Computing low-degree factors of lacunary polynomials: a Newton-Puiseux Approach

Bruno Grenet

LIX — École Polytechnique

MAP 2014 – May 30., 2014 – IHP, Paris

Factorization of a polynomial f

Find $f_1, \ldots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

Factorization of a polynomial f

Find $f_1, \dots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\dots$;
  - in 1, 2, $\dots$, n variables.

Factorization of a polynomial f

Find $f_1, \dots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\dots$;
  - in 1, 2, $\dots$, n variables.
- Complexity: **polynomial in** $\deg(f)$

Factorization of a polynomial f

Find $f_1, \dots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, …;
  - in 1, 2, …, n variables.
- Complexity: **polynomial in** $\deg(f)$

$$X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1$$

Factorization of a polynomial f

Find $f_1, \ldots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\ldots$;
  - in 1, 2, $\ldots$, n variables.
- Complexity: **polynomial in** $\deg(f)$

$$X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1$$
$$= (X + Y - 1) \times (X^{101}Y^{101} - 1)$$

Factorization of a polynomial f

Find $f_1, \ldots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\ldots$;
  - in 1, 2, $\ldots$, n variables.
- Complexity: **polynomial in $\deg(f)$**

$$\begin{aligned} X^{102}Y^{101} &+ X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ &= (X+Y-1) \times (X^{101}Y^{101} - 1) \\ &= (X+Y-1) \times (XY-1) \times (1 + XY + \cdots + X^{100}Y^{100}) \end{aligned}$$

Definition

$$f(X_1, \ldots, X_n) = \sum_{j=1}^{k} c_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}$$

- $\text{size}(f) \simeq k\Big(\max_j(\text{size}(c_j)) + n \log(\deg f)\Big)$

Definition

$$f(X_1, \ldots, X_n) = \sum_{j=1}^{k} c_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}$$

- $\mathsf{size}(f) \simeq k\Big(\max_j(\mathsf{size}(c_j)) + n\log(\deg f)\Big)$

Compute the degree-d factors of f in time $\mathsf{poly}(\mathsf{size}(f), d)$

Definition

$$f(X_1,\dots,X_n)=\sum_{j=1}^{k} c_j X_1^{\alpha_{1j}}\cdots X_n^{\alpha_{nj}}$$

- $\text{size}(f)\simeq k\Big(\max_j(\text{size}(c_j))+n\log(\deg f)\Big)$

Compute the degree-d factors of f in time $\text{poly}(\text{size}(f),d)$

Let $f\in\mathbb{R}[X]$ with k nonzero terms. Then $\#Z_{\mathbb{R}}(f)\leqslant 2k-1$.

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors (integer roots) of $f \in \mathbb{Z}[X]$; **[Cucker-Koiran-Smale'98]**

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors (integer roots) of $f \in \mathbb{Z}[X]$; **[Cucker-Koiran-Smale'98]**
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X]$; **[H. Lenstra'99]**

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors (integer roots) of $f \in \mathbb{Z}[X]$; **[Cucker-Koiran-Smale'98]**
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X]$; **[H. Lenstra'99]**
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X_1, \ldots, X_n]$. **[Kaltofen-Koiran'06]**

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors (integer roots) of $f \in \mathbb{Z}[X]$; [Cucker-Koiran-Smale'98]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X]$; [H. Lenstra'99]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X_1, \dots, X_n]$. [Kaltofen-Koiran'06]

It is **NP-hard** to compute **roots of** $f \in \mathbb{F}_p[X]$. [Bi-Cheng-Rojas'13]

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors (integer roots) of $f \in \mathbb{Z}[X]$; [Cucker-Koiran-Smale'98]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X]$; [H. Lenstra'99]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X_1, \ldots, X_n]$. [Kaltofen-Koiran'06]

It is NP-**hard** to compute **roots of** $f \in \mathbb{F}_p[X]$. [Bi-Cheng-Rojas'13]

- Only available for number fields

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors (integer roots) of $f \in \mathbb{Z}[X]$; **[Cucker-Koiran-Smale'98]**
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X]$; **[H. Lenstra'99]**
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X_1, \ldots, X_n]$. **[Kaltofen-Koiran'06]**

It is NP-**hard** to compute **roots of** $f \in \mathbb{F}_p[X]$. **[Bi-Cheng-Rojas'13]**

- Only available for number fields
- Based on number-theoretic results $\rightsquigarrow$ theoretical algorithms

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors (integer roots) of $f \in \mathbb{Z}[X]$; [Cucker-Koiran-Smale'98]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X]$; [H. Lenstra'99]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X_1, \ldots, X_n]$. [Kaltofen-Koiran'06]

It is NP-hard to compute **roots of** $f \in \mathbb{F}_p[X]$. [Bi-Cheng-Rojas'13]

- Only available for number fields
- Based on number-theoretic results $\rightsquigarrow$ theoretical algorithms

Generalization to other fields? More practical algorithms?

Let $\mathbb{K}$ be any field of characteristic 0.

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ with k nonzero terms and d an integer. The computation of the degree-d factors of f reduces to

- the computation of the degree-d factors of $(nk)^{\mathcal{O}(1)}$ lacunary polynomials of $\mathbb{K}[X]$, plus $d^{\mathcal{O}(1)}$ bit operations per factor in post-processing,

Let $\mathbb{K}$ be any field of characteristic 0.

