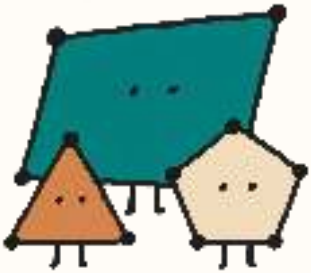
Factoring sparse polynomials fast

Alexander Demin
LIX, CNRS, Sorbonne Université

Joint work with Joris van der Hoeven



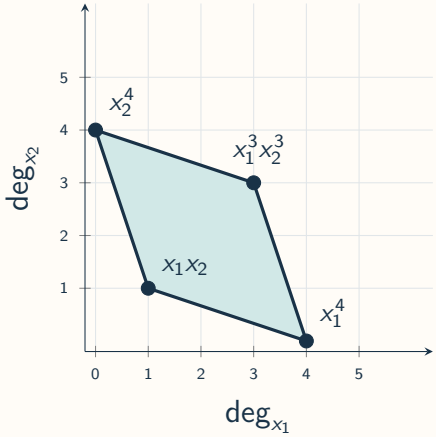
MAX seminar, LIX

9 November 2026

How does geometry help us factor polynomials?

Let $F \in \mathbb{K}[x_1, \ldots, x_n]$.
Consider the Newton polytope of F.

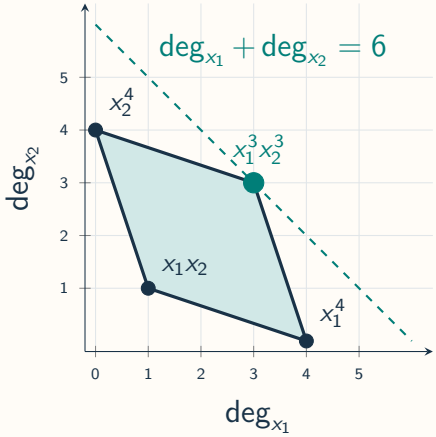
$$F = x_1^3 x_2^3 + x_1^4 + x_2^4 + x_1 x_2.$$



How does geometry help us factor polynomials?

Let $F \in \mathbb{K}[x_1, \ldots, x_n]$.
Consider the Newton polytope of F.

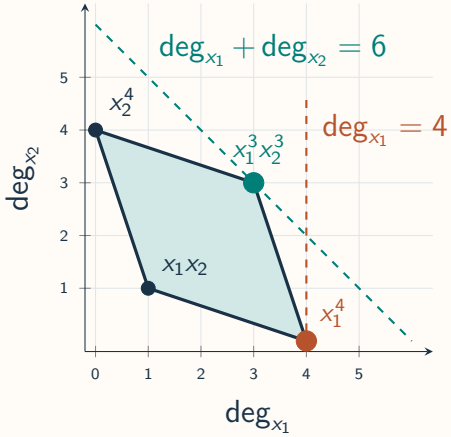
$$F = x_1^3 x_2^3 + x_1^4 + x_2^4 + x_1 x_2.$$



How does geometry help us factor polynomials?

Let $F \in \mathbb{K}[x_1, \ldots, x_n]$.
Consider the Newton polytope of F.

$$F = x_1^3 x_2^3 + x_1^4 + x_2^4 + x_1 x_2.$$



Plan

1. **GCD**
   - Evaluation/interpolation
   - Monic Laurent polynomials
2. **Factorization**

Setup

Talk of Tian Chen

Input: a black-box




```
int* F(const int* a);
```

Setup

Talk of Tian Chen

Input: a black-box




```
int* F(const int* a);
```

This talk

Input: an explicit polynomial

$$P, Q \in \mathbb{K}[x_1, \ldots, x_n],$$

$$P = x_1^4 + x_1^3 x_2 x_3 + \ldots,$$
$$Q = x_1^3 + x_1^2 x_2 x_3 + \ldots$$

Setup

Talk of Tian Chen

Input: a black-box




```
int* F(const int* a);
```

This talk

Input: an explicit polynomial

$$P, Q \in \mathbb{K}[x_1, \ldots, x_n],$$

$$P = x_1^4 + x_1^3 x_2 x_3 + \ldots,$$
$$Q = x_1^3 + x_1^2 x_2 x_3 + \ldots$$

$$\Downarrow$$

Output: an explicit polynomial

$$G = \gcd(P, Q) = x_1 + x_2 x_3 + x_3$$

Gauss lemma + Euclidean algorithm

$$P = x_1^4 + x_1^3 x_2 x_3 + x_1^3 x_3 + x_1 + x_2 x_3 + x_3,$$
$$Q = x_1^3 + x_1^2 x_2 x_3 + x_1^2 x_3 + x_1 x_2 + x_1 x_3 + x_1 + \dots$$

$$G = \gcd(P, Q) = ?$$

Gauss lemma + Euclidean algorithm

$$P = x_1^4 + (x_2x_3 + x_3)x_1^3 + x_1 + (x_2x_3 + x_3),$$
$$Q = x_1^3 + (x_2x_3 + x_3)x_1^2 + (1 + x_2 + x_3)x_1 + (x_2^2x_3 + \ldots).$$

