# *Factorization of lacunary polynomials*

**Bruno Grenet**
LIRMM — Université de Montpellier

Séminaire DALI — April 07., 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 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, …;
  - in 1, 2, …, $n$ variables.
- Complexity: **polynomial in** $\deg(f)$

**Factorization of a polynomial $f$**

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

- Many algorithms
  - over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\mathbb{F}_q$, $\mathbb{R}$, $\mathbb{C}$, …;
  - in $1, 2, \dots, n$ 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 $f_1, \dots, f_t$, irreducible, s.t. $f = f_1 \times \cdots \times f_t$.

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

$$X^{568742}Y^{568741} + X^{568741}Y^{568742} - X^{568741}Y^{568741} - X - Y + 1$$
$$= (X + Y - 1) \times (X^{568741}Y^{568741} - 1)$$
$$= (X + Y - 1) \times (XY - 1) \times (1 + XY + \cdots + X^{568740}Y^{568740})$$

**Definition**

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

- $\operatorname{size}(f)\simeq k\Big(\max_j(\operatorname{size}(c_j))+n\log(\deg f)\Big)$

## Definition

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

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

## 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 $f\in\mathbb{Q}(\alpha)[X_1,\dots,X_n]$. [Kaltofen-Koiran'06, G.'14]

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

## *Univariate polynomials*

*over $\mathbb{Z}$, $\mathbb{Q}$ or a number field*

# *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** $f \in \mathbb{Z}[X]$.

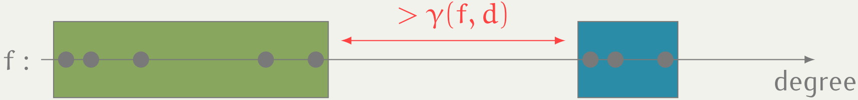
**Gap Theorem** [Cucker-Koiran-Smale'98]

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 $|x| \geqslant 2$,
$f(x) = 0 \implies f_1(x) = f_2(x) = 0$.

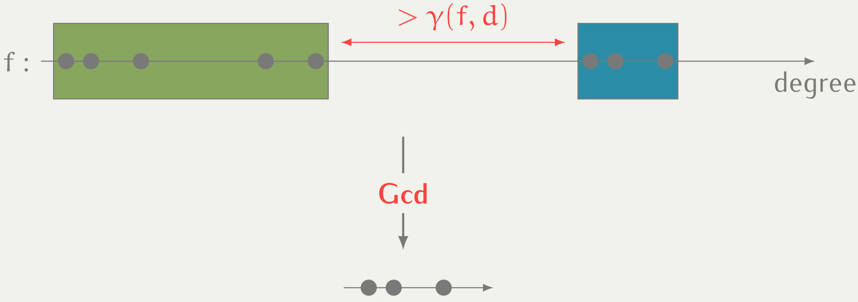
$$-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)$$

# *Lenstra's algorithm (non-cyclotomic factors)*

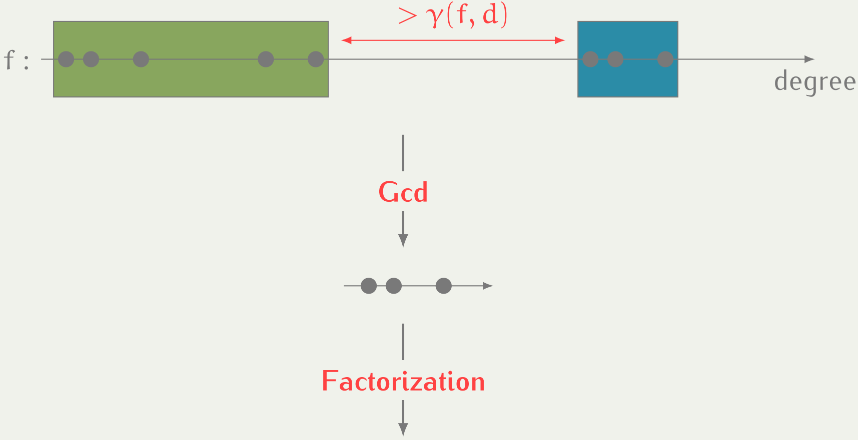
# *Lenstra's algorithm (non-cyclotomic factors)*



