a negligible cost.

Proposition 6.5. *Let $F, G \in \mathbb{P}$ be two prime factors of $f$ and let $i = i(F, G)$ be their index of coincidence. Then,*

$$\operatorname{ind}(F) = \deg F\,(\operatorname{cap}(F) - 1 + f(F))/2,$$
$$v(\operatorname{Res}(F, G)) = \deg F \deg G \left(V_i + \min\{\lambda_F^G, \lambda_G^F\}\right)/e_1 \cdots e_{i-1}m_i.$$

The capacity $\operatorname{cap}(F)$ was given in (4.1) and the index of coincidence $i(F, G)$ was defined in section 4.2. The types $\mathbf{t}_F$ and $\mathbf{t}_G$ coincide at the levels $0, 1, \dots, i-1$ and the data $e_1, \dots, e_{i-1}, m_i, V_i$ are common to both types. The rational numbers $\lambda_F^G$, $\lambda_G^F$ are the *hidden slopes* of the pair $F, G$ and they are stored as secondary data of the types of the OM representation of $f$. They are obtained in the first iteration of the WHILE loop of the Montes algorithm where the prime factors $F$, $G$ are separated by the branching process. Their name reflects the fact that they cannot be read in the genomic trees if one of the branches of $F$ or $G$ detected in that WHILE loop led to a refinement step.

The formula for $\operatorname{ind}(F)$ was proved in [**9**, Prop. 3.5]. Since $F$ and $G$ are irreducible in $\mathcal{O}_v[x]$, we have $v(\operatorname{Res}(F,G)) = \deg F v(G(\theta))$, where $\theta$ is a root of $F$. Hence, the formula for $v(\operatorname{Res}(F,G))$ may be derived from [**7**, Prop. 4.7].

Example 6.6. Let $f = FF^*$ be the polynomial of Example 5.3. We have already seen that $\operatorname{ind}(F) = 3$, $\operatorname{ind}(F^*) = 20$. Along the application of the Montes algorithm to $f \in \mathbb{Q}[x]$ with respect to the 2-adic valuation, it occurs no refinement. Hence, the hidden slopes are $\lambda_F^{F^*} = \lambda_2 = 1$, $\lambda_{F^*}^{F} = \lambda_2^* = 3/2$, so that $v(\operatorname{Res}(F,F^*)) = 24$ by Proposition 6.5. After (6.2), we obtain $\operatorname{ind}(f) = 47$.

If $f$ is irreducible and separable in $\mathcal{O}[x]$, then the non-negative integer $\operatorname{ind}(f)$ defined in (6.2) coincides with the usual concept of index. In fact, let $\alpha \in \overline{K}$ be a root of $f$ and let $B$ be the integral closure of $\mathcal{O}$ in the finite extension $L = K(\alpha)$. Since the extension $L/K$ is separable and $\mathcal{O}$ is a PID, the Dedekind domain $B$ is a free $\mathcal{O}$-module of rank $n = \deg f$. From the well-known identities relating indices and discriminants [**16**, III, §2-4] we deduce that:

$$\operatorname{ind}(f) = v\left((B\colon \mathcal{O}[\alpha])\right) = \operatorname{length}_{\mathcal{O}}(B/\mathcal{O}[\alpha]),$$

where the *index* $(B\colon \mathcal{O}[\alpha])$ is the $\mathcal{O}$-ideal defined in [**16**, I, §5].

**6.4. Computation of discriminants and resultants.** Let $g, h \in \mathcal{O}[x]$ be two monic polynomials having no common prime factors. In [**6**, Thm. 4.10] a formula for $v(\operatorname{Res}(g,h))$ was obtained in terms of the intersection of two OM representations of $g$ and $h$. In [**14**] a concrete algorithm was designed to carry out this computation. This yields a fast computation of $v(\operatorname{Res}(g,h))$ and/or $v(\operatorname{Disc}(g))$ in cases where the naive computation of $\operatorname{Res}(g,h)$ or $\operatorname{Disc}(g)$ is unfeasible because the polynomials have large degree or large coefficients.

**6.5. Computation of $v$-integral bases.** Suppose that $f \in \mathcal{O}[x]$ is monic and irreducible. Let $\alpha \in \overline{K}$ be a root of $f$ and $L = K(\alpha)$ the finite extension of $K$ generated by $\alpha$. The integral closure $B$ of $\mathcal{O}$ in $L$ is a Dedekind domain.

