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

Jean-Charles Faugère

Gröbner Bases - Ideals - Varieties

2019 - 2020 – MPRI

informatics mathematics
Inria
SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257
cnrs
dépasser les frontières
www.cnrs.fr

January 26, 2020

Pedagogical Team:

Jean-Charles Faugère	INRIA&CryptoNext
Ludovic Perret	UPMC&CryptoNext

Introduction - Lecture 2-13-1

- Mathematical background (commutative algebra) provided to students as needed.
- Don't hesitate to contact me :

`Jean-Charles.Faugere@inria.fr`

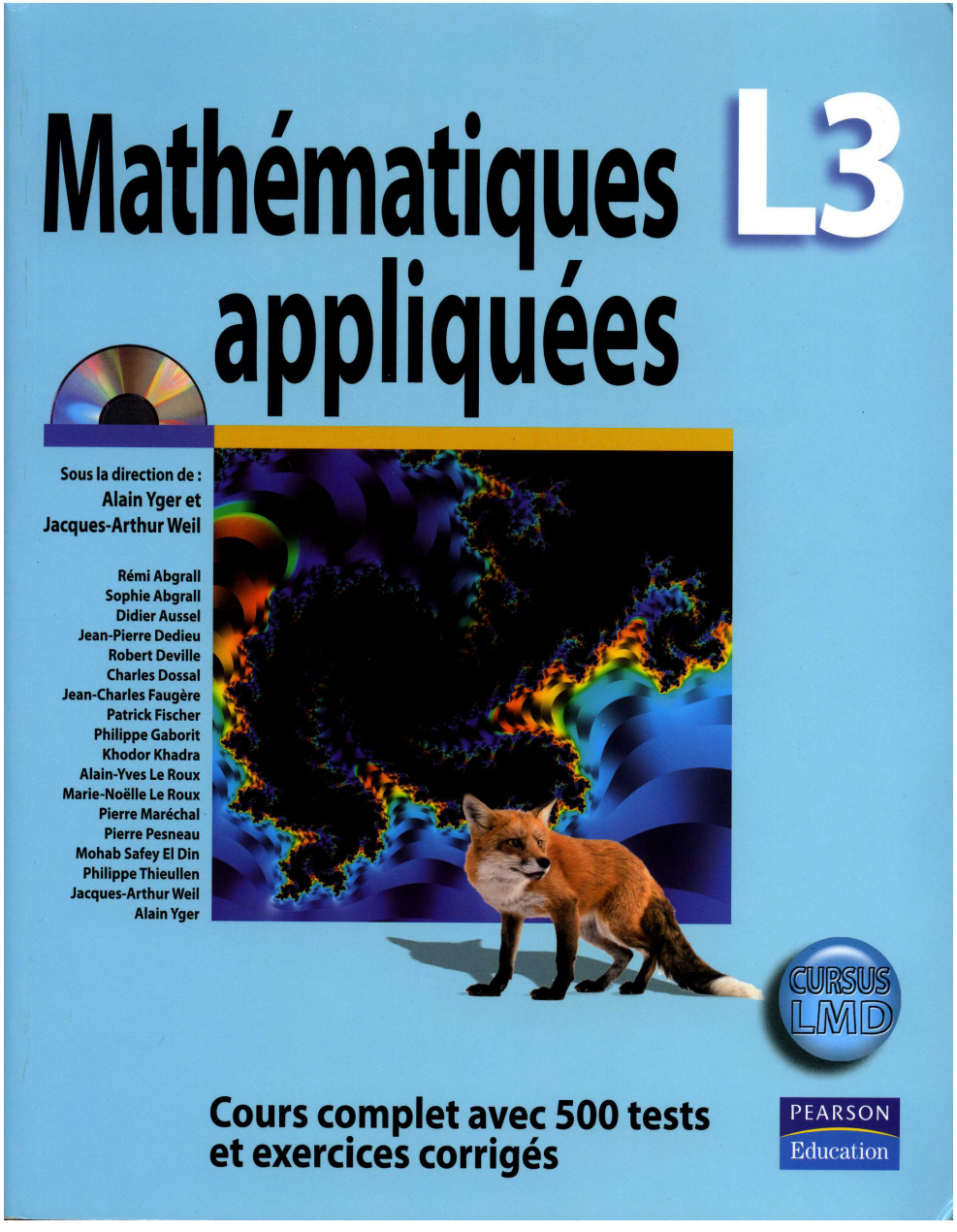
- Lecture $\Longleftrightarrow$ Research : New (published) results are presented.

- **Course Agenda**:

`http://www-polsys.lip6.fr/~jcf/Teaching/index.html`

- Research internships / PhD position: on the Web + contact asap the teachers.

