Factoring bivariate lacunary polynomials without heights

Bruno Grenet

ÉNS Lyon

Arkadev Chattophyay

U. Toronto

Pascal Koiran

ÉNS Lyon

Natacha Portier

ÉNS Lyon

Yann Strozecki

U. Paris Sud XI

Rencontres du GdT CMF – Turing 2012 – Lyon, July 4. 2012

Representation of Univariate Polynomials

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

Representations

- Dense:

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

- Sparse:

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

Representation of Multivariate Polynomials

$$P(x, y, z) = x^2y^3z^5 - 4x^3y^3z^2 + 8x^5z^2 + 5xyz + 1$$

Representations

- Dense:

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

- Lacunary (supersparse):

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

Representation of Multivariate Polynomials

$$P(x, y, z) = x^2y^3z^5 - 4x^3y^3z^2 + 8x^5z^2 + 5xyz + 1$$

Representations

- Dense:

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

- Sparse:

$$\{(||, |||, ||||| : 1), (|||, |||, || : -4), (|||||, , || : 8), (|, |, | : 5), (, , : 1)\}$$

- Lacunary (supersparse):

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

Size of the lacunary representation

Definition

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

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

Factorization of sparse univariate polynomials

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

Factorization of sparse univariate polynomials

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

Theorem (Cucker, Koiran, Smale, 1998)

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

Factorization of sparse univariate polynomials

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

Theorem (Cucker, Koiran, Smale, 1998)

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

Theorem (Lenstra, 1999)

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, 2005)

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

Factorization of lacunary polynomials

Theorem (Kaltofen & Koiran, 2005)

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

Theorem (Kaltofen & Koiran, 2006)

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

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_1}$$

with $\alpha_{n1} \leq \alpha_{n2} \leq \cdots \leq \alpha_{nk}$.

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_1}$$

with $\alpha_{n1} \le \alpha_{n2} \le \cdots \le \alpha_{nk}$. Suppose that

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

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_1}$$

with $\alpha_{n1} \leq \alpha_{n2} \leq \cdots \leq \alpha_{nk}$. Suppose that

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

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

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X_1^{\alpha_{1j}} \cdots X_n^{\alpha_{nj}}}_{P_1}$$

with $\alpha_{n1} \leq \alpha_{n2} \leq \cdots \leq \alpha_{nk}$. Suppose that

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

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

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

This talk

Get rid of the heights!

This talk

Get rid of the heights!

- Linear factors of bivariate lacunary polynomials [KaKoi05]

This talk

Get rid of the heights!

- Linear factors of bivariate lacunary polynomials [KaKoi05]
- gap(P) independent of the height

This talk

Get rid of the heights!

- Linear factors of bivariate lacunary polynomials [KaKoi05]
- $\mathrm{gap}(P)$ independent of the height

  $\rightsquigarrow$ valid over any field of char. 0

This talk

Get rid of the heights!

- Linear factors of bivariate lacunary polynomials [KaKoi05]
- $\mathrm{gap}(P)$ independent of the height

  $\rightsquigarrow$ valid over any field of char. 0
- More elementary algorithms

This talk

Get rid of the heights!

- Linear factors of bivariate lacunary polynomials [KaKoi05]
- $\mathrm{gap}(P)$ independent of the height

  $\rightsquigarrow$ valid over any field of char. 0
- More elementary algorithms
- Extension to multilinear factors

This talk

Get rid of the heights!

- Linear factors of bivariate lacunary polynomials [KaKoi05]
- $\mathrm{gap}(P)$ independent of the height

  $\rightsquigarrow$ valid over any field of char. 0
- More elementary algorithms
- 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

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

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

Linear factors of bivariate polynomials

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

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

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

Bound on the valuation

Definition

Let $P \in \mathbb{K}[X]$. Then $\mathrm{val}(P) = \max\{\alpha : \exists Q, P = X^{\alpha} Q\}$.

Bound on the valuation

Definition

Let $P \in \mathbb{K}[X]$. Then $\mathrm{val}(P) = \max\{\alpha : \exists Q, P = X^{\alpha} Q\}$.

Theorem

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

Let $P \in \mathbb{K}[X]$. Then $\mathrm{val}(P) = \max\{\alpha : \exists Q, P = X^\alpha Q\}$.

Theorem

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(1+X)^{\beta_j} \not\equiv 0$, *with* $\alpha_1 \le \cdots \le \alpha_k$. *Then*

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

- $X^{\alpha_j}(1+X)^{\beta_j}$ linearly independent

Bound on the valuation

Definition

Let $P \in \mathbb{K}[X]$. Then $\mathrm{val}(P) = \max\{\alpha : \exists Q, P = X^\alpha Q\}$.

