*LMS J. Comput. Math.* 16 (2013) 139–171 © 2013 Authors
doi:10.1112/S1461157013000089

# Complexity of OM factorizations of polynomials over local fields

Jens-Dietrich Bauch, Enric Nart and Hayden D. Stainsby

## Abstract

Let $k$ be a locally compact complete field with respect to a discrete valuation $v$. Let $\mathcal{O}$ be the valuation ring, $\mathfrak{m}$ the maximal ideal and $F(x) \in \mathcal{O}[x]$ a monic separable polynomial of degree $n$. Let $\delta = v(\mathrm{Disc}(F))$. The Montes algorithm computes an OM factorization of $F$. The single-factor lifting algorithm derives from this data a factorization of $F(\mathrm{mod}\ \mathfrak{m}^\nu)$, for a prescribed precision $\nu$. In this paper we find a new estimate for the complexity of the Montes algorithm, leading to an estimation of $O(n^{2+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon} + n^2\nu^{1+\epsilon})$ word operations for the complexity of the computation of a factorization of $F(\mathrm{mod}\ \mathfrak{m}^\nu)$, assuming that the residue field of $k$ is small.

## *Introduction*

Let $A$ be a Dedekind domain whose field of fractions $K$ is a global field. Let $L/K$ be a finite separable extension and $B$ the integral closure of $A$ in $L$. Let $\theta \in L$ be a primitive element of $L/K$, with minimal polynomial $f(x) \in A[x]$.

Let $\mathfrak{p}$ be a non-zero prime ideal of $A$, $v_\mathfrak{p}$ the canonical $\mathfrak{p}$-adic valuation, $K_\mathfrak{p}$ the completion of $K$ at $\mathfrak{p}$, and $\mathcal{O}_\mathfrak{p}$ the valuation ring of $K_\mathfrak{p}$.

The Montes algorithm [**5**, **6**] computes an OM *(Okutsu–Montes) representation* of every prime ideal $\mathfrak{P}$ of $B$ lying over $\mathfrak{p}$ [**7**]. This algorithm carries out a program suggested by Ore [**15**, **16**], and developed by MacLane in the context of valuation theory [**10**, **11**]. An OM representation is a computational object supporting several data and operators, linked to one of the irreducible factors (say) $F(x)$ of $f(x)$ in $\mathcal{O}_\mathfrak{p}[x]$. Among these data, the OM representation contains all the *Okutsu invariants* of $F$, which reveal considerable arithmetic information about the finite extension of $K_\mathfrak{p}$ determined by $F$ [**4**, **14**].

The Montes algorithm has been used as the core of several arithmetic routines to compute prime ideal decomposition, integral bases and the discriminant of $L/K$, generators of prime ideals, the $\mathfrak{P}$-adic valuation, $v_\mathfrak{P}\colon L^* \longrightarrow \mathbb{Z}$, the reduction mapping, $B \longrightarrow B/\mathfrak{P}$, the Chinese remainder algorithm in $B$, and the $\mathfrak{p}$-valuation of discriminants and resultants of polynomials with coefficients in $K$ [**5**, **7**, **8**, **13**].

Also, if the Montes algorithm is combined with the single-factor lifting algorithm [**9**], together they yield a fast factorization routine for polynomials over local fields, which turns into an acceleration of some of the above mentioned routines.

The complexity of the Montes algorithm was analyzed by Ford–Veres [**2**] and Pauli [**18**]. Assuming $\mathfrak{p}$ small, they obtained an estimation of $O(n^{2+\epsilon}\delta^{2+\epsilon})$ word operations for the algorithm used as an irreducibility test for polynomials over local fields, where $n = [L\colon K]$ and $\delta = v_\mathfrak{p}(\mathrm{Disc}(f))$. Then, by natural extrapolation arguments they concluded that this estimation is valid for the general algorithm too.

In this paper, we present a new estimation for the complexity of the Montes algorithm. To this end, we find the least precision $\nu$ such that the polynomial $f(x)$ (mod $\mathfrak{p}^\nu$) contains sufficient information to detect that $f(x)$ is irreducible over $\mathcal{O}_\mathfrak{p}$, and the least precision such

Received 20 April 2012; revised 30 November 2012.

*2010 Mathematics Subject Classification* 11Y40 (primary), 11Y05, 12J10, 14H25 (secondary).

The research was partially supported by MTM2009-10359 from the Spanish MEC.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

that a factorization of $f(x) \pmod{\mathfrak{p}^\nu}$ determines a 'sufficiently good' approximate factorization of $f(x)$ over $\mathcal{O}_\mathfrak{p}$.

In Section 1 we review the role of the Okutsu invariants of the irreducible factors of $f(x)$ over $\mathcal{O}_\mathfrak{p}$, which are essential for our purposes. In Section 2, we introduce a new Okutsu invariant, the *exponent of the Okutsu discriminant*, which is a key ingredient to prove that the irreducibility of $f(x)$ over $\mathcal{O}_\mathfrak{p}$ may be tested by working at precision $\nu = \lfloor 2\delta/n \rfloor + 1$ (Theorem 2.3). In Section 3 we introduce the concept of *OM factorization*, giving a precise sense to what we mean by a 'sufficiently good' approximate factorization. We show that the OM representations satisfying certain properties are adequate objects to deal with OM factorizations from a computational perspective, and we prove that an OM factorization of $f(x)$ over $\mathcal{O}_\mathfrak{p}$ can be found by working at precision $\nu = \delta + 1$ (Theorem 3.13). In Section 4, we review the Montes algorithm as a device to compute an OM factorization of $f(x)$ over $\mathcal{O}_\mathfrak{p}$. Finally, in Section 5 we use these results to obtain an estimation of $O(n^{2+\epsilon} + \delta^{2+\epsilon})$ word operations for the complexity of the Montes algorithm used as a polynomial irreducibility test, and an estimation of $O(n^{2+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon})$ word operations for the complexity of the general algorithm. This estimation yields improved estimations for the complexity of all the arithmetic routines mentioned above. For instance, we deduce an estimation of $O(n^{2+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon} + n^2\nu^{1+\epsilon})$ word operations for the complexity of the factorization of $f(x)$ over $\mathcal{O}_\mathfrak{p}[x]$, with an arbitrary prescribed precision $\nu$ (Theorem 5.17). The best known previous estimation for the factorization of polynomials over local fields had total degree $4 + \epsilon$ in $n$, $\delta$ and $\nu$ [9].

## 1. *Okutsu invariants of an irreducible polynomial over a local field*

Let $k$ be a local field, that is, a locally compact and complete field with respect to a discrete valuation $v$. 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 field, which is a finite field. Let $p$ be the characteristic of $\mathbb{F}$.

Let $k^{\mathrm{sep}} \subset \overline{k}$ be the separable closure of $k$ inside a fixed algebraic closure. Let $v\colon \overline{k} \to \mathbb{Q} \cup \{\infty\}$ be the canonical extension of the discrete valuation $v$ to $\overline{k}$, normalized by $v(k) = \mathbb{Z}$.

Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible separable polynomial, $\theta \in k^{\mathrm{sep}}$ a root of $F(x)$, and $L = k(\theta)$ the finite separable extension of $k$ generated by $\theta$. Denote $n := [L\colon k] = \deg F$. Let $\mathcal{O}_L$ be the ring of integers of $L$, $\mathfrak{m}_L$ the maximal ideal and $\mathbb{F}_L$ the residue field. We indicate with a bar, $\overline{\phantom{x}}\colon \mathcal{O}[x] \longrightarrow \mathbb{F}[x]$, the canonical homomorphism of reduction of polynomials modulo $\mathfrak{m}$.

Let $[\phi_1, \ldots, \phi_r]$ be an *Okutsu frame* of $F(x)$, and let $\phi_{r+1}$ be an *Okutsu approximation* to $F(x)$. That is, $\phi_1, \ldots, \phi_{r+1} \in \mathcal{O}[x]$ are monic separable polynomials of strictly increasing degree

$$1 \leqslant m_1 := \deg \phi_1 < \ldots < m_r := \deg \phi_r < m_{r+1} := \deg \phi_{r+1} = n,$$

and for any monic polynomial $g(x) \in \mathcal{O}[x]$ we have

$$m_i \leqslant \deg g < m_{i+1} \Longrightarrow \frac{v(g(\theta))}{\deg g} \leqslant \frac{v(\phi_i(\theta))}{m_i} < \frac{v(\phi_{i+1}(\theta))}{m_{i+1}}, \tag{1.1}$$

for $0 \leqslant i \leqslant r$, with the convention that $m_0 = 1$ and $\phi_0(x) = 1$. It is easy to deduce from (1.1) that the polynomials $\phi_1(x), \ldots, \phi_{r+1}(x)$ are all irreducible in $\mathcal{O}[x]$.

The length $r$ of the frame is called the *Okutsu depth* of $F(x)$. Okutsu frames were introduced by Okutsu in [14] as a tool to construct integral bases. Okutsu approximations were introduced in [4], where it is shown that the family $\phi_1, \ldots, \phi_r, \phi_{r+1}$ determines an *optimal $F$-complete type of order $r + 1$*,

$$\mathbf{t}_F = \begin{cases} (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (\phi_{r+1}, \lambda_{r+1}, \psi_{r+1})), & \text{or} \\ (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (F, -\infty, \text{---})), \end{cases} \tag{1.2}$$

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

for $\phi_{r+1} \neq F$ or $\phi_{r+1} = F$, respectively. We call $\mathbf{t}_F$ an *OM representation* of $F$. In the case $\phi_{r+1} = F$, we say that the OM representation is *exact*.

Any OM representation of the polynomial $F$ carries (stores) several invariants and operators yielding strong arithmetic information about $F$ and the extension $L/k$. Let us recall some of these invariants and operators.

Attached to the type $\mathbf{t}_F$, there is a family of discrete valuations of the rational function field $k(x)$, the *MacLane valuations*

$$v_i \colon k(x) \longrightarrow \mathbb{Z} \cup \{\infty\}, \quad 1 \leqslant i \leqslant r+1,$$

such that $0 = v_1(F) < \ldots < v_{r+1}(F)$. The $v_1$-value of a polynomial in $k[x]$ is the minimum of the $v$-values of its coefficients.

Also, $\mathbf{t}_F$ determines a family of Newton polygon operators

$$N_i \colon k[x] \longrightarrow 2^{\mathbb{R}^2}, \quad 1 \leqslant i \leqslant r+1,$$

where $2^{\mathbb{R}^2}$ is the set of subsets of the Euclidean plane. Any non-zero polynomial $g(x) \in k[x]$ has a canonical $\phi_i$-development

$$g(x) = \sum_{0 \leqslant s} a_s(x)\phi_i(x)^s, \quad \deg a_s < m_i,$$

and the polygon $N_i(g)$ is the lower convex hull of the set of points $(s, v_i(a_s\phi_i^s))$. Usually, we are only interested in the principal polygon $N_i^-(g) \subset N_i(g)$ formed by the sides of negative slope. For all $1 \leqslant i \leqslant r$, the Newton polygons $N_i(F)$ and $N_i(\phi_{i+1})$ are one-sided and they have the same slope, which is a negative rational number $\lambda_i \in \mathbb{Q}_{<0}$. The Newton polygon $N_{r+1}(F)$ is one-sided and it has an (extended) integer negative slope, which we denote by $\lambda_{r+1} \in \mathbb{Z} \cup \{-\infty\}$.

The triple $(\phi_i, v_i, \lambda_i)$ determines the discrete valuation $v_{i+1}$ as follows: for any non-zero polynomial $g(x) \in K[x]$, take a line of slope $\lambda_i$ far below $N_i(g)$ and let it shift upwards till it touches the polygon for the first time; if $u$ is the ordinate of the point of intersection of this line with the vertical axis, then $v_{i+1}(g) = e_i u$.

In MacLane's terminology [**10**, § 4], $\phi_i$ is a *key polynomial* over $v_i$, and [**6**, Proposition 2.7,(4)] shows that $v_{i+1}/e_i$ is the *augmented valuation* attached to the pair $\phi_i, v_i(\phi_i) + |\lambda_i|$.

There is a chain of finite extensions: $\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_{r+1} = \mathbb{F}_L$. The type $\mathbf{t}_F$ stores monic irreducible polynomials $\psi_i(y) \in \mathbb{F}_i[y]$ such that $\mathbb{F}_{i+1} \simeq \mathbb{F}_i[y]/(\psi_i(y))$. We have $\psi_i(y) \neq y$, for all $i > 0$.

Finally, for every negative rational number $\lambda$, there are *residual polynomial* operators

$$R_{\lambda,i} \colon k[x] \longrightarrow \mathbb{F}_i[y], \quad 1 \leqslant i \leqslant r+1.$$

We define $R_i := R_{\lambda_i,i}$. For all $0 \leqslant i \leqslant r$, we have $R_i(F) \sim \psi_i^{\omega_{i+1}}$ and $R_i(\phi_{i+1}) \sim \psi_i$, where the symbol $\sim$ indicates that the polynomials coincide up to a multiplicative constant in $\mathbb{F}_i^*$. For $i = 0$ we take $R_0(F) := \overline{F} = \psi_0^{\omega_1}$ and $R_0(\phi_1) := \overline{\phi_1} = \psi_0$. The exponents $\omega_{i+1}$ are all positive and $\omega_{r+1} = 1$. The operator $R_{r+1}$ is defined only when $\phi_{r+1} \neq F$; in this case, we also have $R_{r+1}(F) \sim \psi_{r+1}$, with $\psi_{r+1}(y) \in \mathbb{F}_{r+1}[y]$ monic of degree one such that $\psi_{r+1}(y) \neq y$.

From these data some more numerical invariants are deduced. Initially we take

$$m_0 := 1, \quad f_0 := \deg \psi_0, \quad e_0 := 1, \quad h_0 := V_0 := \mu_0 := \nu_0 = 0.$$

Then we define, for all $1 \leqslant i \leqslant r+1$,

$h_i$, $e_i$ positive coprime integers such that $\lambda_i = -h_i/e_i$;
$f_i := \deg \psi_i$;
$m_i := \deg \phi_i = e_{i-1}f_{i-1}m_{i-1} = (e_0\, e_1 \ldots e_{i-1})(f_0 f_1 \ldots f_{i-1})$;
$\mu_i := \sum_{1 \leqslant j \leqslant i}(e_j f_j \ldots e_i f_i - 1)h_j/(e_1 \ldots e_j)$;
$\nu_i := \sum_{1 \leqslant j \leqslant i} h_j/(e_1 \ldots e_j)$;
$V_i := v_i(\phi_i) = e_{i-1}f_{i-1}(e_{i-1}V_{i-1} + h_{i-1}) = (e_0 \ldots e_{i-1})(\mu_{i-1} + \nu_{i-1})$.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

The general definition of a type may be found in [6, § 2.1]. In later sections, we shall consider types which are not necessarily optimal nor $F$-complete. So, it may be convenient to distinguish these two properties among all features of a type that we have just mentioned.

Definition 1.1. Let $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots ; (\phi_i, \lambda_i, \psi_i))$ be a type of order $i$ and denote $m_{i+1} := e_i f_i m_i$. Let $g(x) \in K[x]$ be a polynomial.

- We say that $\mathbf{t}$ is *optimal* if $m_1 < \dots < m_i$. We say that $\mathbf{t}$ is *strongly optimal* if $m_1 < \dots < m_i < m_{i+1}$.

- We define $\operatorname{ord}_{\mathbf{t}}(g) := \operatorname{ord}_{\psi_i} R_i(g)$ in $\mathbb{F}_i[y]$. If $\operatorname{ord}_{\mathbf{t}}(g) > 0$, we say that $\mathbf{t}$ *divides* $g(x)$, and we write $\mathbf{t} \mid g(x)$. This function $\operatorname{ord}_{\mathbf{t}}$ behaves well with respect to products: $\operatorname{ord}_{\mathbf{t}}(gh) = \operatorname{ord}_{\mathbf{t}}(g) + \operatorname{ord}_{\mathbf{t}}(h)$.

- We say that $\mathbf{t}$ is *$g$-complete* if $\operatorname{ord}_{\mathbf{t}}(g) = 1$.

- A *representative* of $\mathbf{t}$ is a monic polynomial $\phi(x) \in \mathcal{O}[x]$ of degree $m_{i+1}$, such that $\operatorname{ord}_{\mathbf{t}}(\phi) = 1$. This polynomial is necessarily irreducible in $\mathcal{O}[x]$. The degree $m_{i+1}$ is minimal among all polynomials satisfying this condition.

- For any $0 \leqslant j \leqslant i$, 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 $j$. We have $\operatorname{ord}_{\operatorname{Trunc}_j(\mathbf{t})}(g) \geqslant (e_{j+1} f_{j+1}) \dots (e_i f_i) \operatorname{ord}_{\mathbf{t}}(g)$.

Thus, for a general type of order $i$ dividing $F$, we have $m_1 \mid \dots \mid m_i$ and $\omega_i > 0$, but not necessarily $m_1 < \dots < m_i = \deg F$, and $\omega_i = 1$. These were particular properties of our optimal and $F$-complete type $\mathbf{t}_F$ of order $i = r + 1$, constructed from an Okutsu frame and an Okutsu approximation to $F$.

An irreducible polynomial $F$ admits infinitely many different OM representations. However, the numerical invariants $e_i, f_i, h_i$, for $0 \leqslant i \leqslant r$, and the MacLane valuations $v_1, \dots, v_{r+1}$ attached to $\mathbf{t}_F$, are canonical invariants of $F$.

The data $\lambda_{r+1}, \psi_{r+1}$ are not invariants of $F$; they depend on the choice of the Okutsu approximation $\phi_{r+1}$. The integer slope $\lambda_{r+1} = -h_{r+1}$ measures how close $\phi_{r+1}$ is to $F$. We have $\phi_{r+1} = F$ if and only if $h_{r+1} = \infty$.

Definition 1.2. An *Okutsu invariant* of $F(x)$ is a rational number that depends only on $e_1, \dots, e_r, f_0, f_1, \dots, f_r, h_1, \dots, h_r$.

We are specially interested in the following invariants of the polynomial $F(x)$:

$$\begin{aligned} &e(F) := e(L/k), \text{ the ramification index of } L/k;\\ &f(F) := f(L/k), \text{ the residual degree of } L/k;\\ &\mu(F) := \max\{v(g(\theta)) \mid g(x) \in \mathcal{O}[x] \text{ monic of degree less than } n\};\\ &\delta(F) := v(\operatorname{Disc}(F)). \end{aligned}$$

The different ideal of $L/k$ is $\operatorname{Diff}(L/k) = (\mathfrak{m}_L)^{e-1+\rho}$, for some integer $\rho \geqslant 0$, which is not an Okutsu invariant of $F$. Also, $\rho = 0$ if and only if $L/k$ is tamely ramified.

The results of the next proposition are taken from [6, Corollary 3.8] and [13, Theorem 1.7].

Proposition 1.3. *We have identities*

$$\begin{aligned} &e(F) = e_0\, e_1 \dots e_r, \quad f(F) = f_0 f_1 \dots f_r,\\ &\mu(F) = \mu_r = \sum_{1 \leqslant j \leqslant r} (e_j f_j \dots e_r f_r - 1) h_j / (e_1 \dots e_j),\\ &\delta(F) = n\mu(F) + f(F)\rho. \end{aligned}$$

Thus, $e(F)$, $f(F)$ and $\mu(F)$ are Okutsu invariants of $F$, but $\delta(F)$ is not. Nevertheless, the lower bound by an Okutsu invariant, $\delta(F) \geqslant n\mu(F)$, will be essential for our purposes.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

Definition 1.4. The *length* of a Newton polygon $N$ is the abscissa of its right end point; we denote it by $\ell(N)$.

The following lemma will be frequently used.

Lemma 1.5 [6, Proposition 2.7, Lemma 2.17, Theorem 3.1]. *Let* $\mathbf{t}$ *be a type of order* $r$. *Then:*

(i) $v_i(a) = e_0 \dots e_{i-1} v(a)$, *for all* $a \in k$ *and all* $1 \leqslant i \leqslant r+1$;
(ii) $\ell(N_{r+1}(g)) = \operatorname{ord}_{\mathbf{t}}(g)$, *for any non-zero polynomial* $g(x) \in k[x]$;
(iii) $v(\phi_i(\theta)) = (V_i + |\lambda_i|)/(e_0 \dots e_{i-1}) = \mu_{i-1} + \nu_i$, *for all* $1 \leqslant i \leqslant r+1$;
(iv) $v(\phi_i(\theta))/m_i = V_{i+1}/(m_{i+1} e_0 \dots e_i)$, *for all* $1 \leqslant i \leqslant r$.

We end this background section by recalling the *Okutsu equivalence* of irreducible separable polynomials over $\mathcal{O}$, and the concept of *width* of such a polynomial.

Lemma 1.6 [9, Lemma 3.1]. *Let* $\mathbf{t}$ *be a strongly optimal type of order* $r$, *and let* $\phi \in \mathcal{O}[x]$ *be a monic polynomial of degree* $m_{r+1}$. *Let* $F \in \mathcal{O}[x]$ *be an irreducible separable polynomial such that* $\mathbf{t} \mid F$, *and let* $\theta \in k^{\mathrm{sep}}$ *be a root of* $F$. *Then, the following conditions are equivalent:*

(a) $\phi$ *is a representative of* $\mathbf{t}$;
(b) $v(\phi(\theta)) > V_{r+1}/(e_0 \dots e_r) = (m_{r+1}/m_r) v(\phi_r(\theta))$.

