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

Bruno Grenet

LIRMM — Université Montpellier 2

JNCF — November 3., 2014

Factorization of a polynomial f

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

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** $\deg(f)$

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 $f_1, \dots, f_t$, 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** $\deg(f)$

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

Definition

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

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

Definition

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

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

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]

Definition

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

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

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]

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

Theorem

The computation of the degree-d factors of $f \in \mathbb{K}[X_1, \dots, X_n]$ reduces to

- univariate lacunary factorizations plus post-processing, and
- multivariate low-degree factorization,

in $\mathrm{poly}(\mathrm{size}(f), d)$ bit operations.

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

Theorem

The computation of the degree-d factors of $f \in \mathbb{K}[X_1, \dots, X_n]$ reduces to

- univariate lacunary factorizations plus post-processing, and
- multivariate low-degree factorization,

in $\mathrm{poly}(\mathrm{size}(f), d)$ bit operations.

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

The computation of the degree-d factors of $f \in \mathbb{K}[X_1, \dots, X_n]$ reduces to

- univariate lacunary factorizations plus post-processing, and
- multivariate low-degree factorization,

in $\mathrm{poly}(\mathrm{size}(f), d)$ bit operations.

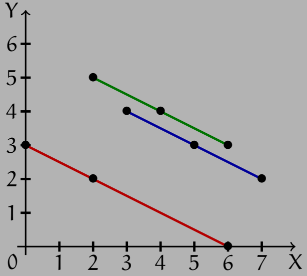
- New algorithm for $\mathbb{K} = \mathbb{Q}(\alpha)$; **some** factors for $\mathbb{K} = \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$
- Case $d = 1$ [G.-Chattopadhyay-Koiran-Portier-Strozecki'13]

Definition

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.
Otherwise, g is said **inhomogeneous**.

Definition

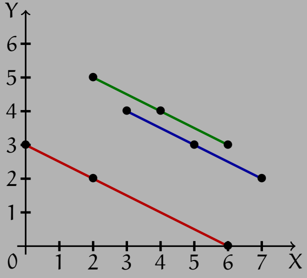
A polynomial $g = \sum_j b_j X^{\gamma_j} Y^{\delta_j}$ is (p, q)-**homogeneous** of order ω if $p\gamma_j + q\delta_j = \omega$ for all j.
Otherwise, g is said **inhomogeneous**.



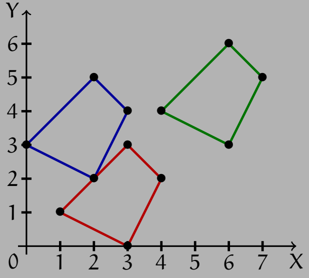
Univariate lacunary factorization

Definition

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.
Otherwise, g is said **inhomogeneous**.

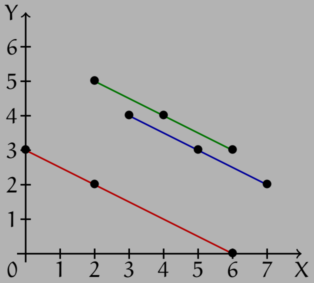


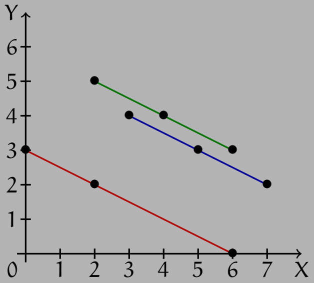
Univariate lacunary factorization



Multivariate low-degree factorization

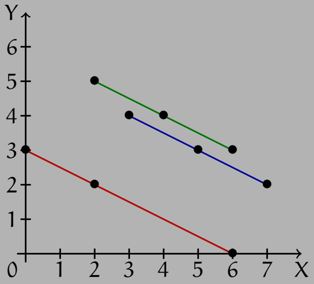
Weighted-homogeneous factors





Reduction to the univariate case

If f, g are (p, q)-homogeneous, g divides f $\iff$ $g(X^{1/q}, 1)$ divides $f(X^{1/q}, 1)$