Course Material



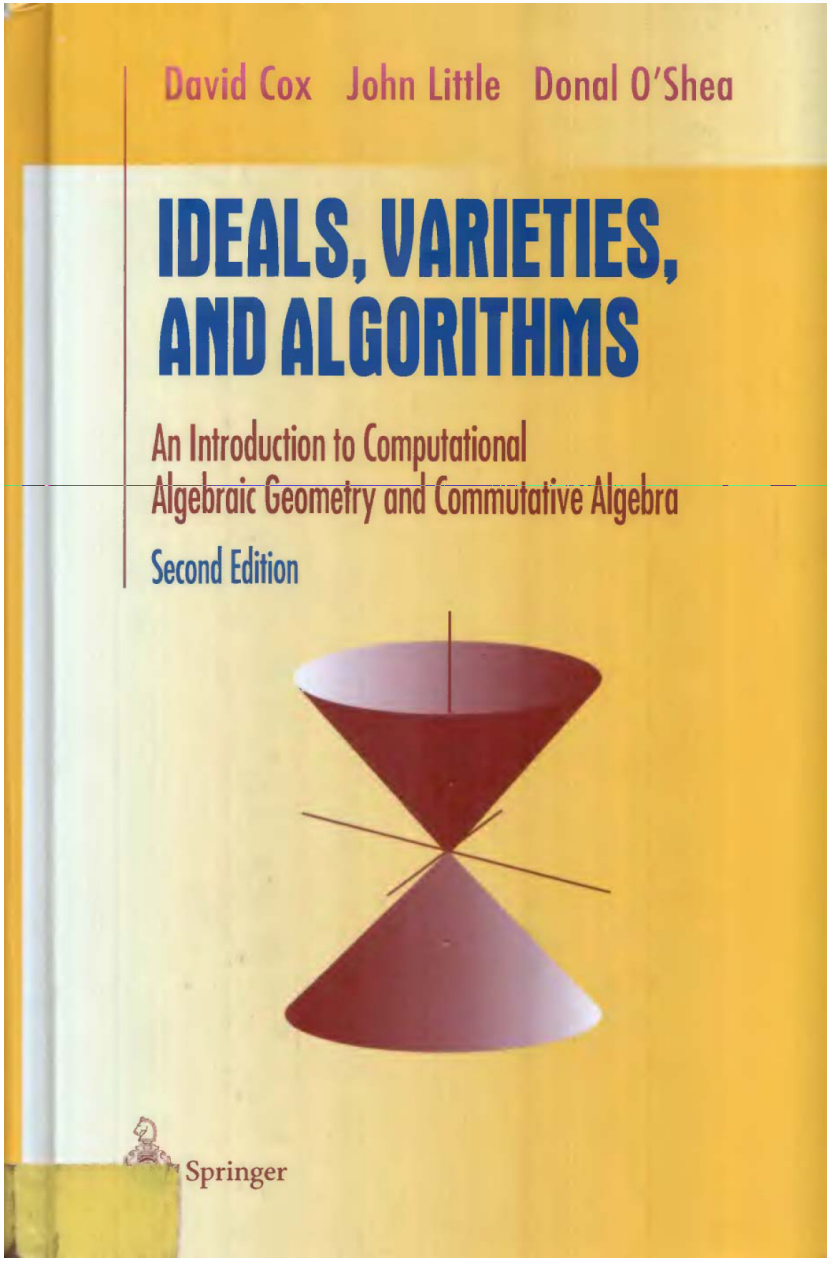
Download Slides

You can download one chapter:

JC Faugère et M Safey El Din

Chapitre d'introduction à la résolution des systèmes polynomiaux (avec exercices)

Course Material



Two main directions

- Computation of Gröbner bases to solve polynomial systems : most important algorithms (will be used in the remaining part of the lecture).
  Recent algorithms rely heavily on linear algebra. Allow us to manipulate efficiently ideals (elimination of variables, projection, intersection, column ideal,. . .).
  Complexity of computing Gröbner bases is also studied.

Two main directions

- Computation of Gröbner bases to solve polynomial systems : most important algorithms (will be used in the remaining part of the lecture).
  Recent algorithms rely heavily on linear algebra. Allow us to manipulate efficiently ideals (elimination of variables, projection, intersection, column ideal,. . .).
  Complexity of computing Gröbner bases is also studied.

- Application in Cryptology : Gröbner bases can be used to design new cryptosystems or evaluate the security of existing cryptosystems (Algebraic Cryptanalysis).
  Polynomial systems are in finite fields and very often they are very structured.
  How to model a problem by a polynomial system is also investigated?
  Last Year (2017): NIST competition - Postquantum Crypto !

Polynomial Systems of Equations

$\mathbb{K}$ a field, $\mathbb{K}[x_1, \ldots, x_n]$ multivariate polynomials in n variables.

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Idea: Reduce the difficult problem (several equations, deg > 1) $\longrightarrow$ easier case (several polynomials in one variable)

Polynomial Systems of Equations

$\mathbb{K}$ a field, $\mathbb{K}[x_1, \ldots, x_n]$ multivariate polynomials in n variables.

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Idea: Reduce the difficult problem (several equations, deg > 1) $\longrightarrow$ easier case (several polynomials in one variable)
Tool: Gröbner bases (rely heavily on linear algebra).

Polynomial Systems of Equations

$\mathbb{K}$ a field, $\mathbb{K}[x_1, \ldots, x_n]$ multivariate polynomials in n variables.

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Idea: Reduce the difficult problem (several equations, $\deg > 1$) $\longrightarrow$ easier case (several polynomials in one variable)
Tool: Gröbner bases (rely heavily on linear algebra).
Combination of the equations:

$$\text{Ideal: } (f_1, \ldots, f_m) \longrightarrow \left\{ \sum_{i=1}^{m} g_i f_i \right\}$$

Property of Gröbner Bases

$\mathbb{K}$ a field, $\mathbb{K}[x_1, \ldots, x_n]$ multivariate polynomials in n variables.

	Linear Systems	Polynomial Equations
Equations	$\begin{cases} l_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ l_m(x_1, \ldots, x_n) = 0 \end{cases}$	
Mathematical	$V = \mathrm{Vect}_{\mathbb{K}}(l_1, \ldots, l_m)$	
Algorithm	Triangular Basis of V	

Definition (Buchberger)

$<$ admissible ordering, $G \subset I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Gröbner basis of the ideal I if

$\forall f \in I$, exists $g \in G$ such that $\mathrm{LT}_<(g) \mid \mathrm{LT}_<(f)$

Property of Gröbner Bases

$\mathbb{K}$ a field, $\mathbb{K}[x_1, \ldots, x_n]$ multivariate polynomials in n variables.

	Linear Systems	Polynomial Equations
Equations	$\begin{cases} l_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ l_m(x_1, \ldots, x_n) = 0 \end{cases}$	$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$
Mathematical	$V = \mathrm{Vect}_{\mathbb{K}}(l_1, \ldots, l_m)$	Ideal generated by f_i: $I = \mathrm{Id}(f_1, \ldots, f_m)$
Algorithm	Triangular Basis of V	Gröbner Basis of I

Definition (Buchberger)

$<$ admissible ordering, $G \subset I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Gröbner basis of the ideal I if

$\forall f \in I$, exists $g \in G$ such that $\mathrm{LT}_<(g) \mid \mathrm{LT}_<(f)$

Property of Gröbner Bases I

Solving polynomial systems: Compute the algebraic variety: $\mathbb{K} \subset \mathbb{L}$ (for instance $\mathbb{L}=\overline{\mathbb{K}}$ the algebraic closure)

$$V_{\mathbb{L}} = \{(z_1, \ldots, z_n) \in \mathbb{L}^n \mid f_i(z_1, \ldots, z_n) = 0, \;\; i = 1, \ldots, m\}$$

Solving in finite field:
Compute the variety $V_{\mathbb{F}_2}$: in that case we have to compute a Gröbner basis of $[f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n]$, in $\mathbb{F}_2[x_1, \ldots, x_n]$.

Theorem

- $V_{\mathbb{F}_2} = \varnothing$ *(no solution) iff* $G_{\mathbb{F}_2} = [1]$.
- $V_{\mathbb{F}_2}$ *has exactly one solution iff* $G_{\mathbb{F}_2} = [x_1 - a_1, \ldots, x_n - a_n]$ *where* $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$.