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ with k nonzero terms and d an integer. The computation of the degree-d factors of f reduces to

- the computation of the degree-d factors of $(nk)^{\mathcal{O}(1)}$ lacunary polynomials of $\mathbb{K}[X]$, plus $d^{\mathcal{O}(1)}$ bit operations per factor in post-processing,

  and

- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum $(\text{size}(f) + d)^{\mathcal{O}(1)}$,

Let $\mathbb{K}$ be any field of characteristic 0.

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ with k nonzero terms and d an integer. The computation of the degree-d factors of f reduces to

- the computation of the degree-d factors of $(nk)^{\mathcal{O}(1)}$ lacunary polynomials of $\mathbb{K}[X]$, plus $d^{\mathcal{O}(1)}$ bit operations per factor in post-processing,

  and

- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum $(\text{size}(f) + d)^{\mathcal{O}(1)}$,

in $(\text{size}(f) + d)^{\mathcal{O}(1)}$ bit operations.

Let $\mathbb{K}$ be any field of characteristic 0.

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ with k nonzero terms and d an integer. The computation of the degree-d factors of f reduces to

- the computation of the degree-d factors of $(nk)^{\mathcal{O}(1)}$ lacunary polynomials of $\mathbb{K}[X]$, plus $d^{\mathcal{O}(1)}$ bit operations per factor in post-processing,

  and

- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum $(\text{size}(f) + d)^{\mathcal{O}(1)}$,

in $(\text{size}(f) + d)^{\mathcal{O}(1)}$ bit operations.

- Case $d = 1$ [G.-Chattopadhyay-Koiran-Portier-Strozecki'13]

Let $\mathbb{K}$ be any field of characteristic 0.

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ with k nonzero terms and d an integer. The computation of the degree-d factors of f reduces to

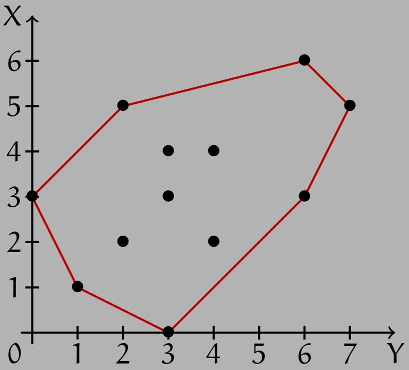
- the computation of the degree-d factors of $(nk)^{\mathcal{O}(1)}$ lacunary polynomials of $\mathbb{K}[X]$, plus $d^{\mathcal{O}(1)}$ bit operations per factor in post-processing,

  and

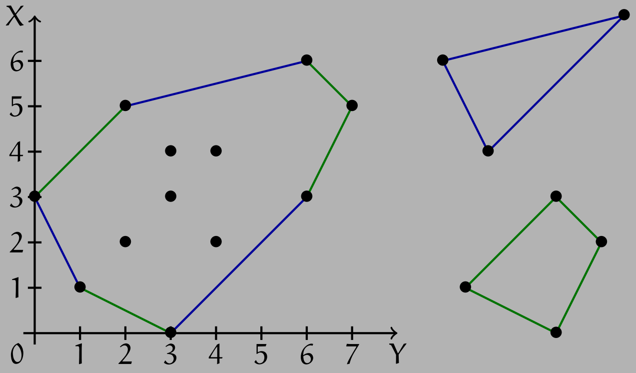
- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum $(\text{size}(f) + d)^{\mathcal{O}(1)}$,

in $(\text{size}(f) + d)^{\mathcal{O}(1)}$ bit operations.

- Case $d = 1$ [G.-Chattopadhyay-Koiran-Portier-Strozecki'13]
- New algorithm for $\mathbb{K} = \mathbb{Q}(\alpha)$; **some** factors for $\mathbb{K} = \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$;

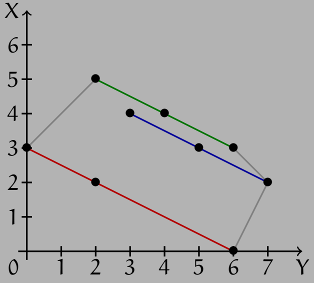


$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

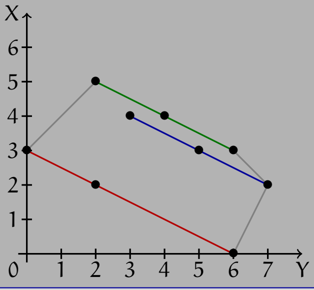


$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

$$= (Y - 2X^2 + X^3Y^4)(Y^2 + 2X - X^2Y^3 + X^3Y^2)$$



A polynomial $g = \sum_j b_j X^{\gamma_j} Y^{\delta_j}$ is (p,q)-**homogeneous** of order ω if $p\gamma_j + q\delta_j = \omega$ for all j.



A polynomial $g = \sum_j b_j X^{\gamma_j} Y^{\delta_j}$ is (p, q)-**homogeneous** of order ω if $p\gamma_j + q\delta_j = \omega$ for all j.

