Lecture 2-13-1
Polynomial systems, computer algebra and applications

Gröbner bases and Buchberger's algorithm

Jean-Charles Faugère[1] Vincent Neiger[2] Mohab Safey El Din[2]

[1]Inria and CryptoNext Security

[2]Sorbonne University, CNRS

Warm-up

During the last course, we have introduced and studied:

- polynomial ideals and solution sets to polynomial systems over algebraically closed fields (algebraic varieties);

Warm-up

During the last course, we have introduced and studied:

- polynomial ideals and solution sets to polynomial systems over algebraically closed fields (algebraic varieties);
- topical algorithmic problems: rewriting into triangular systems, membership ideal problem (recall the weak Hilbert's Nullstellensatz), and many others;

Warm-up

During the last course, we have introduced and studied:

- polynomial ideals and solution sets to polynomial systems over algebraically closed fields (algebraic varieties);
- topical algorithmic problems: rewriting into triangular systems, membership ideal problem (recall the weak Hilbert's Nullstellensatz), and many others;
- notions of dimension and degree for algebraic sets;

Warm-up

During the last course, we have introduced and studied:

- polynomial ideals and solution sets to polynomial systems over algebraically closed fields (algebraic varieties);
- topical algorithmic problems: rewriting into triangular systems, membership ideal problem (recall the weak Hilbert's Nullstellensatz), and many others;
- notions of dimension and degree for algebraic sets;
- monomial orderings;

Warm-up

During the last course, we have introduced and studied:

- polynomial ideals and solution sets to polynomial systems over algebraically closed fields (algebraic varieties);
- topical algorithmic problems: rewriting into triangular systems, membership ideal problem (recall the weak Hilbert's Nullstellensatz), and many others;
- notions of dimension and degree for algebraic sets;
- monomial orderings;
- definition of Gröbner bases.

... all of this being motivated by important applications in engineering sciences and post-quantum cryptology

Warm-up

During the last course, we have introduced and studied:

- polynomial ideals and solution sets to polynomial systems over algebraically closed fields (algebraic varieties);
- topical algorithmic problems: rewriting into triangular systems, membership ideal problem (recall the weak Hilbert's Nullstellensatz), and many others;
- notions of dimension and degree for algebraic sets;
- monomial orderings;
- definition of Gröbner bases.

... all of this being motivated by important applications in engineering sciences and post-quantum cryptology

We need algorithms

Gröbner bases – Definition

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Definition

Let $I \subset R$ be an ideal. One says that $G \subset R$ is a Gröbner basis for $(I, \prec)$ if the following conditions hold:

- G is finite;
- $G \subset I$;
- $\langle \mathsf{LM}_{\prec}(g) \mid g \in G \rangle = \langle \mathsf{LM}(f) \mid f \in I \rangle$.

Gröbner bases – Definition

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Definition

Let $I \subset R$ be an ideal. One says that $G \subset R$ is a Gröbner basis for $(I, \prec)$ if the following conditions hold:

- G is finite;
- $G \subset I$;
- $\langle \mathsf{LM}_{\prec}(g) \mid g \in G \rangle = \langle \mathsf{LM}(f) \mid f \in I \rangle$.

Why is this definition so useful?

Gröbner bases – Definition

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Definition

Let $I \subset R$ be an ideal. One says that $G \subset R$ is a Gröbner basis for $(I, \prec)$ if the following conditions hold:

- G is finite;
- $G \subset I$;
- $\langle \mathsf{LM}_{\prec}(g) \mid g \in G \rangle = \langle \mathsf{LM}(f) \mid f \in I \rangle$.

Why is this definition so useful?

How to compute Gröbner bases?

Reductions of a polynomial modulo a polynomial family

Definitions, properties and algorithms

Reduction (division) notion

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Reduction (division) notion

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Consider f and $f_1, \ldots, f_s$ in R $\rightsquigarrow$ **Decide $f \in \langle f_1, \ldots, f_s \rangle$?**

We can try to mimick the Euclide's algorithm.

Reduction (division) notion

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Consider f and $f_1, \ldots, f_s$ in R $\rightsquigarrow$ **Decide $f \in \langle f_1, \ldots, f_s \rangle$?**

We can try to mimick the Euclide's algorithm.

$$f = q_1 f_1 + \cdots + q_s f_s + r \text{ such that } r, q_i \in R \text{ with}$$
$$\mathsf{LM}_\prec(r) \notin \langle \mathsf{LM}_\prec(f_1), \ldots, \mathsf{LM}_\prec(f_s) \rangle$$

Reduction (division) notion

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Consider f and $f_1, \ldots, f_s$ in R $\rightsquigarrow$ **Decide $f \in \langle f_1, \ldots, f_s \rangle$?**

We can try to mimick the Euclide's algorithm.

$f = q_1 f_1 + \cdots + q_s f_s + r$ such that $r, q_i \in R$ with

$$\mathsf{LM}_\prec(r) \notin \langle \mathsf{LM}_\prec(f_1), \ldots, \mathsf{LM}_\prec(f_s) \rangle$$

- note that $r = 0 \Longrightarrow f \in \langle f_1, \ldots, f_s \rangle$
- note that $f - r \in \langle f_1, \ldots, f_s \rangle$

A first example

Take $f = x_1x_2^3 + x_1^2x_2^2 + x_1^3$, $f_1 = x_1x_2$ and $f_2 = x_1^2 + x_2^2$

$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

A first example

Take $f = x_1x_2^3 + x_1^2x_2^2 + x_1^3$, $f_1 = x_1x_2$ and $f_2 = x_1^2 + x_2^2$

$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

☛ $r = f - (x_1x_2 + x_2^2)f_1 - x_1f_2 + x_2f_1 = 0$

A first example

Take $f = x_1 x_2^3 + x_1^2 x_2^2 + x_1^3$, $f_1 = x_1 x_2$ and $f_2 = x_1^2 + x_2^2$

$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2 x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1 x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

☛ $r = f - (x_1 x_2 + x_2^2) f_1 - x_1 f_2 + x_2 f_1 = 0$

But we could have done:

☛ $r = f - x_2^2 f_2 - x_2^2 f_1 = \boxed{-x_2^4} + x_1^3$

A first example

Take $f = x_1x_2^3 + x_1^2x_2^2 + x_1^3$, $f_1 = x_1x_2$ and $f_2 = x_1^2 + x_2^2$

$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

☛ $r = f - (x_1x_2 + x_2^2)f_1 - x_1f_2 + x_2f_1 = 0$

But we could have done:

☛ $r = f - x_2^2f_2 - x_2^2f_1 = \boxed{-x_2^4} + x_1^3$

- non canonical output
  (order of the computations)
- non fully reduced

A first example

Take $f = x_1x_2^3 + x_1^2x_2^2 + x_1^3$, $f_1 = x_1x_2$ and $f_2 = x_1^2 + x_2^2$

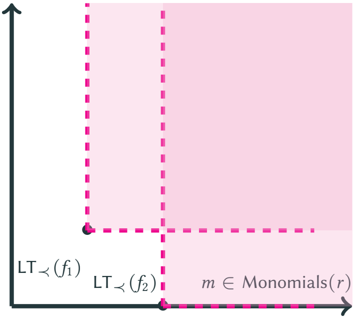
$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

☛ $r = f - (x_1x_2 + x_2^2)f_1 - x_1f_2 + x_2f_1 = 0$

But we could have done:

☛ $r = f - x_2^2f_2 - x_2^2f_1 = \boxed{-x_2^4} + x_1^3$

- non canonical output
  (order of the computations)
- non fully reduced



A first example

Take $f = x_1x_2^3 + x_1^2x_2^2 + x_1^3$, $f_1 = x_1x_2$ and $f_2 = x_1^2 + x_2^2$

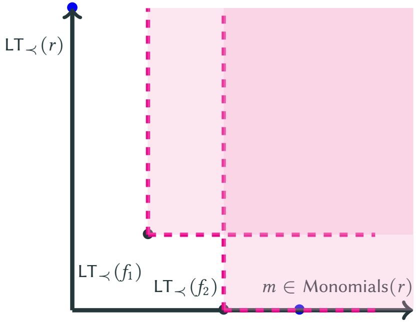
$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

☛ $r = f - (x_1x_2 + x_2^2)f_1 - x_1f_2 + x_2f_1 = 0$

But we could have done:

☛ $r = f - x_2^2f_2 - x_2^2f_1 = \boxed{-x_2^4} + x_1^3$

- non canonical output (order of the computations)
- non fully reduced



Full reduction

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Full reduction

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Consider f and $f_1, \ldots, f_s$ in R $\rightsquigarrow$ **Decide** $f \in \langle f_1, \ldots, f_s \rangle$**?**

For $g \in R$, denote by $\mathrm{Monomials}(g)$ the monomial support of g.

Full reduction

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Consider f and $f_1, \ldots, f_s$ in R $\rightsquigarrow$ **Decide $f \in \langle f_1, \ldots, f_s \rangle$?**

For $g \in R$, denote by $\mathrm{Monomials}(g)$ the monomial support of g.

$$f = q_1 f_1 + \cdots + q_s f_s + r \text{ such that } r, q_i \in R \text{ with}$$
$$\forall m \in \mathrm{Monomials}(r), \quad m \notin \langle \mathrm{LM}_\prec(f_1), \ldots, \mathrm{LM}_\prec(f_s) \rangle$$

Full reduction

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Consider f and $f_1, \ldots, f_s$ in R $\rightsquigarrow$ **Decide $f \in \langle f_1, \ldots, f_s \rangle$?**

For $g \in R$, denote by $\mathrm{Monomials}(g)$ the monomial support of g.

$$f = q_1 f_1 + \cdots + q_s f_s + r \text{ such that } r, q_i \in R \text{ with}$$
$$\forall m \in \mathsf{Monomials}(r), \quad m \notin \langle \mathsf{LM}_\prec(f_1), \ldots, \mathsf{LM}_\prec(f_s) \rangle$$

- note that $r = 0 \Longrightarrow f \in \langle f_1, \ldots, f_s \rangle$
- note that $f - r \in \langle f_1, \ldots, f_s \rangle$

Example (I)

Take $f = x_1x_2^3 + x_1^2x_2^2 + x_1^3$, $f_1 = x_1x_2$ and $f_2 = x_1^2 + x_2^2$

$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

☛ $r = f - x_2^2f_2 - x_2^2f_1 = \boxed{-x_2^4} + x_1^3$

Example (I)

Take $f = x_1x_2^3 + x_1^2x_2^2 + x_1^3$, $f_1 = x_1x_2$ and $f_2 = x_1^2 + x_2^2$

$\boxed{\mathsf{LM}_{grevlex}(f) = x_1^2x_2^2}$ $\boxed{\mathsf{LM}_{grevlex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{grevlex}(f_2) = x_1^2}$

☛ $r = f - x_2^2f_2 - x_2^2f_1 = \boxed{-x_2^4} + x_1^3$

Pushing further the reduction, we obtain

☛ $r = f - x_2^2f_2 - x_2^2f_1\boxed{-x_1f_2 + x_2f_1} = \boxed{-x_2^4}$

Example (II)

Take $f = x_1x_2^2 + 1$, $f_1 = x_1x_2 + 1$ and $f_2 = x_2 + 1$.

$\boxed{\mathsf{LM}_{lex}(f) = x_1x_2^2}$ $\boxed{\mathsf{LM}_{lex}(f_1) = x_1x_2}$ $\boxed{\mathsf{LM}_{lex}(f_2) = x_2}$

➟ $f - x_2f_1 + f_2 = 2$

Note that we can deduce that $\langle f, f_1, f_2 \rangle = \langle 1 \rangle$

Example (III)

Take $f = x_1^2 x_2 + x_1 x_2^2 + x_2^2$, $f_1 = x_1 x_2 + 1$ and $f_2 = x_2^2 - 1$.