Definition 1.7. Let $F \in \mathcal{O}[x]$ be a monic irreducible separable polynomial of Okutsu depth $r$, and let $\mathbf{t}_F$ be an OM representation of $F$ as in (1.2). Let $\mathbf{t} := \operatorname{Trunc}_r(\mathbf{t}_F)$. We say that a monic polynomial $G \in \mathcal{O}[x]$ is an *Okutsu approximation to* $F$, and we write $F \approx G$, if $G$ is a representative of $\mathbf{t}$.

We also say that $F$ and $G$ are *Okutsu equivalent* polynomials.

By Lemma 1.6, this definition does not depend on the choice of the OM representation of $F$. The binary relation $\approx$ is an equivalence relation on the set of all monic irreducible separable polynomials in $\mathcal{O}[x]$ [4, Lemma 4.3]. Okutsu equivalent polynomials have the same Okutsu invariants and the same MacLane valuations [4, Corollary 3.7].

For $F$ as above, and $1 \leqslant i \leqslant r+1$, let $\operatorname{Rep}_i(F) \subseteq \mathcal{O}[x]$ be the set of all representatives of $\operatorname{Trunc}_{i-1}(\mathbf{t}_F)$. Consider

$$\mathcal{V}_i := \{v(\phi(\theta)) \mid \phi \in \operatorname{Rep}_i(F)\} \subseteq \mathbb{Q} \cup \{\infty\}.$$

By the formula (1.1), $\phi_i \in \operatorname{Rep}_i(F)$ and $v(\phi_i(\theta)) = \operatorname{Max}(\mathcal{V}_i)$, for all $1 \leqslant i \leqslant r$. By definition, $\operatorname{Rep}_{r+1}(F)$ is the set of all Okutsu approximations to $F(x)$. The set $\mathcal{V}_{r+1}$ is not finite, and it contains $\infty$, because $F \in \operatorname{Rep}_{r+1}(F)$.

The sets $\mathcal{V}_1, \dots, \mathcal{V}_r$ are finite and easy to describe [9, Proposition 3.4].

Proposition 1.8. *For any* $\lambda \in \mathbb{Q}$, *let* $M_\lambda := \{m \in \mathbb{Z} \mid 1 \leqslant m < |\lambda|\} \cup \{|\lambda|\}$. *Then,*

$$\mathcal{V}_i = \{(V_i + m)/(e_0 \dots e_{i-1}) \mid m \in M_{\lambda_i}\},$$

*for all* $1 \leqslant i \leqslant r$. *In particular,* $\#\mathcal{V}_i = \lceil |\lambda_i| \rceil = \lceil h_i/e_i \rceil$.

The *width* of $F(x)$ is defined to be the vector of positive integers,

$$(\#\mathcal{V}_1, \dots, \#\mathcal{V}_r) = (\lceil h_1/e_1 \rceil, \dots, \lceil h_r/e_r \rceil).$$

As we shall see in Section 5, it is a fundamental invariant for the analysis of the complexity of the Montes algorithm.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

## 2. *The Okutsu discriminant*

We keep all notation from the previous section. In this section we introduce a new Okutsu invariant of an irreducible polynomial $F(x) \in \mathcal{O}[x]$, linked to the problem of determining the least exponent $\nu$ such that all polynomials of degree $n = \deg F$, belonging to $F(x) + \mathfrak{m}^\nu[x]$, are irreducible in $\mathcal{O}[x]$.

Definition 2.1. Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible separable polynomial of degree $n$ and $\mathbf{t}_F$ an OM representation of $F$ as in (1.2). If $r$ is the Okutsu depth of $F(x)$, we define the *Okutsu discriminant* of $F(x)$ as the ideal $\mathfrak{m}^{\delta_0(F)}$, where

$$\delta_0(F) := \frac{V_{r+1}}{e(F)} = \mu_r + \nu_r = \sum_{1 \leqslant i \leqslant r} \frac{|\lambda_i|}{e_0 \ldots e_{i-1}} \frac{n}{m_i}. \tag{2.1}$$

The exponent $\delta_0(F)$ of the Okutsu discriminant coincides, up to a certain normalization, with the ordinate of the left end point of $N_r(F)$.

Lemma 2.2. *With the above notation, denote $u_i := v_i(a_{0,i}(F))$, for $1 \leqslant i \leqslant r$, where $a_{0,i}(F) \in \mathcal{O}[x]$ is the* 0th *coefficient of the $\phi_i$-development of $F$. Then:*

(1) *$u_1 < u_2/e_1 < \ldots < u_r/(e_0 \ldots e_{r-1}) = \delta_0(F)$;*

(2) *$\delta_0(F) \leqslant 2\delta(F)/n$, and equality holds if and only if $r = 0$, or $r = 1$, $e_1 f_1 = 2$, $p > e_1$.*

*Proof.* Denote $\omega_i = n/m_i = (e_i f_i) \ldots (e_r f_r)$. The Newton polygon $N_i(F)$ is one-sided, with end points $(0, u_i)$ and $(\omega_i, v_i(F))$ [6, Lemma 2.17]. Also, the leading term of the $\phi_i$-adic expansion of $F$ is $\phi_i^{\omega_i}$. Thus, $v_i(F) = \omega_i V_i$ and

$$\frac{u_i}{e_0 \ldots e_{i-1}} = \frac{v_i(F) + \omega_i |\lambda_i|}{e_0 \ldots e_{i-1}} = \frac{\omega_i (V_i + |\lambda_i|)}{e_0 \ldots e_{i-1}} = n \frac{v(\phi_i(\theta))}{m_i}, \tag{2.2}$$

the last equality by Lemma 1.5(iii). By the properties (1.1) of the Okutsu frame, $u_1 < u_2/e_1 < \ldots < u_r/(e_0 \ldots e_{r-1})$. Also, by Lemma 1.5(iv),

$$u_r/(e_0 \ldots e_{r-1}) = (n/m_r) v(\phi_r(\theta)) = V_{r+1}/e(F) = \delta_0(F).$$

On the other hand, since $e_i f_i > 1$, for all $1 \leqslant i \leqslant r$, we have $\nu_r \leqslant \mu_r = \mu(F)$. Thus, $\delta_0(F) \leqslant 2\mu(F) \leqslant 2\delta(F)/n$, by Proposition 1.3. Also, equality holds if and only if $\mu_r = \nu_r$ and $F$ determines a tamely ramified extension of $k$ (that is $\rho = 0$). The formulas for $\mu_r$, $\nu_r$ in Section 1 lead to the conditions of item (2). □

The aim of this section is to prove the following result.

Theorem 2.3. *Let $F(x), G(x) \in \mathcal{O}[x]$ be monic separable polynomials of degree $n$, such that $F \equiv G \pmod{\mathfrak{m}^\nu}$, for some positive exponent $\nu$.*

(1) *If $F$ is irreducible and $\nu > \delta_0(F)$, then $G$ is irreducible and $G \approx F$.*

(2) *If $G$ is irreducible and $\nu > 2\delta(F)/n$, then $F$ is irreducible and $F \approx G$.*

Corollary 2.4. *Let $F(x), G(x) \in \mathcal{O}[x]$ be monic separable polynomials of degree $n$, such that $F \equiv G \pmod{\mathfrak{m}^\nu}$, for $\nu > 2\delta(F)/n$. Then, $F$ is irreducible if and only if $G$ is irreducible. If this is the case, then $F \approx G$ and the extensions of $k$ determined by $F$ and $G$ are isomorphic.*

*Proof.* By Theorem 2.3 and Lemma 2.2, $F$ is irreducible if and only if $G$ is irreducible, and then $F \approx G$. In this case,

$$v(\operatorname{Res}(F, G)) = v(\operatorname{Res}(F, G - F)) \geqslant n\nu > 2\delta(F).$$

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

In particular, for every root $\theta \in k^{\mathrm{sep}}$ of $F$, we have $nv(G(\theta)) = v(\operatorname{Res}(F, G)) > 2\delta(F)$. Thus, the conditions of [**17**, Proposition 4.1] are satisfied, and [**17**, Lemma 4.3] shows that $k(\theta) = k(\theta')$, for adequate choices of roots $\theta, \theta' \in k^{\mathrm{sep}}$ of $F$, $G$, respectively. □

The first item of Theorem 2.3 follows immediately from Lemma 2.2. In fact, for $\theta \in k^{\mathrm{sep}}$ a root of $F$, the assumptions of the first item imply that $v(G(\theta)) > \delta_0(F) = nv(\phi_r(\theta))/m_r$, and this is precisely the condition to be an Okutsu approximation to $F$ (cf. Lemma 1.6). As mentioned in Definition 1.1, this implies that $G$ is irreducible.

The second item is more subtle and its proof more involved. We need some previous results.

Definition 2.5. Let $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots ; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1}))$ be a type of order $i - 1 \geqslant 0$, and let $F(x) \in \mathcal{O}[x]$ be a monic polynomial. We say that $F(x)$ is *a polynomial of type* $\mathbf{t}$ if it satisfies the following conditions:

(i) $R_0(F) = \overline{F} = \psi_0^{a_0}$, for a certain positive exponent $a_0$;
(ii) $N_j(F)$ is one-sided of slope $\lambda_j$, for all $1 \leqslant j < i$;
(iii) $R_j(F) \sim \psi_j^{a_j}$, for a certain positive exponent $a_j$, for all $1 \leqslant j < i$.

If $F$ is irreducible and $\mathbf{t}_F$ is an OM representation of $F$, then $F$ is of type $\mathbf{t}_F$. The following properties of the polynomials of a certain type are taken from [**6**, Lemma 2.4, Corollary 2.18].

Lemma 2.6. *Let* $\mathbf{t}$ *be a type of order* $i - 1 \geqslant 0$*, and let* $F(x) \in \mathcal{O}[x]$ *be a monic polynomial of positive degree. Then, the following conditions are equivalent:*

(i) *$F$ is of type* $\mathbf{t}$*;*
(ii) $\deg F = m_i \operatorname{ord}_{\mathbf{t}}(F)$*;*
(iii) *all irreducible factors of $F$ in $\mathcal{O}[x]$ are divisible by* $\mathbf{t}$.

*In this case, we have* $N_i(F) = N_i^-(F)$.

Lemma 2.7. *Let* $\mathbf{t}$ *be as above and let* $F, G \in \mathcal{O}[x]$ *be monic irreducible separable polynomials, both divisible by* $\mathbf{t}$*. Let* $\ell(F), \ell(G), \lambda(F), \lambda(G)$ *be the lengths and the slopes of the Newton polygons* $N_i(F)$*,* $N_i(G)$*, respectively. Then,*

$$v(\operatorname{Res}(F, G)) \geqslant f_0 \ldots f_{i-1}\ell(F)\ell(G)(V_i + \min\{|\lambda(F)|, |\lambda(G)|\}).$$

*Proof.* For all $0 \leqslant j < i$, denote $\ell_{j+1}(F) := \ell(N_{j+1}(F)) = \operatorname{ord}_{\operatorname{Trunc}_j(\mathbf{t})}(F) = \operatorname{ord}_{\psi_j} R_j(F)$, the last equalities by Lemma 1.5(ii). Since $R_j(F) \sim \psi_j^{\ell_{j+1}(F)}$ and $\deg R_j(F)$ coincides with the degree $\ell_j(F)/e_j$ of the unique side of $N_j(F)$, we have

$$\ell_j(F) = e_j \deg R_j(F) = e_j f_j \ell_{j+1}(F) = (e_j f_j) \ldots (e_{i-1} f_{i-1})\ell(F), \quad 1 \leqslant j < i. \tag{2.3}$$

We consider an analogous notation and equality for the polynomial $G$.

We now apply an inequality concerning the $v$-value of the resultant of two polynomials in terms of their Newton polygons [**6**, Theorem 4.10]:

$$\begin{aligned} v(\operatorname{Res}(F, G)) &\geqslant \operatorname{Res}_1(F, G) + \ldots + \operatorname{Res}_i(F, G) \\ &:= \sum_{1 \leqslant j < i} f_0 \ldots f_{j-1}\ell_j(F)\ell_j(G)|\lambda_j| + f_0 \ldots f_{i-1}\ell(F)\ell(G) \min\{|\lambda(F)|, |\lambda(G)|\} \\ &= f_0 \ldots f_{i-1}\ell(F)\ell(G)(V_i + \min\{|\lambda(F)|, |\lambda(G)|\}), \end{aligned}$$

the last equality by (2.3) and the explicit formula for $V_i$ in Section 1. □

Lemma 2.8. *Let* $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots ; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1}))$ *be a strongly optimal type of order* $i - 1 \geqslant 0$*, and* $\phi(x) \in \mathcal{O}[x]$ *a representative of* $\mathbf{t}$*. Let* $F(x) \in \mathcal{O}[x]$ *be a monic polynomial*

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

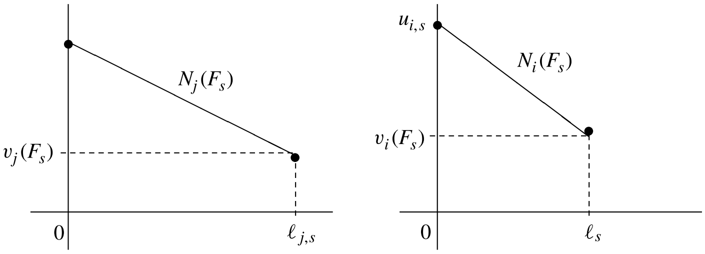


FIGURE 1. *Newton polygons $N_j(F_s)$, $N_i(F_s)$, for $1 \leqslant j < i$.*

*of type* $\mathbf{t}$ *and degree* $n > m_i$. *Then,*

$$\frac{v_i(F) + \ell|\lambda_{\min}|}{e_0 \ldots e_{i-1}} \leqslant \frac{2\delta(F)}{n},$$

*where* $\delta(F) := v(\mathrm{Disc}(F))$, $\ell$ *is the length of the Newton polygon* $N_i(F)$ *with respect to the pair* $(\mathbf{t}, \phi)$, *and* $\lambda_{\min}$ *is the slope of* $N_i(F)$ *for which* $|\lambda_{\min}|$ *is minimal.*

*Proof.* Let $F = F_1 \ldots F_g$ be the factorization of $F$ into a product of monic irreducible polynomials in $\mathcal{O}[x]$, with degrees $n_1, \ldots, n_g$, respectively. By Lemma 2.6, all factors $F_s(x)$ are of type $\mathbf{t}$, $N_i(F) = N_i^-(F)$, and $N_i(F_s) = N_i^-(F_s)$.

For $1 \leqslant s \leqslant g$ and $1 \leqslant j \leqslant i$, we introduce the following notation (see Figure 1):

$\ell := \ell(N_i(F)), \quad \ell_{j,s} := \ell(N_j(F_s)), \quad \ell_s := \ell_{i,s} = \ell(N_i(F_s));$
$u_{i,s} :=$ the ordinate of the left end point of $N_i(F_s)$;
$\mu_s :=$ the slope of $N_i(F_s)$.

We may have $F_s(x) = \phi(x)$ for some factors. In this case, $N_i(F_s)$ is one-sided of slope $\mu_s = -\infty$ [6, § 1.1], and $u_{i,s} = \infty$, $\ell_s = 1$.

By Lemmas 1.5 and 2.6, we have $n = m_i\ell$ and $n_s = m_i\ell_s$, for all $1 \leqslant s \leqslant g$. By the theorem of the product [6, Theorem 2.26],

$$N_i(F) = N_i(F_1) + \ldots + N_i(F_g), \tag{2.4}$$

so that $\ell = \ell_1 + \ldots + \ell_g$ and $|\lambda_{\min}| = \min_{1\leqslant s\leqslant g}\{|\mu_s|\}$. Now, we divide the factors $F_s$ into two categories, according to $\ell_s > 1$ or $\ell_s = 1$.

If $\ell_s > 1$, then $\deg \phi = m_i < n_s$. Let $\theta_s \in \overline{k}$ be a root of $F_s$ and choose a representative $\phi_i$ of $\mathbf{t}$ such that the value $v(\phi_i(\theta_s))$ is maximal (cf. Proposition 1.8). Denote by $N_i'$ the Newton polygon operator with respect to the pair $(\mathbf{t}, \phi_i)$; let $\lambda_{i,s}$ be the slope of the one-sided polygon $N_i'(F_s)$, and let $\psi_{i,s}$ be the irreducible factor of the corresponding residual polynomial $R_i'(F_s)$. By [4, Theorem 3.9], the Okutsu depth of $F_s$ is greater than or equal to $i$, and the type

$$(\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1}); (\phi_i, \lambda_{i,s}, \psi_{i,s})),$$

is the truncation of an OM representation (1.2) of $F_s$. On the other hand, [5, Theorem 3.1] shows that the Newton polygons $N_i(F_s)$, $N_i'(F_s)$ have the same right end point, and $|\mu_s| \leqslant |\lambda_{i,s}|$. Thus, $u_{i,s}$ is less than or equal to the ordinate of the left end point of $N_i'(F_s)$, and Lemma 2.2 and (2.2) show that

$$2\delta(F_s) \geqslant \frac{n_s u_{i,s}}{e_0 \ldots e_{i-1}} = \frac{n_s \ell_s (V_i + |\mu_s|)}{e_0 \ldots e_{i-1}} \geqslant \frac{(\ell_s)^2 m_i (V_i + |\lambda_{\min}|)}{e_0 \ldots e_{i-1}}. \tag{2.5}$$

On the other hand, if $\ell_s = 1$, the type $\mathbf{t}$ is $F_s$-complete (cf. Definition 1.1), $\deg F_s = m_i$ and the Okutsu depth of $F_s$ is $i - 1$. In this case, the ordinate $u_{i,s}$ is not a canonical invariant of $F_s$; for instance, we may have $u_{i,s} = \infty$, if $F_s = \phi$. Nevertheless, if $i > 1$, let us denote by $u_{i-1,s}$

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

the ordinate of the left end point of $N_{i-1}(F_s)$; by the very definition of the MacLane valuation $v_i$, we have $\ell_s V_i = v_i(F_s) = e_{i-1}u_{i-1,s}$, and Lemma 2.2 shows that

$$2\delta(F_s) \geqslant \frac{n_s u_{i-1,s}}{e_0 \dots e_{i-2}} = \frac{n_s \ell_s V_i}{e_0 \dots e_{i-1}} = \frac{(\ell_s)^2 m_i V_i}{e_0 \dots e_{i-1}}. \tag{2.6}$$

If $i=1$, we have $V_1 = 0$, so that (2.6) holds in this case too.

We are ready to prove the lemma. On one hand, since $v_i(F) = \ell V_i$, we have

$$n(v_i(F) + \ell|\lambda_{\min}|) = n\ell(V_i + |\lambda_{\min}|) = m_i \ell^2 (V_i + |\lambda_{\min}|).$$

On the other hand, since $f_0 \dots f_{i-1} = m_i/(e_0 \dots e_{i-1})$ and

$$\delta(F) = \sum_{1\leqslant s\leqslant g} \delta(F_s) + 2 \sum_{1\leqslant s<t\leqslant g} v(\operatorname{Res}(F_s, F_t)),$$

by (2.5), (2.6) and Lemma 2.7, we obtain

$$\begin{aligned} 2e_0 \dots e_{i-1}\delta(F) \geqslant{}& m_i V_i \Bigg( \sum_{1\leqslant s\leqslant g} (\ell_s)^2 + 4 \sum_{1\leqslant s<t\leqslant g} \ell_s \ell_t \Bigg) \\ &+ m_i|\lambda_{\min}| \Bigg( \sum_{s\in I} (\ell_s)^2 + 4 \sum_{1\leqslant s<t\leqslant g} \ell_s\ell_t \Bigg), \end{aligned}$$

where $I := \{1 \leqslant s \leqslant g \mid \ell_s > 1\}$. Thus, in order to prove the lemma it is sufficient to check that

$$\sum_{s\in I} (\ell_s)^2 + 4 \sum_{1\leqslant s<t\leqslant g} \ell_s \ell_t \geqslant (\ell_1 + \dots + \ell_g)^2.$$

It is an easy exercise to show that this is always the case, with the only exception $g=1$, $\ell_1 = 1$. But in this case, $\deg F = m_i$, which is against our assumption. □

Lemma 2.9. *Let* $\mathbf{t}$ *be a type of order* $i-1$ *and* $\phi$ *a representative of* $\mathbf{t}$. *Let* $F, G \in \mathcal{O}[x]$ *be two polynomials such that* $F \equiv G \pmod{\mathfrak{m}^\nu}$, *for some positive integer* $\nu$. *Let* $S$ *be a side of* $N_i^-(F)$ *of slope* $\lambda$ *and right end point* $(\ell, u)$, *such that* $u + \ell|\lambda| < e_0 \dots e_{i-1}\nu$. *Then,* $S$ *is a side of* $N_i^-(G)$ *and* $R_{\lambda,i}(F) = R_{\lambda,i}(G)$.

