The Gröbner Walk

Francesco Nowell

TU Berlin

19.06.2025

What is a Gröbner basis?

Motivation

Task: Given polynomials f, g determine whether g divides f.

Motivation

Task: Given polynomials f, g determine whether g divides f.

Idea: Compute the unique polynomials h, r such that

$$f = gh + r$$

with the division algorithm , and check if $r = 0$.

Motivation

Task: Given polynomials f, g determine whether g divides f.

Idea: Compute the unique polynomials h, r such that

$$f = gh + r$$

with the division algorithm , and check if $r = 0$.

$$\begin{array}{rrrr|l}
3x^3 & -x^2 & +x & -2 & x^2 - x + 1 \\ \cline{5-5}
-3x^3 & +3x^2 & -3x & & 3x + 2 \\ \cline{1-3}
 & 2x^2 & -2x & -2 & \\
 & -2x^2 & +2x & -2 & \\ \cline{2-4}
 & & & -4 &
\end{array}$$

Motivation

Task: Given polynomials f, g determine whether g divides f.

Idea: Compute the unique polynomials h, r such that

$$f = gh + r$$

with the division algorithm , and check if $r = 0$.

$$\begin{array}{rrrr|l} 3x^3 & -x^2 & +x & -2 & x^2 - x + 1 \\ \cline{5-5} -3x^3 & +3x^2 & -3x & & 3x + 2 \\ \cline{1-3} & 2x^2 & -2x & -2 & \\ & -2x^2 & +2x & -2 & \\ \cline{2-4} & & & -4 & \end{array}$$

We want to do this for multivariate polynomials!

Motivation

Task: Given polynomials f and $g_1, g_2, \dots g_s \in \mathbb{Q}[x_1, \dots x_n]$, compute polynomials $h_1, \dots h_s$ and r such that

$$f = h_1 g_1 + \cdots + h_s g_s + r$$

Motivation

Task: Given polynomials f and $g_1, g_2, \dots g_s \in \mathbb{Q}[x_1, \dots x_n]$, compute polynomials $h_1, \dots h_s$ and r such that

$$f = h_1 g_1 + \cdots + h_s g_s + r$$

Idea: Multivariate polynomial division!

Motivation

Task: Given polynomials f and $g_1, g_2, \dots g_s \in \mathbb{Q}[x_1, \dots x_n]$, compute polynomials $h_1, \dots h_s$ and r such that

$$f = h_1 g_1 + \cdots + h_s g_s + r$$

Idea: Multivariate polynomial division!

```
Input : f_1, ..., f_s, f
Output : q_1, ..., q_s, r

q_1 := 0; ...; q_s := 0; r := 0
p := f
WHILE p ≠ 0 DO
        i := 1
        divisionoccurred := false
        WHILE i ≤ s AND divisionoccurred = false DO
            IF LT(f_i) divides LT(p) THEN
                    q_i := q_i + LT(p)/LT(f_i)
                    p := p − (LT(p)/LT(f_i))f_i
                    divisionoccurred := true
            ELSE
                    i := i + 1
        IF divisionoccurred = false THEN
            r := r + LT(p)
            p := p − LT(p)
RETURN q_1, ..., q_s, r
```

Problems:

1) What is the leading term of $x+y$?
2) When are $h_1, \dots h_s$ and r unique?

For 1: Monomial orderings
For 2: Gröbner bases!

Ideals and Gröbner bases

Let $R := \mathbb{Q}[x_1, \dots x_n]$. The *Ideal* generated by $f_1, ..., f_r \in R$ is

$$I := \langle f_1, \dots f_r \rangle := \{\sum_{i=1}^{r} h_i f_i \text{ , where } h_i \in R\} \subset R.$$

Ideals and Gröbner bases

Let $R := \mathbb{Q}[x_1, \dots x_n]$. The *Ideal* generated by $f_1, ..., f_r \in R$ is

$$I := \langle f_1, \dots f_r \rangle := \{\sum_{i=1}^{r} h_i f_i \ , \text{ where } h_i \in R\} \subset R.$$

Generating sets of ideals are not unique! e.g $\langle xy + y, x \rangle = \langle x, y \rangle$.

