Factorization of lacunary polynomials

Bruno Grenet
ÉNS Lyon & U. Rennes 1

Based on a joint work with

Arkadev Chattopadhyay
TIFR, Mumbai

Pascal Koiran
ÉNS Lyon

Natacha Portier
ÉNS Lyon

Yann Strozecki
U. Versailles

Séminaire Pampers — Rennes, April 18, 2013

Factorization: classical algorithms

Factorization of a polynomial P

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

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2$$

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2 = (X - Y + Z)(X^4 + Y)(Z - X)$$

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2$$
$$= (X - Y + Z)(X^4 + Y)(Z - X)$$

- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra-Lenstra-Lovász'82]

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2$$
$$= (X - Y + Z)(X^4 + Y)(Z - X)$$

- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2$$
$$= (X - Y + Z)(X^4 + Y)(Z - X)$$

- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]
  - ⇝ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]
  - ⇝ $\mathbb{Q}(\alpha)[X_1, \dots, X_n]$ [Kaltofen'85, A. Lenstra'87]

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2$$
$$= (X - Y + Z)(X^4 + Y)(Z - X)$$

- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]
  - ⇝ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]
  - ⇝ $\mathbb{Q}(\alpha)[X_1, \dots, X_n]$ [Kaltofen'85, A. Lenstra'87]
- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2$$
$$= (X - Y + Z)(X^4 + Y)(Z - X)$$

- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]
  - ⇝ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]
  - ⇝ $\mathbb{Q}(\alpha)[X_1, \dots, X_n]$ [Kaltofen'85, A. Lenstra'87]
- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - ⇝ $\mathbb{F}_q[X_1, \dots, X_n]$

Factorization: classical algorithms

Factorization of a polynomial P

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

$$-X^6 - X^2Y + X^5Y + XY^2 - X^4YZ - Y^2Z + X^4Z^2 + YZ^2$$
$$= (X - Y + Z)(X^4 + Y)(Z - X)$$

- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]
  - ⇝ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]
  - ⇝ $\mathbb{Q}(\alpha)[X_1, \dots, X_n]$ [Kaltofen'85, A. Lenstra'87]
- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - ⇝ $\mathbb{F}_q[X_1, \dots, X_n]$

Complexity

Polynomial in the **degree** of the polynomials

The case of lacunary polynomials

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

The case of lacunary polynomials

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

The case of lacunary polynomials

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

The case of lacunary polynomials

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

Definition

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

The case of lacunary polynomials

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

Definition

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

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

The case of lacunary polynomials

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

Definition

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

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

The case of lacunary polynomials

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

Definition

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

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

- Algorithms of polynomial complexity in $\log(\deg(P))$ and in k

The case of lacunary polynomials

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

Definition

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

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

- Algorithms of polynomial complexity in $\log(\deg(P))$ and in k
- Restriction to **some** factors only

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$.

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Suppose that

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

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Suppose that

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Suppose that

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

$$-9 + X^2 + 6\,X^7 + 2\,X^8$$

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Suppose that

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

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

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Suppose that
$$\alpha_{\ell+1} - \alpha_\ell > 1 + \log\left(\max_{j\leq\ell} |a_j|\right),$$
then for all x, $|x| \geq 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

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

- Racine commune : -3

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Suppose that

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

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

- Racine commune : -3 et éventuellement 0, 1 et -1.

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 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Suppose that

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies Q(x) = R(x) = 0$.

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

- Racine commune : -3 et éventuellement 0, 1 et -1.

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial time (in $\log(\deg P)$) algorithms to compute

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

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial time (in $\log(\deg P)$) algorithms to compute

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$; [Cucker-Koiran-Smale'98]
- **low-degree** factors of **univariate** polynomials over $\mathbb{Q}(\alpha)$; [Lenstra'99]

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial time (in $\log(\deg P)$) algorithms to compute

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$;
  [Cucker-Koiran-Smale'98]
- **low-degree** factors of **univariate** polynomials over $\mathbb{Q}(\alpha)$;
  [Lenstra'99]
- **linear** factors of **bivariate** polynomials over $\mathbb{Q}$;
  [Kaltofen-Koiran'05]

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial time (in $\log(\deg P)$) algorithms to compute

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$;
  [Cucker-Koiran-Smale'98]
- **low-degree** factors of **univariate** polynomials over $\mathbb{Q}(\alpha)$;
  [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]

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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$.

