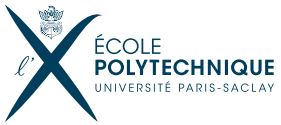
Fast Reduction of Bivariate Polynomials with Respect to Sufficiently Regular Gröbner Bases

Joris van der Hoeven, Robin Larrieu

Laboratoire d'Informatique de l'Ecole Polytechnique (LIX)



ISSAC '18 – New York, USA
18 / 07 / 2018

Introduction

- Fast Gröbner basis algorithms rely on linear algebra (ex: F4, F5...)
- Can we do it with polynomial arithmetic?

Introduction

- Fast Gröbner basis algorithms rely on linear algebra (ex: F4, F5...) $\rightarrow$ Not optimal unless $\omega = 2$.
- Can we do it with polynomial arithmetic? $\rightarrow$ Hope for asymptotically optimal algorithms.

Introduction

- Fast Gröbner basis algorithms rely on linear algebra (ex: F4, F5...) $\rightarrow$ Not optimal unless $\omega = 2$.
- Can we do it with polynomial arithmetic? $\rightarrow$ Hope for asymptotically optimal algorithms.

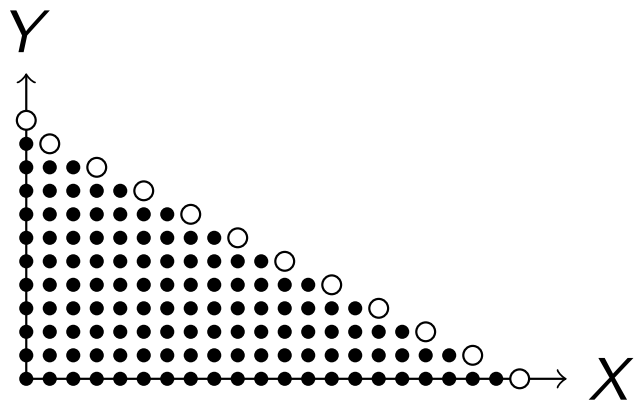
Easier problem

Given a Gröbner basis G, can we reduce P modulo G faster?

Main result

If G is sufficiently regular, a quasi-optimal algorithm exists modulo precomputation.

Polynomial reduction: complexity



- $I := \langle A, B \rangle$: $O(n^2)$ coefficients.
- $\mathbb{K}[X, Y]/I$: dimension $O(n^2)$.
- G: $O(n^3)$ coefficients ($O(n^2)$ for each G_i).

Reduction using G needs at least $O(n^3)$ $\Longrightarrow$ reduction with less information?

Outline

1. Vanilla Gröbner bases
   - Definition
   - Terse representation
2. Polynomial reduction
   - Idea of the algorithm
   - Applications

Outline

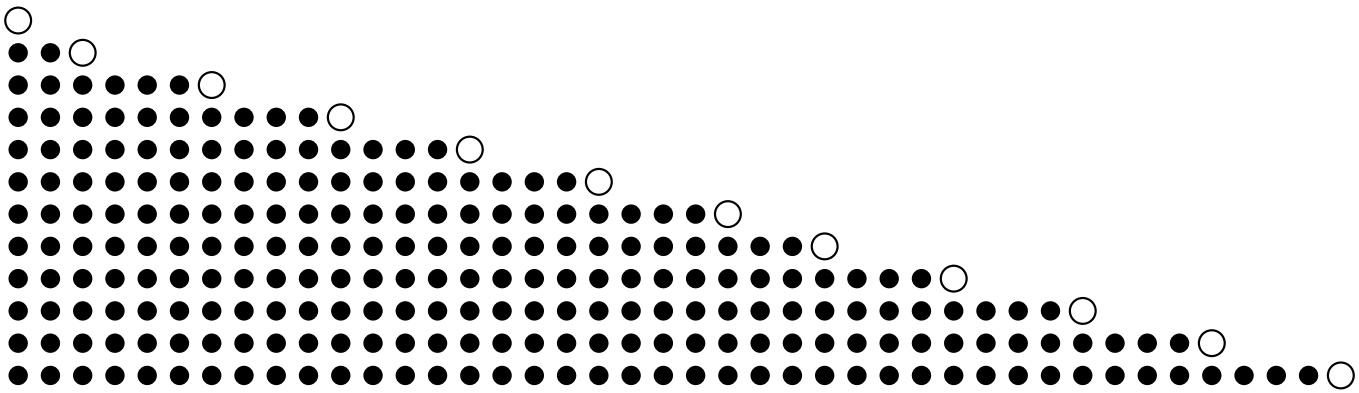
1. Vanilla Gröbner bases
   - Definition
   - Terse representation
2. Polynomial reduction