Algorithm for (p, q)-homogeneous factors

1. Write $f = f_1 + \cdots + f_s$ as a sum of (p, q)-homogeneous polynomials;
2. Compute the common degree-(d/q) factors of the $f_t(X^{1/q}, 1)$'s;
   $\rightsquigarrow$ **univariate lacunary factorization**
3. Return $Y^{p\deg(g)} g(X^q/Y^p)$ for each factor g.

Observation

$$(Y - uX - v) \quad \text{divides} \quad f(X,Y) \quad \Longleftrightarrow \quad f(X, uX + v) \quad \equiv 0$$

Observation

$(Y - uX - v)$	divides	$f(X, Y)$	$\iff$	$f(X, uX + v)$	$\equiv 0$
$g(X, Y)$	divides	$f(X, Y)$	$\iff$	$f(X, \phi(X))$	$\equiv 0$

Observation

$(Y - uX - v)$	divides	$f(X,Y)$	$\iff$	$f(X, uX + v)$	$\equiv 0$
$g(X,Y)$	divides	$f(X,Y)$	$\iff$	$f(X, \phi(X))$	$\equiv 0$

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X))$$

- $g_0 \in \mathbb{K}[X]$
- $\phi_1, \ldots, \phi_d \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ are **Puiseux series**:

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n} \text{ with } a_t \in \overline{\mathbb{K}},\ a_{t_0} \neq 0.$$

Observation

$(Y - uX - v)$	divides	$f(X,Y)$	$\iff$	$f(X, uX + v)$	$\equiv 0$
$g(X,Y)$	divides	$f(X,Y)$	$\iff$	$f(X, \phi(X))$	$\equiv 0$

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X))$$

- $g_0 \in \mathbb{K}[X]$
- $\phi_1, \ldots, \phi_d \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ are **Puiseux series**:

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n} \text{ with } a_t \in \overline{\mathbb{K}},\ a_{t_0} \neq 0.$$

- If g is irreducible, g divides $f \iff \exists i,\ f(X, \phi_i) = 0$
  $\iff \forall i,\ f(X, \phi_i) = 0$

Observation

$$(Y - uX - v) \text{ divides } f(X,Y) \iff f(X, uX+v) \equiv 0$$
$$g(X,Y) \text{ divides } f(X,Y) \iff f(X, \phi(X)) \equiv 0$$

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X))$$

- $g_0 \in \mathbb{K}[X]$
- $\phi_1, \ldots, \phi_d \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ are **Puiseux series**:

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n} \text{ with } a_t \in \overline{\mathbb{K}},\ a_{t_0} \neq 0.$$

- If g is irreducible, g divides $f \iff \exists i,\ f(X, \phi_i) = 0$
  $\iff \forall i,\ f(X, \phi_i) = 0$
- **Valuation**: $\text{val}(\phi) = t_0/n$.

Observation

$(Y - uX - v)$	divides	$f(X, Y)$	$\iff$	$f(X, uX + v)$	$\equiv 0$
$g(X, Y)$	divides	$f(X, Y)$	$\iff$	$f(X, \phi(X))$	$\equiv 0$

$$g(X, Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X))$$

- $g_0 \in \mathbb{K}[X]$
- $\phi_1, \ldots, \phi_d \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ are **Puiseux series**:

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n} \text{ with } a_t \in \overline{\mathbb{K}},\ a_{t_0} \neq 0.$$

- If g is irreducible, g divides $f \iff \exists i,\ f(X, \phi_i) = 0$
  $\iff \forall i,\ f(X, \phi_i) = 0$
- **Valuation**: $\mathrm{val}(\phi) = t_0/n$.

Theorem

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and g a degree-d irreducible polynomial with a root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν.
If the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent,

$$\mathrm{val}(f_1(X,\phi)) \leqslant \min_j(\alpha_j + \nu\beta_j) + (2d(4d+1) - \nu)\binom{\ell}{2}.$$

Theorem

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and g a degree-d irreducible polynomial with a root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν.
If the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent,

$$\operatorname{val}(f_1(X,\phi)) \leqslant \min_j(\alpha_j + \nu\beta_j) + (2d(4d+1) - \nu)\binom{\ell}{2}.$$

Proof idea. Let $\psi_j = X^{\alpha_j}\phi^{\beta_j}$ for all j.

Theorem

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and g a degree-d irreducible polynomial with a root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν.
If the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent,

$$\mathrm{val}(f_1(X,\phi)) \leqslant \min_j(\alpha_j + \nu\beta_j) + (2d(4d+1) - \nu)\binom{\ell}{2}.$$

Proof idea. Let $\psi_j = X^{\alpha_j}\phi^{\beta_j}$ for all j.

- Wronskian: $\mathrm{wr}(\psi_1, \dots, \psi_\ell) = \det\left(\psi_j^{(i)}\right) = \frac{1}{c_1}\mathrm{wr}(f_1, \psi_2, \dots, \psi_\ell)$

Theorem

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and g a degree-d irreducible polynomial with a root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν.
If the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent,

$$\operatorname{val}(f_1(X,\phi)) \leqslant \min_j(\alpha_j + \nu\beta_j) + (2d(4d+1) - \nu)\binom{\ell}{2}.$$

Proof idea. Let $\psi_j = X^{\alpha_j}\phi^{\beta_j}$ for all j.

