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

Bruno Grenet
LIX — École Polytechnique

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. $f = f_1 \times \cdots \times f_t$.

- Algorithms for polynomials over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, ...

Factorization of a polynomial f

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

- Algorithms for polynomials over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, …
- Complexity: **polynomial in** $\deg(f)$

Factorization of a polynomial f

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

- Algorithms for polynomials over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, ...
- 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 $f_1, \dots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Algorithms for polynomials over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\dots$
- 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. $f = f_1 \times \cdots \times f_t$.

- Algorithms for polynomials over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, …
- Complexity: **polynomial in** $\deg(f)$

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

Let $f \in \mathbb{K}[X]$, for some field or ring $\mathbb{K}$.

- For all $\mathbb{K}$, $\#Z_{\mathbb{K}}(f) \leqslant \deg(f)$

Descartes' rule without signs

Let $f \in \mathbb{K}[X]$, for some field or ring $\mathbb{K}$.

- For all $\mathbb{K}$, $\#Z_{\mathbb{K}}(f) \leqslant \deg(f)$
- If $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, $\#Z_{\mathbb{K}}(f) \leqslant 2k - 1$ where k is the **number of nonzero terms** of f.

Let $f \in \mathbb{K}[X]$, for some field or ring $\mathbb{K}$.

- For all $\mathbb{K}$, $\#Z_{\mathbb{K}}(f) \leqslant \deg(f)$
- If $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, $\#Z_{\mathbb{K}}(f) \leqslant 2k-1$ where k is the **number of nonzero terms** of f.

Definition

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

Let $f \in \mathbb{K}[X]$, for some field or ring $\mathbb{K}$.

- For all $\mathbb{K}$, $\#Z_{\mathbb{K}}(f) \leqslant \deg(f)$
- If $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, $\#Z_{\mathbb{K}}(f) \leqslant 2k - 1$ where k is the **number of nonzero terms** of f.

Definition

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

- Lacunary representation: $\{(c_j, \alpha_{1j}, \ldots, \alpha_{nj}) : 1 \leqslant j \leqslant k\}$
- $\mathrm{size}(f) \simeq \sum_j \mathrm{size}(c_j) + \log(\alpha_{1j}) + \cdots + \log(\alpha_{nj})$

$$\leqslant k\Big(\max_j(\mathrm{size}(c_j)) + n\log(d)\Big)$$

Theorem [Cucker-Koiran-Smale'98]

There exists a deterministic **polynomial-time** algorithm to compute the integer roots of a **lacunary polynomial** $f \in \mathbb{Z}[X]$.

Theorem [Cucker-Koiran-Smale'98]

There exists a deterministic **polynomial-time** algorithm to compute the integer roots of a **lacunary polynomial** $f \in \mathbb{Z}[X]$.

Gap Theorem [Cucker-Koiran-Smale'98]

Let

$$f(X) = \underbrace{\sum_{j=1}^{\ell} c_j X^{\alpha_j}}_{f_1} + \underbrace{\sum_{j=\ell+1}^{k} c_j X^{\alpha_j}}_{f_2} \in \mathbb{Z}[X]$$

with $\alpha_1 \leqslant \cdots \leqslant \alpha_k$ and $\alpha_{\ell+1} - \alpha_\ell > 1 + \max_j(\mathrm{size}(c_j))$. Then for $|x| \geqslant 2$, $f(x) = 0 \implies f_1(x) = f_2(x) = 0$.

Theorem [Cucker-Koiran-Smale'98]

There exists a deterministic **polynomial-time** algorithm to compute the integer roots of a **lacunary polynomial** $f \in \mathbb{Z}[X]$.

Gap Theorem [Cucker-Koiran-Smale'98]

Let
$$f(X) = \underbrace{\sum_{j=1}^{\ell} c_j X^{\alpha_j}}_{f_1} + \underbrace{\sum_{j=\ell+1}^{k} c_j X^{\alpha_j}}_{f_2} \in \mathbb{Z}[X]$$
with $\alpha_1 \leqslant \cdots \leqslant \alpha_k$ and $\alpha_{\ell+1} - \alpha_\ell > 1 + \max_j(\mathrm{size}(c_j))$. Then for $|x| \geqslant 2$, $f(x) = 0 \implies f_1(x) = f_2(x) = 0$.

$$-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)$$

Theorems

There exist deterministic polynomial-time algorithms computing

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

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors 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 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 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]**

- Only available for number fields

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors 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]

