Factorization of lacunary polynomials

Bruno Grenet
ÉNS Lyon & U. Rennes 1

Joint work with

Arkadev Chattopadhyay
TIFR, Mumbai

Pascal Koiran
ÉNS Lyon

Natacha Portier
ÉNS Lyon

Yann Strozecki
U. Versailles

École Jeunes Chercheurs en Informatique Mathématique — Perpignan, April 12, 2013

Factorization: classical algorithms

Factorization of a polynomial P

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

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

Factorization: classical algorithms

Factorization of a polynomial P

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

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

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

Complexity

Polynomial in the **degree** of the polynomials

The case of lacunary polynomials

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

The case of lacunary polynomials

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

The case of lacunary polynomials

$$
\begin{aligned}
&X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\
&\quad = (X + Y - 1) \times (X^{101}Y^{101} - 1) \\
&\quad = (X + Y - 1) \times (XY - 1) \times (1 + XY + \cdots + X^{100}Y^{100})
\end{aligned}
$$

The case of lacunary polynomials

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

Definition

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

The case of lacunary polynomials

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

Definition

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

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

The case of lacunary polynomials

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

Definition

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

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

The case of lacunary polynomials

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

Definition

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

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

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

The case of lacunary polynomials

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

Definition

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

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

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

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

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

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies P_0(x) = P_1(x) = 0$.

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies P_0(x) = P_1(x) = 0$.

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

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies P_0(x) = P_1(x) = 0$.

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

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies P_0(x) = P_1(x) = 0$.

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

- Racine commune : -3

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies P_0(x) = P_1(x) = 0$.

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

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

Integral roots of integral polynomials

Gap Theorem (Cucker-Koiran-Smale'98)

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}}_{P_1} \in \mathbb{Z}[X]$$

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

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

then for all x, $|x| \geq 2$, $P(x) = 0 \implies P_0(x) = P_1(x) = 0$.

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

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

Factorization of lacunary polynomials

Theorems

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

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

Factorization of lacunary polynomials

Theorems

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

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

Factorization of lacunary polynomials

Theorems

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

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

Factorization of lacunary polynomials

Theorems

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

- **linear** factors of **univariate** polynomials over $\mathbb{Z}$;
  [Cucker-Koiran-Smale'98]
- **low-degree** factors of **univariate** polynomials over $\mathbb{Q}(\alpha)$;
  [Lenstra'99]
- **linear** factors of **bivariate** polynomials over $\mathbb{Q}$;
  [Kaltofen-Koiran'05]
- **low-degree** factors of **multivariate** polynomials over $\mathbb{Q}(\alpha)$.
  [Kaltofen-Koiran'06]

Linear factors of bivariate polynomials

Observation

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

Linear factors of bivariate polynomials

Observation

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

Gap Theorem

Let

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

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

Linear factors of bivariate polynomials

Observation

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

Gap Theorem

Let

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

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 $P_1 \equiv 0$.

Linear factors of bivariate polynomials

Observation

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

Gap Theorem

Let

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

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 $(Y - uX - v)$ divides P iff it divides both P_0 and P_1.