# *Lenstra's algorithm (non-cyclotomic factors)*



# *Lenstra's algorithm (non-cyclotomic factors)*

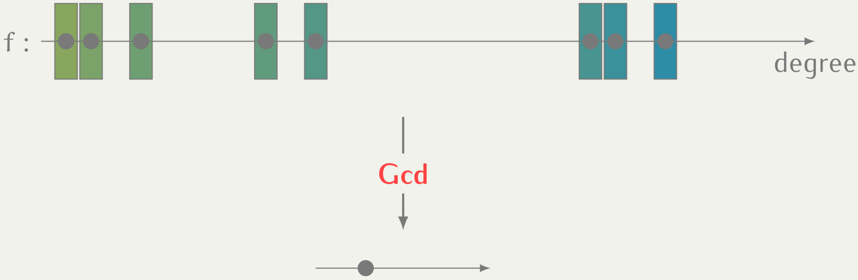



Degree-d non-cyclotomic factors of f

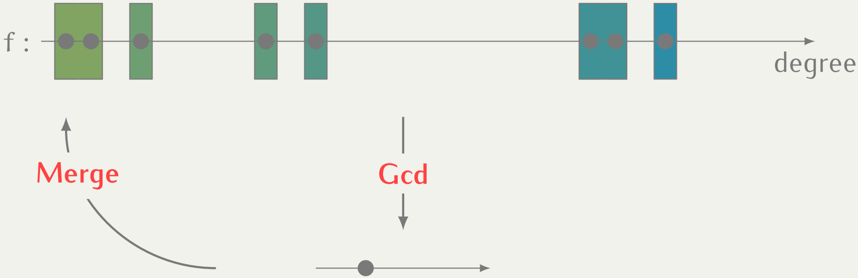
# *Implemented algorithm (non-cyclotomic factors)*

# *Implemented algorithm (non-cyclotomic factors)*

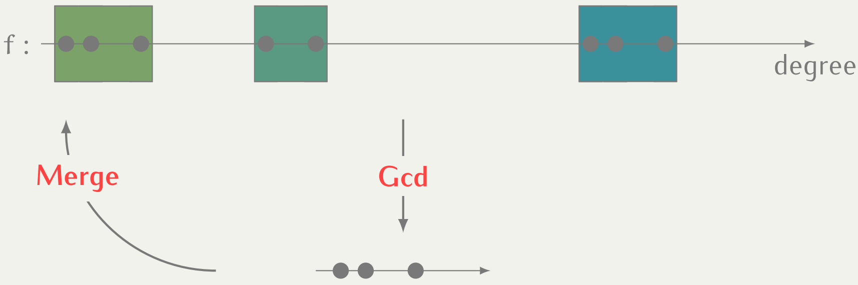
# *Implemented algorithm (non-cyclotomic factors)*



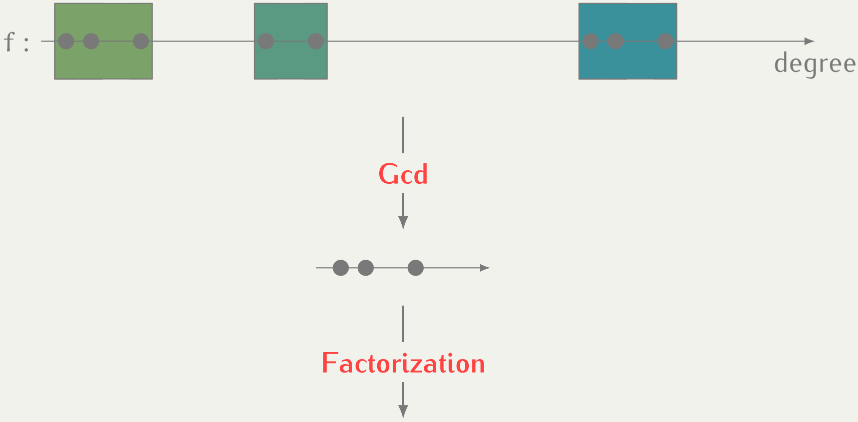
# *Implemented algorithm (non-cyclotomic factors)*