Theorem

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

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

- $X^{\alpha_j}(1+X)^{\beta_j}$ 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

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

The Wronskian

Definition

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

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

Proposition

$W(f_1, \dots, f_k) \neq 0 \iff$ *the f_j's are linearly independent.*

Wronskian & valuation

Lemma

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

Wronskian & valuation

Lemma

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

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

Upper bound for the valuation

Lemma

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

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

Upper bound for the valuation

Lemma

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

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

Proof idea. Write

$$\mathrm{W}(f_1, \ldots, f_k) = X^{\sum_j \alpha_j - \binom{k}{2}}(1+X)^{\sum_j \beta_j - \binom{k}{2}} \det M$$

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

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

Proof of the Theorem

Theorem

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

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

Proof of the Theorem

Theorem

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

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

Proof.

$$\mathrm{val}(\mathrm{W}(f_1, \ldots, f_k)) = \mathrm{val}(\mathrm{W}(P, f_2, \ldots, f_k))$$

Proof of the Theorem

Theorem

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

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

Proof.

$$\sum_{j=1}^{k} \alpha_j \geq \mathrm{val}(\mathrm{W}(f_1, \ldots, f_k)) = \mathrm{val}(\mathrm{W}(P, f_2, \ldots, f_k))$$

$$\geq \mathrm{val}(P) + \sum_{j=2}^{k} \alpha_j - \binom{k}{2}$$

Proof of the Theorem

Theorem

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

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

Proof.

$$\sum_{j=1}^{k} \alpha_j \geq \mathrm{val}(\mathrm{W}(f_1, \ldots, f_k)) = \mathrm{val}(\mathrm{W}(P, f_2, \ldots, f_k))$$

$$\geq \mathrm{val}(P) + \sum_{j=2}^{k} \alpha_j - \binom{k}{2}$$

Some comments

$$\mathrm{val}\left(\sum_{j=1}^{k} a_j X^{\alpha_j}(1+X)^{\beta_j}\right) \leq \max_{1\leq j\leq k}\left(\alpha_j + \binom{k+1-j}{2}\right)$$

- $uX + v = v(Y+1)$, with $Y = \frac{u}{v}X$

Some comments

$$\mathrm{val}\left(\sum_{j=1}^{k} a_j X^{\alpha_j}(1+X)^{\beta_j}\right) \leq \max_{1\leq j\leq k}\left(\alpha_j + \binom{k+1-j}{2}\right)$$

- $uX + v = v(Y+1)$, with $Y = \frac{u}{v}X$
- Generalization: $\displaystyle\sum_{j=1}^{k} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}}$, $\deg(f_i) \leq d$

Some comments

$$\operatorname{val}\left(\sum_{j=1}^{k} a_j X^{\alpha_j}(1+X)^{\beta_j}\right) \leq \max_{1\leq j\leq k}\left(\alpha_j + \binom{k+1-j}{2}\right)$$

- $uX + v = v(Y+1)$, with $Y = \frac{u}{v}X$
- Generalization: $\displaystyle\sum_{j=1}^{k} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}}$, $\deg(f_i) \leq d$
- Lower bound: $\exists P, \operatorname{val}(P) \geq \alpha_1 + (2k-3)$

Our 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* $P_1 \equiv 0$.

Our 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* $P_1 \equiv 0$.

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

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

N.B.: Algorithms are from [Kaltofen & Koiran, 2005]

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 $\sum_j a_j v^{\beta_j} \stackrel{?}{=} 0 \rightsquigarrow$ [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 $\sum_j a_j v^{\beta_j} \stackrel{?}{=} 0 \rightsquigarrow$ [Lenstra'99] (idem $v = 0$)

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 $\sum_j a_j v^{\beta_j} \stackrel{?}{=} 0 \rightsquigarrow$ [Lenstra'99] (idem $v = 0$)
- 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))

Finding linear factors

Observation

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

Finding linear factors

Observation

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

- PIT algorithm $\rightsquigarrow$ test a **given** linear factor

Finding linear factors

Observation

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

- PIT algorithm $\rightsquigarrow$ test a **given** linear factor
- How to **find** linear factors?

Finding linear factors

Observation

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

- PIT algorithm $\rightsquigarrow$ test a **given** linear factor
- How to **find** linear factors?

Gap theorem

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

Finding linear factors

Observation

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

- PIT algorithm $\rightsquigarrow$ test a **given** linear factor
- How to **find** linear factors?