Ideals and Gröbner bases

Let $R := \mathbb{Q}[x_1, \dots x_n]$. The *Ideal* generated by $f_1, ..., f_r \in R$ is

$$I := \langle f_1, \dots f_r \rangle := \{\sum_{i=1}^{r} h_i f_i \ , \text{ where } h_i \in R\} \subset R.$$

Generating sets of ideals are not unique! e.g $\langle xy + y, x \rangle = \langle x, y \rangle$.
Let $\prec$ be a monomial ordering.
Denote by $in_{\prec}(f)$ the *leading term* of $f \in R \setminus 0$ w.r.t. $\prec$.

$$\text{E.g: } in_{x \succ y}(xy + y^2) = xy \quad , \quad in_{y \succ x}(xy + y^2) = y^2$$

Ideals and Gröbner bases

Let $R := \mathbb{Q}[x_1, \dots x_n]$. The *Ideal* generated by $f_1, ..., f_r \in R$ is

$$I := \langle f_1, \dots f_r \rangle := \{\sum_{i=1}^{r} h_i f_i \ , \text{ where } h_i \in R\} \subset R.$$

Generating sets of ideals are not unique! e.g $\langle xy + y, x \rangle = \langle x, y \rangle$.
Let $\prec$ be a monomial ordering.
Denote by $in_\prec(f)$ the *leading term* of $f \in R \setminus 0$ w.r.t. $\prec$.

$$\text{E.g: } in_{x \succ y}(xy + y^2) = xy \quad , \quad in_{y \succ x}(xy + y^2) = y^2$$

The *initial ideal* of I w.r.t.$\prec$ is

$$in_\prec(I) := \langle in_\prec(f) \ , \text{ where } f \in I \rangle.$$

Ideals and Gröbner bases

Let $R := \mathbb{Q}[x_1, \dots x_n]$. The *Ideal* generated by $f_1, ..., f_r \in R$ is

$$I := \langle f_1, \dots f_r \rangle := \{\sum_{i=1}^{r} h_i f_i \ , \text{ where } h_i \in R\} \subset R.$$

Generating sets of ideals are not unique! e.g $\langle xy + y, x \rangle = \langle x, y \rangle$.
Let $\prec$ be a monomial ordering.
Denote by $in_{\prec}(f)$ the *leading term* of $f \in R \setminus 0$ w.r.t. $\prec$.

$$\text{E.g: } in_{x \succ y}(xy + y^2) = xy \quad , \quad in_{y \succ x}(xy + y^2) = y^2$$

The *initial ideal* of I w.r.t. $\prec$ is

$$in_{\prec}(I) := \langle in_{\prec}(f) \ , \text{ where } f \in I \rangle.$$

A generating set $g_1, \dots g_s$ of I is a *Gröbner basis* w.r.t. $\prec$ if

$$\langle in_{\prec}(g_1), \dots in_{\prec}(g_s) \rangle = in_{\prec}(I).$$

Ideals and Gröbner bases

Example

Let $f_1 = xy + y^2$ and $f_2 = x$. With respect to the *lexicographic ordering* $x \succ y$, these polynomials do not form a Gröbner basis of $I = \langle f_1, f_2 \rangle$:

$$f_1 - yf_2 = y^2 \in I \quad \text{but} \quad in_{\prec}(f_1 - yf_2) = y^2 \notin \langle x, xy \rangle = \langle in_{\prec}(f_1), in_{\prec}(f_2) \rangle.$$

A lexicographic Gröbner basis of this ideal is given by $\{x, y^2\}$.

Ideals and Gröbner bases

Example

Let $f_1 = xy + y^2$ and $f_2 = x$. With respect to the *lexicographic ordering* $x \succ y$, these polynomials do not form a Gröbner basis of $I = \langle f_1, f_2 \rangle$:

$$f_1 - yf_2 = y^2 \in I \quad \text{but} \quad in_{\prec}(f_1 - yf_2) = y^2 \notin \langle x, xy \rangle = \langle in_{\prec}(f_1), in_{\prec}(f_2) \rangle.$$

A lexicographic Gröbner basis of this ideal is given by $\{x, y^2\}$.