$\boxed{\mathsf{LM}_{lex}(f) = x_1^2 x_2}$ $\boxed{\mathsf{LM}_{lex}(f_1) = x_1 x_2}$ $\boxed{\mathsf{LM}_{lex}(f_2) = x_2^2}$

Example (III)

Take $f = x_1^2 x_2 + x_1 x_2^2 + x_2^2$, $f_1 = x_1 x_2 + 1$ and $f_2 = x_2^2 - 1$.

$\boxed{\mathsf{LM}_{lex}(f) = x_1^2 x_2}$ $\boxed{\mathsf{LM}_{lex}(f_1) = x_1 x_2}$ $\boxed{\mathsf{LM}_{lex}(f_2) = x_2^2}$

$$r_1 = f - (x_1 + x_2) f_1 = x_1 + x_2^2 + x_2.$$

Example (III)

Take $f = x_1^2 x_2 + x_1 x_2^2 + x_2^2$, $f_1 = x_1 x_2 + 1$ and $f_2 = x_2^2 - 1$.

$\boxed{\mathsf{LM}_{lex}(f) = x_1^2 x_2}$ $\boxed{\mathsf{LM}_{lex}(f_1) = x_1 x_2}$ $\boxed{\mathsf{LM}_{lex}(f_2) = x_2^2}$

$r_1 = f - (x_1 + x_2) f_1 = x_1 + x_2^2 + x_2$.

$r = r_1 - f_2 = x_1 + x_2 + 1$.

Reduction algorithm REDUCTION

INPUT:
- $f, f_1, \ldots, f_s$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: $r \in R$ such that $\mathsf{LT}_\prec(r) \notin \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

Reduction algorithm Reduction

Input:
- $f, f_1, \ldots, f_s$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that $\mathsf{LT}_\prec(r) \notin \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

1. If $f = 0$ then return f
2. $r \leftarrow f$

Reduction algorithm Reduction

Input:
- $f, f_1, \ldots, f_s$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that $\mathsf{LT}_\prec(r) \notin \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s)\rangle$ and $f - r \in \langle f_1, \ldots, f_s\rangle$

1. If $f = 0$ then return f
2. $r \leftarrow f$
3. boo $\leftarrow$ `true`
4. while boo $=$ `true`

    4.1 boo $\leftarrow$ `false`
    4.2 for $1 \leq i \leq s$ do

        4.2.1 if $\mathsf{LM}_\prec(f_i)$ divides $\mathsf{LM}_\prec(r)$ then
        - $r \leftarrow r - \frac{\mathsf{LT}_\prec(r)}{\mathsf{LT}_\prec(f_i)} f_i$
        - boo $\leftarrow$ `true`

Reduction algorithm Reduction

INPUT:
- $f, f_1, \ldots, f_s$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: $r \in R$ such that $\mathsf{LT}_\prec(r) \notin \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s)\rangle$ and $f - r \in \langle f_1, \ldots, f_s\rangle$

1. If $f = 0$ then return f
2. $r \leftarrow f$
3. boo $\leftarrow$ `true`
4. while boo $=$ `true`

   4.1 boo $\leftarrow$ `false`
   4.2 for $1 \leq i \leq s$ do

      4.2.1 if $\mathsf{LM}_\prec(f_i)$ divides $\mathsf{LM}_\prec(r)$ then
      - $r \leftarrow r - \frac{\mathsf{LT}_\prec(r)}{\mathsf{LT}_\prec(f_i)} f_i$
      - boo $\leftarrow$ `true`

5. return r

Reduction algorithm REDUCTION

INPUT:
- $f, f_1, \ldots, f_s$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: $r \in R$ such that $\mathsf{LT}_\prec(r) \notin \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

1. If $f = 0$ then return f
2. $r \leftarrow f$
3. boo $\leftarrow$ `true`
4. while boo $=$ `true`

   4.1 boo $\leftarrow$ `false`
   4.2 for $1 \leq i \leq s$ do

   4.2.1 if $\mathsf{LM}_\prec(f_i)$ divides $\mathsf{LM}_\prec(r)$ then
   - $r \leftarrow r - \frac{\mathsf{LT}_\prec(r)}{\mathsf{LT}_\prec(f_i)} f_i$
   - boo $\leftarrow$ `true`

5. return r

✓ **Termination**

☛ because $\prec$ is admissible

Reduction algorithm REDUCTION

INPUT:
- $f, f_1, \ldots, f_s$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: $r \in R$ such that $\mathrm{LT}_\prec(r) \notin \langle \mathrm{LT}_\prec(f_1), \ldots, \mathrm{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

1. If $f = 0$ then return f
2. $r \leftarrow f$
3. boo $\leftarrow$ `true`
4. while boo $=$ `true`
   - 4.1 boo $\leftarrow$ `false`
   - 4.2 for $1 \leq i \leq s$ do
     - 4.2.1 if $\mathrm{LM}_\prec(f_i)$ divides $\mathrm{LM}_\prec(r)$ then
       - $r \leftarrow r - \frac{\mathrm{LT}_\prec(r)}{\mathrm{LT}_\prec(f_i)} f_i$
       - boo $\leftarrow$ `true`
5. return r

✓ **Termination**

☛ because $\prec$ is admissible

✓ **Correction**

☛ loop invariant

Reduction algorithm

We reuse the above notation.

There exist $(g_1, \ldots, g_k) \subset \{f_1, \ldots, f_s\}^k$ and monomials $m_1, \ldots, m_k$ such that

- $f - r = m_1 g_1 + \cdots + m_k g_k$
- $\mathsf{LM}_\prec(m_k g_k) \prec \mathsf{LM}_\prec(m_{k-1} g_{k-1}) \prec \cdots \prec \mathsf{LM}_\prec(m_1 g_1) \preceq \mathsf{LM}_\prec(f)$

Reduction algorithm

We reuse the above notation.

There exist $(g_1, \dots, g_k) \subset \{f_1, \dots, f_s\}^k$ and monomials $m_1, \dots, m_k$ such that

- $f - r = m_1 g_1 + \cdots + m_k g_k$
- $\mathsf{LM}_{\prec}(m_k g_k) \prec \mathsf{LM}_{\prec}(m_{k-1} g_{k-1}) \prec \cdots \prec \mathsf{LM}_{\prec}(m_1 g_1) \preceq \mathsf{LM}_{\prec}(f)$

The map $f \mapsto \textsc{Reduction}(f, [f_1, \dots, f_s])$ is linear and its kernel lies in $\langle f_1, \dots, f_s \rangle$.

Reduction algorithm

We reuse the above notation.

There exist $(g_1, \ldots, g_k) \subset \{f_1, \ldots, f_s\}^k$ and monomials $m_1, \ldots, m_k$ such that

- $f - r = m_1 g_1 + \cdots + m_k g_k$
- $\mathsf{LM}_\prec(m_k g_k) \prec \mathsf{LM}_\prec(m_{k-1} g_{k-1}) \prec \cdots \prec \mathsf{LM}_\prec(m_1 g_1) \preceq \mathsf{LM}_\prec(f)$

The map $f \mapsto \textsc{Reduction}(f, [f_1, \ldots, f_s])$ is linear and its kernel lies in $\langle f_1, \ldots, f_s \rangle$.

Consequence.

One can rephrase Reduction with linear algebra operations.

Reduction algorithm

We reuse the above notation.

There exist $(g_1, \dots, g_k) \subset \{f_1, \dots, f_s\}^k$ and monomials $m_1, \dots, m_k$ such that

- $f - r = m_1 g_1 + \cdots + m_k g_k$
- $\mathsf{LM}_\prec(m_k g_k) \prec \mathsf{LM}_\prec(m_{k-1} g_{k-1}) \prec \cdots \prec \mathsf{LM}_\prec(m_1 g_1) \preceq \mathsf{LM}_\prec(f)$

The map $f \mapsto \textsc{Reduction}(f, [f_1, \dots, f_s])$ is linear and its kernel lies in $\langle f_1, \dots, f_s \rangle$.

Consequence.

One can rephrase Reduction with linear algebra operations. Let us do it...

Full reduction algorithm FullReduction

Input:
- h and $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that for any $m \in \mathrm{Monomials}(r)$ $m \notin \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

Full reduction algorithm FullReduction

Input:
- h and $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that for any $m \in \mathrm{Monomials}(r)$ $m \notin \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

1. If $h = 0$ then return h
2. $r \leftarrow 0$
3. $g \leftarrow h$

Full reduction algorithm FullReduction

Input:
- h and $\boldsymbol{f} = (f_1, \dots, f_s)$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that for any $m \in \text{Monomials}(r)$ $m \notin \langle \mathsf{LT}_\prec(f_1), \dots, \mathsf{LT}_\prec(f_s)\rangle$ and $f - r \in \langle f_1, \dots, f_s\rangle$

1. If $h = 0$ then return h
2. $r \leftarrow 0$
3. $g \leftarrow h$
4. while $g \neq 0$

   4.1 $g \leftarrow \text{Reduction}(g, \boldsymbol{f}, \prec)$
   4.2 if $g \neq 0$
   - $r \leftarrow r + \mathsf{LT}_\prec(g)$
   - $g \leftarrow g - \mathsf{LT}_\prec(g)$

Full reduction algorithm FullReduction

Input:
- h and $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that for any $m \in \mathrm{Monomials}(r)$ $m \notin \langle \mathsf{LT}_{\prec}(f_1), \ldots, \mathsf{LT}_{\prec}(f_s)\rangle$ and $f - r \in \langle f_1, \ldots, f_s\rangle$

1. If $h = 0$ then return h
2. $r \leftarrow 0$
3. $g \leftarrow h$
4. while $g \neq 0$

    4.1 $g \leftarrow \textsc{Reduction}(g, \boldsymbol{f}, \prec)$
    4.2 if $g \neq 0$
    - $r \leftarrow r + \mathsf{LT}_{\prec}(g)$
    - $g \leftarrow g - \mathsf{LT}_{\prec}(g)$

5. return r

Full reduction algorithm FullReduction

Input:
- h and $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that for any $m \in \text{Monomials}(r)$ $m \notin \langle \text{LT}_\prec(f_1), \ldots, \text{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

1. If $h = 0$ then return h
2. $r \leftarrow 0$
3. $g \leftarrow h$
4. while $g \neq 0$

   4.1 $g \leftarrow \text{Reduction}(g, \boldsymbol{f}, \prec)$
   4.2 if $g \neq 0$
   - $r \leftarrow r + \text{LT}_\prec(g)$
   - $g \leftarrow g - \text{LT}_\prec(g)$
5. return r

✓ **Termination**

☛ because $\prec$ is admissible

Full reduction algorithm FullReduction

Input:
- h and $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

Output: $r \in R$ such that for any $m \in \text{Monomials}(r)$ $m \notin \langle \text{LT}_\prec(f_1), \ldots, \text{LT}_\prec(f_s) \rangle$ and $f - r \in \langle f_1, \ldots, f_s \rangle$

1. If $h = 0$ then return h
2. $r \leftarrow 0$
3. $g \leftarrow h$
4. while $g \neq 0$

   4.1 $g \leftarrow \text{Reduction}(g, \boldsymbol{f}, \prec)$

   4.2 if $g \neq 0$
   - $r \leftarrow r + \text{LT}_\prec(g)$
   - $g \leftarrow g - \text{LT}_\prec(g)$
5. return r

✓ **Termination**

☛ because $\prec$ is admissible

✓ **Correction**

☛ loop invariant

Full reduction algorithm

We reuse the above notation.

Let $r = \textsc{FullReduction}(f, \boldsymbol{f}, \prec)$.
Then $\mathsf{Monomials}(r) \cap \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle = \emptyset$.