Euclidean algorithm in $\mathbb{K}(x_2, x_3)[x_1]$: $G = \gcd(P, Q) = ?$

Gauss lemma + Euclidean algorithm

$$P = x_1^4 + (x_2x_3 + x_3)x_1^3 + x_1 + (x_2x_3 + x_3),$$
$$Q = x_1^3 + (x_2x_3 + x_3)x_1^2 + (1 + x_2 + x_3)x_1 + (x_2^2x_3 + \ldots).$$

Euclidean algorithm in $\mathbb{K}(x_2, x_3)[x_1]$: $\qquad G = \gcd(P, Q) = ?$

$$R_1 = P - x_1 Q,$$
$$R_2 = Q + \left(\frac{1}{1 + x_2 + x_3}x_1 + \frac{1}{(1 + x_2 + x_3)^2}\right) R_1,$$
$$R_3 = 0.$$
$$\rightsquigarrow \boxed{G = \frac{R_2}{\mathrm{lc}_{x_1} R_2} = x_1 + (x_2x_3 + x_3)}.$$

Gauss lemma + Euclidean algorithm

$$P = x_1^4 + (x_2x_3 + x_3)x_1^3 + x_1 + (x_2x_3 + x_3),$$
$$Q = x_1^3 + (x_2x_3 + x_3)x_1^2 + (1 + x_2 + x_3)x_1 + (x_2^2x_3 + \ldots).$$

Euclidean algorithm in $\mathbb{K}(x_2, x_3)[x_1]$: $\quad G = \gcd(P, Q) = ?$

$$R_1 = P - x_1 Q,$$

$$R_2 = Q + \left(\frac{1}{1 + x_2 + x_3}x_1 + \frac{1}{(1 + x_2 + x_3)^2}\right) R_1,$$

$$R_3 = 0.$$



Expression swell

$$\rightsquigarrow \boxed{G = \frac{R_2}{\mathrm{lc}_{x_1} R_2} = x_1 + (x_2x_3 + x_3)}.$$

Evaluation and interpolation

$$P = x_1^4 + (x_2x_3 + x_3)x_1^3 + x_1 + (x_2x_3 + x_3),$$
$$Q = x_1^3 + (x_2x_3 + x_3)x_1^2 + (1 + x_2 + x_3)x_1 + (x_2^2x_3 + \ldots).$$

Evaluation and interpolation

$$P = x_1^4 + (x_2x_3 + x_3)x_1^3 + x_1 + (x_2x_3 + x_3),$$
$$Q = x_1^3 + (x_2x_3 + x_3)x_1^2 + (1 + x_2 + x_3)x_1 + (x_2^2x_3 + \ldots).$$

$$(x_2, x_3) = (1, 1)$$

Evaluation and interpolation

$$P = x_1^4 + 2x_1^3 + x_1 + 2,$$
$$Q = x_1^3 + 2x_1^2 + 3x_1 + 6.$$

$$(x_2, x_3) = (1, 1)$$

Evaluation and interpolation

$$P = x_1^4 + 2x_1^3 + x_1 + 2,$$
$$Q = x_1^3 + 2x_1^2 + 3x_1 + 6.$$

Euclidean algorithm in $\mathbb{Q}[x_1]$:

$$R_1 = P - x_1 Q,$$
$$R_2 = Q + \left(\frac{1}{3}x_1 + \frac{1}{9}\right) R_1,$$
$$R_3 = 0.$$

$$\rightsquigarrow \boxed{G(x_1, 1, 1) = x_1 + 2}.$$

$$(x_2, x_3) = (1, 1)$$

Evaluation and interpolation

$$P = x_1^4 + 9x_1^3 + x_1 + 9,$$
$$Q = x_1^3 + 9x_1^2 + 6x_1 + 54.$$

Euclidean algorithm in $\mathbb{Q}[x_1]$:

$$R_1 = P - x_1 Q,$$
$$R_2 = Q + \left(\frac{1}{6}x_1 + \frac{1}{36}\right) R_1,$$
$$R_3 = 0.$$

$$\rightsquigarrow \boxed{G(x_1, 2, 3) = x_1 + 9}.$$

$$(x_2, x_3) = (2, 3)$$

Evaluation and interpolation

$$P = x_1^4 + 45x_1^3 + x_1 + 45,$$
$$Q = x_1^3 + 45x_1^2 + 14x_1 + 630.$$

Euclidean algorithm in $\mathbb{Q}[x_1]$:

$$R_1 = P - x_1 Q,$$
$$R_2 = Q + \left(\frac{1}{14}x_1 + \frac{1}{196}\right) R_1,$$
$$R_3 = 0.$$

$$\rightsquigarrow \boxed{G(x_1, 4, 9) = x_1 + 45}.$$

$$(x_2, x_3) = (4, 9)$$

Evaluation and interpolation

$(1, 1)$	$\longmapsto$	$x_1 + \mathbf{2}$
$(2, 3)$	$\longmapsto$	$x_1 + \mathbf{9}$
$(4, 9)$	$\longmapsto$	$x_1 + \mathbf{45}$
$(8, 27)$	$\longmapsto$	$x_1 + \mathbf{243}$