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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. 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 $R \equiv 0$.

Linear factors of bivariate polynomials

Observation

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

Gap Theorem

Let

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

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

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

then $(Y - uX - v)$ divides P iff it divides both Q and R.

Linear factors of bivariate polynomials

Observation

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

Gap Theorem

Let

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

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

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

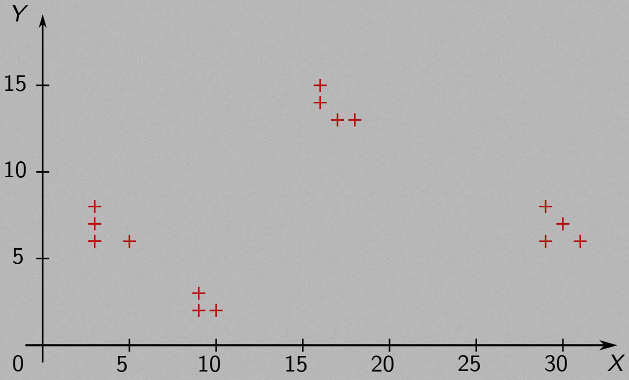
then every linear factor of P divides both Q and R if $uv \neq 0$.

Example

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

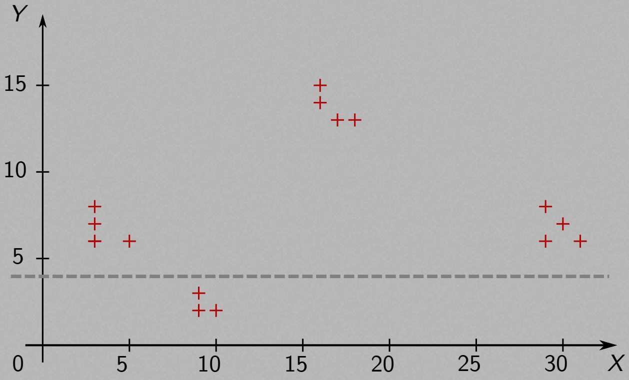
Example

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



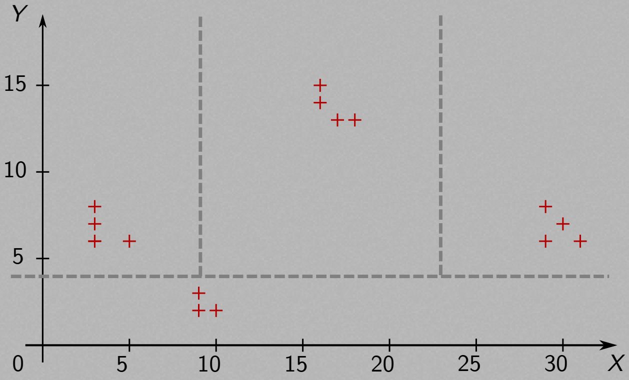
Example

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



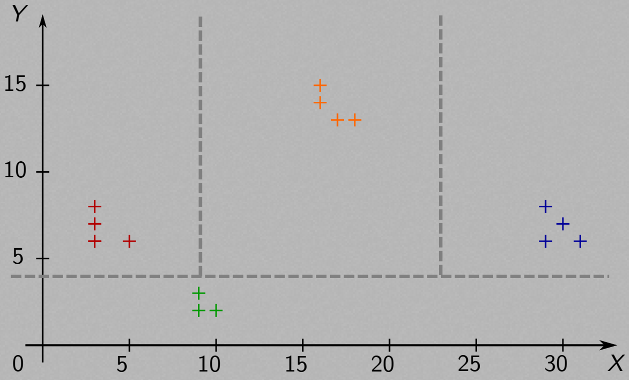
Example

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



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 (2)

$$-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$

$$X^{10}Y^2 - X^9Y^3 + X^9Y^2$$

$$X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14}$$

$$X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6$$

Example (2)

$$-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$
$$= X^3Y^6(-X^2 + Y^2 - 2Y + 1)$$