*Proof.* Let $F(x) = \sum_{0\leqslant s} a_s(x)\phi(x)^s$, $G(x) = \sum_{0\leqslant s} b_s(x)\phi(x)^s$, be the canonical $\phi$-expansions of $F$ and $G$, respectively. For the elements $a \in \mathcal{O}$, we have $v_i(a) = e_0 \dots e_{i-1}v(a)$, by Lemma 1.5; thus, $v_i(F-G) \geqslant e_0 \dots e_{i-1}\nu$, by the hypothesis. Since $F(x) - G(x) = \sum_{0\leqslant s} (a_s(x) - b_s(x))\phi(x)^s$ is the canonical $\phi$-expansion of $F-G$, [6, Lemma 2.17] shows that

$$e_0 \dots e_{i-1}\nu \leqslant v_i(F-G) = \min\{v_i((a_s - b_s)\phi^s) \mid 0 \leqslant s\}.$$

Therefore, the two clouds of points $\{(s, v_i(a_s\phi^s)) \mid 0 \leqslant s\}$, $\{(s, v_i(b_s\phi^s)) \mid 0 \leqslant s\}$, have the same points with ordinate less than $e_0 \dots e_{i-1}\nu$. Let $L$ be the line of slope $\lambda$ containing $S$. No point of the cloud of $F$ lies below the line $L$, and only the points of $S$ lie on this line. The condition $u + \ell|\lambda| < e_0 \dots e_{i-1}\nu$ implies that the cloud of points of $G$ has the same properties. Thus, $S$ is also a side of $N_i^-(G)$.

Let $\lambda = -h/e$, with $h, e$ positive coprime integers. Let $v_{i+1}$ be the MacLane valuation determined by $\mathbf{t}$, $\phi$, $\lambda$. By the definition of $v_{i+1}$ (cf. Section 1),

$$v_{i+1}(F-G) \geqslant e_0 \dots e_{i-1}e\nu > e(u + \ell|\lambda|) = v_{i+1}(F) = v_{i+1}(G).$$

Therefore, $R_{\lambda,i}(F) = R_{\lambda,i}(G)$, by [6, Proposition 2.8]. □

*Proof of Theorem 2.3.* The first item of Theorem 2.3 was proved right after Corollary 2.4. Let us prove the second item. Let $r$ be the Okutsu depth of $G(x)$. Let $\mathbf{t}_G$ be an OM representation

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

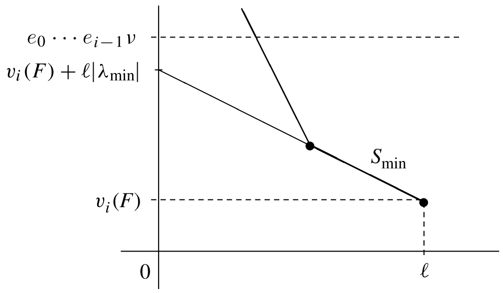


FIGURE 2. *Newton polygon $N_i(F)$ in the context of the proof of Theorem 2.3.*

of $G(x)$ as in (1.2), and consider the strongly optimal type

$$\mathbf{t} := \mathrm{Trunc}_r(\mathbf{t}_G) = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots ; (\phi_r, \lambda_r, \psi_r)),$$

admitting $G$ as a representative. In order to prove the theorem, it is sufficient to show that

$$N_i(F) = N_i(G), \quad R_i(F) = R_i(G), \quad 1 \leqslant i \leqslant r. \tag{2.7}$$

In fact, $R_r(F) = R_r(G)$ implies that $\mathbf{t}$ is $F$-complete too; thus, $F$ is a representative of $\mathbf{t}$, and $F \approx G$, by the definition of $\approx$.

By hypothesis, $F \equiv G \equiv \psi_0^{a_0} \pmod{\mathfrak{m}}$, for a certain positive exponent $a_0$. Let us prove (2.7) by induction on $i$. We assume that it is true for all $1 \leqslant j < i$ (thus, we make an empty assumption if $i = 1$). Since $G$ is a polynomial of type $\mathbf{t}$, our assumption implies that $F$ satisfies the conditions of Lemma 2.8; thus,

$$\frac{v_i(F) + \ell|\lambda_{\min}|}{e_0 \ldots e_{i-1}} \leqslant \frac{2\delta(F)}{n} < \nu, \tag{2.8}$$

where $\ell = \ell(N_i(F))$ and $\lambda_{\min}$ is the largest slope of this polygon ($|\lambda_{\min}|$ is minimal).

Let $S_{\min}$ be the side of $N_i(F)$ of slope $\lambda_{\min}$. By Lemma 2.9, $S_{\min}$ is one of the sides of $N_i(G)$ (see Figure 2). Since $G$ is irreducible, $N_i(G)$ is one-sided, so that $N_i(G) = S_{\min}$. Thus, the left end point of $S_{\min}$ has abscissa zero, so that $N_i(F) = S_{\min} = N_i(G)$. Also, $R_i(F) = R_i(G)$, again by Lemma 2.9. □

REMARK 1. In [1], the *reduced discriminant* $\mathfrak{m}^{\delta^*(F)}$ of an arbitrary polynomial $F(x) \in \mathcal{O}[x]$ is introduced, and it is shown that Corollary 2.4 holds with $2\delta^*(F)$ in the place of $2\delta(F)/n$. However, the reduced discriminant does not satisfy $\delta^*(F) \leqslant \delta(F)/n$, so that Theorem 2.3 cannot be deduced from this result.

For instance, suppose $p$ is odd and consider $F(x) = x^4 + a\pi x^2 + b\pi^2 \in \mathcal{O}[x]$, with $ab(a^2 - 4b) \notin \mathfrak{m}$. This polynomial is irreducible; in fact, if we choose $\phi_1(x) = x$ as a lift of the irreducible factor of $\overline{F}$, the Newton polygon $N_1(F)$ is one-sided of slope $-1/2$ and $R_{-1/2,1}(F)(y) = y^2 + \overline{a}y + \overline{b}$ is irreducible in $\mathbb{F}[y]$. One checks easily that

$$\delta_0(F) = 2, \quad \delta^*(F) = 3, \quad \delta(F) = 6.$$

By the first item of Theorem 2.3, any monic polynomial $G(x) \in \mathcal{O}[x]$ of degree four such that $F \equiv G \pmod{\mathfrak{m}^3}$, is irreducible. If we do not know the irreducibility of $F$, Corollary 2.4 shows that we can test its irreducibility by working modulo $\mathfrak{m}^4$. However, according to the criterion of the reduced discriminant, we should work modulo $\mathfrak{m}^7$ to test the irreducibility of $F$.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

## 3. *OM factorizations of polynomials*

In this section, we deal with the problem of finding 'sufficiently good' approximations to the irreducible factors of a polynomial in $\mathcal{O}[x]$. We first extend the notion of Okutsu equivalence in Section 1 to non-irreducible polynomials.

Definition 3.1. Let $F, G \in \mathcal{O}[x]$ be monic separable polynomials, and let $F = F_1 \dots F_g$, $G = G_1 \dots G_{g'}$ be their factorization into a product of monic irreducible polynomials in $\mathcal{O}[x]$. We say that $F$ and $G$ are *Okutsu equivalent*, and we write $F \approx G$, if $g = g'$ and $F_s \approx G_s$ for all $1 \leqslant s \leqslant g$, up to ordering.

An expression of the form, $F \approx P_1 \dots P_g$, with $P_1, \dots, P_g \in \mathcal{O}[x]$ irreducible, is called an *Okutsu factorization* of $F$.

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

Definition 3.2. Let $F \approx P_1 \dots P_g$ be an Okutsu factorization of a monic separable polynomial $F \in \mathcal{O}[x]$. For each $1 \leqslant s \leqslant g$, let $F_s$ be the irreducible factor of $F$ which is Okutsu equivalent to $P_s$, and let $\theta_s \in k^{\mathrm{sep}}$ be a root of $F_s$.

We say that $F \approx P_1 \dots P_g$ is an *OM factorization of* $F$ if

$$v(P_s(\theta_s)) > v(P_s(\theta_t)), \quad \forall\, 1 \leqslant s \neq t \leqslant g. \tag{3.1}$$

### 3.1. *OM factorizations and OM representations*

In this section, we study basic properties of the OM factorizations and we find a characterization of condition (3.1) in terms of OM representations of the factors of $F$, which facilitates the computation of these factorizations in practice.

We denote by $\phi_i^{\mathbf{t}}$, $\lambda_i^{\mathbf{t}}$, $\psi_i^{\mathbf{t}}$, $V_i^{\mathbf{t}}$, etc. the data at the $i$th level of a type $\mathbf{t}$.

Lemma 3.3. *Let* $\mathbf{t}$, $\mathbf{t}'$ *be two strongly optimal types over* $\mathcal{O}$. *The following conditions are equivalent:*

(a) $\operatorname{Rep}(\mathbf{t}) = \operatorname{Rep}(\mathbf{t}')$, *where* $\operatorname{Rep}(\mathbf{t})$ *denotes the set of representatives of the type* $\mathbf{t}$*;*

(b) *there exist representatives* $\phi$, $\phi'$ *of* $\mathbf{t}$, $\mathbf{t}'$, *respectively, such that* $\phi \approx \phi'$*;*

(c) $\operatorname{ord}_{\mathbf{t}}(F) = \operatorname{ord}_{\mathbf{t}'}(F)$, *for all polynomials* $F \in \mathcal{O}[x]$.

*When these conditions are satisfied, we say that the types* $\mathbf{t}$ *and* $\mathbf{t}'$ *are* equivalent.

*Proof.* By Definition 1.7, (a) and (b) are equivalent. Suppose that $\mathbf{t}$ and $\mathbf{t}'$ admit a common representative $\phi$. By [4, Theorem 3.9], $[\phi_1^{\mathbf{t}}, \dots, \phi_r^{\mathbf{t}}]$ and $[\phi_1^{\mathbf{t}'}, \dots, \phi_{r'}^{\mathbf{t}'}]$, are Okutsu frames of $\phi$; thus, $r = r'$ and the two types have the same Okutsu invariants and MacLane valuations $v_1, \dots, v_{r+1}$ [4, Corollary 3.7]. Hence, the two types have the same Newton operators $N_{r+1}$, and (c) follows from Lemma 1.5(ii). Finally, since the representatives of $\mathbf{t}$ are monic polynomials $\phi$ of minimal degree such that $\operatorname{ord}_{\mathbf{t}}(\phi) = 1$, (c) trivially implies (a). □

If two strongly optimal types $\mathbf{t}$, $\mathbf{t}'$ of order $r$ are equivalent, then Lemmas 1.5 and 1.6 show that $\phi_i^{\mathbf{t}} \approx \phi_i^{\mathbf{t}'}$, for all $1 \leqslant i \leqslant r$. Since $\phi_i^{\mathbf{t}}$ is a representative of $\operatorname{Trunc}_{i-1}(\mathbf{t})$, the truncations of $\mathbf{t}$ and $\mathbf{t}'$ of any order $0 \leqslant i \leqslant r$ are equivalent too.

By [4, Theorems 3.5,3.9], the mapping, $\mathbf{t} \mapsto \operatorname{Rep}(\mathbf{t})$, induces a 1–1 correspondence between equivalence classes of strongly optimal types and equivalence classes of monic irreducible separable polynomials in $\mathcal{O}[x]$, under Okutsu equivalence.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

Let $F \in \mathcal{O}[x]$ be a monic irreducible separable polynomial, and let $r$ be its Okutsu depth. We recall that an *OM representation of* $F$ is just an optimal type $\mathbf{t}_F$ of order $r+1$, satisfying any of the following equivalent conditions:

– $\mathbf{t}_F$ is $F$-complete; that is $\operatorname{ord}_{\mathbf{t}_F}(F) = 1$;

– $\mathbf{t}_F \mid F$ and $F \approx \phi_{r+1}^{\mathbf{t}_F}$.

By Lemma 3.3, if $\mathbf{t}_F$ and $\mathbf{t}'_F$ are OM representations of $F$, the types $\operatorname{Trunc}_r(\mathbf{t}_F)$ and $\operatorname{Trunc}_r(\mathbf{t}'_F)$ are equivalent.

Definition 3.4. Let $F, G \in \mathcal{O}[x]$ be monic irreducible separable polynomials of Okutsu depth $r_F$, $r_G$, and let $\mathbf{t}_F$, $\mathbf{t}_G$ be OM representations of $F$, $G$. Take $\phi_0^{\mathbf{t}_F} = 1 = \phi_0^{\mathbf{t}_G}$, by convention. The *index of coincidence of $F$ and $G$* is the maximal index $0 \leqslant j \leqslant \min\{r_F+1, r_G+1\}$, such that $\phi_j^{\mathbf{t}_F} \approx \phi_j^{\mathbf{t}_G}$. We denote this index by $i(F,G)$.

The following properties of $i(F,G)$ are easy to check:

– $i(F,G)$ does not depend on the chosen OM representations $\mathbf{t}_F$, $\mathbf{t}_G$;

– $i(F,G)$ depends only on the classes of $F$ and $G$ modulo $\approx$;

– $F \approx G$ if and only if $i(F,G) = r_F + 1 = r_G + 1$.

The next result is easily deduced from [6, Proposition 3.5,(5)].

Proposition 3.5. *Let $F, G \in \mathcal{O}[x]$ be monic irreducible separable polynomials, and let $\theta \in k^{\mathrm{sep}}$ be a root of $F$. Let $\mathbf{t}$ be a type of order $i \geqslant 1$ over $\mathcal{O}$, such that $\mathbf{t} \mid F$ and* $\operatorname{Trunc}_{i-1}(\mathbf{t}) \mid G$. *Let $\lambda(G)$ be the slope of (the one-sided polygon) $N_i(G)$.Then,*

$$v(G(\theta))/\deg G \geqslant (V_i + \min\{|\lambda_i|, |\lambda(G)|\})/(m_i e_0 \ldots e_{i-1}),$$

*and equality holds if and only if $\mathbf{t} \nmid G$.*

Lemma 3.6. *Let $F, G \in \mathcal{O}[x]$ be monic irreducible separable polynomials, and let $\theta \in k^{\mathrm{sep}}$ be a root of $F$. Let $\mathbf{t}$ be a strongly optimal type of order $i$ over $\mathcal{O}$, such that $\mathbf{t} \mid F$. Then, the following conditions are equivalent:*

(a) $\mathbf{t} \mid G$;

(b) $i(F,G) > i$;

(c) $v(G(\theta))/\deg G > V_{i+1}/(m_{i+1} e_0 \ldots e_i) = v(\phi_i(\theta))/m_i$.

*Proof.* By [5, 6], the type $\mathbf{t}$ may be extended to an OM representation $\mathbf{t}_F$ of $F$. If $\mathbf{t} \mid G$, it may be extended to an OM representation $\mathbf{t}_G$ of $G$ too; thus, $\phi_{i+1}^{\mathbf{t}_F} \approx \phi_{i+1}^{\mathbf{t}_G}$, because they are both representatives of $\mathbf{t}$. Thus, (a) implies (b). Conversely, let $\mathbf{t}_G$ be an arbitrary OM representation of $G$, and suppose $\phi_{i+1}^{\mathbf{t}_F} \approx \phi_{i+1}^{\mathbf{t}_G}$. This implies that $\phi_{i+1}^{\mathbf{t}_G}$ is a representative of $\mathbf{t}$; thus, the types $\mathbf{t}$ and $\operatorname{Trunc}_i(\mathbf{t}_G)$ are equivalent. By the last item of Definition 1.1, $0 < \operatorname{ord}_{\mathbf{t}_G}(G) \leqslant \operatorname{ord}_{\operatorname{Trunc}_i(\mathbf{t}_G)}(G) = \operatorname{ord}_{\mathbf{t}}(G)$. Therefore, (a) and (b) are equivalent.

Let us show that (a) and (c) are equivalent. If $\psi_0^{\mathbf{t}} \nmid \overline{G}$, then $v(G(\theta)) = 0$ and $\mathbf{t} \nmid G$; thus (a) and (c) are both false in this case. Suppose $\psi_0^{\mathbf{t}} \mid \overline{G}$, and let $1 \leqslant j \leqslant i+1$ be maximal such that $\operatorname{Trunc}_{j-1}(\mathbf{t}) \mid G$. Let $\lambda_{i+1}$ be the slope of $N_{i+1}(F)$. The Newton polygon $N_j^-(G)$ with respect to $\mathbf{t}$ has a positive length by Lemma 1.5; let $\lambda(G) \in \mathbb{Q}_{<0}$ be its slope. By Proposition 3.5,

$$v(G(\theta))/\deg G \geqslant (V_j + \min\{|\lambda_j|, |\lambda(G)|\})/(m_j e_0 \ldots e_{j-1}),$$

and equality holds if $j \leqslant i$, because $\operatorname{Trunc}_j(\mathbf{t}) \nmid G$. If $\mathbf{t} \mid G$, then $j = i+1$, and $v(G(\theta))/\deg G > V_{i+1}/(m_{i+1} e_0 \ldots e_i)$. If $\mathbf{t} \nmid G$, then $j \leqslant i$, and

$$\frac{v(G(\theta))}{\deg G} \leqslant \frac{V_j + |\lambda_j|}{m_j e_0 \ldots e_{j-1}} = \frac{v(\phi_j(\theta))}{m_j} \leqslant \frac{v(\phi_i(\theta))}{m_i} = \frac{V_{i+1}}{m_{i+1} e_0 \ldots e_i},$$

by Lemma 1.5 and the properties (1.1) of the Okutsu polynomials. □

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

LEMMA 3.7. *Let $P, Q \in \mathcal{O}[x]$ be monic irreducible separable polynomials such that $P \approx Q$. Let $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_r, \lambda_r, \psi_r))$ be a strongly optimal type admitting $P$ as a representative. Then, there exist unique data $(\lambda_Q, \psi_Q)$ (or $(-\infty, —)$, if $P = Q$), such that $\mathbf{t}_Q := (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_r, \lambda_r, \psi_r); (P, \lambda_Q, \psi_Q))$, is an OM representation of $Q$.*

*Proof.* Since $Q$ is also a representative of $\mathbf{t}$, we have $\mathrm{ord}_{\mathbf{t}}(Q) = 1$, and the Newton polygon $N^-_{r+1}(Q)$ with respect to $\mathbf{t}$ and $P$ has length one by Lemma 1.5. Let $\lambda_Q \in \mathbb{Z} \cup \{-\infty\}$ be the slope of this polygon. If $\lambda_Q \neq -\infty$ (that is $P \neq Q$), the residual polynomial $R_{\lambda_Q, r+1}(Q)$ has degree one; let $\psi_Q$ be the monic polynomial obtained by dividing this polynomial by its leading coefficient. By construction, $\mathbf{t}_Q \mid Q$. By the last item of Definition 1.1, $\mathrm{ord}_{\mathbf{t}_Q}(Q) \leqslant \mathrm{ord}_{\mathbf{t}}(Q) = 1$; thus, $\mathrm{ord}_{\mathbf{t}_Q}(Q) = 1$, so that $\mathbf{t}_Q$ is an OM representation of $Q$. Also, once we choose $P$ as a representative of $\mathbf{t}$, the condition $\mathbf{t}_Q \mid Q$ uniquely determines these data $(\lambda_Q, \psi_Q)$. □

The computation of an Okutsu factorization $F \approx P_1 \dots P_g$ of a monic separable polynomial $F$ is equivalent to the computation of a family $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ of OM representations of the irreducible factors of $F$. In fact, from the Okutsu factors $P_1, \dots, P_g$ and strongly optimal types $\mathbf{t}_1, \dots, \mathbf{t}_g$ such that each $\mathbf{t}_s$ admits $P_s$ as a representative, we may construct the OM representations of $F_1, \dots, F_g$, as shown in Lemma 3.7. Conversely, from the family $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ we may take $P_s := \phi^{\mathbf{t}_{F_s}}_{r_s+1} \approx F_s$, as Okutsu factors, where $r_s$ is the Okutsu depth of $F_s$.

We now describe the property of being an OM factorization in terms of the family $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ of OM representations.