Gap theorem

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

$\implies$ 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 $\sum_j a_j Y^{\beta_j}$ $\rightsquigarrow$ [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 $\text{gap}(P)$

- [Kaltofen & Koiran, 2005] $\text{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$

Complexity

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

- [Kaltofen & Koiran, 2005] $\mathrm{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$

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, 2005] $\mathrm{gap}(P) = \mathcal{O}(k \log k + k \log h_P)$
- Here: $\mathrm{gap}(P) = \mathcal{O}(k^2)$

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

Generalization for PIT

Theorem

There exists a polynomial-time algorithm to test if $P(X) = \sum_j a_j X^{\alpha_j}(uX^{d} + v)^{\beta_j}$ *vanishes.*

Generalization for PIT

Theorem

There exists a polynomial-time algorithm to test if $P(X) = \sum_j a_j X^{\alpha_j}(uX^{d} + v)^{\beta_j}$ *vanishes.*

Proof. Write $\alpha_j = dq_j + r_j$.

$$P(X) = \sum_{r=0}^{d-1} X^r \underbrace{\sum_{j:r_j=r} a_j (X^d)^{q_j} (uX^d + v)^{\beta_j}}_{P_r(X^d)}$$

Generalization for factorization

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*

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

Generalization for factorization

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 $\sum_j a_j X^{\alpha_j} Y^{\beta_j}$.

Generalization for factorization

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

Generalization for factorization

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

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

Proposition

Let $\mathbb{K}$ be a field of characteristic p, and $f_1, \ldots, f_k \in \mathbb{K}[X]$. Then $f_1, \ldots, f_k$ are linearly independent over $\mathbb{K}[X^p]$ iff $\mathrm{W}(f_1, \ldots, f_k) \neq 0$.

Positive characteristic

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

Proposition

Let $\mathbb{K}$ be a field of characteristic p, and $f_1, \ldots, f_k \in \mathbb{K}[X]$. Then $f_1, \ldots, f_k$ are linearly independent over $\mathbb{K}[X^p]$ iff $\mathrm{W}(f_1, \ldots, f_k) \neq 0$.

Theorem

Let $\mathbb{K}$ be a field of char. p and $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(1+X)^{\beta_j} \not\equiv 0$,

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

If $p > \max_j(\alpha_j + \beta_j)$, then $\mathrm{val}(P) \leq \max_j\left(\alpha_j + \binom{k+1-j}{2}\right)$.

Algorithms in positive characteristic

$\mathbb{K} = \mathbb{F}_{p^s} = \mathbb{F}_p[\xi]/\langle\varphi\rangle$, φ irreducible of degree s

Algorithms in positive characteristic

$\mathbb{K} = \mathbb{F}_{p^s} = \mathbb{F}_p[\xi]/\langle\varphi\rangle$, φ irreducible of degree s

Theorem

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

Algorithms in positive characteristic

$\mathbb{K} = \mathbb{F}_{p^s} = \mathbb{F}_p[\xi]/\langle\varphi\rangle$, φ irreducible of degree s

Theorem

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

Theorem

There exists a randomized polynomial-time algorithm to find factors of the form $(uX+vY+w)$, $uvw \neq 0$, of a polynomial of the form $\sum_j a_j X^{\alpha_j} Y^{\beta_j} \not\equiv 0$, where $p > \max_j(\alpha_j+\beta_j)$.

Algorithms in positive characteristic

$\mathbb{K} = \mathbb{F}_{p^s} = \mathbb{F}_p[\xi]/\langle\varphi\rangle$, φ irreducible of degree s

Theorem

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

Theorem

There exists a randomized polynomial-time algorithm to find factors of the form $(uX+vY+w)$, $uvw \neq 0$, of a polynomial of the form $\sum_j a_j X^{\alpha_j} Y^{\beta_j} \not\equiv 0$, where $p > \max_j(\alpha_j+\beta_j)$.

- If u, v or w is zero, then finding such factors is NP-hard.
  [Kipnis-Shamir'99, Bi-Cheng-Rojas'12]

Algorithms in positive characteristic

$\mathbb{K} = \mathbb{F}_{p^s} = \mathbb{F}_p[\xi]/\langle\varphi\rangle$, φ irreducible of degree s

Theorem

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

Theorem

There exists a randomized polynomial-time algorithm to find factors of the form $(uX+vY+w)$, $uvw \neq 0$, of a polynomial of the form $\sum_j a_j X^{\alpha_j} Y^{\beta_j} \not\equiv 0$, where $p > \max_j(\alpha_j+\beta_j)$.

- If u, v or w is zero, then finding such factors is NP-hard.
  [Kipnis-Shamir'99, Bi-Cheng-Rojas'12]
- Only randomized dense factorization algorithms over $\mathbb{F}_{p^s}$

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

▶ Extend to 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

- Extend to low-degree factors of multivariate polynomials
- Extend to the univariate case

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

- Extend to low-degree factors of multivariate polynomials
- Extend to the univariate case

  $\rightsquigarrow$ 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

- Extend to low-degree factors of multivariate polynomials
- Extend to the univariate case

  $\rightsquigarrow$ Impossible in positive characteristic
- Improve the $\binom{k}{2}$, or the lower bound

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

- Extend to low-degree factors of multivariate polynomials
- Extend to the univariate case

  $\rightsquigarrow$ Impossible in positive characteristic
- Improve the $\binom{k}{2}$, or the lower bound

Thank you!

arXiv:1206.4224