# *Implemented algorithm (non-cyclotomic factors)*

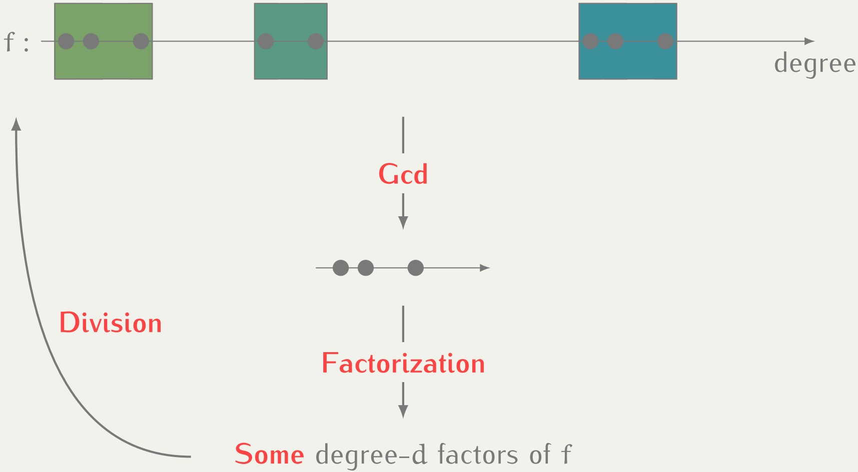


# *Implemented algorithm (non-cyclotomic factors)*



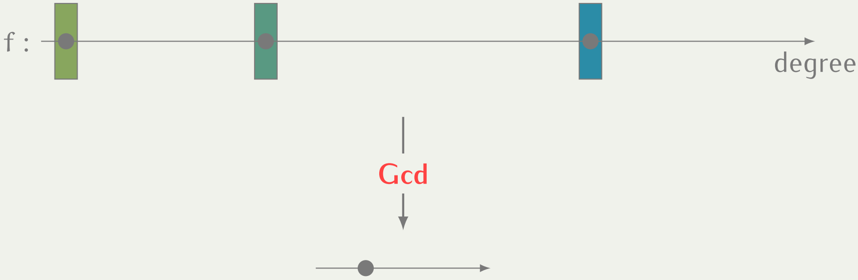

**Some** degree-$d$ factors of $f$

# *Implemented algorithm (non-cyclotomic factors)*

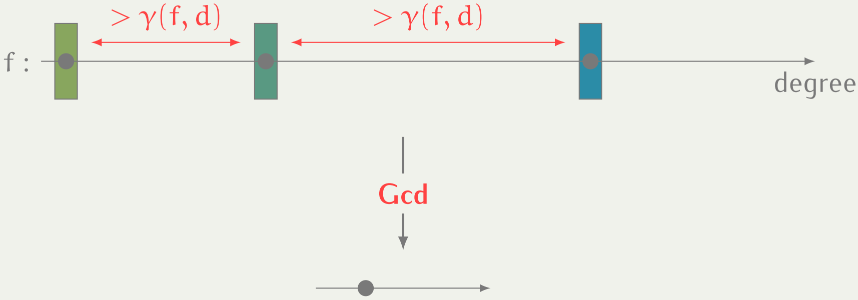


# *Implemented algorithm (non-cyclotomic factors)*

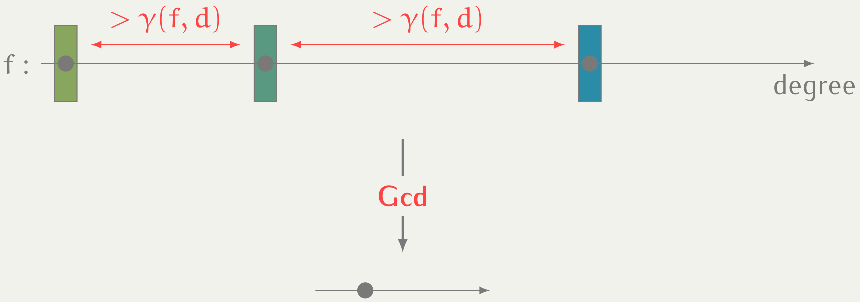
# *Implemented algorithm (non-cyclotomic factors)*



