Factoring lacunary polynomials: the easy way

Bruno Grenet
LIX — École Polytechnique

Joint work with

Arkadev Chattopadhyay
TIFR, Mumbai

Pascal Koiran
ÉNS Lyon

Natacha Portier
ÉNS Lyon

Yann Strozecki
U. Versailles

Rencontres du GT CoA — Paris

November 19, 2013

Classical factorization algorithms

Factorization of a polynomial P

Find $F_1, \ldots, F_t$, irreducible, s.t. $P = F_1 \times \cdots \times F_t$.

Classical factorization algorithms

Factorization of a polynomial P

Find $F_1, \ldots, F_t$, irreducible, s.t. $P = F_1 \times \cdots \times F_t$.

$$\mathbb{Z}[X]$$

[Lenstra-Lenstra-Lovász'82]

$$\downarrow$$

$$\mathbb{Q}(\alpha)[X]$$

[A. Lenstra'83, Landau'83]

$$\downarrow$$

$$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$$

[Kaltofen'85, A. Lenstra'87]

Classical factorization algorithms

Factorization of a polynomial P

Find $F_1, \ldots, F_t$, irreducible, s.t. $P = F_1 \times \cdots \times F_t$.

$\mathbb{Z}[X]$

[Lenstra-Lenstra-Lovász'82]

↓

$\mathbb{Q}(\alpha)[X]$

[A. Lenstra'83, Landau'83]

↓

$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$

[Kaltofen'85, A. Lenstra'87]

$\mathbb{F}_q[X]$

[Berlekamp'67]

↓

$\mathbb{F}_q[X_1, \ldots, X_n]$

Classical factorization algorithms

Factorization of a polynomial P

Find $F_1, \ldots, F_t$, irreducible, s.t. $P = F_1 \times \cdots \times F_t$.

$\mathbb{Z}[X]$

[Lenstra-Lenstra-Lovász'82]

$\downarrow$

$\mathbb{Q}(\alpha)[X]$

$\mathbb{F}_q[X]$

[Berlekamp'67]

Complexity

Polynomial in the **degree** of the polynomials

$\downarrow$

$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$

[Kaltofen'85, A. Lenstra'87]

Lacunary polynomials

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

Lacunary polynomials

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

Lacunary polynomials

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

Lacunary polynomials

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

Definition

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

Lacunary polynomials

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

Definition

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

- Lacunary representation: list of nonzero monomials
- $\text{size}(P) \simeq \sum_j \text{size}(a_j) + \log(\alpha_{1j}) + \cdots + \log(\alpha_{nj})$

Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{Q} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{R} \in \mathbb{Z}[X]$$

with $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_k$. Suppose that

$$\alpha_{\ell+1} - \alpha_\ell > 1 + \log\left(\max_{j \leqslant \ell} |a_j|\right),$$

then for all $x \in \mathbb{Z}$, $|x| \geqslant 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

Integral roots of integral polynomials

Gap Theorem [Cucker-Koiran-Smale'98]

Let
$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{Q} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{R} \in \mathbb{Z}[X]$$

with $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_k$. Suppose that

$$\alpha_{\ell+1} - \alpha_\ell > 1 + \log\left(\max_{j \leqslant \ell} |a_j|\right),$$

then for all $x \in \mathbb{Z}$, $|x| \geqslant 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

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

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$;

[Cucker-Koiran-Smale'98]

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$;

  [Cucker-Koiran-Smale'98]

- **low-degree** factors of **univariate** polynomials over $\mathbb{Q}(\alpha)$;

  [H. Lenstra'99]

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial-time algorithms computing

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$;

  [Cucker-Koiran-Smale'98]

- **low-degree** factors of **univariate** polynomials over $\mathbb{Q}(\alpha)$;

  [H. Lenstra'99]

- **low-degree** factors of **multivariate** polynomials over $\mathbb{Q}(\alpha)$.

  [Kaltofen-Koiran'05 & '06]

Linear factors of bivariate polynomials

Observation

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

Observation

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

Gap Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}}_{Q} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} (uX + v)^{\beta_j}}_{R}$$

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

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

then $P \equiv 0$ iff both $Q \equiv 0$ and $R \equiv 0$.