PROPOSITION 3.8. *Let $F \in \mathcal{O}[x]$ be a monic separable polynomial and $F_1, \dots, F_g \in \mathcal{O}[x]$ its monic irreducible factors, with Okutsu depth $r_1, \dots, r_g$, respectively. Let $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ be OM representations of the factors, and let $P_s := \phi^{\mathbf{t}_{F_s}}_{r_s+1}$. Let $I$ be the set of ordered pairs $(s, t)$ of indices such that $i(F_s, F_t) = r_s + 1$, and for each $(s, t) \in I$, let $\lambda_{s,t}$ be the slope of $N_{r_s+1, \mathbf{t}_{F_s}}(F_t)$. Then, the Okutsu factorization $F \approx P_1 \dots P_g$ is an OM factorization if and only if*

$$|\lambda_{s,s}| > |\lambda_{s,t}|, \quad \forall (s, t) \in I, \ \ s \neq t. \tag{3.2}$$

*Proof.* Denote $\mathbf{t}_s := \mathrm{Trunc}_{r_s}(\mathbf{t}_{F_s})$, and choose a root $\theta_s \in k^{\mathrm{sep}}$ of $F_s$, for each $1 \leqslant s \leqslant g$. Let $(s, t)$ be an ordered pair of indices, $1 \leqslant s, t \leqslant g$. Suppose $i(F_s, F_t) = r_s + 1$. Then, Lemma 3.6 shows that $\mathbf{t}_s \mid F_t$, and

$$v(P_s(\theta_t)) = (V^{\mathbf{t}_s}_{r_s+1} + |\lambda_{s,t}|)/e(F_s),$$

by Lemma 1.5. Suppose now $i := i(F_s, F_t) \leqslant r_s$. Since $i(P_s, F_t) = i(F_s, F_t) = i$, Lemma 3.6 shows that $\mathrm{Trunc}_i(\mathbf{t}_{F_t}) \nmid P_s$. By Proposition 3.5,

$$\begin{aligned} v(P_s(\theta_t)) &= \frac{m^{\mathbf{t}_s}_{r_s+1}}{m_i} \, \frac{V_i + \min\{|\lambda^{\mathbf{t}_s}_i|, |\lambda^{\mathbf{t}_t}_i|\}}{e_0 \dots e_{i-1}} \leqslant \frac{m^{\mathbf{t}_s}_{r_s+1}}{m_i} \, \frac{V_i + |\lambda^{\mathbf{t}_s}_i|}{e_0 \dots e_{i-1}} \\ &= \frac{m^{\mathbf{t}_s}_{r_s+1}}{m^{\mathbf{t}_s}_{i+1}} \, \frac{V^{\mathbf{t}_s}_{i+1}}{e^{\mathbf{t}_s}_0 \dots e^{\mathbf{t}_s}_i} \leqslant \frac{V^{\mathbf{t}_s}_{r_s+1}}{e(F_s)}, \end{aligned}$$

the last inequality by the explicit formulas of $V_j$ in Section 1. Hence, the condition (3.1) is equivalent to (3.2). □

DEFINITION 3.9. Let $F \in \mathcal{O}[x]$ be a monic separable polynomial and $F_1, \dots, F_g \in \mathcal{O}[x]$ the monic irreducible factors of $F$. We say that a family $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ of OM representations of the factors *faithfully represents* $F$ if any of the two following equivalent conditions is satisfied:

(a) $\mathbf{t}_{F_s} \nmid F_t$, $\forall\, 1 \leqslant s \neq t \leqslant g$;

(b) $\mathrm{ord}_{\mathbf{t}_{F_s}}(F) = 1$, $\forall\, 1 \leqslant s \leqslant g$.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

By construction, $\operatorname{ord}_{\mathbf{t}_{F_s}}(F_s) = 1$; hence, the conditions (a) and (b) are equivalent because $\operatorname{ord}_{\mathbf{t}_{F_s}}(F) = \sum_{1 \leqslant t \leqslant g} \operatorname{ord}_{\mathbf{t}_{F_s}}(F_t)$.

COROLLARY 3.10. *With the notation in Proposition 3.8, if $F \approx P_1 \dots P_g$ is an OM factorization, then the family $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ faithfully represents $F$.*

*Proof.* If $\mathbf{t}_{F_s} \mid F_t$, then $F_t$ is a polynomial of type $\mathbf{t}_{F_s}$ (Lemma 2.6) and this implies $\lambda_{s,t} = \lambda_{s,s}$ (Definition 2.5). □

Finally, we show that any family of OM representations that faithfully represents a polynomial $F$, leads immediately to an OM factorization of $F$.

LEMMA 3.11. *Let $F \in \mathcal{O}[x]$ be a monic separable polynomial and $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ a family of OM representations of the irreducible factors of $F$, that faithfully represents $F$. Then, if we take arbitrary representatives $Q_1, \dots, Q_g$ of these types, we get an OM factorization, $F \approx Q_1 \dots Q_g$, of $F$.*

*Proof.* We keep the notation from Proposition 3.8. Consider an index $1 \leqslant s \leqslant g$. All data $e_j, f_j, h_j, V_j$ we are going to use correspond to the type $\mathbf{t}_{F_s}$. Since $\operatorname{ord}_{\mathbf{t}_{F_s}}(F_s) = 1$, the Newton polygon $N^-_{r_s+2,\mathbf{t}_{F_s}}(F_s)$ has length one and slope $-h_s \in \mathbb{Z}_{<0} \cup \{-\infty\}$. By [6, Theorem 3.1],

$$v(Q_s(\theta_s)) = (V_{r_s+2} + h_s)/e(F_s) = (V_{r_s+1} + |\lambda_{s,s}| + h_s)/e(F_s),$$

the last equality by the recurrence $V_{r_s+2} = e_{r_s+1} f_{r_s+1}(e_{r_s+1} V_{r_s+1} + h_{r_s+1})$, in Section 1, having in mind that $e_{r_s+1} = f_{r_s+1} = 1$ and $h_{r_s+1} = |\lambda_{s,s}|$.

For all $t \neq s$, we have $\mathbf{t}_{F_s} \nmid F_t$. If $\mathbf{t}_s \mid F_t$, then Proposition 3.5 shows that

$$v(Q_s(\theta_t)) = (V_{r_s+1} + \min\{|\lambda_{s,s}|, |\lambda_{s,t}|\})/e(F_s) < v(Q_s(\theta_s)).$$

If $\mathbf{t}_s \nmid F_t$, then $i := i(F_s, F_t) = i(Q_s, F_t) \leqslant r_s$, and $\operatorname{Trunc}_i(\mathbf{t}_{F_t}) \nmid Q_s$, by Lemma 3.6. Thus, $v(Q_s(\theta_t)) \leqslant V_{r_s+1}/e(F_s) < v(Q_s(\theta_s))$, as in the proof of Proposition 3.8. □

Let us see an example. Take $a, b \in \mathcal{O}$ such that $v(ab) = 0$ and consider

$$F_1 = x + \pi + \pi^2 + \pi^4 a, \quad F_2 = x + \pi + \pi^3 + \pi^4 b, \quad F = F_1 F_2.$$

The Okutsu factorizations, $F \approx x^2 \approx x(x + \pi)$, are not OM factorizations of $F$, because they both lead to $\mathbf{t}_{F_1} = (y; (x, -1, y + 1)) \mid F_2$.

The Okutsu factorization $F \approx (x + \pi)^2$ leads to a family of OM representations that faithfully represents $F$, because these Okutsu factors are sufficiently close to the true factors to distinguish them:

$$\mathbf{t}_{F_1} = (y; (x + \pi, -2, y + 1)) \nmid F_2, \quad \mathbf{t}_{F_2} = (y; (x + \pi, -3, y + 1)) \nmid F_1.$$

Let us choose as representatives of the above types $\mathbf{t}_{F_1}$, $\mathbf{t}_{F_2}$, the polynomials $Q_1 = x + \pi + \pi^2$, $Q_2 = x + \pi + \pi^3$. By Lemma 3.11, $F \approx Q_1 Q_2$ is an OM factorization. The new OM representations of $F_1$, $F_2$ determined by $Q_1$, $Q_2$ are:

$$\mathbf{t}_{F_1} = (y; (x + \pi + \pi^2, -4, y + \overline{a})), \quad \mathbf{t}_{F_2} = (y; (x + \pi + \pi^3, -4, y + \overline{b})).$$

The Montes algorithm computes a family $\mathbf{t}_{F_1}, \dots, \mathbf{t}_{F_g}$ of OM representations faithfully representing $F$, and derives from it an OM factorization $F \approx P_1 \dots P_g$, as indicated in Lemma 3.11 (cf. Section 4). This is the starting point for the fast computation of an approximate factorization of $F$ with a prescribed precision, by means of the single-factor algorithm [9].

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

### 3.2. *Polynomials having the same OM factorizations*

The aim of this section is to prove Theorem 3.13, where we find the least precision $\nu$ such that two polynomials congruent modulo $\mathfrak{m}^\nu$ have the same OM factorizations. To this end, we need a result similar in spirit to Lemma 2.8.

LEMMA 3.12. *Let* $\mathbf{t}$ *be a strongly optimal type of order* $i-1\geqslant 0$, *and* $\phi\in\mathcal{O}[x]$ *a representative of* $\mathbf{t}$. *Let* $F\in\mathcal{O}[x]$ *be a monic polynomial such that* $\ell(N_i^-(F))>1$, *and denote* $\delta(F):=v(\mathrm{Disc}(F))$. *Let* $S_{\max}$ *be the first side (from left to right) of* $N_i^-(F)$ *and let* $\lambda_{\max}$ *be its slope. Let* $u>u'$ *be the ordinates of the end points of* $S_{\max}$. *If* $\ell(S_{\max})=1$, *let* $S_{\text{next}}$ *be the second side of* $N_i^-(F)$ *and let* $\lambda_{\text{next}}$ *be its slope. Then,*

$$\delta(F)\geqslant\begin{cases}u, & \text{if } \ell(S_{\max})>1,\\ u'+|\lambda_{\text{next}}|, & \text{if } \ell(S_{\max})=1.\end{cases}$$

*Proof.* Let $F=F_1\dots F_g$ be the factorization of $F$ into a product of monic irreducible polynomials in $\mathcal{O}[x]$. For all $1\leqslant j\leqslant i$, $1\leqslant s\leqslant g$, denote:

$\mathbf{t}_{j-1}:=\mathrm{Trunc}_{j-1}(\mathbf{t})$;
$\ell_{j,s}:=\ell(N_j^-(F_s))=\mathrm{ord}_{\mathbf{t}_{j-1}}(F_s)$, the abscissa of the right end point of $N_j^-(F_s)$;
$u_{j,s}:=$ the ordinate of the left end point of $N_j^-(F_s)$.

By [6, Lemma 2.17], the right end point of $N_j^-(F_s)$ is $(\ell_{j,s},v_j(F_s))$. If $\mathbf{t}_{j-1}\mid F_s$, then Lemma 2.6 shows that $\deg F_s=m_j\ell_{j,s}$. In particular, $v_j(F_s)=\ell_{j,s}V_j$ and $u_{j,s}=\ell_{j,s}(V_j+|\lambda_{j,s}|)$, where $\lambda_{j,s}$ is the slope of $N_j^-(F_s)$. If $\mathbf{t}_{j-1}\nmid F_s$, then $\ell_{j,s}=0$ and $u_{j,s}=v_j(F_s)$.

By the theorem of the product (2.4), $u=u_{i,1}+\dots+u_{i,g}$, and there exists an irreducible factor $F_{s_0}$ such that $N_i^-(F_{s_0})$ is one-sided of slope $\lambda_{\max}$. Since $F_{s_0}$ is a polynomial of type $\mathbf{t}$, Lemma 2.6 shows that $\deg F_{s_0}=m_j\ell_{j,s_0}$, for all $1\leqslant j\leqslant i$.

CLAIM. For all $s\neq s_0$, we have $v(\mathrm{Res}(F_s,F_{s_0}))\geqslant u_{i,s}$.

In fact, suppose first that $\mathbf{t}\nmid F_s$. Let $0\leqslant j<i$ be the first level such that $\mathbf{t}_j\nmid F_s$. For all $j<k\leqslant i$, the Newton polygon $N_k^-(F_s)$ is the single point $(0,v_k(F_s))$. By the definition of the MacLane valuations, $u_{i,s}=v_i(F_s)=e_{i-1}\dots e_{j+1}v_{j+1}(F_s)$. If $j=0$, then $v_1(F_s)=0$ and we deduce that $u_{i,s}=0$. If $0<j<i$, then $\mathbf{t}_{j-1}\mid F_s$, and $v_{j+1}(F_s)=e_j(v_j(F_s)+\ell_{j,s}\min\{|\lambda_{j,s}|,|\lambda_j|\})$, by the definition of $v_{j+1}$. Hence,

$$u_{i,s}=e_{i-1}\dots e_j\ell_{j,s}(V_j+\min\{|\lambda_{j,s}|,|\lambda_j|\})\leqslant e_{i-1}\dots e_j\ell_{j,s}(V_j+|\lambda_{j,s}|).$$

On the other hand, Lemma 2.7 applied to the type $\mathbf{t}_{j-1}$ shows that

$$\begin{aligned}v(\mathrm{Res}(F_s,F_{s_0}))&\geqslant f_0\dots f_{j-1}\ell_{j,s}\ell_{j,s_0}(V_j+\min\{|\lambda_{j,s}|,|\lambda_{\max}|\})\\&=m_j\ell_{j,s}\ell_{j,s_0}\frac{V_j+|\lambda_{j,s}|}{e_0\dots e_{j-1}}=\deg(F_{s_0})\ell_{j,s}\frac{V_j+|\lambda_{j,s}|}{e_0\dots e_{j-1}}\\&\geqslant m_i\ell_{j,s}\frac{V_j+|\lambda_{j,s}|}{e_0\dots e_{j-1}}\geqslant e_{i-1}\dots e_j\ell_{j,s}(V_j+|\lambda_{j,s}|)\geqslant u_{i,s}.\end{aligned}$$

If $\mathbf{t}\mid F_s$, we have directly $u_{i,s}=\ell_{i,s}(V_i+|\lambda_{i,s}|)\leqslant v(\mathrm{Res}(F_s,F_{s_0}))$, by Lemma 2.7 applied to the type $\mathbf{t}$. This ends the proof of the claim.

From now on, we denote $\rho_{s,t}:=v(\mathrm{Res}(F_s,F_t))$. We are ready to deduce the lemma from the claim and the equality

$$\delta(F)=\sum_{1\leqslant s\leqslant g}\delta(F_s)+\sum_{1\leqslant s,t\leqslant g}\rho_{s,t}.$$

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

Suppose first that there is at least one $F_{s_1} \neq F_{s_0}$, such that $\mathbf{t} \mid F_{s_1}$ and $\lambda_{i,s_1} = \lambda_{\max}$. In this case, the claim shows by symmetry that $\rho_{s_1,s_0} \geqslant u_{i,s_0}$; hence,

$$\delta(F) \geqslant 2\rho_{s_1,s_0} + \sum_{s \neq s_0,s_1} \rho_{s,s_0} \geqslant \sum_{1 \leqslant s \leqslant g} u_{i,s} = u.$$

Suppose now that for all $F_s \neq F_{s_0}$, such that $\mathbf{t} \mid F_s$, we have $\lambda_{i,s} \neq \lambda_{\max}$. In this case, $\ell_{i,s_0} = \ell(S_{\max})$ and $u = u' + \ell_{i,s_0}|\lambda_{\max}|$. If $\ell_{i,s_0} > 1$, we have $\deg F_{s_0} = m_i \ell_{i,s_0} \geqslant 2m_i$, so that the Okutsu depth of $F_{s_0}$ is greater than or equal to $i$. Lemma 2.2 shows that $2\delta(F_{s_0})/\deg F_{s_0} \geqslant u_{i,s_0}/(e_0 \ldots e_{i-1})$, and we deduce that $\delta(F_{s_0}) \geqslant m_i u_{i,s_0}/(e_0 \ldots e_{i-1}) \geqslant u_{i,s_0}$. Hence,

$$\delta(F) \geqslant \delta(F_{s_0}) + \sum_{s \neq s_0} \rho_{s,s_0} \geqslant \sum_{1 \leqslant s \leqslant g} u_{i,s} = u.$$

Finally, suppose that $\ell_{i,s_0} = \ell(S_{\max}) = 1$. In this case, $\operatorname{ord}_{\mathbf{t}}(F_{s_0}) = \ell_{i,s_0} = 1$, $v_i(F_{s_0}) = \ell_{i,s_0} V_i = V_i$, and $u_{i,s_0} = V_i + |\lambda_{\max}|$. Since $\ell(N_i^-(F)) > 1$, this polygon has at least a second side $S_{\text{next}}$ of slope $\lambda_{\text{next}}$. Let $I$ be the set of all indices $1 \leqslant t \leqslant g$ such that $N_i^-(F_t)$ has slope $\lambda_{\text{next}}$. By the claim, for all $t \in I$, we have

$$2\rho_{t,s_0} \geqslant 2u_{i,t} = \ell_{i,t}(V_i + |\lambda_{\text{next}}|) + u_{i,t} \geqslant v_i(F_{s_0}) + |\lambda_{\text{next}}| + u_{i,t},$$

so that

$$\begin{aligned} \delta(F) &\geqslant 2\sum_{t \in I} \rho_{t,s_0} + \sum_{s \notin I \cup \{s_0\}} \rho_{s,s_0} \geqslant v_i(F_{s_0}) + |\lambda_{\text{next}}| + \sum_{s \neq s_0} u_{i,s} \\ &= |\lambda_{\text{next}}| + \left(\sum_{s} u_{i,s}\right) - |\lambda_{\max}| = |\lambda_{\text{next}}| + u'. \end{aligned}$$ □

REMARK 2. In Lemma 3.12, if $\phi$ divides $F$, then we understand that $S_{\max}$ is a side of slope $\lambda_{\max} = -\infty$, and $u = \infty$ [6, § 1.1]. The statement of the lemma and all arguments in the proof remain valid in this case.

It is easy to construct examples showing that the inequalities of Lemma 3.12 are sharp. For instance, $F(x) = x^2 + \pi^\nu$ has $u = \delta = \nu$ (if $v(2) = 0$); while $F(x) = (x + \pi^\nu)(x + \pi)$ has $u' = |\lambda_{\text{next}}| = 1$ and $\delta = 2$, if $\nu > 1$.

THEOREM 3.13. *Let $F, G \in \mathcal{O}[x]$ be monic separable polynomials, and denote $\delta(F) := v(\operatorname{Disc}(F))$. If $F \equiv G \pmod{\mathfrak{m}^{\delta(F)+1}}$, then $F \approx G$ and any OM factorization $F \approx P_1 \ldots P_g$ of $F$ is also an OM factorization $G \approx P_1 \ldots P_g$ of $G$.*

*Proof.* Let $F_1, \ldots, F_g$ be the monic irreducible factors of $F$, ordered so that $F_s \approx P_s$, for all $1 \leqslant s \leqslant g$. Our aim is to attach to every $P_s$ an irreducible factor $G_s$ of $G$, such that $G_s \approx P_s$ and either (3.1) or (3.2) are satisfied for the pair $P_s, G$.

Let us fix an index $1 \leqslant s \leqslant g$. Let $r$ be the Okutsu depth of $P_s$ and let

$$\mathbf{t}_{F_s} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (P_s, \lambda_{F_s}, \psi_{F_s})),$$

be the OM representation of $F_s$ determined by $P_s$, satisfying $\mathbf{t}_{F_s} \nmid F_t$ for all $t \neq s$. We admit exact OM representations in which $\lambda_{F_s} = -\infty$ and $\psi_{F_s}$ is not defined.

Consider the strongly optimal type $\mathbf{t} := \operatorname{Trunc}_r(\mathbf{t}_{F_s})$. Since $F_s \approx P_s$, the polynomial $F_s$ is a representative of $\mathbf{t}$ too; thus, $\operatorname{ord}_{\mathbf{t}}(F_s) = 1$. The proof of the theorem requires different arguments according to $\operatorname{ord}_{\mathbf{t}}(F) = 1$ or $\operatorname{ord}_{\mathbf{t}}(F) > 1$.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

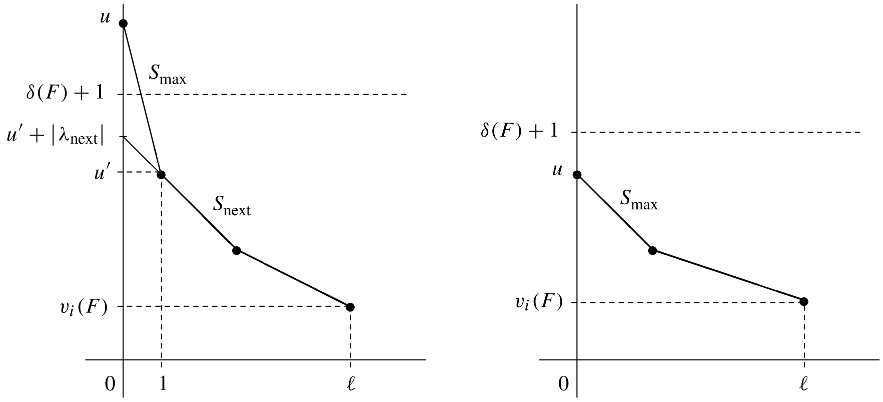


FIGURE 3. *Newton polygon $N_i^-(F)$ in the context of Lemma 3.12.*

*Case* $\mathrm{ord}_{\mathbf{t}}\,(F)=1$. Since $1=\mathrm{ord}_{\mathbf{t}}(F)=\sum_{1\leqslant t\leqslant g}\mathrm{ord}_{\mathbf{t}}(F_t)$, we have $\mathrm{ord}_{\mathbf{t}}(F_t)=0$, for all $t\neq s$. By Definition 1.7, $F_t\not\approx F_s\approx P_s$, for all $t\neq s$.

For monic polynomials $P,Q\in\mathcal{O}[x]$ of Okutsu depth zero we have $P\approx Q$ if and only if $\overline{P}=\overline{Q}$. Thus, if $r=0$, then $\overline{P_s}=\overline{F_s}=\psi_0$ is coprime to $\overline{F_t}$, for all $t\neq s$. By hypothesis, $\overline{G}=\overline{F}=\overline{F_1}\dots\overline{F_g}$; thus, by Hensel's lemma, $G$ has a unique irreducible factor (say) $G_s$, such that $\overline{G_s}=\psi_0$ is coprime to $\overline{G}/\overline{G_s}$. Hence, $P_s\approx G_s$, $v(P_s(\theta_s))>0$ and $v(P_s(\theta))=0$, for any choice of roots $\theta_s,\theta\in k^{\mathrm{sep}}$ of $G_s$ and $G/G_s$, respectively. Thus, (3.1) is satisfied for the pair $P_s,G$.