Gaspard de Prony

src: Wikimedia Commons

Evaluation and interpolation

$(1,1)$	$\longmapsto$	$x_1 + \mathbf{2}$
$(2,3)$	$\longmapsto$	$x_1 + \mathbf{9}$
$(4,9)$	$\longmapsto$	$x_1 + \mathbf{45}$
$(8,27)$	$\longmapsto$	$x_1 + \mathbf{243}$



Gaspard de Prony

src: Wikimedia Commons

$\rightsquigarrow$

Prony/Ben-Or&Tiwari sparse interpolation

Input: $F(1,1),\ F(2,3),\ \ldots,\ F(2^{2s}, 3^{2s}),$

Output: $F \in \mathbb{K}[x_2, x_3].$

Evaluation and interpolation

$(1,1)$	$\longmapsto$	$x_1 + \mathbf{2}$
$(2,3)$	$\longmapsto$	$x_1 + \mathbf{9}$
$(4,9)$	$\longmapsto$	$x_1 + \mathbf{45}$
$(8,27)$	$\longmapsto$	$x_1 + \mathbf{243}$



Gaspard de Prony

src: Wikimedia Commons

$\rightsquigarrow$

Prony/Ben-Or&Tiwari sparse interpolation

Input: $F(1,1),\ F(2,3),\ \ldots,\ F(2^{2s}, 3^{2s})$,

Output: $F \in \mathbb{K}[x_2, x_3]$.

$\rightsquigarrow$ $\boxed{G = x_1 + (x_2 x_3 + x_3)}$.

Non-monic input may cause a problem

Suppose GCD in $\mathbb{K}[x_1, x_2, x_3]$ is

$$G = (x_2 + 1)x_1 + (x_2 + x_3).$$

Non-monic input may cause a problem

Suppose GCD in $\mathbb{K}[x_1, x_2, x_3]$ is

$$G = (x_2 + 1)x_1 + (x_2 + x_3).$$

Then GCD in $\mathbb{K}(x_2, x_3)[x_1]$ is

$$\frac{G}{\mathrm{lc}_{x_1} G} = x_1 + \frac{x_2 + x_3}{x_2 + 1}.$$

Non-monic input may cause a problem

Suppose GCD in $\mathbb{K}[x_1, x_2, x_3]$ is

$$G = (x_2 + 1)x_1 + (x_2 + x_3).$$

Then GCD in $\mathbb{K}(x_2, x_3)[x_1]$ is

$$\frac{G}{\mathrm{lc}_{x_1} G} = x_1 + \frac{x_2 + x_3}{x_2 + 1}.$$

And GCD after setting $(x_2, x_3) = (2, 3)$ is

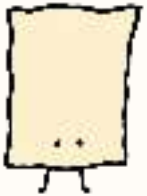
$$x_1 + \frac{5}{3}.$$

Need to interpolate a rational function?.. $\rightsquigarrow$ shift $x_j \mapsto x_j + 1$?

Affine shifts

One monomial over $\mathbb{Q}$

$$F = x_1^m \cdots x_n^m.$$



1 term

Shift $x_j \mapsto x_j + 1$ and expand

$$F(x_1 + 1, \ldots, x_n + 1) = \prod_{j=1}^{n} (x_j + 1)^m.$$



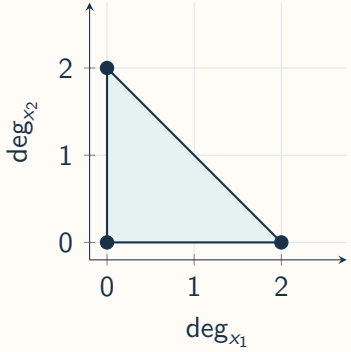
$(m+1)^n$ terms

Wang & Rothschild (1975), Kaltofen & Trager (1990), ...

Monic vs. non-monic

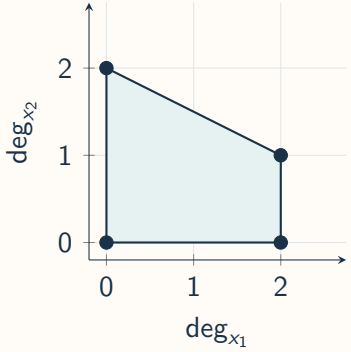
Monic in x_1

$G = 1 \cdot x_1^2 + x_2^2 + 1.$



Non-monic in x_1

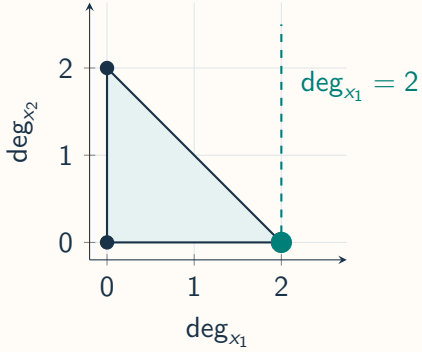
$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$