Bound on the valuation

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

Definition

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

Bound on the valuation

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

Definition

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

Theorem

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

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

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

Bound on the valuation

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

Definition

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

Theorem

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

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

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

- Hajós' Lemma: if $\alpha_1 = \cdots = \alpha_\ell$, $\mathrm{val}(P) \leqslant \alpha_1 + (\ell - 1)$

Definition

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

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

Definition

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

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

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

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

Lemma

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

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

Lemma

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

Lemma

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

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

Proof of the theorem. $\operatorname{wr}(P, f_2, \dots, f_\ell) = a_1 \operatorname{wr}(f_1, \dots, f_\ell)$

Lemma

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

Lemma

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

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

Proof of the theorem. $\operatorname{wr}(P, f_2, \dots, f_\ell) = a_1 \operatorname{wr}(f_1, \dots, f_\ell)$

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

How tight is the bound?

- Hajós' Lemma: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \leqslant \alpha + (\ell - 1)$

How tight is the bound?

- Hajós' Lemma: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \geqslant \alpha + (\ell - 1)$
- Our result: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \geqslant \alpha_1 + \binom{\ell}{2}$

How tight is the bound?

- Hajós' Lemma: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \geqslant \alpha + (\ell - 1)$
- Our result: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \geqslant \alpha_1 + \binom{\ell}{2}$
- Lemmas: bounds attained, but not simultaneously

How tight is the bound?

- Hajós' Lemma: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \geqslant \alpha + (\ell-1)$
- Our result: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \geqslant \alpha_1 + \binom{\ell}{2}$
- Lemmas: bounds attained, but not simultaneously
- $(1+X)^{2\ell-3} - 1 - \sum_{j=3}^{\ell} \frac{2\ell-3}{2j-5}\binom{\ell+j-5}{2j-6} X^{2j-5}(1+X)^{\ell-1-j} = X^{2\ell-3}$

Observation + Gap Theorem (recursively)

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

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

Observation + Gap Theorem (recursively)

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

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

$$\iff P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0$$

Observation + Gap Theorem (recursively)

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

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

$$\iff P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0$$

$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$

Observation + Gap Theorem (recursively)

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

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

$$\iff P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0$$

$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$

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

Observation + Gap Theorem (recursively)

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

$$\iff P(X, uX + v) \equiv 0$$
$$\iff P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0$$
$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$

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

Observation + Gap Theorem (recursively)

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

$$\iff P(X, uX + v) \equiv 0$$
$$\iff P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0$$
$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$