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

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors 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]

- 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 $f \in \mathbb{K}[X_1, \ldots, X_n]$, of degree D 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 $\mathbb{K}[X]$, and

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

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$, of degree D 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 $\mathbb{K}[X]$, and
- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum at most $(nk \log(D) + d)^{\mathcal{O}(1)}$,

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

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \dots, X_n]$, of degree D 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 $\mathbb{K}[X]$, and
- the factorization of polynomials of $\mathbb{K}[X_1, \dots, X_n]$ of total degree sum at most $(nk\log(D) + d)^{\mathcal{O}(1)}$,

plus at most $(nk \log D + d)^{\mathcal{O}(1)}$ bit operations.

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

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$, of degree D 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 $\mathbb{K}[X]$, and
- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum at most $(nk\log(D) + d)^{\mathcal{O}(1)}$,

plus at most $(nk \log D + d)^{\mathcal{O}(1)}$ bit operations.

- New algorithm for $\mathbb{K} = \mathbb{Q}(\alpha)$;

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

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$, of degree D 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 $\mathbb{K}[X]$, and
- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum at most $(nk\log(D) + d)^{\mathcal{O}(1)}$,

plus at most $(nk\log D + d)^{\mathcal{O}(1)}$ bit operations.

- New algorithm for $\mathbb{K} = \mathbb{Q}(\alpha)$;
- Computation of **some** factors for $\mathbb{K} = \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$;

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

Theorem [G.'14]

Let $f \in \mathbb{K}[X_1, \ldots, X_n]$, of degree D 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 $\mathbb{K}[X]$, and
- the factorization of polynomials of $\mathbb{K}[X_1, \ldots, X_n]$ of total degree sum at most $(nk\log(D) + d)^{\mathcal{O}(1)}$,

plus at most $(nk\log D + d)^{\mathcal{O}(1)}$ bit operations.

- New algorithm for $\mathbb{K} = \mathbb{Q}(\alpha)$;
- Computation of **some** factors for $\mathbb{K} = \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$;
- Positive characteristic: discussed later.

Linear factors of bivariate lacunary polynomials

joint work with
A. Chattopadhyay, P. Koiran, N. Portier & Y. Strozecki

Observation

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

Observation

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

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

Let

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

with $uv \neq 0$, $\alpha_1 \leqslant \cdots \leqslant \alpha_k$. If ℓ is the smallest index s.t.

$$\alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2},$$

then $f \equiv 0$ iff both $f_1 \equiv 0$ and $f_2 \equiv 0$.

$\mathbb{K}$: any field of characteristic 0

Definition

$\mathrm{val}(f) = \max\{\nu : X^\nu \text{ divides } f\}$

$\mathbb{K}$: any field of characteristic 0

Definition

$\mathrm{val}(f) = \max\{v : X^v \text{ divides } f\}$

Theorem

Let $f = \sum_{j=1}^{\ell} c_j X^{\alpha_j}(uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leqslant \cdots \leqslant \alpha_\ell$.

Then, if the family $(X^{\alpha_j}(uX+v)^{\beta_j})_j$ is linearly independent,

$$\mathrm{val}(f) \leqslant \alpha_1 + \binom{\ell}{2}.$$

Definition

Let $f_1, \ldots, f_\ell \in \mathbb{K}[X]$. Then

$$\operatorname{wr}(f_1, \ldots, f_\ell) = \det \begin{bmatrix} f_1 & f_2 & \ldots & f_\ell \\ f_1' & f_2' & \ldots & f_\ell' \\ \vdots & \vdots & & \vdots \\ f_1^{(\ell-1)} & f_2^{(\ell-1)} & \ldots & f_\ell^{(\ell-1)} \end{bmatrix}.$$

Definition

Let $f_1, \ldots, f_\ell \in \mathbb{K}[X]$. Then

$$\mathrm{wr}(f_1, \ldots, f_\ell) = \det \begin{bmatrix} f_1 & f_2 & \ldots & f_\ell \\ f_1' & f_2' & \ldots & f_\ell' \\ \vdots & \vdots & & \vdots \\ f_1^{(\ell-1)} & f_2^{(\ell-1)} & \ldots & f_\ell^{(\ell-1)} \end{bmatrix}.$$

Proposition [Bôcher, 1900]

$\mathrm{wr}(f_1, \ldots, f_\ell) \neq 0 \iff$ the f_j's are linearly independent.