Property of Gröbner Bases II

Shape position:
If $m \geqslant n$ and the number of solution is finite ($\#V_K < \infty$), then, most of the time, the shape of a Gröbner Basis for a lexicographical ordering $x_1 > \cdots > x_n$ is the following:

$$\text{Shape Position} \begin{cases} h_n(x_n)(=0) \\ x_{n-1} - h_{n-1}(x_n)(=0) \\ \vdots \\ x_1 - h_1(x_n)(=0) \end{cases}$$

Not only a mathematical object! **Algorithm** proposed by B. Buchberger !

Magma (demo)

```
% magma
Magma V2.23-1     Mon Dec  4 2017 07:18:09 on mbpjcf
Type ? for help.  Type <Ctrl>-D to quit.

> K:=GF(65521);
> P<x,y,z>:=PolynomialRing(K,3);

> ll:=[63-85*x^2-55*x*y-37*x*z-35*x+97*y^2+50*y*z+79*y+56*z^2+49*z,
       66+57*x^2-59*x*y+45*x*z-8*x-93*y^2+92*y*z+43*y-62*z^2+77*z,
       -62+54*x^2-5*x*y+99*x*z-61*x-50*y^2-12*y*z-18*y+31*z^2-26*z];

> ll;
[
    65436*x^2 + 65466*x*y + 65484*x*z + 65486*x + 97*y^2 + 50*y*z + 79*y + 56*z^2 + 49*z + 63,
    57*x^2 + 65462*x*y + 45*x*z + 65513*x + 65428*y^2 + 92*y*z + 43*y + 65459*z^2 + 77*z + 66,
    54*x^2 + 65516*x*y + 99*x*z + 65460*x + 65471*y^2 + 65509*y*z + 65503*y + 31*z^2 + 65495*z + 6
]
```

Magma (demo)

```
% magma
Magma V2.23-1     Mon Dec  4 2017 07:18:09 on mbpjcf
Type ? for help.  Type <Ctrl>-D to quit.

> K:=GF(65521);
> P<x,y,z>:=PolynomialRing(K,3);

> ll;
[
    65436*x^2 + 65466*x*y + 65484*x*z + 65486*x + 97*y^2 + 50*y*z + 79*y + 56*z^2 + 49*z + 63,
    57*x^2 + 65462*x*y + 45*x*z + 65513*x + 65428*y^2 + 92*y*z + 43*y + 65459*z^2 + 77*z + 66,
    54*x^2 + 65516*x*y + 99*x*z + 65460*x + 65471*y^2 + 65509*y*z + 65503*y + 31*z^2 + 65495*z + 6
]

> GroebnerBasis(ll);
[
    x + 49346*z^7 + 2875*z^6 + 704*z^5 + 41752*z^4 + 23162*z^3 + 31131*z^2 + 55491*z + 63930,
    y + 46774*z^7 + 34752*z^6 + 52022*z^5 + 59515*z^4 + 63018*z^3 + 50558*z^2 + 10855*z + 30308,
    z^8 + 8137*z^7 + 34304*z^6 + 29170*z^5 + 19881*z^4 + 18888*z^3 + 14650*z^2 + 55269*z + 16459
]
```

Ideals - Varietes

Ideals. Hilbert Basis Theorem I

- Ground field: $\mathbb{K}$ a field.
- Solutions to be found in: field $\mathbb{L} \supseteq \mathbb{K}$.
- $\overline{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$.
- $\mathbb{K}[x_1, \ldots, x_n]$ is the ring of multivariate polynomials.

A polynomial p in $\mathbb{K}[x_1, \ldots, x_n]$ is a sum of monomials:

$$p = \sum_{\alpha \in \mathbf{N}^n} c_\alpha x^\alpha$$

s.t. almost all coefficients are zero.
Power product:

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

If F is a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$, then $\mathrm{Id}(F) = \langle F \rangle$ is the ideal generated by F .

Ideals. Hilbert Basis Theorem II

To any polynomial system of equations

$$S \begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

we associate I the ideal $\mathrm{Id}(f_1, \ldots, f_m) = \langle f_1, \ldots, f_m \rangle$ generated by the input equations.

Solving symbolically such a system is equivalent to find a *simple* set of generators of I.

Theorem (Hilbert)

Every ideal, I of $\mathbb{K}[x_1, \ldots, x_n]$ has a finite generator sets: there are $(g_1, \ldots, g_k) \in I$ such that $I = \mathrm{Id}(g_1, \ldots, g_k)$.

Theorem (Ascending Chain of Ideals)

Let $(I_i)_{i \in \mathbb{N}}$ be an ascending chain of ideals:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Then, there exists an $N \in \mathbb{N}$ such that:

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

Proof.

...

□

Algebraic Varieties, Nullstellensatz

We want to solve a polynomial system of equations: find the roots of the systems:

Definition (Algebraic Variety)

Let $\mathbb{L}$ be field $\mathbb{K} \subset \mathbb{L}$, the algebraic variety associated to the ideal I is the following set:

$$V_{\mathbb{L}}(I) = \{(a_1, \ldots, a_n) \in \mathbb{L}^n \text{ such that } f(a_1, \ldots, a_n) = 0,\ \forall f \in I\}$$

Algebraic Varieties, Nullstellensatz

We want to solve a polynomial system of equations: find the roots of the systems:

Definition (Algebraic Variety)

Let $\mathbb{L}$ be field $\mathbb{K} \subset \mathbb{L}$, the algebraic variety associated to the ideal I is the following set:

$$V_{\mathbb{L}}(I) = \{(a_1, \ldots, a_n) \in \mathbb{L}^n \text{ such that } f(a_1, \ldots, a_n) = 0,\ \forall f \in I\}$$

For instance if $\mathbb{K} = \mathbb{Q}$:

- sometimes we look for the complex solutions in

$$V_{\mathbb{C}}(I)$$

- sometimes we want to restrict ourselves to real roots:

$$V_{\mathbb{R}}(I) = V_{\mathbb{C}}(I) \cap \mathbb{R}^n.$$

Algebraic Varieties, Nullstellensatz

We want to solve a polynomial system of equations: find the roots of the systems:

Definition (Algebraic Variety)

Let $\mathbb{L}$ be field $\mathbb{K} \subset \mathbb{L}$, the algebraic variety associated to the ideal I is the following set:

$$V_{\mathbb{L}}(I) = \{(a_1, \ldots, a_n) \in \mathbb{L}^n \text{ such that } f(a_1, \ldots, a_n) = 0,\ \forall f \in I\}$$

Example

If $I = \langle x^2 + 1 \rangle$ then

$$V_{\mathbb{C}}(I) = \{\imath, -\imath\}$$
$$V_{\mathbb{R}}(I) = \varnothing$$

If $S = (f_1, \ldots, f_m)$ is the algebraic system to solve, we can consider two mathematical objects associated to S:

- the ideal $I = \mathrm{Id}(f_1, \ldots, f_m)$.
- the variety $V_{\bar{\mathbb{K}}}(I)$

If $S = (f_1, \ldots, f_m)$ is the algebraic system to solve, we can consider two mathematical objects associated to S:

- the ideal $I = \mathrm{Id}(f_1, \ldots, f_m)$.
- the variety $V_{\bar{\mathbb{K}}}(I)$

Remark Variety $\neq$ Ideal !

