Factoring Polynomials over Local Fields and Single Factor Lifting

Sebastian Pauli

Department of Mathematics and Statistics
University of North Carolina at Greensboro

2012

Table of Contents

History of the Algorithm: Round Four

- Ford (1978): On the Computation of the Maximal Order in a Dedekind Domain
- Cantor, Gordon (2000): Factoring polynomials over p-adic fields
- P. (2001): Factoring polynomials over local fields
- Ford, P., Roblot (2002): A fast algorithm for polynomial factorization over $\mathbb{Q}_p$

History of the Algorithm: Montes

- Ore (1928): Newtonsche Polygone in der Theorie der algebraischen Körper
- MacLane (1936): A Construction for absolute values in polynomial rings
- Montes, Nart (1992): On a theorem of Ore
- Montes (1999): Polígonos de Newton de orden superior y aplicaciones aritméticas
- Guardia, Montes, Nart (since 2008): Newton polygons of higher order in algebraic number theory, . . .

Recent Developments

- Ford, Veres (2009/10): Complexity of Montes algorithm

$$O(N^{3+\varepsilon}\nu(\operatorname{disc}\Phi) + N^{2+\varepsilon}\nu(\operatorname{disc}\Phi)^{2+\varepsilon})$$

- P. (2010): Factoring polynomials over local fields II
- Guardia, Nart, P. (2011): Single factor lifting for polynomials over local fields

Implementations

- Ford (197x) in Algeb: Maximal orders of number fields
- Ford, Letard (1994) in Pari: Maximal orders of number fields
- Baier (1996) in KANT / Magma: Maximal orders of number fields
- Guardia (2000) in Mathematica: Ideal decomposition
- Roblot (2001) in Pari: Polynomial factorization over $\mathbb{Z}_p$
- P. (2001/03) in Magma: Polynomial factorization over local fields
- Guardia, Nart (2009) Ideal+ for Magma: Ideal decomposition
- Sinclair (2012) in Sage: Polynomial factorization over $\mathbb{Z}_p$

Applications

Local Fields

- Integral Basis (splitting extensions into unramified and ramified part)
- Two Element Certificates for Irreducibility
- Splitting Fields

Global Fields

- Prime Decomposition
- Integral Basis
- Completions

Notation

K	field complete with respect to a non-archimedian valuation
$\mathcal{O}_K$	valuation ring of K
π	uniformizing element in $\mathcal{O}_K$
ν	exponential valuation normalized such that $\nu(\pi) = 1$
$\underline{K}$	residue class field $\mathcal{O}_K/(\pi)$ of K with char $\underline{K} = p$
$\Phi(x) \in \mathcal{O}_K[x]$	the polynomial to be factored
$\varphi(x) \in \mathcal{O}_K[x]$	an approximation to an irreducible factor of $\Phi(x)$

Reducibility – Classical

Let $\Phi(x) = \sum_{i=0}^{N} \Phi_i x^i = \prod_{j=1}^{N}(x - \alpha_j) \in \mathcal{O}_K[x]$.

Hensel's Lemma

If there is a factorization of $\Phi(x)$ into coprime factors over the residue class field $\underline{K}$, then there is a factorization of $\Phi(x)$ over $\mathcal{O}_K$.

The lower convex hull of the set of points

$$\{(i, \nu(\Phi_i)) \mid 0 \le i \le N\}$$

is the Newton polygon of $\Phi(x)$.

Let v be a the slope of a segment of length n of the Newton Polygon of $\Phi(x)$ then there are $j_1, \ldots, j_n$ such that $\nu(\alpha_{j_i}) = v$ for $1 \le i \le n$.

Theorem

Each segment of the Newton Polygon of $\Phi(x)$ corresponds to a proper factor of $\Phi(x)$.

Approximations to an Irreducible Factor

Let $\Phi(x) \in \mathcal{O}_K[x]$ be the polynomial to be factored

Let α be a root of $\Phi(x)$. α is a root of an irreducible factor $P(x)$ of $\Phi(x)$.

Construct a sequence of approximations

$$\varphi_1(x) = x, \varphi_2(x), \ldots, \varphi_k(x) \in \mathcal{O}_K[x]$$

to the irreducible factor $P(x)$ such that

$$\nu(\varphi_1(\alpha)) < \nu(\varphi_2(\alpha)) < \cdots < \nu(\varphi_k(\alpha))$$

with

$$\deg(\varphi_1) \mid \deg(\varphi_2) \mid \cdots \mid \deg(\varphi_m) = \deg(P).$$

Approximations to an Irreducible Factor

Let

$$\varphi_1(x) = x, \varphi_2(x), \ldots, \varphi_k(x) \in \mathcal{O}_K[x]$$

be a sequence of approximations to an irreducible factor of $\Phi(x)$.

If $\deg(\varphi_{t+1}) = \deg(\varphi_t)$ then this step is called an improvement step.

If $\deg(\varphi_{t+1}) > \deg(\varphi_t)$ then this step is called a Montes step.

$\varphi_{t+1}(x)$ is a key polynomial (MacLane). Each key polynomial, together with the previous key polynomials yields a valuation on $K[x]$.