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_\ell)) \geqslant \sum_{j=1}^{\ell} \mathrm{val}(f_j) - \binom{\ell}{2}$$

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1, \dots, f_\ell)) \geqslant \sum_{j=1}^{\ell} \mathrm{val}(f_j) - \binom{\ell}{2}$$

Lemma

Let $f_j = X^{\alpha_j}(uX + v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geqslant \ell$. Then

$$\mathrm{val}(\mathrm{wr}(f_1, \dots, f_\ell)) \leqslant \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \mathrm{val}(f_j).$$

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_\ell)) \geqslant \sum_{j=1}^{\ell} \mathrm{val}(f_j) - \binom{\ell}{2}$$

Lemma

Let $f_j = X^{\alpha_j}(uX+v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geqslant \ell$. Then

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_\ell)) \leqslant \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \mathrm{val}(f_j).$$

Proof of the theorem. $\mathrm{wr}(f, f_2, \dots, f_\ell) = c_1\,\mathrm{wr}(f_1,\dots,f_\ell)$

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_\ell)) \geqslant \sum_{j=1}^{\ell} \mathrm{val}(f_j) - \binom{\ell}{2}$$

Lemma

Let $f_j = X^{\alpha_j}(uX+v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geqslant \ell$. Then

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_\ell)) \leqslant \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \mathrm{val}(f_j).$$

Proof of the theorem. $\mathrm{wr}(f, f_2, \dots, f_\ell) = c_1\, \mathrm{wr}(f_1, \dots, f_\ell)$

$$\sum_{j=1}^{\ell} \alpha_j \geqslant \mathrm{val}(\mathrm{wr}(f_1,\dots,f_\ell)) \geqslant \mathrm{val}(f) + \sum_{j=2}^{\ell} \alpha_j - \binom{\ell}{2}$$

Observation + Gap Theorem (recursively)

$(Y - uX - v)$ divides $f(X,Y)$

$$\iff f(X, uX + v) \equiv 0$$

Observation + Gap Theorem (recursively)

$$(Y - uX - v) \text{ divides } f(X, Y)$$
$$\iff f(X, uX + v) \equiv 0$$
$$\iff f_1(X, uX + v) \equiv \cdots \equiv f_s(X, uX + v) \equiv 0$$

Observation + Gap Theorem (recursively)

$$
\begin{aligned}
(Y - uX - v) \text{ divides } f(X, Y) & \\
\iff\ & f(X, uX + v) \equiv 0 \\
\iff\ & f_1(X, uX + v) \equiv \cdots \equiv f_s(X, uX + v) \equiv 0 \\
\iff\ & (Y - uX - v) \text{ divides each } f_t(X, Y)
\end{aligned}
$$

Observation + Gap Theorem (recursively)

$$\begin{aligned}(Y-uX-v) \text{ divides } f(X,Y) \\ &\iff f(X,uX+v)\equiv 0 \\ &\iff f_1(X,uX+v)\equiv\cdots\equiv f_s(X,uX+v)\equiv 0 \\ &\iff (Y-uX-v) \text{ divides each } f_t(X,Y)\end{aligned}$$

- $f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leqslant \binom{\ell_t}{2}$

Observation + Gap Theorem (recursively)

$$\begin{aligned}(Y - uX - v) \text{ divides } f(X,Y) \\ &\iff f(X, uX+v) \equiv 0 \\ &\iff f_1(X, uX+v) \equiv \cdots \equiv f_s(X, uX+v) \equiv 0 \\ &\iff (Y - uX - v) \text{ divides each } f_t(X,Y)\end{aligned}$$

- $f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leqslant \binom{\ell_t}{2}$
- Independent from u and v

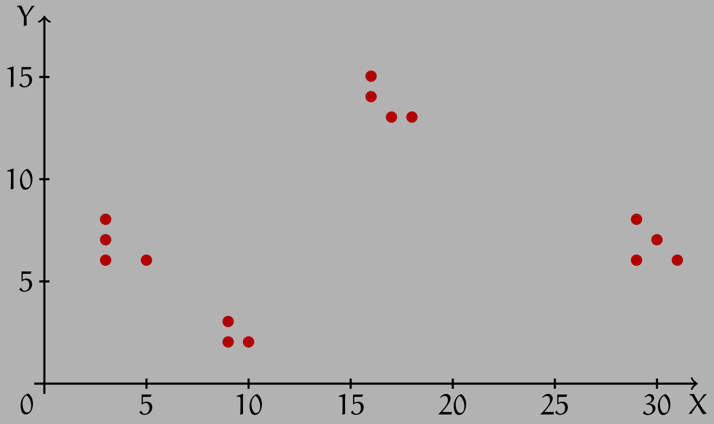
Observation + Gap Theorem (recursively)

$$
\begin{aligned}
(Y-uX-v) \text{ divides } f(X,Y) & \\
&\iff f(X,uX+v)\equiv 0\\
&\iff f_1(X,uX+v)\equiv\cdots\equiv f_s(X,uX+v)\equiv 0\\
&\iff (Y-uX-v) \text{ divides each } f_t(X,Y)
\end{aligned}
$$