Full reduction algorithm

We reuse the above notation.

Let $r = \textsc{FullReduction}(f, \boldsymbol{f}, \prec)$.
Then $\text{Monomials}(r) \cap \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle = \emptyset$.

The map $f \mapsto \textsc{FullReduction}(f, [f_1, \ldots, f_s])$ is linear and its kernel lies in $\langle f_1, \ldots, f_s \rangle$.

Full reduction algorithm

We reuse the above notation.

Let $r = \textsc{FullReduction}(f, \boldsymbol{f}, \prec)$.
Then $\text{Monomials}(r) \cap \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s)\rangle = \emptyset$.

The map $f \mapsto \textsc{FullReduction}(f, [f_1, \ldots, f_s])$ is linear and its kernel lies in $\langle f_1, \ldots, f_s \rangle$.

Consequence.
One can again rephrase Reduction with linear algebra operations.

Full reduction algorithm

We reuse the above notation.

Let $r = \textsc{FullReduction}(f, \boldsymbol{f}, \prec)$.
Then $\text{Monomials}(r) \cap \langle \mathsf{LT}_\prec(f_1), \ldots, \mathsf{LT}_\prec(f_s) \rangle = \emptyset$.

The map $f \mapsto \textsc{FullReduction}(f, [f_1, \ldots, f_s])$ is linear and its kernel lies in $\langle f_1, \ldots, f_s \rangle$.

Consequence.
One can again rephrase Reduction with linear algebra operations.

Let us do it and emphasize the difference...

Back to Hilbert's basis theorem

Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$.

Refined statement of Hilbert's basis theorem

Let $I \subset R$ be an ideal. There exists a finite set $g_1 \ldots, g_s$ in R such that

- $I = \langle g_1, \ldots, g_s \rangle$
- $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(f) \mid f \in I \rangle = \langle \mathsf{LM}_\prec(g_i) \mid 1 \leq i \leq s \rangle$

Back to Hilbert's basis theorem

Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$.

Refined statement of Hilbert's basis theorem

Let $I \subset R$ be an ideal. There exists a finite set $g_1 \ldots, g_s$ in R such that

- $I = \langle g_1, \ldots, g_s \rangle$
- $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(f) \mid f \in I \rangle = \langle \mathsf{LM}_\prec(g_i) \mid 1 \leq i \leq s \rangle$

Proof. Easy case is $I = \langle 0 \rangle$. We assume now $I \neq \langle 0 \rangle$.

Back to Hilbert's basis theorem

Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$.

Refined statement of Hilbert's basis theorem

Let $I \subset R$ be an ideal. There exists a finite set $g_1 \ldots, g_s$ in R such that

- $I = \langle g_1, \ldots, g_s \rangle$
- $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(f) \mid f \in I \rangle = \langle \mathsf{LM}_\prec(g_i) \mid 1 \leq i \leq s \rangle$

Proof. Easy case is $I = \langle 0 \rangle$. We assume now $I \neq \langle 0 \rangle$.

- Dickson's lemma $\Rightarrow$
  $\exists (g_1, \ldots, g_s) \subset I$ such that $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s) \rangle$

Back to Hilbert's basis theorem

Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$.

Refined statement of Hilbert's basis theorem

Let $I \subset R$ be an ideal. There exists a finite set $g_1 \ldots, g_s$ in R such that

- $I = \langle g_1, \ldots, g_s \rangle$
- $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(f) \mid f \in I \rangle = \langle \mathsf{LM}_\prec(g_i) \mid 1 \leq i \leq s \rangle$

Proof. Easy case is $I = \langle 0 \rangle$. We assume now $I \neq \langle 0 \rangle$.

- Dickson's lemma $\Rightarrow$
  $\exists (g_1, \ldots, g_s) \subset I$ such that $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s) \rangle$
- consider $r = \textsc{Reduction}(f, [g_1, \ldots, g_s], \prec)$ for some $f \in I$.

Back to Hilbert's basis theorem

Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$.

Refined statement of Hilbert's basis theorem

Let $I \subset R$ be an ideal. There exists a finite set $g_1 \ldots, g_s$ in R such that

- $I = \langle g_1, \ldots, g_s \rangle$
- $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(f) \mid f \in I \rangle = \langle \mathsf{LM}_\prec(g_i) \mid 1 \leq i \leq s \rangle$

Proof. Easy case is $I = \langle 0 \rangle$. We assume now $I \neq \langle 0 \rangle$.

- Dickson's lemma $\Rightarrow$
  $\exists (g_1, \ldots, g_s) \subset I$ such that $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s) \rangle$
- consider $r = \textsc{Reduction}(f, [g_1, \ldots, g_s], \prec)$ for some $f \in I$.
- $r = 0$ ✓else conclude that $\mathsf{LM}_\prec(r) \in \langle \mathsf{LM}_\prec(I) \rangle$ ✗contradiction

Back to Hilbert's basis theorem

Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$.

Refined statement of Hilbert's basis theorem

Let $I \subset R$ be an ideal. There exists a finite set $g_1 \ldots, g_s$ in R such that

- $I = \langle g_1, \ldots, g_s \rangle$
- $\mathsf{LM}_{\prec}(I) = \langle \mathsf{LM}_{\prec}(f) \mid f \in I \rangle = \langle \mathsf{LM}_{\prec}(g_i) \mid 1 \leq i \leq s \rangle$

Proof. Easy case is $I = \langle 0 \rangle$. We assume now $I \neq \langle 0 \rangle$.

- Dickson's lemma $\Rightarrow$
  $\exists (g_1, \ldots, g_s) \subset I$ such that $\mathsf{LM}_{\prec}(I) = \langle \mathsf{LM}_{\prec}(g_1), \ldots, \mathsf{LM}_{\prec}(g_s) \rangle$
- consider $r = \textsc{Reduction}(f, [g_1, \ldots, g_s], \prec)$ for some $f \in I$.
- $r = 0$ ✓else conclude that $\mathsf{LM}_{\prec}(r) \in \langle \mathsf{LM}_{\prec}(I) \rangle$ ✗contradiction

Good news. Gröbner bases do exist!

Back to Hilbert's basis theorem

Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$.

Refined statement of Hilbert's basis theorem

Let $I \subset R$ be an ideal. There exists a finite set $g_1 \ldots, g_s$ in R such that

- $I = \langle g_1, \ldots, g_s \rangle$
- $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(f) \mid f \in I \rangle = \langle \mathsf{LM}_\prec(g_i) \mid 1 \leq i \leq s \rangle$

Proof. Easy case is $I = \langle 0 \rangle$. We assume now $I \neq \langle 0 \rangle$.

- Dickson's lemma $\Rightarrow$
  $\exists (g_1, \ldots, g_s) \subset I$ such that $\mathsf{LM}_\prec(I) = \langle \mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s) \rangle$
- consider $r = \textsc{Reduction}(f, [g_1, \ldots, g_s], \prec)$ for some $f \in I$.
- $r = 0$ ✓else conclude that $\mathsf{LM}_\prec(r) \in \langle \mathsf{LM}_\prec(I) \rangle$ ✗contradiction

Good news. Gröbner bases do exist!

... but this proof is not constructive

Characterizations and first properties of Gröbner bases

Normal forms

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Let $I \subset R$ be an ideal and $G = (g_1, \ldots, g_s) \subset R$ be a Gröbner basis for $(I, \prec)$. Take $f \in R$. There exists a unique $r \in R$ such that:

Normal forms

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Let $I \subset R$ be an ideal and $G = (g_1, \ldots, g_s) \subset R$ be a Gröbner basis for $(I, \prec)$. Take $f \in R$. There exists a unique $r \in R$ such that:

- No term of r is divisible by any of $\mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s)$;
- There exists $g \in I$ such that $f = g + r$.

Normal forms

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Let $I \subset R$ be an ideal and $G = (g_1, \ldots, g_s) \subset R$ be a Gröbner basis for $(I, \prec)$. Take $f \in R$. There exists a unique $r \in R$ such that:

- No term of r is divisible by any of $\mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s)$;
- There exists $g \in I$ such that $f = g + r$.

Also, $r = \textsc{FullReduction}(f, G, \prec)$ (whatever the choice of ordering of the polynomials in G).

Normal forms

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Let $I \subset R$ be an ideal and $G = (g_1, \ldots, g_s) \subset R$ be a Gröbner basis for $(I, \prec)$. Take $f \in R$. There exists a unique $r \in R$ such that:

- No term of r is divisible by any of $\mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s)$;
- There exists $g \in I$ such that $f = g + r$.

Also, $r = \textsc{FullReduction}(f, G, \prec)$ (whatever the choice of ordering of the polynomials in G). It is called the normal form of f modulo G.

Normal forms

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Let $I \subset R$ be an ideal and $G = (g_1, \ldots, g_s) \subset R$ be a Gröbner basis for $(I, \prec)$. Take $f \in R$. There exists a unique $r \in R$ such that:

- No term of r is divisible by any of $\mathsf{LM}_\prec(g_1), \ldots, \mathsf{LM}_\prec(g_s)$;
- There exists $g \in I$ such that $f = g + r$.

Also, $r = \textsc{FullReduction}(f, G, \prec)$ (whatever the choice of ordering of the polynomials in G). It is called the normal form of f modulo G.

$r = 0$ if and only if $f \in I = \langle G \rangle$

Normal forms

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Let $I \subset R$ be an ideal and $G = (g_1, \ldots, g_s) \subset R$ be a Gröbner basis for $(I, \prec)$. Take $f \in R$. There exists a unique $r \in R$ such that:

- No term of r is divisible by any of $\mathrm{LM}_\prec(g_1), \ldots, \mathrm{LM}_\prec(g_s)$;
- There exists $g \in I$ such that $f = g + r$.

Also, $r = \textsc{FullReduction}(f, G, \prec)$ (whatever the choice of ordering of the polynomials in G). It is called the normal form of f modulo G.

$r = 0$ if and only if $f \in I = \langle G \rangle$

Gröbner bases with the full reduction algorithm solve the ideal membership problem

Normal forms

- Recall that the kernel of the map

$$\mathsf{NF}_{\prec} : f \mapsto \textsc{FullReduction}(f, G, \prec)$$

is $\langle G \rangle$. The function $\mathsf{NF}_{\prec}(., G)$ is a projection on a linear subspace which is normal to $\langle G \rangle$.

Normal forms

- Recall that the kernel of the map

$$\mathsf{NF}_{\prec} : f \mapsto \textsc{FullReduction}(f, G, \prec)$$

  is $\langle G \rangle$. The function $\mathsf{NF}_{\prec}(., G)$ is a projection on a linear subspace which is normal to $\langle G \rangle$.
- The function $\mathsf{NF}_{\prec}(., G)$ returns a canonical representative of the quotient ring $\frac{R}{\langle G \rangle}$.
  Equivalence relation: $f \sim g \iff f - g \in \langle G \rangle$

Normal forms

- Recall that the kernel of the map

$$\mathsf{NF}_{\prec} : f \mapsto \textsc{FullReduction}(f, G, \prec)$$

  is $\langle G \rangle$. The function $\mathsf{NF}_{\prec}(., G)$ is a projection on a linear subspace which is normal to $\langle G \rangle$.

- The function $\mathsf{NF}_{\prec}(., G)$ returns a canonical representative of the quotient ring $\frac{R}{\langle G \rangle}$.
  Equivalence relation: $f \sim g \iff f - g \in \langle G \rangle$
  Example. Consider $G = \langle x_1^2 - 1, x_2^2 - 2 \rangle$.

Is it a Gröbner basis for $\prec_{grevlex}$?

Equivalence classes of $\frac{R}{\langle G \rangle}$?

