Factoring bivariate lacunary polynomials without heights

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

ISSAC 2013 — Boston
June 29, 2013
Classical factorization algorithms

Factorization of a polynomial $P$

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

Factorization of a polynomial $P$

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

\[ \mathbb{Z}[X] \]

[Lenstra-Lenstra-Lovász’82]

\[ \downarrow \]

\[ \mathbb{Q}(\alpha)[X] \]

[A. Lenstra’83, Landau’83]

\[ \downarrow \]

\[ \mathbb{Q}(\alpha)[X_1, \ldots, X_n] \]

[Kaltofen’85, A. Lenstra’87]
Classical factorization algorithms

Factorization of a polynomial $P$

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

$\mathbb{Z}[X]$

$[\text{Lenstra-Lenstra-Lovász’82}]$

$\mathbb{Q}(\alpha)[X]$

$[\text{A. Lenstra’83, Landau’83}]$

$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$

$[\text{Kaltofen’85, A. Lenstra’87}]$

$\mathbb{F}_q[X]$

$[\text{Berlekamp’67}]$

$\mathbb{F}_q[X_1, \ldots, X_n]$
Classical factorization algorithms

Factorization of a polynomial $P$

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

$\mathbb{Z}[X]$

[Lenstra-Lenstra-Lovász’82]

$\mathbb{Q}(\alpha)[X]$

$\mathbb{F}_q[X]$

[Berlekamp’67]

$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$

[Kaltofen’85, A. Lenstra’87]

Complexity

Polynomial in the \textbf{degree} of the polynomials
Lacunary polynomials

\[ X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \]
Lacunary polynomials

\[ X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \]
\[ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \]
Lacunary polynomials

\[ X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \]
\[ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \]
\[ = (X + Y - 1) \times (XY - 1) \times (1 + XY + \ldots + X^{100}Y^{100}) \]
Lacunary polynomials

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

▷ Algorithms polynomial in \( \log(\deg(P)) \)
Lacunary polynomials

\[ X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \]

\[ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \]

\[ = (X + Y - 1) \times (XY - 1) \times (1 + XY + \cdots + X^{100}Y^{100}) \]

- Algorithms polynomial in \( \log(\deg(P)) \)
- Some factors only
Lacunary polynomials

\[ X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \]

\[ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \]

\[ = (X + Y - 1) \times (XY - 1) \times (1 + XY + \cdots + X^{100}Y^{100}) \]

▶ Algorithms polynomial in \( \log(\deg(P)) \)
▶ Some factors only

**Definition**

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

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

- Algorithms polynomial in \( \log(\deg(P)) \)
- Some factors only

**Definition**

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

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

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

- Algorithms polynomial in \(\log(\deg(P))\)
- Some factors only

**Definition**

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

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

Theorems

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

- linear factors of \textit{univariate} polynomials over $\mathbb{Z}$;
  
  \cite{Cucker-Koiran-Smale'98}

- low-degree factors of \textit{univariate} polynomials over $\mathbb{Q}(\alpha)$;
  
  \cite{H. Lenstra'99}

- linear factors of \textit{bivariate} polynomials over $\mathbb{Q}$;
  
  \cite{Kaltofen-Koiran'05}

- low-degree factors of \textit{multivariate} polynomials over $\mathbb{Q}(\alpha)$;
  
  \cite{Kaltofen-Koiran'06}
Theorems

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

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

- low-degree factors of univariate polynomials over $\mathbb{Q}(\alpha)$;  
  [H. Lenstra’99]

- linear factors of bivariate polynomials over $\mathbb{Q}$;  
  [Kaltofen-Koiran’05]

- low-degree factors of multivariate polynomials over $\mathbb{Q}(\alpha)$;  
  [Kaltofen-Koiran’06]

B. Grenet — Factoring bivariate lacunary polynomials without heights
Theorems

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

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

- **low-degree factors of univariate** polynomials over $\mathbb{Q}(\alpha)$;
  
  [H. Lenstra’99]

- **linear factors of bivariate** polynomials over $\mathbb{Q}$;
  
  [Kaltofen-Koiran’05]
Theorem 1

Deterministic polynomial time (in $\log(\deg P)$) algorithms for:

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

- low-degree factors of univariate polynomials over $\mathbb{Q}(\alpha)$;
  
  [H. Lenstra'99]

- linear factors of bivariate polynomials over $\mathbb{Q}$;
  
  [Kaltofen-Koiran'05]

- low-degree factors of multivariate polynomials over $\mathbb{Q}(\alpha)$.
  