Linear factors of bivariate polynomials

Observation

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

Gap Theorem

Let

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

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

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

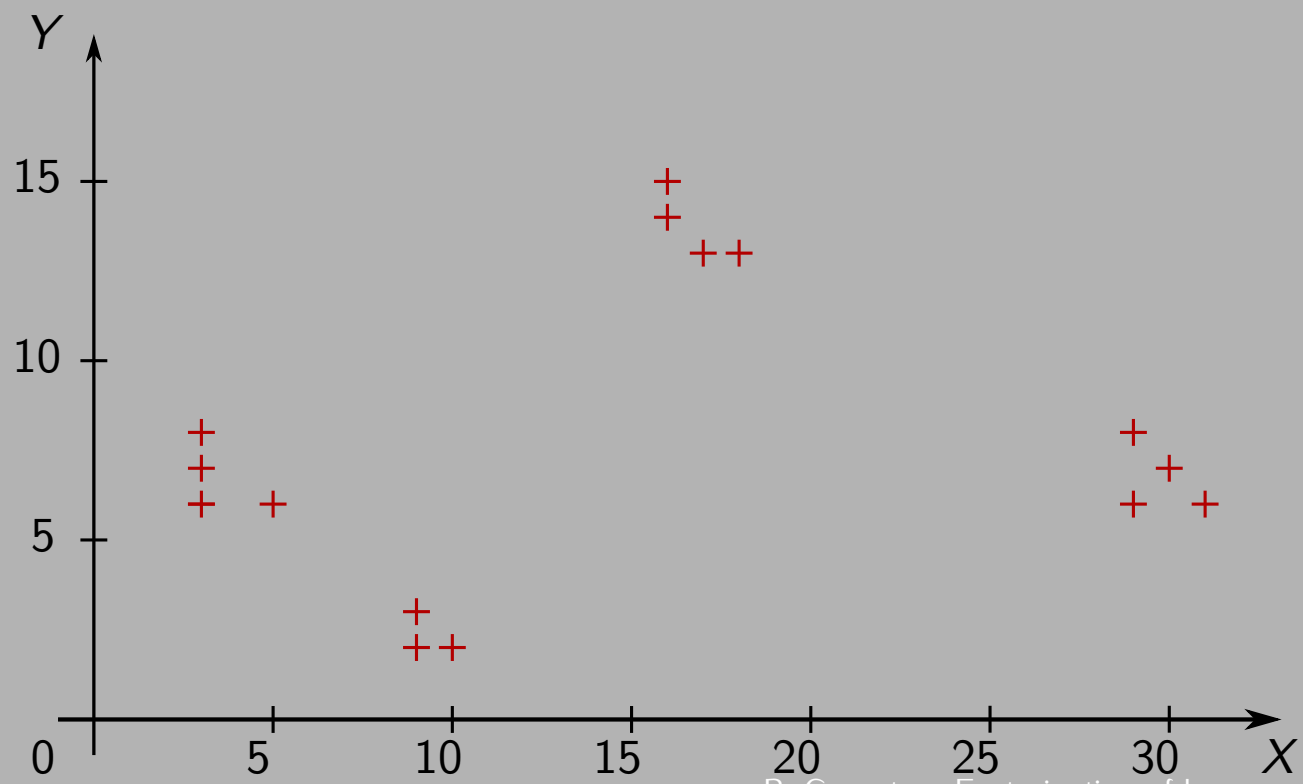
then every linear factor of P divides both P_0 and P_1 if $uv \neq 0$.