$$X^{10}Y^2 - X^9Y^3 + X^9Y^2$$

$$X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14}$$

$$X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6$$

Example (2)

$$\begin{aligned}-X^5Y^6+X^3Y^8-2X^3Y^7+X^3Y^6\\ =X^3Y^6(X-Y+1)(1-X-Y)\end{aligned}$$

$$X^{10}Y^2-X^9Y^3+X^9Y^2$$

$$X^{18}Y^{13}-X^{16}Y^{15}+X^{17}Y^{13}+X^{16}Y^{14}$$

$$X^{31}Y^6-2X^{30}Y^7+X^{29}Y^8-X^{29}Y^6$$

Example (2)

$$-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$X^{10}Y^2 - X^9Y^3 + X^9Y^2 = X^9Y^2(X - Y + 1)$$

$$X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14}$$

$$X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6$$

Example (2)

$$-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$X^{10}Y^2 - X^9Y^3 + X^9Y^2 = X^9Y^2(X - Y + 1)$$

$$X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6$$

Example (2)

$$\begin{aligned}-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \\ = X^3Y^6(X - Y + 1)(1 - X - Y)\end{aligned}$$

$$\begin{aligned}X^{10}Y^2 - X^9Y^3 + X^9Y^2 \\ = X^9Y^2(X - Y + 1)\end{aligned}$$

$$\begin{aligned}X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} \\ = X^{16}Y^{13}(X + Y)(X - Y + 1)\end{aligned}$$

$$\begin{aligned}X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 \\ = X^{29}Y^6(X - Y + 1)(X - Y - 1)\end{aligned}$$

Example (2)

$$-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$
$$= X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$X^{10}Y^2 - X^9Y^3 + X^9Y^2$$
$$= X^9Y^2(X - Y + 1)$$

$$X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14}$$
$$= X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6$$
$$= X^{29}Y^6(X - Y + 1)(X - Y - 1)$$

Example (2)

$$-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$X^{10}Y^2 - X^9Y^3 + X^9Y^2 = X^9Y^2(X - Y + 1)$$

$$X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 = X^{29}Y^6(X - Y + 1)(X - Y - 1)$$

Example (2)

$$-X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$X^{10}Y^2 - X^9Y^3 + X^9Y^2 = X^9Y^2(X - Y + 1)$$

$$X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 = X^{29}Y^6(X - Y + 1)(X - Y - 1)$$

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

Valuation

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

Bound on the valuation

Definition

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

Bound on the valuation

Definition

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

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

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 $\alpha_1 \leq \cdots \leq \alpha_\ell$.

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 $\alpha_1 \leq \cdots \leq \alpha_\ell$.
Then

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

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 $\alpha_1 \leq \cdots \leq \alpha_\ell$.
Then

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

- $X^{\alpha_j}(uX + v)^{\beta_j}$ 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 $\alpha_1 \leq \cdots \leq \alpha_\ell$.
Then

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

- $X^{\alpha_j}(uX+v)^{\beta_j}$ linearly independent
- Hajós' Lemma: if $\alpha_1 = \cdots = \alpha_\ell$, $\mathrm{val}(P) \leq \alpha_1 + (\ell - 1)$

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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. If

$$\alpha_{\ell+1} > \max_{1\leq j\leq \ell}\left(\alpha_j + \binom{\ell+1-j}{2}\right),$$

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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. 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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. 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 $R \equiv 0$.

$$P = \left(c_{\mathrm{val}(Q)} X^{\mathrm{val}(Q)} + \cdots \right)$$

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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. 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 $R \equiv 0$.

