Computing triangular bases of integral closures

Hayden D. Stainsby

Universitat Autònoma de Barcelona

Seminari de Teoria de Nombres de Barcelona

30 January, 2015

Outline

Outline

Setting

(K, v) a discrete valued field, $\mathcal{O}$ valuation ring, $\mathfrak{m} = \pi\mathcal{O}$ maximal ideal, $\mathbb{F}_0 := \mathbb{F} = \mathcal{O}/\mathfrak{m}$ residue field.

K_v completion of K, $\mathcal{O}_v$ valuation ring of K_v.
$v : \overline{K}_v^* \longrightarrow \mathbb{Q}$.

Setting

(K, v) a discrete valued field, $\mathcal{O}$ valuation ring, $\mathfrak{m} = \pi\mathcal{O}$ maximal ideal, $\mathbb{F}_0 := \mathbb{F} = \mathcal{O}/\mathfrak{m}$ residue field.

K_v completion of K, $\mathcal{O}_v$ valuation ring of K_v.
$v : \overline{K}_v^* \longrightarrow \mathbb{Q}$.

$f \in \mathcal{O}[x]$ monic irreducible of degree n, $f(\theta) = 0$.

Setting

(K, v) a discrete valued field, $\mathcal{O}$ valuation ring, $\mathfrak{m} = \pi\mathcal{O}$ maximal ideal, $\mathbb{F}_0 := \mathbb{F} = \mathcal{O}/\mathfrak{m}$ residue field.

K_v completion of K, $\mathcal{O}_v$ valuation ring of K_v.
$v : \overline{K}_v^* \longrightarrow \mathbb{Q}$.

$f \in \mathcal{O}[x]$ monic irreducible of degree n, $f(\theta) = 0$.

$L = K(\theta)$, $\mathcal{O}_L$ integral closure of $\mathcal{O}$ in L.
$\mathcal{P}$ set of prime ideals of $\mathcal{O}_L$.

Setting

(K, v) a discrete valued field, $\mathcal{O}$ valuation ring, $\mathfrak{m} = \pi\mathcal{O}$ maximal ideal, $\mathbb{F}_0 := \mathbb{F} = \mathcal{O}/\mathfrak{m}$ residue field.

K_v completion of K, $\mathcal{O}_v$ valuation ring of K_v.
$v : \overline{K}_v^* \longrightarrow \mathbb{Q}$.

$f \in \mathcal{O}[x]$ monic irreducible of degree n, $f(\theta) = 0$.

$L = K(\theta)$, $\mathcal{O}_L$ integral closure of $\mathcal{O}$ in L.
$\mathcal{P}$ set of prime ideals of $\mathcal{O}_L$.

Hypothesis

We suppose that $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}$-module.

Valuations

For any $\mathfrak{p} \in \mathcal{P}$, consider the valuation

$$w_{\mathfrak{p}}: \quad L \longrightarrow \mathbb{Q} \cup \{\infty\}$$
$$\alpha \longmapsto \frac{v_{\mathfrak{p}}(\alpha)}{e(\mathfrak{p}/\mathfrak{m})},$$

Valuations

For any $\mathfrak{p} \in \mathcal{P}$, consider the valuation

$$w_{\mathfrak{p}}: \quad L \longrightarrow \mathbb{Q} \cup \{\infty\}$$
$$\alpha \longmapsto \frac{v_{\mathfrak{p}}(\alpha)}{e(\mathfrak{p}/\mathfrak{m})},$$

Take

$$w(\alpha) := \min \{w_{\mathfrak{p}}(\alpha)\}_{\mathfrak{p} \in \mathcal{P}}, \qquad \forall\ \alpha \in L,$$

Valuations

For any $\mathfrak{p} \in \mathcal{P}$, consider the valuation

$$w_{\mathfrak{p}} : \quad L \longrightarrow \mathbb{Q} \cup \{\infty\}$$
$$\alpha \longmapsto \frac{v_{\mathfrak{p}}(\alpha)}{e(\mathfrak{p}/\mathfrak{m})},$$

Take

$$w(\alpha) := \min\{w_{\mathfrak{p}}(\alpha)\}_{\mathfrak{p}\in\mathcal{P}}, \qquad \forall\ \alpha \in L,$$

then $\alpha \in \mathcal{O}_L \iff w(\alpha) \geqslant 0$.

Triangular bases

Definition

A triangular family of elements in $\mathcal{O}_L$, are elements

$$\frac{g_0(\theta)}{\pi^{\lfloor \nu_0 \rfloor}}, \frac{g_1(\theta)}{\pi^{\lfloor \nu_1 \rfloor}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{\lfloor \nu_{n-1} \rfloor}},$$

such that $g_i(x) \in \mathcal{O}[x]$ monic of degree i and $\nu_i = w\left(g_i(\theta)\right)$.

Triangular bases

Definition

A triangular family of elements in $\mathcal{O}_L$, are elements

$$\frac{g_0(\theta)}{\pi^{\lfloor \nu_0 \rfloor}}, \frac{g_1(\theta)}{\pi^{\lfloor \nu_1 \rfloor}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{\lfloor \nu_{n-1} \rfloor}},$$

such that $g_i(x) \in \mathcal{O}[x]$ monic of degree i and $\nu_i = w\left(g_i(\theta)\right)$.

Theorem

Let $g_0(\theta)/\pi^{\lfloor \nu_0 \rfloor}, \ldots, g_{n-1}(\theta)/\pi^{\lfloor \nu_{n-1} \rfloor}$ be a triangular family of $\mathcal{O}_L$. Then,

Triangular bases

Definition

A triangular family of elements in $\mathcal{O}_L$, are elements

$$\frac{g_0(\theta)}{\pi^{\lfloor \nu_0 \rfloor}}, \frac{g_1(\theta)}{\pi^{\lfloor \nu_1 \rfloor}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{\lfloor \nu_{n-1} \rfloor}},$$

such that $g_i(x) \in \mathcal{O}[x]$ monic of degree i and $\nu_i = w\left(g_i(\theta)\right)$.

Theorem

Let $g_0(\theta)/\pi^{\lfloor \nu_0 \rfloor}, \ldots, g_{n-1}(\theta)/\pi^{\lfloor \nu_{n-1} \rfloor}$ be a triangular family of $\mathcal{O}_L$. Then,

(1) $\left\{g_i(\theta)/\pi^{\lfloor \nu_i \rfloor}\right\}$ is a v-integral basis $\iff \lfloor \nu_i \rfloor \geqslant \lfloor w\left(g(\theta)\right) \rfloor$ for all $g \in \mathcal{O}[x]$ monic of degree i, $0 \leqslant i < n$.

Triangular bases

Definition

A triangular family of elements in $\mathcal{O}_L$, are elements

$$\frac{g_0(\theta)}{\pi^{\lfloor \nu_0 \rfloor}}, \frac{g_1(\theta)}{\pi^{\lfloor \nu_1 \rfloor}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{\lfloor \nu_{n-1} \rfloor}},$$

such that $g_i(x) \in \mathcal{O}[x]$ monic of degree i and $\nu_i = w\left(g_i(\theta)\right)$.

Theorem

Let $g_0(\theta)/\pi^{\lfloor \nu_0 \rfloor}, \ldots, g_{n-1}(\theta)/\pi^{\lfloor \nu_{n-1} \rfloor}$ be a triangular family of $\mathcal{O}_L$. Then,

(1) $\left\{g_i(\theta)/\pi^{\lfloor \nu_i \rfloor}\right\}$ is a v-integral basis $\iff \lfloor \nu_i \rfloor \geqslant \lfloor w\left(g(\theta)\right) \rfloor$ for all $g \in \mathcal{O}[x]$ monic of degree i, $0 \leqslant i < n$.

(2) $\left\{g_i(\theta)/\pi^{\lfloor \nu_i \rfloor}\right\}$ is a reduced v-integral basis $\iff \nu_i \geqslant w\left(g(\theta)\right)$ for all $g \in \mathcal{O}[x]$ monic of degree i, $0 \leqslant i < n$.