Normal forms

- Recall that the kernel of the map

$$\mathsf{NF}_{\prec} : f \mapsto \textsc{FullReduction}(f, G, \prec)$$

  is $\langle G \rangle$. The function $\mathsf{NF}_{\prec}(., G)$ is a projection on a linear subspace which is normal to $\langle G \rangle$.

- The function $\mathsf{NF}_{\prec}(., G)$ returns a canonical representative of the quotient ring $\frac{R}{\langle G \rangle}$.
  Equivalence relation: $f \sim g \iff f - g \in \langle G \rangle$
  Example. Consider $G = \langle x_1^2 - 1, x_2^2 - 2 \rangle$.
  Is it a Gröbner basis for $\prec_{grevlex}$?
  Equivalence classes of $\frac{R}{\langle G \rangle}$?

  This will be developed further.

Characterizations of Gröbner bases

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Warm-up – S-polynomials

Let f and g be in $R - \{0\}$. Let $\lambda = \mathsf{lcm}_\prec(f, g)$.

We define the S-polynomial of (f, g) w.r.t. $\prec$ as

$$\mathsf{spol}_\prec(f, g) = \frac{\lambda}{\mathsf{LT}_\prec(f)} f - \frac{\lambda}{\mathsf{LT}_\prec(g)} g$$

Characterizations of Gröbner bases

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ an admissible monomial ordering over R.

Warm-up – S-polynomials

Let f and g be in $R - \{0\}$. Let $\lambda = \mathsf{lcm}_\prec(f, g)$.
We define the S-polynomial of (f, g) w.r.t. $\prec$ as

$$\mathsf{spol}_\prec(f, g) = \frac{\lambda}{\mathsf{LT}_\prec(f)} f - \frac{\lambda}{\mathsf{LT}_\prec(g)} g$$

Buchberger's criterion

Let $I \subset R$ be an ideal and $G = (g_1, \ldots, g_s) \subset R$ be such that $I = \langle G \rangle$ (G is a basis for I).
It holds that G is a Gröbner basis for $(I, \prec)$ if and only if

$$\text{for all } 1 \leq i, j \leq s,\ \mathsf{NF}_\prec(\mathsf{spol}_\prec(g_i, g_j)) \text{ is identically zero.}$$

Buchberger's criterion

- ☛ Provides an algorithm which on input $\prec$ and G decides whether G is a Gröbner basis for $(\langle G \rangle, \prec)$;

Buchberger's criterion

☛ Provides an algorithm which on input $\prec$ and G decides whether G is a Gröbner basis for $(\langle G \rangle, \prec)$;

- This algorithm always computes 0 in case G is a Gröbner basis;
- When G is **not** a Gröbner basis,

$\mathsf{NF}_{\prec}(\mathrm{spol}(g_i, g_j), G)$ is still interesting.

Buchberger's criterion

☛ Provides an algorithm which on input $\prec$ and G decides whether G is a Gröbner basis for $(\langle G \rangle, \prec)$;

- This algorithm always computes 0 in case G is a Gröbner basis;
- When G is **not** a Gröbner basis,

  $\mathsf{NF}_{\prec}(\mathrm{spol}(g_i, g_j), G)$ is still interesting.

We reuse the above notation. It holds that

$$g = \mathsf{NF}_{\prec}(\mathrm{spol}(g_i, g_j), G) \in \langle G \rangle.$$

When it is not zero $\mathsf{LM}_{\prec}(g) \notin \langle \mathsf{LM}_{\prec}(G) \rangle$.

Buchberger's algorithm

Buchberger's algorithm

Idea. Consider all pairs (g, g') in the current basis G $\quad\rightsquigarrow$ Pairs(G)

Buchberger's algorithm

INPUT:
- $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: A Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

1. $G \leftarrow \boldsymbol{f}$
2. $G' \leftarrow \emptyset$

Buchberger's algorithm

INPUT:
- $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: A Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

1. $G \leftarrow \boldsymbol{f}$
2. $G' \leftarrow \emptyset$
3. while $G' \neq G$ do

   3.1 $\mathscr{P} \leftarrow \text{Pairs}(G)$

   3.2 $G' \leftarrow G$

   3.3 for all $(g, g') \in \mathscr{P}$ do

Buchberger's algorithm

INPUT:
- $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: A Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

1. $G \leftarrow \boldsymbol{f}$
2. $G' \leftarrow \emptyset$
3. while $G' \neq G$ do
   3.1 $\mathscr{P} \leftarrow \mathrm{Pairs}(G)$
   3.2 $G' \leftarrow G$
   3.3 for all $(g, g') \in \mathscr{P}$ do
   - $r \leftarrow \textsc{FullReduction}(\mathrm{spol}_{\prec}(g, g'), G')$

Buchberger's algorithm

INPUT:
- $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: A Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

1. $G \leftarrow \boldsymbol{f}$
2. $G' \leftarrow \emptyset$
3. while $G' \neq G$ do
   - 3.1 $\mathscr{P} \leftarrow \text{Pairs}(G)$
   - 3.2 $G' \leftarrow G$
   - 3.3 for all $(g, g') \in \mathscr{P}$ do
     - $r \leftarrow \textsc{FullReduction}(\text{spol}_\prec(g, g'), G')$
     - if $r \neq 0$ then
       - $G \leftarrow G \cup \{r\}$
4. return G

Buchberger's algorithm

On input $\boldsymbol{f} \subset R$ and $\prec$, Buchberger$(\boldsymbol{f}, \prec)$ terminates and returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

Buchberger's algorithm

On input $\boldsymbol{f} \subset R$ and $\prec$, Buchberger$(\boldsymbol{f}, \prec)$ terminates and returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

- Prove that $G \subset \langle \boldsymbol{f} \rangle$ at each step.

Buchberger's algorithm

On input $\boldsymbol{f} \subset R$ and $\prec$, Buchberger$(\boldsymbol{f}, \prec)$ terminates and returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

- Prove that $G \subset \langle \boldsymbol{f} \rangle$ at each step.
- Prove that whenever it terminates, it returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$. Buchberger's criterion.

Buchberger's algorithm

On input $\boldsymbol{f} \subset R$ and $\prec$, Buchberger$(\boldsymbol{f}, \prec)$ terminates and returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

- Prove that $G \subset \langle \boldsymbol{f} \rangle$ at each step.
- Prove that whenever it terminates, it returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$. Buchberger's criterion.
- Prove that $\langle \mathsf{LM}_\prec(G') \rangle \subset \langle \mathsf{LM}_\prec(G) \rangle$

Buchberger's algorithm

On input $\boldsymbol{f} \subset R$ and $\prec$, Buchberger$(\boldsymbol{f}, \prec)$ terminates and returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

- Prove that $G \subset \langle \boldsymbol{f} \rangle$ at each step.
- Prove that whenever it terminates, it returns a Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$. Buchberger's criterion.
- Prove that $\langle \mathsf{LM}_{\prec}(G') \rangle \subset \langle \mathsf{LM}_{\prec}(G) \rangle$
- Use the theorem on ascending chain of ideals.

Behaviour of Buchberger's algorithm

☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required

Behaviour of Buchberger's algorithm

☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required

- A commonly used strategy is by refining with the degree of the $\mathrm{lcm}_\prec(g, g')$ but *we need more.*

Behaviour of Buchberger's algorithm

☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required

- A commonly used strategy is by refining with the degree of the $\mathrm{lcm}_{\prec}(g, g')$ but *we need more.*
  There has been a whole industry on identifying a "good" strategy
  Giovini, Mora, Niesi, Robbiano, Traverso'91

Behaviour of Buchberger's algorithm

- ☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required
  - A commonly used strategy is by refining with the degree of the $\mathrm{lcm}_{\prec}(g, g')$ but *we need more.*
    There has been a whole industry on identifying a "good" strategy
    Giovini, Mora, Niesi, Robbiano, Traverso'91
- ☛ Most of reductions in Buchberger's algorithm compute 0 (!)

Behaviour of Buchberger's algorithm

☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required

- A commonly used strategy is by refining with the degree of the $\mathrm{lcm}_{\prec}(g, g')$ but *we need more.*
  There has been a whole industry on identifying a "good" strategy
  Giovini, Mora, Niesi, Robbiano, Traverso'91

☛ Most of reductions in Buchberger's algorithm compute 0 (!)

- These are useless computations

Behaviour of Buchberger's algorithm

☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required

- A commonly used strategy is by refining with the degree of the $\mathrm{lcm}_{\prec}(g, g')$ but *we need more.*
  There has been a whole industry on identifying a "good" strategy
  Giovini, Mora, Niesi, Robbiano, Traverso'91

☛ Most of reductions in Buchberger's algorithm compute 0 (!)

- These are useless computations
- Prove that when some pair reduces to 0, it will always further reduce to 0 $\rightsquigarrow$ rewrite the algorithm.

Behaviour of Buchberger's algorithm

☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required

- A commonly used strategy is by refining with the degree of the $\mathrm{lcm}_{\prec}(g, g')$ but *we need more.*
  There has been a whole industry on identifying a "good" strategy
  Giovini, Mora, Niesi, Robbiano, Traverso'91

☛ Most of reductions in Buchberger's algorithm compute 0 (!)

- These are useless computations
- Prove that when some pair reduces to 0, it will always further reduce to 0 $\rightsquigarrow$ rewrite the algorithm.
- Note that once the selection strategy is fixed, one can remember which pairs reduce to 0
  Useful for multi-modular computations (Gröbner bases over $\mathbb{Q}$).

Behaviour of Buchberger's algorithm

☛ Choice of the pairs (g, g') $\rightsquigarrow$ A selection strategy is required

- A commonly used strategy is by refining with the degree of the $\mathrm{lcm}_{\prec}(g, g')$ but *we need more.*
  There has been a whole industry on identifying a “good” strategy
  Giovini, Mora, Niesi, Robbiano, Traverso'91

☛ Most of reductions in Buchberger's algorithm compute 0 (!)

- These are useless computations
- Prove that when some pair reduces to 0, it will always further reduce to 0 $\rightsquigarrow$ rewrite the algorithm.
- Note that once the selection strategy is fixed, one can remember which pairs reduce to 0
  Useful for multi-modular computations (Gröbner bases over $\mathbb{Q}$).

Modern algorithms (F4/F5) bring new efficient solutions to these issues

Example (I)

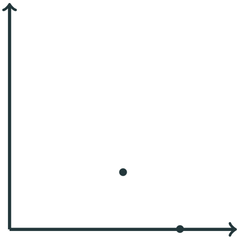
Take $f_1 = x_1^3 - 2x_1x_2$ and $f_2 = x_1^2x_2 - 2x_2^2 + x_1$ and $\prec_{grevlex}$.

Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.

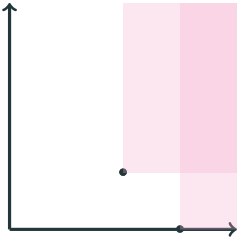
Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.



Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.



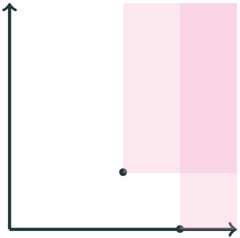
Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.

$\boxed{G = (f_1, f_2)} \rightsquigarrow S_{grevlex}(f_1, f_2) = -x_1^2$, note that $x_1^2 \notin \langle x_1^3, x_1^2x_2 \rangle$

☛ $f_3 = \mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_1, f_2), G) = -x_1^2$

$\boxed{G = (f_1, f_2, f_3)}$



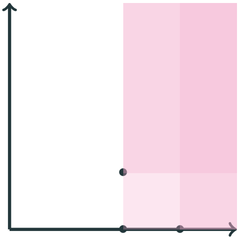
Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.