- Wronskian: $\operatorname{wr}(\psi_1, \dots, \psi_\ell) = \det\left(\psi_j^{(i)}\right) = \frac{1}{c_1}\operatorname{wr}(f_1, \psi_2, \dots, \psi_\ell)$
- $\operatorname{val}(\operatorname{wr}(f_1, \psi_2, \dots, \psi_\ell)) \geqslant \operatorname{val}(f_1) + \sum_{j>1} \operatorname{val}(\psi_j)$

Theorem

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and g a degree-d irreducible polynomial with a root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν.
If the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent,

$$\mathrm{val}(f_1(X,\phi)) \leqslant \min_j(\alpha_j + \nu\beta_j) + (2d(4d+1) - \nu)\binom{\ell}{2}.$$

Proof idea. Let $\psi_j = X^{\alpha_j}\phi^{\beta_j}$ for all j.

- Wronskian: $\mathrm{wr}(\psi_1,\dots,\psi_\ell) = \det\left(\psi_j^{(i)}\right) = \frac{1}{c_1}\mathrm{wr}(f_1,\psi_2,\dots,\psi_\ell)$
- $\mathrm{val}(\mathrm{wr}(f_1,\psi_2,\dots,\psi_\ell)) \geqslant \mathrm{val}(f_1) + \sum_{j>1}\mathrm{val}(\psi_j)$
- $\mathrm{val}(\mathrm{wr}(\psi_1,\dots,\psi_\ell) \leqslant \sum_j \mathrm{val}(\psi_j) + (2d(4d+1)-\nu)\binom{\ell}{2}$

Gap Theorem

Let
$$f = \underbrace{\sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}}_{f_1} + \underbrace{\sum_{j=\ell+1}^{k} c_j X^{\alpha_j} Y^{\beta_j}}_{f_2}$$

with $\alpha_1 + \nu\beta_1 \leqslant \cdots \leqslant \alpha_k + \nu\beta_k$. Let g a degree-d irreducible poynomial, with a root of valuation ν.
If ℓ is the smallest index s.t.
$$\alpha_{\ell+1} + \nu\beta_{\ell+1} > (\alpha_1 + \nu\beta_1) + (2d(4d+1) - \nu)\binom{\ell}{2},$$

then g divides f iff it divides both f_1 and f_2.

Gap Theorem

Let

$$f = \underbrace{\sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}}_{f_1} + \underbrace{\sum_{j=\ell+1}^{k} c_j X^{\alpha_j} Y^{\beta_j}}_{f_2}$$

with $\alpha_1 + \nu\beta_1 \leqslant \cdots \leqslant \alpha_k + \nu\beta_k$. Let g a degree-d irreducible poynomial, with a root of valuation ν.

If ℓ is the smallest index s.t.

$$\alpha_{\ell+1} + \nu\beta_{\ell+1} > (\alpha_1 + \nu\beta_1) + (2d(4d+1) - \nu)\binom{\ell}{2},$$

then g divides f iff it divides both f_1 and f_2.

- Depends only on ν.

Gap Theorem

Let

$$f = \underbrace{\sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}}_{f_1} + \underbrace{\sum_{j=\ell+1}^{k} c_j X^{\alpha_j} Y^{\beta_j}}_{f_2}$$

with $\alpha_1 + \nu\beta_1 \leqslant \cdots \leqslant \alpha_k + \nu\beta_k$. Let g a degree-d irreducible poynomial, with a root of valuation ν.

If ℓ is the smallest index s.t.

$$\alpha_{\ell+1} + \nu\beta_{\ell+1} > (\alpha_1 + \nu\beta_1) + (2d(4d+1) - \nu)\binom{\ell}{2},$$

then g divides f iff it divides both f_1 and f_2.

- Depends only on ν.
- Bounds the growth of $\alpha_j + \nu\beta_j$ in f_1.

Observation + Gap Theorem (recursively)

Let $g(X,Y)$ be irreducible, with a root $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation v.

Then g divides $f(X,Y) \iff f(X,\phi) \equiv 0$

Observation + Gap Theorem (recursively)

Let $g(X,Y)$ be irreducible, with a root $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν.

$$\text{Then } g \text{ divides } f(X,Y) \iff f(X,\phi) \equiv 0$$
$$\iff f_1(X,\phi) \equiv \cdots \equiv f_s(X,\phi) \equiv 0$$

Observation + Gap Theorem (recursively)

Let $g(X,Y)$ be irreducible, with a root $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν.

$$\text{Then } g \text{ divides } f(X,Y) \iff f(X,\phi) \equiv 0$$
$$\iff f_1(X,\phi) \equiv \cdots \equiv f_s(X,\phi) \equiv 0$$
$$\iff g \text{ divides each } f_t(X,Y)$$

Observation + Gap Theorem (recursively)

Let $g(X,Y)$ be irreducible, with a root $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν.

$$\text{Then } g \text{ divides } f(X,Y) \iff f(X,\phi) \equiv 0$$
$$\iff f_1(X,\phi) \equiv \cdots \equiv f_s(X,\phi) \equiv 0$$
$$\iff g \text{ divides each } f_t(X,Y)$$

- $f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$ with

$$\alpha_j + \nu\beta_j \leqslant \alpha_{j_t} + \nu\beta_{j_t} + (2d(4d+1)-\nu)\binom{\ell_t}{2}$$

Observation + Gap Theorem (recursively)

Let $g(X,Y)$ be irreducible, with a root $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν.

$$\begin{aligned}\text{Then } g \text{ divides } f(X,Y) &\iff f(X,\phi) \equiv 0\\ &\iff f_1(X,\phi) \equiv \cdots \equiv f_s(X,\phi) \equiv 0\\ &\iff g \text{ divides each } f_t(X,Y)\end{aligned}$$

- $f_t = \displaystyle\sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$ with

  $$\alpha_j + \nu\beta_j \leqslant \alpha_{j_t} + \nu\beta_{j_t} + (2d(4d+1)-\nu)\binom{\ell_t}{2}$$

- Neither α_j nor β_j is bounded.