Definition

We consider the term orders $\prec_k$ ($k \in \mathbb{N}^*$) as the weighted-degree lexicographic order with weights $(X : 1, Y : k)$.

Vanilla Gröbner stairs

The monomials below the stairs are the minimal elements with respect to $\prec_k$



Example for $k = 4$ and an ideal I of degree $D = 237$

Definition (2)

Retractive property

let $I := \{0, 1, n\}$. The retractive property means that for any $i \leqslant n$ we have a linear combination

$$G_i = \sum_{j \in I} C_{i,j} \; G_j \qquad .$$

Definition (2)

Retractive property

For $\ell \in \mathbb{N}^*$, let $I_\ell := \{0, 1, n\} \cup \ell\mathbb{N} \cap (0, n)$. The retractive property means that for any $i, \ell \leqslant n$ we have a linear combination

$$G_i = \sum_{j \in I_\ell} C_{i,j,\ell} G_j \text{ with } \deg_k C_{i,j,\ell} = O(kl).$$

Definition (2)

Retractive property

For $\ell \in \mathbb{N}^*$, let $I_\ell := \{0, 1, n\} \cup \ell\mathbb{N} \cap (0, n)$. The retractive property means that for any $i, \ell \leqslant n$ we have a linear combination

$$G_i = \sum_{j \in I_\ell} C_{i,j,\ell} G_j \text{ with } \deg_k C_{i,j,\ell} = O(kl).$$

More precisely, $\deg_k C_{i,j,\ell} < k(2\ell - 1)$.

Definition (2)

Retractive property

For $\ell \in \mathbb{N}^*$, let $I_\ell := \{0, 1, n\} \cup \ell\mathbb{N} \cap (0, n)$. The retractive property means that for any $i, \ell \leqslant n$ we have a linear combination

$$G_i = \sum_{j \in I_\ell} C_{i,j,\ell} G_j \text{ with } \deg_k C_{i,j,\ell} = O(kl).$$

More precisely, $\deg_k C_{i,j,\ell} < k(2\ell - 1)$.

A Gröbner basis for the k-order is vanilla if it is a vanilla Gröbner stairs and has the retractive property.

Conjecture: vanilla Gröbner bases are generic

Experimentally, for generators chosen at random, and for various term orders, the Gröbner basis is vanilla.

Terse representation

G_0, G_1, G_n and well-chosen retraction coefficients hold all information (in space $\tilde{O}(n^2)$) and allow to retrieve G fast.

The coefficients of each G_i are needed to compute the reduction, but there are too many.

Terse representation

G_0, G_1, G_n and well-chosen retraction coefficients hold all information (in space $\tilde{O}(n^2)$) and allow to retrieve G fast.

The coefficients of each G_i are needed to compute the reduction, but there are too many.

$\Longrightarrow$ Keep only enough coefficients to evaluate Q_i.

Terse representation

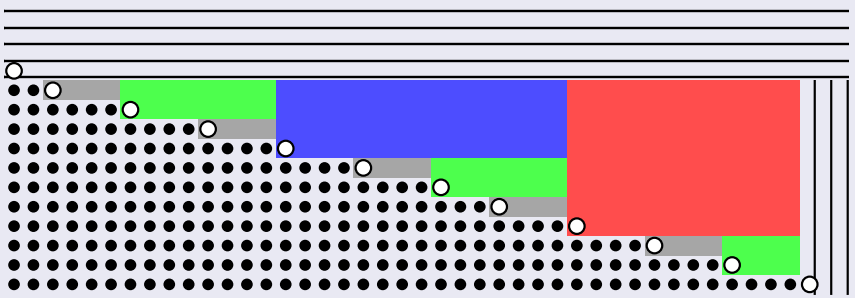
G_0, G_1, G_n and well-chosen retraction coefficients hold all information (in space $\tilde{O}(n^2)$) and allow to retrieve G fast.