Irreducibility – Bound

Theorem

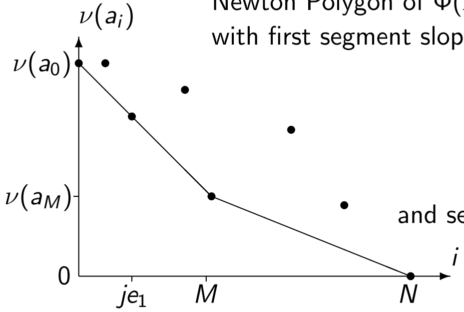
If $\alpha_1, \ldots, \alpha_N$ are elements of an algebraic closure of K,

- $\Phi(x) = \prod_{j=1}^{N}(x - \alpha_j) \in \mathcal{O}_K[x]$ squarefree,
- $\varphi(x) \in \mathcal{O}_K[x]$,
- $N \cdot \nu(\varphi(\alpha_j)) > 2 \cdot \nu(\operatorname{disc} \Phi)$ for all $1 \leq j \leq N$, and
- the degree of any irreducible factor of $\Phi(x)$ is greater than or equal to $\deg \varphi$,

then $N = \deg(\varphi)$ and $\Phi(x)$ is irreducible over K.

1st Iteration – Newton Polygon

Newton Polygon of $\Phi(x) = x^N + \sum_{i=0}^{N-1} a_i x^i$
with first segment slope $-\frac{h_1}{e_1}$, $\gcd(h_1, e_1) = 1$



and second segment slope $-\frac{h_1'}{e_1'}$

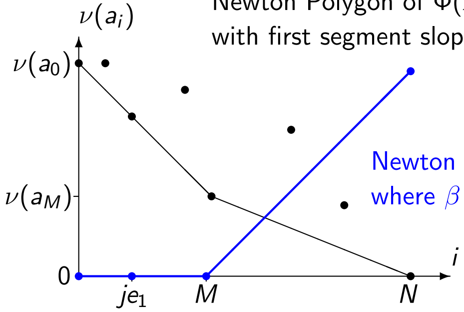
The Newton polygon of $\Phi(x)$ yields the valuations $\nu(\varphi_1(\alpha))$ for $\varphi_1(x) = x$ for the roots α of $\Phi(x)$.

Here (after reordering the roots $\alpha = \alpha_1, \ldots, \alpha_N$ of $\Phi(x)$ if necessary):

$\nu(\alpha_1) = \cdots = \nu(\alpha_M) = \frac{h_1}{e_1}$ and $\nu(\alpha_{M+1}) = \cdots = \nu(\alpha_N) = \frac{h_1'}{e_1'}$.

$E_1 := e_1$ is a divisor of the ramification index of $K(\alpha_i)/K$ $(1 \le i \le M)$.

1st Iteration – Residual Polynomial



Newton Polygon of $\Phi(x) = x^N + \sum_{i=0}^{N-1} a_i x^i$ with first segment slope $-\frac{h_1}{e_1}$, $\gcd(h_1, e_1) = 1$

Newton Polygon of $\Phi^\flat(y) := \Phi(\beta y)/(\beta^M \pi^{\nu(a_M)})$ where $\beta \in \overline{K}$ such that $\beta^{e_1} = \pi^{h_1}$

We have $\Phi^\flat(y) = \Phi(\beta y)/(\beta^M \pi^{\nu(a_M)}) = \sum_{i=0}^{N} a_i \beta^{i-M} \pi^{-\nu(a_M)} y^i$. We set

$$A_1(z) := \sum_{j=0}^{M/e_1} a_{je_1} \pi^{h_1(j-M/e_1)-\nu(a_M)} z^j.$$

$\underline{A}_1(z) \in \underline{K}$ is the *residual polynomial* of $\Phi(x)$ with respect to the first segment.

1st Iteration – The next φ

Let $\underline{A}_1(z)$ be the residual polynomial, so $\nu\left(A_1\left(\frac{\varphi_1^{e_1}(\alpha)}{\pi^{h_1}}\right)\right) > 0$.

$\underline{A}_1(z) = \underline{\rho}_1(z)^{r_1} \cdot \dots \cdot \underline{\rho}_m^{r_m}(z)$ for some irreducible $\underline{\rho}_i(z) \in \underline{K}$ $(1 \leq i \leq m)$.

$F_1 := \deg \underline{\rho}_1$ is a divisor of the inertia degree of $K(\alpha_i)$ for $1 \leq i \leq F_1 \cdot r_1$ (after reordering the roots $\alpha = \alpha_1, \dots, \alpha_M$ of $\Phi(x)$ if necessary).

1st Iteration – The next φ

Let $\underline{A}_1(z)$ be the residual polynomial, so $\nu\left(A_1\left(\frac{\varphi_1^{e_1}(\alpha)}{\pi^{h_1}}\right)\right) > 0$.

$\underline{A}_1(z) = \underline{\rho}_1(z)^{r_1} \cdot \dots \cdot \underline{\rho}_m^{r_m}(z)$ for some irreducible $\underline{\rho}_i(z) \in \underline{K}$ $(1 \le i \le m)$.

$F_1 := \deg \underline{\rho}_1$ is a divisor of the inertia degree of $K(\alpha_i)$ for $1 \le i \le F_1 \cdot r_1$ (after reordering the roots $\alpha = \alpha_1, \dots, \alpha_M$ of $\Phi(x)$ if necessary).

