Bounded-degree factorization of lacunary polynomials

Bonus: PIT algorithms

Bruno Grenet

LIRMM — Université de Montpellier

WACT — Tel Aviv — February 11., 2016

Factorization of a polynomial f

Find $f_1, \ldots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

Factorization of a polynomial f

Find $f_1, \ldots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\ldots$;
  - in $1, 2, \ldots, n$ variables.
- Complexity: **polynomial in $\deg(f)$**

Factorization of a polynomial f

Find $f_1, \ldots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\ldots$;
  - in $1, 2, \ldots, n$ variables.
- Complexity: **polynomial in $\deg(f)$**

$$X^{568742}Y^{568741} + X^{568741}Y^{568742} - X^{568741}Y^{568741} - X - Y + 1$$
$$= (X + Y - 1) \times (X^{568741}Y^{568741} - 1)$$

Factorization of a polynomial f

Find $f_1, \ldots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, $\ldots$;
  - in $1, 2, \ldots, n$ variables.
- Complexity: **polynomial in $\deg(f)$**

$$\begin{aligned} &X^{568742}Y^{568741} + X^{568741}Y^{568742} - X^{568741}Y^{568741} - X - Y + 1 \\ &\quad = (X + Y - 1) \times (X^{568741}Y^{568741} - 1) \\ &\quad = (X + Y - 1) \times (XY - 1) \times (1 + XY + \cdots + X^{568740}Y^{568740}) \end{aligned}$$

Definition

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

- $\text{size}(f) \simeq k\left(\max_j(\text{size}(c_j)) + n\underline{\log(\deg f)}\right)$

Definition

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

- $\text{size}(f) \simeq k\left(\max_j(\text{size}(c_j)) + n\underline{\log(\deg f)}\right)$

Theorems

There exist deterministic polynomial-time algorithms computing

- **integer roots** of $f \in \mathbb{Z}[X]$; [Cucker-Koiran-Smale'98]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X]$; [Lenstra'99]
- **low-degree** factors of $f \in \mathbb{Q}(\alpha)[X_1, \ldots, X_n]$. [Kaltofen-Koiran'06]

It is NP-**hard** (under BPP reductions) to compute **roots of** $f \in \mathbb{F}_p[X]$. [Bi-Cheng-Rojas'13]

Integer roots of integral polynomials

Theorem [Cucker-Koiran-Smale'98]

There exists a deterministic **polynomial-time** algorithm to compute the integer roots of a **lacunary polynomial** $f \in \mathbb{Z}[X]$.

Integer roots of integral polynomials

Theorem [Cucker-Koiran-Smale'98]

There exists a deterministic **polynomial-time** algorithm to compute the integer roots of a **lacunary polynomial** $f \in \mathbb{Z}[X]$.

Gap Theorem [Cucker-Koiran-Smale'98]

Let $f = f_1 + f_2 \in \mathbb{Z}[X]$, with coefficients of absolute value $\leqslant 2^s$, s.t. $\mathrm{val}(f_2) - \deg(f_1) > 1 + s$. Then for $|x| \geqslant 2$,
$f(x) = 0 \implies f_1(x) = f_2(x) = 0$.

Theorem [Cucker-Koiran-Smale'98]

There exists a deterministic **polynomial-time** algorithm to compute the integer roots of a **lacunary polynomial** $f \in \mathbb{Z}[X]$.

Gap Theorem [Cucker-Koiran-Smale'98]

Let $f = f_1 + f_2 \in \mathbb{Z}[X]$, with coefficients of absolute value $\leqslant 2^s$, s.t. $\mathrm{val}(f_2) - \deg(f_1) > 1 + s$. Then for $|x| \geqslant 2$, $f(x) = 0 \implies f_1(x) = f_2(x) = 0$.

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

Our settings

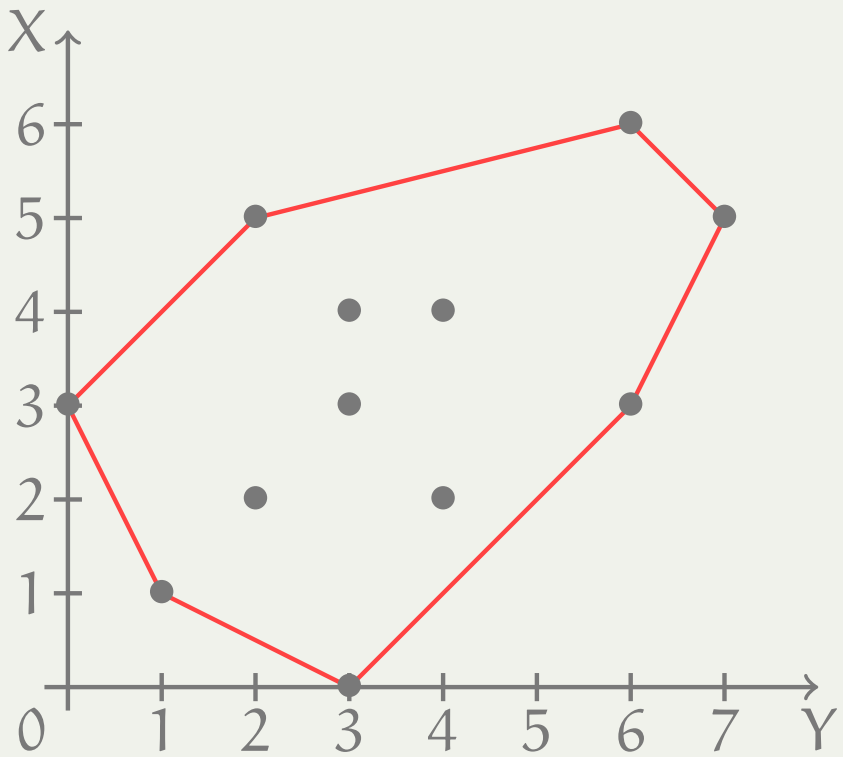
- Generalization to other fields?
- Simpler, more combinatorial proofs?

- Generalization to other fields?
- Simpler, more combinatorial proofs?

