Factoring bivariate lacunary polynomials without heights

Bruno Grenet
ÉNS Lyon & U. Rennes 1

Joint work with

Arkadev Chattophyay
TIFR, Mumbai

Pascal Koiran
ÉNS Lyon

Natacha Portier
ÉNS Lyon

Yann Strozecki
U. Versailles

Séminaire de théorie des nombres du LMNO — Caen, le 1^er^ février 2013

Representation of Univariate Polynomials

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

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

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

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

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

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

Factorization of polynomials

Factorization of a polynomial P

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

Factorization of polynomials

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]

Factorization of polynomials

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \ldots, X_n]$

Factorization of polynomials

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \ldots, X_n]$
- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]

Factorization of polynomials

Factorization of a polynomial P

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

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

Factorization of polynomials

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: 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]

Factorization of polynomials

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: 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]

Example

$$X^p - 1 = (X - 1)(1 + X + \cdots + X^{p-1})$$

Factorization of polynomials

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: 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]

Example

$$X^p - 1 = (X - 1)(1 + X + \cdots + X^{p-1})$$

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

Factorization of sparse univariate polynomials

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

Factorization of sparse univariate polynomials

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

Theorem (Cucker-Koiran-Smale'98)

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

Factorization of sparse univariate polynomials

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

Theorem (Cucker-Koiran-Smale'98)

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

Theorem (H. Lenstra'99)

Polynomial-time algorithm to find **factors of degree $\leq d$** if $a_j \in \mathbb{Q}(\alpha)$.

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 $\mathbb{Q}(\alpha)$.

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 $\mathbb{Q}(\alpha)$.

Theorem (Avendaño-Krick-Sombra'07)

Polynomial-time algorithm to find **low-degree factors** of **bivariate** lacunary polynomials over $\mathbb{Q}(\alpha)$.

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:

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

- Factor out P_1, ..., P_s 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, …, P_s using a dense factorization algorithm
- Refinements:

Common algorithmic idea

- Recursively apply the Gap Theorem:

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

- Factor out P_1, …, P_s using a dense factorization algorithm
- Refinements:
  - Factor out $\gcd(P_1, \ldots, P_s)$

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, …, P_s using a dense factorization algorithm
- Refinements:
  - Factor out $\gcd(P_1, \ldots, P_s)$
  - Factor out only P_1 & check which factors divide the other P_t's

Common algorithmic idea

- Recursively apply the Gap Theorem:

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

- Factor out P_1, …, P_s using a dense factorization algorithm
- Refinements:
  - Factor out $\gcd(P_1, \dots, P_s)$
  - Factor out only P_1 & check which factors divide 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, Avendaño-Krick-Sombra'07]

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, Avendaño-Krick-Sombra'07]
- 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, Avendaño-Krick-Sombra'07]
- gap(P) **independent of the height**
  - ⇝ 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, Avendaño-Krick-Sombra'07]
- gap(P) **independent of the height**
  - ⇝ More elementary algorithms
  - ⇝ 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, Avendaño-Krick-Sombra'07]
- 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, Avendaño-Krick-Sombra'07]
- gap(P) **independent of the height**
  - ⇝ More elementary algorithms
  - ⇝ 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

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

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

Bound on the valuation

Definition

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

Theorem

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

Then

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

Bound on the valuation

Definition

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

Theorem

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

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

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

Bound on the valuation

Definition

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

Theorem

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

Then

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

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

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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. 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 $P_0 \equiv 0$ 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 $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. If ℓ is the smallest index s.t.

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

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

The Wronskian

Definition

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

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

The Wronskian

Definition

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

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

Proposition (Bôcher, 1900)

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

Wronskian & valuation

Lemma

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

Wronskian & valuation

Lemma

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

Proof.

$$\begin{array}{c} \\ 0 \\ -1 \\ \vdots \\ -(k-1) \end{array} \begin{array}{c} \begin{array}{cccc} \mathrm{val}(f_1) & \mathrm{val}(f_2) & \dots & \mathrm{val}(f_k) \end{array} \\ \begin{bmatrix} f_1 & f_2 & \dots & f_k \\ f_1' & f_2' & \dots & f_k' \\ \vdots & \vdots & & \vdots \\ f_1^{(k-1)} & f_2^{(k-1)} & \dots & f_k^{(k-1)} \end{bmatrix} \end{array}$$

Upper bound for the valuation

Lemma

Let $f_j = X^{\alpha_j}(uX+v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geq k-1$. Then

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

Upper bound for the valuation

Lemma

Let $f_j = X^{\alpha_j}(uX+v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geq k-1$. Then

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

Proof idea. Write

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

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. $\alpha_j, \beta_j \geq k-1$. Then

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

Proof idea. Write

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

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

Proof of the Theorem

Theorem

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

Then

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

Proof of the Theorem

Theorem

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

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

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

Proof of the Theorem

Theorem

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

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

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

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

Proof of the Theorem

Theorem

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

Then

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

Proof. $\operatorname{wr}(P, f_2, \dots, f_k) = a_1 \operatorname{wr}(f_1, \dots, f_k)$

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

How far from optimality?