If $r>0$, we may consider $\mathbf{t}_{r-1}:=\mathrm{Trunc}_{r-1}(\mathbf{t})$. By the last item of Definition 1.1, $\mathrm{ord}_{\mathbf{t}_{r-1}}(F)\geqslant\mathrm{ord}_{\mathbf{t}_{r-1}}(F_s)\geqslant e_rf_r\,\mathrm{ord}_{\mathbf{t}}(F_s)>1$. Since $\mathbf{t}\mid F_s$, the polygon $N_r^-(F_s)$ is one-sided of slope $\lambda_r$ and it has length $\mathrm{ord}_{\mathbf{t}_{r-1}}(F_s)>1$, by Lemma 1.5. By (2.4), $N_r^-(F)$ has a side $S$ of slope $\lambda_r$ and length $\ell(S)>1$, where $\ell(S)$ is the length of the projection of $S$ to the horizontal axis.

We now apply Lemma 3.12 to the pair $\mathbf{t}_{r-1}$, $F$. If $\ell(S_{\max})=1$, then $S\neq S_{\max}$, because $\ell(S)>1$. In any case, Lemma 3.12 shows that $\delta(F)+1$ is greater than the ordinate of the point of the vertical axis lying on the line determined by $S$. By Lemma 2.9, the Newton polygon $N_r^-(G)$ has a side of slope $\lambda_r$ and $R_r(G)=R_r(F)$; thus, $\mathrm{ord}_{\mathbf{t}}(G):=\mathrm{ord}_{\psi_r}R_r(G)=\mathrm{ord}_{\psi_r}R_r(F)=:\mathrm{ord}_{\mathbf{t}}(F)=1$. Hence, there is a unique irreducible factor (say) $G_s$ of $G$, such that $\mathrm{ord}_{\mathbf{t}}(G_s)=1$, and $\mathrm{ord}_{\mathbf{t}}(G_0)=0$, for any other irreducible factor $G_0$ of $G$. By Lemma 2.6, $\deg G_s=m_{r_s+1}\,\mathrm{ord}_{\mathbf{t}}(G_s)=m_{r_s+1}$; thus, $G_s$ is a representative of $\mathbf{t}$, and $G_s\approx P_s$. Finally, the set $I$ in Proposition 3.8 contains only the pair $(s,s)$, so that (3.2) is trivially satisfied.

*Case* $\mathrm{ord}_{\mathbf{t}}\,(F)>1$. Since $F_s\approx P_s$ is a representative of $\mathbf{t}$, we have $\mathrm{ord}_{\mathbf{t}}(F_s)=1$, so that $N_{r+1}(F_s)$ has length one and slope $\lambda_{s,s}$, in the notation from Proposition 3.8. Since $F\approx P_1\dots P_g$ is an OM factorization, (3.2) holds; this implies that $N_{r+1}^-(F)$ indeed has a side $S_{\max}$ of slope $\lambda_{\max}=\lambda_{s,s}$ and end points $(0,u)$ and $(1,u')$, by the theorem of the product (2.4).

We now apply Lemma 3.12 to the pair $\mathbf{t}$, $F$. Arguing as before, $N_{r+1}^-(G)$ coincides with $N_{r+1}^-(F)$, except for, eventually, the ordinate $u$ of the point of abscissa zero (see Figure 3). Thus, $N_{r+1}^-(G)$ also has a first side $S_{\max}(G)$ of length one and slope $\lambda_{s,s}(G)$, with $|\lambda_{s,s}(G)|>|\lambda_{s,t}|$, for all $t$ such that $\mathbf{t}\mid F_t$. The equality of the Newton polygons (up to the first side) and the theorem of the product, show that all irreducible factors $G_0\neq G_s$ of $G$, which are divisible by $\mathbf{t}$, have $N_{r+1}(G_0)$ one-sided of slope $\lambda_{s,t}$ for some $t\neq s$. Hence, (3.2) is satisfied for $P_s,G$ as well. □

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

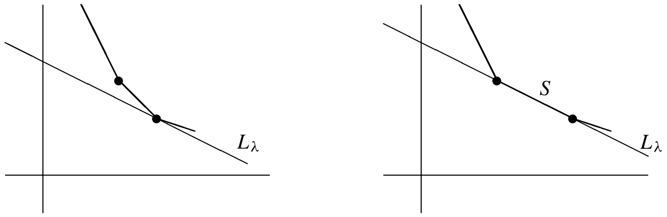


FIGURE 4. *The $\lambda$-component of a polygon; $L_\lambda$ is the line of slope $\lambda$ having first contact with the polygon from below.*

## 4. *The OM factorization algorithm*

Let us go back to the global setting of the introduction. Let $A$ be a Dedekind domain whose field of fractions $K$ is a global field. Let $L/K$ be a finite separable extension and $B$ the integral closure of $A$ in $L$. Let $\theta \in L$ be a primitive element of $L/K$, with minimal polynomial $F(x) \in A[x]$.

Let $\mathfrak{p}$ be a non-zero prime ideal of $A$, $v := v_{\mathfrak{p}}$ the canonical $\mathfrak{p}$-adic valuation, $K_{\mathfrak{p}}$ the completion of $K$ at $\mathfrak{p}$, and $\mathcal{O}_{\mathfrak{p}}$ the valuation ring of $K_{\mathfrak{p}}$. We denote by $\mathbb{F} = A/\mathfrak{p}$ the residue field of $\mathfrak{p}$. We fix a local generator $\pi$ of $\mathfrak{p}$; that is, an element $\pi \in A$, whose image in the local ring $A_{\mathfrak{p}}$ generates the maximal ideal. If $A$ is a principal domain, we assume moreover that $\mathfrak{p} = \pi A$.

We review in this section the factorization algorithm developed by Montes in his 1999 PhD thesis, inspired by the ideas of Ore and MacLane. It was first published in [5], based on the theoretical background developed in [6]. A short review may be found in the survey [12] as well.

The algorithm is based on four routines: `Factorization`, `Newton`, `ResidualPolynomial` and `Representative`. Let us briefly review them.

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

INPUT:
– A finite field $\mathcal{F}$.
– A monic polynomial $\varphi(y) \in \mathcal{F}[y]$.

OUTPUT:
– The factorization of $\varphi(y)$ into a product of irreducible polynomials of $\mathcal{F}[y]$.

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

INPUT:
– A type $\mathbf{t}$ over $A$, of order $i - 1 \geqslant 0$, and a representative $\phi \in A[x]$ of $\mathbf{t}$.
– A non-negative integer $\omega$.
– A non-zero polynomial $g(x) \in K[x]$.

Compute the first $\omega + 1$ coefficients $a_0(x), \ldots, a_\omega(x)$ of the canonical $\phi$-expansion of $g(x)$ and the Newton polygon $N$ of the set of points $(s, v_i(a_s\phi^s))$, for $0 \leqslant s \leqslant \omega$.

OUTPUT:
– $N = N_i^-(g)$, the principal $i$th order Newton polygon of $g$ with respect to the pair $(\mathbf{t}, \phi)$.

DEFINITION 4.1. Let $\lambda \in \mathbb{Q}_{<0}$ and let $N$ be a Newton polygon. We define the $\lambda$-*component* of $N$ to be $S_\lambda(N) := \{(x, y) \in N \mid y - \lambda x \text{ is minimal}\}$. If $N$ has a side $S$ of slope $\lambda$, then $S_\lambda(N) = S$; otherwise, $S_\lambda(N)$ is a vertex of $N$ (see Figure 4).

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

Routine ResidualPolynomial(**t**, $\lambda$, $g$)

INPUT:

– A type **t** over $A$, of order $i-1 \geqslant 0$, and a representative $\phi \in A[x]$ of **t**.
– A slope $\lambda = -h/e \in \mathbb{Q}_{<0}$, with $h$, $e$ positive coprime integers.
– A non-zero polynomial $g(x) \in K[x]$.

Let $g(x) = \sum_{0 \leqslant s} a_s(x)\phi(x)^s$ be the canonical $\phi$-adic expansion of $g(x)$. Let $S$ be the $\lambda$-component of $N_i(g)$, and let $s_0$ be the abscissa of the left end point of $S$. Let $d := d(S)$ be the degree of $S$, so that $s_0 + de$ is the right end point of $S$. The points of integer coordinates lying on $S$ have abscissa $s_j := s_0 + je$, $0 \leqslant j \leqslant d$.

Compute, for each abscissa $s_j$, the residual coefficient $c_j \in \mathbb{F}_i$ defined as

$$c_j := \begin{cases} 0, & \text{if } (s_j, v_i(a_{s_j}\phi^{s_j})) \text{ lies above } S, \\ z_{i-1}^{t_{i-1}(s_j)} R_{i-1}(a_{s_j})(z_{i-1}), & \text{if } (s_j, v_i(a_{s_j}\phi^{s_j})) \text{ lies on } S, \end{cases}$$

where $t_0(s_j) := 0$, $t_{i-1}(s_j)$ is described in [6, Definition 2.19] for $i > 1$, and $z_{i-1} \in \mathbb{F}_i$ is the image of $y$ through the isomorphism $\mathbb{F}_i \simeq \mathbb{F}_{i-1}[y]/(\psi_{i-1}(y))$.

OUTPUT:

– The residual polynomial $R_{\lambda,i}(g)(y) := c_0 + c_1 y + \ldots + c_d y^d \in \mathbb{F}_i[y]$, with respect to the triple (**t**, $\phi$, $\lambda$).

The routine Construct carries out the procedure described in [6, Proposition 2.10]. It will only be used to construct representatives of the types.

Routine Construct(**t**, $\lambda$, $\varphi$, $V$)

INPUT:

– A type **t** over $A$, of order $i-1 \geqslant 0$, and a representative $\phi \in A[x]$ of **t**.
– A slope $\lambda = -h/e \in \mathbb{Q}_{<0}$, with $h$, $e$ positive coprime integers.
– A polynomial $\varphi(y) \in \mathbb{F}_i[y]$, of degree $d$.
– A positive integer $V \geqslant ed(eV_i + h)$.

Let $(s, u)$ be minimal non-negative integers such that $V = ue + sh$. Our aim is to construct a polynomial $g(x) \in A[x]$, whose $i$th order Newton polygon with respect to (**t**, $\phi$) is contained in the segment of slope $\lambda$, degree $d$ and left end point $(s, u)$ (see Figure 5), and having moreover a prescribed residual polynomial.

Let $\varphi(y) = a_0 + a_1 y + \ldots + a_d y^d \in \mathbb{F}_i[y]$. If $i = 1$, the coefficients $a_j \in \mathbb{F}_1 = \mathbb{F}[y]/(\psi_0(y))$ can be expressed as polynomials in $z_0$ of degree less than $f_0$, with coefficients in $\mathbb{F}$. If we denote by $a_j(x)$ their arbitrary liftings to $A[x]$, we take

$$g(x) = \phi(x)^s(a_0(x)\pi^u + a_1(x)\pi^{u-h}\phi(x)^e + \ldots + a_d(x)\pi^{u-dh}\phi(x)^{de}).$$

If $i > 1$, the polynomial we are looking for is

$$g(x) = \phi(x)^s(g_0(x) + g_1(x)\phi(x)^e + \ldots + g_d(x)\phi(x)^{de}),$$

where $g_j(x) \in A[x]$ are the output of Construct(Trunc$_{i-1}$(**t**), $\lambda_{i-1}$, $\varphi_j$, $w_j$), for adequate polynomials $\varphi_j(y) \in \mathbb{F}_{i-1}[y]$ with $\deg \varphi_j < f_{i-1}$, and integers $w_j \geqslant V_i$.

OUTPUT:

– A polynomial $g(x) \in A[x]$ such that $v_{i+1}(g) = V$ and $y^{\operatorname{ord}_y(\varphi)} R_{\lambda,i}(g)(y) = \varphi(y)$.

Routine Representative(**t**)

INPUT:

– A type **t** over $A$, of order $i \geqslant 1$.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

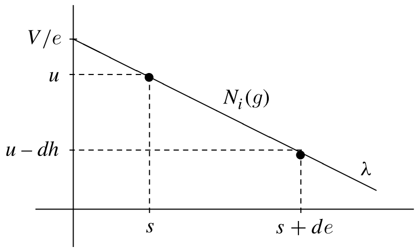


FIGURE 5. *Routine* `Construct`.

Express $\psi_i(y)=y^{f_i}+\varphi(y)\in\mathbb{F}_i[y]$, for some polynomial $\varphi(y)$ of degree less than $f_i$. Let $g(x)$ be the output of `Construct(`$\mathbf{t}$`,`$\lambda_i$`,`$c\varphi$`,`$V_{i+1}$`)`, for an adequate constant $c\in\mathbb{F}_i$ [6, Theorem 2.11].

OUTPUT:
– A representative of $\mathbf{t}$, constructed as: $\phi(x)=\phi_i(x)^{e_if_i}+g(x)$.

We now describe the Montes algorithm in pseudocode. Our design is slightly different from the original one. The output OM representations are optimal and complete types of order $r+1$, as described in (1.2), where $r$ is the Okutsu depth of the corresponding $\mathfrak{p}$-adic irreducible factor. In the original version, types of order $r+2$ were used in some occasions (cf. [4, Theorem 4.2]). The changes we introduce do not affect the complexity. 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.

## THE MONTES ALGORITHM

INPUT:
– A monic separable polynomial $F(x)\in A[x]$.
– A non-zero prime ideal $\mathfrak{p}$ of $A$.

```
1  Initialize an empty list OMReps.
2  Factorization($\mathbb{F}$,$\overline{F}$).
3  FOR each monic irreducible factor $\varphi$ of $\overline{F}$ DO
4      Take a monic lift, $\phi(x)\in A[x]$, of $\varphi$ and create a type $\mathbf{t}$ of order zero with
       $\psi_0^{\mathbf{t}}\leftarrow\varphi$,   $\omega_1^{\mathbf{t}}\leftarrow\operatorname{ord}_\varphi\overline{F}$,   $\phi_1^{\mathbf{t}}\leftarrow\phi$.
5      Initialize an empty list Leaves, and the list Types=[$\mathbf{t}$].
       WHILE #Types >0 DO
6          Extract (and delete) the last type $\mathbf{t}_0$ from Types. Let $i-1$ be its order.
7          Newton($\mathbf{t}_0$,$\omega_i^{\mathbf{t}_0}$,$F$). Let $N$ be the Newton polygon.
8          FOR every side $S$ of $N$ DO
9              Set $\lambda_i^{\mathbf{t}_0}\leftarrow$ slope of $S$. IF $\lambda_i^{\mathbf{t}_0}=-\infty$, THEN add $\mathbf{t}:=(\mathbf{t}_0;(\phi_i^{\mathbf{t}_0},-\infty,-))$ to Leaves
               and continue to the next side $S$.
10             ResidualPolynomial($\mathbf{t}_0$,$\lambda_i^{\mathbf{t}_0}$,$F$).
11             Factorization($\mathbb{F}_i$,$R_i(F)$).
12             FOR every monic irreducible factor $\psi$ of $R_i(F)$ DO
13                 Set $\mathbf{t}\leftarrow\mathbf{t}_0$, and extend $\mathbf{t}$ to an order $i$ type by setting $\psi_i^{\mathbf{t}}\leftarrow\psi$.
14                 IF $\omega_i^{\mathbf{t}_0}=1$, THEN add $\mathbf{t}$ to Leaves and go to 6.
15                 Set $\omega_{i+1}^{\mathbf{t}}\leftarrow\operatorname{ord}_\psi R_i(F)$, and call Representative($\mathbf{t}$) to fill $\phi_{i+1}^{\mathbf{t}}$.
```

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

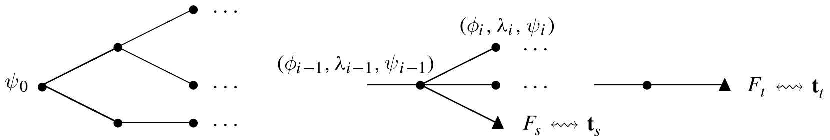

$\psi_0$
$(\phi_{i-1},\lambda_{i-1},\psi_{i-1})$
$(\phi_i,\lambda_i,\psi_i)$
$F_s \rightsquigarrow \mathbf{t}_s$
$F_t \rightsquigarrow \mathbf{t}_t$
...

FIGURE 6. *Connected tree of OM representations of the irreducible factors of $F$ whose reduction modulo $\mathfrak{p}$ is a power of $\psi_0$. The leaves are represented by ▲.*

```
16              IF $\deg \phi_{i+1}^{\mathbf{t}} = \deg \phi_i^{\mathbf{t}}$ THEN set $\phi_i^{\mathbf{t}} \leftarrow \phi_{i+1}^{\mathbf{t}}$, $\omega_i^{\mathbf{t}} \leftarrow \omega_{i+1}^{\mathbf{t}}$, and delete all data in
                the $(i+1)$th level of $\mathbf{t}$.
17              Add $\mathbf{t}$ to Types.
        END WHILE
18      Add all elements of Leaves to the list OMReps.
```

OUTPUT:

– An OM factorization of $F$ over $\mathcal{O}_\mathfrak{p}[x]$, and the corresponding family $\mathbf{t}_{F_1},\dots,\mathbf{t}_{F_g}$ of OM representations of the irreducible factors of $F$. The Okutsu factors are the $\phi$-polynomials at the last level of these types.

When the WHILE loop (corresponding to some irreducible factor $\varphi$ of $\overline{F}$) ends, the list Leaves contains a tree of $F$-complete optimal types in 1–1 correspondence with all irreducible factors of $F(x)$ over $\mathcal{O}_\mathfrak{p}[x]$, which are congruent to a power of $\varphi$ modulo $\mathfrak{p}$. The nodes of this tree (except for the root node) are labelled with a triple of fundamental invariants $(\phi_i, \lambda_i, \psi_i)$. Each leaf of the tree determines the type obtained by gathering the invariants of all nodes in the unique path joining the leaf to the root node. See Figure 6.

Step **16** takes care of the optimization. The list Types stores only strongly optimal types. If the enlarged type $\mathbf{t}$ of order $i$ of step **13** still has this property, then it is added to Types. Otherwise, we send the $(i-1)$th order type $\mathbf{t}_0$ to Types again, but equipped with a different (and better) representative; this is called a *refinement step* [**5**, § 3.2].

When the algorithm ends, the list OMReps contains a forest (disjoint union of trees) of optimal $F$-complete types. Nevertheless, the list OMReps is only a sequence of the leaves of all these trees, and the tree structure is not preserved.

*The Montes algorithm as an irreducibility test*

For any level $i$, the existence of two sides of different slope in $N_i^-(F)$, or two coprime factors of $R_i(F)$ in $\mathbb{F}_i[y]$, implies that $F(x)$ is not irreducible [**6**, Theorems 3.1,3.7]. On the other hand, if no factorization has been detected in lower levels, the Newton polygon $N_i^-(F)$ is one-sided and the corresponding residual polynomial $R_i(F)$ is irreducible in $F_i[y]$, then $F(x)$ is irreducible [**6**, Corollary 3.8].

Therefore, we can use the following version of the Montes algorithm as an irreducibility test for polynomials over $\mathcal{O}_\mathfrak{p}[x]$.

**IRREDUCIBILITY TEST**

INPUT:

– A monic separable polynomial $F(x) \in A[x]$.
– A non-zero prime ideal $\mathfrak{p}$ of $A$.

```
 1  Factorization($\mathbb{F}$,$\overline{F}$). IF there are at least two irreducible factors THEN return false.
 2  Consider a monic lift, $\phi(x) \in A[x]$, of the unique irreducible factor $\varphi$ of $\overline{F}$ and create a
    type $\mathbf{t}$ of order zero with:   $\psi_0^{\mathbf{t}} \leftarrow \varphi$,   $\omega_1^{\mathbf{t}} \leftarrow \operatorname{ord}_\varphi \overline{F}$,   $\phi_1^{\mathbf{t}} \leftarrow \phi$.
 3  Initialize the list Types = [t].
```

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

```
    WHILE #Types > 0 DO
        Extract (and delete) the last type $\mathbf{t}_0$ from Types. Let $i-1$ be its order.
        $N$=Newton($\mathbf{t}_0$,$\omega_i^{\mathbf{t}_0}$,$F$). IF $N$ has at least two sides THEN return false.
        Set $\lambda_i^{\mathbf{t}_0} \leftarrow$ slope of the unique side of $N$. IF $\lambda_i^{\mathbf{t}_0} = -\infty$, THEN return true.
        ResidualPolynomial($\mathbf{t}_0$,$\lambda_i^{\mathbf{t}_0}$,$F$).
        Factorization($\mathbb{F}_i$,$R_i(F)$). IF there are at least two irreducible factors THEN return
            false, ELSE let $\psi$ be the unique irreducible factor of $R_i(F)$.
        Set $\mathbf{t} \leftarrow \mathbf{t}_0$, and extend $\mathbf{t}$ to an order $i$ type by setting $\psi_i^{\mathbf{t}} \leftarrow \psi$.
        IF $\operatorname{ord}_\psi R_i(F) = 1$, THEN return true.
        Set $\omega_{i+1}^{\mathbf{t}} \leftarrow \operatorname{ord}_\psi R_i(F)$, and call Representative(t) to fill $\phi_{i+1}^{\mathbf{t}}$.
        IF $\deg \phi_{i+1}^{\mathbf{t}} = \deg \phi_i^{\mathbf{t}}$ THEN $\phi_i^{\mathbf{t}} \leftarrow \phi_{i+1}^{\mathbf{t}}$, $\omega_i^{\mathbf{t}} \leftarrow \omega_{i+1}^{\mathbf{t}}$, and delete the $(i+1)$th level of t.
        Add t to Types.
    END WHILE
OUTPUT:
  – true if $F(x)$ is irreducible over $\mathcal{O}_{\mathfrak{p}}[x]$ and false otherwise.
```

## 5. *Complexity analysis of the Montes algorithm*

All tasks we are interested in may be performed modulo $\mathfrak{p}^\nu$, for a sufficiently high precision $\nu$. Thus, we may assume that the elements of $A$ are finite $\pi$-adic developments. In particular, the computation of the $\mathfrak{p}$-adic valuation $v = v_{\mathfrak{p}}$ has a negligible cost.