Monic vs. non-monic

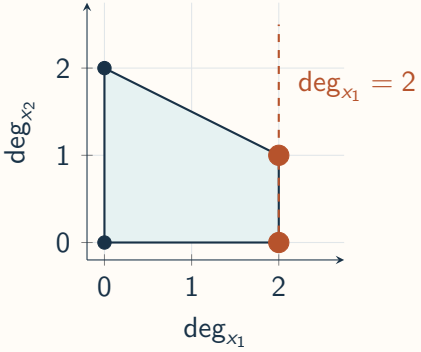
Monic in x_1

$G = 1 \cdot x_1^2 + x_2^2 + 1.$



Non-monic in x_1

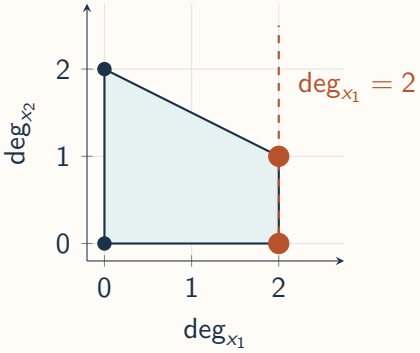
$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$



Projective change of variables

Non-monic in x_1

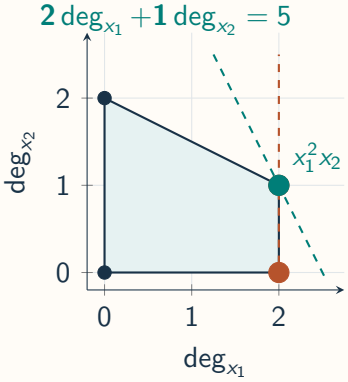
$$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$$



Projective change of variables

Non-monic in x_1

$$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$$



Projective change of variables

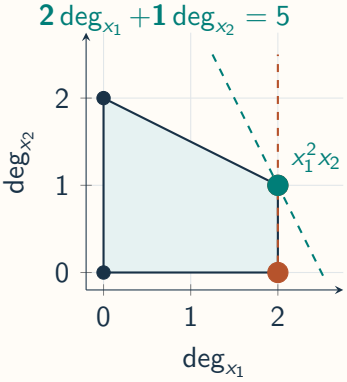
Non-monic in x_1

$$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$$

$$\boxed{(x_1, x_2) \mapsto (x_1 t^2, x_2 t^1)}$$

$$G(x_1 t^2, x_2 t^1) =$$

$$= \ (x_1^2 x_2) \cdot t^5 + (x_1^2) t^4 + (x_2^2) t^2 + (1)$$



Projective change of variables

Non-monic in x_1

$$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$$

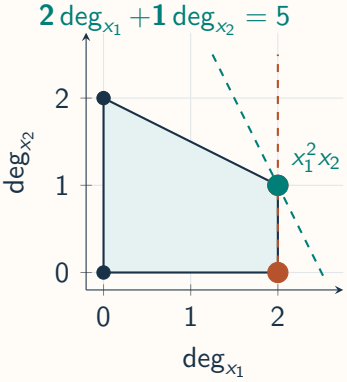
$$\boxed{(x_1, x_2) \mapsto (x_1 t^2, x_2 t^1)}$$

$$G(x_1 t^2, x_2 t^1) =$$

$$= (x_1^2 x_2) \cdot t^5 + (x_1^2) t^4 + (x_2^2) t^2 + (1)$$

$$\propto (1) \cdot t^5 + (x_2^{-1}) t^4 + (x_1^{-2} x_2) t^2 + (x_1^{-2} x_2^{-1})$$

$$\in \mathbb{K}[t, x_1, x_2, x_1^{-1}, x_2^{-1}]$$



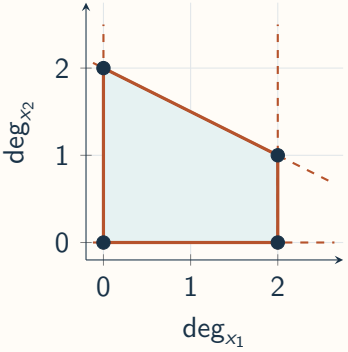
Projective change of variables

Non-monic in x_1

$$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$$

Unlucky weights $= \mathrm{Trop}(V(G))$

$(w_1, w_2) \in \{(1,0), (1,2), (-1,0),\ (0,-1)\}.$



Projective change of variables

Non-monic in x_1

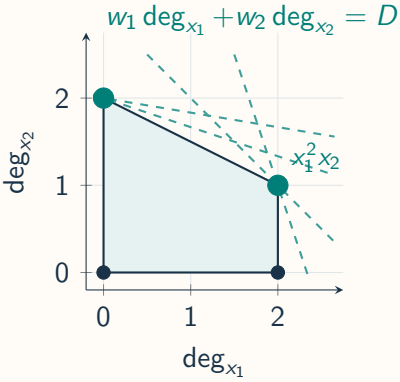
$$G = (x_2 + 1) \cdot x_1^2 + x_2^2 + 1.$$

Unlucky weights $= \mathrm{Trop}(V(G))$

$(w_1, w_2) \in \{(1,0), (1,2), (-1,0), \ (0,-1)\}.$

Almost any weights (w_1, w_2) work:

$$G(x_1 t^{w_1}, x_2 t^{w_2}) = (x_1^{e_1} x_2^{e_2}) t^D + \ldots$$



Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ [Demin & van der Hoeven]

Output: $G = \gcd(P, Q)$.