As $\nu\left(\rho_1\left(\frac{(\varphi_1(\alpha_i))^{e_1}}{\pi^{h_1}}\right)\right) > 0$ for a lift $\rho_1(z)$ of $\underline{\rho}_1(z)$ to $\mathcal{O}_K[x]$ we have

$$\nu\left(\pi^{F_1 h_1}\rho_1\left(\frac{(\varphi_1(\alpha_i))^{e_1}}{\pi^{h_1}}\right)\right) > F_1 h_1 \ge \frac{h_1}{e_1} = \nu(\varphi_1(\alpha_i)).$$

Also $\deg\left(\rho_1(\varphi_1^{e_1}/\pi^{h_1})\right) = E_1 F_1 \le N$.

We set $\varphi_2(x) := \pi^{F_1 h_1}\rho_1\left(\frac{(\varphi_1(x))^{e_1}}{\pi^{h_1}}\right)$. $\varphi_2(x)$ is irreducible.

1st Iteration – Data

$\varphi_1(x) = x \in \mathcal{O}_K[x]$	an approximation to an irreducible factor of $\Phi(x)$
h_1/e_1	slope of a segment of the Newton polygon of $\Phi(x)$ with $\gcd(h_1, e_1) = 1$
$E_1 = e_1$	the maximum known ramification index
$\underline{A}_1(z)$	the residual polynomial with respect to φ_1
$\rho_1(z) \in \mathcal{O}_K[z]$	irreducible factor of $\underline{A}_1(z)$ $\underline{K}_1 = \underline{K}[x]/((\underline{\rho}_1))$
$F_1 = [K_1 : K]$	the maximum known inertia degree

1st Iteration

Let $\theta(x) = \sum_{i=0}^{\deg \varphi_2 - 1} b_i x^i$, that is $\deg(\theta) < \deg(\varphi_2) = E_1 \cdot F_1$

As the valuations

$$\nu(\varphi_1(\alpha)) = \nu(\alpha) = \frac{h_1}{e_1}, \ \dots\ , \ \nu(\varphi_1(\alpha)^{e_1 - 1}) = \nu(\alpha^{e_1-1}) = \frac{(e_1 - 1)h_1}{e_1}$$

are distinct (and not in $\mathbb{Z}$) and

$$1, \varphi_1(\alpha)^{e_1}/\pi^{h_1} \equiv \gamma_1 \bmod (\pi), \ \dots\ , \left(\varphi_1(\alpha)^{e_1}/\pi^{h_1}\right)^{F_1 - 1} \equiv \gamma_1^{F_1 - 1} \bmod (\pi)$$

are linearly independent over $\mathcal{O}_K$, we have

$$\nu(\theta(\alpha_1)) = \min_i \nu(b_i) \left(\frac{h_1}{e_1}\right)^i .$$

For $\frac{H}{E_1}$, $H \in \mathbb{Z}$, we can find $\Psi(x) \in K[x]$ such that $\nu(\Psi(\alpha_1)) = \frac{H}{E_1}$.

2nd Iteration – φ_2-expansion

φ_2-expansion of $\Phi(x)$

There are unique $a_i(x) \in \mathcal{O}_K[x]$ with $\deg a_i < \deg \varphi_2 = n_2$ such that

$$\Phi(x) = \sum_{i \geq 0} a_i(x)(\varphi_2(x))^i.$$

For each root α of $\Phi(x)$ we have

$$\Phi(\alpha) = \sum_{i \geq 0} a_i(\alpha)(\varphi_2(\alpha))^i = 0$$

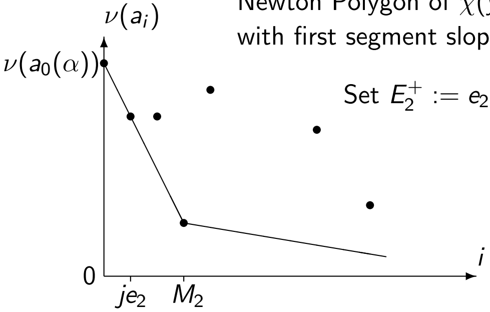
Thus

$$\chi(y) = \sum_{i \geq 0} a_i(\alpha) y^i$$

is a polynomial with root $\varphi_2(\alpha)$.

The Newton Polygon of $\chi(y)$ yields the valuations of $\varphi_2(\alpha)$ for all roots α of $\Phi(x)$ with $\nu(\alpha) = \frac{h_1}{e_1}$.

2nd Iteration – Newton Polygon



Newton Polygon of $\chi(y) = \sum_{i \geq 0} a_i(x) y^i$
with first segment slope $-\frac{h_2}{e_2}$, $\gcd(h_2, e_2) = 1$

Set $E_2^+ := e_2 / \gcd(e_2, E_1)$ and $E_2 := E_1 \cdot E_2^+$

The Newton polygon of $\Phi(x)$ yields the valuations $\nu(\varphi_1(\alpha))$ for $\varphi_1(x) = x$ for the roots α of $\Phi(x)$.