Reduced families

Definition

A family $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ is called reduced if for any family $a_1, \ldots, a_n \in \mathcal{O}_v$:

$$w\left(\sum_{i=1}^{n} a_i \alpha_i\right) = \min\left\{w\left(a_i \alpha_i\right) : 1 \leqslant i \leqslant n\right\}.$$

Reduced families

Definition

A family $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ is called reduced if for any family $a_1, \ldots, a_n \in \mathcal{O}_v$:

$$w\left(\sum_{i=1}^{n} a_i\alpha_i\right) = \min\left\{w\left(a_i\alpha_i\right) : 1 \leqslant i \leqslant n\right\}.$$

Reduced bases are useful for some applications in function fields.

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

$$f = F_{\mathfrak{p}_1} \dots F_{\mathfrak{p}_s} \text{ in } \mathcal{O}_v[x] \quad \longleftrightarrow \quad \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = \mathcal{P}.$$

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

$$f = F_{\mathfrak{p}_1} \dots F_{\mathfrak{p}_s} \text{ in } \mathcal{O}_v[x] \quad \longleftrightarrow \quad \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = \mathcal{P}.$$

$$\mathfrak{p}_1 \rightsquigarrow \mathbb{t}_{\mathfrak{p}_1}$$

$$\vdots \qquad \vdots$$

$$\mathfrak{p}_s \rightsquigarrow \mathbb{t}_{\mathfrak{p}_s}$$

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

$$f = F_{\mathfrak{p}_1} \dots F_{\mathfrak{p}_s} \text{ in } \mathcal{O}_v[x] \quad \longleftrightarrow \quad \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = \mathcal{P}.$$

$\mathfrak{p}_1 \rightsquigarrow \mathbb{t}_{\mathfrak{p}_1}$

$\vdots$ Montes algorithm $\vdots$

$\mathfrak{p}_s \rightsquigarrow \mathbb{t}_{\mathfrak{p}_s}$

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

$$f = F_{\mathfrak{p}_1} \dots F_{\mathfrak{p}_s} \text{ in } \mathcal{O}_v[x] \quad \longleftrightarrow \quad \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = \mathcal{P}.$$

$$\left.\begin{array}{ccc} \mathfrak{p}_1 & \rightsquigarrow & \mathbb{t}_{\mathfrak{p}_1} \\ \vdots & \text{Montes algorithm} & \vdots \\ \mathfrak{p}_s & \rightsquigarrow & \mathbb{t}_{\mathfrak{p}_s} \end{array}\right\} \xrightarrow{\text{“MaxMin”}} g_0(\theta)/\pi^{\lfloor \nu_0 \rfloor}, \dots, g_{n-1}(\theta)/\pi^{\lfloor \nu_{n-1} \rfloor}$$

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

$$f = F_{\mathfrak{p}_1} \dots F_{\mathfrak{p}_s} \text{ in } \mathcal{O}_v[x] \quad \longleftrightarrow \quad \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = \mathcal{P}.$$

$$\left.\begin{array}{ccc} \mathfrak{p}_1 & \rightsquigarrow & \mathbb{t}_{\mathfrak{p}_1} \\ \vdots & \text{Montes algorithm} & \vdots \\ \mathfrak{p}_s & \rightsquigarrow & \mathbb{t}_{\mathfrak{p}_s} \end{array}\right\} \xrightarrow{\text{"MaxMin"}} g_0(\theta)/\pi^{\lfloor \nu_0 \rfloor}, \dots, g_{n-1}(\theta)/\pi^{\lfloor \nu_{n-1} \rfloor}$$

It's also reduced!

Outline

OM representations of prime ideals

An OM representation of the prime ideal $\mathfrak{p} \in \mathcal{P}$:

$$\mathbb{t}_{\mathfrak{p}} = \big(\psi_{0,\mathfrak{p}}; (\phi_{1,\mathfrak{p}}, \lambda_{1,\mathfrak{p}}, \psi_{1,\mathfrak{p}}); \ldots; (\phi_{r_{\mathfrak{p}},\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}}); (\phi_{r_{\mathfrak{p}}+1,\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}})\big)$$

OM representations of prime ideals

An OM representation of the prime ideal $\mathfrak{p} \in \mathcal{P}$:

$$\mathbb{t}_{\mathfrak{p}} = \big(\psi_{0,\mathfrak{p}}; (\phi_{1,\mathfrak{p}}, \lambda_{1,\mathfrak{p}}, \psi_{1,\mathfrak{p}}); \ldots; (\phi_{r_{\mathfrak{p}},\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}}); (\phi_{r_{\mathfrak{p}}+1,\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}})\big)$$

Invariants at each level: $\frac{h_{i,\mathfrak{p}}}{e_{i,\mathfrak{p}}} = \lambda_{i,\mathfrak{p}}$, $f_{i,\mathfrak{p}} = \deg \psi_{i,\mathfrak{p}}$.

OM representations of prime ideals

An OM representation of the prime ideal $\mathfrak{p} \in \mathcal{P}$:

$$\mathbb{t}_{\mathfrak{p}} = \left(\psi_{0,\mathfrak{p}}; (\phi_{1,\mathfrak{p}}, \lambda_{1,\mathfrak{p}}, \psi_{1,\mathfrak{p}}); \ldots; (\phi_{r_{\mathfrak{p}},\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}}); (\phi_{r_{\mathfrak{p}}+1,\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}})\right)$$

Invariants at each level: $\dfrac{h_{i,\mathfrak{p}}}{e_{i,\mathfrak{p}}} = \lambda_{i,\mathfrak{p}}$, $f_{i,\mathfrak{p}} = \deg \psi_{i,\mathfrak{p}}$.

$\phi_{i,\mathfrak{p}} \in \mathcal{O}[x]$ monic of degree m_i with $w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{p}}(\theta)\right)$ maximal for monic degree m_i polynomials in $\mathcal{O}[x]$.

OM representations of prime ideals

An OM representation of the prime ideal $\mathfrak{p} \in \mathcal{P}$:

$$\mathbb{t}_{\mathfrak{p}} = \left(\psi_{0,\mathfrak{p}}; (\phi_{1,\mathfrak{p}}, \lambda_{1,\mathfrak{p}}, \psi_{1,\mathfrak{p}}); \ldots; (\phi_{r_{\mathfrak{p}},\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}}); (\phi_{r_{\mathfrak{p}}+1,\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}})\right)$$

Invariants at each level: $\dfrac{h_{i,\mathfrak{p}}}{e_{i,\mathfrak{p}}} = \lambda_{i,\mathfrak{p}}$, $f_{i,\mathfrak{p}} = \deg \psi_{i,\mathfrak{p}}$.

$\phi_{i,\mathfrak{p}} \in \mathcal{O}[x]$ monic of degree m_i with $w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{p}}(\theta)\right)$ maximal for monic degree m_i polynomials in $\mathcal{O}[x]$.

$$g_{k,\mathfrak{p}} := x^{a_0} \prod_{i=1}^{r} \phi_i^{a_i}, \qquad 0 \leqslant k < n_{\mathfrak{p}},$$
$$k = a_0 + a_1 m_1 + \cdots + a_r m_r, \qquad 0 \leqslant a_i < m_{i+1}/m_i = e_i f_i.$$

Okutsu $\mathfrak{p}$-bases

Taking $\nu_{k,\mathfrak{p}} = w_{\mathfrak{p}}\left(g_{k,\mathfrak{p}}(\theta)\right)$, we have a basis of $\mathcal{O}_{\mathfrak{p}} := \mathcal{O}_v[x]/(F_{\mathfrak{p}})$,

$$\mathcal{B}_{\mathfrak{p}} = \left\{ g_{0,\mathfrak{p}}(\theta)/\pi^{\lfloor \nu_{0,\mathfrak{p}} \rfloor}, \ldots, g_{n_{\mathfrak{p}}-1,\mathfrak{p}}(\theta)/\pi^{\lfloor \nu_{n_{\mathfrak{p}}-1,\mathfrak{p}} \rfloor} \right\}.$$

We call this an Okutsu $\mathfrak{p}$-basis.

Okutsu $\mathfrak{p}$-bases

Taking $\nu_{k,\mathfrak{p}} = w_{\mathfrak{p}}\left(g_{k,\mathfrak{p}}(\theta)\right)$, we have a basis of $\mathcal{O}_{\mathfrak{p}} := \mathcal{O}_v[x]/(F_{\mathfrak{p}})$,

$$\mathcal{B}_{\mathfrak{p}} = \left\{ g_{0,\mathfrak{p}}(\theta)/\pi^{\lfloor \nu_{0,\mathfrak{p}} \rfloor}, \ldots, g_{n_{\mathfrak{p}}-1,\mathfrak{p}}(\theta)/\pi^{\lfloor \nu_{n_{\mathfrak{p}}-1,\mathfrak{p}} \rfloor} \right\}.$$

We call this an Okutsu $\mathfrak{p}$-basis.