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ [Demin & van der Hoeven]

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ [Demin & van der Hoeven]

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.
2. For $i = 0, 1, 2, \ldots$

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ [Demin & van der Hoeven]

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.
2. For $i = 0, 1, 2, \ldots$
   - Evaluate at $(x_1, \ldots, x_n) := (\alpha_1^i, \ldots, \alpha_n^i)$ to get $\hat{P}_i(t), \hat{Q}_i(t)$.

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ [Demin & van der Hoeven]

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.
2. For $i = 0, 1, 2, \ldots$
   - Evaluate at $(x_1, \ldots, x_n) := (\alpha_1^i, \ldots, \alpha_n^i)$ to get $\hat{P}_i(t), \hat{Q}_i(t)$.
   - Compute univariate $\hat{G}_i(t) = \gcd(\hat{P}_i, \hat{Q}_i)$.

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ [Demin & van der Hoeven]

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.
2. For $i = 0, 1, 2, \ldots$
   - Evaluate at $(x_1, \ldots, x_n) := (\alpha_1^i, \ldots, \alpha_n^i)$ to get $\hat{P}_i(t), \hat{Q}_i(t)$.
   - Compute univariate $\hat{G}_i(t) = \gcd(\hat{P}_i, \hat{Q}_i)$.
3. Interpolate $\hat{G}$, put $t = 1$, and return it.

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ **How many terms?** $\rightsquigarrow$ s_{in}

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.
2. For $i = 0, 1, 2, \ldots$ **How many iterations?** $\rightsquigarrow$ $2s_{\text{out}}$
   - Evaluate at $(x_1, \ldots, x_n) := (\alpha_1^i, \ldots, \alpha_n^i)$ to get $\hat{P}_i(t), \hat{Q}_i(t)$.
   - Compute univariate $\hat{G}_i(t) = \gcd(\hat{P}_i, \hat{Q}_i)$.
3. Interpolate $\hat{G}$, put $t = 1$, and return it.

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ **How many terms?** $\rightsquigarrow$ s_{in}

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.
2. For $i = 0, 1, 2, \ldots$ **How many iterations?** $\rightsquigarrow$ $2s_{\text{out}}$
   - Evaluate at $(x_1, \ldots, x_n) := (\alpha_1^i, \ldots, \alpha_n^i)$ to get $\hat{P}_i(t), \hat{Q}_i(t)$.
   - Compute univariate $\hat{G}_i(t) = \gcd(\hat{P}_i, \hat{Q}_i)$.
3. Interpolate $\hat{G}$, put $t = 1$, and return it.

Total cost in $\mathbb{K}$:

$$2s_{\text{out}} \cdot (\text{eval} + \gcd) \; + \; \text{interpolate}$$

Multivariate sparse GCD

Input: $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ **How many terms?** $\rightsquigarrow$ s_{in}

Output: $G = \gcd(P, Q)$.

1. Choose weights $w = (w_1, \ldots, w_n)$ and form $\hat{P} = P(x_1 t^{w_1}, \ldots, x_n t^{w_n})$ and $\hat{Q}$.
2. For $i = 0, 1, 2, \ldots$ **How many iterations?** $\rightsquigarrow$ $2s_{\text{out}}$
   - Evaluate at $(x_1, \ldots, x_n) := (\alpha_1^i, \ldots, \alpha_n^i)$ to get $\hat{P}_i(t), \hat{Q}_i(t)$.
   - Compute univariate $\hat{G}_i(t) = \gcd(\hat{P}_i, \hat{Q}_i)$.
3. Interpolate $\hat{G}$, put $t = 1$, and return it.

Total cost in $\mathbb{K}$:

$$2s_{\text{out}} \cdot (\text{eval} + \gcd) \ + \ \text{interpolate}$$

$$= \widetilde{O}(s_{\text{in}} + D \ s_{\text{out}})$$

Plan

1. ~~GCD~~
   - ~~Evaluation/interpolation~~
   - ~~Monic Laurent polynomials~~
2. **Factorization**
   - Slope factorization
   - Reconciling with reality

Reduction from multivariate case

Input: $F \in \mathbb{K}[x_1, \ldots, x_n]$

Output: $F = cP_1 \cdots P_k$, where P_i is irreducible

Reduction from multivariate case

Input: $F \in \mathbb{K}[x_1, \ldots, x_n]$

Output: $F = cP_1 \cdots P_k$, where P_i is irreducible

First idea: set $\hat{F} = F(x_1 t^{w_1}, \ldots, x_n t^{w_n})$, factor univariate $\hat{F}(t)_{x_1=2, x_2=3, \ldots}$, repeat?

Reduction from multivariate case

Input: $F \in \mathbb{K}[x_1, \ldots, x_n]$

Output: $F = cP_1 \cdots P_k$, where P_i is irreducible

First idea: set $\hat{F} = F(x_1 t^{w_1}, \ldots, x_n t^{w_n})$, factor univariate $\hat{F}(t)_{x_1=2, x_2=3, \ldots}$, repeat?