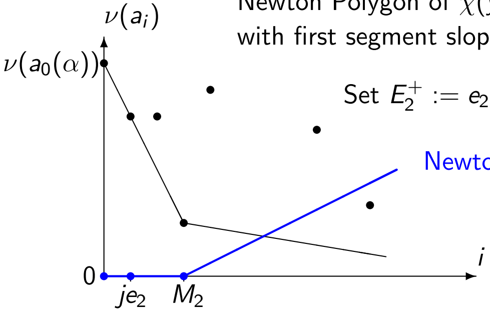
Here (after reordering the roots of $\Phi(x)$ if necessary):
$\nu(\varphi(\alpha_1)) = \cdots = \nu(\varphi(\alpha_{M_2})) = \frac{h_2}{e_2}$

E_2 is a divisor of the ramification index of $K(\alpha_i)/K$.

2nd Iteration – Residual Polynomial

Newton Polygon of $\chi(y) = \sum_{i\geq 0} a_i(x)y^i$
with first segment slope $-\frac{h_2}{e_2}$, $\gcd(h_2, e_2) = 1$

Set $E_2^+ := e_2/\gcd(e_2, E_1)$ and $E_2 := E_1 \cdot E_2^+$



Newton Polygon of $\chi^\flat(y)$

Find $\Pi(x) \in \mathcal{O}_K[x]$ with $\nu(\Pi(\alpha)) = \frac{1}{E_1}$
We set

$$A_2(z) := \sum_{j\geq 0} a_{je_2}(x)\Pi(x)^{h_1(j-M/e_1-e_1\nu(a_{M_2}(\alpha)))}z^j.$$

$\underline{A}_2(z)$ is the *residual polynomial* of $\Phi(x)$ with respect to the first segment.

2nd Iteration – The next $\varphi(x)$

Let $\psi_2(x) \in \mathcal{O}_K[x]$ with $\nu(\psi_2(\alpha)) = \frac{E_2^+ h_2}{e_2}$. From

$$\varphi_3^*(x) := \psi_2(x)^{F_1^+} \rho_2\left(\frac{\varphi_2(x)^{E_2^+}}{\psi_2(x)}\right) = \sum_{i=0}^{F_2^+} \sum_{j=0}^{F_1-1} r_{i,j}\left(\frac{x^{e_1}}{\pi^{h_1}}\right)^j \psi_2(x)^{F_2^+-i} \varphi_2(x)^{iE_2^+}$$

we construct $\varphi_3(x) \in \mathcal{O}_K[x]$ such that

- $\nu(\varphi_3^*(\alpha) - \varphi_3(\alpha) > \nu(\varphi_3^*(\alpha))$ and
- $\deg \varphi_3 = E_2 F_2 = E_2^+ F_2^+ E_1 F_1$.

using that

- $r_{i,j}$ is congruent to a linear combination of $\varphi_1^{e_1}/\pi^{h_1}$,
- $\nu(\rho_1((\varphi_1(\alpha)^{e_1}/\pi^{h_1})) > 0$, and $\deg(\rho_1(\varphi_1^{e_1}/\pi^{h_1})) = E_1 F_1$

2nd Iteration – The next $\varphi(x)$

Let $\psi_2(x) \in \mathcal{O}_K[x]$ with $\nu(\psi_2(\alpha)) = \frac{E_2^+ h_2}{e_2}$. From

$$\varphi_3^*(x) := \psi_2(x)^{F_1^+} \rho_2\left(\frac{\varphi_2(x)^{E_2^+}}{\psi_2(x)}\right) = \sum_{i=0}^{F_2^+} \sum_{j=0}^{F_1-1} r_{i,j}\left(\frac{x^{e_1}}{\pi^{h_1}}\right)^j \psi_2(x)^{F_2^+ - i} \varphi_2(x)^{iE_2^+}$$

we construct $\varphi_3(x) \in \mathcal{O}_K[x]$ such that

- $\nu(\varphi_3^*(\alpha) - \varphi_3(\alpha) > \nu(\varphi_3^*(\alpha))$ and
- $\deg \varphi_3 = E_2 F_2 = E_2^+ F_2^+ E_1 F_1$.

using that

- $r_{i,j}$ is congruent to a linear combination of $\varphi_1^{e_1}/\pi^{h_1}$,
- $\nu(\rho_1((\varphi_1(\alpha)^{e_1}/\pi^{h_1})) > 0$, and $\deg(\rho_1(\varphi_1^{e_1}/\pi^{h_1})) = E_1 F_1$

Remark

$\varphi_3(x)$ is irreducible.

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$

  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$

  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.
  4. $h_t/e_t \leftarrow v_\Phi^*(\varphi_t)$, $E_t^+ = \frac{e_t}{\gcd(e_t, E_{t-1})}$, $E_t \leftarrow E_{t-1} \cdot E_t^+$.

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$

  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.
  4. $h_t/e_t \leftarrow v_\Phi^*(\varphi_t)$, $E_t^+ = \frac{e_t}{\gcd(e_t, E_{t-1})}$, $E_t \leftarrow E_{t-1} \cdot E_t^+$.
  5. Find the residual polynomial $\underline{A}_t(y)$ of $\Phi(x)$ with respect to $\varphi_t(x)$.