In some sense extra data can be encoded in the ideal I.
For instance if we compare the following two systems (one variable, one equation):

$x_1^2 = 0$ the associated ideal is $I_1 = \mathrm{Id}(x_1^2)$
$x_1 = 0$ the associated ideal is $I_2 = \mathrm{Id}(x_1) \neq I_1$.

But the algebraic variety is the same: $V_{\mathbb{C}}(I_1) = V_{\mathbb{C}}(I_2) = \{0\}$

The notion of **multiplicity** is lost in the algebraic variety.

The Weak NullStellenSatz

Null=zero Stellen=places Satz=Theorem

The following theorem allow us to have a criterion on the ideal to guarantee that the set of roots of a polynomial system is not empty (in the algebraic closure):

Theorem (The Weak Nullstellensatz)

If $f_1, \cdots, f_m$ *are polynomials in* $\mathbb{K}[x_1, \ldots, x_n]$ *and* $I = \mathrm{Id}(f_1, \cdots, f_m)$ *then* $V_{\bar{\mathbb{K}}}(I) = \varnothing$ *implies that* $I = \mathrm{Id}(1) = \mathbb{K}[x_1, \ldots, x_n]$.

Proof.

See the proof in Cox Little O'Shea page 169. □

Ideal associated to points

Reciprocally, to a set of points we can associate an ideal:

Definition

If W is a subset of $\mathbb{K}^n$ we define the following set

$$I(W) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in W\}.$$

$I(W)$ is an ideal.

Hilbert Nullstellensatz

If a multivariate polynomial f vanishes on all the points of an algebraic variety $V(I)$, this **does not imply necessarily that** $f \in I$ but some power of f is in I :

Theorem (Hilbert Nullstellensatz)

$\mathbb{K}$ is an algebraically closed field.
If $f, f_1, \cdots, f_m$ are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ then
$f \in I(V_{\mathbb{K}}(\mathrm{Id}(f_1, \cdots, f_m)))$ implies that there exists $k \in \mathbb{N}$ such that
$f^k \in \mathrm{Id}(f_1, \cdots, f_m)$.

Hilbert Nullstellensatz

Theorem (Hilbert Nullstellensatz)

$\mathbb{K}$ is an algebraically closed field.
If $f, f_1, \cdots, f_m$ are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ then
$f \in I(V_{\mathbb{K}}(\mathrm{Id}(f_1, \cdots, f_m)))$ implies that there exists $k \in \mathbb{N}$ such that
$f^k \in \mathrm{Id}(f_1, \cdots, f_m)$.

Definition (Radical of an ideal)

If I is an ideal, then following set

$$\sqrt{I} = \left\{ f \in \mathbb{K}[x_1, \ldots, x_n] \mid \exists k \in \mathbb{N} \text{ such that } f^k \in I \right\}$$

is an a ideal: we call it the radical of I.

Hilbert Nullstellensatz

Theorem (Hilbert Nullstellensatz)

$\mathbb{K}$ is an algebraically closed field.
If $f, f_1, \cdots, f_m$ are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ then
$f \in I(V_{\mathbb{K}}(\mathrm{Id}\,(f_1, \cdots, f_m)))$ implies that there exists $k \in \mathbb{N}$ such that
$f^k \in \mathrm{Id}\,(f_1, \cdots, f_m)$.

Definition (Radical of an ideal)

If I is an ideal, then following set

$$\sqrt{I} = \left\{ f \in \mathbb{K}[x_1, \ldots, x_n] \mid \exists k \in \mathbb{N} \text{ such that } f^k \in I \right\}$$

is an a ideal: we call it the radical of I.

Example (radical)

If $I = \langle x^2 y \rangle$ then $\sqrt{I} = \langle xy \rangle$
If $I = \langle x^2 y, xy^2 \rangle$ then $\sqrt{I} = \langle xy \rangle$

Ideal variety correspondence

Theorem

1. *If $\mathbb{K}$ is an algebraic close field and I an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ then*

$$I(V_{\mathbb{K}}(I)) = \sqrt{I}$$

2. *If V is an algebraic variety over $\mathbb{K}$ then*

$$V_{\mathbb{K}}(I(V)) = V$$

Ideal variety correspondence

Theorem

1. *If $\mathbb{K}$ is an algebraic close field and I an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ then*

$$I(V_{\mathbb{K}}(I)) = \sqrt{I}$$

2. *If V is an algebraic variety over $\mathbb{K}$ then*

$$V_{\mathbb{K}}(I(V)) = V$$

Consequence of this theorem: any question about varieties can be *rephrased* as an algebraic question about radical ideals and conversely (assuming that $\mathbb{K}$ is an algebraically closed field).

Prime ideals - Irreducible Varieties

Union of two varieties is an algebraic variety.
Conversely, we can split a variety into a union of irreducible varieties.

Prime ideals - Irreducible Varieties

Union of two varieties is an algebraic variety.
Conversely, we can split a variety into a union of irreducible varieties.

Definition (Irreducible Variety)

A variety V is irreducible if whenever V is written in the form $V = V_1 \cup V_2$ where V_1 and V_2 are varieties, then either $V = V_1$ or $V = V_2$.

Prime ideals - Irreducible Varieties

Union of two varieties is an algebraic variety.
Conversely, we can split a variety into a union of irreducible varieties.

Definition (Irreducible Variety)

A variety V is irreducible if whenever V is written in the form $V = V_1 \cup V_2$ where V_1 and V_2 are varieties, then either $V = V_1$ or $V = V_2$.