Main (informal) result

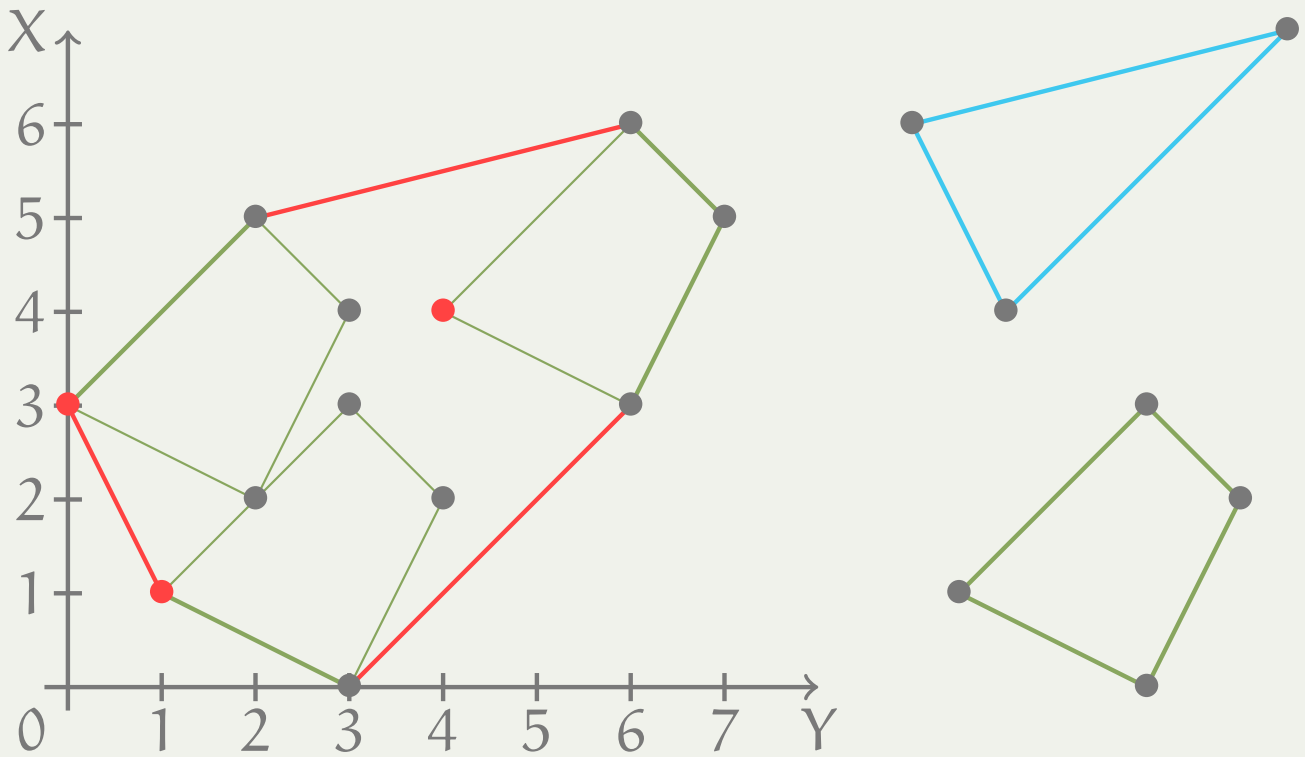
Inputs:	$f \in \mathbb{K}[X_1, \ldots, X_n]$; bound d
Assumption:	$\mathbb{K}$ of characteristic 0 or $> \deg(f)$
Output:	Degree-d factors of f
Algorithms:	"Combinatorial" reductions to
	▶ the univariate case
	▶ low-degree multivariate factorization
Complexity:	Deterministic $\mathrm{poly}(\mathrm{size}(f), d)$