$\boxed{G = (f_1, f_2)} \rightsquigarrow S_{grevlex}(f_1, f_2) = -x_1^2$, note that $x_1^2 \notin \langle x_1^3, x_1^2x_2 \rangle$

☛ $f_3 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_2), G) = -x_1^2$

$\boxed{G = (f_1, f_2, f_3)}$



Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.

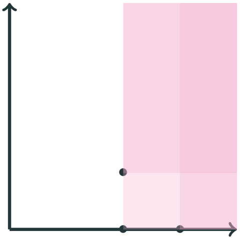
$\boxed{G = (f_1, f_2)} \rightsquigarrow S_{grevlex}(f_1, f_2) = -x_1^2$, note that $x_1^2 \notin \langle x_1^3, x_1^2x_2 \rangle$

☛ $f_3 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_2), G) = -x_1^2$

$\boxed{G = (f_1, f_2, f_3)}$

$\rightsquigarrow \mathrm{spol}_{grevlex}(f_1, f_3) = -x_1x_2$

☛ $f_4 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_3), G) = -x_1x_2$
with $x_1x_2 \notin \langle x_1^3, x_1^2x_2, x_1^2 \rangle$

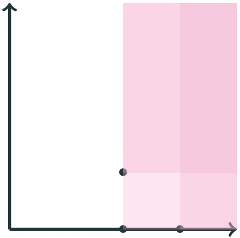


Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.

$\boxed{G = (f_1, f_2)}$ $\rightsquigarrow S_{grevlex}(f_1, f_2) = -x_1^2$, note that $x_1^2 \notin \langle x_1^3, x_1^2x_2 \rangle$

☛ $f_3 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_2), G) = -x_1^2$



$\boxed{G = (f_1, f_2, f_3)}$

$\rightsquigarrow \mathrm{spol}_{grevlex}(f_1, f_3) = -x_1x_2$

☛ $f_4 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_3), G) = -x_1x_2$
with $x_1x_2 \notin \langle x_1^3, x_1^2x_2, x_1^2 \rangle$

$\rightsquigarrow \mathrm{spol}_{grevlex}(f_2, f_3) = -2x_2^2 + x_1$

☛ $f_5 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_2, f_3), G) = -2x_2^2 + x_1$

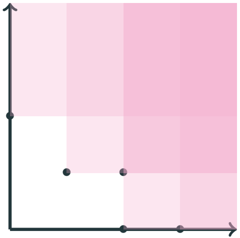
$\boxed{G = (f_1, f_2, f_3, f_4, f_5)}$

Example (I)

Take $f_1 = \boxed{x_1^3} - 2x_1x_2$ and $f_2 = \boxed{x_1^2x_2} - 2x_2^2 + x_1$ and $\prec_{grevlex}$.

$\boxed{G = (f_1, f_2)} \rightsquigarrow S_{grevlex}(f_1, f_2) = -x_1^2$, note that $x_1^2 \notin \langle x_1^3, x_1^2x_2 \rangle$

☛ $f_3 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_2), G) = -x_1^2$



$\boxed{G = (f_1, f_2, f_3)}$

$\rightsquigarrow \mathrm{spol}_{grevlex}(f_1, f_3) = -x_1x_2$

☛ $f_4 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_3), G) = -x_1x_2$
with $x_1x_2 \notin \langle x_1^3, x_1^2x_2, x_1^2 \rangle$

$\rightsquigarrow \mathrm{spol}_{grevlex}(f_2, f_3) = -2x_2^2 + x_1$

☛ $f_5 = \mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_2, f_3), G) = -2x_2^2 + x_1$

$\boxed{G = (f_1, f_2, f_3, f_4, f_5)}$

Example (II)

$$\boxed{G = (f_1, f_2, f_3, f_4)}$$

If remains to investigate $(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), \ldots$

Example (II)

$\boxed{G = (f_1, f_2, f_3, f_4)}$

If remains to investigate $(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), \ldots$

$\rightsquigarrow$ $\text{spol}_{grevlex}(f_1, f_4) = x_2 f_4$ ☛ $\text{NF}_{grevlex}(\text{spol}_{grevlex}(f_1, f_4), G) = 0$

Example (II)

$$\boxed{G = (f_1, f_2, f_3, f_4)}$$

If remains to investigate $(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), \ldots$

$\rightsquigarrow$ $\mathrm{spol}_{grevlex}(f_1, f_4) = x_2 f_4$ ☛ $\mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_4), G) = 0$

$\rightsquigarrow$ $\mathrm{spol}_{grevlex}(f_2, f_4) = f_5$ ☛ $\mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_2, f_4), G) = 0$

Example (II)

$\boxed{G = (f_1, f_2, f_3, f_4)}$

If remains to investigate $(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), \ldots$

$\rightsquigarrow$ $\mathsf{spol}_{grevlex}(f_1, f_4) = x_2 f_4$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_1, f_4), G) = 0$

$\rightsquigarrow$ $\mathsf{spol}_{grevlex}(f_2, f_4) = f_5$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_2, f_4), G) = 0$

$\rightsquigarrow$ $\mathsf{spol}_{grevlex}(f_3, f_4) = 0$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_3, f_4), G) = 0$

Example (II)

$\boxed{G = (f_1, f_2, f_3, f_4)}$

If remains to investigate $(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), \ldots$

$\rightsquigarrow \mathsf{spol}_{grevlex}(f_1, f_4) = x_2 f_4$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_1, f_4), G) = 0$

$\rightsquigarrow \mathsf{spol}_{grevlex}(f_2, f_4) = f_5$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_2, f_4), G) = 0$

$\rightsquigarrow \mathsf{spol}_{grevlex}(f_3, f_4) = 0$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_3, f_4), G) = 0$

$\rightsquigarrow \mathsf{spol}_{grevlex}(f_1, f_5) = -\frac{1}{2} x_1 f_3 + x_2 f_4$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_1, f_5), G) = 0$

Example (II)

$G = (f_1, f_2, f_3, f_4)$

If remains to investigate $(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), \ldots$

$\rightsquigarrow$ $\mathsf{spol}_{grevlex}(f_1, f_4) = x_2 f_4$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_1, f_4), G) = 0$

$\rightsquigarrow$ $\mathsf{spol}_{grevlex}(f_2, f_4) = f_5$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_2, f_4), G) = 0$

$\rightsquigarrow$ $\mathsf{spol}_{grevlex}(f_3, f_4) = 0$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_3, f_4), G) = 0$

$\rightsquigarrow$ $\mathsf{spol}_{grevlex}(f_1, f_5) = -\frac{1}{2} x_1 f_3 + x_2 f_4$ ☛ $\mathsf{NF}_{grevlex}(\mathsf{spol}_{grevlex}(f_1, f_5), G) = 0$

And so on... All S-polynomials reduce to 0.

Example (II)

$\boxed{G = (f_1, f_2, f_3, f_4)}$

If remains to investigate $(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), \ldots$

$\rightsquigarrow$ $\mathrm{spol}_{grevlex}(f_1, f_4) = x_2 f_4$ ☛ $\mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_4), G) = 0$

$\rightsquigarrow$ $\mathrm{spol}_{grevlex}(f_2, f_4) = f_5$ ☛ $\mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_2, f_4), G) = 0$

$\rightsquigarrow$ $\mathrm{spol}_{grevlex}(f_3, f_4) = 0$ ☛ $\mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_3, f_4), G) = 0$

$\rightsquigarrow$ $\mathrm{spol}_{grevlex}(f_1, f_5) = -\frac{1}{2} x_1 f_3 + x_2 f_4$ ☛ $\mathrm{NF}_{grevlex}(\mathrm{spol}_{grevlex}(f_1, f_5), G) = 0$

And so on... All S-polynomials reduce to 0.

We can conclude that G is a Gröbner basis for $(\langle f_1, f_2 \rangle, \prec_{grevlex})$

Uniqueness of Gröbner bases (I)

$$G = \begin{cases} x_1^3 - 2x_1x_2 \\ x_1^2x_2 - 2x_2^2 + x_1 \\ f_3 = -x_1^2, \qquad\qquad f_4 = -x_1x_2 \\ f_5 = -2x_2^2 + x_1 \end{cases}$$

Uniqueness of Gröbner bases (I)

$$G = \begin{cases} x_1^3 - 2x_1x_2 & = -x_1 f_3 + 2f_4 \\ x_1^2x_2 - 2x_2^2 + x_1 & \\ f_3 = -x_1^2, & f_4 = -x_1x_2 \\ f_5 = -2x_2^2 + x_1 & \end{cases}$$

Uniqueness of Gröbner bases (I)

$$G = \begin{cases} x_1^3 - 2x_1x_2 & = -x_1f_3 + 2f_4 \\ x_1^2x_2 - 2x_2^2 + x_1 & = -x_2f_4 + f_5 \\ f_3 = -x_1^2, & f_4 = -x_1x_2 \\ f_5 = -2x_2^2 + x_1 & \end{cases}$$

Uniqueness of Gröbner bases (I)

$$G = \begin{cases} x_1^3 - 2x_1x_2 & = -x_1f_3 + 2f_4 \\ x_1^2x_2 - 2x_2^2 + x_1 & = -x_2f_4 + f_5 \\ f_3 = -x_1^2, & f_4 = -x_1x_2 \\ f_5 = -2x_2^2 + x_1 & \end{cases}$$

➡ **redundant elements...**

Uniqueness of Gröbner bases (I)

$$G = \begin{cases} x_1^3 - 2x_1x_2 & = -x_1 f_3 + 2f_4 \\ x_1^2 x_2 - 2x_2^2 + x_1 & = -x_2 f_4 + f_5 \\ f_3 = -x_1^2, & f_4 = -x_1 x_2 \\ f_5 = -2x_2^2 + x_1 \end{cases}$$

➟ **redundant elements...**

Minimal Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$. One says that G is a minimal Gröbner basis if for all $f \in G$:

- $\mathrm{LC}_\prec(f) = 1$;
- $\mathrm{LM}_\prec(f) \notin \langle \mathrm{LM}_\prec(G \setminus \{f\}) \rangle$.

Uniqueness of Gröbner bases (I)

$$G = \begin{cases} x_1^3 - 2x_1x_2 & = -x_1f_3 + 2f_4 \\ x_1^2x_2 - 2x_2^2 + x_1 & = -x_2f_4 + f_5 \\ f_3 = -x_1^2, & f_4 = -x_1x_2 \\ f_5 = -2x_2^2 + x_1 & \end{cases}$$

➟ **redundant elements...**

Minimal Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$. One says that G is a minimal Gröbner basis if for all $f \in G$:

- $\mathsf{LC}_\prec(f) = 1$;
- $\mathsf{LM}_\prec(f) \notin \langle \mathsf{LM}_\prec(G \setminus \{f\}) \rangle$.

Reduced Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$. One says that G is a reduced Gröbner basis if for all $f \in G$:

- $\mathsf{LC}_\prec(f) = 1$;
- no monomial of f lies in $\langle \mathsf{LM}_\prec(G \setminus \{f\}) \rangle$.

Uniqueness of Gröbner bases (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Let I be an ideal of R which is not $\{0\}$. There exists a unique reduced Gröbner basis for $(I, \prec)$.

Uniqueness of Gröbner bases (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Let I be an ideal of R which is not $\{0\}$. There exists a unique reduced Gröbner basis for $(I, \prec)$.

- G reduced $\Rightarrow$ G minimal $\Rightarrow$ $\langle \mathsf{LM}_\prec(G) \rangle$ is unique

Uniqueness of Gröbner bases (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Let I be an ideal of R which is not $\{0\}$. There exists a unique reduced Gröbner basis for $(I, \prec)$.