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

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

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

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

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

The Wronskian

Definition

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

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

The Wronskian

Definition

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

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

Proposition (Bôcher, 1900)

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

Wronskian & valuation

Lemma

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

Wronskian & valuation

Lemma

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

Proof.

$$\begin{vmatrix} f_1 & f_2 & \ldots & f_\ell \\ f_1' & f_2' & \ldots & f_\ell' \\ \vdots & \vdots & & \vdots \\ f_1^{(\ell-1)} & f_2^{(\ell-1)} & \ldots & f_\ell^{(\ell-1)} \end{vmatrix}$$

Wronskian & valuation

Lemma

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

Proof.

$$\begin{array}{r|cccc|} & \mathrm{val}(f_1) & \mathrm{val}(f_2) & \dots & \mathrm{val}(f_\ell) \\ 0 & f_1 & f_2 & \dots & f_\ell \\ -1 & f_1' & f_2' & \dots & f_\ell' \\ \vdots & \vdots & \vdots & & \vdots \\ -(\ell-1) & f_1^{(\ell-1)} & f_2^{(\ell-1)} & \dots & f_\ell^{(\ell-1)} \end{array}$$

Upper bound for the valuation

Lemma

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

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

Upper bound for the valuation

Lemma

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

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

Proof idea. Write

$$\mathrm{wr}(f_1,\dots,f_\ell) = X^{\sum_j \alpha_j - \binom{\ell}{2}}(uX+v)^{\sum_j \beta_j - \binom{\ell}{2}} \times \det(M)$$

with $\deg(M_{ij}) \leq i$.

Upper bound for the valuation

Lemma

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

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

Proof idea. Write

$$\operatorname{wr}(f_1,\dots,f_\ell) = X^{\sum_j \alpha_j - \binom{\ell}{2}}(uX+v)^{\sum_j \beta_j - \binom{\ell}{2}} \times \det(M)$$

with $\deg(M_{ij}) \leq i$. Use $\operatorname{val}(\det M) \leq \deg(\det M) \leq \binom{\ell}{2}$.

Proof of the Theorem

Theorem

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

Then

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

Proof of the Theorem

Theorem

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

$$\operatorname{val}(P) \leq \alpha_1 + \binom{\ell}{2}.$$

Proof. $\operatorname{wr}(P, f_2, \ldots, f_\ell) = a_1 \operatorname{wr}(f_1, \ldots, f_\ell)$

Proof of the Theorem

Theorem

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

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

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

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

Proof of the Theorem

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leq \cdots \leq \alpha_\ell$.
Then
$$\operatorname{val}(P) \leq \max_{1\leq j\leq \ell}\left(\alpha_j + \binom{\ell+1-j}{2}\right).$$

Proof. $\operatorname{wr}(P, f_2, \ldots, f_\ell) = a_1 \operatorname{wr}(f_1, \ldots, f_\ell)$

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

How far from optimality?

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

How far from optimality?

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

How far from optimality?

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

How far from optimality?

- Hajós' Lemma: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \leq \alpha + (\ell - 1)$
- Our result: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leq \alpha_1 + \binom{\ell}{2}$
- Lemmas: bounds attained, but not simultaneously $\rightsquigarrow$ trade-off?
- $\exists P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ s.t. $\operatorname{val}(P) = \alpha_1 + (2\ell - 3)$

How far from optimality?

- Hajós' Lemma: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \leq \alpha + (\ell - 1)$
- Our result: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leq \alpha_1 + \binom{\ell}{2}$
- Lemmas: bounds attained, but not simultaneously $\rightsquigarrow$ trade-off?
- $\exists P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ s.t. $\operatorname{val}(P) = \alpha_1 + (2\ell - 3)$

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

How far from optimality?

- Hajós' Lemma: $\mathrm{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \le \alpha + (\ell - 1)$
- Our result: $\mathrm{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \le \alpha_1 + \binom{\ell}{2}$
- Lemmas: bounds attained, but not simultaneously $\rightsquigarrow$ trade-off?
- $\exists P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ s.t. $\mathrm{val}(P) = \alpha_1 + (2\ell - 3)$

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

A generalization

Theorem

Let $(\alpha_{ij}) \in \mathbb{Z}_+^{\ell\times m}$ and

$$P = \sum_{j=1}^{\ell} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}},$$

where $f_i \in \mathbb{K}[X]$, $\deg(f_i) = d_i$ and $\mathrm{val}(f_i) = \mu_i$.