We suppose that $B$ is finitely generated as an $\mathcal{O}$-module. This condition holds under very natural assumptions; for instance, if $L/K$ is separable, or $(K,v)$ is complete, or $\mathcal{O}$ is a finitely generated algebra over a field [**16**, I, §4].

Under this assumption, $B$ is a free $\mathcal{O}$-module of rank $n = \deg f$. A *$v$-integral basis* of $L$ is by definition an $\mathcal{O}$-basis of $B$.

The *method of the quotients* of [**8**] is valid in this general setting and it computes a $v$-integral basis of $L$. The $v$-integral basis is computed as the by-product of a standard application of the Montes algorithm to $f$. Whenever a $\phi$-expansion of $f$ is computed along the flow of the algorithm, the quotients of the successive divisions with remainder are stored. The members of the $v$-integral basis are computed as $g_i(\alpha)\pi^{-d_i}$, for $0 \le i < n$, where $g_i \in \mathcal{O}[x]$ are an adequate product of the stored quotients, and the non-negative integers $d_i$ are determined by combinatorial data of the Newton polygons computed along the flow of the Montes algorithm.

The complexity of the method is the cost of the Montes algorithm plus $O(n)$ multiplications in $\mathcal{O}[\alpha]$. This method is extremely fast in practice.

**6.6. OM representations of prime ideals in a number field.** Suppose $K = \mathbb{Q}$ and $v = v_p$ is the $p$-adic valuation attached to a prime number $p$, so that $\mathcal{O}$ is the local ring $\mathbb{Z}_{(p)}$.

Let $f\in\mathbb{Z}[x]$ be a monic irreducible polynomial, $\alpha\in\overline{\mathbb{Q}}$ a root of $f$ and $L=\mathbb{Q}(\alpha)$ the number field determined by $f$. Denote by $\mathbb{Z}_L$ the ring of integers of $L$.

After a celebrated theorem by Hensel, the prime ideals of $L$ lying over $p$ are in 1-1 correspondence with the prime factors of $f$ in $\mathbb{Z}_p[x]$. From a computational perspective, the prime ideals may be represented in a computer as the OM representations of these prime factors of $f$, which may be computed by a single application of the Montes algorithm with input $f, v_p$. The main arithmetic tasks concerning prime ideals may be easily performed by using the MacLane-Okutsu invariants and the operators encoded by these OM representations.

In [**7**] it was presented a computational approach to ideal theory in number fields based on this principle. This approach has the advantage that many arithmetic tasks may be carried out avoiding the computation of the maximal order of $L$ and the factorization of the discriminant of the defining polynomial $f$. The most relevant ones are:

(1) Compute the $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}\colon L^*\to\mathbb{Z}$, for any prime ideal $\mathfrak{p}$ of $L$.
(2) Obtain the prime ideal decomposition of a fractional ideal.
(3) Compute a two-elements representation of a fractional ideal.
(4) Add, multiply and intersect fractional ideals.
(5) Compute the reduction maps $\mathbb{Z}_L\to\mathbb{Z}_L/\mathfrak{p}^a$.
(6) Solve Chinese remainders problems.
(7) Compute a $p$-integral basis of $L$.

The genetic-based routines designed to perform these tasks are much faster than the classical ones, especially for those number fields defined by polynomials with a large genomic tree at some prime.

The Magma package *+Ideals.m* based on this approach may be downloaded from `http://www-ma4.upc.edu/~guardia/+Ideals.html`.

**6.7. OM representations of places in a function field.** Suppose that $K=k(t)$ is the function field of the projective line $\mathbb{P}^1$ over a field $k$. An irreducible polynomial $f(t,x)\in k[t,x]$, separable over $k[t]$, determines a unique smooth projective curve $C$ as the normalization of the projective closure of the affine curve $f(t,x)=0$. The function field of $C$ is $L=k(t,x)=K[x]/(f)$.

Let $A=k[t]$ and denote by $A_\infty=k[t^{-1}]$ the local ring at the point at infinity of $\mathbb{P}^1$. Let $B$ and $B_\infty$ be the integral closures in $L$ of $A$ and $A_\infty$, respectively. As indicated in [**10**], a divisor of $C$ may be identified to a pair $D=(I,I_\infty)$ of fractional ideals of $B$ and $B_\infty$ respectively. The Riemann-Roch space attached to the divisor is simply $L(D)=I\cap I_\infty$.