The coefficients of each G_i are needed to compute the reduction, but there are too many.

$\Longrightarrow$ Keep only enough coefficients to evaluate Q_i.

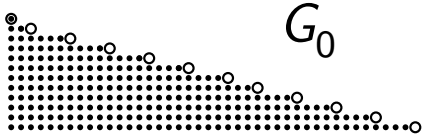
$\Longrightarrow$ Control the degree of the quotients.

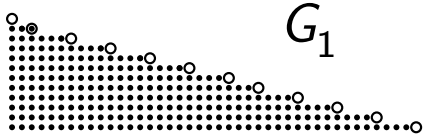
Dichotomic selection strategy

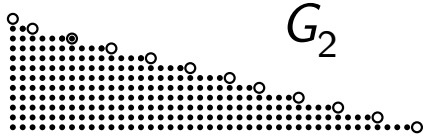


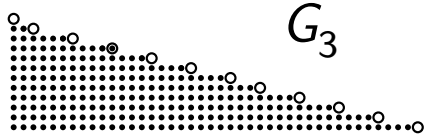
- $n/2$ quotients of degree d.
- $n/4$ quotients of degree $2d$.
- $n/8$ quotients of degree $4d$.
- ...

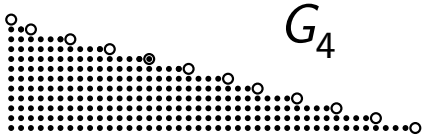
Terse representation – Example

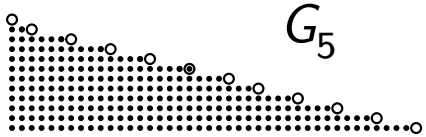


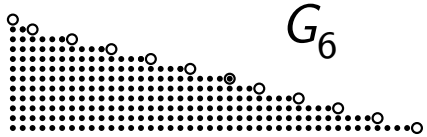


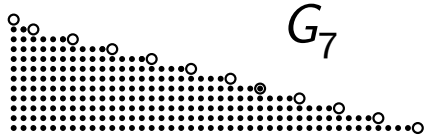


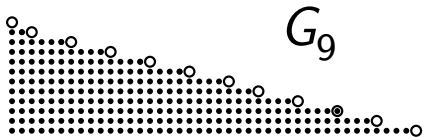


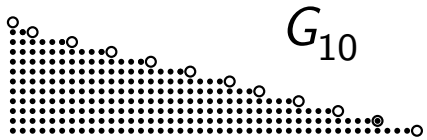


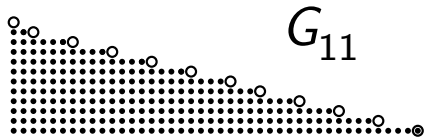




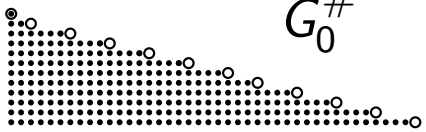


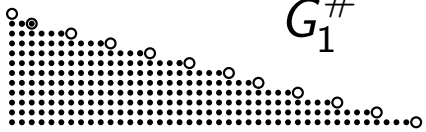


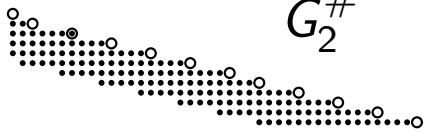




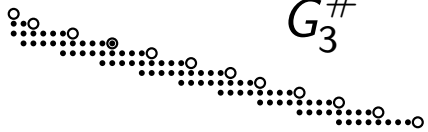
Terse representation – Example



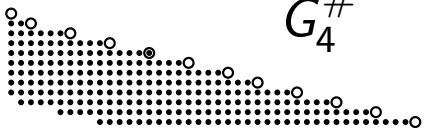




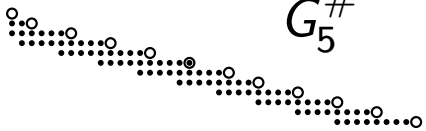
+ the linear combination
$G_2 = f_2(G_i, i \in \{0, 1, 4, 8, 11\})$
(5 polynomials of degree 27)