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$

  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.
  4. $h_t/e_t \leftarrow v_\Phi^*(\varphi_t)$, $E_t^+ = \frac{e_t}{\gcd(e_t, E_{t-1})}$, $E_t \leftarrow E_{t-1} \cdot E_t^+$.
  5. Find the residual polynomial $\underline{A}_t(y)$ of $\Phi(x)$ with respect to $\varphi_t(x)$.
  6. Choose an irreducible factor $\underline{\rho}_t(y) \in \underline{K}_{t-1}$ of $\underline{A}_t(y)$.

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$

  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.
  4. $h_t/e_t \leftarrow v_\Phi^*(\varphi_t)$, $E_t^+ = \frac{e_t}{\gcd(e_t, E_{t-1})}$, $E_t \leftarrow E_{t-1} \cdot E_t^+$.
  5. Find the residual polynomial $\underline{A}_t(y)$ of $\Phi(x)$ with respect to $\varphi_t(x)$.
  6. Choose an irreducible factor $\underline{\rho}_t(y) \in \underline{K}_{t-1}$ of $\underline{A}_t(y)$.
  7. $F_t^+ \leftarrow \deg \underline{\rho}_t(y)$, $F_t \leftarrow F_{t-1} \cdot F_t^+$, $\underline{K}_t \leftarrow \underline{K}_{t-1}[x]/(\underline{\rho}_t)$.

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$

  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.
  4. $h_t/e_t \leftarrow v_\Phi^*(\varphi_t)$, $E_t^+ = \frac{e_t}{\gcd(e_t, E_{t-1})}$, $E_t \leftarrow E_{t-1} \cdot E_t^+$.
  5. Find the residual polynomial $\underline{A}_t(y)$ of $\Phi(x)$ with respect to $\varphi_t(x)$.
  6. Choose an irreducible factor $\underline{\rho}_t(y) \in \underline{K}_{t-1}$ of $\underline{A}_t(y)$.
  7. $F_t^+ \leftarrow \deg \underline{\rho}_t(y)$, $F_t \leftarrow F_{t-1} \cdot F_t^+$, $\underline{K}_t \leftarrow \underline{K}_{t-1}[x]/(\underline{\rho}_t)$.
  8. Find $\varphi_{t+1}(x) \in \mathcal{O}_K[x]$ with $\nu(\varphi_{t+1}(\alpha)) > \nu(\varphi_t(\alpha))$, $\deg \varphi_{t+1} = E_t F_t$.

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$
  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.
  4. $h_t/e_t \leftarrow v_\Phi^*(\varphi_t)$, $E_t^+ = \frac{e_t}{\gcd(e_t, E_{t-1})}$, $E_t \leftarrow E_{t-1} \cdot E_t^+$.
  5. Find the residual polynomial $\underline{A}_t(y)$ of $\Phi(x)$ with respect to $\varphi_t(x)$.
  6. Choose an irreducible factor $\underline{\rho}_t(y) \in \underline{K}_{t-1}$ of $\underline{A}_t(y)$.
  7. $F_t^+ \leftarrow \deg \underline{\rho}_t(y)$, $F_t \leftarrow F_{t-1} \cdot F_t^+$, $\underline{K}_t \leftarrow \underline{K}_{t-1}[x]/(\underline{\rho}_t)$.
  8. Find $\varphi_{t+1}(x) \in \mathcal{O}_K[x]$ with $\nu(\varphi_{t+1}(\alpha)) > \nu(\varphi_t(\alpha))$, $\deg \varphi_{t+1} = E_t F_t$.
  9. $t \leftarrow t + 1$

Algorithm

Input: a monic, separable, squarefree polynomial $\Phi(x) \in \mathcal{O}_K[x]$
Output: an irreducible factor of $\Phi(x)$

- $t \leftarrow 1$, $\varphi_1 \leftarrow x$, $E_0 \leftarrow 1$, $F_0 \leftarrow 1$, $\underline{K}_0 \leftarrow \underline{K}$.
- Repeat:
  1. Find the Newton Polygon for $\varphi_t(x)$
  2. If the length of the first segment is one, lift the factor $\varphi_t(x)$
  3. Choose a segment of the Newton Polygon, let h_t/e_t be its slope.
  4. $h_t/e_t \leftarrow v_\Phi^*(\varphi_t)$, $E_t^+ = \frac{e_t}{\gcd(e_t, E_{t-1})}$, $E_t \leftarrow E_{t-1} \cdot E_t^+$.
  5. Find the residual polynomial $\underline{A}_t(y)$ of $\Phi(x)$ with respect to $\varphi_t(x)$.
  6. Choose an irreducible factor $\underline{\rho}_t(y) \in \underline{K}_{t-1}$ of $\underline{A}_t(y)$.
  7. $F_t^+ \leftarrow \deg \underline{\rho}_t(y)$, $F_t \leftarrow F_{t-1} \cdot F_t^+$, $\underline{K}_t \leftarrow \underline{K}_{t-1}[x]/(\underline{\rho}_t)$.
  8. Find $\varphi_{t+1}(x) \in \mathcal{O}_K[x]$ with $\nu(\varphi_{t+1}(\alpha)) > \nu(\varphi_t(\alpha))$, $\deg \varphi_{t+1} = E_t F_t$.
  9. $t \leftarrow t + 1$