We take the numerators of this basis, and extend them by appending $\phi_{\mathfrak{p}}$ a Montes approximation to $F_{\mathfrak{p}}$ as a factor of f,

$$\mathcal{N}_{\mathfrak{p}} = \left\{ 1 =: g_{0,\mathfrak{p}}, \ldots, g_{n_{\mathfrak{p}}-1,\mathfrak{p}}, g_{n_{\mathfrak{p}},\mathfrak{p}} := \phi_{\mathfrak{p}} \right\}.$$

Optimal polynomials as products of ϕ-polynomials

Consider the multiplicative semi-group:

$$\Phi(\mathcal{P}) := \left\langle 1, \{\phi_{i,\mathfrak{p}}\}_{\mathfrak{p}\in\mathcal{P}}, \bigcup_{\mathfrak{p}\in\mathcal{P}} \mathrm{Rep}(\mathbb{t}_{\mathfrak{p}}) \right\rangle \subset \mathcal{O}[x].$$

where $\mathrm{Rep}(\mathbb{t}_{\mathfrak{p}}) = [F_{\mathfrak{p}}] \cap \mathcal{O}[x]$ the set of all representatives of $\mathbb{t}_{\mathfrak{p}}$ with coefficients in $\mathcal{O}$.

Optimal polynomials as products of ϕ-polynomials

Consider the multiplicative semi-group:

$$\Phi(\mathcal{P}) := \left\langle 1, \{\phi_{i,\mathfrak{p}}\}_{\mathfrak{p}\in\mathcal{P}}, \bigcup_{\mathfrak{p}\in\mathcal{P}} \operatorname{Rep}(\mathbb{t}_{\mathfrak{p}}) \right\rangle \subset \mathcal{O}[x].$$

where $\operatorname{Rep}(\mathbb{t}_{\mathfrak{p}}) = [F_{\mathfrak{p}}] \cap \mathcal{O}[x]$ the set of all representatives of $\mathbb{t}_{\mathfrak{p}}$ with coefficients in $\mathcal{O}$.

Theorem

For any $h \in \mathcal{O}[x]$ monic of degree $0 \leqslant d < n$, there exists $\phi \in \Phi(\mathcal{P})$ also of degree d such that,

$$w_{\mathfrak{p}}\left(\phi(\theta)\right) \geqslant w_{\mathfrak{p}}\left(h(\theta)\right), \qquad \forall\ \mathfrak{p} \in \mathcal{P}.$$

Optimal polynomials as products of numerators of Okutsu bases

We may now consider the Okutsu set of monic polynomials:

$$\mathrm{Ok}(\mathcal{P}) := \left\{ \prod_{\mathfrak{p}\in\mathcal{P}} g_{i_\mathfrak{p},\mathfrak{p}} : 0 \leqslant i_\mathfrak{p} \leqslant n_\mathfrak{p} \right\} \subset \Phi(\mathcal{P}).$$

Optimal polynomials as products of numerators of Okutsu bases

We may now consider the Okutsu set of monic polynomials:

$$\mathrm{Ok}(\mathcal{P}) := \left\{ \prod_{\mathfrak{p}\in\mathcal{P}} g_{i_\mathfrak{p},\mathfrak{p}} : 0 \leqslant i_\mathfrak{p} \leqslant n_\mathfrak{p} \right\} \subset \Phi(\mathcal{P}).$$

Theorem

For any $\phi \in \Phi(\mathcal{P})$ monic of degree $0 \leqslant d < n$, there exists $g \in \mathrm{Ok}(\mathcal{P})$ also monic and of degree d such that,

$$w_\mathfrak{p}\left(g(\theta)\right) \geqslant w_\mathfrak{p}\left(\phi(\theta)\right), \qquad \forall\ \mathfrak{p} \in \mathcal{P}.$$

Outline

Formal extension of the Okutsu $\mathfrak{p}$-bases

Definition

For all $\mathfrak{p} \in \mathcal{P}$,

$$w_{\mathfrak{p}} : \mathrm{Ok}(\mathcal{P}) \longrightarrow \mathbb{Q} \cup \{\infty\}$$
$$\phi \longmapsto \begin{cases} w_{\mathfrak{p}}\left(\phi(\theta)\right), & \text{if } \phi_{\mathfrak{p}} \nmid \phi, \\ \infty, & \text{if } \phi_{\mathfrak{p}} \mid \phi. \end{cases}$$

Formal extension of the Okutsu $\mathfrak{p}$-bases

Definition

For all $\mathfrak{p} \in \mathcal{P}$,

$$w_{\mathfrak{p}} : \mathrm{Ok}(\mathcal{P}) \longrightarrow \mathbb{Q} \cup \{\infty\}$$
$$\phi \longmapsto \begin{cases} w_{\mathfrak{p}}\left(\phi(\theta)\right), & \text{if } \phi_{\mathfrak{p}} \nmid \phi, \\ \infty, & \text{if } \phi_{\mathfrak{p}} \mid \phi. \end{cases}$$

The value $w_{\mathfrak{q}}\left(\phi_{\mathfrak{p}}(\theta)\right)$ for each $\mathfrak{q} \neq \mathfrak{p}$ is fixed, and $w_{\mathfrak{p}}\left(\phi_{\mathfrak{p}}(\theta)\right)$ can be made arbitrarily large.

Formal extension of the Okutsu $\mathfrak{p}$-bases

Definition

For all $\mathfrak{p} \in \mathcal{P}$,

$$w_{\mathfrak{p}} : \mathrm{Ok}(\mathcal{P}) \longrightarrow \mathbb{Q} \cup \{\infty\}$$
$$\phi \longmapsto \begin{cases} w_{\mathfrak{p}}\left(\phi(\theta)\right), & \text{if } \phi_{\mathfrak{p}} \nmid \phi, \\ \infty, & \text{if } \phi_{\mathfrak{p}} \mid \phi. \end{cases}$$

The value $w_{\mathfrak{q}}\left(\phi_{\mathfrak{p}}(\theta)\right)$ for each $\mathfrak{q} \neq \mathfrak{p}$ is fixed, and $w_{\mathfrak{p}}\left(\phi_{\mathfrak{p}}(\theta)\right)$ can be made arbitrarily large.

We take $\phi_{\mathfrak{p}}$ to be a symbolic polynomial of degree $n_{\mathfrak{p}}$.

Maximal multi-indices

We may define a polynomial in $\mathrm{Ok}(\mathcal{P})$ by a multi-index $\mathbb{i} = (i_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{P}} \in \mathbb{N}^s$, so that

$$g_{\mathbb{i}} = \prod_{\mathfrak{p}\in\mathcal{P}} g_{i_{\mathfrak{p}},\mathfrak{p}},$$

Maximal multi-indices

We may define a polynomial in $\mathrm{Ok}(\mathcal{P})$ by a multi-index $\mathbb{i} = (i_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}} \in \mathbb{N}^s$, so that

$$g_\mathbb{i} = \prod_{\mathfrak{p}\in\mathcal{P}} g_{i_\mathfrak{p},\mathfrak{p}},$$

$$\deg \mathbb{i} := \sum_{\mathfrak{p}\in\mathcal{P}} i_\mathfrak{p} = \deg(g_\mathbb{i}).$$

$$\mathbb{u}_j = (0, \ldots, \underset{j\text{-th}}{1}, \ldots, 0).$$

Maximal multi-indices

We may define a polynomial in $\mathrm{Ok}(\mathcal{P})$ by a multi-index $\mathbb{i} = (i_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}} \in \mathbb{N}^s$, so that

$$g_\mathbb{i} = \prod_{\mathfrak{p}\in\mathcal{P}} g_{i_\mathfrak{p},\mathfrak{p}},$$

$$\deg \mathbb{i} := \sum_{\mathfrak{p}\in\mathcal{P}} i_\mathfrak{p} = \deg(g_\mathbb{i}).$$

$$\mathbb{u}_j = (0,\dots,\underset{j\text{-th}}{1},\dots,0).$$

Definition

A multi-index $\mathbb{i}$ is maximal if $w(g_\mathbb{i}) \geqslant w(g_\mathbb{j})$, for all multi-indices $\mathbb{j}$ with $\deg \mathbb{j} = \deg \mathbb{i}$.