Observation + Gap Theorem (recursively)

Let $g(X,Y)$ be irreducible, with a root $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν.

$$\begin{aligned} \text{Then } g \text{ divides } f(X,Y) &\iff f(X,\phi) \equiv 0 \\ &\iff f_1(X,\phi) \equiv \cdots \equiv f_s(X,\phi) \equiv 0 \\ &\iff g \text{ divides each } f_t(X,Y) \end{aligned}$$

- $f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$ with

  $\alpha_j + \nu\beta_j \leqslant \alpha_{j_t} + \nu\beta_{j_t} + (2d(4d+1)-\nu)\binom{\ell_t}{2}$
- Neither α_j nor β_j is bounded.
- A second root of distinct valuation is needed!

Proposition

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and $v_1 \neq v_2$ such that for all j

$$\begin{cases} \alpha_j + v_1\beta_j \leqslant \alpha_1 + v_1\beta_1 + (2d(4d+1) - v_1)\binom{\ell}{2} \\ \alpha_j + v_2\beta_j \leqslant \alpha_2 + v_2\beta_2 + (2d(4d+1) - v_2)\binom{\ell}{2}. \end{cases}$$

Then for all p, q, $|\alpha_p - \alpha_q| \leqslant \mathcal{O}(\ell^2 d^4)$ and $|\beta_p - \beta_q| \leqslant \mathcal{O}(\ell^2 d^4)$.

Proposition

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and $v_1 \neq v_2$ such that for all j

$$\begin{cases} \alpha_j + v_1\beta_j \leqslant \alpha_1 + v_1\beta_1 + (2d(4d+1) - v_1)\binom{\ell}{2} \\ \alpha_j + v_2\beta_j \leqslant \alpha_2 + v_2\beta_2 + (2d(4d+1) - v_2)\binom{\ell}{2}. \end{cases}$$

Then for all p, q, $|\alpha_p - \alpha_q| \leqslant \mathcal{O}(\ell^2 d^4)$ and $|\beta_p - \beta_q| \leqslant \mathcal{O}(\ell^2 d^4)$.

Given $d \in \mathbb{Z}_+$, $v_1, v_2 \in \mathbb{Q}$ and $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$, we can write

$$f = X^{a_1} Y^{b_1} f_1 + \cdots X^{a_s} Y^{b_s} f_s$$

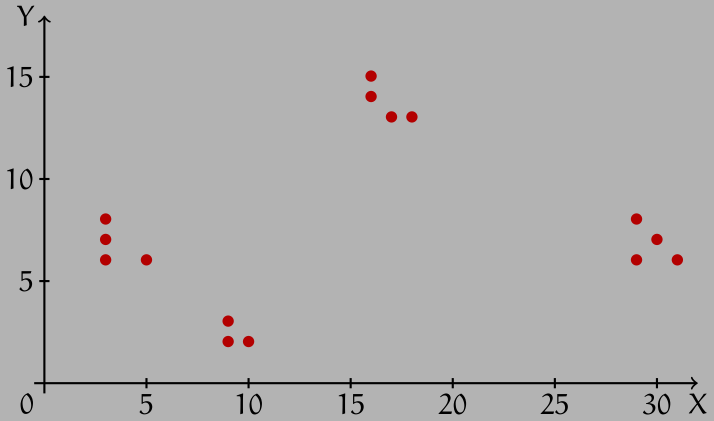
where $\sum_t \deg(f_t) \leqslant \mathcal{O}(k^2 d^4)$, such that g divides f iff g divides each f_t as soon as g has roots of valuation v_1 and v_2.

An example with $\nu_1 = 0, \nu_2 = \infty$

$$
\begin{aligned}
f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\
- X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\
+ X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6
\end{aligned}
$$

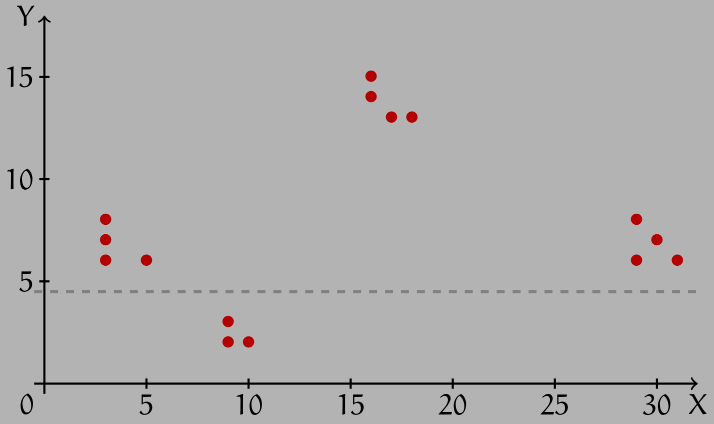
An example with $v_1 = 0$, $v_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$



