Factoring bivariate lacunary polynomials without heights

Bruno Grenet
ÉNS Lyon & U. Rennes 1

Joint work with

Arkadev Chattopadhyay
TIFR, Mumbai

Pascal Koiran
ÉNS Lyon

Natacha Portier
ÉNS Lyon

Yann Strozecki
U. Versailles

ISSAC 2013 — Boston

June 29, 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]

$\downarrow$

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

Complexity

Polynomial in the **degree** of the polynomials

$\downarrow$

$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$
[Kaltofen'85, A. Lenstra'87]

$\mathbb{F}_q[X]$
[Berlekamp'67]

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

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

Lacunary polynomials

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

- Algorithms polynomial in $\log(\deg(P))$

Lacunary polynomials

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

- Algorithms polynomial in $\log(\deg(P))$
- Some factors only

Lacunary polynomials

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

- Algorithms polynomial in $\log(\deg(P))$
- Some factors only

Definition

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

Lacunary polynomials

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

- Algorithms polynomial in $\log(\deg(P))$
- Some factors only

Definition

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

- Lacunary representation: $\{(\alpha_{1j}, \ldots, \alpha_{nj} : a_j) : 1 \leqslant j \leqslant k\}$

Lacunary polynomials

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

- Algorithms polynomial in $\log(\deg(P))$
- Some factors only

Definition

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

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

Factorization of lacunary polynomials

Theorems

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$;
  [Cucker-Koiran-Smale'98]

Factorization of lacunary polynomials

Theorems

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

- **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

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

- **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]

- **linear** factors of **bivariate** polynomials over $\mathbb{Q}$;

  [Kaltofen-Koiran'05]

Factorization of lacunary polynomials

Theorems

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

- **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]
- **linear** factors of **bivariate** polynomials over $\mathbb{Q}$;
  [Kaltofen-Koiran'05]
- **low-degree** factors of **multivariate** polynomials over $\mathbb{Q}(\alpha)$.
  [Kaltofen-Koiran'06]

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

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

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

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

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

$$(-9 + X^2) \searrow -3 \swarrow (6 + 2X)$$

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

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

$$\searrow \quad \swarrow$$

-3 + check 0, 1 and -1

Linear factors of bivariate polynomials

Observation

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

Linear factors of bivariate polynomials

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

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

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

Proof of the Gap Theorem

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

Bound on the valuation

Definition

$\mathrm{val}(P) =$ degree of the **lowest degree monomial** of $P \in \mathbb{K}[X]$

- $\mathrm{val}(X^3 + 2X^5 - X^{17}) = 3$

Bound on the valuation

Definition

val(P) = degree of the **lowest degree monomial** of $P \in \mathbb{K}[X]$

- $\mathrm{val}(X^3 + 2X^5 - X^{17}) = 3$

Theorem

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

$$\mathrm{val}(P) \leqslant \max_{1 \leqslant j \leqslant \ell} \left(\alpha_j + \binom{\ell + 1 - j}{2} \right).$$

Bound on the valuation

Definition

val(P) = degree of the **lowest degree monomial** of $P \in \mathbb{K}[X]$

- $\mathrm{val}(X^3 + 2X^5 - X^{17}) = 3$

Theorem

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

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

- $X^{\alpha_j}(uX+v)^{\beta_j}$ linearly independent

Bound on the valuation

Definition

$\mathrm{val}(P)$ = degree of the **lowest degree monomial** of $P \in \mathbb{K}[X]$

- $\mathrm{val}(X^3 + 2X^5 - X^{17}) = 3$

Theorem

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

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

- $X^{\alpha_j}(uX+v)^{\beta_j}$ linearly independent
- If $\alpha_1 = \cdots = \alpha_\ell$, $\mathrm{val}(P) \leqslant \alpha_1 + (\ell - 1)$ [Hajós'53]

The Wronskian

Definition

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

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

The Wronskian

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.