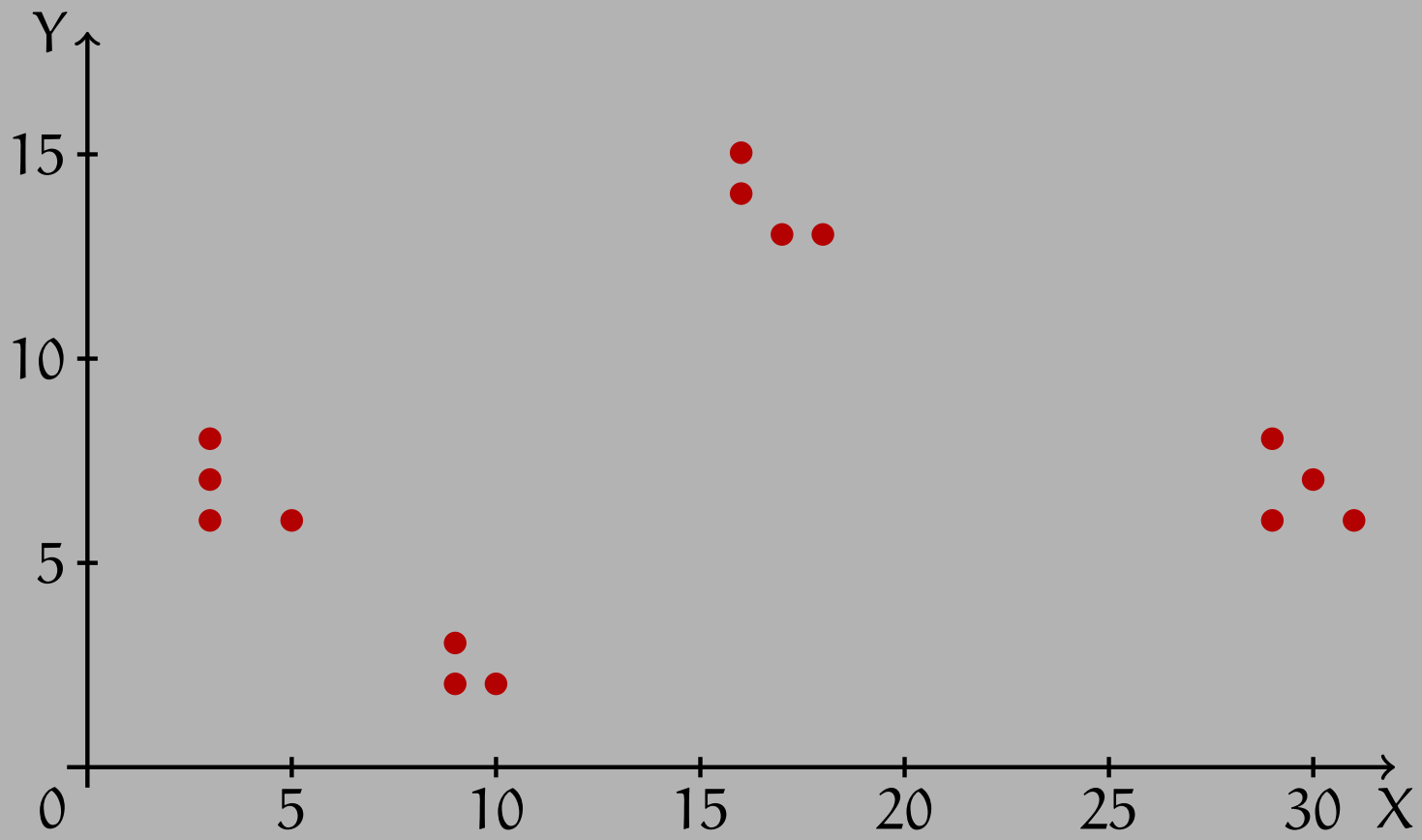
- $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leqslant \binom{\ell_t}{2}$
- Independent from u and v
- X does not play a special role