- $f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leqslant \binom{\ell_t}{2}$
- Independent from u and v
- X does not play a special role

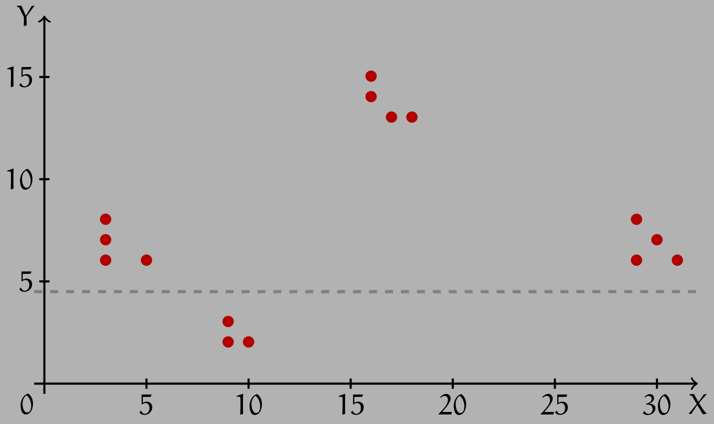
$$f = X^{31}Y^{6} - 2X^{30}Y^{7} + X^{29}Y^{8} - X^{29}Y^{6} + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^{2} - X^{9}Y^{3} + X^{9}Y^{2} - X^{5}Y^{6} + X^{3}Y^{8} - 2X^{3}Y^{7} + X^{3}Y^{6}$$

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



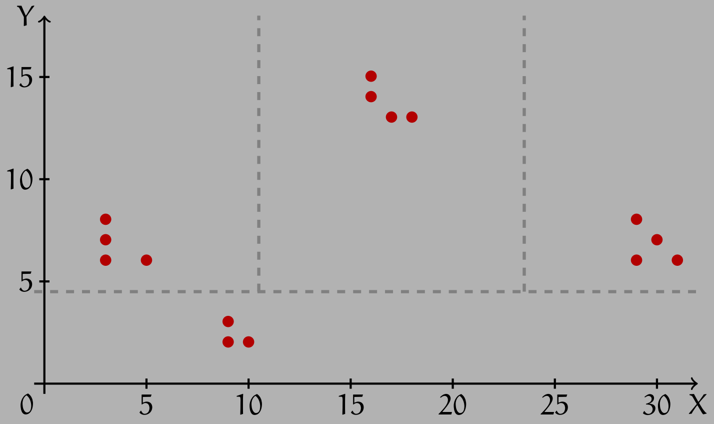
Example

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

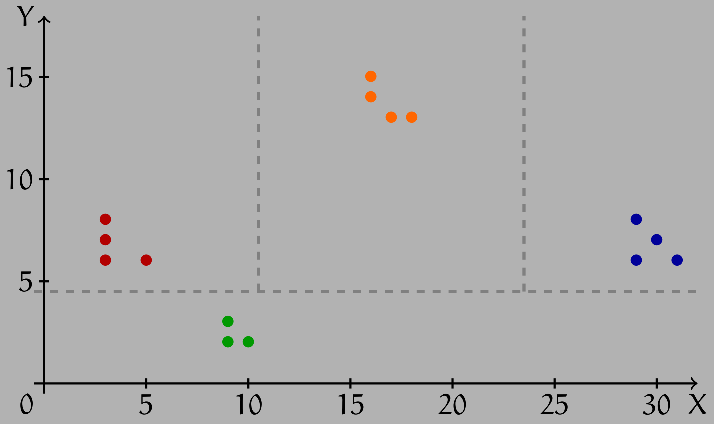


Example

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



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



Example

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

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

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

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

Example

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

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

Example

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

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

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

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

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

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

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

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

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

Complete algorithm for linear factors

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

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

Complete algorithm for linear factors

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

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

monomials

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

Complete algorithm for linear factors

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

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

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

binomials →

$(X - a)$: Factors of $\sum_j c_j X^{\alpha_j}$

$(Y - uX)$: Roots of $u \mapsto \sum_j c_j u^{\beta_j}$

Univariate lacunary factorization

[H. Lenstra'99]