In this representation, a prime divisor corresponds to a prime ideal in either $B$ or $B_\infty$, and it may be represented by a prime factor of $f(t,x)$ over the completion of $A$ or $A_\infty$ at a place (finite or infinite) of $K$.

J.-D. Bauch has developed a Magma package *+Divisors.m* where divisors are manipulated as such pairs $D=(I,I_\infty)$, and ideals are handled as OM representations. This approach leads to a fast method to compute the genus of a curve [**1**] and to an acceleration of the classical methods to compute $k$-bases of the Riemann-Roch spaces of divisors defined over $k$.

**6.8. Construction of number fields and function fields with prescribed ramification.** The procedure for the construction of types described in section 3.2 can be used to generate number fields $L$ with prescribed decomposition of several rational primes. For every prescribed factorization $p\mathbb{Z}_L = \mathfrak{p}_1 \dots \mathfrak{p}_g$ one constructs proper types $\mathbf{t}_1, \dots, \mathbf{t}_g$; the product of the $\phi$-polynomials in the last level of all these types plus a high enough power of $p$ will generate a number field where $p$ has the desired factorization. Actually, we can even prescribe different values for the Okutsu invariants of the prime factors of the generating polynomial corresponding to the different prime ideals. In order to combine prescribed data for different prime numbers, one has only to apply the Chinese remainder theorem. The same idea works for function fields.

We have used these ideas in [**9**] to design a bank of benchmark polynomials for the analysis of algorithms on number fields or function fields.

## References


[1] J.-D. Bauch, *Genus computation of global function fields*, arXiv:1209.0309v3 [math.NT], Journal of Symbolic Computation, to appear.

[2] J.-D. Bauch, E. Nart, H. D. Stainsby, *Complexity of OM factorizations of polynomials over local fields*, LMS Journal of Computation and Mathematics **16** (2013), 139–171.

[3] J. Fernández, J. Guàrdia, J. Montes, E. Nart, *Residual ideals of MacLane valuations*, arXiv:1305.0775v2 [math.NT].

[4] J. Guàrdia, J. Montes, E. Nart, *Okutsu invariants and Newton polygons*, Acta Arithmetica **145** (2010), 83–108.

[5] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, Journal de Théorie des Nombres de Bordeaux **23** (2011), no. 3, 667–696.

[6] J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

[7] J. Guàrdia, J. Montes, E. Nart, *A new computational approach to ideal theory in number fields*, Foundations of Computational Mathematics **13** (2013), 729–762.

[8] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons and integral bases*, arXiv: 0902.3428v2[math.NT].

[9] J. Guàrdia, E. Nart, S. Pauli, *Single-factor lifting and factorization of polynomials over local fields*, Journal of Symbolic Computation **47** (2012), 1318–1346.

[10] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symb. Comput. **33** (2002), 425–445.

[11] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society, **40**(1936), pp. 363–395.

[12] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2**(1936), pp. 492–510.

[13] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, PhD Thesis, Universitat de Barcelona, 1999.

[14] E. Nart, *Local computation of differents and discriminants*, Mathematics of Computation 83 (2014), no 287, 1513–1534.

[15] K. Okutsu, *Construction of integral basis, I, II*, Proceedings of the Japan Academy **58**, Ser. A (1982), 47–49, 87–89.

[16] J. P. Serre, *Corps Locaux*, second Edition, Hermann, Paris, 1968.

[17] M. Vaquié, *Extension d'une valuation*, Transactions of the American Mathematical Society **359** (2007), no. 7, 3439–3481.

[18] M. Vaquié, *Famille admissible de valuations et défaut d'une extension*, Journal of Algebra **311** (2007), no. 2, 859–876.

[19] M. Vaquié, *Extensions de valuation et polygone de Newton*, Annales de l'Institute Fourier (Grenoble) **58** (2008), no. 7, 2503–2541.

Departament de Matemàtica Aplicada IV, Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, Av. Víctor Balaguer s/n. E-08800 Vilanova i la Geltrú, Catalonia

*E-mail address*: guardia@ma4.upc.edu

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalonia

*E-mail address*: nart@mat.uab.cat