Reduction to the univariate case

If f, g are (p,q)-homogeneous,
g divides $f \iff$
$g(X^{1/q}, 1)$ divides $f(X^{1/q}, 1)$

For all *possible* pairs (p,q):

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

- Weighted-homogeneous factors ⇝ **Unidimensional factors**:

$$\exists \tilde{g} \in \mathbb{K}[Z] \text{ s.t. } g(X_1, \dots, X_n) = \mathbf{X}^{\gamma} g(\mathbf{X}^{\delta})$$

- Weighted-homogeneous factors $\rightsquigarrow$ **Unidimensional factors**:

$$\exists \tilde{g} \in \mathbb{K}[Z] \text{ s.t. } g(X_1, \dots, X_n) = \mathbf{X}^\gamma g(\mathbf{X}^\delta)$$

For all pairs of monomials $(\mathbf{X}^{\alpha_1}, \mathbf{X}^{\alpha_2})$:

1. Write $f = f_1 + \cdots + f_s$ as a sum of unidimensional polynomials;
2. Compute the degree-d factors of the $\tilde{f}_t$'s;
   $\rightsquigarrow$ **univariate lacunary factorization**
3. Return $\mathbf{X}^\gamma g(\mathbf{X}^\delta)$ for each factor g.

Linear factors of bivariate polynomials

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

Observation

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

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

Observation

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

Theorem

$$\operatorname{val}\left(\sum_{j=1}^{\ell} c_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leqslant \alpha_1 + \binom{\ell}{2} \text{ if nonzero and } uv \neq 0.$$

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

Observation

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

Theorem

$$\operatorname{val}\left(\sum_{j=1}^{\ell} c_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leqslant \alpha_1 + \binom{\ell}{2} \text{ if nonzero and } uv \neq 0.$$

Gap Theorem

Suppose that $f = f_1 + f_2$ with $\operatorname{val}_X(f_2) > \operatorname{val}_X(f_1) + \binom{\ell(f_1)}{2}$. Then for all $uv \neq 0$, $(Y-uX-v)$ divides f iff it divides both f_1 and f_2.

Observation for low-degree factors

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

Observation for low-degree factors

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

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X)) \in \overline{\mathbb{K}(X)}[Y]$$

Observation for low-degree factors

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

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X)) \in \overline{\mathbb{K}(X)}[Y]$$

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

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

Observation for low-degree factors

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

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X)) \in \overline{\mathbb{K}(X)}[Y]$$

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

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

- If g is irreducible,

$$g \text{ divides } f \iff \exists i,\ f(X,\phi_i) = 0 \iff \forall i,\ f(X,\phi_i) = 0$$

Theorem

Let $\phi \in \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ of valuation ν, g of degree d s.t. $g(X, \phi(X)) = 0$, and $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$.

If the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent,

$$\operatorname{val}(f_1(X, \phi)) \leqslant \min_j(\alpha_j + \nu\beta_j) + (8d^2 - \nu)\binom{\ell}{2}.$$

Theorem

Let $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν, g of degree d s.t. $g(X, \phi(X)) = 0$, and $f_1 = \sum_{j=1}^{\ell} c_j X^{\alpha_j} Y^{\beta_j}$.

If the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent,

$$\mathrm{val}(f_1(X, \phi)) \leqslant \min_j(\alpha_j + \nu\beta_j) + (8d^2 - \nu)\binom{\ell}{2}.$$

- Proof based on the *Wronskian* of the family $(X^{\alpha_j}\phi^{\beta_j})_j$.
- Optimality?

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 polynomial, with a root of valuation ν.

If ℓ is the smallest index s.t.

$$\alpha_{\ell+1} + \nu\beta_{\ell+1} > (\alpha_1 + \nu\beta_1) + (8d^2 - \nu)\binom{\ell}{2},$$

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 polynomial, with a root of valuation ν.