Complete algorithm for linear factors

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

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

monomials — binomials — trinomials

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

binomials →

$(X - a)$: Factors of $\sum_j c_j X^{\alpha_j}$

$(Y - uX)$: Roots of $u \mapsto \sum_j c_j u^{\beta_j}$

Univariate lacunary factorization
[H. Lenstra'99]

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
[Kaltofen'82, …, Lecerf'07]

Complete algorithm for linear factors

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

Let $f = \sum_{j=1}^{k} c_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{Q}(\alpha)[X,Y]$ be given in lacunary representation. There exists a **deterministic polynomial-time** algorithm to compute its linear factors, with multiplicities.

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

binomials → $(X - a)$: Factors of $\sum_j c_j X^{\alpha_j}$; $(Y - uX)$: Roots of $u \mapsto \sum_j c_j u^{\beta_j}$

Univariate lacunary factorization
[H. Lenstra'99]

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
[Kaltofen'82, ..., Lecerf'07]

$$(1+X)^{2^n} + (1+X)^{2^{n+1}} = X^{2^n}(X+1) \mod 2$$

$$(1+X)^{2^n} + (1+X)^{2^{n+1}} = X^{2^n}(X+1) \mod 2$$

Theorem

Let $f = \sum_{j=1}^{\ell} c_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j+\beta_j)$. If $(X^{\alpha_j}(uX+v)^{\beta_j})_j$ is linearly independent, then $\mathrm{val}(f) \leqslant \alpha_1 + \binom{\ell}{2}$, provided $f \not\equiv 0$.

$$(1+X)^{2^n} + (1+X)^{2^{n+1}} = X^{2^n}(X+1) \mod 2$$

Theorem

Let $f = \sum_{j=1}^{\ell} c_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j+\beta_j)$. If $(X^{\alpha_j}(uX+v)^{\beta_j})_j$ is linearly independent, then $\mathrm{val}(f) \leqslant \alpha_1 + \binom{\ell}{2}$, provided $f \not\equiv 0$.

Proposition

$\mathrm{wr}(f_1,\ldots,f_k) \neq 0 \iff f_j$'s linearly independent **over** $\mathbb{F}_{p^s}[X^p]$.

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

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]

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** → $(X, \min_j \alpha_j)$ $(Y, \min_j \beta_j)$
- **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]

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** → $(X, \min_j \alpha_j)$, $(Y, \min_j \beta_j)$
- **binomials** → $(uX - v$ … R … variate la… polynomials
  - NP-complete under BPP reductions
  - [Kipnis-Shamir'99, Bi-Cheng-Rojas'13]
- **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]

Low-degree factors of bivariate lacunary polynomials

Let $g \in \mathbb{K}[X,Y]$ of degree d in Y. Then g can be written

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

where $g_0 \in \mathbb{K}[X]$

Let $g \in \mathbb{K}[X,Y]$ of degree d in Y. Then g can be written

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

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

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n},$$

with $a_t \in \overline{\mathbb{K}}$, $a_{t_0} \neq 0$.

Let $g \in \mathbb{K}[X,Y]$ of degree d in Y. Then g can be written

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

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

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n},$$

with $a_t \in \overline{\mathbb{K}}$, $a_{t_0} \neq 0$. The **valuation** of ϕ is t_0/n.

Let $g \in \mathbb{K}[X, Y]$ of degree d in Y. Then g can be written

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

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

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n},$$

with $a_t \in \overline{\mathbb{K}}$, $a_{t_0} \neq 0$. The **valuation** of ϕ is t_0/n.

Proposition

Let $f, g \in \mathbb{K}[X, Y]$, and suppose g irreducible. Then g divides f iff $f(X, \phi) = 0$ for some/each root $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of g.

Theorem [G.'14]

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 [G.'14]

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 along the same lines, using the Wronskian.

Gap Theorem [G.'14]

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 $uv \neq 0$, $\alpha_1 + v\beta_1 \leqslant \cdots \leqslant \alpha_k + v\beta_k$. Let g a degree-d irreducible poynomial, with a root of valuation v.
If ℓ is the smallest index s.t.