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

Aim

Aim

Construct a triangular v-integral basis of $\mathcal{O}_L$.

$$\downarrow$$

Aim

The aim of the MaxMin algorithm is to efficiently select maximal multi-indices of degree $0, 1, \ldots, n-1$.

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Input

Numerators $\{g_{i,\mathfrak{p}} : 0 \leqslant i \leqslant n_\mathfrak{p}\}$ of Okutsu $\mathfrak{p}$-bases for each prime ideal $\mathfrak{p} \in \mathcal{P}$.

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Input

Numerators $\{g_{i,\mathfrak{p}} : 0 \leqslant i \leqslant n_{\mathfrak{p}}\}$ of Okutsu $\mathfrak{p}$-bases for each prime ideal $\mathfrak{p} \in \mathcal{P}$.

Output

A family $\mathbb{i}_0, \mathbb{i}_1, \ldots, \mathbb{i}_n \in \mathbb{N}^s$ of maximal multi-indices of degree $0, 1, \ldots, n$ respectively.

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Input

Numerators $\{g_{i,\mathfrak{p}} : 0 \leqslant i \leqslant n_\mathfrak{p}\}$ of Okutsu $\mathfrak{p}$-bases for each prime ideal $\mathfrak{p} \in \mathcal{P}$.

Output

A family $\mathbb{i}_0, \mathbb{i}_1, \ldots, \mathbb{i}_n \in \mathbb{N}^s$ of maximal multi-indices of degree $0, 1, \ldots, n$ respectively.

Algorithm

1: $\mathbb{i}_0 \leftarrow (0, \ldots, 0)$
2: **for** $k = 0 \to n-1$ **do**
3: $\quad j \leftarrow \min\{1 \leqslant i \leqslant s : w_{\mathfrak{p}_i}(g_{\mathbb{i}_k}) = w(g_{\mathbb{i}_k})\}$
4: $\quad \mathbb{i}_{k+1} \leftarrow \mathbb{i}_k + \mathbb{u}_j$
5: **end for**

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Theorem

All output multi-indices of $\mathrm{MaxMin}[\mathcal{P}]$ are maximal.

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Theorem

All output multi-indices of $\mathrm{MaxMin}[\mathcal{P}]$ are maximal.

MaxMin finds the maximal value amongst the minima of certain numerical data, hence the name.

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Theorem

All output multi-indices of $\mathrm{MaxMin}[\mathcal{P}]$ are maximal.

MaxMin finds the maximal value amongst the minima of certain numerical data, hence the name.

Remarks

Guaranteed termination

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Theorem

All output multi-indices of $\mathrm{MaxMin}[\mathcal{P}]$ are maximal.

MaxMin finds the maximal value amongst the minima of certain numerical data, hence the name.

Remarks

- Guaranteed termination
- Polynomial products are not computed

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Theorem

All output multi-indices of $\mathrm{MaxMin}[\mathcal{P}]$ are maximal.

MaxMin finds the maximal value amongst the minima of certain numerical data, hence the name.

Remarks

- Guaranteed termination
- Polynomial products are not computed
- Initial conditions

The $\mathrm{MaxMin}[\mathcal{P}]$ algorithm

Theorem

All output multi-indices of $\mathrm{MaxMin}[\mathcal{P}]$ are maximal.

MaxMin finds the maximal value amongst the minima of certain numerical data, hence the name.

Remarks

- Guaranteed termination
- Polynomial products are not computed
- Initial conditions
- Ordering of input prime ideals

Explicit formulas for valuations of ϕ-polynomials

For all prime ideals $\mathfrak{p} \in \mathcal{P}$,

$$w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{p}}(\theta)\right) = \frac{V_{i,\mathfrak{p}} + \lambda_{i,\mathfrak{p}}}{e_{1,\mathfrak{p}} \cdots e_{i-1,\mathfrak{p}}}.$$

Explicit formulas for valuations of ϕ-polynomials

For all prime ideals $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \neq \mathfrak{p}$ and $\ell = i(\mathfrak{p}, \mathfrak{q})$,

$$w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) = \begin{cases} 0, & \text{if } \ell = 0, \\ \dfrac{V_i + \lambda_i}{e_1 \cdots e_{i-1}}, & \text{if } i < \ell, \\ \dfrac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{q}}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p}, \mathfrak{q}), \\ \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} \neq \phi(\mathfrak{p}, \mathfrak{q}), \\ \dfrac{m_{i,\mathfrak{q}}}{m_\ell} \cdot \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i > \ell > 0. \end{cases}$$

Explicit formulas for valuations of ϕ-polynomials

For all prime ideals $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \neq \mathfrak{p}$ and $\ell = i(\mathfrak{p}, \mathfrak{q})$,

$$w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) = \begin{cases} 0, & \text{if } \ell = 0, \\ \dfrac{V_i + \lambda_i}{e_1 \cdots e_{i-1}}, & \text{if } i < \ell, \\ \dfrac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{q}}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p},\mathfrak{q}), \\ \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} \neq \phi(\mathfrak{p},\mathfrak{q}), \\ \dfrac{m_{i,\mathfrak{q}}}{m_\ell} \cdot \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i > \ell > 0. \end{cases}$$

$i(\mathfrak{p}, \mathfrak{q})$ - index of coincidence

$\phi(\mathfrak{p}, \mathfrak{q})$ - last shared ϕ-polynomial

$\lambda_{\mathfrak{p}}^{\mathfrak{q}}$ - hidden slope

Explicit formulas for valuations of ϕ-polynomials

For all prime ideals $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \neq \mathfrak{p}$ and $\ell = i(\mathfrak{p}, \mathfrak{q})$,

$$w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) = \begin{cases} 0, & \text{if } \ell = 0, \\ \dfrac{V_i + \lambda_i}{e_1 \cdots e_{i-1}}, & \text{if } i < \ell, \\ \dfrac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{q}}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p},\mathfrak{q}), \\ \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} \neq \phi(\mathfrak{p},\mathfrak{q}), \\ \dfrac{m_{i,\mathfrak{q}}}{m_\ell} \cdot \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i > \ell > 0. \end{cases}$$

$i(\mathfrak{p}, \mathfrak{q})$ - index of coincidence

$\phi(\mathfrak{p}, \mathfrak{q})$ - last shared ϕ-polynomial

$\lambda_{\mathfrak{p}}^{\mathfrak{q}}$ - hidden slope

Explicit formulas for valuations of ϕ-polynomials

For all prime ideals $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \neq \mathfrak{p}$ and $\ell = i(\mathfrak{p}, \mathfrak{q})$,

$$w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) = \begin{cases} 0, & \text{if } \ell = 0, \\ \dfrac{V_i + \lambda_i}{e_1 \cdots e_{i-1}}, & \text{if } i < \ell, \\ \dfrac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{q}}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p},\mathfrak{q}), \\ \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} \neq \phi(\mathfrak{p},\mathfrak{q}), \\ \dfrac{m_{i,\mathfrak{q}}}{m_\ell} \cdot \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i > \ell > 0. \end{cases}$$

$i(\mathfrak{p}, \mathfrak{q})$ - index of coincidence

$\phi(\mathfrak{p}, \mathfrak{q})$ - last shared ϕ-polynomial

$\lambda_{\mathfrak{p}}^{\mathfrak{q}}$ - hidden slope

Explicit formulas for valuations of ϕ-polynomials

For all prime ideals $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \neq \mathfrak{p}$ and $\ell = i(\mathfrak{p}, \mathfrak{q})$,

$$w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) = \begin{cases} 0, & \text{if } \ell = 0, \\ \dfrac{V_i + \lambda_i}{e_1 \cdots e_{i-1}}, & \text{if } i < \ell, \\ \dfrac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{q}}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p}, \mathfrak{q}), \\ \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell > 0 \text{ and } \phi_{\ell,\mathfrak{q}} \neq \phi(\mathfrak{p}, \mathfrak{q}), \\ \dfrac{m_{i,\mathfrak{q}}}{m_\ell} \cdot \dfrac{V_\ell + \min\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{if } i > \ell > 0. \end{cases}$$