If ℓ is the smallest index s.t.

$$\alpha_{\ell+1} + \nu\beta_{\ell+1} > (\alpha_1 + \nu\beta_1) + (8d^2 - \nu)\binom{\ell}{2},$$

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 (neither α_j nor β_j)

Gap Theorem for inhomogeneous factors

Let

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

where ℓ is the largest index s.t. for $1 \leqslant i, j \leqslant \ell$,

$$|\alpha_i - \alpha_j|, |\beta_i - \beta_j| \leqslant (4d^4 + 2d^2)\binom{\ell - 1}{2}.$$

Then every **degree-d inhomogeneous** $g \in \mathbb{K}[X, Y]$,

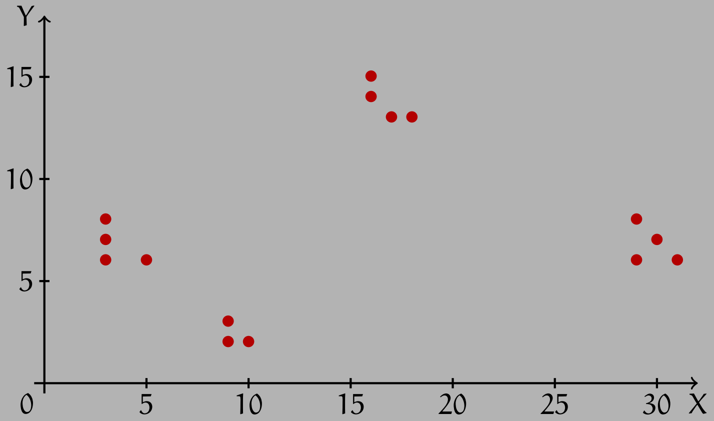
$$\mathrm{mult}_g(f) = \min(\mathrm{mult}_g(f_1), \mathrm{mult}_g(f_2)).$$