Example

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

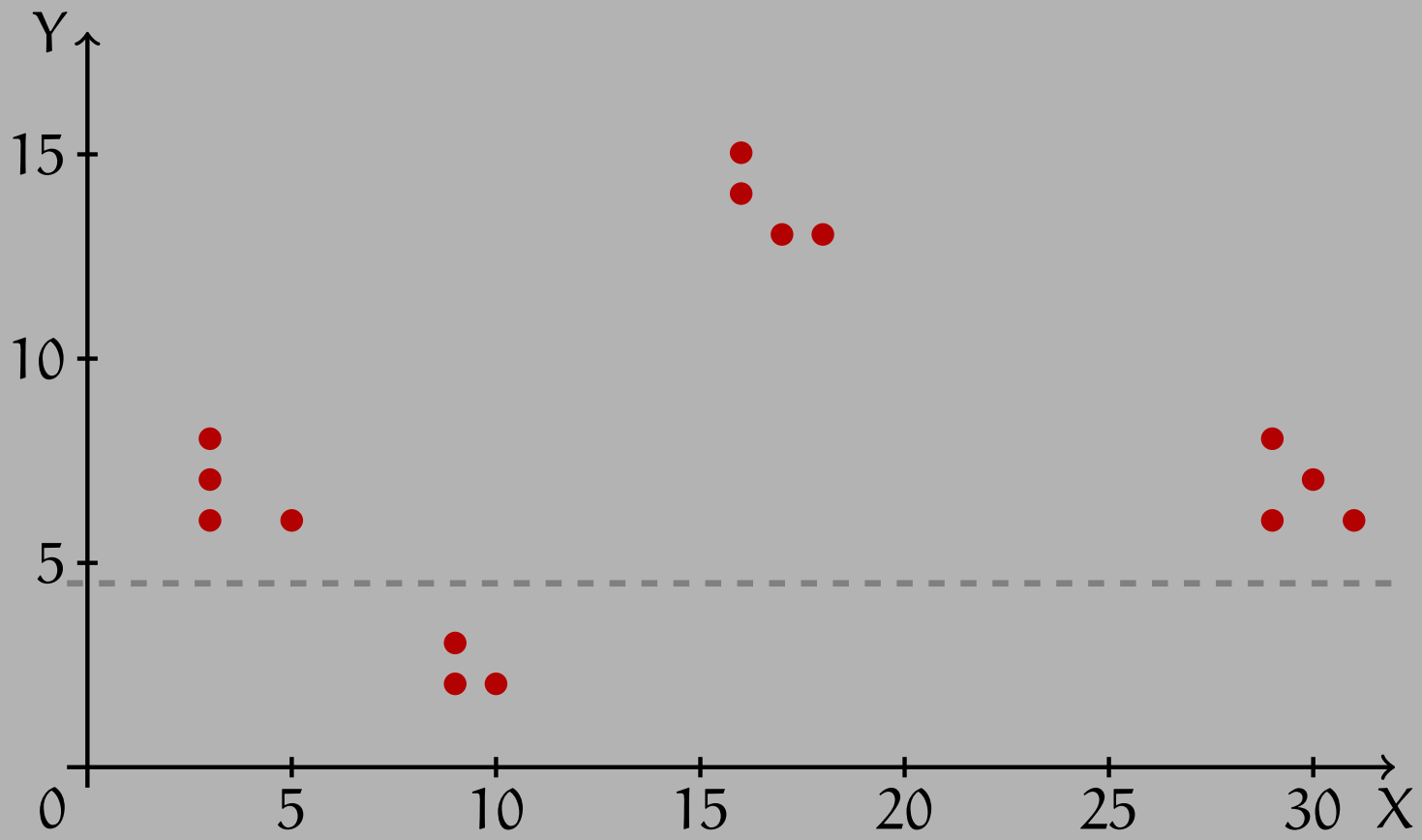
Example

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



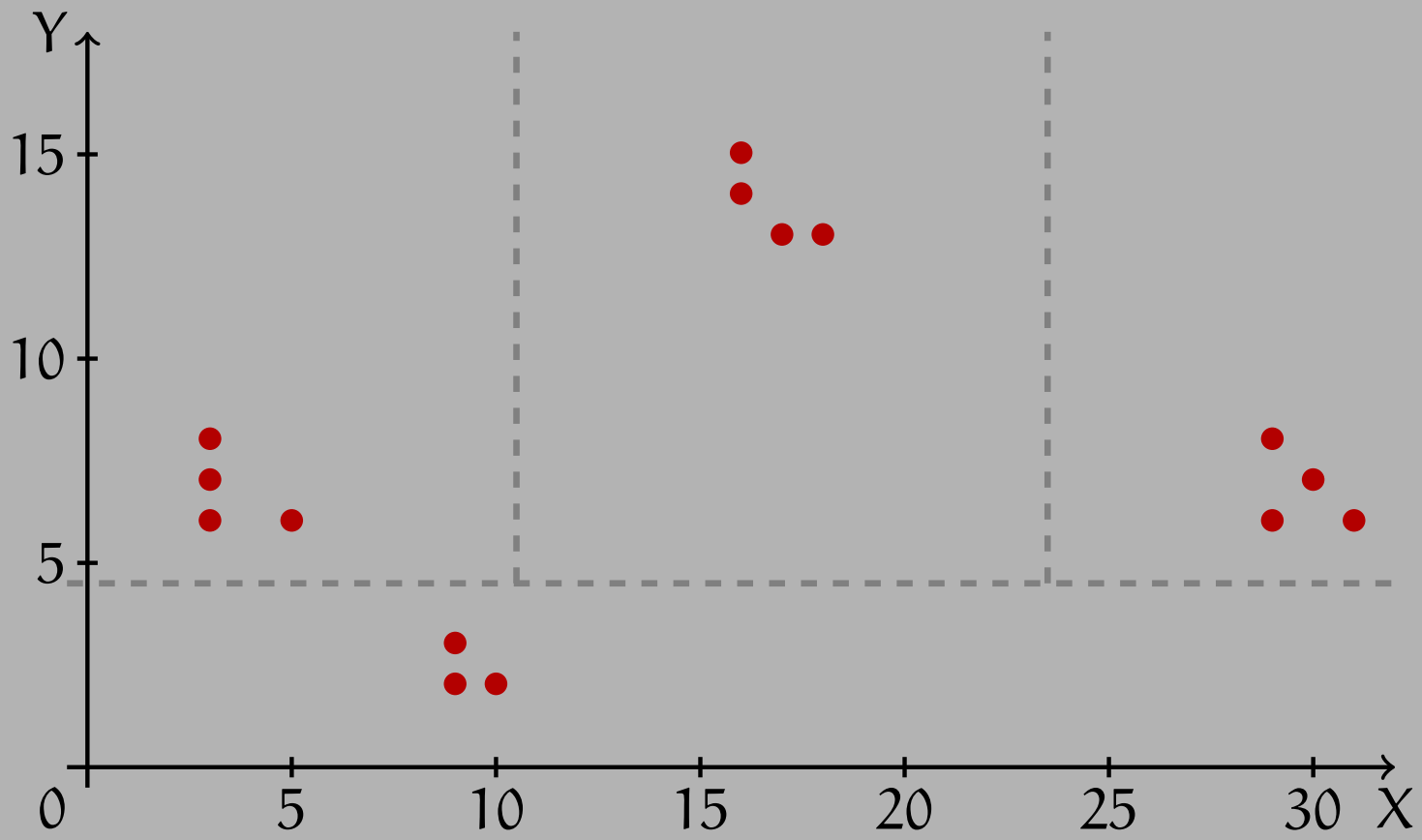
Example

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



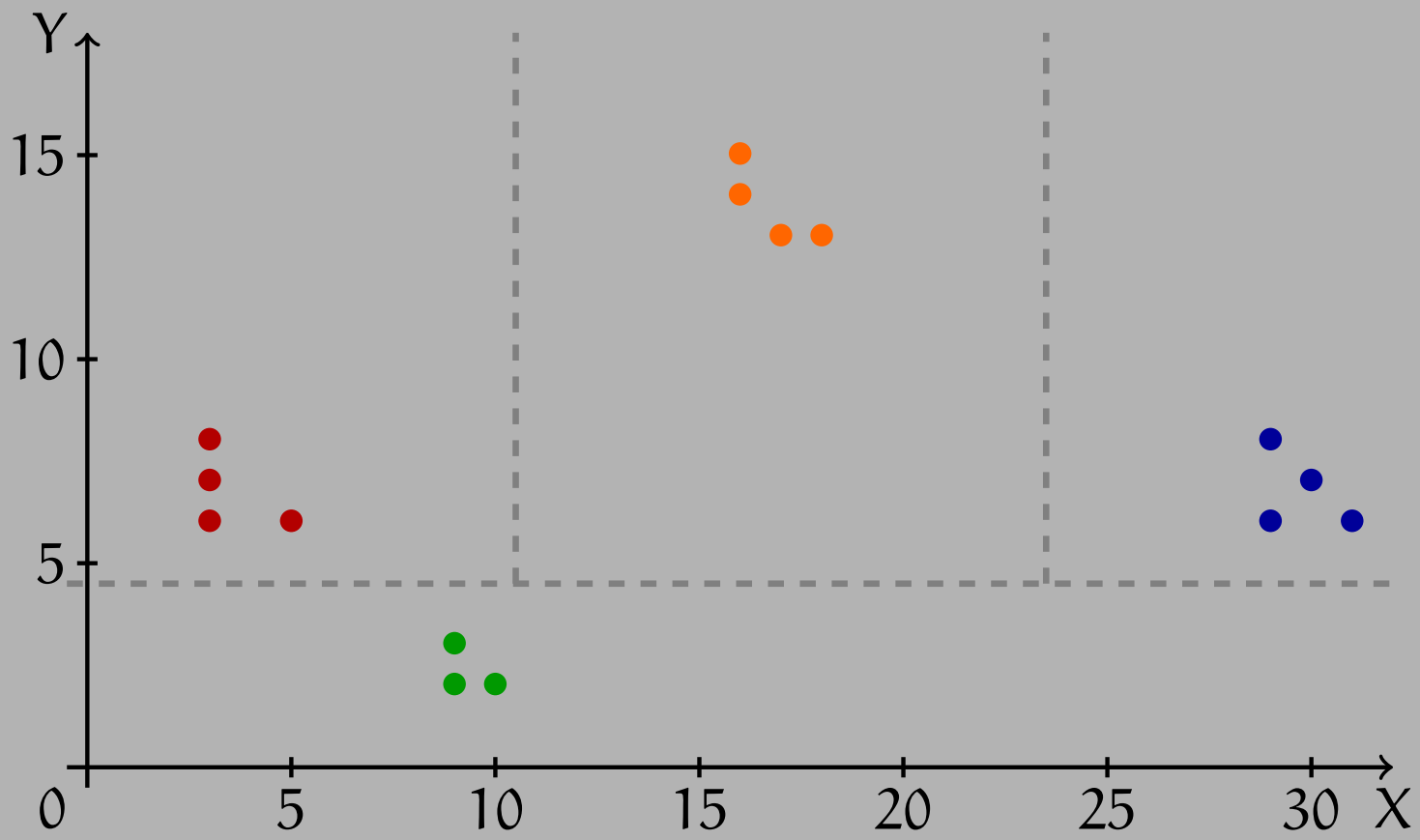
Example

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



Example

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



Example

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

$$P_1 = X^3Y^6(-X^2 + Y^2 - 2Y + 1)$$

Example

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

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

Example

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

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$
$$P_2 = X^9Y^2(X - Y + 1)$$
$$P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$
$$P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

Example

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

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$
$$P_2 = X^9Y^2(X - Y + 1)$$
$$P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$
$$P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

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

Example

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

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$
$$P_2 = X^9Y^2(X - Y + 1)$$
$$P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$
$$P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