Newton polygon/tope



$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

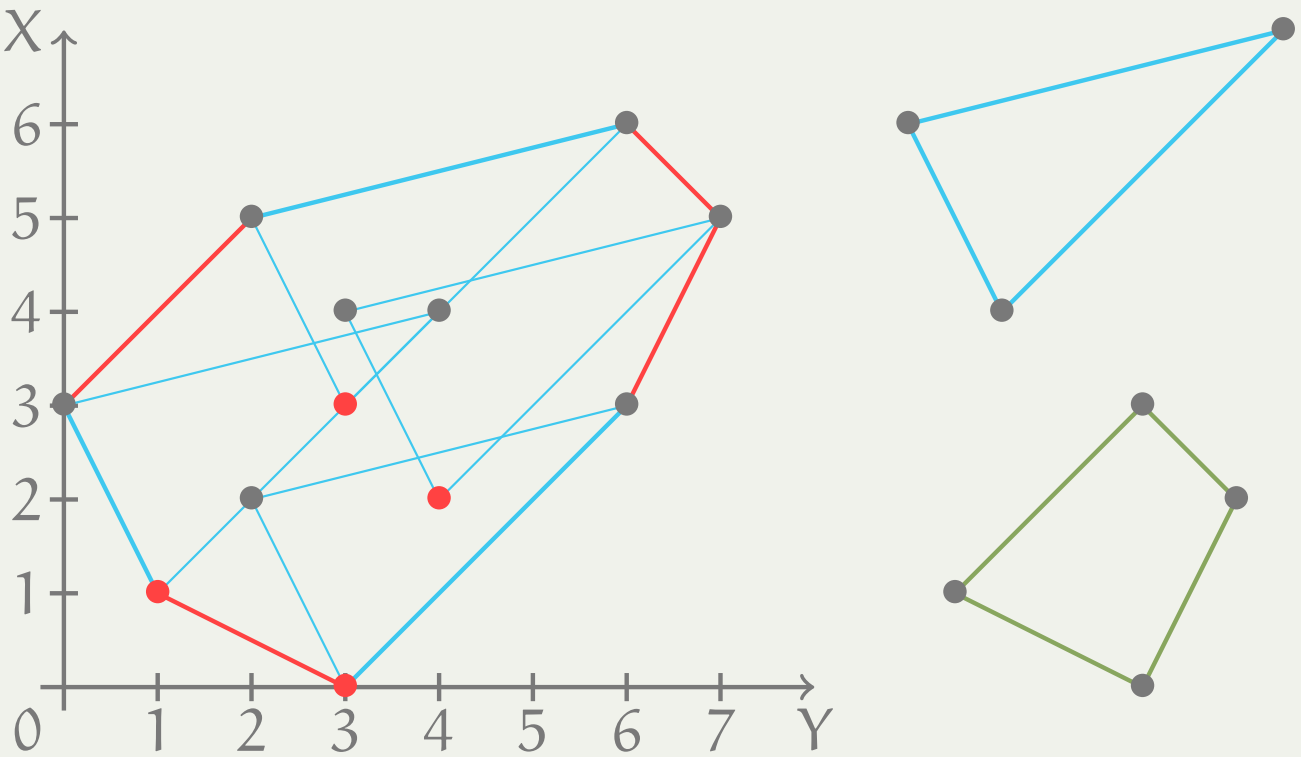
Newton polygon/tope



$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

$$= (Y - 2X^2 + X^3Y^4)(Y^2 + 2X - X^2Y^3 + X^3Y^2)$$

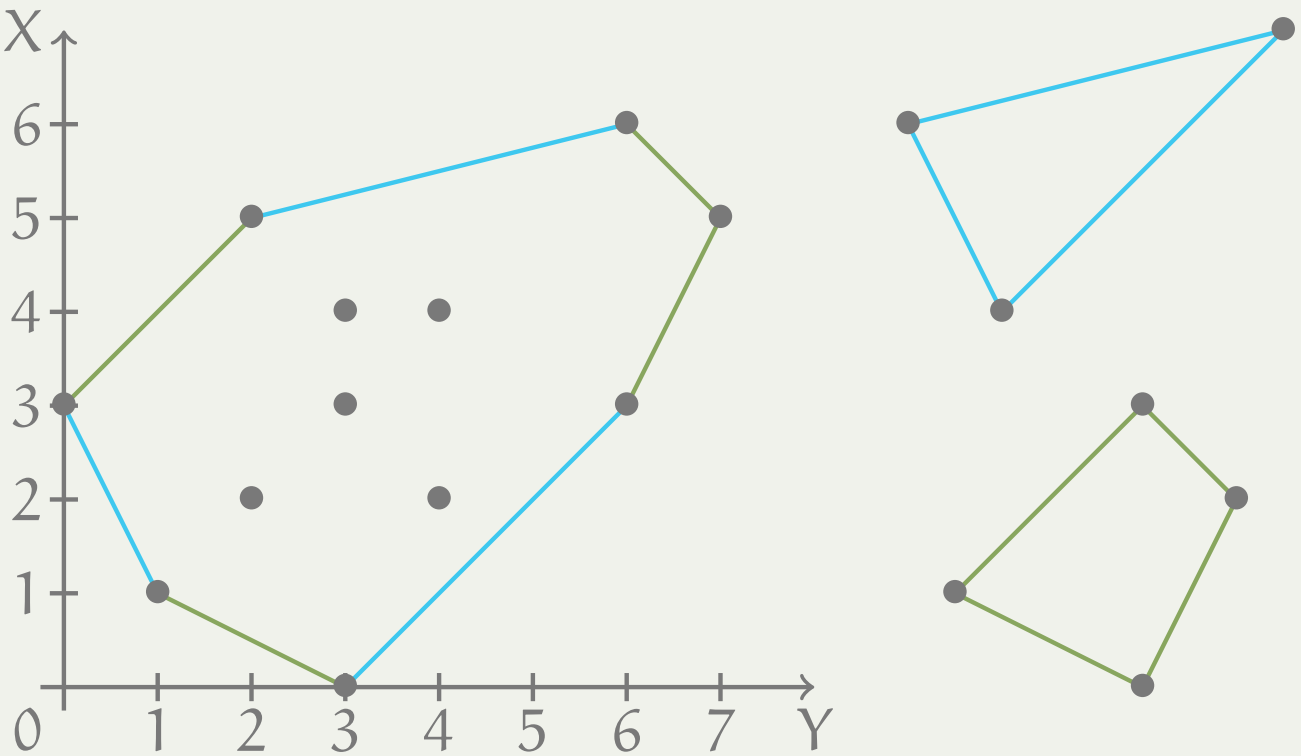
Newton polygon/tope



$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

$$= (Y - 2X^2 + X^3Y^4)(Y^2 + 2X - X^2Y^3 + X^3Y^2)$$

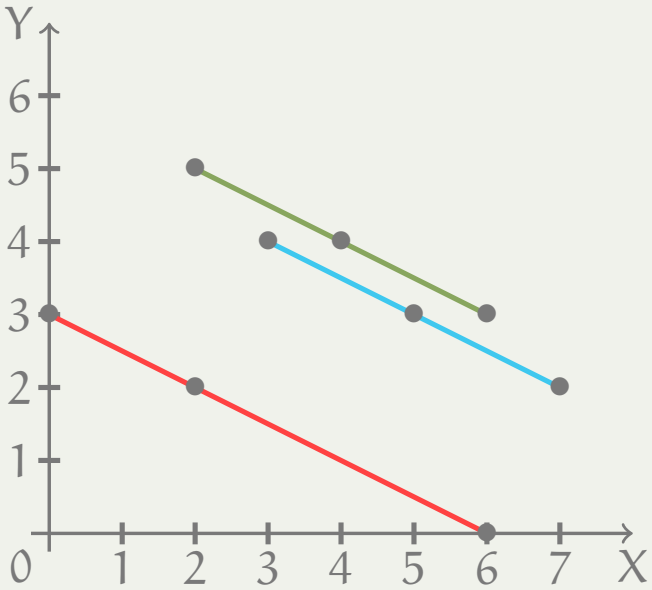
Newton polygon/tope



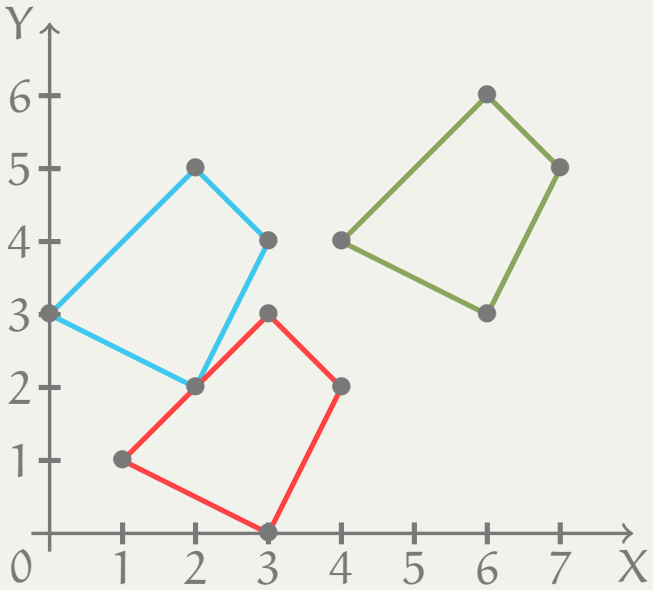
$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