  [Kaltofen-Koiran'06]
Integral roots of integral polynomials

**Gap Theorem**

Let

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

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 \in \mathbb{Z}, |x| \geq 2, P(x) = 0 \implies Q(x) = R(x) = 0. \]
Integral roots of integral polynomials

**Gap Theorem** [Cucker-Koiran-Smale’98]

Let

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

with \(\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k\). Suppose that

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

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

\[
-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)
\]

B. Grenet — Factoring bivariate lacunary polynomials without heights
Integral roots of integral polynomials

**Gap Theorem**

Let

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

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

\[-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)\]
Let
\[ P(X) = \sum_{j=1}^{\ell} a_j X^{\alpha_j} + \sum_{j=\ell+1}^{k} a_j X^{\alpha_j} \in \mathbb{Z}[X] \]
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 \( x \in \mathbb{Z}, |x| \geq 2, P(x) = 0 \implies Q(x) = R(x) = 0 \).

\[ -9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X) \]

-3 + check 0, 1 and -1
**Observation**

\[(Y - uX - v) \text{ divides } P(X, Y) \iff P(X, uX + v) \equiv 0\]
Linear factors of bivariate polynomials

**Observation**

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

**Gap Theorem**

Let

\[P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} + \sum_{j=\ell+1}^{k} a_j X^{\alpha_j} (uX + v)^{\beta_j}\]

with \(uv \neq 0\), \(\alpha_1 \leq \cdots \leq \alpha_k\). If \(\ell\) is the smallest index s.t.

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

then \(P \equiv 0\) iff both \(Q \equiv 0\) and \(R \equiv 0\).
Proof of the Gap Theorem

\( \mathbb{K} \): any field of characteristic 0
Bound on the valuation

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

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

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

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

Theorem

Let \( P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX+v)^{\beta_j} \neq 0 \), with \( uv \neq 0 \) and \( \alpha_1 \leq \cdots \leq \alpha_\ell \).

Then

\[ \text{val}(P) \leq \max_{1 \leq j \leq \ell} \left( \alpha_j + \left( \frac{\ell + 1 - j}{2} \right) \right). \]
**Definition**

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

\[ \text{val}(x^3 + 2x^5 - x^{17}) = 3 \]

**Theorem**

Let \( P = \sum_{j=1}^{\ell} a_j x^{\alpha_j} (uX + v)^{\beta_j} \neq 0 \), with \( uv \neq 0 \) and \( \alpha_1 \leq \cdots \leq \alpha_{\ell} \).

Then

\[ \text{val}(P) \leq \alpha_1 + {\ell \choose 2}. \]

\( x^{\alpha_j} (uX + v)^{\beta_j} \) linearly independent.
Bound on the valuation

**Definition**

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

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

**Theorem**

Let \( P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \neq 0 \), with \( uv \neq 0 \) and \( \alpha_1 \leq \cdots \leq \alpha_\ell \).

Then

\[ \text{val}(P) \leq \alpha_1 + \binom{\ell}{2}. \]

\[ X^{\alpha_j} (uX + v)^{\beta_j} \text{ linearly independent} \]

\[ \text{If } \alpha_1 = \cdots = \alpha_\ell, \text{ val}(P) \leq \alpha_1 + (\ell - 1) \]

[Hajós’53]
The Wronskian

**Definition**

Let \( f_1, \ldots, f_\ell \in K[X] \). Then

\[
\text{wr}(f_1, \ldots, f_\ell) = \det \begin{bmatrix}
    f_1 & f_2 & \ldots & f_\ell \\
    f'_1 & f'_2 & \ldots & f'_\ell \\
    \vdots & \vdots & \ddots & \vdots \\
    f_1^{(\ell-1)} & f_2^{(\ell-1)} & \ldots & f_\ell^{(\ell-1)}
\end{bmatrix}.
\]
The Wronskian

**Definition**

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

\[
wr(f_1,\ldots, f_\ell) = \det \begin{bmatrix}
  f_1 & f_2 & \cdots & f_\ell \\
  f'_1 & f'_2 & \cdots & f'_\ell \\
  \vdots & \vdots & \ddots & \vdots \\
  f_{(\ell-1)} & f_{(\ell-1)} & \cdots & f_{(\ell-1)}
\end{bmatrix}.
\]