Example

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

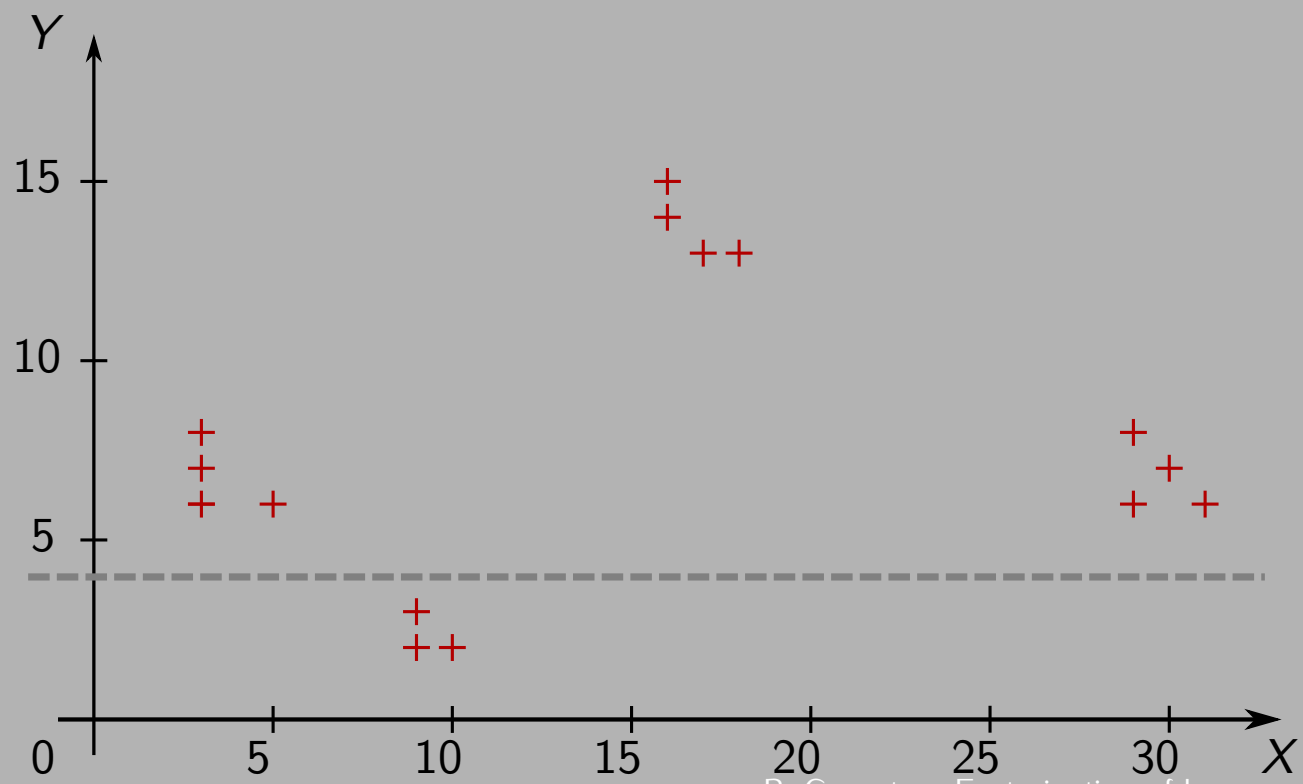
Example

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



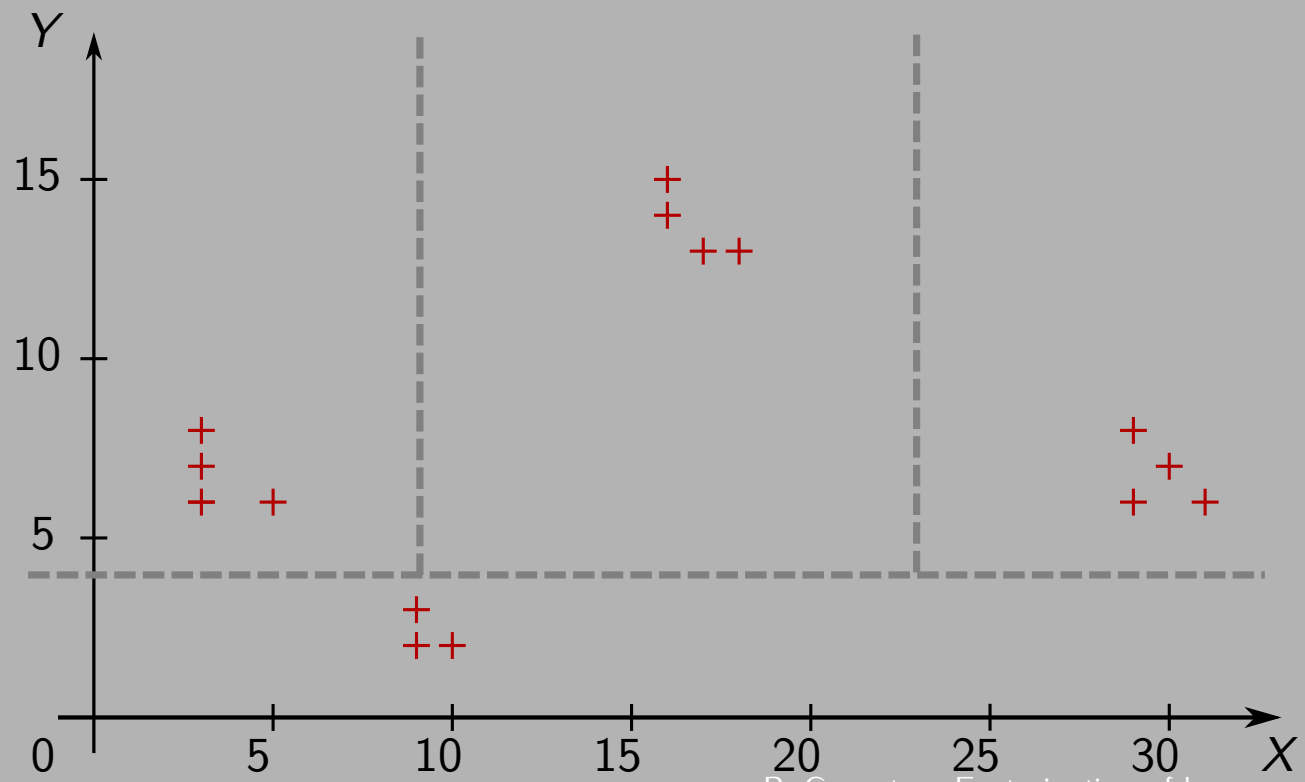
Example

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



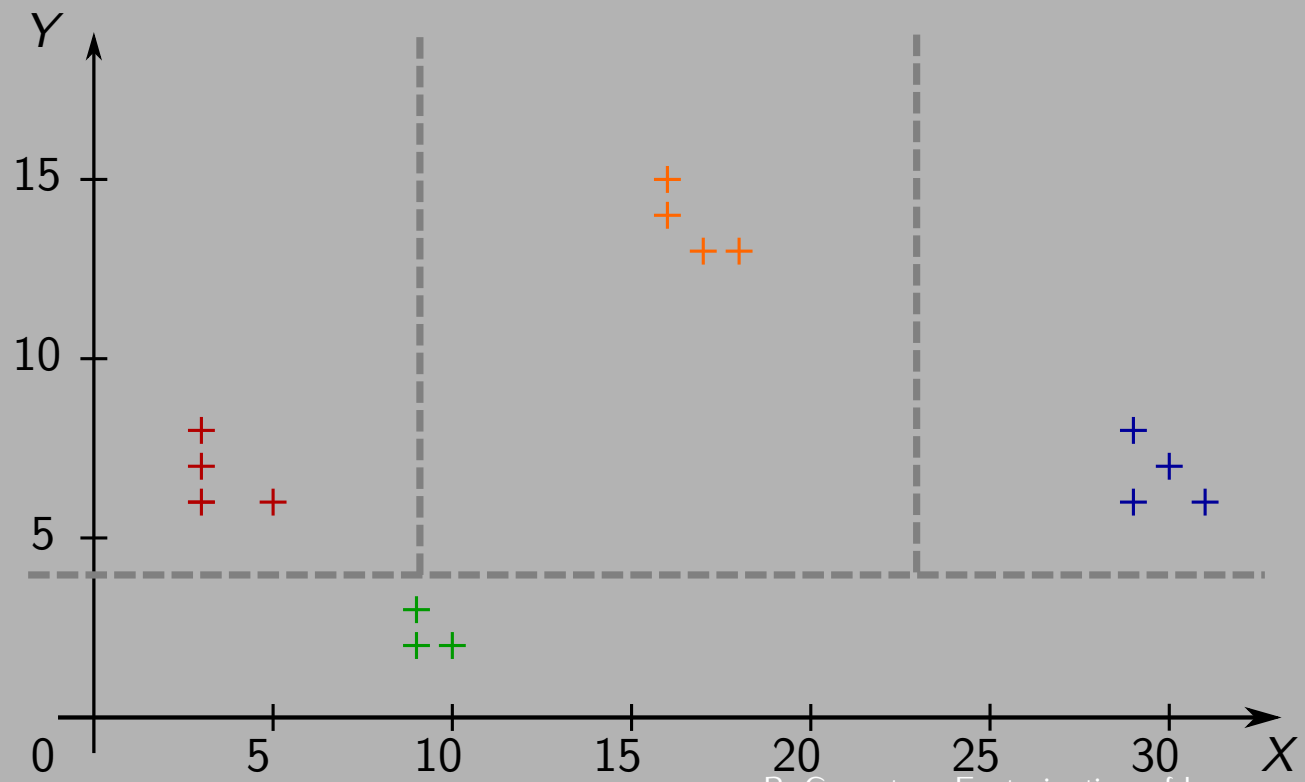
Example

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



Example

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



Example (2)

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

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

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

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

Example (2)

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

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

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

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

Example (2)

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

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

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

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

Example (2)

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

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

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

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

Example (2)

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

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

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

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

Example (2)

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

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

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

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

Example (2)

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

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

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

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

Example (2)

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

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

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

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

Example (2)

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

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

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

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

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

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 $P \in \mathbb{K}[X]$

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

Bound on the valuation

Definition

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

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

Theorem

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

Bound on the valuation

Definition

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

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

Theorem

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

Then

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

Bound on the valuation

Definition

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

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

Theorem

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

Then

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

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

Bound on the valuation

Definition

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

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

Theorem

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

Then

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

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

Gap Theorem

Theorem

Let

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

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 $P_1 \equiv 0$.