An example with $d = 1$

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

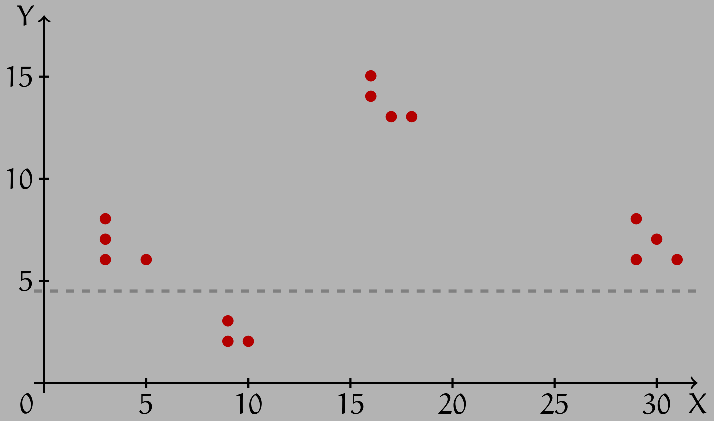
An example with $\mathrm{d} = 1$

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



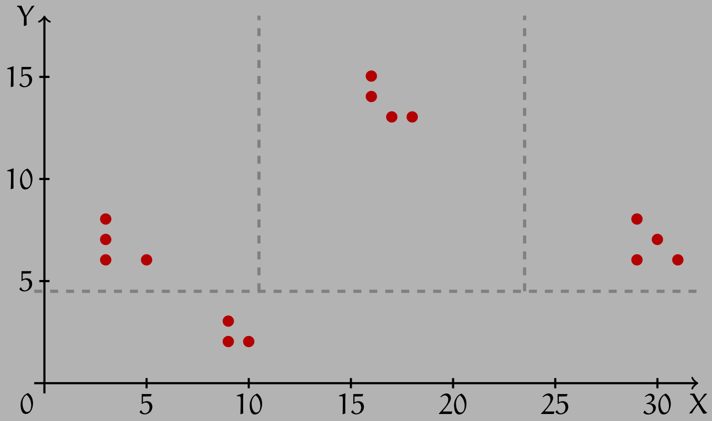
An example with $\mathrm{d} = 1$

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



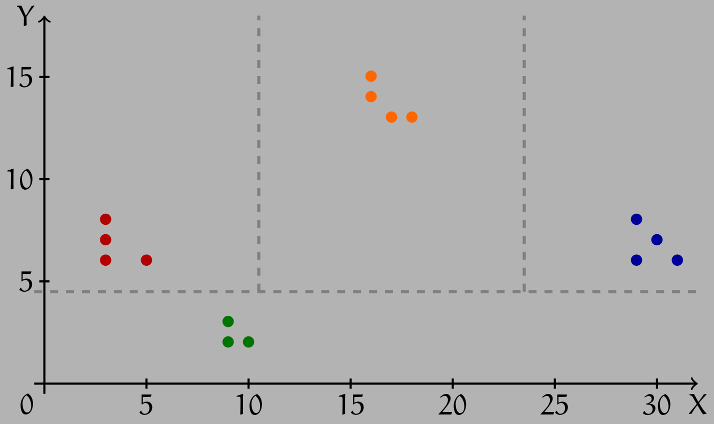
An example with $\mathrm{d} = 1$

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



An example with $d = 1$

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



An example with $d = 1$

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

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

An example with $d = 1$

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

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

An example with $\mathrm{d} = 1$

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

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

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

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

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

An example with $d = 1$

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

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

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

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

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

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

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

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

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

Theorem

Given $f \in \mathbb{K}[X, Y]$ in lacunary representation, one can compute in time $\mathrm{poly}(\mathrm{size}(f), d)$ a degree-$O(d^4k^2)$ polynomial f_{ld} s.t. for all inhomogeneous degree-d polynomial g,

$$\mathrm{mult}_g(f) = \mathrm{mult}_g(f_{ld}).$$

Theorem

Given $f \in \mathbb{K}[X_1, \ldots, X_n]$ in lacunary representation, one can compute in time $\mathrm{poly}(\mathrm{size}(f), d)$ a degree-$O(d^4k^2)$ polynomial f_{ld} s.t. for all inhomogeneous degree-d polynomial g,

$$\mathrm{mult}_g(f) = \mathrm{mult}_g(f_{\mathrm{ld}}).$$

Theorem

Given $f \in \mathbb{K}[X_1, \dots, X_n]$ in lacunary representation, one can compute in time $\mathrm{poly}(\mathrm{size}(f), d)$ a degree-$O(d^4k^2)$ polynomial f_{ld} s.t. for all inhomogeneous degree-d polynomial g,

$$\mathrm{mult}_g(f) = \mathrm{mult}_g(f_{ld}).$$

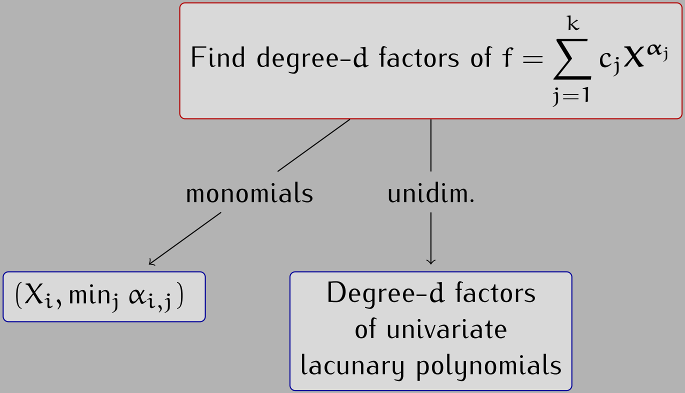
1. Write $f = f_1 + \cdots + f_s$ where $\deg_{X_i}(f_t) - \mathrm{val}_{X_i}(f_t) \leqslant (4d^4 - 2d^2)\binom{\ell_t}{2}$ for all i;
2. Return $\gcd(f_1, \dots, f_t)$.
3. (Factor the gcd using a low-degree factorization algorithm.)