**Proposition** [Bôcher, 1900]

\( wr(f_1,\ldots, f_\ell) \neq 0 \iff \) the \( f_j \)'s are linearly independent.
Wronskian & valuation

Lemma

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

Proof of the theorem.

\[ \text{wr}(P, f_2, \ldots, f_\ell) = a_1 \text{wr}(f_1, \ldots, f_\ell) \]

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

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

Lemma

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

\[ \text{val}(\text{wr}(f_1, \ldots, f_\ell)) \leq \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \text{val}(f_j). \]
Lemma

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

Lemma

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

\[
\text{val}(\text{wr}(f_1, \ldots, f_\ell)) \leq \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \text{val}(f_j).
\]

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

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

Lemma

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

\[ \text{val}(\text{wr}(f_1, \ldots, f_\ell)) \leq \sum_{j=1}^\ell \alpha_j = \sum_{j=1}^\ell \text{val}(f_j). \]

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

\[ \sum_{j=1}^\ell \alpha_j \geq \text{val}(\text{wr}(f_1, \ldots, f_\ell)) \geq \text{val}(P) + \sum_{j=2}^\ell \alpha_j - \binom{\ell}{2} \]
How far from optimality?

\[
\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \begin{cases} 
\alpha_1 + (\ell - 1) & \text{[Hajós'53] (constant } \alpha_j) \\
\alpha_1 + \left( \frac{\ell}{2} \right) & \text{[Our result]}
\end{cases}
\]
How far from optimality?

\[
\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \begin{cases} 
\alpha_1 + (\ell - 1) & \text{[Hajós'53] (constant } \alpha_j \text{)} \\
\alpha_1 + \left( \frac{\ell}{2} \right) & \text{[Our result]} 
\end{cases}
\]

▶ Lemmas: tight, but not simultaneously
How far from optimality?

\[ \text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \begin{cases} \alpha_1 + (\ell - 1) & \text{[Hajós'53] (constant } \alpha_j) \\ \alpha_1 + \left( \frac{\ell}{2} \right) & \text{[Our result]} \end{cases} \]

- Lemmas: tight, but not simultaneously
- For all \( \ell \geq 3 \), there exists \( P_\ell \) s.t. \( \text{val}(P_\ell) = \alpha_1 + (2\ell - 3) \)
How far from optimality?

\[
\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \left\{ \begin{array}{l}
\alpha_1 + (\ell - 1) \\
\alpha_1 + \left( \frac{\ell}{2} \right)
\end{array} \right. 
\]

[Hajós’53] (constant \( \alpha_j \))

[Our result]

▶ Lemmas: tight, but not simultaneously

▶ For all \( \ell \geq 3 \), there exists \( P_\ell \) s.t. \( \text{val}(P_\ell) = \alpha_1 + (2\ell - 3) \)

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

\[
= X^{2\ell-3}
\]
Gap Theorem

**Theorem**

Let

\[
P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX + v)^{\beta_j} + \sum_{j=\ell+1}^{k} a_j X^{\alpha_j}(uX + v)^{\beta_j}
\]

with \(uv \neq 0\), \(\alpha_1 \leq \cdots \leq \alpha_k\). If \(\ell\) is the smallest index s.t.

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

then \(P \equiv 0\) iff both \(Q \equiv 0\) and \(R \equiv 0\).
Gap Theorem

Theorem

Let

\[ P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} + \sum_{j=\ell+1}^{k} a_j X^{\alpha_j} (uX + v)^{\beta_j} \]

with \( uv \neq 0 \), \( \alpha_1 \leq \cdots \leq \alpha_k \). If \( \ell \) is the smallest index s.t.

\[ \alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2} \geq \text{val}(Q), \]

then \( P \equiv 0 \) iff both \( Q \equiv 0 \) and \( R \equiv 0 \).

\[ P = \left( c_{\text{val}(Q)} X^{\text{val}(Q)} + \cdots \right) + X^{\alpha_{\ell+1}} \left( a_{\ell+1} (uX + v)^{\beta_{\ell+1}} + \cdots \right) \]
Algorithms

$K = \mathbb{Q}(\alpha)$: algebraic number field
Finding linear factors

Observation + Gap Theorem (recursively)

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

\(\iff P(X, uX + v) \equiv 0\)
Finding linear factors

Observation + Gap Theorem (recursively)