Definition 5.1. An operation of $A$ is called $\mathfrak{p}$-*small* if it involves two elements belonging to a fixed system of representatives of $A/\mathfrak{p}$.

Working at precision $\nu$, each multiplication in $A$ costs $O(\nu^{1+\epsilon})$ $\mathfrak{p}$-small operations if we assume the fast multiplications techniques of Schönhage–Strassen [19].

Let $q := \#\mathbb{F}$. We assume that a $\mathfrak{p}$-small operation is equivalent to $O(\log(q)^{1+\epsilon})$ word operations, the cost of an operation in the residue field $\mathbb{F} = A/\mathfrak{p}$. This is the case in most of the Dedekind rings that naturally arise in practice.

### 5.1. *Complexity of the basic subroutines*

Lemma 5.2 [3, Corollary 14.30]. *Let $\mathcal{F}$ be a finite field with $q_{\mathcal{F}}$ elements, and $g(x) \in \mathcal{F}[x]$ a polynomial of degree $d$. The cost of the routine* `Factorization(`$\mathcal{F}$, $g$`)` *is $O(d^{2+\epsilon} + d^{1+\epsilon}\log(q_{\mathcal{F}}))$ operations in $\mathcal{F}$.*

The following observation is easy to prove by an inductive argument.

Lemma 5.3. *Let $m_1, \ldots, m_i$ be positive integers such that $m_1 \mid \ldots \mid m_i$ and $m_1 < \ldots < m_i$. Then, $m_1 + \ldots + m_i \leqslant 2m_i$.*

Lemma 5.4 [18, Lemma 18]. *Let $\mathbf{t}$ be a strongly optimal type of order $i-1 \geqslant 1$. Let $a(x) \in \mathcal{O}[x]$ be a polynomial with $\deg a < m_i$. The computation of the multiadic expansion of $a(x)$,*

$$a(x) = \sum_{\mathbf{j}=(j_1,\ldots,j_{i-1})} a_{\mathbf{j}}(x)\phi_1(x)^{j_1} \ldots \phi_{i-1}(x)^{j_{i-1}}, \quad \deg a_{\mathbf{j}} < m_1, \tag{5.1}$$

*where $0 \leqslant j_k < e_k f_k$, for all $1 \leqslant k < i$, has a cost of $O((m_i)^{1+\epsilon})$ operations in $A$.*

Actually, in [18] it was proved an estimation of $O(m_i^2)$ operations in $A$, assuming ordinary arithmetic. If we assume fast multiplication, the cost of the computation of the $\phi_{i-1}$-expansion of $a(x)$ may be estimated in $O((m_i)^{1+\epsilon})$ operations in $A$ [3, Theorem 9.15]. By using this estimation, the proof of [18, Lemma 18] leads to Lemma 5.4.

LEMMA 5.5. *Let* $\mathbf{t}$ *be a strongly optimal type of order* $i-1 \geqslant 0$, *with representative* $\phi(x)$. *Let* $\omega$ *be a positive integer and* $g(x) \in A[x]$ *a polynomial of degree* $d \geqslant \omega m_i$. *Then, the cost of the routine* `Newton(t,`$\omega$`,`$g$`)` *is* $O(\omega d^{1+\epsilon})$ *operations in* $A$.

*Proof.* The computation of the first $\omega+1$ coefficients of the $\phi$-development of $g(x)$ requires $\omega+1$ divisions with remainder

$$g = \phi \cdot q_1 + a_0, \quad q_1 = \phi \cdot q_2 + a_1, \quad \dots \quad , \quad q_\omega = \phi \cdot q_{\omega+1} + a_\omega.$$

The number of operations in $A$ that are necessary to carry out each one of these divisions is $O(d^{1+\epsilon})$ [3, Theorem 9.6]. Thus, we want to see that this cost dominates the whole routine.

The next step is the computation of $v_i(a_k)$, for $0 \leqslant k \leqslant \omega$. Denote by $a(x) = a_k(x)$ any of these $\omega+1$ coefficients, and consider the multiadic development (5.1) of $a(x)$. By [8, Lemma 4.2],

$$v_i(a(x)) = \min_{\mathbf{j}=(j_1,\dots,j_{i-1})} \{v_i(a_{\mathbf{j}}) + j_1 v_i(\phi_1) + \dots + j_{i-1} v_i(\phi_{i-1})\}. \tag{5.2}$$

By [6, Proposition 2.15], we may use closed formulas for the values $v_i(\phi_j)$ in terms of the Okutsu invariants, and since $\deg a_{\mathbf{j}} < m_1$, [6, Proposition 2.7] shows that

$$v_i(a_{\mathbf{j}}) = e_0 \dots e_{i-1} \min\{v_{\mathfrak{p}}(c) \mid c \text{ coefficient of } a_{\mathbf{j}}(x)\}.$$

Thus, the cost of computing $v_i(a_k)$ is dominated by the cost of the computation of the multiadic development of $a_k$. By Lemma 5.4, the total cost of this step is $(\omega+1)O((m_i)^{1+\epsilon})$ operations in $A$. This cost is clearly dominated by the cost of the first divisions with remainder.

Finally, the computation of the Newton polygon has a cost of $O(\omega^2)$ multiplications of integers. If we work at precision $\nu$, (5.2) shows that $e_0 \dots e_{i-1}\nu$ is an upper bound of $v_i(a_k)$; hence, each multiplication of integers of this size requires $O(\log(m_i\nu)^{1+\epsilon})$ word operations. Since $\omega \leqslant d/m_i$, this complexity is also dominated by that of the first divisions with remainder, which is $O(\omega(d\nu\log(q))^{1+\epsilon})$ word operations. □

LEMMA 5.6. *Let* $\mathbf{t}$ *be a strongly optimal type of order* $i-1 \geqslant 0$, *with representative* $\phi(x)$, *and take* $\lambda \in \mathbb{Q}_{<0}$, $g(x) \in A[x]$. *Let* $S$ *be the* $\lambda$*-component of* $N_i(g)$, *and let* $d = d(S)$ *be the degree of* $S$. *Then, the cost of* `ResidualPolynomial(t,`$\lambda$`,`$g$`)` *is* $O(d(f_0 \dots f_{i-1})(m_i)^{1+\epsilon}\log(q))$ $\mathfrak{p}$*-small operations.*

*Proof.* Let $e$ be the least positive denominator of $\lambda$. Let $s_0$ be the abscissa of the left end point of $S$, and take $s_j := s_0 + je$, for $0 \leqslant j \leqslant d$. We assume that in a previous call to the routine `Newton`, we computed (and stored) the coefficients $a_{s_j}$ of the $\phi$-adic expansion of $g(x)$, and their $(\phi_1, \dots, \phi_{i-1})$-multiadic expansion. Also, along this computation it is easy to store the necessary data to compute the exponents $t_{i-1}(s_j)$ at zero cost [6, Definition 2.19].

Thus, the computation of the coefficients $c_0, \dots, c_d \in \mathbb{F}_i$ of the residual polynomial $R_{\lambda,i}(g)$, requires two tasks:

(a) compute $R_{i-1}(a_{s_j})(y) \in \mathbb{F}_{i-1}[y]$, for each $0 \leqslant j \leqslant d$;

(b) compute $c_j := z_{i-1}^{t_{i-1}(s_j)} R_{i-1}(a_{s_j})(z_{i-1}) \in F_i$, for each $0 \leqslant j \leqslant d$.

Denote by $C_i(d)$ the cost of the computation of $R_{\lambda,i}(g)$, measured by the number of $\mathfrak{p}$-small operations. Since $\deg a_{s_j} < m_i = e_{i-1}f_{i-1}m_{i-1}$, the Newton polygon $N_{i-1}(a_{s_j})$ has length less than $e_{i-1}f_{i-1}$; hence, the $\lambda_{i-1}$-component of this polygon has degree less than $f_{i-1}$. Therefore, the cost of task (a) is dominated by $C_{i-1}(f_{i-1})$.

The computation of $z_{i-1}^{t_{i-1}(s_j)}$ requires $O(\log(\#\mathbb{F}_i))$ multiplications in $\mathbb{F}_i$. Since $\#\mathbb{F}_i = q^{f_0\cdots f_{i-1}}$, the cost is $O((f_0\dots f_{i-1})^{2+\epsilon}\log(q))$ $\mathfrak{p}$-small operations.

Since $\deg R_{i-1}(a_{s_j}) < f_{i-1}$, the cost of the computation of $R_{i-1}(a_{s_j})(z_{i-1})$ by Horner's rule is $O(f_{i-1})$ multiplications in $\mathbb{F}_i$; thus, it is dominated by the computation of a power of $z_{i-1}$. Altogether, we get

$$C_i(d) \leqslant (d+1)(C_{i-1}(f_{i-1}) + (f_0\dots f_{i-1})^{2+\epsilon}\log(q)).$$

From this recurrence, it is easy to derive

$$C_i(d) = (d+1)O(f_0\dots f_{i-1}\log(q)\left(f_0^{1+\epsilon} + (f_0f_1)^{1+\epsilon} + \dots + (f_0\dots f_{i-1})^{1+\epsilon}\right)).$$

Finally, we may use Lemma 5.3 to estimate

$$f_0^{1+\epsilon} + \dots + (f_0\dots f_{i-1})^{1+\epsilon} \leqslant (m_0)^{1+\epsilon} + \dots + (m_i)^{1+\epsilon} = O(m_i^{1+\epsilon}). \qquad \square$$

LEMMA 5.7. *Let $\mathbf{t}$ be a strongly optimal type of order $i-1 \geqslant 0$, with representative $\phi(x)$. Let $\lambda = -h/e$, where $h, e$ are positive coprime integers. Let $\varphi(y) \in \mathbb{F}_i[y]$ be a polynomial of degree $d$, and $V \geqslant ed(eV_i + h)$ a positive integer. Then, the cost of* `Construct(t,`$\lambda$`,`$\varphi$`,`$V$`)` *is $O((f_0\dots f_{i-1}d)^{2+\epsilon}V^{1+\epsilon})$ $\mathfrak{p}$-small operations.*

*Proof.* The output polynomial is constructed as

$$g(x) = \phi(x)^s(g_0(x) + g_1(x)\phi(x)^e + \dots + g_d(x)\phi(x)^{de}),$$

where $0 \leqslant s < e$, and the polynomials $g_j(x) \in A[x]$ may be taken as the output of an adequate call to `Construct` at level $i-1$. In particular, $\deg g_j < m_i$, for all $j$.

We must compute the polynomials $\phi(x)^s$, $\phi(x)^e$, $g_0(x), \dots, g_d(x)$, and finally compute $g(x)$ by Horner's rule. This latter task requires $d+1$ multiplications of polynomials. In each multiplication, the two factors have degree (bounded by)

$$(m_i, em_i), ((e+1)m_i, em_i), ((2e+1)m_i, em_i), \dots, (((d+1)e+1)m_i, em_i),$$

respectively. The multiplication of two polynomials of degrees $m' \leqslant m$ requires $O(m^{1+\epsilon})$ operations in $A$. Thus, if we denote $m_{i+1} := edm_i$, the number of operations in $A$ required for the final evaluation of $g(x)$ is of the order of

$$(em_i)^{1+\epsilon}(1^{1+\epsilon} + 2^{1+\epsilon} + \dots + d^{1+\epsilon}) = O((em_i)^{1+\epsilon}d^{2+\epsilon}) = O(d(m_{i+1})^{1+\epsilon}).$$

This estimation clearly dominates the cost of the computation of $\phi(x)^s$ and $\phi(x)^e$. Thus, we analyze only the cost of the computation of $g_0(x), \dots, g_d(x)$.

Denote by $C_i(d)$ the total cost of `Construct`, measured by the number of operations in $A$. We have seen that $C_i(d) = d(C_{i-1}(f_{i-1}) + O((m_{i+1})^{1+\epsilon}))$. By using Lemma 5.3, this recurrence leads to

$$\begin{aligned} C_i(d) &= O(d\,(m_{i+1})^{1+\epsilon} + d\,f_{i-1}(m_i)^{1+\epsilon} + \dots + d\,f_{i-1}\dots f_0(m_0)^{1+\epsilon}) \\ &= O(d\,f_{i-1}\dots f_0((m_{i+1})^{1+\epsilon} + (m_i)^{1+\epsilon} + \dots + (m_0)^{1+\epsilon})) \\ &= O(d\,f_{i-1}\dots f_0\,(m_{i+1})^{1+\epsilon}). \end{aligned} \tag{5.3}$$

Finally, we may work with precision $\nu := \lfloor V/(e_0\dots e_{i-1}e)\rfloor + 1$, without changing the desired properties of $g(x)$:

$$v_{i+1}(g) = V, \quad y^{\operatorname{ord}_y \varphi} R_{\lambda,i}(g)(y) = \varphi(y),$$

where $v_{i+1}$ is the valuation determined by $\mathbf{t}$, $\phi$ and $\lambda$. In fact, suppose $G(x) = g(x) + h(x)$, for a polynomial $h(x) \in A[x]$, all of whose coefficients $c$ satisfy $v_{\mathfrak{p}}(c) > V/(e_0\dots e_{i-1}e)$. Then, $v_{i+1}(c) = (e_0\dots e_{i-1}e)v_{\mathfrak{p}}(c) > V$, by Lemma 1.5, so that $v_{i+1}(h) > v_{i+1}(g)$, and $v_{i+1}(G) = v_{i+1}(g)$. Also, we get $R_{\lambda,i}(G)(y) = R_{\lambda,i}(g)(y)$ by [6, Proposition 2.8].

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

Therefore, the total cost of `Construct`, measured in number of $\mathfrak{p}$-small operations, is obtained by multiplying the estimation of (5.3) by $\nu^{1+\epsilon}$. □

Corollary 5.8. *Let $\mathbf{t}' = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1}); (\phi, \lambda, \psi))$ be an optimal type of order $i \geqslant 1$, where $\lambda = -h/e$ for some positive coprime integers $h, e$, and $y \neq \psi(y) \in \mathbb{F}_i[y]$ is a monic irreducible polynomial of degree $f$. Let $V := ef(eV_i + h)$. The cost of the computation of a representative $\phi'$ of $\mathbf{t}'$ is $O((f_0 \ldots f_{i-1} f)^{2+\epsilon} V^{1+\epsilon})$ $\mathfrak{p}$-small operations.*

*Proof.* The polynomial $\phi'(x)$ is constructed as $\phi(x)^{ef} + g(x)$, where $g(x)$ is the output of the routine `Construct(t,`$\lambda$`,`$\psi(y) - y^f$`,`$V$`)`. The computation of $\phi^{ef}$ by repeated squarings costs $O((efm_i)^{1+\epsilon})$ operations in $A$; this cost is dominated by the estimation (5.3) of the cost of the computation of $g(x)$. Thus, the corollary is an immediate consequence of Lemma 5.7. □

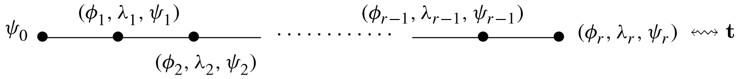
### 5.2. *Complexity of the polynomial irreducibility test*

The aim of this section is to prove a new estimation for the complexity of the polynomial irreducibility test based on the Montes algorithm. In comparison with previous estimations [**2, 18**], the total degree in $n$ and $\delta$ is reduced from $4 + \epsilon$ to $2 + \epsilon$.

Theorem 5.9. *The cost of the irreducibility test over $\mathcal{O}_{\mathfrak{p}}[x]$, applied to a monic separable polynomial $F \in A[x]$ of degree $n$, is $O(n^{2+\epsilon} + n^{1+\epsilon}(1 + \delta)\log(q) + \delta^{2+\epsilon})$ $\mathfrak{p}$-small operations, where $\delta := v_{\mathfrak{p}}(\mathrm{Disc}(F))$.*

Corollary 5.10. *If we assume $\mathfrak{p}$ small (that is, $\log(q) = O(1)$), we obtain an estimation of $O(n^{2+\epsilon} + \delta^{2+\epsilon})$ word operations.*

Before proving this theorem, we discuss some features of the flow of the algorithm. The irreducibility test provides as a by-product an optimal type $\mathbf{t}$ of order $r$, represented by a tree with unibranch nodes and a unique leaf.


$\psi_0$
$(\phi_1, \lambda_1, \psi_1)$
$(\phi_2, \lambda_2, \psi_2)$
$(\phi_{r-1}, \lambda_{r-1}, \psi_{r-1})$
$(\phi_r, \lambda_r, \psi_r) \rightsquigarrow \mathbf{t}$

If $\mathrm{ord}_{\mathbf{t}}(F) = 1$, then $F$ was recognized to be irreducible. Otherwise, after several refinement steps, a representative $\phi_{r+1}$ of $\mathbf{t}$ was eventually found, such that $N_{r+1}(F)$ had more than one side, or $R_{r+1}(F)$ had more than one irreducible factor; then, $F$ was recognized to be reducible. In this latter case, all irreducible factors of $F$ are of type $\mathbf{t}$ (Definition 2.5), and they have degree a multiple of $m_{r+1}$, by Lemma 2.6. In particular, $n = fm_{r+1}$, for some integer $f \geqslant 2$.

We may choose a monic irreducible polynomial $\psi \in \mathbb{F}_{r+1}[y]$ of degree $f$ and use `Representative` to construct a representative $\phi \in A[x]$ of the type of order $r + 1$:

$$\mathbf{t}' = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (\phi_{r+1}, -1, \psi)).$$

The polynomial $\phi$ is irreducible over $\mathcal{O}_{\mathfrak{p}}$ and it has degree $m_{r+2} = fm_{r+1} = n$. The irreducibility test applied to $\phi$ performs the same steps at all levels $i \leqslant r$, the same refinement steps at level $r + 1$ to find $\phi_{r+1}$, and it will compute $N_{r+1}(\phi)$ and $R_{r+1}(\phi)$, to deduce the irreducibility of $\phi$ from the property $R_{r+1}(\phi) \sim \psi$. We shall see below that the cost of reaching $\phi_{r+1}$ depends only on $n$ and $\phi_{r+1}$. By Lemmas 5.5, 5.6, the cost of the computation of $N_{r+1}(\phi)$, $R_{r+1}(\phi)$ is not lower than the cost of the computation of $N_{r+1}(F)$, $R_{r+1}(F)$, respectively. Hence we have the following remark.

Remark 3. For the estimation of the complexity of the irreducibility test, we may assume that the input polynomial is irreducible.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

For the estimation of the complexity we need to estimate the cost of advancing from the $(i-1)$th node of the tree to the $i$th node. This step may require several iterations of the WHILE loop, because of the refinement steps at the $i$th level. Thus, the crucial questions are the evaluation of the cost of each iteration at the $i$th level and to find an upper bound for the number of these iterations.

LEMMA 5.11. *The width of $F$ at the $i$th level, $\lceil|\lambda_i|\rceil$, is an upper bound for the number of iterations of the WHILE loop at the $i$th level, that are necessary to reach the right values of $(\phi_i, \lambda_i, \psi_i)$.*

*Proof.* The first WHILE loop at the $i$th level picks the type of order $i-1 \geqslant 0$,

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1})),$$

and a representative $\phi$ of degree $m_i$ (a first candidate to be the polynomial $\phi_i$), from the list `Types`. Then, it computes the slope $\lambda = -h/e$, with $h, e$ positive coprime integers, of the one-sided Newton polygon $N_i(F)$ with respect to $(\mathbf{t}, \phi)$, and the unique irreducible factor $\psi \in \mathbb{F}_i[y]$ of the residual polynomial $R_{\lambda,i}(F)$. Finally, it constructs a representative $\phi'$ of the type

$$\mathbf{t}' = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1}); (\phi, \lambda, \psi)).$$

Let $f = \deg \psi$, $V = ef(eV_i + h)$. By [6, Theorems 2.11, 3.1], $\deg \phi' = efm_i$, and

$$v(\phi(\theta)) = (V_i + |\lambda|)/(e_0 \dots e_{i-1}) < v(\phi'(\theta)) = (V + |\lambda'|)/(e_0 \dots e_{i-1}e),$$

where $\theta$ is a root of $F$ in $\overline{K}_{\mathfrak{p}}$, $v$ is the canonical extension of $v_{\mathfrak{p}}$ to $\overline{K}_{\mathfrak{p}}$, and $\lambda'$ is the slope of the Newton polygon $N_{i+1}(F)$, computed with respect to $(\mathbf{t}', \phi')$.