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

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

monomials

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



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

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

- **monomials** → $(X_i, \min_j \alpha_{i,j})$
- **unidim.** → Degree-d factors of univariate lacunary polynomials
  - Available for $\mathbb{Q}(\alpha)$ only
  - Impossible for $\overline{\mathbb{Q}}$, $\mathbb{C}$
- **multidim.** → Factors of f_{ld} of degree $\leqslant O(d^4k^2)$
  - Low-degree factorization
  - $\mathbb{Q}(\alpha), \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$, etc.

`http://www.mathemagix.org/ > Packages > Lacunaryx`

Factorization-related algorithms for lacunary polynomials

- Integer roots of lacunary univariate polynomials
- Linear factors of lacunary univariate and bivariate polynomials
- Bounded-degree factors: in progress
- Very large degree polynomials (G. Lecerf)

```
Mmx] use "lacunaryx"; x : LPolynomial Integer == lpolynomial(1,1);
     p == x^3*(x-2)*(2*x+3)^2*(-x+3)*(2*x+7)*(x^2+x+1)*(3*x+5);
     q == x^3 - 6 - 2*x^4 + 12*x + x^5 - 6*x^2+ 3*x^1345 - 6*x^1346 + 3*x^1347 +
          8*x^432534 - 18*x^432535 + 12*x^432536 - 2*x^432537 + 1 - 2*x + x^2;
     e : Integer == 35154014504040115230143514;
     r == 1 + 3*x^1345 - 2*(x-4)*x^e + (x^3-6)*x^(2*e);
     pqr == p*q*r; (log deg pqr/log 2, #pqr)
```

$(85.861891823199, 149)$

49 msec

```
Mmx] roots pqr
```

$[[2, 1], [3, 1], [0, 3], [1, 2]]$

43 msec

```
Mmx] X == coordinate ('x); x : LMVPolynomial Integer == lmvpolynomial(1, X);
     Y == coordinate ('y); y : LMVPolynomial Integer == lmvpolynomial(1, Y);
     f == x^2*y*(x-2)*(2*y+3)^2*(y-x+3)*(2*x+7*y)*(x*y+x+1)*(3*x-6*y+5);
     g == x^3*y^54354165 - 6*y^54354165 - 2*x^4*y^54354164 + 12*x*y^54354164
     + x^5*y^54354163 - 6*x^2*y^54354163 + 3*x^1345*y^54336 - 6*x^1346*y^54335
     + 3*x^1347*y^54334 + 8*x^432534*y^5 - 18*x^432535*y^4 + 12*x^432536*y^3 -
     2*x^432537*y^2 + y^2 - 2*x*y + x^2;
     h == 1 + 3*x^1345*y^54334 - 2*(x-4*y)*x^e*y^2 + (x^3-6)*y^(2*e);
     fgh == f*g*h; (log deg fgh/log 2, #fgh)
```

$(85.861891823199, 1028)$

60 msec

```
Mmx] linear_factors fgh
```

$[[x, 2], [-x+2, 1], [y, 1], [2\,y+3, 2], [-y+x, 2], [-7\,y-2\,x, 1], [-y+x-3, 1], [-6\,y+3\,x+5, 1]]$

299 msec

- 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:
  - **Lacunary factors** in polynomial time?
  - More general settings: SLP/arithmetic circuits

- 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:
  - **Lacunary factors** in polynomial time?
  - More general settings: SLP/arithmetic circuits
  - Degree-d factors in **positive characteristic**?
  - **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:
  - **Lacunary factors** in polynomial time?
  - More general settings: SLP/arithmetic circuits

  - Degree-d factors in **positive characteristic**?
  - **Small positive characteristic**?

Thank you!