- G reduced $\Rightarrow$ G minimal $\Rightarrow$ $\langle \mathsf{LM}_{\prec}(G) \rangle$ is unique
- Existence:
  design an algorithm which makes a Gröbner basis reduced (!)

Uniqueness of Gröbner bases (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Let I be an ideal of R which is not $\{0\}$. There exists a unique reduced Gröbner basis for $(I, \prec)$.

- G reduced $\Rightarrow$ G minimal $\Rightarrow$ $\langle \mathsf{LM}_{\prec}(G) \rangle$ is unique
- Existence:
  design an algorithm which makes a Gröbner basis reduced (!)
- Uniqueness: by contradiction + uniqueness of the normal form

Uniqueness of Gröbner bases (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Let I be an ideal of R which is not $\{0\}$. There exists a unique reduced Gröbner basis for $(I, \prec)$.

- G reduced $\Rightarrow$ G minimal $\Rightarrow$ $\langle \mathsf{LM}_{\prec}(G) \rangle$ is unique
- Existence:
  design an algorithm which makes a Gröbner basis reduced (!)
- Uniqueness: by contradiction + uniqueness of the normal form

One can decide whether two ideals given by distinct generating sets are equal.

Properties of Gröbner bases

The elimination theorem (I)

Goal. Represent projections of $\mathbb{K}$-algebraic sets.

The elimination theorem (I)

Goal. Represent projections of $\mathbb{K}$-algebraic sets.

Remark. Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$ and $V \subset \overline{\mathbb{K}}^n$ be a $\mathbb{K}$-algebraic set. It holds that $\pi_i(V)$ may **not** be a $\mathbb{K}$-algebraic set.

The elimination theorem (I)

Goal. Represent projections of $\mathbb{K}$-algebraic sets.

Remark. Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$ and $V \subset \overline{\mathbb{K}}^n$ be a $\mathbb{K}$-algebraic set. It holds that $\pi_i(V)$ may **not** be a $\mathbb{K}$-algebraic set.

Example. $x_1 x_2 - 1 = 0$.

The elimination theorem (I)

Goal. Represent projections of $\mathbb{K}$-algebraic sets.

Remark. Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$ and $V \subset \overline{\mathbb{K}}^n$ be a $\mathbb{K}$-algebraic set. It holds that $\pi_i(V)$ may **not** be a $\mathbb{K}$-algebraic set.

Example. $x_1 x_2 - 1 = 0$.

Locally closed algebraic sets

Let $W \subset \overline{\mathbb{K}}^n$. One says that W is a locally closed algebraic set if it is the intersection of a Zariski open set with an algebraic set (defined over $\mathbb{K}$).

The elimination theorem (I)

Goal. Represent projections of $\mathbb{K}$-algebraic sets.

Remark. Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$ and $V \subset \overline{\mathbb{K}}^n$ be a $\mathbb{K}$-algebraic set. It holds that $\pi_i(V)$ may **not** be a $\mathbb{K}$-algebraic set.

Example. $x_1 x_2 - 1 = 0$.

Locally closed algebraic sets

Let $W \subset \overline{\mathbb{K}}^n$. One says that W is a locally closed algebraic set if it is the intersection of a Zariski open set with an algebraic set (defined over $\mathbb{K}$).

Constructible sets

A constructible set is a finite union of locally closed sets.

The elimination theorem (I)

Goal. Represent projections of $\mathbb{K}$-algebraic sets.

Remark. Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$ and $V \subset \overline{\mathbb{K}}^n$ be a $\mathbb{K}$-algebraic set. It holds that $\pi_i(V)$ may **not** be a $\mathbb{K}$-algebraic set.

Example. $x_1 x_2 - 1 = 0.$

Locally closed algebraic sets

Let $W \subset \overline{\mathbb{K}}^n$. One says that W is a locally closed algebraic set if it is the intersection of a Zariski open set with an algebraic set (defined over $\mathbb{K}$).

Constructible sets

A constructible set is a finite union of locally closed sets.

Let $V \subset \overline{\mathbb{K}}^n$ be an algebraic set and π_i as above. Then, $\pi_i(V)$ is a constructible set.

The elimination theorem (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Elimination ordering

We say that $\prec$ is an elimination ordering, which eliminates $(x_1, \ldots, x_i)$ if for all $f \in R - \{0\}$,

$$\mathsf{LM}_{\prec}(f) \in \mathbb{K}[x_{i+1}, \ldots, x_n] \Longrightarrow f \in \mathbb{K}[x_{i+1}, \ldots, x_n]$$

The elimination theorem (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Elimination ordering

We say that $\prec$ is an elimination ordering, which eliminates $(x_1, \ldots, x_i)$ if for all $f \in R - \{0\}$,

$$\mathsf{LM}_{\prec}(f) \in \mathbb{K}[x_{i+1}, \ldots, x_n] \Longrightarrow f \in \mathbb{K}[x_{i+1}, \ldots, x_n]$$

- The lexicographical ordering is an elimination ordering;

The elimination theorem (II)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Elimination ordering

We say that $\prec$ is an elimination ordering, which eliminates $(x_1, \ldots, x_i)$ if for all $f \in R - \{0\}$,

$$\mathsf{LM}_{\prec}(f) \in \mathbb{K}[x_{i+1}, \ldots, x_n] \Longrightarrow f \in \mathbb{K}[x_{i+1}, \ldots, x_n]$$

- The lexicographical ordering is an elimination ordering;
- Consider $\prec_{grevlex_1}$ and $\prec_{grevlex_2}$, two grevlex orderings over monomials of $\mathbb{K}[x_1, \ldots, x_i]$ and $\mathbb{K}[x_{i+1}, \ldots, x_n]$. The block ordering $\prec$ using these two grevlex orderings is an elimination ordering.

The elimination theorem (III)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible block monomial ordering which eliminates $x_1, \ldots, x_i$ built with $\prec_1$ and $\prec_2$.

Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$.

The elimination theorem (III)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible block monomial ordering which eliminates $x_1, \ldots, x_i$ built with $\prec_1$ and $\prec_2$.

Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$.

The elimination theorem

Let $I \subset R$ be an ideal and G be a Gröbner basis of $(I, \prec)$. Denote by I_i the ideal $I \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$.
Then $G_i = G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $(I_i, \prec_2)$. Besides, $V(G_i)$ equals the Zariski closure of $\pi_i(V(I))$.

The elimination theorem (III)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible block monomial ordering which eliminates $x_1, \ldots, x_i$ built with $\prec_1$ and $\prec_2$.

Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$.

The elimination theorem

Let $I \subset R$ be an ideal and G be a Gröbner basis of $(I, \prec)$. Denote by I_i the ideal $I \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$.
Then $G_i = G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $(I_i, \prec_2)$. Besides, $V(G_i)$ equals the Zariski closure of $\pi_i(V(I))$.

Proof of the first statement.

- It suffices to prove that $\langle \mathsf{LM}_{\prec_2}(G_i) \rangle = \langle \mathsf{LM}_{\prec_2}(I_i) \rangle$.

The elimination theorem (III)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible block monomial ordering which eliminates $x_1, \ldots, x_i$ built with $\prec_1$ and $\prec_2$.

Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$.

The elimination theorem

Let $I \subset R$ be an ideal and G be a Gröbner basis of $(I, \prec)$. Denote by I_i the ideal $I \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$.
Then $G_i = G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $(I_i, \prec_2)$. Besides, $V(G_i)$ equals the Zariski closure of $\pi_i(V(I))$.

Proof of the first statement.

- It suffices to prove that $\langle \mathsf{LM}_{\prec_2}(G_i) \rangle = \langle \mathsf{LM}_{\prec_2}(I_i) \rangle$.
- Use the property of elimination orderings to prove that for $f \in I_i$, $\mathsf{LM}_{\prec_2}(f)$ is divisible by $\mathsf{LM}_{\prec_2}(g)$ for some $g \in I_i$.

The elimination theorem (III)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible block monomial ordering which eliminates $x_1, \ldots, x_i$ built with $\prec_1$ and $\prec_2$.

Let π_i be the canonical projection $(x_1, \ldots, x_n) \to (x_i, \ldots, x_n)$.

The elimination theorem

Let $I \subset R$ be an ideal and G be a Gröbner basis of $(I, \prec)$. Denote by I_i the ideal $I \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$.
Then $G_i = G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $(I_i, \prec_2)$. Besides, $V(G_i)$ equals the Zariski closure of $\pi_i(V(I))$.

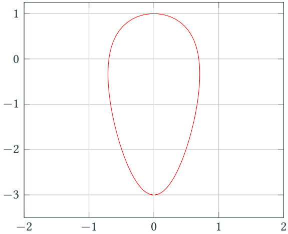
Proof of the first statement.

- It suffices to prove that $\langle \mathsf{LM}_{\prec_2}(G_i)\rangle = \langle \mathsf{LM}_{\prec_2}(I_i)\rangle$.
- Use the property of elimination orderings to prove that for $f \in I_i$, $\mathsf{LM}_{\prec_2}(f)$ is divisible by $\mathsf{LM}_{\prec_2}(g)$ for some $g \in I_i$.

See **Cox, Little, O'Shea** for a proof of the 2nd statement.

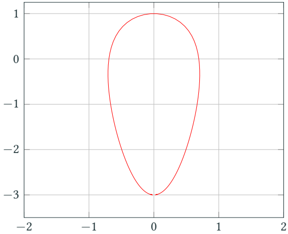
Application: implicitization

Consider the parametric curve
$t \mapsto \left(\frac{2t}{1+2t^2}, \frac{1-3t^2}{1+t^2}\right)$
Problem. Compute the implicit equation
$f = 0$ (for $f \in \mathbb{Q}[x, y]$)



Application: implicitization

Consider the parametric curve
$t \mapsto \left(\frac{2t}{1+2t^2}, \frac{1-3t^2}{1+t^2}\right)$
Problem. Compute the implicit equation
$f = 0$ (for $f \in \mathbb{Q}[x, y]$)



$\rightsquigarrow$ **Gröbner basis computation** for an elimination ordering $t \succ_{elim} x, y$

$$f = x^2y^2 - 10x^2y + 25x^2 + 4y^2 + 8y - 12$$

Shape of Gröbner bases (lex)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal and G be a Gröbner basis for $(I, \prec_{lex})$. Then $G = T_n \cup T_{n-1} \cup \cdots \cup T_1$ with:

- $T_i \subset \mathbb{K}[x_i, \ldots, x_n]$;
- $T_n \cup \cdots \cup T_i$ is a Gröbner basis for $(I \cap \mathbb{K}[x_i, \ldots, x_n], \prec_{lex})$;
- $V(T_n \cup \cdots \cup T_i)$ is the Zariski closure of the projection of $V(I)$ on the $(x_i, \ldots, x_n)$-space.

Shape of Gröbner bases (lex)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal and G be a Gröbner basis for $(I, \prec_{lex})$. Then $G = T_n \cup T_{n-1} \cup \cdots \cup T_1$ with:

- $T_i \subset \mathbb{K}[x_i, \ldots, x_n]$;
- $T_n \cup \cdots \cup T_i$ is a Gröbner basis for $(I \cap \mathbb{K}[x_i, \ldots, x_n], \prec_{lex})$;
- $V(T_n \cup \cdots \cup T_i)$ is the Zariski closure of the projection of $V(I)$ on the $(x_i, \ldots, x_n)$-space.

- When $V(I)$ is finite, $I \cap \mathbb{K}[x_n]$ is not $\{0\}$;
  ➟ $I \cap \mathbb{K}[x_i]$ is not $\{0\}$ for all $1 \leq i \leq n$.