$(t-1)$-st Iteration – Data

$\varphi_{t-1}(x) \in \mathcal{O}_K[x]$	an approximation to an irreducible factor of $\Phi(x)$ with $\deg \varphi_{t-1} = E_{t-2}F_{t-2}$
h_{t-1}/e_{t-1}	a slope of the Newton Polygon for φ_{t-1}
$E_{t-1}^{+} = \frac{e_{t-1}}{\gcd(E_{t-2}, e_{t-1})}$	the increase of known ramification index
$E_{t-1} = E_{t-2} \cdot E_{t-1}^{+}$	the maximal known ramification index
$\psi_{t-1} = \pi^{s_\pi} \prod_{i=1}^{t-2} \varphi_i^{s_i}$	where $s_\pi \in \mathbb{Z}$ and $0 \leq s_i < E_i^{+}$ with $v_\Phi^*(\psi) = E_{t-1}^{+} h_{t-1}/e_{t-1}$
$\underline{A}_{t-1}(z)$	the residual polynomial with respect to φ_{t-1}
$\underline{\rho}_{t-1}(z) \in \underline{K}[z]$	an irreducible factor of $\underline{A}_{t-1}(z)$
$\underline{K}_{t-1} = \underline{K}_{t-2}[x]/((\underline{(}\rho_{t-1})$	
$F_{t-1} = \mathrm{lcm}(F_{t-2}, [\underline{K}_{t-1} : \underline{K}])$	the maximum known inertia degree

t-th Iteration – the $(\varphi_1, \ldots, \varphi_{t-1})$-expansion

We compute the $\varphi_t(x)$-expansion of $\Phi(x)$ in order to find $v^*_\Phi(\varphi_t)$.

The $(\varphi_1, \ldots, \varphi_{t-1})$-expansion of the coefficients of the expansion yields the necessary information.

Let $a(x) \in \mathcal{O}_K[x]$ with $\deg a < E_{t-1}F_{t-1}$.

$(\varphi_1, \ldots, \varphi_{t-1})$-expansion of $a(x)$

$$a(x) = \sum_{j_{t-1}=0}^{E^+_{t-1}F^+_{t-1}-1} \varphi_{t-1}^{j_{t-1}}(x) \quad \cdots \sum_{j_{t-2}=0}^{E^+_{t-2}F^+_{t-2}-1} \varphi_2^{j_2}(x) \sum_{j_1=0}^{E^+_1F^+_1-1} x^{j_1} \cdot a_{j_1,\ldots,j_{t-1}}$$

Lemma

$$\nu(a(\alpha)) = \min_{\substack{1\le i\le t-1\\ 1\le j_i<E^+_i}} \nu\left(\varphi_{t-1}^{j_{t-1}}(\alpha)\cdots\varphi_2^{j_2}(\alpha)\cdot x^{j_1}\cdot a_{j_1,\ldots,j_{t-1}}\right)$$

Example: Factorization of $\Phi = x^{16} + 16 \in \mathbb{Q}_2[x]$

1st Iteration $\varphi_1 = x$

$\chi_1 = \Phi = y^{16} + 16$, thus $h_1/e_1 = 1/4$, $E_1^+ = 4$ and $E_1 = 4$.
Residual polynomial: $\underline{A}_1 = z^4 + 1 = (z+1)^4 \in \mathbb{F}_2[z]$, hence $F_1 = 1$.
$\psi_1 = 2$, such that $\nu(\psi_1) = \nu(\varphi_1^{E_1^+})$ and $\deg(\psi_1) < E_1 F_1$

Example: Factorization of $\Phi = x^{16} + 16 \in \mathbb{Q}_2[x]$

1st Iteration $\varphi_1 = x$

$\chi_1 = \Phi = y^{16} + 16$, thus $h_1/e_1 = 1/4$, $E_1^+ = 4$ and $E_1 = 4$.
Residual polynomial: $\underline{A}_1 = z^4 + 1 = (z+1)^4 \in \mathbb{F}_2[z]$, hence $F_1 = 1$.
$\psi_1 = 2$, such that $\nu(\psi_1) = \nu(\varphi_1^{E_1^+})$ and $\deg(\psi_1) < E_1 F_1$

2nd Iteration $\varphi_2 = \varphi_1^{e_1} - \psi_1 = x^4 - 2$

$\Phi = 32 + \varphi_2(32 + \varphi_2(24 + \varphi_2(8 + \varphi_2)))$
$\chi_2 = y^4 + 8y^3 + 24y^2 + 32y + 32$, thus $h_2/e_2 = 5/4$, $E_2^+ = 1$ and $E_2 = 4$.
Residual polynomial: $\underline{A}_2 = z^4 + 1 = (z+1)^4 \in \mathbb{F}_2[z]$, hence $F_2 = 1$.
$\psi_2 = 2\varphi_1$, such that $\nu(\psi_2^{E_2^+}) = \nu(\varphi_1)$ and $\deg(\psi_2) < E_2 F_2$

Example: Factorization of $\Phi = x^{16} + 16 \in \mathbb{Q}_2[x]$

1st Iteration $\varphi_1 = x$

$\chi_1 = \Phi = y^{16} + 16$, thus $h_1/e_1 = 1/4$, $E_1^+ = 4$ and $E_1 = 4$.
Residual polynomial: $\underline{A}_1 = z^4 + 1 = (z+1)^4 \in \mathbb{F}_2[z]$, hence $F_1 = 1$.
$\psi_1 = 2$, such that $\nu(\psi_1) = \nu(\varphi_1^{E_1^+})$ and $\deg(\psi_1) < E_1 F_1$