Definition (Prime Ideal)

An ideal I of $\mathbb{K}[x_1, \ldots, x_n]$ is *prime* if $f \cdot g \in I$ implies $f \in I$ or $g \in I$.

Prime ideals - Irreducible Varieties

Union of two varieties is an algebraic variety.
Conversely, we can split a variety into a union of irreducible varieties.

Definition (Irreducible Variety)

A variety V is irreducible if whenever V is written in the form $V = V_1 \cup V_2$ where V_1 and V_2 are varieties, then either $V = V_1$ or $V = V_2$.

Definition (Prime Ideal)

An ideal I of $\mathbb{K}[x_1, \ldots, x_n]$ is *prime* if $f \cdot g \in I$ implies $f \in I$ or $g \in I$.

Proposition

Let V be an algebraic variety then V is irreducible if and only if $I(V)$ is prime.

Decompositions

Theorem

If I is an ideal, then there are $P_1, \ldots, P_k$ prime ideals such that :

$$\sqrt{I} = \bigcap_{i=1}^{k} P_i$$

If V is an algebraic variety, then there are $V_1, \ldots, V_k$ irreducible algebraic varieties such that :

$$V = \bigcup_{i=1}^{k} V_i$$

Decompositions

Theorem

If I is an ideal, then there are $P_1, \ldots, P_k$ prime ideals such that :

$$\sqrt{I} = \bigcap_{i=1}^{k} P_i$$

If V is an algebraic variety, then there are $V_1, \ldots, V_k$ irreducible algebraic varieties such that :

$$V = \bigcup_{i=1}^{k} V_i$$

Example

$I = \langle x\,y + 1 \rangle$ is a prime ideal in $\mathbb{Q}[x]$
$I = \langle x\,y \rangle$ is note since it can be written $I = \langle x \rangle \cap \langle y \rangle$.

Gröbner Bases

Gröbner Bases - Admissible Orderings

Describe an analog of the Gauß' algorithm for multivariate polynomials.

☞ define a monomial ordering so that we can define the leading monomial of a polynomial: $T(x_1, \ldots, x_n) = T$ is the set of terms that can be obtained from the variables $(x_1, \ldots, x_n)$.

Power product:

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in T \text{ where } \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$$

$\deg(\mathbf{x}^\alpha)$ is the *total degree* of $\mathbf{x}^\alpha$:

$$\deg(\mathbf{x}^\alpha) = \sum_{i=1}^{n} \alpha_i$$

Admissible Orderings I

Definition (Admissible monomial ordering)

Let $<$ be a total order of $T \approx \mathbb{N}^n$; $<$ is an admissible monomial ordering if the following conditions are satisfied:

(i) $0 \leqslant \alpha$ for all $\alpha \in T$.

(ii) $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$ for all $\gamma \in T$
(the ordering is compatible with multiplication).

(iii) there is no infinite strictly decreasing sequence $(\alpha_i)_{i \in \mathbb{N}}$.

Useful monomial orderings: lexicographical, DRL(grevlex), ... (the shape of Gröbner basis will be related to the choice of the ordering).

***Lexicographical* monomial ordering**

$$x^{\alpha} = x^{(\alpha_1,\ldots,\alpha_n)} <_{\text{Lex}} x^{\beta} = x^{(\beta_1,\ldots,\beta_n)} \text{ if } \exists\, i \text{ such that } \begin{cases} \alpha_j = \beta_j & \text{for} \quad j < i \\ \alpha_i < \beta_i \end{cases}$$

Admissible Orderings II

Degre-Lexicographical monomial ordering

$$x^{\alpha} = x^{(\alpha_1,\ldots,\alpha_n)} <_{\text{Deg}} x^{\beta} = x^{(\beta_1,\ldots,\beta_n)} \text{ if } \begin{cases} \alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n \\ \text{or} \\ \alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n \\ \text{and} \begin{cases} \alpha_j = \beta_j & \text{for } \ j < i \\ \alpha_i < \beta_i \end{cases} \end{cases}$$

Admissible Orderings III

The most efficient monomial ordering (see [4]) is:

Degre-Reverse-Lexicographical (DRL)monomial ordering:

$$x^{\alpha} = x^{(\alpha_1,\ldots,\alpha_n)} <_{\mathrm{DRL}} x^{\beta} = x^{(\beta_1,\ldots,\beta_n)} \text{ if } \begin{cases} \alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n \\ \text{or} \\ \alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n \\ \text{and} \begin{cases} \alpha_j = \beta_j & \text{for} \quad j > i \\ \alpha_i > \beta_i \end{cases} \end{cases}$$

Admissible Orderings IV

Block orderings

Split the set of variables $X = [x_1, \ldots, x_n]$ into two blocks

$$X = X_1 \cup X_2$$

where $X_1 = [x_1, \ldots, x_i]$ and $X_2 = [x_{i+1}, \ldots, x_n]$.
Given two admissible monomial orderings $<_1$ over $\mathbb{N}^i$ and $<_2$ over $\mathbb{N}^{n-i}$ we can build a new ordering:

$$x^\alpha = x^{(\alpha_1,\ldots,\alpha_n)} <_{X_1,X_2} x^\beta = x^{(\beta_1,\ldots,\beta_n)} \text{ if } \begin{cases} x^{(\alpha_1,\ldots,\alpha_i)} <_1 x^{(\beta_1,\ldots,\beta_i)} \\ \text{or} \\ \begin{cases} (\alpha_1,\ldots,\alpha_i) = (\beta_1,\ldots,\beta_i) \\ \text{and } x^{(\alpha_{i+1},\ldots,\alpha_n)} <_2 x^{(\beta_{i+1},\ldots,\beta_n)} \end{cases} \end{cases}$$

Support of a polynomial

Monomial ordering $<$ is fixed.

Let $f \in \mathbb{K}[x_1, \ldots, x_n]$, $f \neq 0$, such that $f = \sum c(\alpha_1, \ldots, \alpha_n) x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ (where $c(\alpha_1, \ldots, \alpha_n)$ is an element of $\mathbb{K}$).

The set $M(f)$ of monomials of f (the support of f) is:

$$M(f) = \left\{ c(\alpha_1, \ldots, \alpha_n) x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid c(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

The set $T(f)$ of terms of f is:

$$T(f) = \left\{ x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid c(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

Leading terms, Leading Monomials,...

The *total degree* of $f \neq 0$ is $\deg(f) = \max\{\deg(t) \mid t \in T(f)\}$.