Shape of Gröbner bases (lex)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal and G be a Gröbner basis for $(I, \prec_{lex})$. Then $G = T_n \cup T_{n-1} \cup \cdots \cup T_1$ with:

- $T_i \subset \mathbb{K}[x_i, \ldots, x_n]$;
- $T_n \cup \cdots \cup T_i$ is a Gröbner basis for $(I \cap \mathbb{K}[x_i, \ldots, x_n], \prec_{lex})$;
- $V(T_n \cup \cdots \cup T_i)$ is the Zariski closure of the projection of $V(I)$ on the $(x_i, \ldots, x_n)$-space.

- When $V(I)$ is finite, $I \cap \mathbb{K}[x_n]$ is not $\{0\}$;
  ➟ $I \cap \mathbb{K}[x_i]$ is not $\{0\}$ for all $1 \leq i \leq n$.
- Gröbner basis computed for lexicographical monomial orderings provide a triangular rewriting.

Shape of Gröbner bases (lex)

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal and G be a Gröbner basis for $(I, \prec_{lex})$. Then $G = T_n \cup T_{n-1} \cup \cdots \cup T_1$ with:

- $T_i \subset \mathbb{K}[x_i, \ldots, x_n]$;
- $T_n \cup \cdots \cup T_i$ is a Gröbner basis for $(I \cap \mathbb{K}[x_i, \ldots, x_n], \prec_{lex})$;
- $V(T_n \cup \cdots \cup T_i)$ is the Zariski closure of the projection of $V(I)$ on the $(x_i, \ldots, x_n)$-space.

- When $V(I)$ is finite, $I \cap \mathbb{K}[x_n]$ is not $\{0\}$;
  ➟ $I \cap \mathbb{K}[x_i]$ is not $\{0\}$ for all $1 \leq i \leq n$.
- Gröbner basis computed for lexicographical monomial orderings provide a triangular rewriting.
  ➟ Comprehensive description of varieties through projections

Consequence

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal. The quotient ring $\frac{R}{I}$ is defined as the set of equivalence classes $f \sim g \Leftrightarrow f - g \in I$ (where $+$ and $\times$ are induced by polynomial addition an multiplication). It is also a $\mathbb{K}$-vector space.

Consequence

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal. The quotient ring $\frac{R}{I}$ is defined as the set of equivalence classes $f \sim g \Leftrightarrow f - g \in I$ (where $+$ and $\times$ are induced by polynomial addition an multiplication). It is also a $\mathbb{K}$-vector space.

Let $I \subset R$ be an ideal. Assume that $V(I)$ is finite. Then the quotient ring is a finite dimensional $\mathbb{K}$-vector space.

Consequence

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal. The quotient ring $\frac{R}{I}$ is defined as the set of equivalence classes $f \sim g \Leftrightarrow f - g \in I$ (where $+$ and $\times$ are induced by polynomial addition an multiplication). It is also a $\mathbb{K}$-vector space.

Let $I \subset R$ be an ideal. Assume that $V(I)$ is finite. Then the quotient ring is a finite dimensional $\mathbb{K}$-vector space.

When $V(I)$ is finite and a Gröbner basis is known for $(I, \prec)$, we obtain unique representatives in $\frac{R}{I}$ (depending on the chosen basis).

Consequence

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Let $I \subset R$ be an ideal. The quotient ring $\frac{R}{I}$ is defined as the set of equivalence classes $f \sim g \Leftrightarrow f - g \in I$ (where $+$ and $\times$ are induced by polynomial addition an multiplication). It is also a $\mathbb{K}$-vector space.

Let $I \subset R$ be an ideal. Assume that $V(I)$ is finite. Then the quotient ring is a finite dimensional $\mathbb{K}$-vector space.

When $V(I)$ is finite and a Gröbner basis is known for $(I, \prec)$, we obtain unique representatives in $\frac{R}{I}$ (depending on the chosen basis). Many algorithmic questions can then be rephrased as linear algebra problems / matrix operations.

Shape of Gröbner bases (graded ordering)

Let f be a homogeneous polynomial in R.

- if for $k \in \mathbb{N}$, x_n^k divides $\mathsf{LM}_{grevlex}(f)$ then x_n^k divides f;
- if for all $1 \leq j \leq n$, $\mathsf{LM}_{grevlex}(f)$ is divisible by x_j and $f \in \mathbb{K}[x_1, \ldots, x_j]$, then f is divisible by x_j.

Shape of Gröbner bases (graded ordering)

Let f be a homogeneous polynomial in R.

- if for $k \in \mathbb{N}$, x_n^k divides $\mathsf{LM}_{grevlex}(f)$ then x_n^k divides f;
- if for all $1 \leq j \leq n$, $\mathsf{LM}_{grevlex}(f)$ is divisible by x_j and $f \in \mathbb{K}[x_1, \ldots, x_j]$, then f is divisible by x_j.

Let $I \subset R$ be an ideal and $d = \min(\deg(f) \mid f \in I \setminus \{0\})$. Consider a Gröbner basis G for $(I, \prec_{grevlex})$.
It holds that

$$\mathsf{Span}\left(g \in G \mid \deg(G) = d\right) = \mathsf{Span}\left(f \in I \mid \deg(f) = d\right).$$

Shape of Gröbner bases (graded ordering)

Let f be a homogeneous polynomial in R.

- if for $k \in \mathbb{N}$, x_n^k divides $\mathsf{LM}_{grevlex}(f)$ then x_n^k divides f;
- if for all $1 \leq j \leq n$, $\mathsf{LM}_{grevlex}(f)$ is divisible by x_j and $f \in \mathbb{K}[x_1, \ldots, x_j]$, then f is divisible by x_j.

Let $I \subset R$ be an ideal and $d = \min(\deg(f) \mid f \in I \setminus \{0\})$. Consider a Gröbner basis G for $(I, \prec_{grevlex})$.
It holds that

$$\mathsf{Span}\,(g \in G \mid \deg(G) = d) = \mathsf{Span}\,(f \in I \mid \deg(f) = d)\,.$$

- This theorem holds for all graded orderings.

Shape of Gröbner bases (graded ordering)

Let f be a homogeneous polynomial in R.

- if for $k \in \mathbb{N}$, x_n^k divides $\mathsf{LM}_{grevlex}(f)$ then x_n^k divides f;
- if for all $1 \leq j \leq n$, $\mathsf{LM}_{grevlex}(f)$ is divisible by x_j and $f \in \mathbb{K}[x_1, \ldots, x_j]$, then f is divisible by x_j.

Let $I \subset R$ be an ideal and $d = \min(\deg(f) \mid f \in I \setminus \{0\})$. Consider a Gröbner basis G for $(I, \prec_{grevlex})$.
It holds that

$$\mathsf{Span}\left(g \in G \mid \deg(G) = d\right) = \mathsf{Span}\left(f \in I \mid \deg(f) = d\right).$$

- This theorem holds for all graded orderings.
- G contains polynomials of the least possible degree in $I \setminus \{0\}$

Back to Hilbert series (I)

We had defined Hilbert series for **monomial ideals**. We define the Hilbert function as follows:

$$d \mapsto \mathsf{HF}_I(d) = \sharp\{\boldsymbol{\beta} \in \mathbb{N}^n \mid \deg(\boldsymbol{x}^{\boldsymbol{\beta}}) = d \text{ and } \boldsymbol{x}^{\boldsymbol{\beta}} \notin I\}.$$

Back to Hilbert series (I)

We had defined Hilbert series for **monomial ideals**. We define the Hilbert function as follows:

$$d \mapsto \mathsf{HF}_I(d) = \sharp\{\boldsymbol{\beta} \in \mathbb{N}^n \mid \deg(\boldsymbol{x}^{\boldsymbol{\beta}}) = d \text{ and } \boldsymbol{x}^{\boldsymbol{\beta}} \notin I\}.$$

The Hilbert series is $\mathsf{HS}_I(t) = \sum_{d=0}^{\infty} \mathsf{HF}_I(d) t^d$.

Back to Hilbert series (I)

We had defined Hilbert series for **monomial ideals**. We define the Hilbert function as follows:

$$d \mapsto \mathrm{HF}_I(d) = \sharp\{\boldsymbol{\beta} \in \mathbb{N}^n \mid \deg(\boldsymbol{x}^{\boldsymbol{\beta}}) = d \text{ and } \boldsymbol{x}^{\boldsymbol{\beta}} \notin I\}.$$

The Hilbert series is $\mathrm{HS}_I(t) = \sum_{d=0}^{\infty} \mathrm{HF}_I(d) t^d$.

Recall that $\frac{R}{I}$ is a $\mathbb{K}$-vector space.

There is a monomial basis for $\frac{R}{I}$.

Back to Hilbert series (I)

We had defined Hilbert series for **monomial ideals**. We define the Hilbert function as follows:

$$d \mapsto \mathrm{HF}_I(d) = \sharp\{\boldsymbol{\beta} \in \mathbb{N}^n \mid \deg(\boldsymbol{x}^{\boldsymbol{\beta}}) = d \text{ and } \boldsymbol{x}^{\boldsymbol{\beta}} \notin I\}.$$

The Hilbert series is $\mathrm{HS}_I(t) = \sum_{d=0}^{\infty} \mathrm{HF}_I(d) t^d$.

Recall that $\frac{R}{I}$ is a $\mathbb{K}$-vector space.

There is a monomial basis for $\frac{R}{I}$.

$\mathrm{HF}_I(d)$ counts the number of elements in this basis of degree d.

➟ The Hilbert series is actually associated to $\frac{R}{I}$

Hilbert series (II)

We can now extend the definition to ideals in R.

Let I be in R.

$$\text{Degree compliant monomial basis } \mathscr{B} \text{ of } \frac{R}{I} \leftrightarrow \text{Monomial basis } \mathscr{B} \text{ of } \langle \mathsf{LM}_{grevlex}(I) \rangle.$$

Hilbert series (II)

We can now extend the definition to ideals in R.

Let I be in R.

$$\text{Degree compliant monomial basis } \mathscr{B} \text{ of } \frac{R}{I} \leftrightarrow \text{Monomial basis } \mathscr{B} \text{ of } \langle \mathsf{LM}_{grevlex}(I) \rangle.$$

$$\mathsf{HF}_{R/I} : d \mapsto \sharp\{\beta \in \mathscr{B} \mid \deg(\beta) = d\}.$$

Hilbert series (II)

We can now extend the definition to ideals in R.

Let I be in R.

Degree compliant monomial basis $\mathscr{B}$ of $\frac{R}{I} \leftrightarrow$ Monomial basis $\mathscr{B}$ of $\langle \mathsf{LM}_{grevlex}(I) \rangle$.

$$\mathsf{HF}_{R/I} : d \mapsto \sharp\{\beta \in \mathscr{B} \mid \deg(\beta) = d\}.$$

The Hilbert series is then defined as

$$\mathsf{HS}_{R/I}(t) = \sum_{d=0}^{\infty} \mathsf{HF}_{R/I}(d) t^d.$$

Hilbert series (III)

Let $I \subset R$ be an ideal. When $V(I)$ is finite, $\frac{R}{I}$ is a finite dimensional $\mathbb{K}$-vector space.

Hilbert series (III)

Let $I \subset R$ be an ideal. When $V(I)$ is finite, $\frac{R}{I}$ is a finite dimensional $\mathbb{K}$-vector space.
Let G be a Gröbner basis for $(I, \prec)$. For all $1 \leq i \leq n$, there exists $k_i \in \mathbb{N}$ and $g \in G$ such that $x_i^{k_i} = \mathsf{LM}_{\prec}(g)$.

Hilbert series (III)

Let $I \subset R$ be an ideal. When $V(I)$ is finite, $\frac{R}{I}$ is a finite dimensional $\mathbb{K}$-vector space.
Let G be a Gröbner basis for $(I, \prec)$. For all $1 \leq i \leq n$, there exists $k_i \in \mathbb{N}$ and $g \in G$ such that $x_i^{k_i} = \mathsf{LM}_{\prec}(g)$.