$i(\mathfrak{p}, \mathfrak{q})$ - index of coincidence

$\phi(\mathfrak{p}, \mathfrak{q})$ - last shared ϕ-polynomial

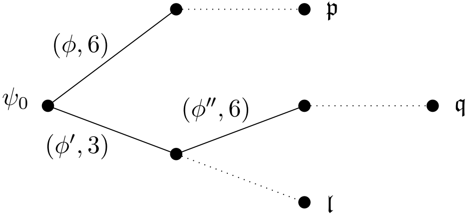
$\lambda_{\mathfrak{p}}^{\mathfrak{q}}$ - hidden slope

MaxMin Example

$$\mathcal{P} = \begin{cases} \mathfrak{p}: & e_1 = 1, f_1 = 4, h_1 = 6; \\ \mathfrak{q}: & e_1 = 1, f_1 = 3, h_1 = 3; \quad e_2 = 1, f_2 = 2, h_2 = 6; \\ \mathfrak{l}: & e_1 = 1, f_1 = 3, h_1 = 3. \end{cases}$$

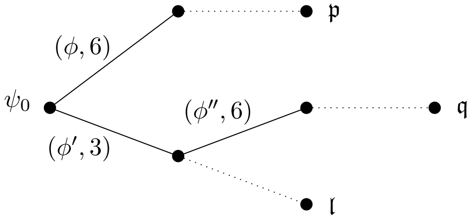
MaxMin Example

$$\mathcal{P} = \begin{cases} \mathfrak{p}: & e_1 = 1, f_1 = 4, h_1 = 6; \\ \mathfrak{q}: & e_1 = 1, f_1 = 3, h_1 = 3; \quad e_2 = 1, f_2 = 2, h_2 = 6; \\ \mathfrak{l}: & e_1 = 1, f_1 = 3, h_1 = 3. \end{cases}$$



MaxMin Example

$$\mathcal{P} = \begin{cases} \mathfrak{p}: & e_1 = 1, f_1 = 4, h_1 = 6; \\ \mathfrak{q}: & e_1 = 1, f_1 = 3, h_1 = 3; \quad e_2 = 1, f_2 = 2, h_2 = 6; \\ \mathfrak{l}: & e_1 = 1, f_1 = 3, h_1 = 3. \end{cases}$$



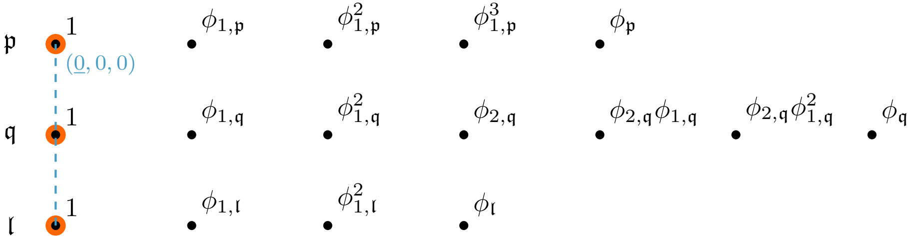
$$\mathcal{N}_{\mathfrak{p}}: \ 1,\ \phi_{1,\mathfrak{p}},\ \phi_{1,\mathfrak{p}}^2,\ \phi_{1,\mathfrak{p}}^3,\ \phi_{\mathfrak{p}};$$
$$\mathcal{N}_{\mathfrak{q}}: \ 1,\ \phi_{1,\mathfrak{q}},\ \phi_{1,\mathfrak{q}}^2,\ \phi_{2,\mathfrak{q}},\ \phi_{2,\mathfrak{q}}\phi_{1,\mathfrak{q}},\ \phi_{2,\mathfrak{q}}\phi_{1,\mathfrak{q}}^2,\ \phi_{\mathfrak{q}};$$
$$\mathcal{N}_{\mathfrak{l}}: \ 1,\ \phi_{1,\mathfrak{l}},\ \phi_{1,\mathfrak{l}}^2,\ \phi_{\mathfrak{l}}.$$

MaxMin Example

$\mathfrak{p}$	1	$\phi_{1,\mathfrak{p}}$	$\phi_{1,\mathfrak{p}}^2$	$\phi_{1,\mathfrak{p}}^3$	$\phi_{\mathfrak{p}}$		
$\mathfrak{q}$	1	$\phi_{1,\mathfrak{q}}$	$\phi_{1,\mathfrak{q}}^2$	$\phi_{2,\mathfrak{q}}$	$\phi_{2,\mathfrak{q}}\phi_{1,\mathfrak{q}}$	$\phi_{2,\mathfrak{q}}\phi_{1,\mathfrak{q}}^2$	$\phi_{\mathfrak{q}}$
$\mathfrak{l}$	1	$\phi_{1,\mathfrak{l}}$	$\phi_{1,\mathfrak{l}}^2$	$\phi_{\mathfrak{l}}$			

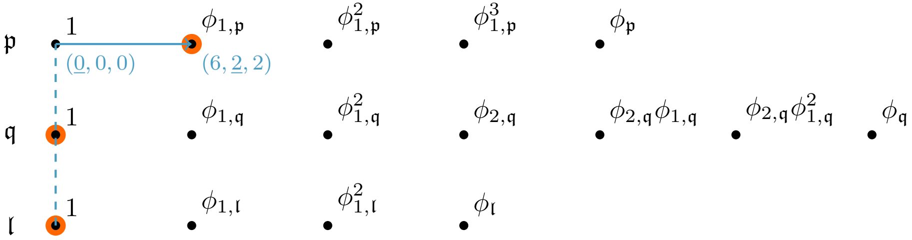
$$\vec{w}\,(\phi_{1,\mathfrak{p}}) = (6,2,2), \qquad \vec{w}\,(\phi_{\mathfrak{p}}) = (\infty,8,8),$$
$$\vec{w}\,(\phi_{1,\mathfrak{q}}) = (2,3,3), \qquad \vec{w}\,(\phi_{2,\mathfrak{q}}) = (6,15,14) \qquad \vec{w}\,(\phi_{\mathfrak{q}}) = (12,\infty,28),$$
$$\vec{w}\,(\phi_{1,\mathfrak{l}}) = (2,3,3), \qquad \vec{w}\,(\phi_{\mathfrak{l}}) = (6,14,\infty).$$

MaxMin Example



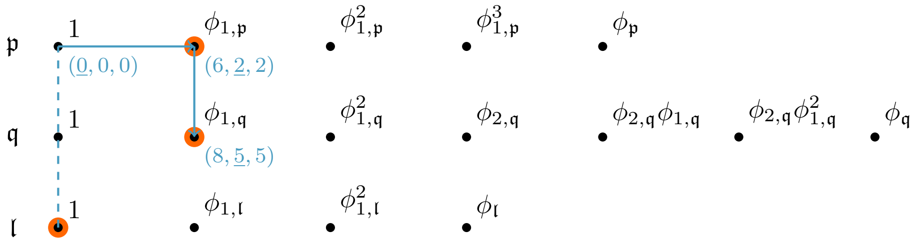
$$\vec{w}\,(\phi_{1,\mathfrak{p}}) = (6, 2, 2), \qquad \vec{w}\,(\phi_{\mathfrak{p}}) = (\infty, 8, 8),$$
$$\vec{w}\,(\phi_{1,\mathfrak{q}}) = (2, 3, 3), \qquad \vec{w}\,(\phi_{2,\mathfrak{q}}) = (6, 15, 14) \qquad \vec{w}\,(\phi_{\mathfrak{q}}) = (12, \infty, 28),$$
$$\vec{w}\,(\phi_{1,\mathfrak{l}}) = (2, 3, 3), \qquad \vec{w}\,(\phi_{\mathfrak{l}}) = (6, 14, \infty).$$

MaxMin Example



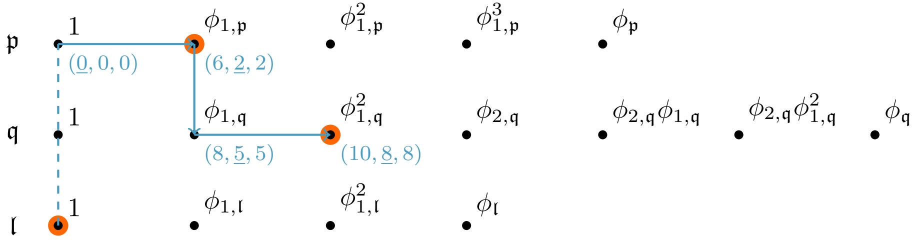
$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2), \qquad \vec{w}(\phi_{\mathfrak{p}}) = (\infty, 8, 8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3), \qquad \vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14) \qquad \vec{w}(\phi_{\mathfrak{q}}) = (12,\infty,28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3), \qquad \vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty).$$