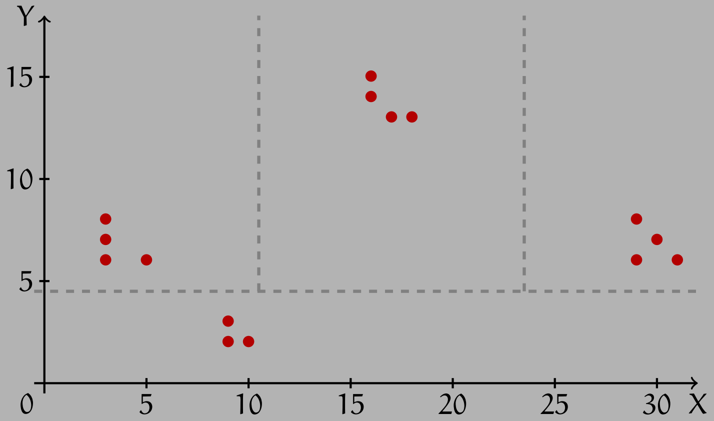
An example with $\nu_1 = 0$, $\nu_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$



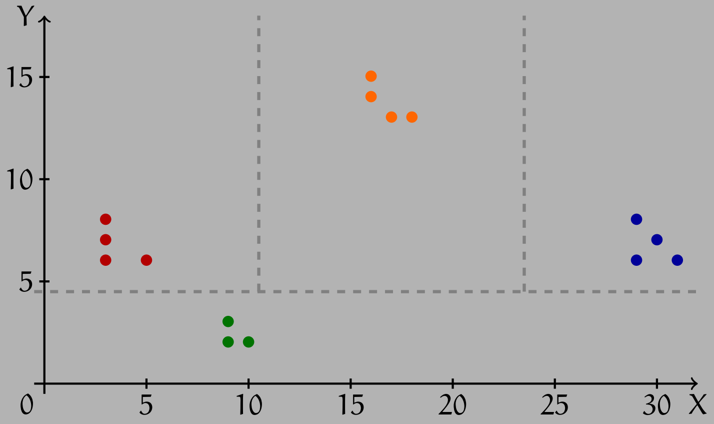
An example with $v_1 = 0$, $v_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$



An example with $v_1 = 0, v_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$



An example with $v_1 = 0, v_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$

$$f_1 = X^3Y^6(-X^2 + Y^2 - 2Y + 1)$$

An example with $v_1 = 0, v_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$

$$f_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

An example with $v_1 = 0, v_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$

$$f_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$f_2 = X^9Y^2(X - Y + 1)$$

$$f_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$f_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

An example with $\nu_1 = 0, \nu_2 = \infty$

$$f = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$

$$f_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$f_2 = X^9Y^2(X - Y + 1)$$

$$f_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$f_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

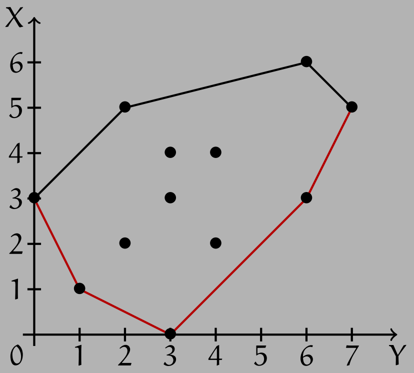
$\Longrightarrow$ linear factors of f: $(X - Y + 1, 1)$

An example with $v_1 = 0, v_2 = \infty$

$$\begin{aligned} f = {} & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

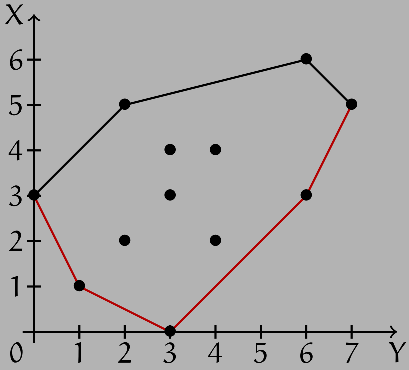
$$\begin{aligned} f_1 &= X^3Y^6(X-Y+1)(1-X-Y) \\ f_2 &= X^9Y^2(X-Y+1) \\ f_3 &= X^{16}Y^{13}(X+Y)(X-Y+1) \\ f_4 &= X^{29}Y^6(X+Y-1)(X-Y+1) \end{aligned}$$

$\implies$ linear factors of f: $(X-Y+1, 1)$, $(X, 3)$, $(Y, 2)$



Newton-Puiseux Theorem

For each edge in the **lower hull** of slope $-\nu$, f has a root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν.



Newton-Puiseux Theorem
For each edge in the **lower hull** of slope $-\nu$, f has a root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν.

Non-homogeneous factors:

- The Newton polygon has at least two non-parallel edges;
- The factor has two roots of distinct valuations.

Input: $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$ and $d \in \mathbb{Z}_+$;

Output: The irreducible degree-d factors of f, with multiplicity.