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

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

Gap Theorem [G.'14]

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 $uv \neq 0$, $\alpha_1 + v\beta_1 \leqslant \cdots \leqslant \alpha_k + v\beta_k$. Let g a degree-d irreducible poynomial, with a root of valuation v.
If ℓ is the smallest index s.t.

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

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

- Depends on v.

Gap Theorem [G.'14]

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 $uv \neq 0$, $\alpha_1 + v\beta_1 \leqslant \cdots \leqslant \alpha_k + v\beta_k$. Let g a degree-d irreducible poynomial, with a root of valuation v.
If ℓ is the smallest index s.t.

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

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

- Depends on v.
- Does not bound α_j, nor β_j!

Gap Theorem [G.'14]

Let

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

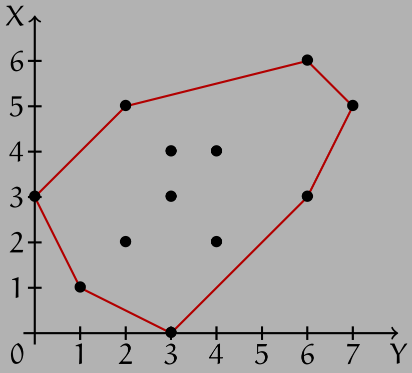
with $uv \neq 0$, $\alpha_1 + \nu\beta_1 \leqslant \cdots \leqslant \alpha_k + \nu\beta_k$. Let g a degree-d irreducible poynomial, with a root of valuation ν.
If ℓ is the smallest index s.t.

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

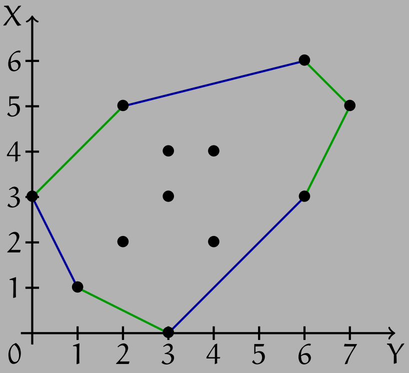
then g divides f iff it divides both f_1 and f_2.

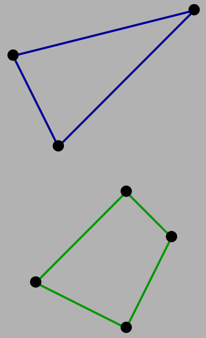
- Depends on ν.
- Does not bound α_j, nor β_j!
- Several distinct valuations needed.

Newton polygon



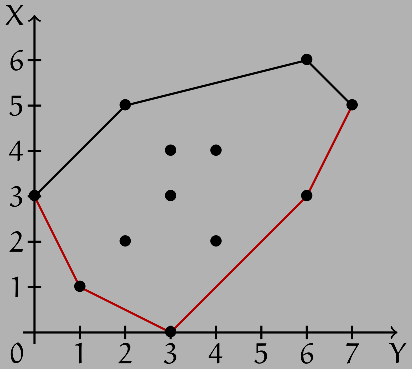
$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$



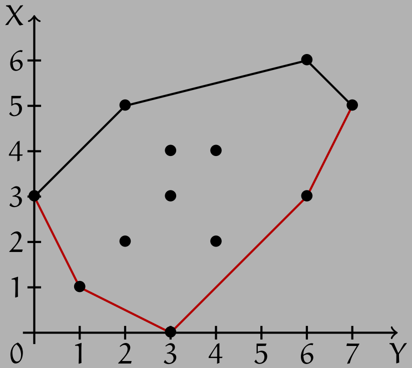


$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

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



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.



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.

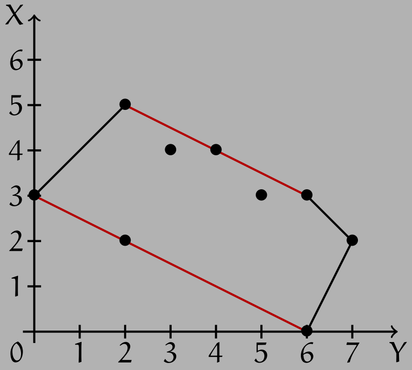
Two kinds of factors $g = \sum_j b_j X^{\gamma_j} Y^{\beta_j}$

- Quasi-homogeneous: $\exists\, p, q, \omega$ s.t. $p\gamma_j + q\beta_j = \omega$

  $\rightsquigarrow$ the Newton polygon is a line;