Gröbner bases solve the ideal membership problem!

$$f \in \langle g_1, \dots g_s \rangle \iff \text{dividing } f \text{ by } g_1, \dots g_s \text{ gives remainder zero.}$$

Ideals and Gröbner bases

Example

Let $f_1 = xy + y^2$ and $f_2 = x$. With respect to the *lexicographic ordering* $x \succ y$, these polynomials do not form a Gröbner basis of $I = \langle f_1, f_2 \rangle$:

$$f_1 - yf_2 = y^2 \in I \quad \text{but} \quad in_{\prec}(f_1 - yf_2) = y^2 \notin \langle x, xy \rangle = \langle in_{\prec}(f_1), in_{\prec}(f_2) \rangle.$$

A lexicographic Gröbner basis of this ideal is given by $\{x, y^2\}$.

Gröbner bases solve the ideal membership problem!

$$f \in \langle g_1, \dots g_s \rangle \iff \text{dividing } f \text{ by } g_1, \dots g_s \text{ gives remainder zero.}$$

Also, they can be used to ...
- Solve systems of polynomial equations
- Compute implicit representations of parametric surfaces
- Do integer programming

Ideals and Gröbner bases

Applications include ..
- Numerical Analysis
- Mathematical Physics
- Statistics
- PDEs
- Robotics...

Ideals and Gröbner bases

Applications include ..
- Numerical Analysis
- Mathematical Physics
- Statistics
- PDEs
- Robotics...

However: They can take a VERY long time to compute.

Ideals and Gröbner bases

Applications include ..
- Numerical Analysis
- Mathematical Physics
- Statistics
- PDEs
- Robotics...

However: They can take a VERY long time to compute.

This is especially true for Gröbner bases with respect to lexicographic orderings! For example: computing a degree reverse lexicographic Gröbner basis of

$$I = \langle 6 + 3x^3 + 16x^2z + 14x^2y^3 \ , \ 6 + y^3z + 17x^2z^2 + 7xy^2z^2 + 13x^3z^2 \rangle$$

using the default `groebner_basis` function in OSCAR is immediate. Computing a *lexicographic* basis of the same ideal does not terminate.

The Gröbner Walk

Cones, Fans and Ideals

Idea: Incremental approach to Gröbner basis computation, based on polyhedral geometry.

Cones, Fans and Ideals

Idea: Incremental approach to Gröbner basis computation, based on polyhedral geometry.

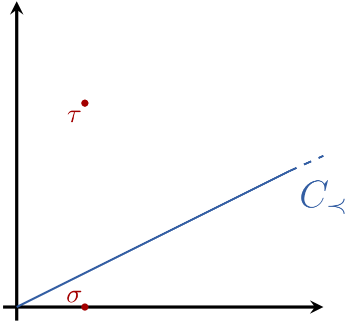
Let I be a fixed ideal in $\mathbb{Q}[x_1, \dots x_n]$. Each Gröbner basis $G_\prec = \{g_1, \dots g_s\}$ of I is associated to a polyhedral cone $C_\prec \subset \mathbb{R}^n$.

$$\left\{ \begin{array}{c} \text{Initial ideals} \\ in_\prec(I) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{marked Gröbner bases} \\ G_\prec \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Gröbner cones} \\ C_\prec \end{array} \right\}.$$

The cones form a **polyhedral fan**, called the *Gröbner Fan* of I.

The standard Gröbner walk

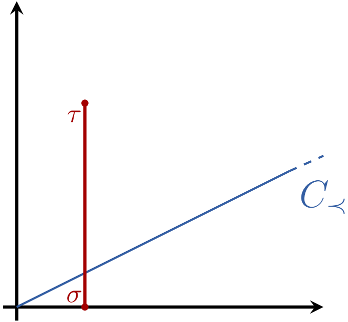
Task: Given a starting Gröbner basis $G_{\prec}$ and a target ordering $\prec'$, compute $G_{\prec'}$



Strategy: Starting from $C_{\prec}$, 'walk' to $C_{\prec'}$, computing every intermediate Gröbner basis along the way.

The standard Gröbner walk

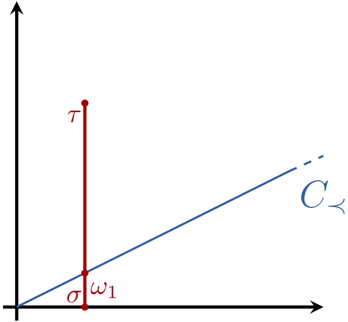
Task: Given a starting Gröbner basis $G_{\prec}$ and a target ordering $\prec'$, compute $G_{\prec'}$



Strategy: Starting from $C_{\prec}$, 'walk' to $C_{\prec'}$, computing every intermediate Gröbner basis along the way.