First complication: let $\mathbb{K} = \mathbb{C}$ and consider irreducible

$$F = x_1^2 - x_2 x_3.$$

Reduction from multivariate case

Input: $F \in \mathbb{K}[x_1, \ldots, x_n]$

Output: $F = cP_1 \cdots P_k$, where P_i is irreducible

First idea: set $\hat{F} = F(x_1 t^{w_1}, \ldots, x_n t^{w_n})$, factor univariate $\hat{F}(t)_{x_1=2, x_2=3, \ldots}$, repeat?

First complication: let $\mathbb{K} = \mathbb{C}$ and consider irreducible

$$F = x_1^2 - x_2 x_3.$$

For every $a, b \in \mathbb{C}$,

$$\begin{aligned} F(x_1, a, b) &= x_1^2 - ab \\ &= (x_1 - \sqrt{ab})(x_1 + \sqrt{ab}). \end{aligned}$$

Reduction from multivariate case

Input: $F \in \mathbb{K}[x_1, \ldots, x_n]$

Output: $F = cP_1 \cdots P_k$, where P_i is irreducible

First idea: set $\hat{F} = F(x_1 t^{w_1}, \ldots, x_n t^{w_n})$, factor **bivariate** $\hat{F}(x_1, t)_{x_2=2, x_3=3, \ldots}$, repeat?

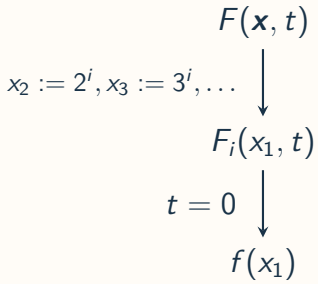
First complication: let $\mathbb{K} = \mathbb{C}$ and consider irreducible

$$F = x_1^2 - x_2 x_3.$$

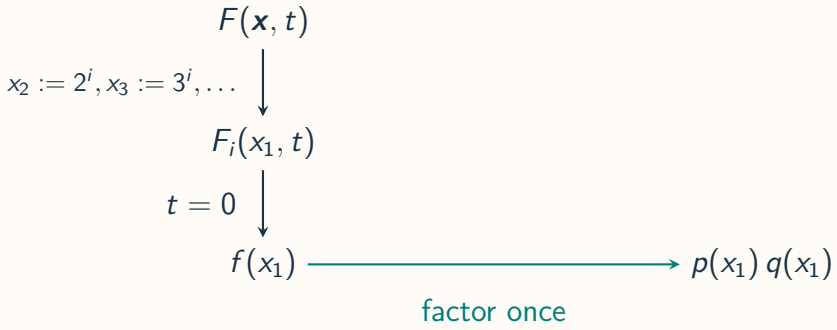
For every $a, b \in \mathbb{C}$,

$$\begin{aligned} F(x_1, at, bt) &= x_1^2 - abt^2 \\ &= (x_1 - \sqrt{ab}t)(x_1 + \sqrt{ab}t). \end{aligned}$$

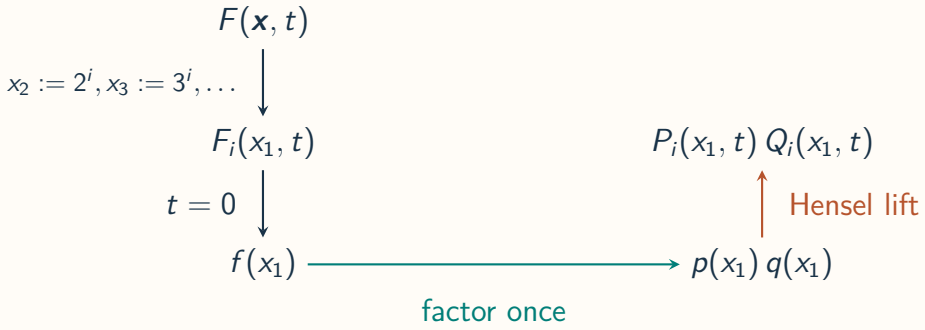
Against all the odds



Against all the odds

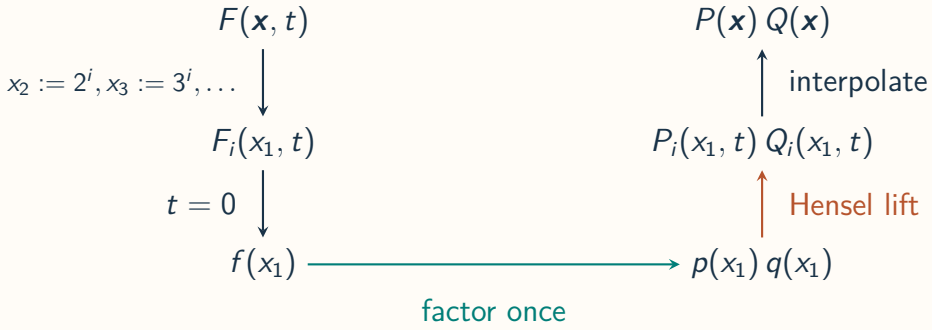


Against all the odds



For Hensel lift to succeed, require $\boxed{\deg_{x_1} F_i(x_1, t) = \deg f}$ and p, q coprime.