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 $P_1 \equiv 0$.

$$P = \left(c_{\mathrm{val}(P_0)} X^{\mathrm{val}(P_0)} + \cdots \right)$$

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 $P_1 \equiv 0$.

$$P = \left(c_{\mathrm{val}(P_0)} X^{\mathrm{val}(P_0)} + \cdots \right) + X^{\alpha_{\ell+1}} \left(a_{\ell+1} (uX+v)^{\beta_{\ell+1}} + \cdots \right)$$

The Wronskian

Definition

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

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

The Wronskian

Definition

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

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

Proposition (Bôcher, 1900)

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

Wronskian & valuation

Lemma

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

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

Wronskian & valuation

Lemma

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

Lemma

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

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

Wronskian & valuation

Lemma

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

Lemma

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

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

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

Wronskian & valuation

Lemma

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

Lemma

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

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

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

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

Final algorithm

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

Final algorithm

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

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

Final algorithm

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

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

Final algorithm

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

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

Final algorithm

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

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

Final algorithm

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

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

Final algorithm

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

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

Final algorithm

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

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

Final algorithm

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

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

Code Sage

```
def SplitList(listOfCouples,comp,cst):
    listOfCouples.sort(key=lambda c:c[comp])
    gap=listOfCouples[0][comp];
    imin=0
    res=[]

    for i in range(1,len(listOfCouples)):
        if listOfCouples[i][comp] > cst*gap:
            res+=[listOfCouples[imin:i]];
            gap=listOfCouples[i][comp];
            imin=i;
        else:
            gap+=i-imin;
    res+=[listOfCouples[imin:]];

    return res

def Clusterize(listOfCouples,cst):

    firstSplit=SplitList(listOfCouples,0,cst)
    secondSplit=[]

    for l in firstSplit:
        secondSplit+=SplitList(l,1,cst)

    if len(secondSplit) == 1:
        return secondSplit
    else:
        res=[]
        for l in secondSplit:
            res+=Clusterize(l,cst)
        return res
```

```
def TrulyBivariateLinearFactors(poly):

    exponents=poly.exponents();
    clustersExp=Clusterize(exponents,1);

    pvar=poly.variables();
    x=pvar[0]
    y=pvar[1]

    clustersPoly=[]

    for cluster in clustersExp:
        xmin=min(cluster,key=lambda c:c[0])[0]
        ymin=min(cluster,key=lambda c:c[1])[1]
        p=sum([poly[e]*x^(e[0]-xmin)*y^(e[1]-
              ymin) for e in cluster])
        if p.nvariables()<2:
            return {}
        else:
            clustersPoly+=[p]

    d = dict(gcd(clustersPoly).factor())
    return dict((k,d[k]) for k in d.keys() \
                if k.nvariables()==2 and k.
                    degree()==1)
```

Positive characteristic

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

Positive characteristic

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

Theorem

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

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

Positive characteristic

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

Theorem

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

Theorem

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

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

Positive characteristic

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

Theorem

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

Theorem

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

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

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]
- Results in large **positive characteristic**

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]
- Results in large **positive characteristic**
- There exists $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}$ s.t. $\mathrm{val}(P) = \alpha_1 + (2\ell - 3)$

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]
- Results in large **positive characteristic**
- There exists $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}$ s.t. $\mathrm{val}(P) = \alpha_1 + (2\ell - 3)$

Main open problem

Extend to low-degree factors of multivariate polynomials

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]
- Results in large **positive characteristic**
- There exists $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}$ s.t. $\mathrm{val}(P) = \alpha_1 + (2\ell - 3)$

Main open problem

Extend to low-degree factors of multivariate polynomials

Thank you!