- Non-homogeneous

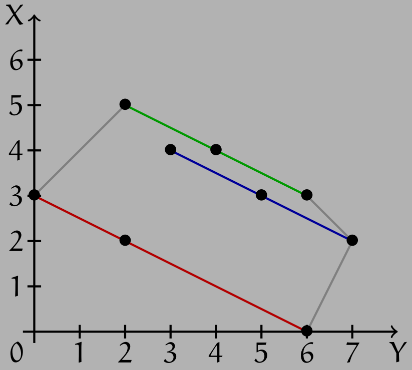
  $\rightsquigarrow$ the Newton polygon has at least two non-parallel edges.



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

(quasi-homogeneous with $p = 2$, $q = 1$, $\omega = 4$)

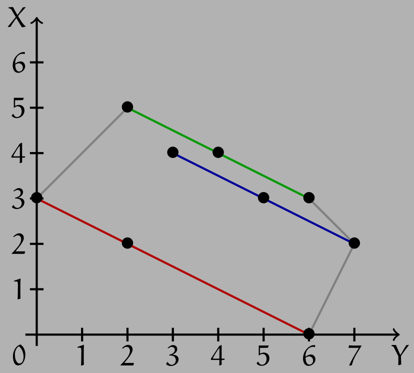
Quasi-homogeneous factors



- Write $f = f_1 + \cdots + f_s$ into quasi-homogeneous parts

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

(quasi-homogeneous with $p = 2$, $q = 1$, $\omega = 4$)

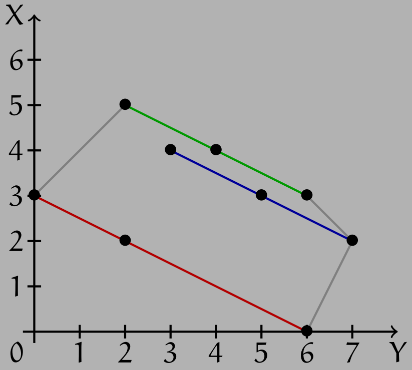


- Write $f = f_1 + \cdots + f_s$ into quasi-homogeneous parts
- g divides f iff it divides each f_t

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

(quasi-homogeneous with $p = 2$, $q = 1$, $\omega = 4$)

Quasi-homogeneous factors

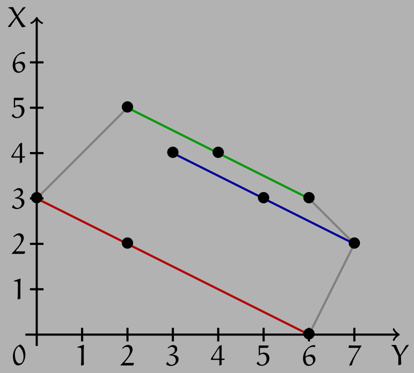


- Write $f = f_1 + \cdots + f_s$ into quasi-homogeneous parts
- g divides f iff it divides each f_t
- g divides $f_t \iff g(X^{1/q}, 1)$ divides $f_t(X^{1/q}, 1)$

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

(quasi-homogeneous with $p = 2$, $q = 1$, $\omega = 4$)

Quasi-homogeneous factors



- Write $f = f_1 + \cdots + f_s$ into quasi-homogeneous parts
- g divides f iff it divides each f_t
- g divides $f_t \iff g(X^{1/q}, 1)$ divides $f_t(X^{1/q}, 1)$

$\rightsquigarrow$ **univariate lacunary factorization**

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

(quasi-homogeneous with $p = 2$, $q = 1$, $\omega = 4$)

Proposition

Let $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$ and $\nu_1 \neq \nu_2$ such that for all j

$$\begin{cases} \alpha_j + \nu_1 \beta_j \leqslant \alpha_1 + \nu_1 \beta_1 + (2d(4d+1) - \nu_1)\binom{\ell}{2} \\ \alpha_j + \nu_2 \beta_j \leqslant \alpha_2 + \nu_2 \beta_2 + (2d(4d+1) - \nu_2)\binom{\ell}{2}. \end{cases}$$

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 $|\beta_p - \beta_q| \leqslant \mathcal{O}(\ell^2 d^4)$.

For all pair of non-parallel edges, of slopes v_1 and v_2:

- Write $f = f_1 + \cdots + f_s$, using both v_1 and v_2;
- Write $f_t = X^a Y^b f_t^\circ$ with $\deg(f_t^\circ) \leqslant \mathcal{O}(\ell^2 d^4)$;
- Factor each f_t°.

