Elementary algorithms for the factorization of bivariate lacunary polynomials

Bruno Grenet
U. Rennes 1 & ÉNS Lyon

Based on a joint work with

Arkadev Chattopadhyay
TIFR, Mumbai

Pascal Koiran
ÉNS Lyon

Natacha Portier
ÉNS Lyon

Yann Strozecki
U. Versailles

Journées Nationales de Calcul Formel

CIRM, Marseille — May 16, 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. $P = F_1 \times \cdots \times F_t$.

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

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

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

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

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

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

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

- Algorithms of polynomial complexity in $\log(\deg(P))$ and in k
- 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 $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_k$.

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

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

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

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

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

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

- Common root: -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 $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_k$. Suppose that

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

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

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

- Common root: -3 and potentially 0, 1 and -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 $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_k$. Suppose that

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

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

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

- Common root: -3 and potentially 0, 1 and -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 $\mathbb{Q}(\alpha)$; [H. 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 $\mathbb{Q}(\alpha)$;
  [H. 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 $\mathbb{Q}(\alpha)$;
  [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]

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

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 $R \equiv 0$.

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

Valuation

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

Bound on the valuation

Definition

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

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

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

$\mathrm{val}(P)$ = 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

Bound on the valuation

Definition

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\alpha_1 \leqslant \cdots \leqslant \alpha_\ell$.

Then

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

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

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

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

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

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

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

How far from optimality?

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

How far from optimality?

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

How far from optimality?

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

How far from optimality?

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

How far from optimality?

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

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

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

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

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

$$\alpha_{\ell+1} > \max_{1 \leqslant j \leqslant \ell} \left(\alpha_j + \binom{\ell+1-j}{2} \right) \geqslant \mathrm{val}(Q),$$

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)

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

Finding linear factors

Observation + Gap Theorem (recursively)

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

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)

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

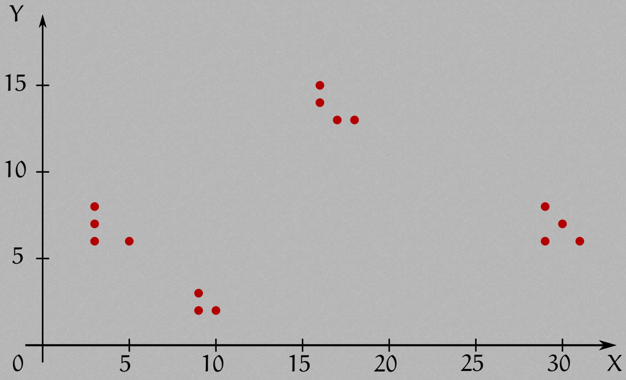
- $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{j_t+\ell_t-1}-\alpha_{j_t} \leqslant \binom{\ell_t}{2}$
- Independent from u and v
- X does not play a special role