$$= (Y - 2X^2 + X^3Y^4)(Y^2 + 2X - X^2Y^3 + X^3Y^2)$$

Two kinds of factors

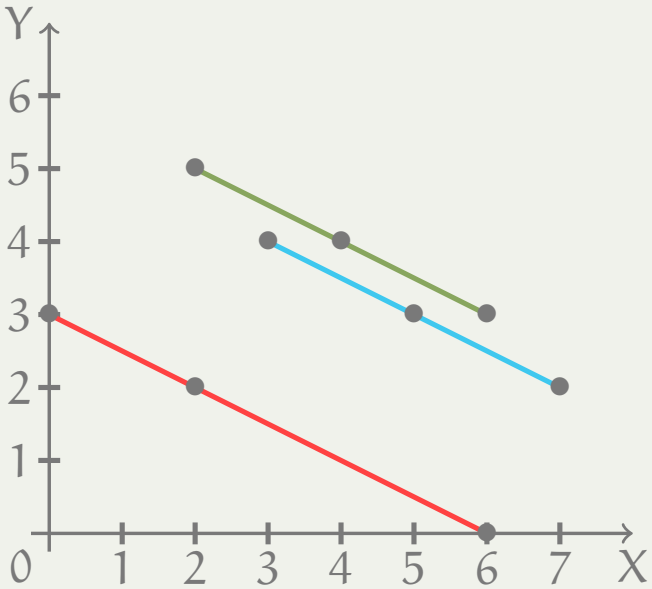


Unidimensional factors



Multidimensional factors

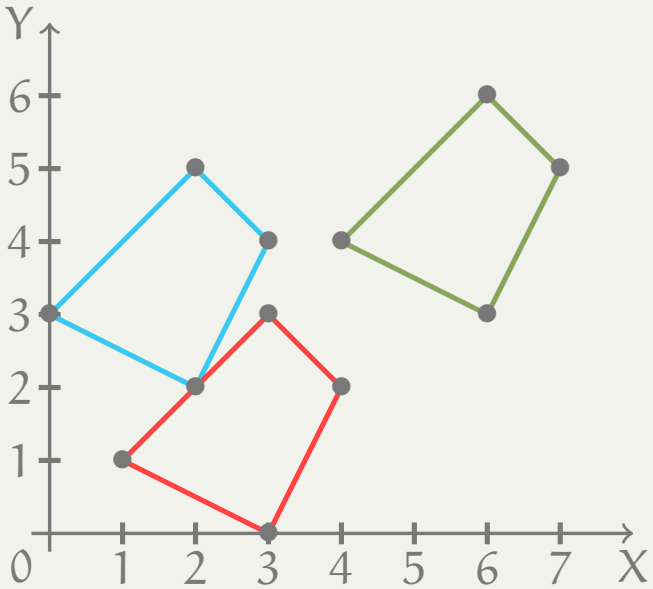
Two kinds of factors



Unidimensional factors

⇓

Univariate lacunary factorization

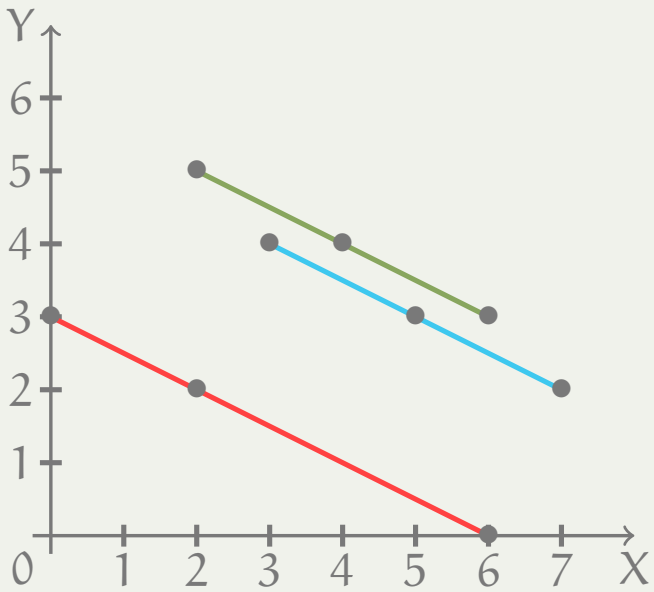


Multidimensional factors

⇓

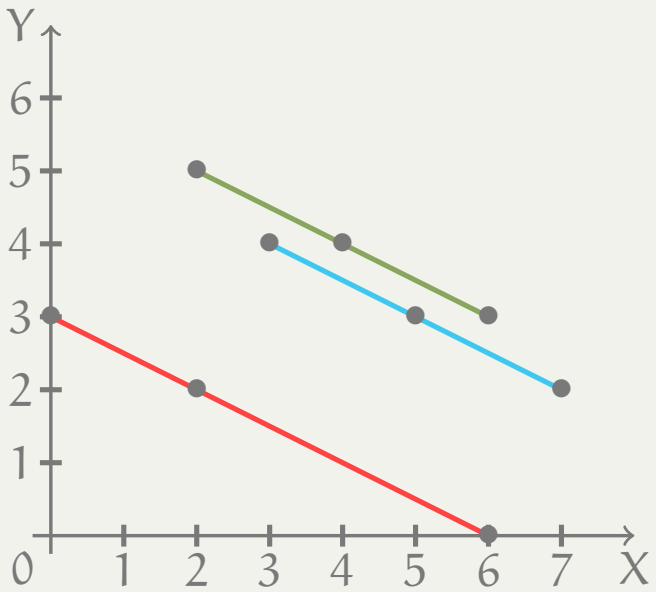
Multivariate low-degree factorization

Unidimensional factors



- Unidimensional: $X^\gamma f(X^\delta)$ for some univariate $f \in \mathbb{K}[Z]$
- Directions given by the support
- Each direction δ independently