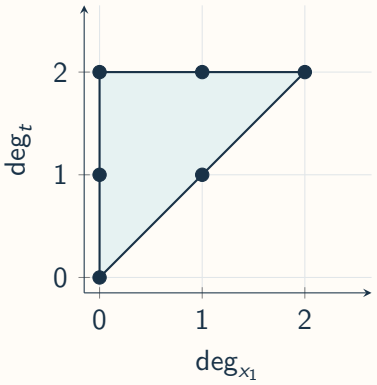
Against all the odds



For Hensel lift to succeed, require $\boxed{\deg_{x_1} F_i(x_1, t) = \deg f}$ and p, q coprime.

Condition on the degree

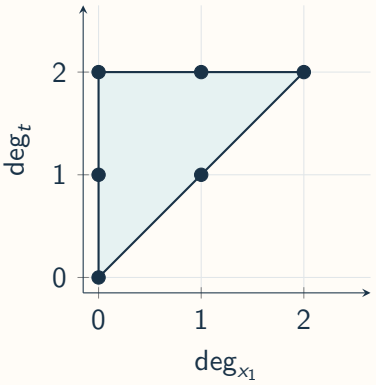
$$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$$



Condition on the degree

$$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$$

$$\boxed{\deg_{x_1} F(x_1, t) \stackrel{?}{=} \deg F(x_1, 0)}$$

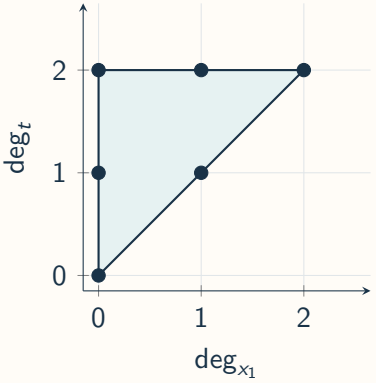


Condition on the degree

$$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$$

$$\boxed{\deg_{x_1} F(x_1, t) \stackrel{?}{=} \deg F(x_1, 0)}$$

$$\rightsquigarrow \quad 2 \neq 0.$$

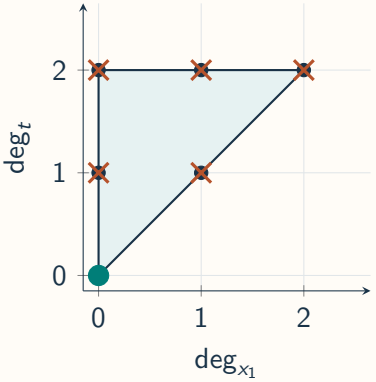


Condition on the degree

$$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$$

$$\boxed{\deg_{x_1} F(x_1, t) \stackrel{?}{=} \deg F(x_1, 0)}$$

$$\rightsquigarrow \quad 2 \neq 0.$$

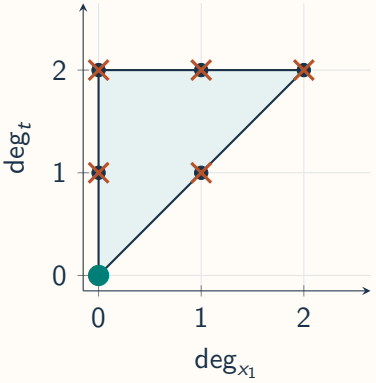


Condition on the degree

$$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$$

$$\boxed{\deg_{x_1} F(x_1, t) \stackrel{?}{=} \deg F(x_1, 0)}$$

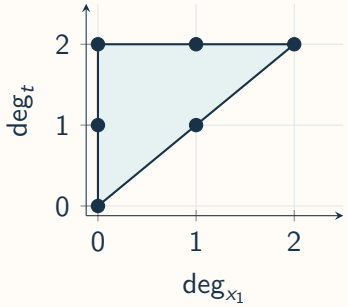
$\rightsquigarrow \quad 2 \neq 0.$



Remedy with a change of variables?