Definition

The leading term $\mathrm{LT}_<(f)$, (resp. the *leading monomial* $\mathrm{LM}_<(f)$, the *leading coefficient coefficient* $\mathrm{LC}_<(f)$) of f w.r.t. $<$:

$$\mathrm{LT}_<(f) = \max_<(T(f)) \text{ and } \mathrm{LM}_<(f) = \max_<(M(f))$$

$\mathrm{LC}_<(f)$ is the coefficient of $\mathrm{LM}_<(f)$.

Leading terms, Leading Monomials,...

The *total degree* of $f \neq 0$ is $\deg(f) = \max\{\deg(t) \mid t \in T(f)\}$.

Definition

The leading term $\mathrm{LT}_<(f)$, (resp. the *leading monomial* $\mathrm{LM}_<(f)$, the *leading coefficient coefficient* $\mathrm{LC}_<(f)$) of f w.r.t. $<$:

$$\mathrm{LT}_<(f) = \max_<(T(f)) \text{ and } \mathrm{LM}_<(f) = \max_<(M(f))$$

$\mathrm{LC}_<(f)$ is the coefficient of $\mathrm{LM}_<(f)$.

Example Assuming $x > y$

$$f = 2x^2y^2 + 3xy^2 + 5$$
$$\mathrm{LT}(f) = ?$$
$$\mathrm{LC}(f) = ?$$
$$\mathrm{LM}(f) = ?$$

Leading terms, Leading Monomials,...

The *total degree* of $f \neq 0$ is $\deg(f) = \max\{\deg(t) \mid t \in T(f)\}$.

Definition

The leading term $\mathrm{LT}_<(f)$, (resp. the *leading monomial* $\mathrm{LM}_<(f)$, the *leading coefficient coefficient* $\mathrm{LC}_<(f)$) of f w.r.t. $<$:

$$\mathrm{LT}_<(f) = \max_<(T(f)) \text{ and } \mathrm{LM}_<(f) = \max_<(M(f))$$

$\mathrm{LC}_<(f)$ is the coefficient of $\mathrm{LM}_<(f)$.

Example Assuming $x > y$

$$f = \boxed{2x^2y^2} + 3xy^2 + 5$$
$$\mathrm{LT}(f) = x^2y^2$$
$$\mathrm{LC}(f) = 2$$
$$\mathrm{LM}(f) = \mathrm{LC}(f)\ \mathrm{LT}(f) = 2x^2y^2$$

First Try

We have polynomials and we try to eliminate the leading terms . . .

Example

$$f = 2xy^2 + 3$$
$$g = 7xy + 2x + 4$$

Easy to kill the LT of f: compute $f - \frac{2}{7}\, y\, g$ ☞ Reduction of f by g

Example

$$f = 2xy^2 + 3$$
$$g = 7x^2y + 2x + 4$$

Kill the LT of f or g ? ☞ Notion of critical pairs

Lcm of polynomials

$$\mathrm{Id}(\mathbf{x}^{\alpha}) \cap \mathrm{Id}(\mathbf{x}^{\beta}) \quad =?$$

Lcm of polynomials

$$\begin{aligned} \mathrm{Id}(\mathbf{x}^{\alpha}) \cap \mathrm{Id}(\mathbf{x}^{\beta}) &= ? \\ &= \mathrm{lcm}(\mathbf{x}^{\alpha}, \mathbf{x}^{\beta}) \qquad \text{(principal ideal)} \end{aligned}$$

Lcm of polynomials

$$\mathrm{Id}(\mathbf{x}^\alpha) \cap \mathrm{Id}(\mathbf{x}^\beta) \quad =?$$
$$= \mathrm{lcm}(\mathbf{x}^\alpha, \mathbf{x}^\beta) \qquad \text{(principal ideal)}$$

Definition

We define the lcm of two terms by:

$$\mathrm{lcm}(\mathbf{x}^\alpha, \mathbf{x}^\beta) = x_1^{\max(\alpha_1,\beta_1)} \cdots x_n^{\max(\alpha_n,\beta_n)}$$

If $<$ is a monomial ordering we define

$$\mathrm{lcm}(f, g) = \mathrm{lcm}(\mathrm{LT}_<(f), \mathrm{LT}_<(g))$$

where f and g are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.

Lcm of polynomials

Definition

We define the lcm of two terms by:

$$\operatorname{lcm}(\mathbf{x}^{\alpha}, \mathbf{x}^{\beta}) = x_1^{\max(\alpha_1,\beta_1)} \cdots x_n^{\max(\alpha_n,\beta_n)}$$

If $<$ is a monomial ordering we define

$$\operatorname{lcm}(f, g) = \operatorname{lcm}(\operatorname{LT}_<(f), \operatorname{LT}_<(g))$$

where f and g are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.

Example

$$f = 2xy^2 + 3$$
$$g = 7x^2y + 2x + 4$$
$$lcm(f, g) = x^2y^2$$

Kill the LT of f and g ?

Main Concept for computing Gröbner Bases

A fundamental notion used in the description (and the proof) of the Buchberger algorithm is the notion of of polynomials (f, g):

Definition

We define the S-polynomial of a critical pair (f, g) by:

$$\mathrm{S(f,g)} = \mathrm{Spol}(f,g) = \frac{\mathrm{lcm}(f,g)}{\mathrm{LM}(f)} f - \frac{\mathrm{lcm}(f,g)}{\mathrm{LM}(g)} g$$

Reduction of a polynomial

We will introduce two notions of reduction of a polynomial f by a polynomial p.

We have to distinguish the mathematical notion of reduction

$$f \xrightarrow{p} g$$

(car be rephrased by f *could be reduce in* g modulo p) and the algorithmic (and deterministic) definition

$$g := \text{REDUCTION}(f, p).$$

Reduction of a polynomial

Definition

$(f, g, p) \in \mathbb{K}[x_1, \ldots, x_n]^3$ and $P \subset \mathbb{K}[x_1, \ldots, x_n]$:

- *f reduces to g modulo p* (notation $f \xrightarrow{p} g$), if there exists $t \in T(f)$, and $s \in T$ such that $s\,\mathrm{LT}(p) = t$ and $g = f - \frac{a}{\mathrm{LC}(p)}\, s\, p$ where a is the cofficient of t in f.
- *f reduces to g modulo P* (notation $f \xrightarrow{P} g$), if $f \xrightarrow{p} g$ for some $p \in P$.
- *f is reducible modulo p* if there exists $g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f \xrightarrow{p} g$.
- *f is reducible modulo P* if there exists $g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f \xrightarrow{P} g$.
- *f is top reducible modulo P* if there exists $g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f \xrightarrow{P} g$ and $\mathrm{LT}(g) < \mathrm{LT}(f)$.
- $f \xrightarrow[P]{*} g$ is the reflexive-transitive closure of $\longrightarrow$.