The loop is a refinement step if and only if $\deg \phi' = m_i$, or equivalently, $e = f = 1$. In this case, $\phi'$ is also a representative of $\mathbf{t}$, and we proceed to a new iteration of the WHILE loop at the $i$th level, with the pair $(\mathbf{t}, \phi')$ as starting data. Otherwise, [5, Theorem 3.1] shows that $v(\phi(\theta))$ is maximal among all other representatives of $\mathbf{t}$; thus, it may be taken as an Okutsu polynomial of the $i$th level. We take $\phi_i := \phi$, $\lambda_i := \lambda$, $\psi_i := \psi$ and we proceed to a new iteration of the WHILE loop at the $(i+1)$th level with the pair $(\mathbf{t}', \phi')$ as starting data.

Therefore, the number of iterations of the WHILE loop at the $i$th level is bounded from above by the number of values of $v(\phi(\theta))$, where $\phi$ runs on all possible representatives of $\mathbf{t}$. This number of values is $\lceil|\lambda_i|\rceil$ by Proposition 1.8. □

*Proof of Theorem 5.9.* By Remark 3 we may assume that the input polynomial $F$ is irreducible over $\mathcal{O}_{\mathfrak{p}}[x]$. Let $r$ be the Okutsu depth of $F$ and $\mathbf{t}_{F,r} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_r, \lambda_r, \psi_r))$ the strongly optimal type of order $r$ computed along the flow of the algorithm.

We shall frequently use an estimation that is an immediate consequence of formula (2.1) and the inequality $\delta_0(F) \leqslant 2\delta/n$ of Lemma 2.2:

$$\sum_{1 \leqslant i \leqslant r} \frac{|\lambda_i|}{e_0 \dots e_{i-1}} \frac{n^2}{m_i} = O(\delta). \tag{5.4}$$

The initial steps compute the pair $(\mathbf{t}, \phi)$, where $\mathbf{t} = (\psi_0)$ is the type of order zero determined by the unique irreducible factor of $F$ modulo $\mathfrak{p}$ and $\phi$ is a monic lift to $A[x]$ of $\psi_0$. The cost of these operations is dominated by the factorization of $F$ modulo $\mathfrak{p}$, which costs $O(n^{2+\epsilon} + n^{1+\epsilon} \log(q))$ $\mathfrak{p}$-small operations.

Each iteration of the WHILE loop calls each subroutine `Newton`, `ResidualPolynomial`, `Factorization` and `Representative` only once. Let `R` be one of these subroutines; by Lemma 5.11, the total cost of the calls to `R` of all iterations of the WHILE loop is not greater than

$$\sum_{1 \leqslant i \leqslant r} |\lambda_i| \, C_{\mathtt{R},i}, \tag{5.5}$$

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

where $C_{\mathtt{R},i}$ is an upper bound of the cost of any call to $\mathtt{R}$ along the different iterations of the WHILE loop at the $i$th level. We proceed to estimate $C_{\mathtt{R},i}$ and (5.5), for each subroutine. We keep the notation introduced in the proof of Lemma 5.11 for the data $\mathbf{t}$, $\phi$, $\lambda$, $\psi$, $e$, $f$, $h$, $\phi'$, $V$, $\mathbf{t}'$, used in any of these iterations.

$\mathtt{R}=$`Newton`. By Lemma 5.5, the cost of one call to `Newton` depends only on $n=\deg F$ and $\omega:=\ell(N_i(F))=n/\deg\phi$. Since $\deg\phi=m_i=e_{i-1}f_{i-1}m_{i-1}$ does not depend on the choice of $\phi$, the cost is constant for all the iterations at the $i$th level. By Lemma 5.5, this cost is $O((n/m_i)n^{1+\epsilon})$ operations in $A$.

By Theorem 2.3, we may work at any precision $\nu>2\delta/n$, so that we may take

$$C_{\mathtt{R},i}=O((n/m_i)n^{1+\epsilon}(\delta/n)^{1+\epsilon})=O((n/m_i)\delta^{1+\epsilon})$$

$\mathfrak{p}$-small operations. By (5.4), we obtain

$$\sum_{1\leqslant i\leqslant r}|\lambda_i|\,C_{\mathtt{R},i}=\delta^{1+\epsilon}\sum_{1\leqslant i\leqslant r}|\lambda_i|\,\frac{n}{m_i}\leqslant\delta^{1+\epsilon}\sum_{1\leqslant i\leqslant r}\frac{|\lambda_i|}{e_0\dots e_{i-1}}\,\frac{n^2}{m_i}=O(\delta^{2+\epsilon}).$$

$\mathtt{R}=$`ResidualPolynomial`. By Lemma 5.6, the cost of one call to `ResidualPolynomial` depends only on $f_0,\dots,f_{i-1}$ and the degree of the side $d(N_i(F))=\omega/e=n/(m_ie)$. Thus, the cost is constant for all refinement steps $(e=1)$ and eventually lower in the last iteration of WHILE $(ef>1)$. By Lemma 5.6, we may take

$$C_{\mathtt{R},i}=O((n/m_i)(f_0\dots f_{i-1})m_i^{1+\epsilon}\log(q))=O((n/e_0\dots e_{i-1})n^{1+\epsilon}\log(q))\tag{5.6}$$

$\mathfrak{p}$-small operations. By (5.4), we obtain

$$\sum_{1\leqslant i\leqslant r}|\lambda_i|\,C_{\mathtt{R},i}\leqslant n^{1+\epsilon}\log(q)\sum_{1\leqslant i\leqslant r}\frac{|\lambda_i|\,n}{e_0\dots e_{i-1}}=O(n^{1+\epsilon}\log(q)\delta).$$

$\mathtt{R}=$`Factorization`. The cost of one call to `Factorization` depends only on $\deg R_{\lambda,i}(F)=d(N_i(F))=\omega/e=n/(m_ie)$, and it is $O((n/m_i)^{2+\epsilon}+(n/m_i)^{1+\epsilon}(f_0\dots f_{i-1})\log(q))$ operations in $\mathbb{F}_i$, by Lemma 5.2. We may estimate

$$\begin{aligned}C_{\mathtt{R},i}&=O((n/m_i)^{2+\epsilon}(f_0\dots f_{i-1})^{1+\epsilon}+(n/m_i)^{1+\epsilon}(f_0\dots f_{i-1})^{2+\epsilon}\log(q))\\&=O(n^{2+\epsilon}/(m_i(e_0\dots e_{i-1})^{1+\epsilon})+(n/e_0\dots e_{i-1})^{1+\epsilon}f_0\dots f_{i-1}\log(q))\end{aligned}$$

$\mathfrak{p}$-small operations. Both summands of this expression are dominated by the estimation of (5.6). Thus, the total cost of `Factorization` is dominated by the total cost of `ResidualPolynomial`.

$\mathtt{R}=$`Representative`. The cost of one call to `Representative` is $O((f_0\dots f_{i-1}f)^{2+\epsilon}V^{1+\epsilon})$ $\mathfrak{p}$-small operations, by Corollary 5.8. Along the refinement steps, we have $f=1$, $V=V_i+h$; since the value of $h=|\lambda|$ grows at each iteration, the cost is dominated by the cost of the last iteration, where $f=f_i$, $V=V_{i+1}=e_if_i(e_iV_i+h_i)$. Thus, we may take

$$C_{\mathtt{R},i}=O((f_0\dots f_{i-1}f_i)^{2+\epsilon}(V_{i+1})^{1+\epsilon})$$

$\mathfrak{p}$-small operations. We have, $V_{i+1}/(e_0\dots e_i)\leqslant V_{r+1}/(e_0\dots e_r)\leqslant 2\delta/n$, by the recurrent formulas for $V_i$ (Section 1), and Lemma 2.2. Hence, $f_0\dots f_iV_{i+1}\leqslant 2\delta$. By (5.4), we obtain

$$\begin{aligned}\sum_{1\leqslant i\leqslant r}|\lambda_i|\,C_{\mathtt{R},i}&\leqslant(2\delta)^{1+\epsilon}\sum_{1\leqslant i\leqslant r}|\lambda_i|\,f_0\dots f_i=(2\delta)^{1+\epsilon}\sum_{1\leqslant i\leqslant r}\frac{|\lambda_i|}{e_0\dots e_{i-1}}\,m_if_i\\&\leqslant(2\delta)^{1+\epsilon}\sum_{1\leqslant i\leqslant r}\frac{|\lambda_i|}{e_0\dots e_{i-1}}\,\frac{n^2}{m_i}=O(\delta^{2+\epsilon}).\end{aligned}$$ □

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

### 5.3. *Complexity of the general factorization algorithm*

Let $F_1, \dots, F_g \in \mathcal{O}_\mathfrak{p}[x]$ be the monic irreducible factors of the input polynomial $F \in A[x]$. Denote $n_s = \deg F_s$, $\delta_s = \delta(F_s)$, and let $r_s$ be the Okutsu depth of $F_s$, for all $1 \leqslant s \leqslant g$.

The output of the Montes algorithm is a forest $\mathcal{T} = \mathcal{T}_1 \cup \dots \cup \mathcal{T}_k$, a disjoint union of $k$ connected trees, one for each irreducible factor of $\overline{F}$. Let $\mathcal{R} \subset \mathcal{T}$ be the set of the $k$ root nodes of $\mathcal{T}$, each one labelled by an irreducible factor $\psi_0$ of $\overline{F}$ (see Figure 6). If we agree that the root nodes have level zero, the *level* of a node $\mathbf{n} \in \mathcal{T} \setminus \mathcal{R}$ is, by definition, the level of its unique previous node plus one. These nodes are labelled by a triple of fundamental invariants, $\mathbf{n} = (\phi_\mathbf{n}, \lambda_\mathbf{n}, \psi_\mathbf{n})$.

*Notation.* For each $\mathbf{n} \in \mathcal{T}$ of level $i$, we denote:

$\mathbf{t_n}$ := the type of order $i$ obtained by gathering the fundamental invariants of all nodes in the unique path joining $\mathbf{n}$ with its root node;

$F_\mathbf{n}$ := the product of all irreducible factors of $F$ which are divisible by $\mathbf{t_n}$;

$\mathcal{B}_\mathbf{n}$ := the set of nodes of level $i+1$ whose previous node is $\mathbf{n}$. We say that the nodes of $\mathcal{B}_\mathbf{n}$ are *branches* of $\mathbf{n}$.

Let $\mathcal{L} \subset \mathcal{T}$ be the set of all leaves of $\mathcal{T}$. These leaves are in 1–1 correspondence with the $g$ irreducible factors of $F$ over $\mathcal{O}_\mathfrak{p}$. Suppose that $\mathbf{n}$ is the leaf attached to $F_s$. The level of $\mathbf{n}$ is $r_s + 1$, and we denote by $\mathbf{t}_s := \mathbf{t_n}$ the corresponding type of order $r_s + 1$. By construction, $\mathbf{t}_s$ is an OM representation of $F_s$, and the family of the $\phi_{r_s+1}$ polynomials of $\mathbf{t}_1, \dots, \mathbf{t}_g$ is an OM factorization of $F$ over $\mathcal{O}_\mathfrak{p}$. In particular, $F_\mathbf{n} = F_s$, by Corollary 3.10.

The root nodes are determined by the factorization of $\overline{F}$ over $\mathbb{F}[y]$. Hence, their computation has a cost of $O(n^{2+\epsilon} + n^{1+\epsilon}\log(q))$ $\mathfrak{p}$-small operations. Let

$$\texttt{Rout:=}\{\texttt{Newton}, \texttt{ResidualPolynomial}, \texttt{Factorization}, \texttt{Representative}\},$$

be the family of the four fundamental subroutines of the Montes algorithm. For each routine $\texttt{R} \in \texttt{Rout}$ and each node $\mathbf{m} \in \mathcal{T} \setminus \mathcal{L}$, let $B_{\texttt{R},\mathbf{m}}$ be an upper bound of the cost, measured by the number of $\mathfrak{p}$-small operations, of any call to $\texttt{R}$ along the different iterations of the WHILE loop that are necessary to compute all nodes of $\mathcal{B}_\mathbf{m}$. Then, the total cost of the Montes algorithm is

$$O\biggl(n^{2+\epsilon} + n^{1+\epsilon}\log(q) + \sum_{\texttt{R}\in\texttt{Rout}}\ \sum_{\mathbf{m}\in\mathcal{T}\setminus\mathcal{L}} B_{\texttt{R},\mathbf{m}}\biggr). \tag{5.7}$$

Our first task is to find estimations for these upper bounds $B_{\texttt{R},\mathbf{m}}$.

Lemma 5.12. *For all $\mathbf{m} \in \mathcal{T} \setminus \mathcal{L}$, we have $F_\mathbf{m} = \prod_{\mathbf{n}\in\mathcal{B}_\mathbf{m}} F_\mathbf{n}$.*

*Proof.* For an arbitrary node $\mathbf{n} \in \mathcal{T}$, let $\mathcal{L}_\mathbf{n} \subset \mathcal{L}$ be the set of leaves that are connected to $\mathbf{n}$. By definition, $F_\mathbf{n}$ is the product of all irreducible factors of $F$ attached to the leaves in $\mathcal{L}_\mathbf{n}$. On the other hand, $\mathcal{L}_\mathbf{m}$ is clearly the disjoint union of all $\mathcal{L}_\mathbf{n}$, for $\mathbf{n} \in \mathcal{B}_\mathbf{m}$. □

Lemma 5.13. *Let $\mathbf{m} \in \mathcal{T} \setminus \mathcal{L}$ be a node of level $i - 1 \geqslant 0$. Let $e_j, f_j, h_j$, $0 \leqslant j < i$, be the Okutsu invariants of the type $\mathbf{t_m}$, and take $m_i := e_{i-1}f_{i-1}m_{i-1}$. Denote*

$$B := \sum_{\mathbf{n}\in\mathcal{B}_\mathbf{m}\setminus\mathcal{L}} |\lambda_\mathbf{n}| \frac{\deg F_\mathbf{n}}{m_i} + \sum_{\mathbf{n}\in\mathcal{B}_\mathbf{m}\cap\mathcal{L}} \frac{v_\mathfrak{p}(\operatorname{Res}(F_\mathbf{n}, F_t))}{f_0 \cdots f_{i-1}},$$

*where, for each $\mathbf{n} \in \mathcal{B}_\mathbf{m} \cap \mathcal{L}$, $F_t \neq F_\mathbf{n}$ is an adequate choice of an irreducible factor of $F$ such that $\mathbf{t_m} \mid F_t$. Then, for $\texttt{R} = \texttt{Newton}$ or $\texttt{Representative}$, we have $B_{\texttt{R},\mathbf{m}} = O(n^{1+\epsilon}\delta^{1+\epsilon}B)$, whereas for $\texttt{R} = \texttt{ResidualPolynomial}$ or $\texttt{Factorization}$, we have $B_{\texttt{R},\mathbf{m}} = O(n^{1+\epsilon}f_0 \dots f_{i-1}\log(q)B)$.*

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

*Proof.* Denote for simplicity $\mathbf{t}=\mathbf{t}_{\mathbf{m}}$, $\mathcal{B}=\mathcal{B}_{\mathbf{m}}$. Since $\mathbf{m}$ is not a leaf, the type $\mathbf{t}$ is strongly optimal. Along the construction of the node $\mathbf{m}$, the algorithm computes an initial representative $\phi$ of $\mathbf{t}$ (of degree $m_i$) and the positive integer $\omega:=\operatorname{ord}_{\mathbf{t}}(F)$. By the definition of $F_{\mathbf{m}}$, and Lemmas 2.6, 5.12,

$$\omega=\operatorname{ord}_{\mathbf{t}}(F)=\operatorname{ord}_{\mathbf{t}}(F_{\mathbf{m}})=\deg F_{\mathbf{m}}/m_i=\left(\sum_{\mathbf{n}\in\mathcal{B}}\deg F_{\mathbf{n}}\right)/m_i. \tag{5.8}$$

Suppose `R = Newton`. In the first iteration of the WHILE loop concerning $\mathbf{m}$, the routine `Newton(t,`$\omega$`,`$F$`)` is called to compute the polygon $N_{i,\omega}(F)$ determined by the first $\omega+1$ coefficients of the $\phi$-expansion of $F$. By Lemma 5.5, this has a cost of $O(\omega n^{1+\epsilon})$ operations in $A$. By Theorem 3.13, we may work with precision $\delta+1$, so that the computation requires $O(\omega n^{1+\epsilon}\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations. By (5.8), this cost may be distributed into a cost of $O((\deg F_{\mathbf{n}}/m_i)n^{1+\epsilon}\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations for each node $\mathbf{n}\in\mathcal{B}$.

The WHILE loop yields a factorization, $F_{\mathbf{m}}=\prod_{\lambda,\psi}F_{\lambda,\psi}$, where $\lambda$ runs on all slopes of $N_{i,\omega}(F)$ and, for each $\lambda$, the polynomial $\psi$ runs on the monic irreducible factors of $R_{\lambda,i}(F)$. For each ‘branch’ $(\lambda,\psi)$, a representative $\phi_{\lambda,\psi}$ of the type $\mathbf{t}_{\lambda,\psi}:=(\mathbf{t};(\phi,\lambda,\psi))$ is computed, and the positive integer $\omega_{\lambda,\psi}:=\operatorname{ord}_{\mathbf{t}_{\lambda,\psi}}(F)$ is determined. The polynomial $F_{\lambda,\psi}$ is, by definition, the product of all irreducible factors of $F$ that are divisible by $\mathbf{t}_{\lambda,\psi}$. The factorization of $F_{\mathbf{m}}$ determines in turn a partition, $\mathcal{B}=\coprod_{\lambda,\psi}\mathcal{B}_{\lambda,\psi}$, where $\mathcal{B}_{\lambda,\psi}$ contains all nodes $\mathbf{n}\in\mathcal{B}$ such that $\mathbf{t}_{\lambda,\psi}\mid F_{\mathbf{n}}$. If $e_\lambda$ is the least positive denominator of $\lambda$ and $f_\psi=\deg\psi$, we have

$$\deg\phi_{\lambda,\psi}=e_\lambda f_\psi m_i,\quad \omega=\sum_{\lambda,\psi}e_\lambda f_\psi\omega_{\lambda,\psi}. \tag{5.9}$$

In order to analyze these branches, there are four different situations to consider.

**(a) When** $\lambda=-\infty$**.** Then, $\mathcal{B}_{\lambda,\psi}=\{\mathbf{n}\}$ has a single node, which is a leaf of $\mathcal{T}$. The irreducible factor attached to this leaf is $F_s=\phi$, and we take $\mathbf{n}=(\phi,-\infty,-)$.

**(b) When** $\omega=1$**.** There is only one branch $(\lambda,\psi)$, with $e_\lambda=f_\psi=\omega_{\lambda,\psi}=1$. The set $\mathcal{B}_{\lambda,\psi}=\{\mathbf{n}\}$ has a single node, which is a leaf of $\mathcal{T}$, and we take $\mathbf{n}=(\phi,\lambda,\psi)$.

**(c) When** $\mathbf{e}_\lambda\mathbf{f}_\psi>1$**.** Then, $\mathbf{n}:=(\phi,\lambda,\psi)\in\mathcal{B}$ is already a node of level $i$ of $\mathcal{T}\setminus\mathcal{L}$. In other words, $\mathcal{B}_{\lambda,\psi}=\{\mathbf{n}\}$ already singles out a node of $\mathcal{B}$, which is not a leaf of $\mathcal{T}$.

**(d) When** $\omega>1$**,** $\mathbf{e}_\lambda\mathbf{f}_\psi=1$**.** We fall in a refinement step; the slope $\lambda$ is a negative integer ($e_\lambda=1$), and $\psi$ has degree $f_\psi=1$. We consider $\phi_{\lambda,\psi}$ as a new representative of $\mathbf{t}$, and $\omega_{\lambda,\psi}$ as the new future length of the Newton polygons of $i$th order to analyze.

In case (d), we take $(\mathbf{t},\phi_{\lambda,\psi},\omega_{\lambda,\psi})$ as the input data of a future call of the WHILE loop, yielding a further factorization of $F_{\lambda,\psi}$ and a further partition of $\mathcal{B}_{\lambda,\psi}$. This loop will follow the same pattern as above, with a minor difference. In the first iteration, $N_{i,\omega}(F)=N_i^-(F)$ is the principal Newton polygon of $F$ with respect to $(\mathbf{t},\phi)$; however, after a refinement step, $N_{i,\omega_{\lambda,\psi}}(F)$ is only the part of $N_i^-(F)$ (now with respect to $(\mathbf{t},\phi_{\lambda,\psi})$) formed by the sides of slope greater than $|\lambda|$ in absolute size [5, § 3]. In any case, the cost of the new call to `Newton` is again $O(\omega_{\lambda,\psi}n^{1+\epsilon}\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations, and it may be distributed again into a cost of $O((\deg F_{\mathbf{n}}/m_i)n^{1+\epsilon}\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations for each node $\mathbf{n}\in\mathcal{B}_{\lambda,\psi}$.

Therefore, the total cost of the computation of $\mathcal{B}$ is obtained by counting a cost of $O((\deg F_{\mathbf{n}}/m_i)n^{1+\epsilon}\delta^{1+\epsilon})$, for each $\mathbf{n}\in\mathcal{B}$ and for each iteration of the WHILE loop where this node was concerned (that is $\mathbf{n}\in\mathcal{B}_{\lambda,\psi}$). Let us find upper bounds for these numbers of iterations. The discussion is different for $\mathbf{n}$ being a leaf or not. Note that if $\mathbf{n}$ is a leaf then $\deg F_{\mathbf{n}}/m_i=1$.