A generalization

Theorem

Let $(\alpha_{ij}) \in \mathbb{Z}_+^{\ell\times m}$ and

$$P = \sum_{j=1}^{\ell} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}},$$

where $f_i \in \mathbb{K}[X]$, $\deg(f_i) = d_i$ and $\operatorname{val}(f_i) = \mu_i$. Then

$$\operatorname{val}(P) \leq \max_{1\leq j\leq \ell} \sum_{i=1}^{m} \left(\mu_i\alpha_{ij} + (d_i - \mu_i)\binom{\ell+1-j}{2}\right).$$

A generalization

Theorem

Let $(\alpha_{ij}) \in \mathbb{Q}^{\ell \times m}$ and

$$P = \sum_{j=1}^{\ell} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}},$$

where $f_i \in \mathbb{K}[X]$, $\deg(f_i) = d_i$ and $\mathrm{val}(f_i) = \mu_i$. Then

$$\mathrm{val}(P) \leq \max_{1 \leq j \leq \ell} \sum_{i=1}^{m} \left(\mu_i \alpha_{ij} + (d_i - \mu_i) \binom{\ell + 1 - j}{2} \right).$$

Algorithms

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

Algorithms

1. Polynomial Identity Testing
2. Finding (multi)linear factors

Algorithms

1. Polynomial Identity Testing
2. Finding (multi)linear factors

Definition

$$\mathbb{K} = \mathbb{Q}[\xi]/\langle\varphi\rangle, \qquad \varphi \in \mathbb{Z}[\xi] \text{ irreducible of degree } \delta$$

Algorithms

1. Polynomial Identity Testing
2. Finding (multi)linear factors

Definition

$$\mathbb{K} = \mathbb{Q}[\xi]/\langle\varphi\rangle, \qquad \varphi \in \mathbb{Z}[\xi] \text{ irreducible of degree } \delta$$

- $x \in \mathbb{K}$ represented as $(\frac{n_0}{d_0}, \dots, \frac{n_{\delta-1}}{d_{\delta-1}})$
- $\mathrm{size}(x) \simeq \log(n_0 d_0) + \cdots + \log(n_{\delta-1} d_{\delta-1})$

Algorithms

1. Polynomial Identity Testing
2. Finding (multi)linear factors

Definition

$$\mathbb{K} = \mathbb{Q}[\xi]/\langle\varphi\rangle, \qquad \varphi \in \mathbb{Z}[\xi] \text{ irreducible of degree } \delta$$

- $x \in \mathbb{K}$ represented as $(\frac{n_0}{d_0}, \dots, \frac{n_{\delta-1}}{d_{\delta-1}})$
- $\text{size}(x) \simeq \log(n_0 d_0) + \cdots + \log(n_{\delta-1} d_{\delta-1})$

- $\mathbb{K}$ is part of the input, given by φ in dense representation

Polynomial Identity Testing

Theorem

There exists a deterministic polynomial-time algorithm to test if $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ vanishes.

Polynomial Identity Testing

Theorem

There exists a deterministic polynomial-time algorithm to test if $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ vanishes.

Proof.

- If $u = 0$: test $\sum_j a_j v^{\beta_j} \stackrel{?}{=} 0$ [Lenstra'99]

Polynomial Identity Testing

Theorem

There exists a deterministic polynomial-time algorithm to test if $P = \sum_{j=1}^{k} a_j X^{\alpha_j} (uX+v)^{\beta_j}$ vanishes.

Proof.

- If $u = 0$: test $\sum_j a_j v^{\beta_j} \stackrel{?}{=} 0$ [Lenstra'99]
- If $v = 0$: similar [Lenstra'99]

Polynomial Identity Testing

Theorem

There exists a deterministic polynomial-time algorithm to test if $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ vanishes.

Proof.

- If $u = 0$: test $\sum_j a_j v^{\beta_j} \stackrel{?}{=} 0$ [Lenstra'99]
- If $v = 0$: similar [Lenstra'99]
- If $u, v \neq 0$: $P = P_1 + \cdots + P_s$ s.t.

$$P = 0 \iff P_1 = \cdots = P_s = 0$$

where $P_t = \sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{k}{2}$

Polynomial Identity Testing, cont'd

$$Q(X) = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j},\ \text{with } \alpha_\ell \leq \alpha_1 + \binom{\ell}{2}$$

Polynomial Identity Testing, cont'd

$$Q(X) = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}, \text{ with } \alpha_\ell \leq \qquad \binom{\ell}{2}$$