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

\[\text{Independent from } u \text{ and } v\]
\[X \text{ does not play a special role}\]
Observation + Gap Theorem (recursively)

\[(Y - uX - v) \text{ divides } P(X, Y)\]
\[\iff P(X, uX + v) \equiv 0\]
\[\iff P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0\]
\[\iff (Y - uX - v) \text{ divides each } P_t(X, Y)\]
Finding linear factors

**Observation + Gap Theorem (recursively)**

\[(Y - uX - v) \text{ divides } P(X, Y)\]

\[\iff \quad P(X, uX + v) \equiv 0\]

\[\iff \quad P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0\]

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

\[P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j} \quad \text{with } \alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leq \binom{\ell_t}{2}\]

B. Grenet — Factoring bivariate lacunary polynomials without heights
Finding linear factors

**Observation + Gap Theorem (recursively)**

\[(Y - uX - v) \text{ divides } P(X, Y)\]

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

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

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

\[
P_t = \sum_{j=j_t}^{j_t + \ell_t - 1} a_j X^{\alpha_j} Y^{\beta_j} \text{ with } \alpha_{j_t + \ell_t - 1} - \alpha_{j_t} \leq \binom{\ell_t}{2}\]

▷ Independent from \(u\) and \(v\)
Finding linear factors

**Observation + Gap Theorem (recursively)**

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

\[P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j} \text{ with } \alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leq \binom{\ell_t}{2}\]

- Independent from \(u\) and \(v\)
- \(X\) does not play a special role
Example

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

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

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

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

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

\[ P = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \]

\[ - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \]

\[ + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \]

\[ P_1 = X^3Y^6(-X^2 + Y^2 - 2Y + 1) \]
Example

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

\[ P_1 = X^3Y^6(X - Y + 1)(1 - X - Y) \]
Example

\[ P = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \]

\[ - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \]

\[ + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \]

\[ P_1 = X^3Y^6(X - Y + 1)(1 - X - Y) \]

\[ P_2 = X^9Y^2(X - Y + 1) \]

\[ P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1) \]

\[ P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1) \]
Example

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

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

\[ \implies \text{linear factors of } P: (X - Y + 1, 1) \]
Example

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

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

\[ \implies \text{linear factors of } P: (X - Y + 1, 1), (X, 3), (Y, 2) \]
Complete algorithm

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

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

monomials

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

- **Monomials**
  - \((X, \min_j \alpha_j)\)
  - \((Y, \min_j \beta_j)\)

- **Binomials**
  - \((X - a)\)
  - \((Y - uX)\)

Factors of \( \sum_j a_j X^{\alpha_j} \)

Roots of \( u \mapsto \sum_j a_j u^{\beta_j} \)

**Univariate lacunary factorization**

[H. Lenstra’99]
Complete algorithm

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

- monomials
- binomials
- trinomials

\( (X, \min_j \alpha_j) \)
\( (Y, \min_j \beta_j) \)

\( (X - a) \)
Factors of \( \sum_j a_j X^{\alpha_j} \)

\( (Y - uX) \)
Roots of \( u \mapsto \sum_j a_j u^{\beta_j} \)

Univariate lacunary factorization
[H. Lenstra’99]

Common factors of \( j_t + \ell_t - 1 \)
\( P_t = \sum_{j=j_t}^{j_t + \ell_t - 1} a_j X^{\alpha_j} Y^{\beta_j} \)
\((\deg(P_t) \leq \Theta(\ell_t^2))\)

Low-degree factorization
[Kaltofen’82, ..., Lecerf’07]

B. Grenet — Factoring bivariate lacunary polynomials without heights
Complete algorithm

Let \( P = \sum_{j=1}^{k} a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{Q}(\alpha)[X, Y] \) be given in lacunary representation. There exists a **deterministic polynomial-time** algorithm to compute its linear factors, with multiplicities.