Wronskian & valuation

Lemma

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

Wronskian & valuation

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

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

Wronskian & valuation

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. $\mathrm{wr}(P, f_2, \dots, f_\ell) = a_1 \,\mathrm{wr}(f_1, \dots, f_\ell)$

Wronskian & valuation

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. $\mathrm{wr}(P, f_2,\dots,f_\ell) = a_1\,\mathrm{wr}(f_1,\dots,f_\ell)$

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

How far from optimality?

$$\mathrm{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leqslant \begin{cases} \alpha_1 + (\ell - 1) & \text{[Hajós'53] (constant } \alpha_j) \\ \alpha_1 + \binom{\ell}{2} & \text{[Our result]} \end{cases}$$

How far from optimality?

$$\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leqslant \begin{cases} \alpha_1 + (\ell - 1) & \text{[Hajós'53] (constant } \alpha_j) \\ \alpha_1 + \binom{\ell}{2} & \text{[Our result]} \end{cases}$$

- Lemmas: tight, but not simultaneously

How far from optimality?

$$\mathrm{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leqslant \begin{cases} \alpha_1 + (\ell - 1) & \text{[Hajós'53] (constant } \alpha_j) \\ \alpha_1 + \binom{\ell}{2} & \text{[Our result]} \end{cases}$$

- Lemmas: tight, but not simultaneously
- For all $\ell \geqslant 3$, there exists P_ℓ s.t. $\mathrm{val}(P_\ell) = \alpha_1 + (2\ell - 3)$

How far from optimality?

$$\mathrm{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leqslant \begin{cases} \alpha_1 + (\ell-1) & \text{[Hajós'53] (constant } \alpha_j) \\ \alpha_1 + \binom{\ell}{2} & \text{[Our result]} \end{cases}$$

- Lemmas: tight, but not simultaneously
- For all $\ell \geqslant 3$, there exists P_ℓ s.t. $\mathrm{val}(P_\ell) = \alpha_1 + (2\ell - 3)$

$$P_\ell(X) = (1+X)^{2\ell+3} - 1 - \sum_{j=3}^{\ell} \frac{2\ell-3}{2j-5}\binom{\ell+j-5}{2j-6} X^{2j-5}(1+X)^{\ell-1-j}$$
$$= X^{2\ell-3}$$

Gap Theorem

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

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

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

Gap Theorem

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

$$\alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2} \geqslant \mathrm{val}(Q),$$

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

$$P = \left(c_{\mathrm{val}(Q)} X^{\mathrm{val}(Q)} + \cdots\right) + X^{\alpha_{\ell+1}} \left(a_{\ell+1} (uX+v)^{\beta_{\ell+1}} + \cdots\right)$$

Algorithms

$\mathbb{K} = \mathbb{Q}(\alpha)$: **algebraic number field**

Finding linear factors

Observation + Gap Theorem (recursively)

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

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

Finding linear factors

Observation + Gap Theorem (recursively)

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

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

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

Finding linear factors

Observation + Gap Theorem (recursively)

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

Finding linear factors

Observation + Gap Theorem (recursively)

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

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

Finding linear factors

Observation + Gap Theorem (recursively)

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

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

Finding linear factors

Observation + Gap Theorem (recursively)

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

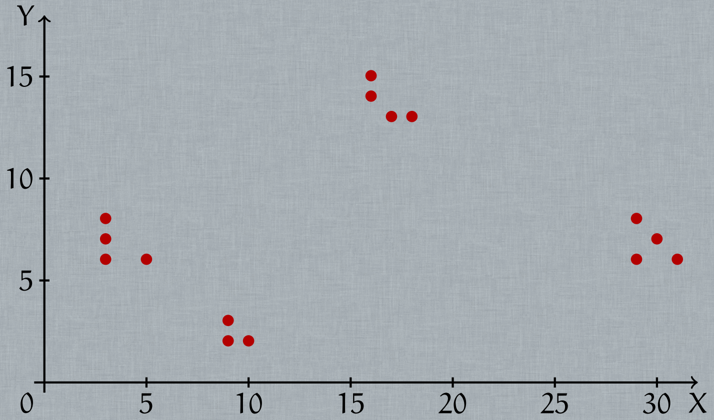
- $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leqslant \binom{\ell_t}{2}$
- Independent from u and v
- X does not play a special role