2nd Iteration $\varphi_2 = \varphi_1^{e_1} - \psi_1 = x^4 - 2$

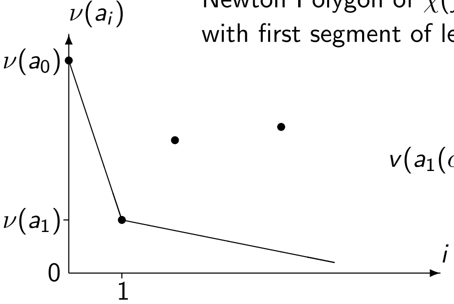
$\Phi = 32 + \varphi_2(32 + \varphi_2(24 + \varphi_2(8 + \varphi_2)))$
$\chi_2 = y^4 + 8y^3 + 24y^2 + 32y + 32$, thus $h_2/e_2 = 5/4$, $E_2^+ = 1$ and $E_2 = 4$.
Residual polynomial: $\underline{A}_2 = z^4 + 1 = (z+1)^4 \in \mathbb{F}_2[z]$, hence $F_2 = 1$.
$\psi_2 = 2\varphi_1$, such that $\nu(\psi_2^{E_2^+}) = \nu(\varphi_1)$ and $\deg(\psi_2) < E_2 F_2$

3rd Iteration $\varphi_3 = \varphi_2 - 2\varphi_1(x) = x^4 - 2x + 2$

$\Phi = -64x^3 + 96x^2 - 32x + \varphi_3(32x^3 - 96x^2 + 96x - 16 + \varphi_3(24x^2 - 48x + 24 + \varphi_3(8x - 8 + \varphi_3)))$.
$\chi_3 = -64x^3 + 96x^2 - 32x + (32x^3 - 96x^2 + 96x - 16)y + (24x^2 - 48x + 24)y^2 + (8x - 8)y^3 + y^4$.
The valuations of the coefficients are $21/4$, 4, 3, 3 and 0, hence $h_3/e_3 = 21/16$.

Good Approximations

Consider the φ_t-expanson of $\Phi(x) = \sum_{i\geq 0} a_i(x)\varphi_t^i(x)$. If the first segment of the newton polygon has length one $\varphi_t(x)$ is an approximation to a unique factor of degree $\deg(\varphi_t)$. $\varphi_t(x)$ is called a good approximation.



Newton Polygon of $\chi(y) = \sum_{i\geq 0} a_i(x)y^i$
with first segment of length 1 and slope $\nu\left(\varphi_t(\alpha)\right)$

$v(a_1(\alpha)\varphi(\alpha)) < v(a_i(\alpha)\varphi_t(\alpha)^i)$ for $2 \leq i$

We have $0 = \Phi(\alpha) = \sum_{i\geq 0} a_i(\alpha)\varphi_t^i(\alpha)$, so $a_1(\alpha)\varphi_t(\alpha) + a_0(\alpha) = -\sum_{i\geq 2} a_i(\alpha)\varphi_t^i(\alpha)$.

$$\nu\left(\varphi_t(\alpha) + \frac{a_0(\alpha)}{a_1(\alpha)}\right) = \nu\left(\frac{\sum_{i\geq 2} a_i(\alpha)\varphi_t^i(\alpha)}{a_1(\alpha)}\right).$$

Single Factor Lifting Idea

Assume the first segment of the newton polygon for $\varphi_t(x)$ has length one, then $\varphi_t(x)$ is an approximation to a unique factor $P(x)$ of $\Phi(x)$.

We have

$$\varphi_t(\alpha) + \frac{a_0(\alpha)}{a_1(\alpha)} = -\frac{\sum_{2\leq s} a_s(\alpha)\varphi_t(\alpha)^s}{a_1(\alpha)}.$$

Now

$$v\left(\varphi_t(\alpha) + \frac{a_0(\alpha)}{a_1(\alpha)}\right) = v\left(\frac{\sum_{2\leq s} a_s(\alpha)\varphi_t(\alpha)^s}{a_1(\alpha)}\right) > v\left(\varphi_t(\alpha)\right).$$

Find $a_1^{-1}(x) \in K[x]$ with $a_1(x)a_1^{-1}(x) \equiv 1 \mod \varphi_t(x)$.
For $\varphi^*(x) := \varphi_t(x) + A(x)$ where $A(x) \equiv a_0(x)a_1^{-1}(x) \mod \varphi_t(x)$, with $\deg A < \deg \varphi_t$, we get

$$v(\varphi^*(\alpha)) = v(\varphi_t(\alpha) + A(\alpha)) > v(\varphi_t(\alpha))$$

So $\varphi^*(x)$ is a better approximation to the irreducible factor $P(x)$.