# *Implemented algorithm (non-cyclotomic factors)*



# *Implemented algorithm (non-cyclotomic factors)*




**Partial factorization:**

$$f = \underbrace{\prod_{g \in G} g}_{\text{low-degree factors}} \times \underbrace{\prod_{h \in H} h}_{\text{sparse polynomials}}$$

*Package Lacunaryx of Mathemagix*

$$f = l \times c \times s$$

- $l$: product of low-degree polynomials
- $c$: product of $X^r - 1$
- $s$: *perturbated* sparse polynomial: $s = \sum_{j=1}^{n} X^{\alpha_j} p_j(X)$

$$f = l \times c \times s$$

- $l$: product of low-degree polynomials
- $c$: product of $X^r - 1$
- $s$: *perturbated* sparse polynomial: $s = \sum_{j=1}^{n} X^{\alpha_j} p_j(X)$

$\rightsquigarrow$ **degree $\geqslant 1\,000\,000$, $\geqslant 10\,000$ terms, coefficients $\geqslant 5 \times 10^9$**

$$f = l \times c \times s$$

- $l$: product of low-degree polynomials
- $c$: product of $X^r - 1$
- $s$: *perturbated* sparse polynomial: $s = \sum_{j=1}^{n} X^{\alpha_j} p_j(X)$

$\rightsquigarrow$ **degree $\geqslant 1\,000\,000$, $\geqslant 10\,000$ terms, coefficients $\geqslant 5 \times 10^9$**

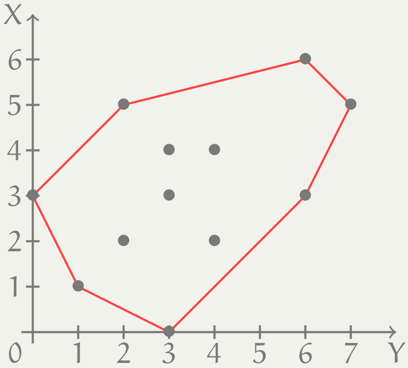
| degree | 5 | 10 | 15 | 20 |
|---|---|---|---|---|
| time (ms) | 1994 | 2924 | 12190 | 26165 |