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

How far from optimality?

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

How far from optimality?

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

How far from optimality?

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

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

A generalization

Theorem

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

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

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

A generalization

Theorem

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

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

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

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

A generalization

Theorem

Let $(\alpha_{ij}) \in \mathbb{R}^{k\times m}$ and

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

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

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

Algorithms

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

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

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

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
- **N.B.**: Algorithms are from [Kaltofen-Koiran'05]

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 (2)

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

Polynomial Identity Testing (2)

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

Polynomial Identity Testing (2)

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

Let $Y = uX + v$. Then

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

Polynomial Identity Testing (2)

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

Let $Y = uX + v$. Then

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

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

Polynomial Identity Testing (2)

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

Let $Y = uX + v$. Then

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

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

number of monomials, exponents $\leq$ poly(size(Q))

Generalization of PIT

Theorem

Let

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

where $f_1, \dots, f_m \in \mathbb{K}[X]$ are given in **dense** representation, $(\alpha_{ij}) \in \mathbb{Z}_+^{k \times m}$ and $(a_j) \in \mathbb{K}^k$. Then one can test if P vanishes in deterministic polynomial time.

Generalization of PIT

Theorem

Let

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

where $f_1, \dots, f_m \in \mathbb{K}[X]$ are given in **dense** representation, $(\alpha_{ij}) \in \mathbb{Z}_+^{k \times m}$ and $(a_j) \in \mathbb{K}^k$. Then one can test if P vanishes in deterministic polynomial time.

Proof sketch.

- Factor out each f_i and rewrite $P = \sum_{j=1}^{k} b_j \prod_{i=1}^{M} g_i^{\beta_{ij}}$.

Generalization of PIT

Theorem

Let

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

where $f_1, \dots, f_m \in \mathbb{K}[X]$ are given in **dense** representation, $(\alpha_{ij}) \in \mathbb{Z}_+^{k \times m}$ and $(a_j) \in \mathbb{K}^k$. Then one can test if P vanishes in deterministic polynomial time.

Proof sketch.

- Factor out each f_i and rewrite $P = \sum_{j=1}^{k} b_j \prod_{i=1}^{M} g_i^{\beta_{ij}}$.
- Then $\mu_{g_i}(P) \leq \max_{1 \leq j \leq k} \left(\beta_{ij} + \sum_{\ell \neq i} \frac{\deg(g_\ell)}{\deg(g_i)} \binom{k+1-j}{2} \right)$ for each g_i.

Generalization of PIT

Theorem

Let

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

where $f_1, \dots, f_m \in \mathbb{K}[X]$ are given in **dense** representation, $(\alpha_{ij}) \in \mathbb{Z}_+^{k \times m}$ and $(a_j) \in \mathbb{K}^k$. Then one can test if P vanishes in deterministic polynomial time.

Proof sketch.

- Factor out each f_i and rewrite $P = \sum_{j=1}^{k} b_j \prod_{i=1}^{M} g_i^{\beta_{ij}}$.
- Then $\mu_{g_i}(P) \leq \max_{1\leq j\leq k} \left(\beta_{ij} + \sum_{\ell \neq i} \frac{\deg(g_\ell)}{\deg(g_i)} \binom{k+1-j}{2}\right)$ for each g_i.
- Gap Theorem $\rightsquigarrow$ write P as a sum of low-degree polynomials.

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

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

$\rightsquigarrow$ 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 $u, v \neq 0$:
   - 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 $\sum_j a_j Y^{\beta_j}$ [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 $u, v \neq 0$:
   - 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 $\sum_j a_j Y^{\beta_j}$ [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 $u, v \neq 0$:
   - 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]

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
$\Longrightarrow$ 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 $\mathrm{gap}(P)$

- [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

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

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

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 multi-linear 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

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

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

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

$\mathrm{wr}(f_1, \dots, f_k) \neq 0 \iff f_j$'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 $p > \max_j(\alpha_j + \beta_j)$. Finding factors of the form $(uX + vY + w)$ is

- doable 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 $p > \max_j(\alpha_j + \beta_j)$. Finding factors of the form $(uX + vY + w)$ is

- doable in **randomized polynomial time** if $uvw \neq 0$;
- NP-**hard** 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 $p > \max_j(\alpha_j + \beta_j)$.
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 $\mathbb{F}_{p^s}$

Finding linear factors

Theorem

Let $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_{p^s}[X, Y]$, where $p > \max_j(\alpha_j + \beta_j)$.
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

Summary

- **Elementary** proofs & algorithms for the factorization of lacunary bivariate polynomials

Summary

+ **Elementary** proofs & algorithms for the factorization of lacunary bivariate polynomials
    - Easier to implement

Summary

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

Summary

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

Summary

- **Elementary** proofs & algorithms for the factorization 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 the factorization 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 the factorization 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 the factorization 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 the factorization 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