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

Complete algorithm

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

Complete algorithm

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

monomials

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

Complete algorithm

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

monomials

trinomials

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

Common factors of
$P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$
$(\deg(P_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization
[Kaltofen'82, ..., Lecerf'07]

Complete algorithm

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

monomials | binomials | trinomials

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

$$\frac{(X-a)}{\text{Factors of } \sum_j a_j X^{\alpha_j}} \qquad \frac{(Y-uX)}{\text{Roots of } u \mapsto \sum_j a_j u^{\beta_j}}$$

Univariate lacunary factorization
[H. Lenstra'99]

Common factors of
$$P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$$
$(\deg(P_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization
[Kaltofen'82, ..., Lecerf'07]

Complete algorithm

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

monomials | binomials | trinomials

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

$$\frac{(X - a)}{(Y - uX)}$$
Factors of $\sum_j a_j X^{\alpha_j}$
Roots of $u \mapsto \sum_j a_j u^{\beta_j}$

Univariate lacunary factorization
[H. Lenstra'99]

Common factors of
$$P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$$
$(\deg(P_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization
[Kaltofen'82, ..., Lecerf'07]

Extensions

- **Multilinear** factors, with a new Gap Theorem;

Extensions

- **Multilinear** factors, with a new Gap Theorem;
- **Multivariate** polynomials: Apply the Gap Theorem for $P \in \mathbb{K}(X_3, \ldots, X_n)[X_1, X_2]$;

Extensions

- **Multilinear** factors, with a new Gap Theorem;
- **Multivariate** polynomials: Apply the Gap Theorem for $P \in \mathbb{K}(X_3, \ldots, X_n)[X_1, X_2]$;
- Multilinear factors with $\geqslant 3$ monomials over
  - $\overline{\mathbb{Q}}$: absolute factorization;
  - $\mathbb{R}$, $\mathbb{C}$: approximate factorization;
  - ...

Extensions

- **Multilinear** factors, with a new Gap Theorem;
- **Multivariate** polynomials: Apply the Gap Theorem for $P \in \mathbb{K}(X_3, \ldots, X_n)[X_1, X_2]$;
- Multilinear factors with $\geqslant 3$ monomials over
  - $\overline{\mathbb{Q}}$: absolute factorization;
  - $\mathbb{R}$, $\mathbb{C}$: approximate factorization;
  - ...
- **Low-degree** factors:

Extensions

- **Multilinear** factors, with a new Gap Theorem;
- **Multivariate** polynomials: Apply the Gap Theorem for $P \in \mathbb{K}(X_3, \ldots, X_n)[X_1, X_2]$;
- Multilinear factors with $\geqslant 3$ monomials over
  - $\overline{\mathbb{Q}}$: absolute factorization;
  - $\mathbb{R}$, $\mathbb{C}$: approximate factorization;
  - ...
- **Low-degree** factors:
  - F divides P iff $P(X, \phi) = 0$ where $\phi = \sum_{t \geqslant \nu} c_t X^{t/d}$ is a Puiseux series