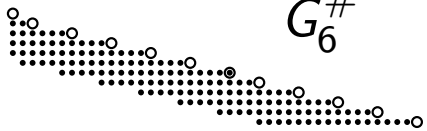
+ the linear combination
$G_3 = f_3(G_i, i \in \{0, 1, 2, 4, 6, 8, 10, 11\})$
(8 polynomials of degree 11)



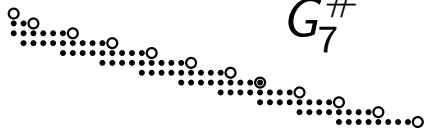
+ the linear combination
$G_4 = f_4(G_i, i \in \{0, 1, 8, 11\})$
(4 polynomials of degree 59)



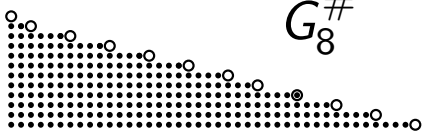
+ the linear combination
$G_5 = f_5(G_i, i \in \{0, 1, 2, 4, 6, 8, 10, 11\})$
(8 polynomials of degree 11)



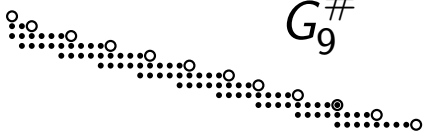
+ the linear combination
$G_6 = f_6(G_i, i \in \{0, 1, 4, 8, 11\})$
(5 polynomials of degree 27)



+ the linear combination
$G_7 = f_7(G_i, i \in \{0, 1, 2, 4, 6, 8, 10, 11\})$
(8 polynomials of degree 11)

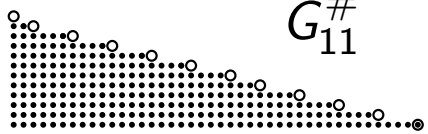


+ the linear combination
$G_8 = f_8(G_i, i \in \{0, 1, 11\})$
(3 polynomials of degree 123)



+ the linear combination
$G_9 = f_9(G_i, i \in \{0, 1, 2, 4, 6, 8, 10, 11\})$
(8 polynomials of degree 11)

+ the linear combination
$G_{10} = f_{10}(G_i, i \in \{0, 1, 4, 8, 11\})$
(5 polynomials of degree 27)



Outline

1. Vanilla Gröbner bases
2. Polynomial reduction
   - Idea of the algorithm
   - Applications

Idea of the algorithm

Theorem (van der Hoeven – ACA 2015)

Using relaxed multiplications, the extended reduction of P modulo G can be computed in quasi-linear time for the size of the equation

$$P = \sum_i Q_i G_i + R.$$

But this equation has size $O(n^3)$ and we would like to achieve $\tilde{O}(n^2)$.

Idea of the algorithm

Theorem (van der Hoeven – ACA 2015)

Using relaxed multiplications, the extended reduction of P modulo G can be computed in quasi-linear time for the size of the equation

$$P = \sum_i Q_i G_i + R.$$

But this equation has size $O(n^3)$ and we would like to achieve $\tilde{O}(n^2)$.

Adapt the algorithm to take advantage of the terse representation:

- Use the truncated elements $G_i^{\#}$ instead ($\tilde{O}(n^2)$ coefficients).
- Then, use the retraction coefficients to compute the remainder.