Polynomial Identity Testing, cont'd

$$Q(X) = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}, \text{ with } \alpha_\ell \leq \qquad \binom{\ell}{2}$$

Let $Y = uX + v$. Then

$$Q(Y) = \sum_{j=1}^{\ell} a_j u^{-\alpha_j}(Y-v)^{\alpha_j} Y^{\beta_j}$$

Polynomial Identity Testing, cont'd

$$Q(X) = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}, \text{ with } \alpha_\ell \leq \binom{\ell}{2}$$

Let $Y = uX + v$. Then

$$Q(Y) = \sum_{j=1}^{\ell} a_j u^{-\alpha_j}(Y-v)^{\alpha_j} Y^{\beta_j}$$

$$= \sum_{j=1}^{\ell}\sum_{t=0}^{\alpha_j} a_j u^{-\alpha_j}\binom{\alpha_j}{t}(-v)^t Y^{\alpha_j+\beta_j-t}$$

Polynomial Identity Testing, cont'd

$$Q(X) = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}, \text{ with } \alpha_\ell \leq \binom{\ell}{2}$$

Let $Y = uX + v$. Then

$$Q(Y) = \sum_{j=1}^{\ell} a_j u^{-\alpha_j}(Y-v)^{\alpha_j} Y^{\beta_j}$$

$$= \sum_{j=1}^{\ell}\sum_{t=0}^{\alpha_j} a_j u^{-\alpha_j}\binom{\alpha_j}{t}(-v)^t Y^{\alpha_j+\beta_j-t}$$

number of monomials, exponents $\leq$ $\text{size}(Q)^{\mathcal{O}(1)}$

Polynomial Identity Testing, cont'd

$$Q(X) = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}, \text{ with } \alpha_\ell \leq \binom{\ell}{2}$$

Let $Y = uX + v$. Then

$$Q(Y) = \sum_{j=1}^{\ell} a_j u^{-\alpha_j}(Y-v)^{\alpha_j} Y^{\beta_j}$$

$$= \sum_{j=1}^{\ell}\sum_{t=0}^{\alpha_j} a_j u^{-\alpha_j}\binom{\alpha_j}{t}(-v)^t Y^{\alpha_j+\beta_j-t}$$

number of monomials, exponents $\leq$ $\text{size}(Q)^{\mathcal{O}(1)}$ $\implies$ brute force

Finding linear factors

Observation + Gap Theorem

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

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

Finding linear factors

Observation + Gap Theorem

$(Y - uX - v)$ 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

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

Finding linear factors

Observation + Gap Theorem

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

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

$\rightsquigarrow$ find linear factors of low-degree polynomials

Some details

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

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [Lenstra'99]

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j+\beta_j}$ [Lenstra'99]

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [Lenstra'99]
3. If $u, v \neq 0$:

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [Lenstra'99]
3. If $u, v \neq 0$:
   3.1 Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_{j \le \ell_t} a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \le \alpha_{\min} + \binom{\ell_t}{2}$ and $\beta_{\max} \le \beta_{\min} + \binom{\ell_t}{2}$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [Lenstra'99]
3. If $u, v \neq 0$:
   3.1 Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_{j \leq \ell_t} a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{\ell_t}{2}$ and $\beta_{\max} \leq \beta_{\min} + \binom{\ell_t}{2}$
   3.2 Write $P_t = X^{\alpha_{\min}} Y^{\beta_{\min}} Q_t$ with $\deg(Q_t) \leq \ell_t(\ell_t - 1)$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [Lenstra'99]
3. If $u, v \neq 0$:
   - 3.1 Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_{j \leq \ell_t} a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{\ell_t}{2}$ and $\beta_{\max} \leq \beta_{\min} + \binom{\ell_t}{2}$
   - 3.2 Write $P_t = X^{\alpha_{\min}} Y^{\beta_{\min}} Q_t$ with $\deg(Q_t) \leq \ell_t(\ell_t - 1)$
   - 3.3 Apply some dense factorization algorithm to each Q_t or $\gcd(Q_1, \ldots, Q_s)$ [Kaltofen'82, ..., Lecerf'07]