Extensions

- **Multilinear** factors, with a new Gap Theorem;
- **Multivariate** polynomials: Apply the Gap Theorem for $P \in \mathbb{K}(X_3, \ldots, X_n)[X_1, X_2]$;
- Multilinear factors with $\geqslant 3$ monomials over
  - $\overline{\mathbb{Q}}$: absolute factorization;
  - $\mathbb{R}$, $\mathbb{C}$: approximate factorization;
  - ...
- **Low-degree** factors:
  - F divides P iff $P(X, \phi) = 0$ where $\phi = \sum_{t \geqslant \nu} c_t X^{t/d}$ is a Puiseux series
  - $\mathrm{val}(P(X, \phi)) \leqslant \alpha_1 + O(\delta_F^2)\binom{\ell}{2}$

Extensions

- **Multilinear** factors, with a new Gap Theorem;
- **Multivariate** polynomials: Apply the Gap Theorem for $P \in \mathbb{K}(X_3, \ldots, X_n)[X_1, X_2]$;
- Multilinear factors with $\geqslant 3$ monomials over
  - $\overline{\mathbb{Q}}$: absolute factorization;
  - $\mathbb{R}$, $\mathbb{C}$: approximate factorization;
  - ...
- **Low-degree** factors:
  - F divides P iff $P(X, \phi) = 0$ where $\phi = \sum_{t \geqslant \nu} c_t X^{t/d}$ is a Puiseux series
  - $\mathrm{val}(P(X, \phi)) \leqslant \alpha_1 + O(\delta_F^2)\binom{\ell}{2}$
  - Many details to fix $\rightsquigarrow$ work in progress!

- Valuation bound valid for **large** characteristics

$$\text{Find multilinear factors of } P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$
$$\text{where } a_j \in \mathbb{F}_{p^s} \text{ and } p > \deg(P)$$

- Valuation bound valid for **large** characteristics

Find multilinear factors of $P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$

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

monomials

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

$(\geqslant 3)$-nomials

Common factors of $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j}$

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

Low-degree factorization

[Gao'03, Lecerf'10]

- Valuation bound valid for **large** characteristics

Find multilinear factors of $P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$

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

monomials

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

binomials

$(uX^\beta - vX^\gamma)$

$\Updownarrow$

Roots of univariate lacunary polynomials

$(\geqslant 3)$-nomials

Common factors of $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j}$

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

Low-degree factorization

[Gao'03, Lecerf'10]

- Valuation bound valid for **large** characteristics

Find multilinear factors of $P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$

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

monomials

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

binomials

$(uX^{\beta} - $

P variate

la g polynomials

NP-complete under BPP reductions

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

$(\geqslant 3)$-nomials

Common factors of $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j}$

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

Low-degree factorization

[Gao'03, Lecerf'10]

Conclusion

- Multilinear factors of lacunary multivariate polynomials:

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Fields of characteristic 0;
    - Large positive characteristic.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Fields of characteristic 0;
    - Large positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Number fields only;
    - NP-hard in positive characteristic.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Fields of characteristic 0;
    - Large positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Number fields only;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Fields of characteristic 0;
    - Large positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Number fields only;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation.
- PIT algorithms for $\sum_j a_j \prod_i f_i^{\alpha_{ij}}$, $\sum_j a_j X^{\alpha_j} (uX^d + v)^{\beta_j}$.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Fields of characteristic 0;
    - Large positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Number fields only;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation.
- PIT algorithms for $\sum_j a_j \prod_i f_i^{\alpha_{ij}}$, $\sum_j a_j X^{\alpha_j} (uX^d + v)^{\beta_j}$.
- Extensions: Low-degree/lacunary factors, small characteristic.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Fields of characteristic 0;
    - Large positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Number fields only;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation.
- PIT algorithms for $\sum_j a_j \prod_i f_i^{\alpha_{ij}}$, $\sum_j a_j X^{\alpha_j} (uX^d + v)^{\beta_j}$.
- Extensions: Low-degree/lacunary factors, small characteristic.
- Correct bound for the valuation?

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Fields of characteristic 0;
    - Large positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Number fields only;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation.
- PIT algorithms for $\sum_j a_j \prod_i f_i^{\alpha_{ij}}$, $\sum_j a_j X^{\alpha_j} (uX^d + v)^{\beta_j}$.
- Extensions: Low-degree/lacunary factors, small characteristic.
- Correct bound for the valuation?

Thank you!