Single Factor Lifting Convergence

Theorem

Let φ_t be a good approximation to an irreducible factor $P(x)$ of $\Phi(x)$ and let α be a root of $P(x)$. Let $\Phi(x) = \sum_{i \geq 0} a_i(x)\varphi_t^i(x)$ nbe the φ_t-expansion of $\Phi(x)$. Let $a_1^{-1}(x) \in K[x]$ with $a_1(x)a_1^{-1}(x) \equiv 1 \mod \varphi_t(x)$ and $A(x) \in \mathcal{O}_K[x]$ with $A(x) \equiv a_0(x)a_1^{-1}(x) \mod \varphi_t(x)$ Then

$$v(\varphi_t(\alpha) + A(\alpha)) \geq 2v(\varphi_t(\alpha)).$$

Single Factor Lifting Algorithm

Input: a good approximation $\varphi(x)$ to an irreducible factor $P(x)$ of $\Phi(x)$
Output: a lift of $\varphi(x)$ to a given precision $\nu \in \mathbb{N}$

(1) $a, a_0 \leftarrow \mathrm{quotrem}(f, \varphi)$, $a_1 \leftarrow a \bmod \varphi$

(2) $h_\varphi \leftarrow w(a_0) - w(a_1\varphi)$

(3) Find $\Psi \in K[x]$ with $\deg \Psi < \deg \varphi$ and $v(\Psi(\alpha)) = -v(a_1(\alpha))$

(4) $A_0 \leftarrow \Psi a_0 \bmod \varphi$, $A_1 \leftarrow \Psi a_1 \bmod \varphi$

(5) Find $A_1^{-1} \in K[x]$ with $v\left((A_1^{-1}A_1 \bmod \varphi(\alpha)) - 1\right) > 0$

(6) $s \leftarrow 1$

(7) while $s < h_\varphi$: **(Newton inversion)**

  (a) $A_1^{-1} \leftarrow A_1^{-1}(2 - A_1 A_1^{-1}) \bmod \varphi$
  (b) $s \leftarrow 2s$

(8) $A \leftarrow A_0 A_1^{-1} \bmod \varphi$, $\Phi \leftarrow \varphi + A$, $C_1^{-1} \leftarrow A_1^{-1}$

(9) $h \leftarrow 2h_\varphi$

Single Factor Lifting Algorithm

(10) while $h < e(\nu - \nu_0)$: **(The main loop)**

  (a) $c, c_0 \leftarrow \text{quotrem}(f, \Phi)$, $c_1 \leftarrow c \bmod \Phi$
  (b) $C_0 \leftarrow \Psi c_0 \bmod \Phi$, $C_1 \leftarrow \Psi c_1 \bmod \Phi$
  (c) $C_1^{-1} \leftarrow C_1^{-1}(2 - C_1 C_1^{-1}) \bmod \Phi$
  (d) $C \leftarrow C_0 C_1^{-1} \bmod \Phi$
  (e) $\Phi \leftarrow \Phi + C$
  (f) $h \leftarrow 2h$

(11) return Φ

where $\nu_0 := \frac{h_1}{e_1} + \frac{h_2}{e_1 e_2} + \cdots + \frac{h_r}{e_1 \cdots e_r}$

Applications

Assume that the first segment of the Newton Polygon for $\varphi_t(x)$ has length one. Let α be a root of $\Phi(x)$ that corresponds to this segment.

Uniformizers

There are $s_\pi \in \mathbb{Z}$ and $s_1, \ldots, s_t \in \mathbb{N}$ with $0 \leq s_i \leq E_i^+$ such that $\nu(\Pi(\alpha)) = \frac{1}{E_t}$ for

$$\Pi(x) = \pi^{s_\pi} \varphi_1(x)^{s_1} \cdot \cdots \cdot \varphi_t^{s_t} \in K[x].$$

Splitting Extensions into Unramified and Ramified Part

Let L/K be unramified of degree F_t and $g(y)$ be factor of

$$\chi_\Pi(y) = \mathrm{res}_x(\Phi(x), y - \Pi(x))$$

over L. Then

$$K(\alpha) \cong L(\Pi(\alpha)) \cong L[y]/(g(y))$$

where $L[y]/(g(y))$ over L is totally ramified of degree E_t.

Applications

Assume that the first segment of the Newton Polygon for $\varphi_t(x)$ has length one. Let α be a root of $\Phi(x)$ that corresponds to this segment and let $P(x) \in \mathcal{O}_K[x]$ be the corresponding irreducible factor of $\Phi(x)$.

Two Element Certificates

There are $r_\pi \in \mathbb{Z}$ and $r_1, \ldots, r_t \in \mathbb{N}$ with $0 \leq r_i \leq E_i^+ F_i^+$ such that $[\underline{K}(\underline{\Gamma(\alpha)}) : \underline{K}] = F_t$ for

$$\Gamma(x) = \pi^{r_\pi} \varphi_1(x)^{r_1} \cdot \cdots \cdot \varphi_t^{r_t} \in K[x].$$

$\Gamma(x)$ and $\Pi(x)$ with $[\underline{K}(\underline{\Gamma(\alpha)}) : \underline{K}] = F_t$ and $\nu(\Pi(\alpha)) = \frac{1}{E_t}$ are a certificate for the irreducibility of $P(x)$ with $\deg(P) = E_t \cdot F_t$.

Integral Basis

$$\left\{ \Gamma(\alpha)^i \Pi(\alpha)^j \mid 0 \leq i < F_\Gamma, 0 \leq j < E_\Pi \right\}$$

is an integral basis of $K(\alpha)$.