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 $|\beta_p - \beta_q| \leqslant \mathcal{O}(\ell^2 d^4)$.

For all pair of non-parallel edges, of slopes v_1 and v_2:

- Write $f = f_1 + \cdots + f_s$, using both v_1 and v_2;
- Write $f_t = X^a Y^b f_t^\circ$ with $\deg(f_t^\circ) \leqslant \mathcal{O}(\ell^2 d^4)$;
- Factor each f_t°.

$\rightsquigarrow$ **low-degree bivariate factorization**

- Multivariate polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$:

- Multivariate polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$:
  - For all $i \neq j$, consider $f \in R[X_i, X_j]$ where R is the ring of polynomials in the other variables;

- Multivariate polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$:
  - For all $i \neq j$, consider $f \in R[X_i, X_j]$ where R is the ring of polynomials in the other variables;
  - Apply the algorithm for the bivariate case;

- Multivariate polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$:
  - For all $i \neq j$, consider $f \in R[X_i, X_j]$ where R is the ring of polynomials in the other variables;
  - Apply the algorithm for the bivariate case;
  - Proceed carefully to avoid an exponential complexity in n.

- Multivariate polynomial $f \in \mathbb{K}[X_1, \dots, X_n]$:
  - For all $i \neq j$, consider $f \in R[X_i, X_j]$ where R is the ring of polynomials in the other variables;
  - Apply the algorithm for the bivariate case;
  - Proceed carefully to avoid an exponential complexity in n.
- Positive characteristic:

- Multivariate polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$:
  - For all $i \neq j$, consider $f \in R[X_i, X_j]$ where R is the ring of polynomials in the other variables;
  - Apply the algorithm for the bivariate case;
  - Proceed carefully to avoid an exponential complexity in n.
- Positive characteristic:
  - Puiseux series $\rightsquigarrow$ Hahn series;

Extensions

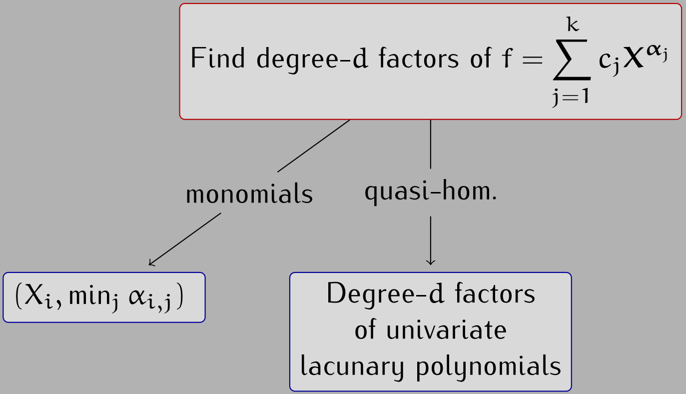
- Multivariate polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$:
  - For all $i \neq j$, consider $f \in R[X_i, X_j]$ where R is the ring of polynomials in the other variables;
  - Apply the algorithm for the bivariate case;
  - Proceed carefully to avoid an exponential complexity in n.
- Positive characteristic:
  - Puiseux series $\rightsquigarrow$ Hahn series;
  - Wronskian for Hahn series?

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

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

monomials

$(X_i, \min_j \alpha_{i,j})$



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

Complete algorithm

Find degree-d factors of $f = \sum_{j=1}^{k} c_j \mathbf{X}^{\boldsymbol{\alpha}_j}$

- **monomials** → $(X_i, \min_j \alpha_{i,j})$
- **quasi-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 $f_t = \sum_{j=j_t}^{j_t+\ell_t-1} c_j \mathbf{X}^{\boldsymbol{\alpha}_j}$ $(\deg(f_t) \leqslant \mathcal{O}(\ell_t^2 d^4))$
  - Low-degree factorization
  - $\mathbb{Q}(\alpha), \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$, etc.

Conclusion

Conclusion

- Computing low-degree factors of lacunary multivariate polynomials

Conclusion

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

- 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”

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

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**

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:

- 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?

- 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?
  - What can be done in **small positive characteristic**?

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?
  - What can be done in **small positive characteristic**?
  - More general settings: arithmetic circuits/straight-line programs

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?
  - What can be done in **small positive characteristic**?
  - More general settings: arithmetic circuits/straight-line programs

Thank you!