Input: $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$ and $d \in \mathbb{Z}_+$;

Output: The irreducible degree-d factors of f, with multiplicity.

1. Compute the Newton polygon N_f of f;

Input: $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$ and $d \in \mathbb{Z}_+$;

Output: The irreducible degree-d factors of f, with multiplicity.

1. Compute the Newton polygon N_f of f;
2. For each pair of non-parallel edges of slopes ν_1 & ν_2:
   2.1 Using the Gap Theorem twice, with ν_1 and ν_2, write

$$f = X^{a_1} Y^{b_1} f_1 + \cdots + X^{a_s} Y^{b_s} f_s,$$

   where $\sum_t \deg(f_t) \leqslant \mathcal{O}(k^2 d^4)$;

Input: $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$ and $d \in \mathbb{Z}_+$;

Output: The irreducible degree-d factors of f, with multiplicity.

1. Compute the Newton polygon N_f of f;
2. For each pair of non-parallel edges of slopes ν_1 & ν_2:
   2.1 Using the Gap Theorem twice, with ν_1 and ν_2, write

   $$f = X^{a_1} Y^{b_1} f_1 + \cdots + X^{a_s} Y^{b_s} f_s,$$

   where $\sum_t \deg(f_t) \leqslant \mathcal{O}(k^2 d^4)$;

   2.2 Compute the degree-d factors of $\gcd(f_1, \ldots, f_s)$;

Input: $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$ and $d \in \mathbb{Z}_+$;

Output: The irreducible degree-d factors of f, with multiplicity.

1. Compute the Newton polygon N_f of f;
2. For each pair of non-parallel edges of slopes ν_1 & ν_2:
   2.1 Using the Gap Theorem twice, with ν_1 and ν_2, write
   $$f = X^{a_1} Y^{b_1} f_1 + \cdots + X^{a_s} Y^{b_s} f_s,$$
   where $\sum_t \deg(f_t) \leqslant \mathcal{O}(k^2 d^4)$;
   2.2 Compute the degree-d factors of $\gcd(f_1, \ldots, f_s)$;
3. Return the union of the sets of computed factors, with multiplicity.

Complete algorithm

$$\text{Find degree-}d\text{ factors of } f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$$

Find degree-d factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$

monomials

$(X, \min_j \alpha_j)$
$(Y, \min_j \beta_j)$

Find degree-d factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$

monomials → $(X, \min_j \alpha_j)$, $(Y, \min_j \beta_j)$

weighted hom. → Degree-d factors of univariate lacunary polynomials

Available for $\mathbb{Q}(\alpha)$ only
Impossible for $\overline{\mathbb{Q}}$, $\mathbb{C}$

Find degree-d factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$

monomials — weighted hom. — non-hom.

monomials:

$(X, \min_j \alpha_j)$
$(Y, \min_j \beta_j)$

weighted hom.:

Degree-d factors of univariate lacunary polynomials

Available for $\mathbb{Q}(\alpha)$ only
Impossible for $\overline{\mathbb{Q}}$, $\mathbb{C}$

non-hom.:

Common factors of

$$f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$$

$(\deg(f_t) \leqslant \mathcal{O}(\ell_t^2 d^4))$

Low-degree factorization
$\mathbb{Q}(\alpha), \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$, etc.

$$\text{Degree-}d \text{ factors of } f = \sum_{j=1}^{k} c_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

$$\text{Degree-}d \text{ factors of } f = \sum_{j=1}^{k} c_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

- Do not compute the n-dimensional Newton polygon!

$$\text{Degree-}d \text{ factors of } f = \sum_{j=1}^{k} c_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

- Do not compute the n-dimensional Newton polygon!
- For all $i < j$, compute the Newton polygon $N_{i,j}$ of $f \in R[X_i, X_j]$ where $R = \mathbb{K}[\mathbf{X} \setminus X_i, X_j]$;

$$\text{Degree-}d \text{ factors of } f = \sum_{j=1}^{k} c_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

- Do not compute the n-dimensional Newton polygon!
- For all $i < j$, compute the Newton polygon $N_{i,j}$ of $f \in R[X_i, X_j]$ where $R = \mathbb{K}[\mathbf{X} \setminus X_i, X_j]$;
- Weighted homogeneous factors $\rightsquigarrow$ 1-dimensional factors

$$\text{Degree-}d \text{ factors of } f = \sum_{j=1}^{k} c_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

- Do not compute the n-dimensional Newton polygon!
- For all $i < j$, compute the Newton polygon $N_{i,j}$ of $f \in R[X_i, X_j]$ where $R = \mathbb{K}[\mathbf{X} \setminus X_i, X_j]$;
- Weighted homogeneous factors $\rightsquigarrow$ 1-dimensional factors
  - Every $N_{i,j}$ is 1-dimensional (or 0-dimensional)
  - **Univariate lacunary factorization**

$$\text{Degree-}d \text{ factors of } f = \sum_{j=1}^{k} c_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