Example

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

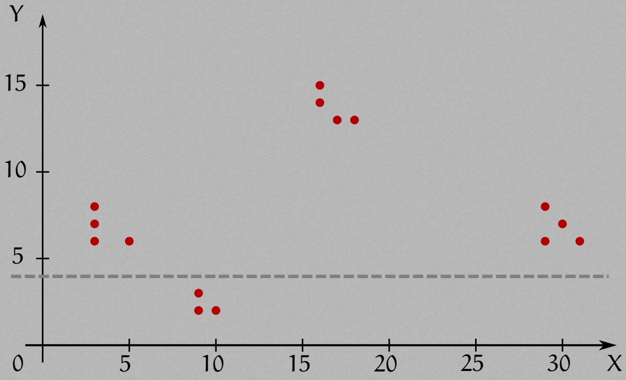
Example

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



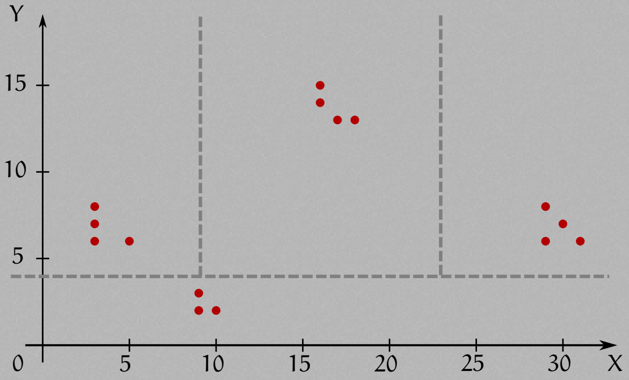
Example

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



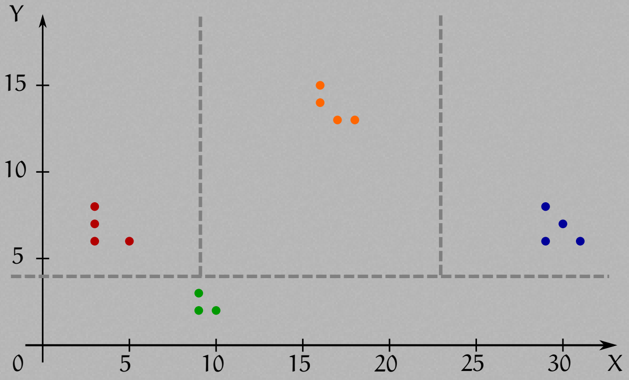
Example

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



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

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

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

Example

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

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

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

Complete algorithm

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 $\sum_j a_j Y^{\beta_j}$

Complete algorithm

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 $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]

Complete algorithm

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

Complete algorithm

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

Complete algorithm

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

Complete algorithm

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

Complete algorithm

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

Complete algorithm

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

$\implies$ Complexity in terms of gap(P)

Comments

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

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

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 $P \in \mathbb{Z}[X, Y]$

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

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 $P \in \mathbb{Z}[X, Y]$

- Here: $\mathrm{gap}(P) = \mathcal{O}(k^2)$
- Algebraic number field: only for Lenstra's algorithm

Positive characteristic

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

In large characteristics

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

In large characteristics

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

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

In large characteristics

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

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

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 $uvw \neq 0$;

In large characteristics

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

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

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**.

Conclusion

Summary

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

Summary

- Elementary proofs & algorithms for *multilinear* factors of lacunary bivariate polynomials
  - Reduction to univariate and low-degree cases

Summary

+ **Elementary** proofs & algorithms for *multilinear* factors of lacunary bivariate polynomials
    - Reduction to univariate and low-degree cases
    - Easy to implement

Summary

+ **Elementary** proofs & algorithms for *multilinear* factors of lacunary bivariate polynomials
  - Reduction to univariate and low-degree cases
  - Easy to implement
  - Two Gap Theorems: mix both!

Summary

- **Elementary** proofs & algorithms for *multilinear* factors of lacunary bivariate polynomials
  - Reduction to univariate and low-degree cases
  - Easy to implement
  - Two Gap Theorems: mix both!
- Gap Theorem independent of the height

Summary

- **Elementary** proofs & algorithms for *multilinear* factors of lacunary bivariate polynomials
  - Reduction to univariate and low-degree cases
  - Easy 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
  - Reduction to univariate and low-degree cases
  - Easy 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
  - Reduction to univariate and low-degree cases
  - Easy 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
  - Reduction to univariate and low-degree cases
  - Easy 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 [H. Lenstra'99]

Summary

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

- Reduction to univariate and low-degree cases
- Easy 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 [H. Lenstra'99]

- Number fields

Open questions

- Extensions:

Open questions

- Extensions:
  - **low-degree** factors

Open questions

- Extensions:
  - **low-degree** factors
  - **multivariate** polynomials

Open questions

- Extensions:
  - **low-degree** factors
  - **multivariate** polynomials
  - **univariate** polynomials ⚠ positive characteristic

Open questions

- Extensions:
  - **low-degree** factors
  - **multivariate** polynomials
  - **univariate** polynomials ⚠ positive characteristic
  - **lacunary** factors

Open questions

- Extensions:
  - **low-degree** factors
  - **multivariate** polynomials
  - **univariate** polynomials ⚠ positive characteristic
  - **lacunary** factors
  - **smaller characteristics**

Open questions

- Extensions:
  - **low-degree** factors
  - **multivariate** polynomials
  - **univariate** polynomials ⚠ positive characteristic
  - **lacunary** factors
  - **smaller characteristics**
- Is the correct bound for the valuation **quadratic or linear**?

Open questions

- Extensions:
  - **low-degree** factors
  - **multivariate** polynomials
  - **univariate** polynomials ⚠ positive characteristic
  - **lacunary** factors
  - **smaller characteristics**
- Is the correct bound for the valuation **quadratic or linear**?

Thank you!

arXiv:1206.4224