Polynomial Reduction : the algorithm

Algorithm (REDUCTION)

Input: $\begin{cases} p \text{ a polynomial} \\ F = [f_1, \ldots, f_m] \text{ a list of polynomials} \\ < \text{ monomial (admissible) ordering} \end{cases}$

Output: a reduced polynomial.

if $p = 0$ **then**
  return p
for $i := 1$ **to** m **do**
  if $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ **then**
    return REDUCTION$(p - \frac{\mathrm{LM}(p)}{\mathrm{LM}(f_i)} f_i, F)$
return p

Polynomial Reduction:properties

Proposition

The previous algorithm terminates.

Proposition

If $r = \text{REDUCTION}(p, F)$ *then* $r - p \in \mathrm{Id}(F)$

Corollary

If $r = \text{REDUCTION}(p, F)$ *then there are two finite sequences* $(g_i)_{i=1,\ldots,k}$ *and* $(m_i)_{i=1,\ldots,k}$ *of monomials such that* $g_i \in F$ *and* $r - p = \sum_{i=1}^{k} m_i g_i$ *with* $\mathrm{LT}(p) = \mathrm{LT}(m_1 g_1) > \mathrm{LT}(m_2 g_2) > \cdots > \mathrm{LT}(m_k g_k)$

Proposition

The map $\varphi : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[x_1, \ldots, x_n]$, *defined by* $\varphi(p) = \text{REDUCTION}(p, F)$ *is a linear map and* $\mathrm{Ker}(\varphi) \subset \mathrm{Id}(F)$ *(but we have note necessarily equality).*

Reduction : example

Note that the reduction of a polynomial by a list of polynomials is usually not unique and that the result depends on the order of polynomials in F.

Example

This is an example where the result may change depending on the order of the polynomials: $f = X^2 + X, f_1 = X^2 + 1, f_2 = X + 2$ (the monomial order is the lexicographical ordering).

1. REDUCTION$(f, [f_1, f_2], <)$: f is top-reducible modulo $[f_1, f_2]$ sice $\mathrm{LM}(f_1) = X^2$ divides $\mathrm{LM}(f) = X^2$.
   We compute $f' := f - \frac{1}{1} f_1 = X - 1$; again f' is top-reducible modulo $[f_1, f_2]$ sice $\mathrm{LM}(f_2) = X$ divides $\mathrm{LM}(f') = X$.
   We compute $f'' := f' - \frac{1}{1} f_2 = -3$; the algorithm stops since $\mathrm{LM}\left(f''\right) = 1$ is non longer reducible.

2. REDUCTION$(f, [f_2, f_1], <)$

Reduction : example

Note that the reduction of a polynomial by a list of polynomials is usually not unique and that the result depends on the order of polynomials in F.

Example

This is an example where the result may change depending on the order of the polynomials: $f = X^2 + X, f_1 = X^2 + 1, f_2 = X + 2$.

1. $\text{REDUCTION}(f, [f_1, f_2], <) := -3$

2. $\text{REDUCTION}(f, [f_2, f_1], <)$: now $\text{LM}(f_2) = X$ divides $\text{LM}(f) = X^2$. We compute $f' := f - \frac{X}{1} f_2 = X - 2X = -X$; again, $\text{LM}(f_2) = X$ divides $\text{LM}(f') = X$ and we compute $f'' := f' - \frac{-1}{1} f_2 = 2$; the algorithm stops since $\text{LM}\left(f''\right) = 1$ is non longer top reducible.

Reduction : example

Note that the reduction of a polynomial by a list of polynomials is usually not unique and that the result depends on the order of polynomials in F.

Example

This is an example where the result may change depending on the order of the polynomials: $f = X^2 + X, f_1 = X^2 + 1, f_2 = X + 2$.

1. $\text{REDUCTION}(f, [f_1, f_2], <) := -3$
2. $\text{REDUCTION}(f, [f_2, f_1], <) := 2$

We have:

$$\text{REDUCTION}(f, [f_1, f_2], <) = -3 \neq 2 = \text{REDUCTION}(f, [f_2, f_1], <).$$

Reduction : example

Note that the reduction of a polynomial by a list of polynomials is usually not unique and that the result depends on the order of polynomials in F.

Example

This is an example where the result may change depending on the order of the polynomials: $f = X^2 + X, f_1 = X^2 + 1, f_2 = X + 2$.

1. $\text{REDUCTION}(f, [f_1, f_2], <) := -3$
2. $\text{REDUCTION}(f, [f_2, f_1], <) := 2$

Using the mathematical definition we have simultaneously:
$f \xrightarrow[[f_1,f_2]]{*} -3$ and $f \xrightarrow[[f_1,f_2]]{*} 2$.

Full Reduction I

REDUCTION "simplifies" as much as possible the leading monomial of a polynomial.
FULLREDUCTION reduce *all the monomials* :

Algorithm (FULLREDUCTION)

Input: $\begin{cases} p \text{ a polynomial} \\ F = [f_1, \ldots, f_m] \text{ a list of polynomials} \\ < \text{ admissible ordering} \end{cases}$
Output: a totally reduced polynomial.
$q := 0$
while $p \neq 0$ **do**
  $p :=$REDUCTION(p, F)
  $q := q + \mathrm{LM}(p)$
  $p := p - \mathrm{LM}(p)$
return q

Full Reduction II

Proposition

The algorithm FULLREDUCTION *terminates.*

Proposition

If $p =$FULLREDUCTION(f, F) *then* $T(p) \cap \mathrm{Id}(\mathrm{LT}(F)) = \varnothing$