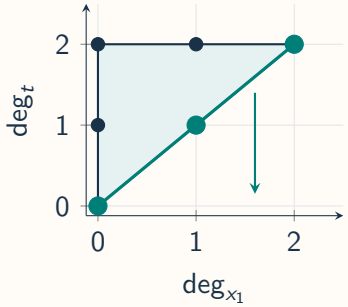
Single slope factorization

$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$



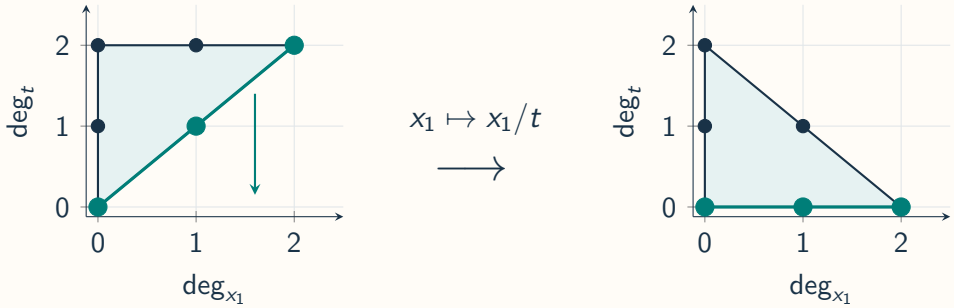
Single slope factorization

$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$



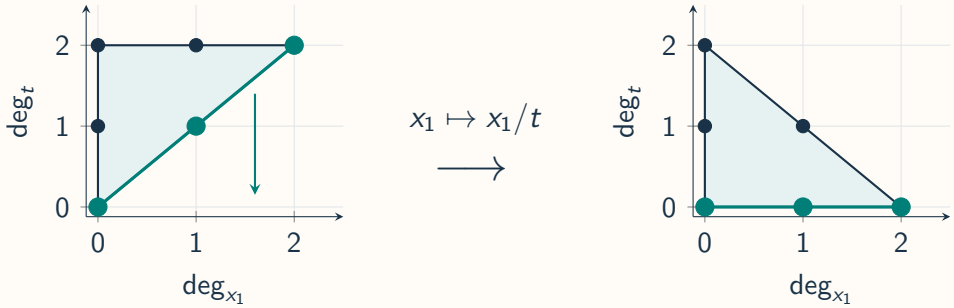
Single slope factorization

$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$



Single slope factorization

$F(x_1, t) = x_1^2 t^2 + 4x_1 t^2 + 3x_1 t + 3t^2 + 7t + 2.$



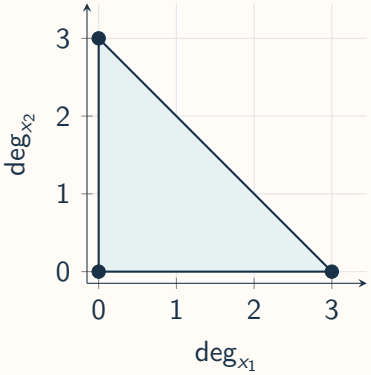
$F(x_1/t, t) = x_1^2 + 4x_1 t + 3x_1 + 3t^2 + 7t + 2$ (à la Weierstrass preparation)

Condition on being coprime

Let $F = PQ$, where

$$P = 1 + x_1^3 + x_2^3 + x_1 x_2,$$

$$Q = 1 + x_1^3 + x_2^3 + 2x_1 x_2.$$



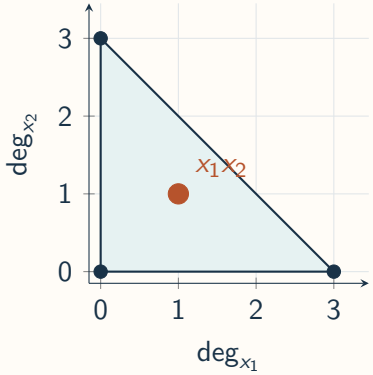
Condition on being coprime

Let $F = PQ$, where

$$P = 1 + x_1^3 + x_2^3 + x_1x_2,$$

$$Q = 1 + x_1^3 + x_2^3 + 2x_1x_2.$$

$P(x_1, 0), Q(x_1, 0)$ coprime?



Condition on being coprime

Let $F = PQ$, where

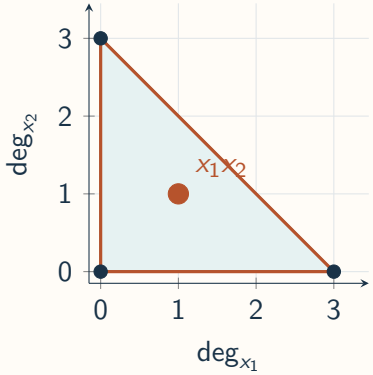
$$P = 1 + x_1^3 + x_2^3 + x_1x_2,$$

$$Q = 1 + x_1^3 + x_2^3 + 2x_1x_2.$$

$P(x_1, 0), Q(x_1, 0)$ coprime?

$\rightsquigarrow$

No, and cannot distinguish their polytopes



Controlled expression swell

Bertini irreducibility theorem

If $F \in \mathbb{K}[x_1, \ldots, x_n]$ is irreducible, then for generic a_i, b_i, c_i,

$$F(a_1 t + b_1 u + c_1, \ldots, a_n t + b_n u + c_n)$$

is irreducible in $\mathbb{K}[t, u]$.

Controlled expression swell

Bertini irreducibility theorem

If $F \in \mathbb{K}[x_1, \ldots, x_n]$ is irreducible, then for generic a_i, b_i, c_i,

$$F(a_1 t + b_1 u + c_1, \ldots, a_n t + b_n u + c_n)$$

is irreducible in $\mathbb{K}[t, u]$.

Complete algorithm

[Demin & van der Hoeven]

Let $d = \deg F$; s is the max. number of terms in input and output.

Assume $\operatorname{char} \mathbb{K} = 0$ or $\operatorname{char} \mathbb{K} > 2d^2$. With

$$\boxed{\widetilde{O}(d^3 s + d^{10})} \quad \text{operations in } \mathbb{K}$$

we can factor a polynomial in $\mathbb{K}[x_1, \ldots, x_n]$.



Future work: efficient implementation

"Before implementing a particular algorithm, one has to implement carefully many other routines for basic polynomial arithmetic, and designing a polynomial factorization package may require several woman-years."

von zur Gathen & Gerhard
Modern Computer Algebra (1999)

Thank you!