Intel© Core™ CPU @ 2.60GHz with 7.7GB RAM

*Multivariate polynomials*

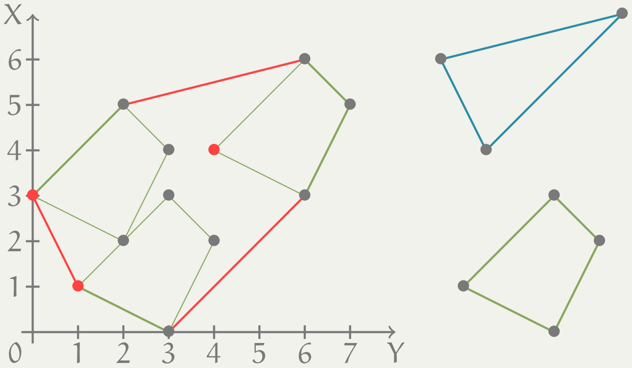
*over any field of characteristic 0*

## *Newton polygon/tope*




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

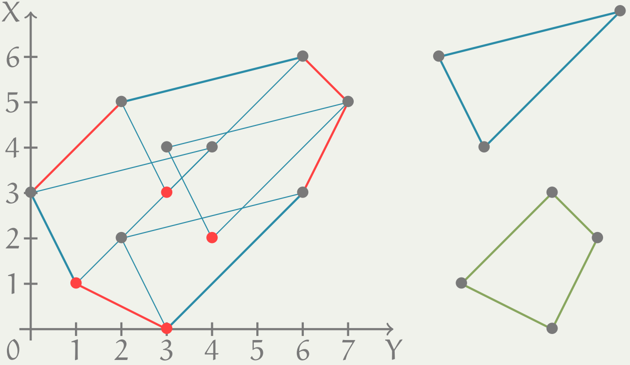
# *Newton polygon/tope*




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

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

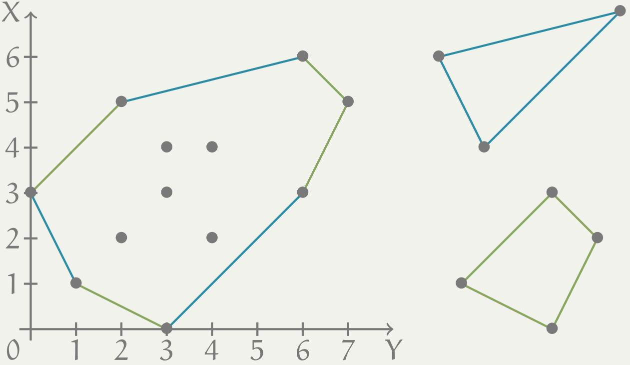
# *Newton polygon/tope*




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

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

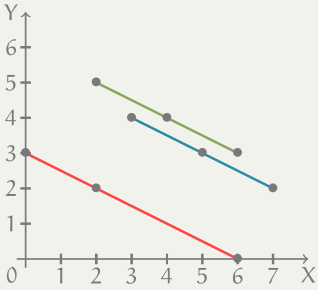
## *Newton polygon/tope*



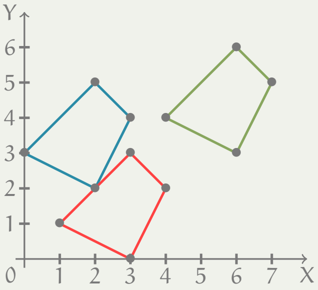

$$f = Y^3 + 2XY - X^2Y^4 + X^3Y^3 - 2X^2Y^2 - 4X^3 + 2X^4Y^3 - 2X^5Y^2 + X^3Y^6 + 2X^4Y^4 - X^5Y^7 + X^6Y^6$$

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

# *Two kinds of factors*

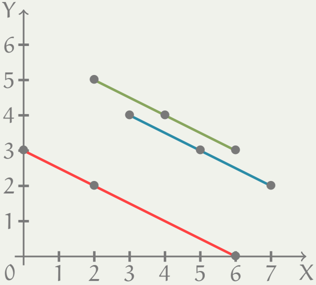



Unidimensional factors




Multidimensional factors

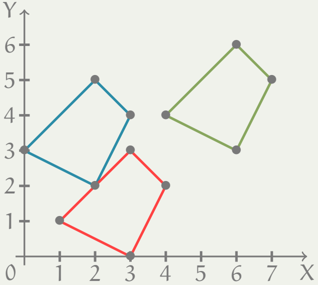
# *Two kinds of factors*




Unidimensional factors

⇓

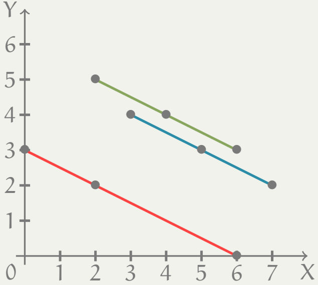
Univariate lacunary factorization




Multidimensional factors

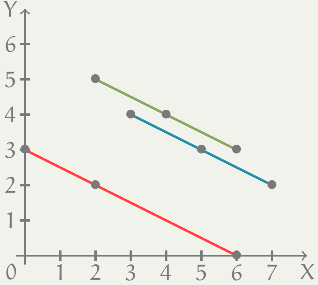
⇓

Multivariate low-degree factorization




- $X^\gamma f(X^\delta)$ for some univariate $f \in \mathbb{K}[Z]$
- Each direction $\delta$ independently

# *Unidimensional factors*




- $X^\gamma f(X^\delta)$ for some univariate $f \in \mathbb{K}[Z]$
- Each direction $\delta$ independently