Example

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

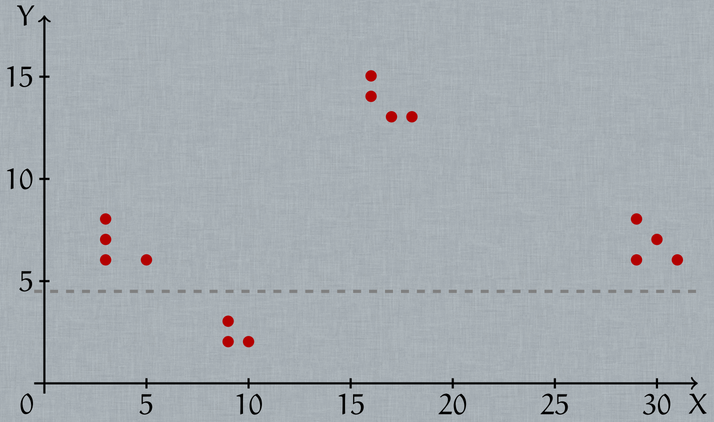
Example

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



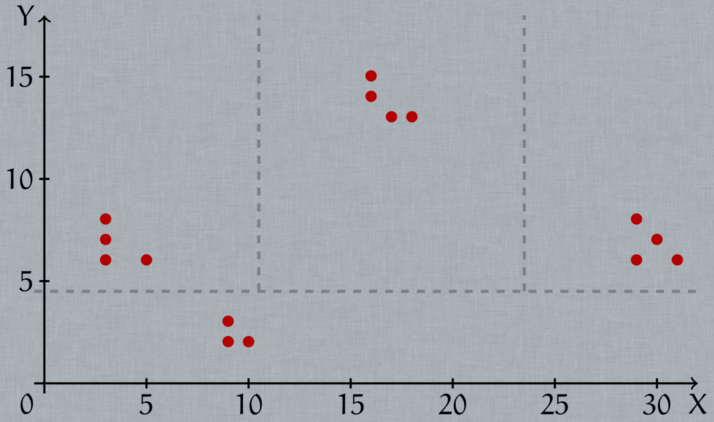
Example

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



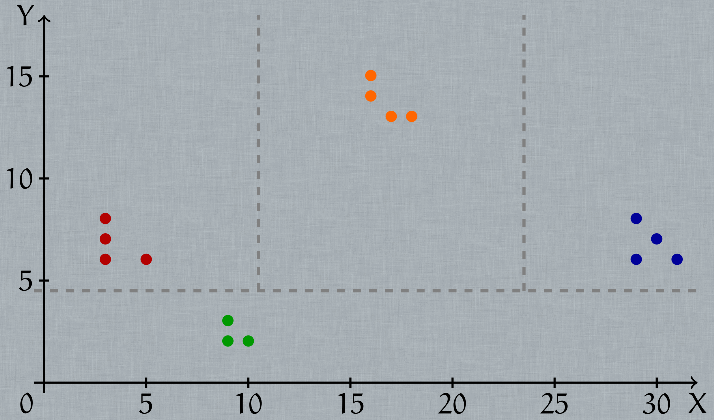
Example

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



Example

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



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

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

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

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

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

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

$\implies$ 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

$(X, \min_j \alpha_j)$

$(Y, \min_j \beta_j)$

binomials

$(X - a)$

Factors of $\sum_j a_j X^{\alpha_j}$

$(Y - uX)$

Roots of $u \mapsto \sum_j a_j u^{\beta_j}$

Univariate lacunary factorization

[H. Lenstra'99]

Complete algorithm

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

monomials — binomials — trinomials

monomials:

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

binomials:

$(X - a)$

Factors of $\sum_j a_j X^{\alpha_j}$

$(Y - uX)$

Roots of $u \mapsto \sum_j a_j u^{\beta_j}$

Univariate lacunary factorization
[H. Lenstra'99]

trinomials:

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

monomials:

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

binomials:

$(X - a)$

Factors of $\sum_j a_j X^{\alpha_j}$

$(Y - uX)$

Roots of $u \mapsto \sum_j a_j u^{\beta_j}$

Univariate lacunary factorization
[H. Lenstra'99]

trinomials:

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]

Comments

Bottleneck: Factorization of low-degree polynomials

Comments

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

Comments

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

- $\text{gap}(P) = \begin{cases} \mathcal{O}(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\ \mathcal{O}(k^2) & \text{[This work]} \end{cases}$

$h_P = \max_j |a_j|$ if $P \in \mathbb{Z}[X, Y]$

Comments

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

- $\mathrm{gap}(P) = \begin{cases} \mathcal{O}(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\ \mathcal{O}(k^2) & \text{[This work]} \end{cases}$

  $h_P = \max_j |a_j|$ if $P \in \mathbb{Z}[X, Y]$

- Algebraic number field only: based on **[H. Lenstra'99]**

Comments

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

- $\text{gap}(P) = \begin{cases} \mathcal{O}(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\ \mathcal{O}(k^2) & \text{[This work]} \end{cases}$