Applications – multiplication in the quotient algebra

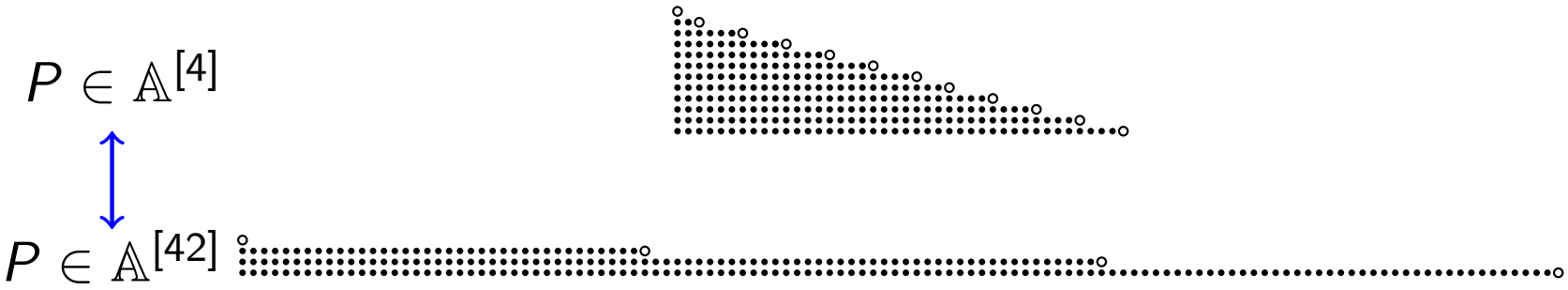
Given $P, Q \in \mathbb{A} := \mathbb{K}[X, Y]/I$, compute $PQ \in \mathbb{A}$ in normal form.
Assume that:

- The Gröbner basis G of I for some term order is vanilla.
- Its terse representation has been precomputed.
- P and Q are given in normal form with respect to G.

Theorem

Multiplication in $\mathbb{A}$ can be computed in time $\tilde{O}(\dim \mathbb{A})$.

Applications – conversion between representation



Perform a Gröbner walk

$$\mathbb{A}^{[4]} \longleftrightarrow \mathbb{A}^{[8]} \longleftrightarrow \mathbb{A}^{[16]} \longleftrightarrow \mathbb{A}^{[32]} \longleftrightarrow \mathbb{A}^{[42]}$$

(assuming these terse representations have been precomputed).

Theorem

The change of representation can be done in time $\tilde{O}(\dim \mathbb{A})$.

Conclusion

Main result

Under regularity assumptions, the extended reduction of P modulo a Gröbner basis G can be computed in quasi-linear time (with respect to the size of P and the dimension of the quotient algebra).

Proof-of-concept implementation (in Sage) at
`https://www.lix.polytechnique.fr/~larrieu/`

- Mainly intended as correctness proof.
- Missing (fast) implementation of some primitives $\Longrightarrow$ does not achieve quasi-optimal complexity.
- For the same reason (+ very expensive precomputation), it is not competitive in practice.

Future work

Generalization:

- More general term orders ?
- Slightly degenerate cases ?
- More than 2 variables ?

Future work

Generalization:

- More general term orders ? $\rightarrow$ start with $\prec_k, k \in \mathbb{Q}$.
- Slightly degenerate cases ? $\rightarrow$ seems feasible.
- More than 2 variables ? $\rightarrow$ seems feasible but very technical.

Future work

Generalization:

- More general term orders ? $\rightarrow$ start with $\prec_k, k \in \mathbb{Q}$.
- Slightly degenerate cases ? $\rightarrow$ seems feasible.
- More than 2 variables ? $\rightarrow$ seems feasible but very technical.

Helpful for Gröbner basis computation?

- In a very specific setting, yes $\rightarrow$ see my poster.
- In general, no idea (but maybe you have some).

Future work

Generalization:

- More general term orders ? $\rightarrow$ start with $\prec_k, k \in \mathbb{Q}$.
- Slightly degenerate cases ? $\rightarrow$ seems feasible.
- More than 2 variables ? $\rightarrow$ seems feasible but very technical.

Helpful for Gröbner basis computation?

- In a very specific setting, yes $\rightarrow$ see my poster.
- In general, no idea (but maybe you have some).

Thank you for your attention