Factoring bivariate lacunary polynomials without heights

Bruno Grenet
ÉNS Lyon

Joint work with

Arkadev Chattophyay
TIFR, Mumbai

Pascal Koiran
ÉNS Lyon

Natacha Portier
ÉNS Lyon

Yann Strozecki
U. Versailles

Palindromic Dagstuhl Seminar 13031: Computational Counting

January 16. 2013

Representation of Univariate Polynomials

$$P(X) = X^{10} - 4\,X^8 + 8\,X^7 + 5\,X^3 + 1$$

Representations

- Dense:

$$[1, 0, -4, 8, 0, 0, 0, 5, 0, 0, 1]$$

- Sparse:

$$\Big\{(10 : 1), (8 : -4), (7 : 8), (3 : 5), (0 : 1)\Big\}$$

Representation of Multivariate Polynomials

$$P(X, Y, Z) = X^2 Y^3 Z^5 - 4\, X^3 Y^3 Z^2 + 8\, X^5 Z^2 + 5\, XYZ + 1$$

Representations

- Dense:

$$[1, \ldots, -4, \ldots, 8, \ldots, 5, \ldots, 1]$$

- Lacunary (supersparse):

$$\Big\{(2, 3, 5 : 1), (3, 3, 2 : -4), (5, 0, 2 : 8), (1, 1, 1 : 5), (0 : 1)\Big\}$$

Size of the lacunary representation

Definition

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

$$\Longrightarrow \ \text{size}(P) = \sum_{j=1}^{k} \text{size}(a_j) + \log(\alpha_{1j}) + \cdots + \log(\alpha_{nj})$$

Factorization of lacunary polynomials

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

Factorization of lacunary polynomials

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

Factorization of lacunary polynomials

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

Factorization of a polynomial P

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

Factorization of lacunary polynomials

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

Factorization of a polynomial P

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

Proposition

A lacunary polynomial can have **exponentially many factors**.

$\Longrightarrow$ restriction to finding **some** factors

Factorization of sparse univariate polynomials

$$P(X) = \sum_{j=1}^{k} a_j X^{\alpha_j} \qquad \text{size}(P) = \sum_{j=1}^{k} \text{size}(a_j) + \log(\alpha_j)$$

Factorization of sparse univariate polynomials

$$P(X) = \sum_{j=1}^{k} a_j X^{\alpha_j} \qquad \text{size}(P) = \sum_{j=1}^{k} \text{size}(a_j) + \log(\alpha_j)$$

Theorem (Cucker-Koiran-Smale'98)

Polynomial-time algorithm to find **integer roots** if $a_j \in \mathbb{Z}$.

Factorization of sparse univariate polynomials

$$P(X) = \sum_{j=1}^{k} a_j X^{\alpha_j} \qquad \text{size}(P) = \sum_{j=1}^{k} \text{size}(a_j) + \log(\alpha_j)$$

Theorem (Cucker-Koiran-Smale'98)

Polynomial-time algorithm to find **integer roots** if $a_j \in \mathbb{Z}$.

Theorem (Lenstra'99)

Polynomial-time algorithm to find **factors of degree** $\leq d$ if $a_j \in \mathbb{K}$, where $\mathbb{K}$ is an algebraic number field.

Factorization of lacunary polynomials

Theorem (Kaltofen-Koiran'05)

Polynomial-time algorithm to find **linear factors** of **bivariate** lacunary polynomials over $\mathbb{Q}$.

Factorization of lacunary polynomials

Theorem (Kaltofen-Koiran'05)

Polynomial-time algorithm to find **linear factors** of **bivariate** lacunary polynomials over $\mathbb{Q}$.

Theorem (Kaltofen-Koiran'06)

Polynomial-time algorithm to find **low-degree factors** of **multivariate** lacunary polynomials over algebraic number fields.

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

$$\alpha_{\ell+1} - \alpha_\ell > \mathrm{gap}(P)$$

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

$$\alpha_{\ell+1} - \alpha_\ell > \mathrm{gap}(P),$$

then F divides P iff F divides both P_0 and P_1.

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

$$\alpha_{\ell+1} - \alpha_\ell > \mathrm{gap}(P),$$

then F divides P iff F divides both P_0 and P_1.

gap(P): function of the **algebraic height** of P.