MaxMin Example



$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2), \quad \vec{w}(\phi_{\mathfrak{p}}) = (\infty, 8, 8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3), \quad \vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14) \quad \vec{w}(\phi_{\mathfrak{q}}) = (12, \infty, 28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3), \quad \vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty).$$

MaxMin Example

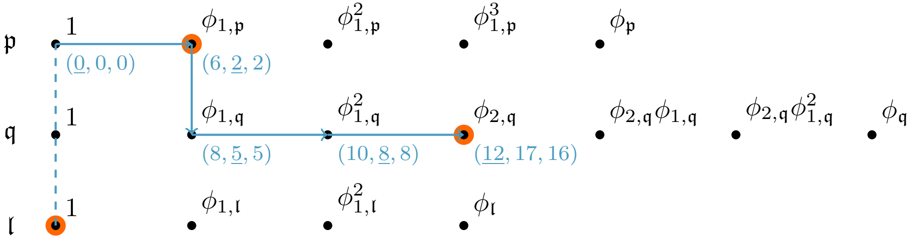


$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2)$, $\vec{w}(\phi_{\mathfrak{p}}) = (\infty,8,8)$,

$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3)$, $\vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14)$ $\vec{w}(\phi_{\mathfrak{q}}) = (12,\infty,28)$,

$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3)$, $\vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty)$.

MaxMin Example

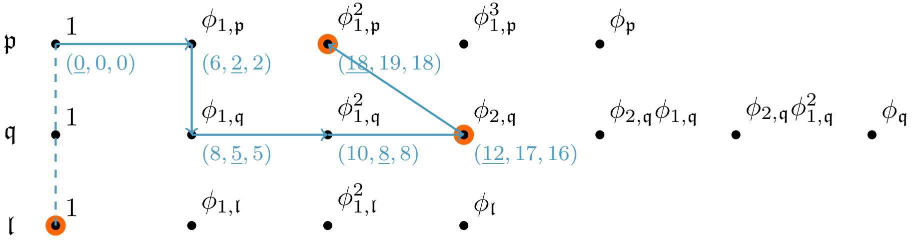


$$\vec{w}\,(\phi_{1,\mathfrak{p}}) = (6, 2, 2), \qquad \vec{w}\,(\phi_{\mathfrak{p}}) = (\infty, 8, 8),$$

$$\vec{w}\,(\phi_{1,\mathfrak{q}}) = (2, 3, 3), \qquad \vec{w}\,(\phi_{2,\mathfrak{q}}) = (6, 15, 14) \qquad \vec{w}\,(\phi_{\mathfrak{q}}) = (12, \infty, 28),$$

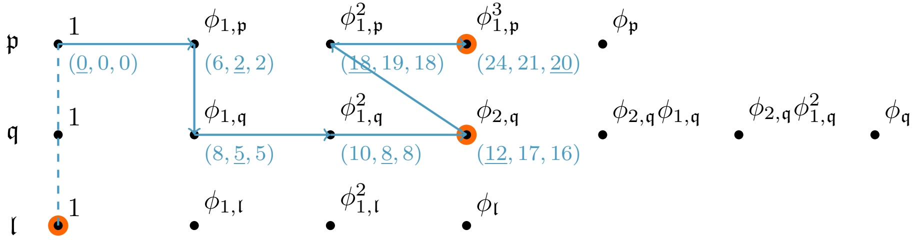
$$\vec{w}\,(\phi_{1,\mathfrak{l}}) = (2, 3, 3), \qquad \vec{w}\,(\phi_{\mathfrak{l}}) = (6, 14, \infty).$$

MaxMin Example



$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6, 2, 2), \quad \vec{w}(\phi_{\mathfrak{p}}) = (\infty, 8, 8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2, 3, 3), \quad \vec{w}(\phi_{2,\mathfrak{q}}) = (6, 15, 14) \quad \vec{w}(\phi_{\mathfrak{q}}) = (12, \infty, 28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2, 3, 3), \quad \vec{w}(\phi_{\mathfrak{l}}) = (6, 14, \infty).$$

MaxMin Example

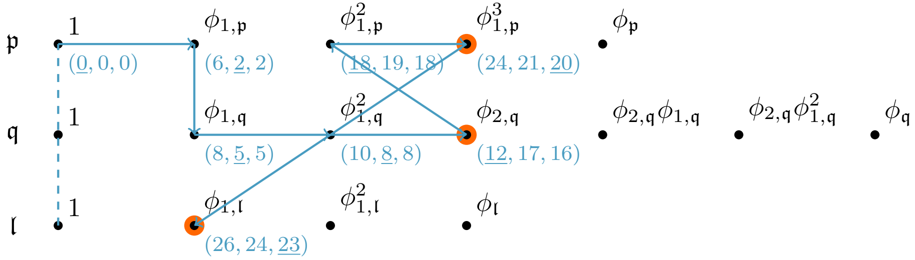


$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2)$, $\vec{w}(\phi_{\mathfrak{p}}) = (\infty,8,8)$,

$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3)$, $\vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14)$ $\vec{w}(\phi_{\mathfrak{q}}) = (12,\infty,28)$,

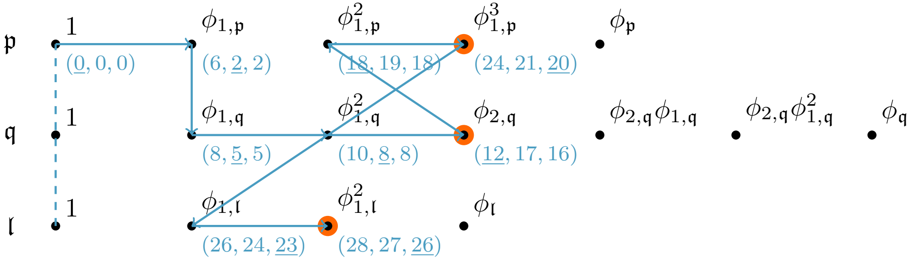
$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3)$, $\vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty)$.

MaxMin Example



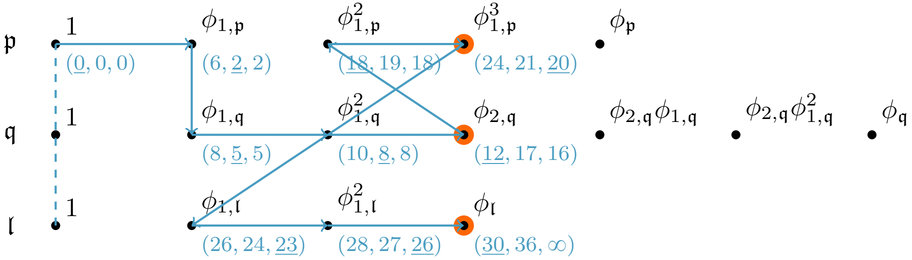
$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6, 2, 2), \qquad \vec{w}(\phi_{\mathfrak{p}}) = (\infty, 8, 8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2, 3, 3), \qquad \vec{w}(\phi_{2,\mathfrak{q}}) = (6, 15, 14) \qquad \vec{w}(\phi_{\mathfrak{q}}) = (12, \infty, 28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2, 3, 3), \qquad \vec{w}(\phi_{\mathfrak{l}}) = (6, 14, \infty).$$

MaxMin Example



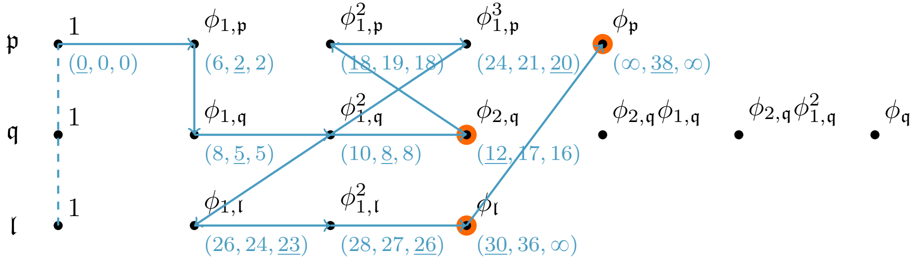
$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2), \qquad \vec{w}(\phi_{\mathfrak{p}}) = (\infty, 8, 8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3), \qquad \vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14) \qquad \vec{w}(\phi_{\mathfrak{q}}) = (12, \infty, 28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3), \qquad \vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty).$$