Unidimensional factors



- Unidimensional: $X^{\gamma} f(X^{\delta})$ for some univariate $f \in \mathbb{K}[Z]$
- Directions given by the support
- Each direction δ independently

1. Write f as a sum of **δ-components**
2. **Project** each component to a univariate lacunary polynomial
3. Compute the common **bounded-degree factors** of the projections
   Available for number field only. NP-hard in positive characteristic.
4. **Lift** the univariate factors to unidimensional factors

Linear factors of bivariate polynomials

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Observation

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

Linear factors of bivariate polynomials

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Observation

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

Theorem

$$\mathrm{val}\left(\sum_{j=1}^{\ell} c_j X^{\alpha_j} (uX + v)^{\beta_j}\right) \leqslant \alpha_1 + \binom{\ell}{2} \text{ if nonzero and } uv \neq 0.$$

Linear factors of bivariate polynomials

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Observation

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

Theorem

$$\mathrm{val}\left(\sum_{j=1}^{\ell} c_j X^{\alpha_j} (uX + v)^{\beta_j}\right) \leqslant \alpha_1 + \binom{\ell}{2} \text{ if nonzero and } uv \neq 0.$$

Gap Theorem

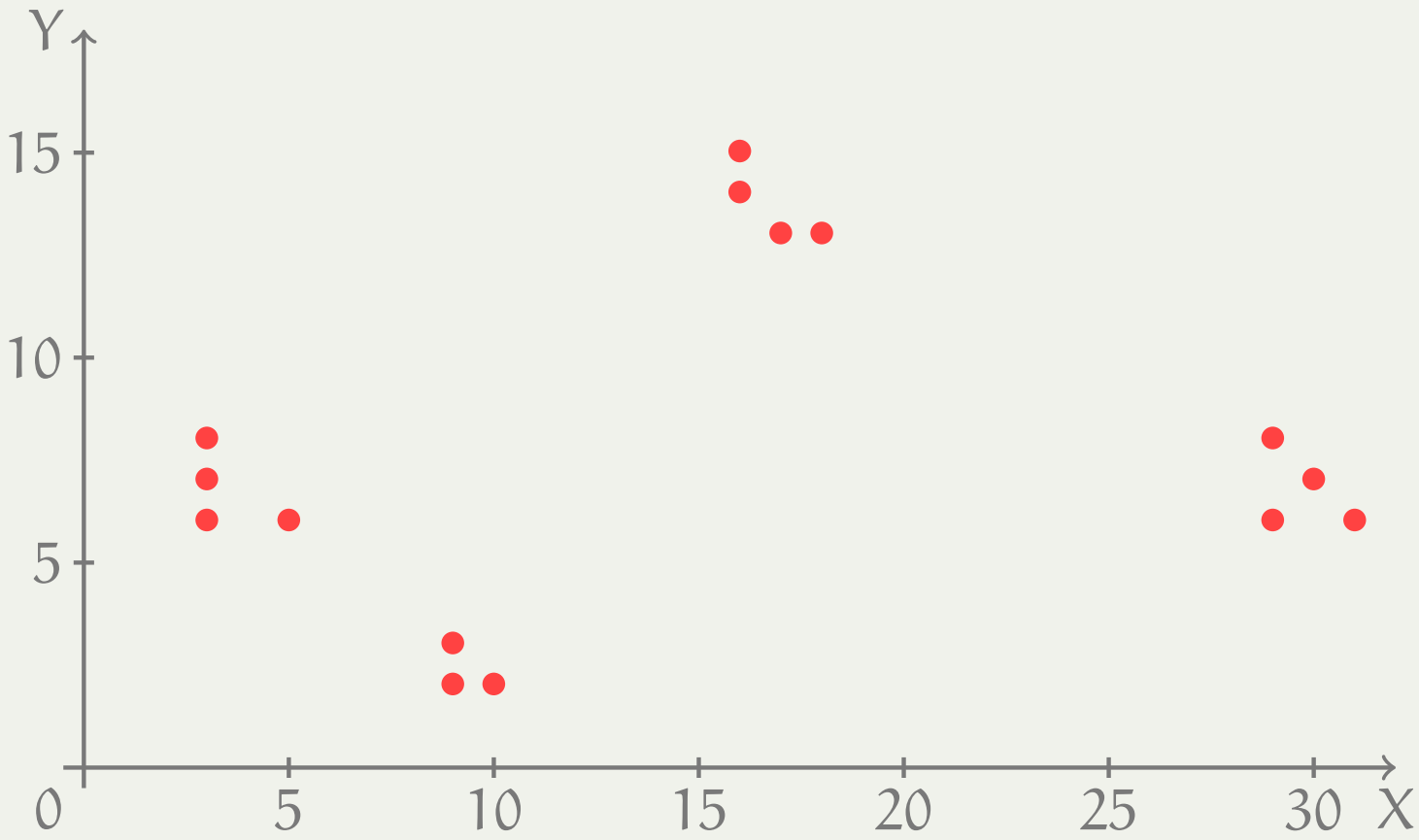
Suppose that $f = f_1 + f_2$ with $\mathrm{val}_X(f_2) - \mathrm{val}_X(f_1) > \binom{s(f_1)}{2}$. Then for all $uv \neq 0$, $(Y - uX - v)$ divides f iff it divides both f_1 and f_2.