**Monomials**
- \((X, \min_j \alpha_j)\)
- \((Y, \min_j \beta_j)\)

**Binomials**
- \((X - \alpha)\)
- \((Y - uX)\)

**Trinomials**
- Common factors of \( j_{t+\ell_t-1} \)
  \[ P_t = \sum_{j=j_t}^{j_{t+\ell_t-1}} a_j X^{\alpha_j} Y^{\beta_j} \]
  \((\deg(P_t) \leq \mathcal{O}(\ell_t^2))\)

**Univariate lacunary factorization**
- [H. Lenstra’99]

**Low-degree factorization**
- [Kaltofen’82, …, Lecerf’07]
Bottleneck: Factorization of low-degree polynomials
Bottleneck: Factorization of low-degree polynomials

Complexity measure: $\text{gap}(P)$
Bottleneck: Factorization of low-degree polynomials

\[ \text{Complexity measure: } \text{gap}(P) \]

\[
\text{gap}(P) = \begin{cases} 
O(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\
O(k^2) & \text{[This work]} 
\end{cases}
\]

\[ h_P = \max_j |a_j| \text{ if } P \in \mathbb{Z}[X,Y] \]
Bottleneck: Factorization of low-degree polynomials

- Complexity measure: $\text{gap}(P)$

- $\text{gap}(P) = \begin{cases} O(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\ O(k^2) & \text{[This work]} \end{cases}$

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

- Algebraic number field only: based on [H. Lenstra'99]
Bottleneck: Factorization of low-degree polynomials

Complexity measure: \( \text{gap}(P) \)

- \( \text{gap}(P) = \begin{cases} 
\Theta(\log k + \log h_P) & \text{[Kaltofen-Koiran'05]} \\
\Theta(k^2) & \text{[This work]} 
\end{cases} \)

\[ h_P = \max_j |a_j| \text{ if } P \in \mathbb{Z}[X,Y] \]

- Algebraic number field only: based on \[H. Lenstra'99\]

- Generalization to multilinear factors
Bottleneck: Factorization of low-degree polynomials

Complexity measure: \( \text{gap}(P) \)

\[
\text{gap}(P) = \begin{cases} 
\mathcal{O}(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\
\mathcal{O}(k^2) & \text{[This work]}
\end{cases}
\]

\[ h_P = \max_j |a_j| \text{ if } P \in \mathbb{Z}[X,Y] \]

- Algebraic number field only: based on [H. Lenstra'99]
- Generalization to multilinear factors
- PIT algorithm for \( \sum_j a_j X^{\alpha_j} (uX + v)^{\beta_j} \)
Positive characteristic

\[ K = \mathbb{F}_{p^s} : \text{field with } p^s \text{ elements} \]
Valuation & PIT

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

**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 \( \text{val}(P) \leq \max_j (\alpha_j + (\ell + 1 - j)) \), provided \( P \neq 0 \).
\[(1 + X)^{2^n} + (1 + X)^{2^{n+1}} = X^{2^n}(X + 1) \text{ mod } 2\]

**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 \( \text{val}(P) \leq \max_j (\alpha_j + (\ell + \frac{1}{2} - j)), \) provided \( P \neq 0. \)

**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.
Valuation & PIT

\[(1 + X)^{2^n} + (1 + X)^{2^{n+1}} = X^{2^n}(X + 1) \pmod{2}\]

**Theorem**

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

Then \( \text{val}(P) \leq \max_j (\alpha_j + (\ell + 1 - j)/2) \), provided \( P \neq 0 \).

**Theorem**

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

**Proof.**

- If \( uv \neq 0 \): as in characteristic 0, using a Gap Theorem.
\[(1 + X)^{2^n} + (1 + X)^{2^{n+1}} = X^{2^n} (X + 1) \mod 2\]

**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 \( \text{val}(P) \leq \max_j (\alpha_j + (\ell + 1 - j)/2) \), provided \( P \not\equiv 0 \).

**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*. 

B. Grenet — Factoring bivariate lacunary polynomials without heights
\[(1 + X)^{2^n} + (1 + X)^{2^{n+1}} \equiv X^{2^n}(X + 1) \pmod{2}\]

**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 \( \text{val}(P) \leq \max_j \left( \alpha_j + \left( \frac{\ell + 1 - j}{2} \right) \right), \) provided \( P \neq 0. \)

**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.
Factorization algorithm

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

where \( a_j \in \mathbb{F}_p^s \) and \( p > \deg(P) \)
Factorization algorithm

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

where \( a_j \in \mathbb{F}_p \) and \( p > \text{deg}(P) \)

monomials

\((X, \min_j \alpha_j)\)

\((Y, \min_j \beta_j)\)

trinomials

Common factors of

\[ P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j} \]

\( (\text{deg}(P_t) \leq O(\ell_t^2)) \)

Low-degree factorization

\([Gao'03, Lecerf'10]\)
Factorization algorithm

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

where \( a_j \in \mathbb{F}_{p^s} \) and \( p > \deg(P) \)