Comments

Main computational task: Factorization of dense polynomials

Comments

Main computational task: Factorization of dense polynomials

$\Longrightarrow$ Complexity in terms of $\mathrm{gap}(P)$

Comments

Main computational task: Factorization of dense polynomials
$\implies$ Complexity in terms of $\mathrm{gap}(P)$

- [Kaltofen-Koiran'05]: $\mathrm{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$

Comments

Main computational task: Factorization of dense polynomials
$\implies$ Complexity in terms of $\mathrm{gap}(P)$

- [Kaltofen-Koiran'05]: $\mathrm{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$

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

Comments

Main computational task: Factorization of dense polynomials
$\Longrightarrow$ Complexity in terms of $\text{gap}(P)$

- [Kaltofen-Koiran'05]: $\text{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$

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

- Here: $\text{gap}(P) = \mathcal{O}(k^2)$

Comments

Main computational task: Factorization of dense polynomials
$\implies$ Complexity in terms of $\text{gap}(P)$

- [Kaltofen-Koiran'05]: $\text{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$

  $h_P = \max_j |a_j|$ if $P \in \mathbb{Z}[X, Y]$
- Here: $\text{gap}(P) = \mathcal{O}(k^2)$
- Algebraic number field: only for Lenstra's algorithm

Finding multilinear factors

Lemma

Let $P = \sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}(wX+t)^{\gamma_j} \not\equiv 0$, $uvwt \neq 0$. Then

$$\mathrm{val}(P) \leq \max_j \left(\alpha_j + 2\binom{k+1-j}{2}\right).$$

Finding multilinear factors

Lemma

Let $P = \sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}(wX+t)^{\gamma_j} \not\equiv 0$, $uvwt \neq 0$. Then

$$\operatorname{val}(P) \leq \max_j \left(\alpha_j + 2\binom{k+1-j}{2}\right).$$

Theorem

There exists a polynomial-time algorithm to compute the multilinear factors of $\sum_j a_j X^{\alpha_j} Y^{\beta_j}$.

Finding multilinear factors

Lemma

Let $P = \sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}(wX+t)^{\gamma_j} \not\equiv 0$, $uvwt \neq 0$. Then

$$\mathrm{val}(P) \leq \max_j \left(\alpha_j + 2\binom{k+1-j}{2}\right).$$

Theorem

There exists a polynomial-time algorithm to compute the multilinear factors of $\sum_j a_j X^{\alpha_j} Y^{\beta_j}$.

Proof.

- $XY-(uX-vY+w)$ divides $P \iff P(X, \frac{uX+w}{X+v}) \equiv 0$.

Finding multilinear factors

Lemma

Let $P=\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}(wX+t)^{\gamma_j}\not\equiv 0$, $uvwt\neq 0$. Then

$$\operatorname{val}(P)\leq \max_j \left(\alpha_j + 2\binom{k+1-j}{2}\right).$$

Theorem

There exists a polynomial-time algorithm to compute the multilinear factors of $\sum_j a_j X^{\alpha_j} Y^{\beta_j}$.

Proof.

- $XY-(uX-vY+w)$ divides $P \iff P(X,\frac{uX+w}{X+v})\equiv 0$.
- Gap Theorem for $Q(X)=(X+v)^{\max_j \beta_j} P(X,\frac{uX+w}{X+v})$.

Positive characteristic

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

Valuation

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

Valuation

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

Theorem

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

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

Valuation

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

Theorem

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

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

Proposition

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

Polynomial Identity Testing

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.

Polynomial Identity Testing

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.

Polynomial Identity Testing

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**.

Polynomial Identity Testing

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.

Finding linear factors

Theorem

Let $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_{p^s}[X, Y]$, where $p > \max_j(\alpha_j + \beta_j)$. Factors of the form $(uX + vY + w)$ are

- computable in **randomized polynomial time** if $uvw \neq 0$;

Finding linear factors

Theorem

Let $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_{p^s}[X, Y]$, where $p > \max_j(\alpha_j + \beta_j)$.
Factors of the form $(uX + vY + w)$ are

- computable in **randomized polynomial time** if $uvw \neq 0$;
- NP-**hard** to detect under randomized reductions **otherwise**.