MaxMin Example



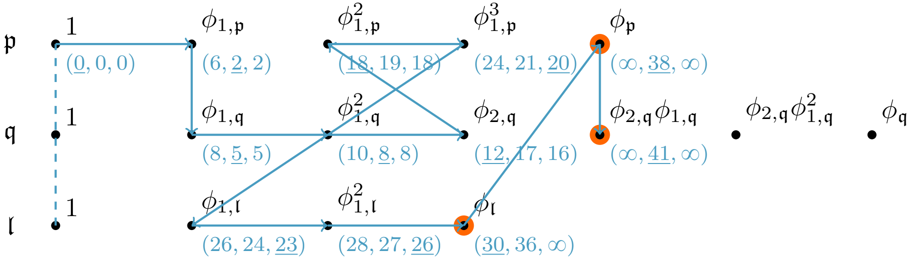
$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2), \qquad \vec{w}(\phi_{\mathfrak{p}}) = (\infty,8,8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3), \qquad \vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14) \qquad \vec{w}(\phi_{\mathfrak{q}}) = (12,\infty,28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3), \qquad \vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty).$$

MaxMin Example



$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2), \qquad \vec{w}(\phi_{\mathfrak{p}}) = (\infty,8,8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3), \qquad \vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14) \qquad \vec{w}(\phi_{\mathfrak{q}}) = (12,\infty,28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3), \qquad \vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty).$$

MaxMin Example

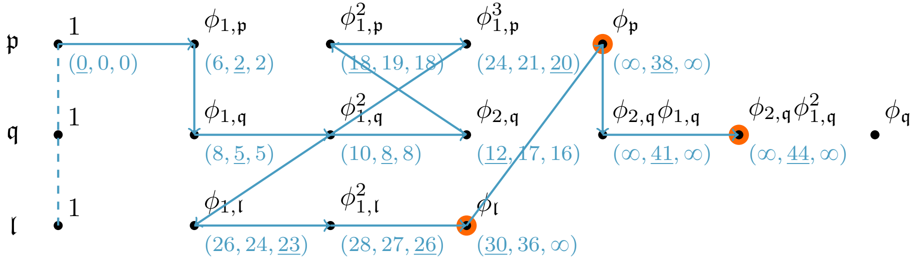


$\vec{w}(\phi_{1,\mathfrak{p}}) = (6, 2, 2)$, $\vec{w}(\phi_{\mathfrak{p}}) = (\infty, 8, 8)$,

$\vec{w}(\phi_{1,\mathfrak{q}}) = (2, 3, 3)$, $\vec{w}(\phi_{2,\mathfrak{q}}) = (6, 15, 14)$ $\vec{w}(\phi_{\mathfrak{q}}) = (12, \infty, 28)$,

$\vec{w}(\phi_{1,\mathfrak{l}}) = (2, 3, 3)$, $\vec{w}(\phi_{\mathfrak{l}}) = (6, 14, \infty)$.

MaxMin Example

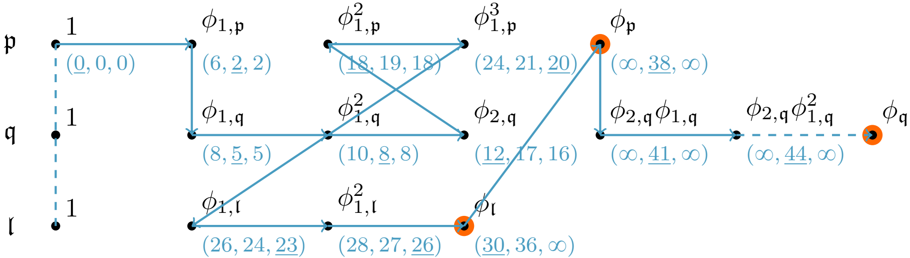


$\vec{w}(\phi_{1,\mathfrak{p}}) = (6, 2, 2)$, $\vec{w}(\phi_{\mathfrak{p}}) = (\infty, 8, 8)$,

$\vec{w}(\phi_{1,\mathfrak{q}}) = (2, 3, 3)$, $\vec{w}(\phi_{2,\mathfrak{q}}) = (6, 15, 14)$ $\vec{w}(\phi_{\mathfrak{q}}) = (12, \infty, 28)$,

$\vec{w}(\phi_{1,\mathfrak{l}}) = (2, 3, 3)$, $\vec{w}(\phi_{\mathfrak{l}}) = (6, 14, \infty)$.

MaxMin Example



$$\vec{w}(\phi_{1,\mathfrak{p}}) = (6,2,2), \qquad \vec{w}(\phi_{\mathfrak{p}}) = (\infty,8,8),$$
$$\vec{w}(\phi_{1,\mathfrak{q}}) = (2,3,3), \qquad \vec{w}(\phi_{2,\mathfrak{q}}) = (6,15,14) \qquad \vec{w}(\phi_{\mathfrak{q}}) = (12,\infty,28),$$
$$\vec{w}(\phi_{1,\mathfrak{l}}) = (2,3,3), \qquad \vec{w}(\phi_{\mathfrak{l}}) = (6,14,\infty).$$

Outline

Example computations

Number fields:

$$f \in \mathbb{Z}[x], \qquad L = \mathbb{Q}[x]/(f)$$

Example computations

Number fields:

$$f \in \mathbb{Z}[x], \qquad L = \mathbb{Q}[x]/(f)$$

Function fields:

$$f \in \mathbb{F}_q[t][x], \qquad L = \mathbb{F}_q(t)[x]/(f)$$

A small example (number fields)

$B_{p,k}(x) = (x^2 - 2x + 4)^3 + p^k$, $\#\mathcal{P} = 6$.

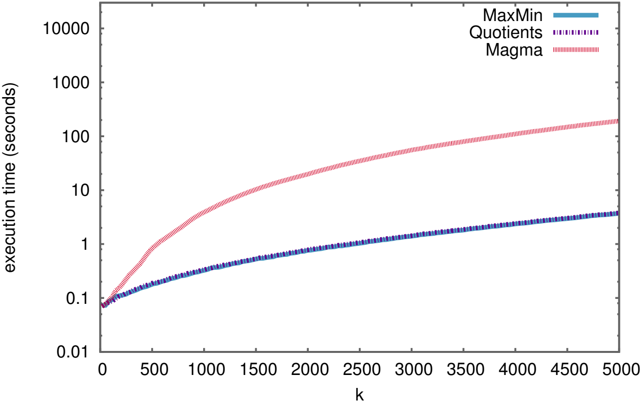
$f(x) = B_{13,k} \in \mathbb{Z}[x]$ with $\deg f = 6$, $L = \mathbb{Q}[x]/(f)$.

A small example (number fields)

$B_{p,k}(x) = (x^2 - 2x + 4)^3 + p^k$, $\#\mathcal{P} = 6$.

$f(x) = B_{13,k} \in \mathbb{Z}[x]$ with $\deg f = 6$, $L = \mathbb{Q}[x]/(f)$.

Times to compute Hermitian p-integral basis of $\mathcal{O}_L$:

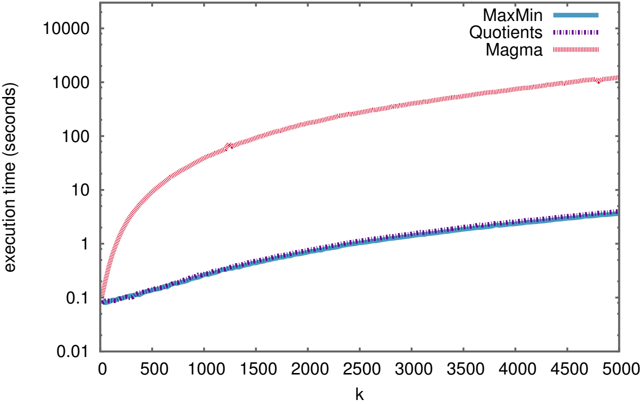


A small example (function fields)

$B_{p,k}(x) = (x^2 - 2x + 4)^3 + p^k$, $\#\mathcal{P} = 6$.

$f(x) = B_{t^3+2,k} \in \mathbb{F}_7[t,x]$ with $\deg f = 6$, $L = \mathbb{F}_7(t)[x]/(f)$.