An example

$$\begin{aligned} f = {} & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

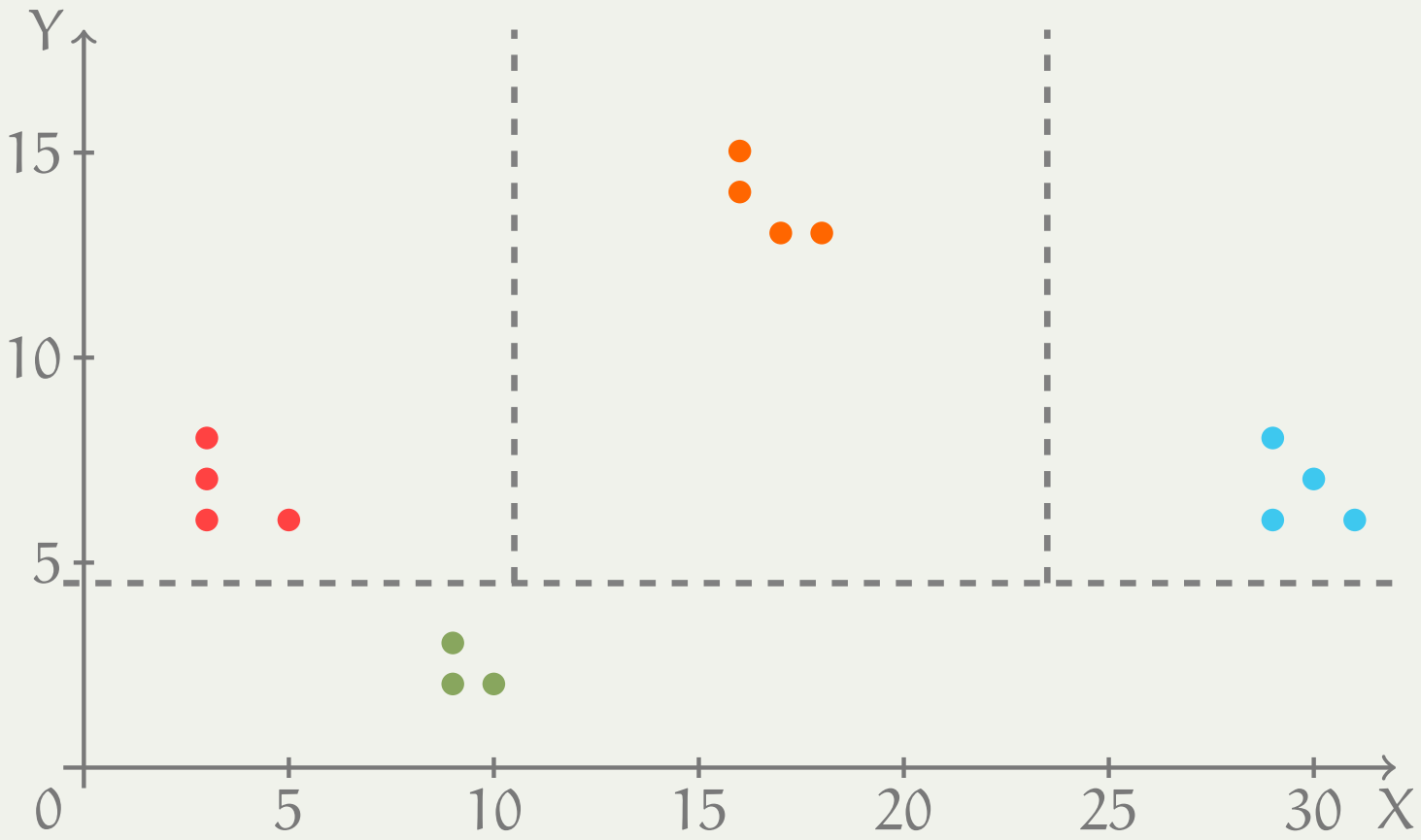
An example

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



An example

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



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

$$f_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$
$$f_2 = X^9Y^2(X - Y + 1)$$
$$f_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$
$$f_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

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

$$f_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$
$$f_2 = X^9Y^2(X - Y + 1)$$
$$f_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$
$$f_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

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

Observation for low-degree factors

$g(X, Y)$ divides $f(X, Y) \iff f(X, \phi(X)) \equiv 0$

Observation for low-degree factors

$g(X,Y)$ divides $f(X,Y) \iff f(X,\phi(X)) \equiv 0$

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X)) \in \overline{\mathbb{K}(X)}[Y]$$

Observation for low-degree factors

$g(X,Y)$ divides $f(X,Y) \iff f(X,\phi(X)) \equiv 0$

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X)) \in \overline{\mathbb{K}(X)}[Y]$$

- $g_0 \in \mathbb{K}[X]$
- $\phi_1, \ldots, \phi_d \in \overline{\mathbb{K}(X)} \subset \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ are **Puiseux series**:

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n} \text{ with } a_t \in \overline{\mathbb{K}},\ a_{t_0} \neq 0. \qquad (\mathrm{val}(\phi) = t_0/n)$$

Observation for low-degree factors

$g(X,Y)$ divides $f(X,Y) \iff f(X,\phi(X)) \equiv 0$

$$g(X,Y) = g_0(X) \prod_{i=1}^{\deg_Y(g)} (Y - \phi_i(X)) \in \overline{\mathbb{K}(X)}[Y]$$

- $g_0 \in \mathbb{K}[X]$
- $\phi_1, \ldots, \phi_d \in \overline{\mathbb{K}(X)} \subset \overline{\mathbb{K}}\langle\langle X \rangle\rangle$ are **Puiseux series**:

$$\phi(X) = \sum_{t \geqslant t_0} a_t X^{t/n} \text{ with } a_t \in \overline{\mathbb{K}},\ a_{t_0} \neq 0. \qquad (\mathrm{val}(\phi) = t_0/n)$$

- If g is irreducible,
  g divides $f \iff \exists i,\ f(X,\phi_i) = 0 \iff \forall i,\ f(X,\phi_i) = 0$

Theorem

$$\operatorname{val}\left(\sum_{j=1}^{\ell} c_j X^{\alpha_j} \phi(X)^{\beta_j}\right) \leqslant \min_j(\alpha_j + \nu\beta_j) + (8d^2 - \nu)\binom{\ell}{2},$$

where

- $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν and degree-d minimal polynomial,
- the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent.

Theorem

$$\mathrm{val}\left(\sum_{j=1}^{\ell} c_j X^{\alpha_j}\phi(X)^{\beta_j}\right) \leqslant \min_j(\alpha_j + \nu\beta_j) + (8d^2 - \nu)\binom{\ell}{2},$$

where

- $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν and degree-d minimal polynomial,
- the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent.