Finding linear factors

Theorem

Let $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_{p^s}[X, Y]$, where $p > \max_j(\alpha_j + \beta_j)$.
Factors of the form $(uX + vY + w)$ are

- computable in **randomized polynomial time** if $uvw \neq 0$;
- NP-**hard** to detect under randomized reductions **otherwise**.

- Only randomized dense factorization algorithms over $\mathbb{F}_{p^s}$

Finding linear factors

Theorem

Let $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_{p^s}[X, Y]$, where $p > \max_j(\alpha_j + \beta_j)$. Factors of the form $(uX + vY + w)$ are

- computable in **randomized polynomial time** if $uvw \neq 0$;
- NP-**hard** to detect under randomized reductions **otherwise**.

- Only randomized dense factorization algorithms over $\mathbb{F}_{p^s}$
- NP-hardness: reduction from **root detection** over $\mathbb{F}_{p^s}$
  [Kipnis-Shamir'99, Bi-Cheng-Rojas'12]

Conclusion

Summary

- **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials

Summary

+ **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials
  - Easier to implement

Summary

- **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials
  - Easier to implement
  - Two Gap Theorems: mix both!

Summary

- Elementary proofs & algorithms for multilinear factors of lacunary bivariate polynomials
  - Easier to implement
  - Two Gap Theorems: mix both!
- Gap Theorem independent of the height

Summary

- **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials
  - Easier to implement
  - Two Gap Theorems: mix both!
- Gap Theorem independent of the height
  - **Large coefficients**

Summary

- **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials
  - Easier to implement
  - Two Gap Theorems: mix both!
- Gap Theorem independent of the height
  - **Large coefficients**
  - Valid to some extent for other fields

Summary

- **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials
  - Easier to implement
  - Two Gap Theorems: mix both!
- Gap Theorem independent of the height
  - **Large coefficients**
  - Valid to some extent for other fields
- Results in large **positive characteristic**

Summary

+ **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials
  - Easier to implement
  - Two Gap Theorems: mix both!
+ Gap Theorem independent of the height
  - **Large coefficients**
  - Valid to some extent for other fields
+ Results in large **positive characteristic**

− Still relies on [Lenstra'99]

Summary

+ **Elementary** proofs & algorithms for multilinear factors of lacunary bivariate polynomials
    - Easier to implement
    - Two Gap Theorems: mix both!
+ Gap Theorem independent of the height
    - **Large coefficients**
    - Valid to some extent for other fields
+ Results in large **positive characteristic**
− Still relies on [Lenstra'99]
    - Number fields

Open questions

- Can we find **low-degree factors** of **multivariate** polynomials?

Open questions

- Can we find low-degree factors of **multivariate** polynomials?
- And low-degree factors of **univariate** polynomials?

Open questions

- Can we find low-degree factors of **multivariate** polynomials?
- And low-degree factors of **univariate** polynomials?

$\rightsquigarrow$ Impossibility results in positive characteristic

Open questions

- Can we find **low-degree factors** of **multivariate** polynomials?
- And low-degree factors of **univariate** polynomials?

  $\rightsquigarrow$ Impossibility results in positive characteristic
- Can we find **lacunary factors**?

Open questions

- Can we find **low-degree factors** of **multivariate** polynomials?
- And low-degree factors of **univariate** polynomials?

  $\rightsquigarrow$ Impossibility results in positive characteristic
- Can we find **lacunary factors**?
- Can we handle polynomials in **small characteristic**?

Open questions

- Can we find **low-degree factors** of **multivariate** polynomials?
- And low-degree factors of **univariate** polynomials?

  $\rightsquigarrow$ Impossibility results in positive characteristic
- Can we find **lacunary factors**?
- Can we handle polynomials in **small characteristic**?
- Is the correct bound for the valuation **quadratic or linear**?

Open questions

- Can we find **low-degree factors** of **multivariate** polynomials?
- And low-degree factors of **univariate** polynomials?

  $\rightsquigarrow$ Impossibility results in positive characteristic
- Can we find **lacunary factors**?
- Can we handle polynomials in **small characteristic**?
- Is the correct bound for the valuation **quadratic or linear**?

Thank you!

arXiv:1206.4224