  $h_P = \max_j |a_j|$ if $P \in \mathbb{Z}[X, Y]$

- Algebraic number field only: based on [H. Lenstra'99]
- Generalization to **multilinear** factors

Comments

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

- $\mathrm{gap}(P) = \begin{cases} \mathcal{O}(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\ \mathcal{O}(k^2) & \text{[This work]} \end{cases}$

  $h_P = \max_j |a_j|$ if $P \in \mathbb{Z}[X,Y]$

- Algebraic number field only: based on [H. Lenstra'99]
- Generalization to **multilinear** factors
- PIT algorithm for $\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}$

Positive characteristic

$\mathbb{K} = \mathbb{F}_{p^s}$: **field with p^s elements**

Valuation & PIT

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

Valuation & PIT

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

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j + \beta_j)$.

Then $\mathrm{val}(P) \leqslant \max_j\left(\alpha_j + \binom{\ell+1-j}{2}\right)$, provided $P \not\equiv 0$.

Valuation & PIT

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

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j + \beta_j)$.
Then $\mathrm{val}(P) \leqslant \max_j\left(\alpha_j + \binom{\ell+1-j}{2}\right)$, provided $P \not\equiv 0$.

Theorem

There exists a deterministic polynomial-time algorithm to test if $\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j+\beta_j)$, vanishes.

Valuation & PIT

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

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j + \beta_j)$.
Then $\mathrm{val}(P) \leqslant \max_j\left(\alpha_j + \binom{\ell+1-j}{2}\right)$, provided $P \not\equiv 0$.

Theorem

There exists a deterministic polynomial-time algorithm to test if $\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j+\beta_j)$, vanishes.

Proof.

- If $uv \neq 0$: as in characteristic 0, using a Gap Theorem.

Valuation & PIT

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

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j + \beta_j)$.

Then $\mathrm{val}(P) \leqslant \max_j\left(\alpha_j + \binom{\ell+1-j}{2}\right)$, provided $P \not\equiv 0$.

Theorem

There exists a deterministic polynomial-time algorithm to test if $\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j+\beta_j)$, vanishes.

Proof.

- If $uv \neq 0$: as in characteristic 0, using a Gap Theorem.
- If $u = 0$: Evaluate $\sum_j a_j v^{\beta_j}$ using **repeated squaring**.

Valuation & PIT

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

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j + \beta_j)$.
Then $\mathrm{val}(P) \leqslant \max_j\left(\alpha_j + \binom{\ell+1-j}{2}\right)$, provided $P \not\equiv 0$.

Theorem

There exists a deterministic polynomial-time algorithm to test if $\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j+\beta_j)$, vanishes.

Proof.

- If $uv \neq 0$: as in characteristic 0, using a Gap Theorem.
- If $u = 0$: Evaluate $\sum_j a_j v^{\beta_j}$ using **repeated squaring**.
- The case $v = 0$ is similar.

Factorization algorithm

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

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

Factorization algorithm

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

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

monomials

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

trinomials

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
[Gao'03, Lecerf'10]

Factorization algorithm

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

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

monomials

$(X, \min_j \alpha_j)$

$(Y, \min_j \beta_j)$

binomials

$(X - a)$

Factors of $\sum_j a_j X^{\alpha_j}$

$(Y - uX)$

Roots of $u \mapsto \sum_j a_j u^{\beta_j}$

trinomials

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

[Gao'03, Lecerf'10]

Factorization algorithm

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

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

monomials | binomials | trinomials

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

$(X - a)$ …

Factors …

… $X)$

R… $u \mapsto \sum_j a_j u^{\beta_j}$

NP-complete
under BPP reductions

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

Talk at 2:25pm

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

[Gao'03, Lecerf'10]

Conclusion

Conclusion

- Computing linear factors of lacunary bivariate polynomials

Conclusion

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

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
- Extensions:

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
- Extensions:
  - **Low-degree** factors

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
- Extensions:
  - **Low-degree** factors
  - **Lacunary** factors

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
- Extensions:
  - **Low-degree** factors
  - **Lacunary** factors
  - **Smaller characteristics**

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases}\text{univariate lacunary polynomials}\\ \text{low-degree bivariate polynomials}\end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
- Extensions:
  - **Low-degree** factors
  - **Lacunary** factors
  - **Smaller characteristics**
- Correct bound for the valuation?

Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
- Extensions:
  - **Low-degree** factors
  - **Lacunary** factors
  - **Smaller characteristics**
- Correct bound for the valuation?

Thank you!