Suppose that $\mathbf{n}=(\phi_{\mathbf{n}},\lambda_{\mathbf{n}},\psi_{\mathbf{n}})\in\mathcal{B}$ is not a leaf. Let $F_s$ be one of the irreducible factors of $F_{\mathbf{n}}$, and $\theta_s\in k^{\mathrm{sep}}$ a root of $F_s$. Along the different iterations of the WHILE loop where this node

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

is concerned, we consider different representatives $\phi$ of the type $\mathbf{t}$ such that $v(\phi(\theta_s))$ increases strictly (cf. the proof of Lemma 5.11). By Proposition 1.8, the total number of iterations before we reach the node $\mathbf{n}$ is bounded from above by $\lceil|\lambda_{\mathbf{n}}|\rceil$.

Suppose now $\mathbf{n}\in\mathcal{B}\cap\mathcal{L}$, and let $F_s$ be the irreducible factor attached to this leaf. We may assume that there are at least two iterations of the WHILE loop concerning $\mathbf{n}$. Let $(\mathbf{t},\phi,\omega)$ be the input data of the penultimate of these iterations. Since we do not fall in case (b), we necessarily have $\omega>1$. Let $(\lambda,\psi)$ be the branch such that $\mathbf{n}\in\mathcal{B}_{\lambda,\psi}$. If $\#\mathcal{B}_{\lambda,\psi}>1$, we take $F_t$ to be an irreducible factor of $F_{\lambda,\psi}$ such that $F_t\neq F_s$. If $\mathcal{B}_{\lambda,\psi}=\{\mathbf{n}\}$, then $F_{\lambda,\psi}=F_{\mathbf{n}}$, and the formula (5.8) shows that $\omega_{\lambda,\psi}=\deg F_{\lambda,\psi}/m_i=1$. By (5.9), there is some branch $(\lambda',\psi')\neq(\lambda,\psi)$, because $\omega>1$ and $e_\lambda=f_\psi=1$; in this case we take $F_t$ to be one of the irreducible factors of $F_{\lambda',\psi'}$. Lemma 2.7 shows in any case that

$$v(\mathrm{Res}(F_s,F_t))/(f_0\dots f_{i-1})\geqslant\ell(F_s)\ell(F_t)(V_i+\min\{|\lambda|,|\lambda'|\})\geqslant\min\{|\lambda|,|\lambda'|\},$$

where $\ell(F_s),\ell(F_t)$ are the lengths of $N_i(F_s),N_i(F_t)$, respectively. In all previous iterations of WHILE, the branch concerning $\mathbf{n}$ was a refinement step, and the absolute size of the corresponding slope was an integer that grows strictly in each iteration; thus, the total number of iterations concerning $\mathbf{n}$ is bounded from above by $1+|\mu|$, for every slope $\mu$ of the Newton polygon of the penultimate iteration.

Therefore, all estimations of the lemma about the contributions of the different nodes $\mathbf{n}\in\mathcal{B}$ to the total cost of `Newton` are correct. This ends the proof of the lemma in the case `R = Newton`.

Assume now `R` $\neq$ `Newton`. In every iteration of the WHILE loop, with input data $(\mathbf{t},\phi,\omega)$, we compute the residual polynomials $R_{\lambda,i}(F)$, for $\lambda$ running on all slopes of $N_{i,\omega}(F)$. Then we factorize these polynomials over $\mathbb{F}_i$, and for each monic irreducible factor $\psi$ of $R_{\lambda,i}(F)$, we compute a representative of the type $\mathbf{t}_{\lambda,\psi}$.

Let $\ell(\lambda)$, $d(\lambda)$ be the length and degree of the side of slope $\lambda$. Lemma 5.6 shows that the cost of the computation of $R_{\lambda,i}(F)$ is $O(d(\lambda)(f_0\dots f_{i-1})(m_i)^{1+\epsilon}\log(q))$ $\mathfrak{p}$-small operations. Since $\omega$ is the length of $N_{i,\omega}(F)$, we have

$$\omega=\sum_\lambda\ell(\lambda)=\sum_\lambda e_\lambda d(\lambda)\geqslant\sum_\lambda d(\lambda).$$

Therefore, the total cost of all calls to `ResidualPolynomial` during this iteration is bounded from above by $O(\omega(f_0\dots f_{i-1})(m_i)^{1+\epsilon}\log(q))$. As in the case `R = Newton`, this cost is the product of a constant part, $(f_0\dots f_{i-1})(m_i)^{1+\epsilon}\log(q)$, times a variable part, $\omega$. As before, we can distribute $\omega$ into a cost of $\deg F_{\mathbf{n}}/m_i$, for every node of $\mathcal{B}$, and the same arguments lead to an analogous estimation for $B_{\mathtt{R},\mathtt{m}}$, for `R = ResidualPolynomial`, just by changing the constant part.

Assume now `R = Factorization`. By Lemma 5.17, the cost of the factorization of $R_{\lambda,i}(F)$ over $\mathbb{F}_i$ is $O(d(\lambda)^{2+\epsilon}(f_0\dots f_{i-1})^{1+\epsilon}+d(\lambda)^{1+\epsilon}(f_0\dots f_{i-1})^{2+\epsilon}\log(q))$ $\mathfrak{p}$-small operations. Since $d(\lambda)\leqslant\omega=\deg F_{\mathtt{m}}/m_i\leqslant n/m_i\leqslant n/(f_0\dots f_{i-1})$, this cost is $O(d(\lambda)n^{1+\epsilon}f_0\dots f_{i-1}\log(q))$. Thus, the cost of all calls to `Factorization` during this iteration is $O(\omega n^{1+\epsilon}f_0\dots f_{i-1}\log(q))$. We obtain the estimation of $B_{\mathtt{R},\mathbf{m}}$ by the same arguments as in the previous cases.

Finally, let `R = Representative`. Let $V_{\lambda,\psi}:=(e_\lambda)^2f_\psi(V_i+|\lambda|)$. By Lemma 5.8, the cost of the computation of a representative of $\mathbf{t}_{\lambda,\psi}$ is $O((f_0\dots f_{i-1}f_\psi)^{2+\epsilon}(V_{\lambda,\psi})^{1+\epsilon})$ $\mathfrak{p}$-small operations. Along all refinement steps, we have $f_\psi=1$ and $V_{\lambda,\psi}=V_i+|\lambda|$, where $|\lambda|$ is a positive integer that grows strictly at each iteration; thus, the higher cost occurs at the last iteration.

Instead of distributing the cost into the nodes of $\mathcal{B}_{\lambda,\psi}$, we now attach the whole cost to every node $\mathbf{n}\in\mathcal{B}_{\lambda,\psi}$, so that our estimation is sharp only when $\#\mathcal{B}_{\lambda,\psi}=1$. Let us estimate the accumulated cost of every node $\mathbf{n}\in\mathcal{B}$.

Suppose $\mathbf{n}\in\mathcal{B}\setminus\mathcal{L}$. Eventually, after some refinement steps, in the last iteration, $f_\psi=f_{i,\mathbf{n}}$, $V_{\lambda,\psi}=V_{i+1,\mathbf{n}}$, are Okutsu data of the type $\mathbf{t}_{\mathbf{n}}$. Let $F_s$ be any irreducible factor of $F_{\mathbf{n}}$. As in the proof of Theorem 5.9, $f_0\dots f_{i-1}f_{i,\mathbf{n}}V_{i+1,\mathbf{n}}\leqslant 2\delta(F_s)\leqslant 2\delta$. Since there are at most $\lceil|\lambda_{\mathbf{n}}|\rceil$

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

iterations (Proposition 1.8), the accumulated cost of the computation of $\mathbf{n}$ is bounded from above by

$$\lceil|\lambda_{\mathbf{n}}|\rceil(f_0\dots f_{i-1}f_{i,\mathbf{n}})^{2+\epsilon}(V_{i+1,\mathbf{n}})^{1+\epsilon}=O(|\lambda_{\mathbf{n}}|n\delta^{1+\epsilon}).$$

Finally, let $\mathbf{n}\in\mathcal{B}\cap\mathcal{L}$. In the last iteration there is no call to `Representative`. Let $(\mathbf{t},\phi,\omega)$ be the input data of the penultimate iteration, and let $(\lambda,\psi)$ be the branch concerning $\mathbf{n}$. Let $u$ be the ordinate of the left end point of the side of slope $\lambda$ of $N_{i,\omega}(F)$. Since $u\neq 0$ and we work with precision $\delta+1$, we necessarily have $u\leqslant\delta e_0\dots e_{i-1}$. Now, $V_i+|\lambda|$ is the ordinate of the left end point of $N_i(F_{\mathbf{n}})$; by the theorem of the product, $V_i+|\lambda|\leqslant u\leqslant\delta e_0\dots e_{i-1}$. As we saw in the proof of the case `R=Newton`, the total number of all-but-last iterations is bounded from above by $v(\operatorname{Res}(F_{\mathbf{n}},F_t))/(f_0\dots f_{i-1})$; thus, the accumulated cost of all calls to `Representative` along the computation of $\mathbf{n}$ is

$$O((f_0\dots f_{i-1})^{1+\epsilon}(V_i+|\lambda|)^{1+\epsilon}v(\operatorname{Res}(F_{\mathbf{n}},F_t)))=O((m_i)^{1+\epsilon}\delta^{1+\epsilon}v(\operatorname{Res}(F_{\mathbf{n}},F_t))).$$

This ends the proof of the lemma. □

THEOREM 5.14. *The cost of the Montes algorithm over $\mathcal{O}_{\mathfrak{p}}$, applied to a monic separable polynomial $F\in A[x]$ of degree $n$ is $O(n^{2+\epsilon}+n^{1+\epsilon}(1+\delta)\log(q)+n^{1+\epsilon}\delta^{2+\epsilon})$ $\mathfrak{p}$-small operations, where $\delta:=v_{\mathfrak{p}}(\operatorname{Disc}(F))$.*

*Proof.* Let $\mathcal{N}:=\mathcal{T}\setminus(\mathcal{R}\cup\mathcal{L})$ be the set of nodes that are neither a root nor a leaf of $\mathcal{T}$. Let us denote the Okutsu invariants of $\mathbf{t}_s$ at level $i\leqslant r_s$ by $\lambda_{i,s}$, $e_{i,s}$, $f_{i,s}$, $m_{i,s}$, etc. Also, we denote $\rho_{s,t}:=v(\operatorname{Res}(F_s,F_t))$, for all $1\leqslant s\neq t\leqslant g$.

We shall use the estimation (5.4), and two obvious identities:

$$\sum_{\mathbf{n}\in\mathcal{N}}|\lambda_{\mathbf{n}}|\frac{\deg F_{\mathbf{n}}}{m_{\mathbf{n}}}=\sum_{1\leqslant s\leqslant g}\sum_{i=1}^{r_s}|\lambda_{i,s}|\frac{n_s}{m_{i,s}},\qquad\sum_{1\leqslant s\leqslant g}(\delta_s+\rho_{s,t})=O(\delta).\tag{5.10}$$

By (5.7), we need only to estimate $\sum_{\mathbf{m}\in\mathcal{T}\setminus\mathcal{L}}B_{\mathtt{R},\mathbf{m}}$, for each subroutine $\mathtt{R}\in\mathtt{Rout}$.

`R=Newton` or `Representative`. By Lemma 5.13, (5.4) and (5.10),

$$\begin{aligned}\sum_{\mathbf{m}\in\mathcal{T}\setminus\mathcal{L}}B_{\mathtt{R},\mathbf{m}}&\leqslant n^{1+\epsilon}\delta^{1+\epsilon}\Bigg(\sum_{\mathbf{n}\in\mathcal{N}}|\lambda_{\mathbf{n}}|\frac{\deg F_{\mathbf{n}}}{m_{\mathbf{n}}}+\sum_{\mathbf{n}\in\mathcal{L}}\rho_{s,t}\Bigg)\\&=n^{1+\epsilon}\delta^{1+\epsilon}\Bigg(\sum_{1\leqslant s\leqslant g}\Bigg(\sum_{1\leqslant i\leqslant r_s}|\lambda_{i,s}|\frac{n_s}{m_{i,s}}\Bigg)+\rho_{s,t}\Bigg)\\&=n^{1+\epsilon}\delta^{1+\epsilon}O\Bigg(\sum_{1\leqslant s\leqslant g}\delta_s+\rho_{s,t}\Bigg)=O(n^{1+\epsilon}\delta^{2+\epsilon}).\end{aligned}$$

`R = ResidualPolynomial` or `Factorization`. The argument is analogous:

$$\begin{aligned}\sum_{\mathbf{m}\in\mathcal{T}\setminus\mathcal{L}}B_{\mathtt{R},\mathbf{m}}&\leqslant n^{1+\epsilon}\log(q)\Bigg(\sum_{\mathbf{n}\in\mathcal{N}}|\lambda_{\mathbf{n}}|f_0\dots f_{i-1}\frac{\deg F_{\mathbf{n}}}{m_{\mathbf{n}}}+\sum_{\mathbf{n}\in\mathcal{L}}\rho_{s,t}\Bigg)\\&=n^{1+\epsilon}\log(q)\Bigg(\sum_{1\leqslant s\leqslant g}\Bigg(\sum_{1\leqslant i\leqslant r_s}|\lambda_{i,s}|\frac{f_{0,s}\dots f_{i-1,s}n_s}{m_{i,s}}\Bigg)+\rho_{s,t}\Bigg)\\&=n^{1+\epsilon}\log(q)O\Bigg(\sum_{1\leqslant s\leqslant g}\delta_s+\rho_{s,t}\Bigg)=O(n^{1+\epsilon}\delta\log(q)).\end{aligned}$$

□

COROLLARY 5.15. *The complexity of the Montes algorithm is $O(n^{2+\epsilon}+n^{1+\epsilon}\delta^{2+\epsilon})$ word operations, if $\mathfrak{p}$ is small.*

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

### 5.4. *Approximate factorization of polynomials over local fields*

Theorem 5.14 leads to an improvement of the complexity estimates of all routines mentioned in the introduction. In this section, we discuss the new estimation obtained for the factorization of polynomials over local fields, up to a prescribed precision.

Let $F \in A[x]$ be a monic separable polynomial of degree $n$, and denote $\delta := v_{\mathfrak{p}}(\operatorname{Disc}(F))$. Let $\mathfrak{p}$ be a non-zero prime ideal of $A$, and $F_1, \ldots, F_g \in \mathcal{O}_{\mathfrak{p}}[x]$ the irreducible factors of $F$ over $\mathcal{O}_{\mathfrak{p}}$. Suppose an OM factorization of $F$ over $\mathcal{O}_{\mathfrak{p}}[x]$ has been computed, in the form of a family $\mathbf{t}_{F_1}, \ldots, \mathbf{t}_{F_g}$ of OM representations of the irreducible factors, that faithfully represents $F$, and satisfies (3.2). Then, the single-factor lifting algorithm (SFL) derives from each $\mathbf{t}_{F_s}$ a monic polynomial $P_s \in A[x]$, irreducible over $\mathcal{O}_{\mathfrak{p}}$, such that $P_s \approx F_s$ and $P_s \equiv F_s \pmod{\mathfrak{m}^{\nu}}$, for an arbitrary prescribed precision $\nu$.

THEOREM 5.16. *The* SFL *algorithm requires $O(nn_s\nu^{1+\epsilon} + n\delta_s^{1+\epsilon})$ $\mathfrak{p}$-small operations, where $n_s := \deg F_s$, $\delta_s := \delta(F_s)$.*

*Proof.* Let $r_s$ be the Okutsu depth of $F_s$. In the proof of [9, Lemma 6.5], an estimation of $O(nn_s(\nu^{1+\epsilon} + (V_{r_s+1}/e(F_s))^{1+\epsilon}))$ $\mathfrak{p}$-small operations is obtained. In Lemma 2.2 we have seen that the Okutsu discriminant $\delta_0(F_s) := V_{r_s+1}/e(F_s)$ is bounded from above by $2\delta_s/n_s$. This proves the theorem. □

By applying the SFL routine to each OM representation $\mathbf{t}_{F_1}, \ldots, \mathbf{t}_{F_g}$, we get an OM factorization, $F \approx P_1 \ldots P_g$, such that $P_s \equiv F_s \pmod{\mathfrak{m}^{\nu}}$, for all $1 \leqslant s \leqslant g$.

THEOREM 5.17. *A combined application of the Montes and SFL algorithms computes an OM factorization of $F$ with prescribed precision $\nu$, at the cost of*

$$O(n^{2+\epsilon} + n^{1+\epsilon}(1+\delta)\log q + n^{1+\epsilon}\delta^{2+\epsilon} + n^2\nu^{1+\epsilon}) \quad \mathfrak{p}\text{-small operations.}$$

*If $\mathfrak{p}$ is small, we obtain a cost of $O(n^{2+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon} + n^2\nu^{1+\epsilon})$ word operations.*

*Proof.* The estimation is obtained by adding to the cost of the Montes algorithm, given in Theorem 5.14, the sum of the costs of SFL given in Theorem 5.16, for $1 \leqslant s \leqslant g$, having in mind that $n_1 + \ldots + n_g = n$, $\delta_1 + \ldots + \delta_g \leqslant \delta$. □

In comparison with previous estimations, the total degree in $n$, $\delta$ and $\nu$ is reduced from $4+\epsilon$ to $3+\epsilon$.

*Acknowledgement.* We are indebted to the anonymous referees for their suggestions, leading to an improved version of Corollary 2.4.

## *References*

1. D. FORD, S. PAULI and X.-F. ROBLOT, ‘A fast algorithm for polynomial factorization over $\mathbb{Q}_p$’, *J. Théor. Nombres de Bordeaux* 14 (2002) 151–169.
2. D. FORD and O. VERES, ‘On the complexity of the Montes ideal factorization algorithm’, *Algorithmic number theory, 9th International Symposium, ANTS-IX*, Nancy, France, July 19–23, 2010, Lecture Notes in Computer Science (eds G. Hanrot, F. Morain and E. Thomé; Springer, 2010).
3. J. VON ZUR GATHEN and J. GERHARD, *Modern computer algebra*, 2nd edn (Cambridge University Press, Cambridge, 2003).
4. J. GUÀRDIA, J. MONTES and E. NART, ‘Okutsu invariants and Newton polygons’, *Acta Arith.* 145 (2010) 83–108.
5. J. GUÀRDIA, J. MONTES and E. NART, ‘Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields’, *J. Théor. Nombres Bordeaux* 23 (2011) no. 3, 667–696.
6. J. GUÀRDIA, J. MONTES and E. NART, ‘Newton polygons of higher order in algebraic number theory’, *Trans. Amer. Math. Soc.* 364 (2012) no. 1, 361–416.

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press

**7.** J. Guàrdia, J. Montes and E. Nart, ‘A new computational approach to ideal theory in number fields’, *Found. Comput. Math.*, doi:10.1007/s10208-012-9137-5.

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

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

**10.** S. MacLane, ‘A construction for absolute values in polynomial rings’, *Trans. Amer. Math. Soc.* 40 (1936) 363–395.

**11.** S. MacLane, ‘A construction for prime ideals as absolute values of an algebraic field’, *Duke Math. J.* 2 (1936) 492–510.

**12.** E. Nart, ‘Okutsu–Montes representations of prime ideals of one-dimensional integral closures’, *Publ. Mat.* 55 (2011) no. 3, 261–294.

**13.** E. Nart, ‘Local computation of differents and discriminants’, *Math. Comput.*, to appear, arXiv:1205.1340v1 [math.NT].

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

**15.** Ø. Ore, ‘Zur Theorie der algebraischen Körper’, *Acta. Math.* 44 (1923) 219–314.

**16.** Ø. Ore, ‘Newtonsche Polygone in der Theorie der algebraischen Körper’, *Math. Ann.* 99 (1928) 84–117.

**17.** S. Pauli, ‘Factoring polynomials over local fields’, *J. Symbolic Comput.* 32 (2001) 533–547.

**18.** S. Pauli, ‘Factoring polynomials over local fields, II’, *Algorithmic number theory, 9th International Symposium, ANTS-IX,* Nancy, France, July 19–23, 2010, Lecture Notes in Computer Science (eds G. Hanrot, F. Morain and E. Thomé; Springer, 2010).

**19.** A. Schönhage and V. Strassen, ‘Schnelle Multiplikation großer Zahlen’, *Computing* 7 (1971) 281–292.

*Jens-Dietrich Bauch*
*Departament de Matemàtiques*
*Universitat Autònoma de Barcelona*
*Edifici C, E-08193 Bellaterra*
*Barcelona, Catalonia*
*Spain*

bauch@mat.uab.cat

*Enric Nart*
*Departament de Matemàtiques*
*Universitat Autònoma de Barcelona*
*Edifici C, E-08193 Bellaterra*
*Barcelona, Catalonia*
*Spain*

nart@mat.uab.cat

*Hayden D. Stainsby*
*Departament de Matemàtiques*
*Universitat Autònoma de Barcelona*
*Edifici C, E-08193 Bellaterra*
*Barcelona, Catalonia*
*Spain*

hds@mat.uab.cat

https://doi.org/10.1112/S1461157013000089 Published online by Cambridge University Press