The standard Gröbner walk

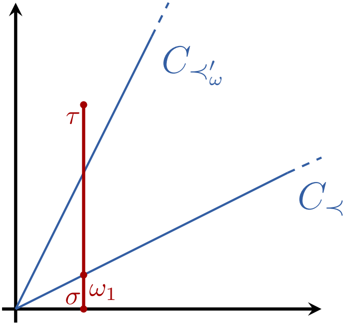
Task: Given a starting Gröbner basis $G_{\prec}$ and a target ordering $\prec'$, compute $G_{\prec'}$



Strategy: Starting from $C_{\prec}$, 'walk' to $C_{\prec'}$, computing every intermediate Gröbner basis along the way.

The standard Gröbner walk

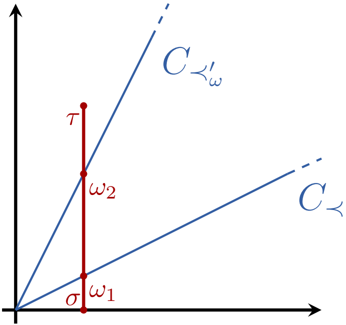
Task: Given a starting Gröbner basis $G_{\prec}$ and a target ordering $\prec'$, compute $G_{\prec'}$



Strategy: Starting from $C_{\prec}$, 'walk' to $C_{\prec'}$, computing every intermediate Gröbner basis along the way.

The standard Gröbner walk

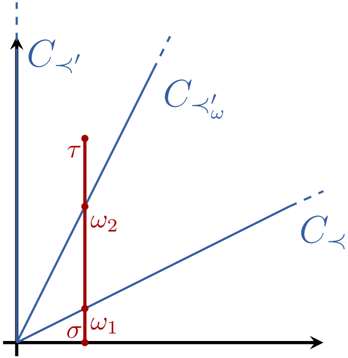
Task: Given a starting Gröbner basis $G_{\prec}$ and a target ordering $\prec'$, compute $G_{\prec'}$



Strategy: Starting from $C_{\prec}$, 'walk' to $C_{\prec'}$, computing every intermediate Gröbner basis along the way.

The standard Gröbner walk

Task: Given a starting Gröbner basis $G_{\prec}$ and a target ordering $\prec'$, compute $G_{\prec'}$



Strategy: Starting from $C_{\prec}$, 'walk' to $C_{\prec'}$, computing every intermediate Gröbner basis along the way.

My Contribution

From this...

Algorithm 1 StandardGroebnerWalk($G_{\prec}$, $A_{\prec}$, $A_{\prec'}$)

Input: $G_{\prec}$, $A_{\prec}$ and $A_{\prec'}$

Output: $G_{\prec'}$

$\sigma \leftarrow (A_{\prec})_{1,\cdot}$
$\tau \leftarrow (A_{\prec'})_{1,\cdot}$
done $\leftarrow$ "False"
while done = "False" **do**

  $\omega \leftarrow$ GetNextW($G_{\prec}$, σ, τ)
  $G' \leftarrow$ Lift($G_{\prec}$, ω, τ)
  $G' \leftarrow$ Reduce(G')

  if $\omega = \tau$ **then**
    done $\leftarrow$ "True"

  else
    $\sigma \leftarrow \omega$
    $G_{\prec} \leftarrow G'$
    $A_{\prec} \leftarrow A_{\prec'_{\omega}}$
  end if
end while
return G'

To this!

Oscar.jl / experimental / GroebnerWalk / src / common.jl

Code Blame 138 lines (110 loc) · 4.49 KB

````julia
    lex([x, y])

  ```
  """
  function groebner_walk(
    I::MPolyIdeal,
    target::MonomialOrdering = lex(base_ring(I)),
    start::MonomialOrdering = default_ordering(base_ring(I));
    algorithm::Symbol = :standard
  )
    if algorithm == :standard
      walk = (x) -> standard_walk(x, target)
    elseif algorithm == :generic
      walk = (x) -> generic_walk(x, start, target)
    else
      throw(NotImplementedError(:groebner_walk, algorithm))
    end

    Gb = groebner_basis(I; ordering=start, complete_reduction=true)
    Gb = walk(Gb)

    return Oscar.IdealGens(Gb, target; isGB=true)
  end

````
````

OSCAR demonstration

`fpnowell.github.io`