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_t} P_s \text{ with } \deg(P_t) \leq \text{gap}(P)$$

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_t} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out $P_1, \ldots, P_t$ using a dense factorization algorithm

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_t} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out $P_1, \ldots, P_t$ using a dense factorization algorithm
- Refinements:

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_t} P_s \text{ with } \deg(P_t) \leq \text{gap}(P)$$

- Factor out $P_1, \ldots, P_t$ using a dense factorization algorithm
- Refinements:
  - Factor out the gcd of the P_t's

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_t} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out $P_1, \ldots, P_t$ using a dense factorization algorithm
- Refinements:
  - Factor out the gcd of the P_t's
  - Factor out only one P_t & check which factors are common to the other P_t's

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_t} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out $P_1, \ldots, P_t$ using a dense factorization algorithm
- Refinements:
  - Factor out the gcd of the P_t's
  - Factor out only one P_t & check which factors are common to the other P_t's
  - ...

Results

Theorem

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

Results

Theorem

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]

Results

Theorem

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) independent of the height

Results

Theorem

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) independent of the height
  - $\rightsquigarrow$ More elementary algorithms

Results

Theorem

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) independent of the height
  - $\rightsquigarrow$ More elementary algorithms
  - $\rightsquigarrow$ Gap Theorem valid over **any field of characteristic 0**

Results

Theorem

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) independent of the height
  - ⇝ More elementary algorithms
  - ⇝ Gap Theorem valid over **any field of characteristic 0**
- Extension to **multilinear** factors

Results

Theorem

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) independent of the height
  - $\rightsquigarrow$ More elementary algorithms
  - $\rightsquigarrow$ Gap Theorem valid over **any field of characteristic 0**
- Extension to **multilinear** factors
- Results in **positive characteristics**

Linear factors of bivariate polynomials

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

Linear factors of bivariate polynomials

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

Observation

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

Linear factors of bivariate polynomials

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

Observation

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

- Study of polynomials of the form $\sum_j a_j X^{\alpha_j} (uX+v)^{\beta_j}$

Linear factors of bivariate polynomials

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

Observation

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

- Study of polynomials of the form $\sum_j a_j X^{\alpha_j} (uX+v)^{\beta_j}$
- $\mathbb{K}$: 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

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

Theorem

$$P = \sum_{j=1}^{k} a_j X^{\alpha_j} (uX + v)^{\beta_j} \not\equiv 0, \text{ with } \alpha_1 \leq \cdots \leq \alpha_k$$

Bound on the valuation

Definition

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

Theorem

$$P = \sum_{j=1}^{k} a_j X^{\alpha_j} (uX + v)^{\beta_j} \not\equiv 0, \text{ with } \alpha_1 \leq \cdots \leq \alpha_k$$

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

Bound on the valuation

Definition

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

Theorem

$$P = \sum_{j=1}^{k} a_j X^{\alpha_j} (uX + v)^{\beta_j} \not\equiv 0, \text{ with } \alpha_1 \leq \cdots \leq \alpha_k$$

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

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

Bound on the valuation

Definition

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

Theorem

$$P = \sum_{j=1}^{k} a_j X^{\alpha_j} (uX + v)^{\beta_j} \not\equiv 0, \text{ with } \alpha_1 \leq \cdots \leq \alpha_k$$

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

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

The Wronskian

Definition

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

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

The Wronskian

Definition

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

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

Proposition (Bôcher, 1900)

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

Wronskian & valuation

Lemma

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

Wronskian & valuation

Lemma

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

Lemma

Let $f_j = X^{\alpha_j}(uX + v)^{\beta_j}$, linearly independent, s.t. $\alpha_j, \beta_j \geq k - 1$.

$$\mathrm{val}(\mathrm{wr}(f_1, \ldots, f_k)) \leq \sum_{j=1}^{k} \alpha_j$$

Wronskian & valuation

Lemma

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

Lemma

Let $f_j = X^{\alpha_j}(uX + v)^{\beta_j}$, linearly independent, s.t. $\alpha_j, \beta_j \geq k - 1$.

$$\mathrm{val}(\mathrm{wr}(f_1, \ldots, f_k)) \leq \sum_{j=1}^{k} \alpha_j$$

Proof of the theorem. $\mathrm{wr}(P, f_2, \ldots, f_k) = a_1 \,\mathrm{wr}(f_1, \ldots, f_k)$

Wronskian & valuation

Lemma

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

Lemma

Let $f_j = X^{\alpha_j}(uX + v)^{\beta_j}$, linearly independent, s.t. $\alpha_j, \beta_j \geq k - 1$.

$$\mathrm{val}(\mathrm{wr}(f_1, \ldots, f_k)) \leq \sum_{j=1}^{k} \alpha_j$$

Proof of the theorem. $\mathrm{wr}(P, f_2, \ldots, f_k) = a_1 \,\mathrm{wr}(f_1, \ldots, f_k)$

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

With some dirty computations...