1. Write $f$ as a sum of **$\delta$-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**

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

# *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**

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

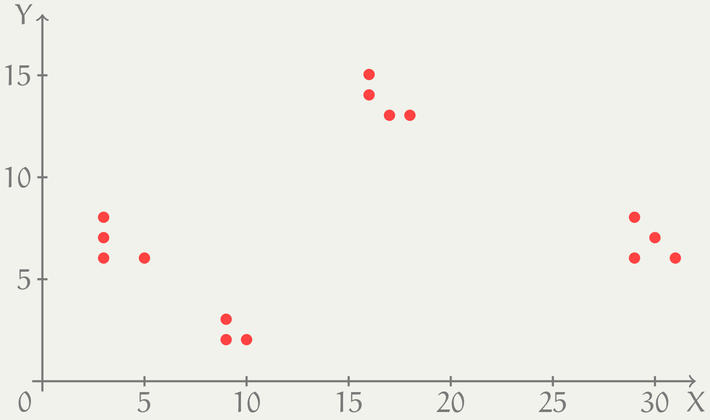
**Gap Theorem**

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

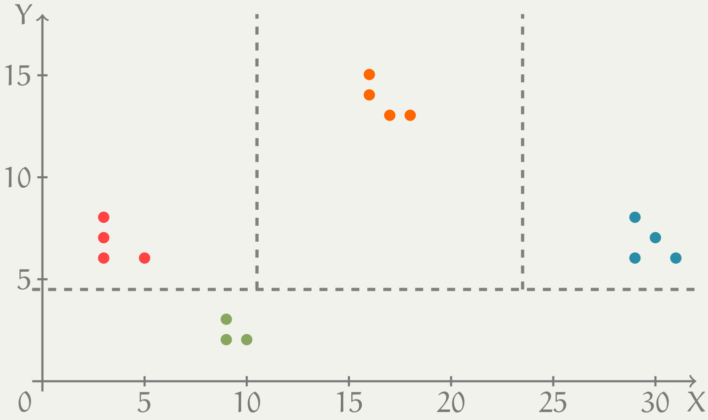
$$f = X^{31}Y^{6} - 2X^{30}Y^{7} + X^{29}Y^{8} - X^{29}Y^{6} + X^{18}Y^{13} - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^{2} - X^{9}Y^{3} + X^{9}Y^{2} - X^{5}Y^{6} + X^{3}Y^{8} - 2X^{3}Y^{7} + X^{3}Y^{6}$$

# *An example*

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



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



# *An example*

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

$$f_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$f_2 = X^9Y^2(X - Y + 1)$$

$$f_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$f_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

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

$$f_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$f_2 = X^9Y^2(X - Y + 1)$$

$$f_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$f_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

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

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

- $\phi_1, \dots, \phi_d$ are **Puiseux series**:

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

**Theorem** [G.'14]

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

where

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

**Theorem** [G.'14]

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

where

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

- Gap Theorem:
  "If $f = f_1 + f_2$ with a gap, $g$ divides $f$ iff it divides $f_1$ and $f_2$"

**Theorem** [G.'14]

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

where

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

- 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 $\nu$'s

**Theorem** [G.'14]

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

where

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

- 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 $\nu$'s
- Multivariate polynomials: recursive use of the Gap Theorem

**Corollary**

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

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

**Complexity:** Deterministic polynomial time

**Corollary**

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

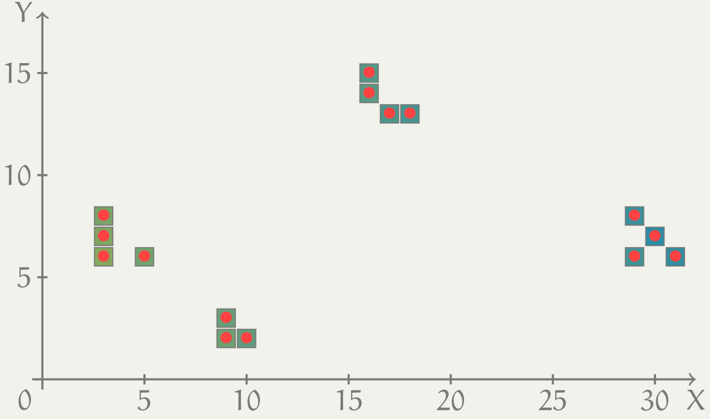
**Output:** Degree-$O(d^4 s(f)^2)$ polynomial $f_{ld}$ s.t for all multidimensional degree-$d$ polynomial $g$, $\text{mult}_g(f) = \text{mult}_g(f_{ld})$