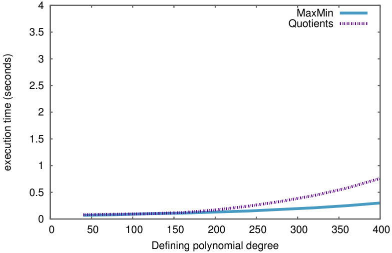
Times to compute Hermitian $p(t)$-integral basis of $\mathcal{O}_L$:



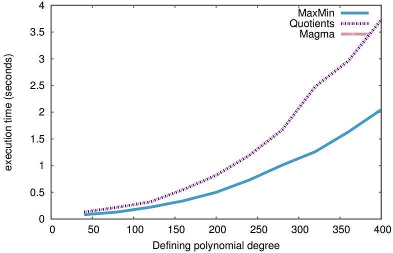
A bigger example (number fields)

$$A^m_{p,n,k}(x) = (x^n + 2p^k)((x+2)^n + 2p^k)\cdots((x+2m-2)^n + 2p^k) + 2p^{mnk}$$

$f(x) = A^4_{101,n,29} \in \mathbb{Z}[x]$ with $\deg f = 4 \cdot n$, $L = \mathbb{Q}[x]/(f)$.



Without HNF



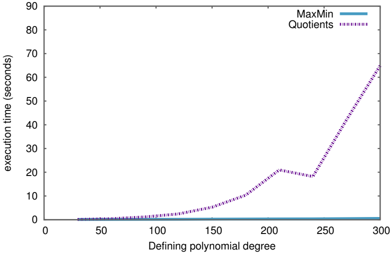
With HNF

Magma takes 257s to complete $\deg f = 40$, and cannot compute $\deg f = 80$ in 3 hours.

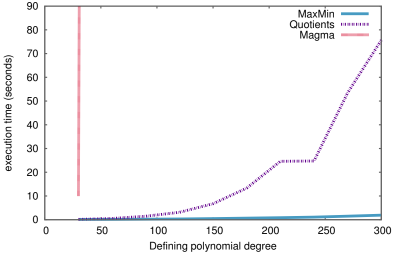
A bigger example (function fields)

$$A^m_{p,n,k}(x) = (x^n + 2p^k)((x+2)^n + 2p^k)\cdots((x+2m-2)^n + 2p^k) + 2p^{mnk}$$

$f(x) = A^3_{t^2+2,n,6} \in \mathbb{F}_7[t,x]$ with $\deg f = 3 \cdot n$, $L = \mathbb{F}_{37}(t)[x]/(f)$.



Without HNF



With HNF

Magma takes 3304s to complete $\deg f = 60$, and computes $\deg f = 90$ in over 6 hours.

A big example

$$
\begin{aligned}
E_{p,1}(x) &= x^2 + p,\\
E_{p,2}(x) &= E_{p,1}(x)^2 + (p-1)p^3x,\\
E_{p,3}(x) &= E_{p,2}(x)^3 + p^{11},\\
E_{p,4}(x) &= E_{p,3}(x)^3 + p^{29}xE_{p,2}(x),\\
E_{p,5}(x) &= E_{p,4}(x)^2 + (p-1)p^{42}xE_{p,1}(x)E_{p,3}(x)^2,\\
E_{p,6}(x) &= E_{p,5}(x)^2 + p^{88}xE_{p,3}(x)E_{p,4}(x),\\
E_{p,7}(x) &= E_{p,6}(x)^3 + p^{295}E_{p,2}(x)E_{p,4}(x)E_{p,5}(x),\\
E_{p,8}(x) &= E_{p,7}(x)^2 + (p-1)p^{632}xE_{p,1}(x)E_{p,2}(x)^2E_{p,3}(x)^2E_{p,6}(x).
\end{aligned}
$$

A big example

$$
\begin{aligned}
E_{p,1}(x) &= x^2 + p,\\
E_{p,2}(x) &= E_{p,1}(x)^2 + (p-1)p^3 x,\\
E_{p,3}(x) &= E_{p,2}(x)^3 + p^{11},\\
E_{p,4}(x) &= E_{p,3}(x)^3 + p^{29} x E_{p,2}(x),\\
E_{p,5}(x) &= E_{p,4}(x)^2 + (p-1)p^{42} x E_{p,1}(x) E_{p,3}(x)^2,\\
E_{p,6}(x) &= E_{p,5}(x)^2 + p^{88} x E_{p,3}(x) E_{p,4}(x),\\
E_{p,7}(x) &= E_{p,6}(x)^3 + p^{295} E_{p,2}(x) E_{p,4}(x) E_{p,5}(x),\\
E_{p,8}(x) &= E_{p,7}(x)^2 + (p-1)p^{632} x E_{p,1}(x) E_{p,2}(x)^2 E_{p,3}(x)^2 E_{p,6}(x).
\end{aligned}
$$

$$C_{p,k}(x) = ((x^6 + 4px^3 + 3p^2x^2 + 4p^2)^2 + p^6)^3 + p^k,$$

A big example

$$
\begin{aligned}
E_{p,1}(x) &= x^2 + p,\\
E_{p,2}(x) &= E_{p,1}(x)^2 + (p-1)p^3 x,\\
E_{p,3}(x) &= E_{p,2}(x)^3 + p^{11},\\
E_{p,4}(x) &= E_{p,3}(x)^3 + p^{29} x E_{p,2}(x),\\
E_{p,5}(x) &= E_{p,4}(x)^2 + (p-1)p^{42} x E_{p,1}(x) E_{p,3}(x)^2,\\
E_{p,6}(x) &= E_{p,5}(x)^2 + p^{88} x E_{p,3}(x) E_{p,4}(x),\\
E_{p,7}(x) &= E_{p,6}(x)^3 + p^{295} E_{p,2}(x) E_{p,4}(x) E_{p,5}(x),\\
E_{p,8}(x) &= E_{p,7}(x)^2 + (p-1)p^{632} x E_{p,1}(x) E_{p,2}(x)^2 E_{p,3}(x)^2 E_{p,6}(x).
\end{aligned}
$$

$$C_{p,k}(x) = ((x^6 + 4px^3 + 3p^2x^2 + 4p^2)^2 + p^6)^3 + p^k,$$

$$EC_{p,j}(x) = E_{p,j}(x) \cdot C_{p,28} + p^{900}.$$

A big example (number fields)

$f(x) = EC_{101,8}(x) \in \mathbb{Z}[x]$ with $\deg f = 900$, $L = \mathbb{Q}[x]/(f)$.

Time to compute a p-integral basis of $\mathcal{O}_L$:

Algorithm	*Basis (s)*	*HNF basis (s)*
MaxMin	9.9	
Quotients	21.1	

A big example (number fields)

$f(x) = EC_{101,8}(x) \in \mathbb{Z}[x]$ with $\deg f = 900$, $L = \mathbb{Q}[x]/(f)$.

Time to compute a p-integral basis of $\mathcal{O}_L$:

Algorithm	*Basis (s)*	*HNF basis (s)*
MaxMin	9.9	112.6
Quotients	21.1	429.3

A big example (number fields)

$f(x) = EC_{101,8}(x) \in \mathbb{Z}[x]$ with $\deg f = 900$, $L = \mathbb{Q}[x]/(f)$.

Time to compute a p-integral basis of $\mathcal{O}_L$:

Algorithm	*Basis (s)*	*HNF basis (s)*
MaxMin	9.9	112.6
Quotients	21.1	429.3

This is with a “fast” HNF routine!

A big example (function fields)

$f(x) = EC_{t^2+4,4}(x) \in \mathbb{F}_7[t,x]$ with $\deg f = 72$, $L = \mathbb{F}_7(t)[x]/(f)$.

Time to compute a $p(t)$-integral basis of $\mathcal{O}_L$:

Algorithm	*Basis (s)*	*HNF basis (s)*
MaxMin	13.3	
Quotients	89.5	

A big example (function fields)

$f(x) = EC_{t^2+4,4}(x) \in \mathbb{F}_7[t,x]$ with $\deg f = 72$, $L = \mathbb{F}_7(t)[x]/(f)$.

Time to compute a $p(t)$-integral basis of $\mathcal{O}_L$:

Algorithm	*Basis (s)*	*HNF basis (s)*
MaxMin	13.3	21.5
Quotients	89.5	8353.8

Thank-you for your attention.