- Proof based on the *Wronskian* of the family $(X^{\alpha_j}\phi^{\beta_j})_j$.
- Optimality?
- Gap Theorem:
  "If $f = f_1 + f_2$ with a gap, g divides f iff it divides f_1 and f_2"

Theorem

$$\operatorname{val}\left(\sum_{j=1}^{\ell} c_j X^{\alpha_j} \phi(X)^{\beta_j}\right) \leqslant \min_j(\alpha_j + \nu\beta_j) + (8d^2 - \nu)\binom{\ell}{2},$$

where

- $\phi \in \overline{\mathbb{K}}\langle\langle X\rangle\rangle$ of valuation ν and degree-d minimal polynomial,
- the family $(X^{\alpha_j}\phi^{\beta_j})_j$ is linearly independent.

- Proof based on the *Wronskian* of the family $(X^{\alpha_j}\phi^{\beta_j})_j$.
- Optimality?
- Gap Theorem:
  "If $f = f_1 + f_2$ with a gap, g divides f iff it divides f_1 and f_2"
- Bounds $\alpha_j + \nu\beta_j$, not the degree $\rightsquigarrow$ use two different ν's

Corollary

Inputs: $f \in \mathbb{K}[X_1, \ldots, X_n]$ in lacunary representation bound d

Output: Degree-$O(d^4 s(f)^2)$ polynomial f_{ld} s.t for all multidimensional degree-d polynomial g, $\mathrm{mult}_g(f) = \mathrm{mult}_g(f_{ld})$

Complexity: Deterministic polynomial time

Corollary

Inputs: $f \in \mathbb{K}[X_1, \ldots, X_n]$ in lacunary representation
bound d

Output: Degree-$O(d^4 s(f)^2)$ polynomial f_{ld} s.t for all multidimensional degree-d polynomial g, $\mathrm{mult}_g(f) = \mathrm{mult}_g(f_{ld})$

Complexity: Deterministic polynomial time

1. Write $f = f_1 + \cdots + f_s$ where $\deg_{X_i}(f_t) - \mathrm{val}_{X_i}(f_t) \leqslant (4d^4 - 2d^2)\binom{s(f_t)}{2}$ for all i;
2. Return $\gcd(f_1, \ldots, f_s)$.
3. (Factor the gcd using a low-degree factorization algorithm.)