**Complexity:** Deterministic polynomial time

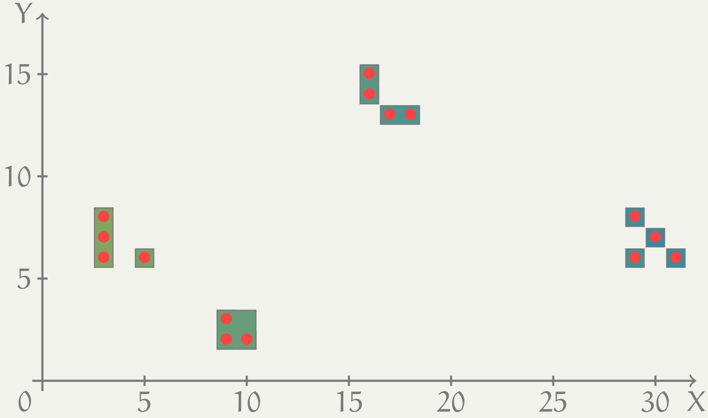
1. Write $f = f_1 + \cdots + f_s$ where $\deg_{X_i}(f_t) - \text{val}_{X_i}(f_t) \leqslant (4d^4 - 2d^2)\binom{s(f_t)}{2}$ for all $i$;
2. Return $\gcd(f_1, \dots, f_s)$.

(3. Factor the gcd using a low-degree factorization algorithm.)

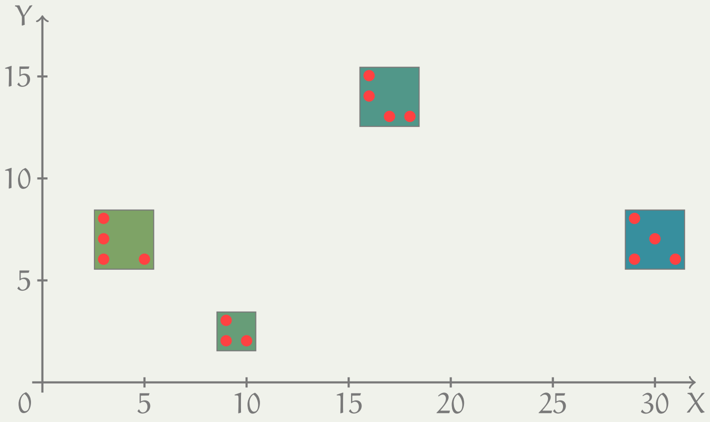
# *Implemented algorithm*

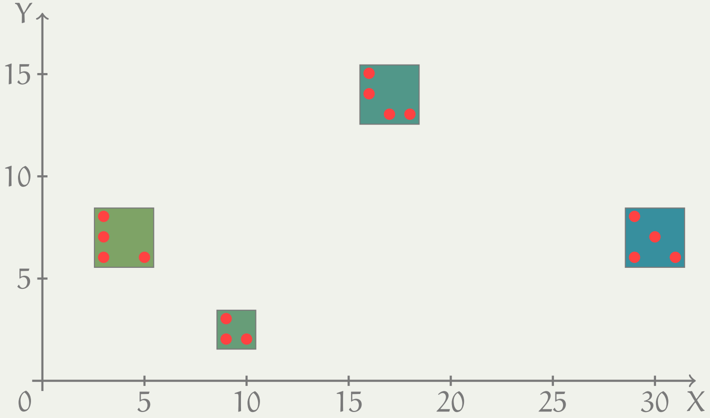


# *Implemented algorithm*

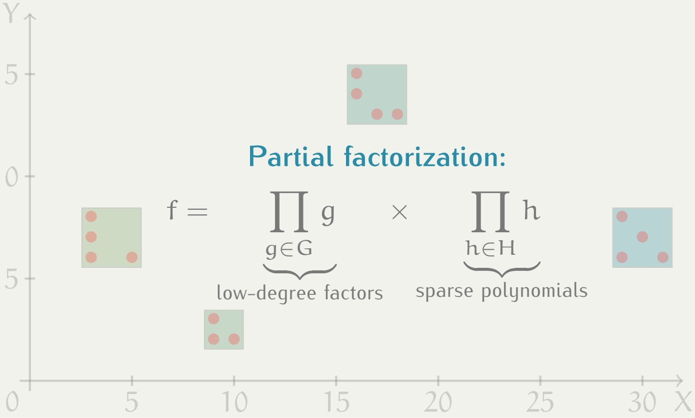


# *Implemented algorithm*






**Single-linkage clustering**




**Partial factorization:**

$$f = \underbrace{\prod_{g \in G} g}_{\text{low-degree factors}} \times \underbrace{\prod_{h \in H} h}_{\text{sparse polynomials}}$$

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

monomials

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

unidim.