When $V(I)$ is finite, $\mathsf{HS}_{R/I}(t)$ is a polynomial. Its evaluation at 1 is the degree of I, which coincides with dimension of $\frac{R}{I}$ (as a $\mathbb{K}$ vector space).

Hilbert series (III)

Let $I \subset R$ be an ideal. When $V(I)$ is finite, $\frac{R}{I}$ is a finite dimensional $\mathbb{K}$-vector space.
Let G be a Gröbner basis for $(I, \prec)$. For all $1 \leq i \leq n$, there exists $k_i \in \mathbb{N}$ and $g \in G$ such that $x_i^{k_i} = \mathsf{LM}_\prec(g)$.

When $V(I)$ is finite, $\mathsf{HS}_{R/I}(t)$ is a polynomial. Its evaluation at 1 is the degree of I, which coincides with dimension of $\frac{R}{I}$ (as a $\mathbb{K}$ vector space).
When I is radical, it coincides with the cardinality of $V(I)$.

Hilbert series (III)

Let $I \subset R$ be an ideal. When $V(I)$ is finite, $\frac{R}{I}$ is a finite dimensional $\mathbb{K}$-vector space.
Let G be a Gröbner basis for $(I, \prec)$. For all $1 \leq i \leq n$, there exists $k_i \in \mathbb{N}$ and $g \in G$ such that $x_i^{k_i} = \mathsf{LM}_{\prec}(g)$.

When $V(I)$ is finite, $\mathsf{HS}_{R/I}(t)$ is a polynomial. Its evaluation at 1 is the degree of I, which coincides with dimension of $\frac{R}{I}$ (as a $\mathbb{K}$ vector space). When I is radical, it coincides with the cardinality of $V(I)$.

Some interesting Hilbert series.

- When $I = \langle R \rangle$, $\mathsf{HS}_{R/I}(t) =?$
- When $I = \langle 0 \rangle$, $\mathsf{HS}_{R/I}(t) =?$
- When $I = \langle x_1, \ldots, x_n \rangle$, $\mathsf{HS}_{R/I}(t) =?$

The hunt of reductions to zero

A crucial activity

☛ The ratio of critical pairs which reduce to 0 tends to 1.

This is observed for all known monomial orderings.

➟ 99% of the runtime is spent in computing 0 (!)

A crucial activity

☛ The ratio of critical pairs which reduce to 0 tends to 1.

This is observed for all known monomial orderings.

➟ 99% of the runtime is spent in computing 0 (!)

Some reductions to 0 arise naturally:

- $f_i f_j = f_j f_i$ yields a reduction to 0 $\rightsquigarrow$ **Syzygies**
- If there exists $h \in R$ such that $hf_i \in \langle f_1, \ldots, f_{i-1} \rangle$ and $h \notin \langle f_1, \ldots, f_{i-1} \rangle$ then a reduction to 0 will occur.

Buchberger's first criterion

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Product criterion (First Buchberger criterion)

Let $G \subset R - \{0\}$ and g_1, g_2 in G. Assume that $\mathsf{lcm}_\prec(f, g) = \mathsf{LM}_\prec(f)\mathsf{LM}_\prec(g)$. Then $\mathrm{spol}_\prec(f, g)$ reduces to 0 modulo G.

Buchberger's first criterion

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ be a an admissible monomial ordering.

Product criterion (First Buchberger criterion)

Let $G \subset R - \{0\}$ and g_1, g_2 in G. Assume that $\mathsf{lcm}_\prec(f, g) = \mathsf{LM}_\prec(f)\mathsf{LM}_\prec(g)$. Then $\mathrm{spol}_\prec(f, g)$ reduces to 0 modulo G.

Proof. Assume $f = \mathsf{LM}_\prec(f) + p$, $g = \mathsf{LM}_\prec(g) + q$. Write
$\mathrm{spol}_\prec(f, g) = pg - qf$.
Observe that $\mathsf{LM}_\prec(\mathrm{spol}(f, g)) = \max_\prec(\mathsf{LM}_\prec(pg), \mathsf{LM}_\prec(qf))$

(using again $\mathsf{lcm}_\prec(f, g) = \mathsf{LM}_\prec(f)\mathsf{LM}_\prec(g)$).

Buchberger's second criterion (I)

Standard representation.

Let $G \subset R - \{0\}$ be a finite set. We say that f has a standard representation w.r.t. $G, \prec$ if:

- $f = \sum_{i=1}^{s} m_i g_i$ for some $m_i \neq 0$ (and the g_i's are pairwise distinct)
- $\max_{\prec}(\mathsf{LM}_{\prec}(m_i g_i), 1 \leq i \leq s) \prec \mathsf{LM}_{\prec}(f)$.

Buchberger's second criterion (I)

Standard representation.

Let $G \subset R - \{0\}$ be a finite set. We say that f has a standard representation w.r.t. $G, \prec$ if:

- $f = \sum_{i=1}^{s} m_i g_i$ for some $m_i \neq 0$ (and the g_i's are pairwise distinct)
- $\max_{\prec}(\mathsf{LM}_{\prec}(m_i g_i), 1 \leq i \leq s) \prec \mathsf{LM}_{\prec}(f)$.

A second characterization of Gröbner bases

Let $G \subset R - \{0\}$ be a finite set. If for any $f \in \langle G \rangle$ with $f \neq 0$, f has a standard representation w.r.t. $G, \prec$ then G is a Gröbner basis for $(\langle G \rangle, \prec)$.

Buchberger's second criterion (II)

Chain criterion (Second Buchberger criterion)

Let f, g and h in R, and $G \subset R - \{0\}$ finite. If

- $\mathsf{LM}_\prec(h)$ divides $\mathrm{lcm}(\mathsf{LM}_\prec(f), \mathsf{LM}_\prec(g))$
- and $\mathrm{spol}_\prec(f, h)$ and $\mathrm{spol}_\prec(g, h)$ both have a standard representation w.r.t G

then $\mathrm{spol}_\prec(f, g)$ has a standard representation w.r.t $G, \prec$.

Buchberger's second criterion (II)

Chain criterion (Second Buchberger criterion)

Let f, g and h in R, and $G \subset R - \{0\}$ finite. If

- $\mathsf{LM}_\prec(h)$ divides $\mathrm{lcm}(\mathsf{LM}_\prec(f), \mathsf{LM}_\prec(g))$
- and $\mathrm{spol}_\prec(f, h)$ and $\mathrm{spol}_\prec(g, h)$ both have a standard representation w.r.t G

then $\mathrm{spol}_\prec(f, g)$ has a standard representation w.r.t $G, \prec$.

➟ $\mathrm{spol}_\prec(f, h)$ and $\mathrm{spol}_\prec(g, h)$ reduce to 0 modulo G, then $\mathrm{spol}_\prec(f, g)$ will reduce to 0 modulo G

Back to the example

We had $\boxed{G = (f_1, f_2, f_3, f_4)}$ with

$\mathsf{LM}(f_1) = x_1^3, \mathsf{LM}(f_2) = x_1^2 x_2, \mathsf{LM}(f_3) = x_1^2, \mathsf{LM}(f_4) = x_1 x_2, \mathsf{LM}(f_5) = x_2^2$

Back to the example

We had $\boxed{G = (f_1, f_2, f_3, f_4)}$ with

$\mathsf{LM}(f_1) = x_1^3, \mathsf{LM}(f_2) = x_1^2 x_2, \mathsf{LM}(f_3) = x_1^2, \mathsf{LM}(f_4) = x_1 x_2, \mathsf{LM}(f_5) = x_2^2$

- (f_3, f_4) reduces to 0 and we know that (f_3, f_5) will reduce to 0.
  ➠ (f_4, f_5) will reduce to 0 (look at the LM's).

Back to the example

We had $\boxed{G = (f_1, f_2, f_3, f_4)}$ with

$\mathsf{LM}(f_1) = x_1^3, \mathsf{LM}(f_2) = x_1^2 x_2, \mathsf{LM}(f_3) = x_1^2, \mathsf{LM}(f_4) = x_1 x_2, \mathsf{LM}(f_5) = x_2^2$

- (f_3, f_4) reduces to 0 and we know that (f_3, f_5) will reduce to 0.
  ➟ (f_4, f_5) will reduce to 0 (look at the LM's).
- The pair (f_3, f_5) can be discarded (but not too early);

Back to the example

We had $\boxed{G = (f_1, f_2, f_3, f_4)}$ with

$\mathsf{LM}(f_1) = x_1^3, \mathsf{LM}(f_2) = x_1^2 x_2, \mathsf{LM}(f_3) = x_1^2, \mathsf{LM}(f_4) = x_1 x_2, \mathsf{LM}(f_5) = x_2^2$

- (f_3, f_4) reduces to 0 and we know that (f_3, f_5) will reduce to 0.
  ➟ (f_4, f_5) will reduce to 0 (look at the LM's).
- The pair (f_3, f_5) can be discarded (but not too early);
- Can you discard more pairs ?

Back to the example

We had $\boxed{G = (f_1, f_2, f_3, f_4)}$ with

$\mathsf{LM}(f_1) = x_1^3, \mathsf{LM}(f_2) = x_1^2 x_2, \mathsf{LM}(f_3) = x_1^2, \mathsf{LM}(f_4) = x_1 x_2, \mathsf{LM}(f_5) = x_2^2$

- (f_3, f_4) reduces to 0 and we know that (f_3, f_5) will reduce to 0.
  ➟ (f_4, f_5) will reduce to 0 (look at the LM's).
- The pair (f_3, f_5) can be discarded (but not too early);
- Can you discard more pairs ?

Gebauer/Möller'88

Improved Buchberger

- $\boldsymbol{f} = (f_1, \ldots, f_s)$ in R
- $\prec$ an admissible monomial order over R

OUTPUT: The reduced Gröbner basis for $(\langle \boldsymbol{f} \rangle, \prec)$.

1. $G \leftarrow \boldsymbol{f}$ and $m \leftarrow s$
2. $\mathscr{P} \leftarrow \emptyset$
3. while $\boldsymbol{f} \neq \emptyset$
   - 3.1 Choose $f \in \boldsymbol{f}, \boldsymbol{f} \setminus \{f\}$
   - 3.2 $(G, \mathscr{P}) \leftarrow$ UPDATE$(f, G, \mathscr{P}, \prec)$
4. while $\mathscr{P} \neq \emptyset$
   - 4.1 select (f, g) from $\mathscr{P}$ and $\mathscr{P} \leftarrow \mathscr{P} \setminus \{(f, g)\}$
   - 4.2 $f_{m+1} \leftarrow$ FULLREDUCTION$(\mathrm{spol}_{\prec}(f, g), G, \prec)$
   - 4.3 if $f_{m+1} \neq 0$ then
     - $m \leftarrow m + 1$
     - $(G, \mathscr{P}) \leftarrow$ UPDATE$(f_m, G, \mathscr{P}, \prec)$
5. return REDUCEBASIS$(G, \prec)$

The Update routine

1. $\mathscr{P}_1 \leftarrow \{(f, g) \mid g \in G\}$
2. $\mathscr{P}_2 \leftarrow \emptyset$ and $\mathscr{P}_2 \leftarrow \emptyset$
3. while $\mathscr{P}_1 \neq \emptyset$
   3.1 select (f, g) from $\mathscr{P}_1$ and $\mathscr{P}_1 \leftarrow \mathscr{P}_1 \setminus \{(f, g)\}$
   3.2 if Criterion1(f, g) or NOT(Criterion2$(f, g, \mathscr{P}_1 \cup \mathscr{P}_2)$)
   3.3 3.3.1
       3.3.2

Change of orderings

The FGLM algorithm