Complete algorithm

Find degree-d factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j}$

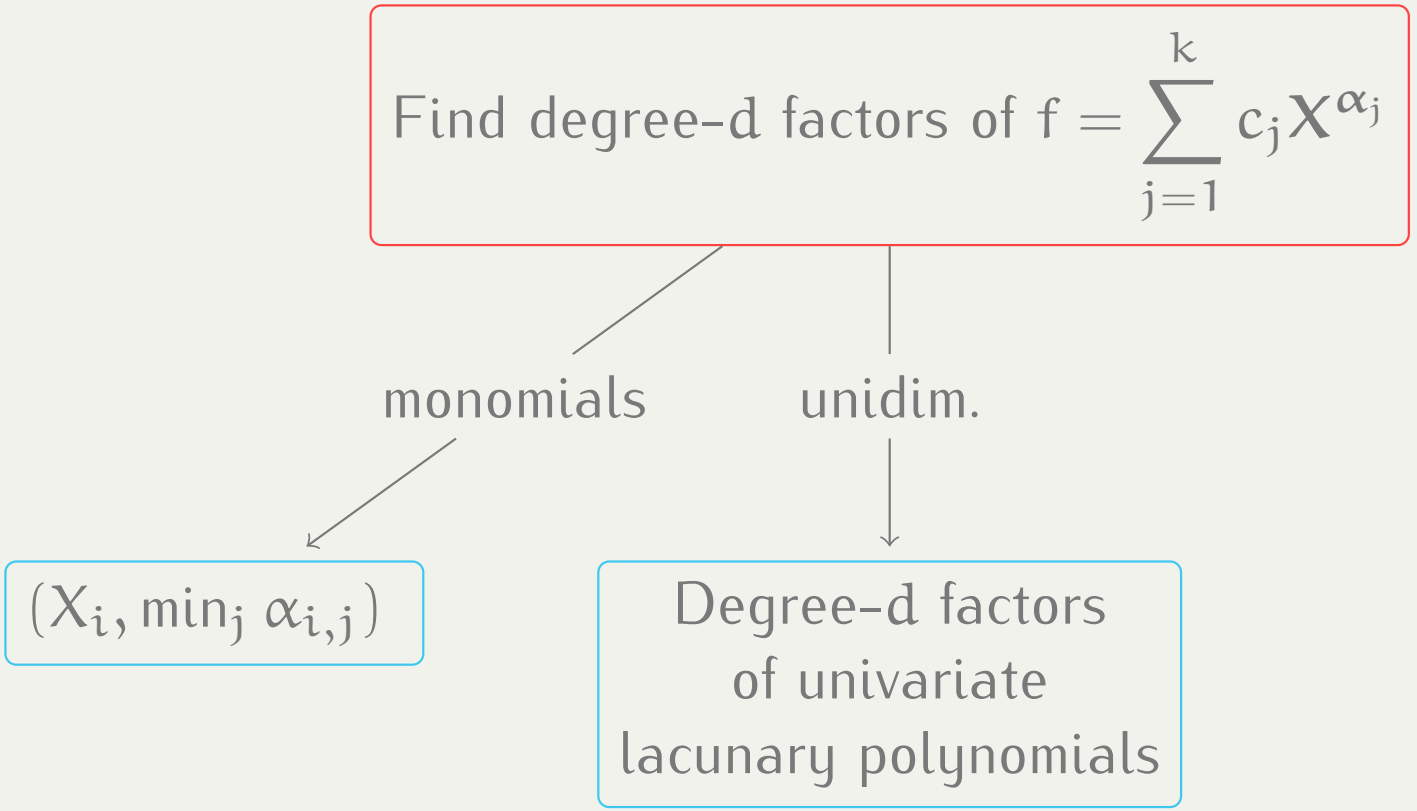
Complete algorithm

Find degree-d factors of $f = \sum_{j=1}^{k} c_j X^{\alpha_j}$

monomials

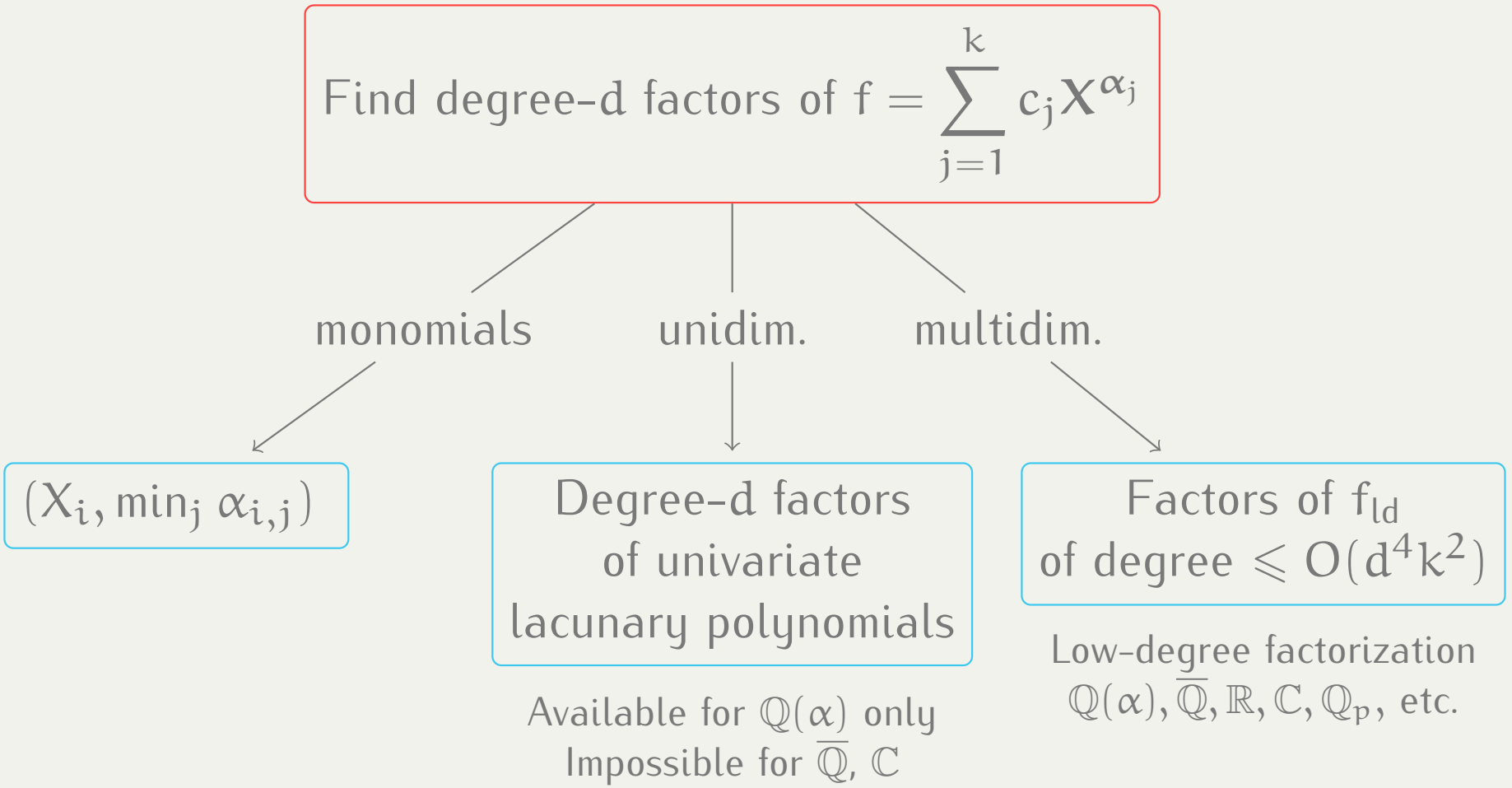
$(X_i, \min_j \alpha_{i,j})$

Complete algorithm



Available for $\mathbb{Q}(\alpha)$ only
Impossible for $\overline{\mathbb{Q}}$, $\mathbb{C}$

Complete algorithm



- $\sum_{j=1}^{k} a_j X^{\alpha_j} (uX^d + v)^{\beta_j} \in \mathbb{Q}(\alpha)[X]$
  - Deterministic PIT algorithm in $\mathrm{poly}(k, \log(\alpha_j), \log(\beta_j), \log d)$
  - Gap Theorem for linear factors + write $\alpha_j = q_j d + r_j$

Application to PIT

- $\sum_{j=1}^{k} a_j X^{\alpha_j} (uX^d + v)^{\beta_j} \in \mathbb{Q}(\alpha)[X]$
  - Deterministic PIT algorithm in $\mathrm{poly}(k, \log(\alpha_j), \log(\beta_j), \log d)$
  - Gap Theorem for linear factors + write $\alpha_j = q_j d + r_j$
- $\sum_{j=1}^{k} a_j \prod_{i=1}^{m} f_i^{\alpha_{ij}} \in \mathbb{Q}(\alpha)[X]$ with monic f_i's
  - Det. PIT alg. in $\mathrm{poly}(k, \log(\alpha_{ij}), \deg(f_i))$
  - Modified Gap Theorem (for multiplicity of factors)
  - If f_i's not monic: needs to test $\sum_j \prod_i \lambda_i^{\alpha_{ij}} = 0$?
  - Maybe valid with multivariate f_i's...

Conclusion

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree multivariate polynomials} \end{cases}$

Conclusion

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree multivariate polynomials} \end{cases}$
  - "Field-independent"
  - **Simpler** and **more general** than previous algorithms
  - Partial results in **large positive characteristic**
  - Implementation available: package Lacunaryx of Mathemagix

Conclusion

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree multivariate polynomials} \end{cases}$
  - "Field-independent"
  - **Simpler** and **more general** than previous algorithms
  - Partial results in **large positive characteristic**
  - Implementation available: package Lacunaryx of Mathemagix
- Open questions:
  - **Lacunary factors** in polynomial time?
  - More general settings: SLP/arithmetic circuits
  - **Small positive characteristic**?

Conclusion

- Computing low-degree factors of lacunary multivariate polynomials
  - Reduction to $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree multivariate polynomials} \end{cases}$
  - "Field-independent"
  - **Simpler** and **more general** than previous algorithms
  - Partial results in **large positive characteristic**
  - Implementation available: package Lacunaryx of Mathemagix
- Open questions:
  - **Lacunary factors** in polynomial time?
  - More general settings: SLP/arithmetic circuits
  - **Small positive characteristic**?

תודה