Degree-d factors of univariate lacunary polynomials

cyclo.

*Ad hoc* reduction to low-degree poly.

non-cyclo.

Factors of a low-degree poly.

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

multidim.

Factors of $f_{ld}$ of degree $\leqslant O(d^4k^2)$

Low-degree factorization $\mathbb{Q}(\alpha), \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$, etc.

```
Mmx] use "lacunaryx"; x : LPolynomial Integer == lpolynomial(1,1);
     p == x^3*(x-2)*(2*x+3)^2*(-x+3)*(2*x+7)*(x^2+x+1)*(3*x+5);
     q == x^3 - 6 - 2*x^4 + 12*x + x^5 - 6*x^2+ 3*x^1345 - 6*x^1346 + 3*x^1347 +
          8*x^432534 - 18*x^432535 + 12*x^432536 - 2*x^432537 + 1 - 2*x + x^2;
     e : Integer == 351540145040401152301435l4;
     r == 1 + 3*x^1345 - 2*(x-4)*x^e + (x^3-6)*x^(2*e);
     pqr == p*q*r; (log deg pqr/log 2, #pqr)
```

$(85.861891823199, 149)$

49 msec

```
Mmx] roots pqr
```

$[[2, 1], [3, 1], [0, 3], [1, 2]]$

43 msec

```
Mmx] X == coordinate ('x); x : LMVPolynomial Integer == lmvpolynomial(1, X);
     Y == coordinate ('y); y : LMVPolynomial Integer == lmvpolynomial(1, Y);
     f == x^2*y*(x-2)*(2*y+3)^2*(y-x+3)*(2*x+7*y)*(x*y+x+1)*(3*x-6*y+5);
     g == x^3*y^54354165 - 6*y^54354165 - 2*x^4*y^54354164 + 12*x*y^54354164
     + x^5*y^54354163 - 6*x^2*y^54354163 + 3*x^1345*y^54336 - 6*x^1346*y^54335
     + 3*x^1347*y^54334 + 8*x^432534*y^5 - 18*x^432535*y^4 + 12*x^432536*y^3 -
     2*x^432537*y^2 + y^2 - 2*x*y + x^2;
     h == 1 + 3*x^1345*y^54334 - 2*(x-4*y)*x^e*y^2 + (x^3-6)*y^(2*e);
     fgh == f*g*h; (log deg fgh/log 2, #fgh)
```

$(85.861891823199, 1028)$

60 msec

```
Mmx] linear_factors fgh
```

$[[x, 2], [-x+2, 1], [y, 1], [2\,y+3, 2], [-y+x, 2], [-7\,y-2\,x, 1], [-y+x-3, 1], [-6\,y+3\,x+5, 1]]$

299 msec

# *Conclusion*

- Computing bounded-degree factors of lacunary polynomials
  - **Reduction** to low-degree factorization
  - Univariate: over number fields
  - Multivariate: over fields of characteristic 0
    + partial results in positive characteristic
  - Implementation: package Lacunaryx of Mathemagix

- Computing bounded-degree factors of lacunary polynomials
  - **Reduction** to low-degree factorization
  - Univariate: over number fields
  - Multivariate: over fields of characteristic 0
    + partial results in positive characteristic
  - Implementation: package Lacunaryx of Mathemagix
- Open questions:
  - **Lacunary factors**
  - Structural questions: how dense can be the factors?
  - Good notion of partial factorization

- Computing bounded-degree factors of lacunary polynomials
  - **Reduction** to low-degree factorization
  - Univariate: over number fields
  - Multivariate: over fields of characteristic 0
    + partial results in positive characteristic
  - Implementation: package Lacunaryx of Mathemagix
- Open questions:
  - **Lacunary factors**
  - Structural questions: how dense can be the factors?
  - Good notion of partial factorization

# Merci !