- Do not compute the n-dimensional Newton polygon!
- For all $i < j$, compute the Newton polygon $N_{i,j}$ of $f \in R[X_i, X_j]$ where $R = \mathbb{K}[\mathbf{X} \setminus X_i, X_j]$;
- Weighted homogeneous factors $\rightsquigarrow$ 1-dimensional factors
  - Every $N_{i,j}$ is 1-dimensional (or 0-dimensional)
  - **Univariate lacunary factorization**
- Non-homogeneous factors $\rightsquigarrow$ multidimensional factors

$$\text{Degree-}d \text{ factors of } f = \sum_{j=1}^{k} c_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

- Do not compute the n-dimensional Newton polygon!
- For all $i < j$, compute the Newton polygon $N_{i,j}$ of $f \in R[X_i, X_j]$ where $R = \mathbb{K}[\mathbf{X} \setminus X_i, X_j]$;
- Weighted homogeneous factors $\rightsquigarrow$ 1-dimensional factors
  - Every $N_{i,j}$ is 1-dimensional (or 0-dimensional)
  - **Univariate lacunary factorization**
- Non-homogeneous factors $\rightsquigarrow$ multidimensional factors
  - At least one $N_{i,j}$ is multidimensional
  - **Multivariate low-degree factorization**

- Consider f as before, and let g be a multidimensional factor of f:
  - If "$X_i \notin g$", g divides each coefficient of $f \in \mathbb{K}[\mathbf{X} \setminus X_i][X_i]$;
  - Else $N_{i,j}(g)$ is multidimensional for some j.

- Consider f as before, and let g be a multidimensional factor of f:
  - If "$X_i \notin g$", g divides each coefficient of $f \in \mathbb{K}[\mathbf{X} \setminus X_i][X_i]$;
  - Else $N_{i,j}(g)$ is multidimensional for some j.

1. Let $\mathcal{H} = \{f\}$;
2. For each variable X_i, and $h \in \mathcal{H}$:
   2.1 Partition $h = \sum_d h_i(\mathbf{X} \setminus X_i) X_i^d$;
   2.2 For each X_j such that $N_{i,j}(h)$ is multidimensional, partition h with respect to each pair of non-parallel edges in $N_{i,j}(h)$;
   2.3 *Merge* those $\mathcal{O}(nk^2)$ partitions to get $\mathcal{H}_h$;
   2.4 Replace h by the elements of $\mathcal{H}_h$ in $\mathcal{H}$.
3. Return the degree-d factors of $\gcd(\mathcal{H}^\circ)$.

Positive characteristic

[G.-Chattopadhyay-Koiran-Portier-Strozecki'13]

$$\text{Find linear factors of } f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$$
$$\text{where } c_j \in \mathbb{F}_{p^s} \text{ and } p > \deg(f)$$

[G.-Chattopadhyay-Koiran-Portier-Strozecki'13]

Find linear factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$

where $c_j \in \mathbb{F}_{p^s}$ and $p > \deg(f)$

monomials

$(X, \min_j \alpha_j)$
$(Y, \min_j \beta_j)$

trinomials

Common factors of

$$f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$$

$(\deg(f_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization

[Gao'03, Lecerf'10]

Positive characteristic

[G.-Chattopadhyay-Koiran-Portier-Strozecki'13]

Find linear factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$

where $c_j \in \mathbb{F}_{p^s}$ and $p > \deg(f)$

monomials — binomials — trinomials

- monomials → $(X, \min_j \alpha_j)$, $(Y, \min_j \beta_j)$
- binomials → $(uX - vY)$ $\Updownarrow$ Roots of univariate lacunary polynomials
- trinomials → Common factors of $f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$ $(\deg(f_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization

[Gao'03, Lecerf'10]

[G.-Chattopadhyay-Koiran-Portier-Strozecki'13]

Find linear factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j}$

where $c_j \in \mathbb{F}_{p^s}$ and $p > \deg(f)$

monomials | binomials | trinomials

$(X, \min_j \alpha_j)$
$(Y, \min_j \beta_j)$

$(uX - v$ …

R… variate
la… polynomials

NP-complete
under BPP reductions

[Kipnis-Shamir'99, Bi-Cheng-Rojas'13]

Common factors of

$f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$

$(\deg(f_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization
[Gao'03, Lecerf'10]

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree multivariate polynomials}\end{cases}$

Conclusion

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree multivariate polynomials}\end{cases}$
  - "Field-independent"
  - **Simpler** and **more general** than previous algorithms
  - Partial results in **large positive characteristic**
  - Implementation: work in progress

Conclusion

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree multivariate polynomials}\end{cases}$
  - "Field-independent"
  - **Simpler** and **more general** than previous algorithms
  - Partial results in **large positive characteristic**
  - Implementation: work in progress
- Open questions:
  - Can we compute **lacunary factors** in polynomial time?
  - More general settings: arithmetic circuits/straight-line programs
  - **Higher degree factors** in positive characteristic: Hahn series?
  - What can be done in **small positive characteristic**?

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree multivariate polynomials}\end{cases}$
  - “Field-independent”
  - **Simpler** and **more general** than previous algorithms
  - Partial results in **large positive characteristic**
  - Implementation: work in progress
- Open questions:
  - Can we compute **lacunary factors** in polynomial time?
  - More general settings: arithmetic circuits/straight-line programs
  - **Higher degree factors** in positive characteristic: Hahn series?
  - What can be done in **small positive characteristic**?

Thank you!

arXiv:1401.4720