- monomials
  - \((X, \min_j \alpha_j)\)
  - \((Y, \min_j \beta_j)\)
- binomials
  - \((X - a)\)
    - Factors of \( \sum_j a_j X^{\alpha_j} \)
  - \((Y - uX)\)
    - Roots of \( u \mapsto \sum_j a_j u^{\beta_j} \)
- trinomials
  - Common factors of \( P_t = \sum_{j=t}^{j+t-1} a_j X^{\alpha_j} Y^{\beta_j} \)
    - \( (\deg(P_t) \leq O(\ell_t^2)) \)

Low-degree factorization

- \([\text{Gao'03, Lecerf'10}]\)
Factorization algorithm

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

where \( a_j \in \mathbb{F}_p \) and \( p > \deg(P) \)

monomials  binomials  trinomials

\((X, \min_j \alpha_j)\)
\((Y, \min_j \beta_j)\)

Factors of \( \sum_j a_j X^{\alpha_j}(Y-uX)^{\beta_j} \)

Common factors of \( P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j} \)

\( (\deg(P_t) \leq O(\ell_t^3)) \)

Low-degree factorization

[Kipnis-Shamir’99, Bi-Cheng-Rojas’13]
Talk at 2:25pm

[NP-complete under BPP reductions]

B. Grenet — Factoring bivariate lacunary polynomials without heights
Conclusion
Conclusion

- Computing linear factors of lacunary bivariate polynomials
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  
  - NEW! Multivariate polynomials
  
  - New Gap Theorem (independent of the height)

  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)

  - Two Gap Theorems: mix both!

- Extensions:
  - Low-degree factors
  - Lacunary factors
  - Smaller characteristics

- Correct bound for the valuation?

Thank you!

B. Grenet — Factoring bivariate lacunary polynomials without heights
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  - **Multilinear** factors

- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

- Extensions:
  - Low-degree factors
  - Lacunary factors
  - Smaller characteristics

Thank you!
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials \low-degree bivariate polynomials \}
  - Multilinear factors
  - Multivariate polynomials

NEW!

Thank you!
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \( \{ \) univariate lacunary polynomials, low-degree bivariate polynomials \( \} \)
  - Multilinear factors
  - Multivariate polynomials

- New Gap Theorem (independent of the height)
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  - \textbf{Multilinear} factors
  - \textbf{Multivariate} polynomials

- \textbf{New Gap Theorem} (independent of the height)
  - Easy to implement
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials \\
  \quad \text{low-degree bivariate polynomials } \}
  - **Multilinear** factors
  - **Multivariate** polynomials

- **New Gap Theorem** (independent of the height)
  - Easy to implement
  - Large coefficients
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  - Multilinear factors
  - Multivariate polynomials

- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)

Thank you!
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  - Multilinear factors
  - Multivariate polynomials

- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{cases}$
  - **Multilinear** factors
  - **Multivariate** polynomials

- **New Gap Theorem** (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

- Extensions:
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  - **Multilinear** factors
  - **Multivariate** polynomials

- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

- Extensions:
  - **Low-degree** factors
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \(\{\text{univariate lacunary polynomials}, \text{low-degree bivariate polynomials}\}\)
  - **Multilinear** factors
  - **Multivariate** polynomials
- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!
- Extensions:
  - **Low-degree** factors
  - **Lacunary** factors
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \( \{ \) univariate lacunary polynomials, low-degree bivariate polynomials \( \} \)
  - Multilinear factors
  - Multivariate polynomials

- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

- Extensions:
  - Low-degree factors
  - Lacunary factors
  - Smaller characteristics

B. Grenet — Factoring bivariate lacunary polynomials without heights
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  - **Multilinear** factors
  - **Multivariate** polynomials

- **New Gap Theorem** (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

- **Extensions:**
  - **Low-degree** factors
  - **Lacunary** factors
  - **Smaller characteristics**

- Correct bound for the valuation?

B. Grenet — Factoring bivariate lacunary polynomials without heights
Conclusion

- Computing linear factors of lacunary bivariate polynomials
  - Reduction to \{ univariate lacunary polynomials, low-degree bivariate polynomials \}
  - Multilinear factors
  - Multivariate polynomials

- New Gap Theorem (independent of the height)
  - Easy to implement
  - Large coefficients
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

- Extensions:
  - Low-degree factors
  - Lacunary factors
  - Smaller characteristics

- Correct bound for the valuation?

Thank you!