- Generalization: $\sum_{j=1}^{k} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}}$, $\deg(f_i) \leq d$

With some dirty computations...

- Generalization: $\sum_{j=1}^{k} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}}$, $\deg(f_i) \leq d$
- Lower bound: $\exists P, \mathrm{val}(P) \geq \alpha_1 + (2k-3)$

With some dirty computations...

- Generalization: $\sum_{j=1}^{k} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}}$, $\deg(f_i) \leq d$
- Lower bound: $\exists P, \mathrm{val}(P) \geq \alpha_1 + (2k-3)$

$$-1 + (1+X)^{2k+3} - \sum_{j=0}^{k} \frac{2k+3}{2j+1} \binom{k+1+j}{k+1-j} X^{2j+1} (1+X)^{k+1-j}$$

With some dirty computations...

- Generalization: $\sum_{j=1}^{k} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}}$, $\deg(f_i) \leq d$
- Lower bound: $\exists P, \mathrm{val}(P) \geq \alpha_1 + (2k-3)$

$$-1 + (1+X)^{2k+3} - \sum_{j=0}^{k} \frac{2k+3}{2j+1} \binom{k+1+j}{k+1-j} X^{2j+1} (1+X)^{k+1-j}$$

$$= X^{2k+3}$$

Gap Theorem

Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_1}$$

with $u, v \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. 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 $P_0 \equiv 0$ and $P_1 \equiv 0$.

Gap Theorem

Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_1}$$

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

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

then $P \equiv 0$ iff both $P_0 \equiv 0$ and $P_1 \equiv 0$.

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

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

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

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

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

Finding linear factors

Observation + Gap Theorem

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

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

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

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

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

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

Remark

We need $\mathbb{K}$ to be an algebraic number field.

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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ $\rightsquigarrow$ [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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ $\rightsquigarrow$ [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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ $\rightsquigarrow$ [Lenstra'99]
3. If $u, v \neq 0$:
   - Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_j a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{k}{2}$

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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ $\rightsquigarrow$ [Lenstra'99]
3. If $u, v \neq 0$:
   - Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_j a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{k}{2}$
   - Invert the roles of X and Y, to get $\beta_{\max} \leq \beta_{\min} + \binom{k}{2}$

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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ $\rightsquigarrow$ [Lenstra'99]
3. If $u, v \neq 0$:
   - Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_j a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{k}{2}$
   - Invert the roles of X and Y, to get $\beta_{\max} \leq \beta_{\min} + \binom{k}{2}$
   - Apply some dense factorization algorithm [Kaltofen'82, ..., Lecerf'07]

Complexity

Main computational task: Factorization of dense polynomials

Complexity

Main computational task: Factorization of dense polynomials

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

Complexity

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

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

Complexity

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

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

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

Complexity

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

- [Kaltofen-Koiran'05]: $\mathrm{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$
- Here: $\mathrm{gap}(P) = \mathcal{O}(k^2)$

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

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

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

Theorem

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

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

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

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

Positive characteristic

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

Positive characteristic

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

Theorem

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

Algorithms in positive characteristic

Theorem

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

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

Algorithms in positive characteristic

Theorem

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

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

Algorithms in positive characteristic

Theorem

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

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

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

Algorithms in positive characteristic

Theorem

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

- doable in **randomized polynomial time** if $uvw \neq 0$;
- NP-**hard** 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

+ More **elementary** proofs for [Kaltofen & Koiran'05]

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
– Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

$\rightsquigarrow$ Impossible in positive characteristic

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

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

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

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

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

  $\rightsquigarrow$ Impossible 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**?

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

  $\rightsquigarrow$ Impossible 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**?
- What is the complexity of **counting** the number of factors?

Conclusion

+ More **elementary** proofs for [Kaltofen & Koiran'05]
+ Complexity independent of the height $\rightsquigarrow$ **large coefficients**
+ Consequences in large **positive characteristic**
− Still relies on [Lenstra'99] $\rightsquigarrow$ number fields

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

  $\rightsquigarrow$ Impossible 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**?
- What is the complexity of **counting** the number of factors?

arXiv:1206.4224