Proposition

If $r =$FULLREDUCTION(p, F) *then* $r - p \in \mathrm{Id}(F)$

Gröbner Bases

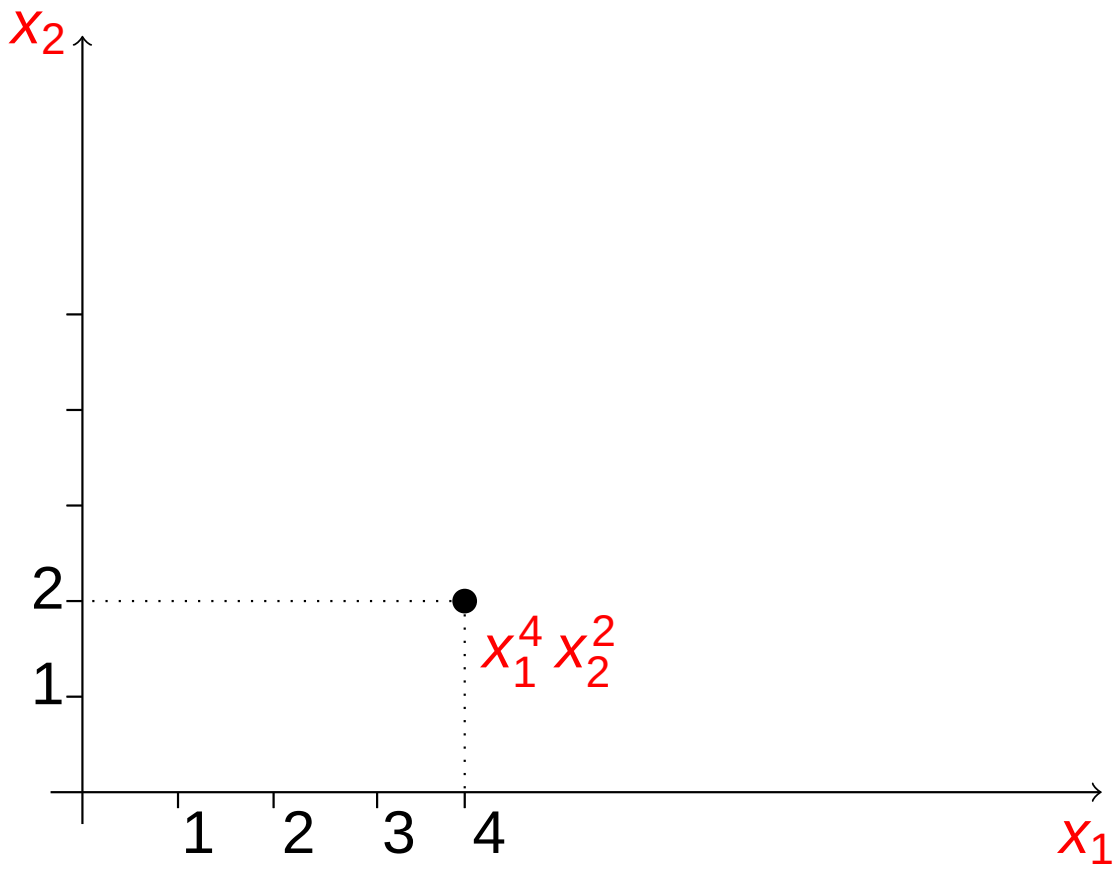
The following definition is pure mathematical and thus we can a Gröbner basis independently from any algorithm.
Gröbner bases can be computed using several algorithms.

Definition Gröbner Basis (Buchberger)

Let I be an ideal.
A finite subset $G = [g_1, \ldots, g_k]$ of I is a Gröbner of I wrt the admissible monomial ordering $<$
if for any $f \in I$ there exists $i \in \{1, \ldots, k\}$ such that $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(f)$.

Gröbner Bases

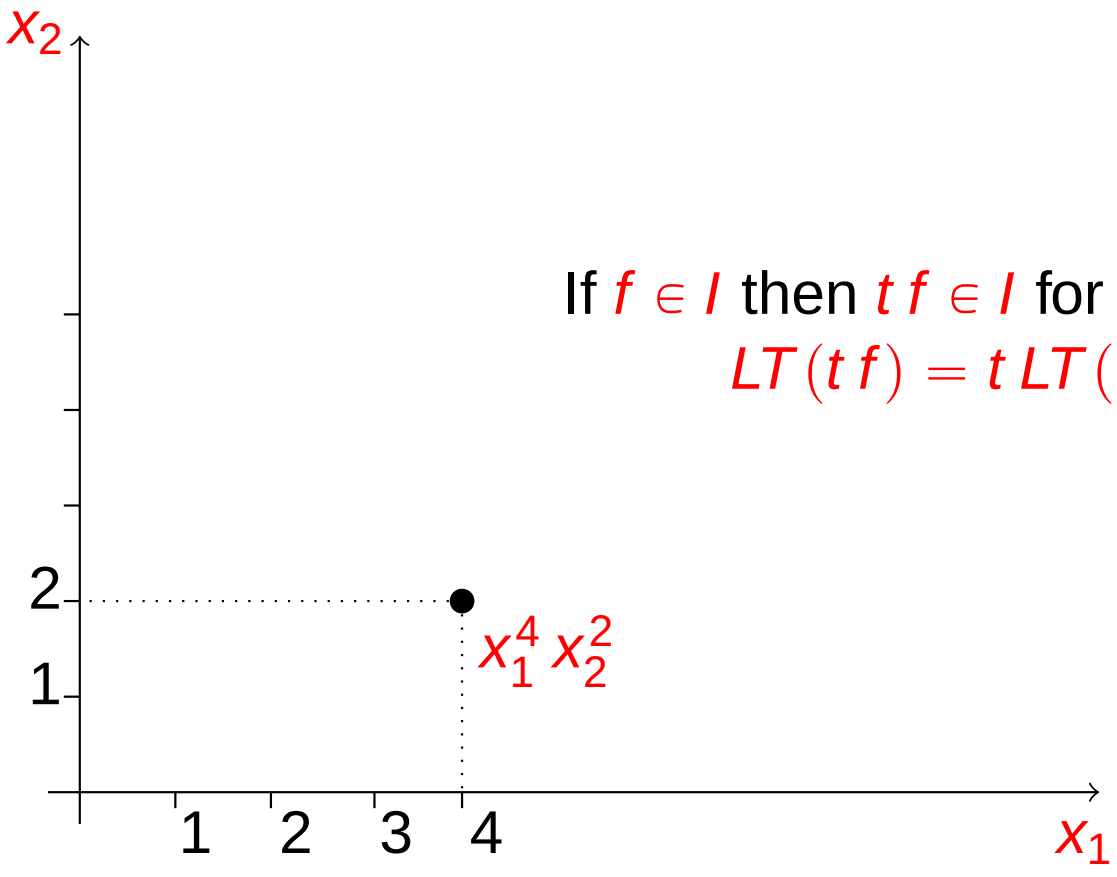
For any $f \in I$ we draw the point $\mathrm{LT}(f) \in \mathbb{N}^n$:



The staircase of a Gröbner basis.

Gröbner Bases

For any $f \in I$ we draw the point $\mathrm{LT}(f) \in \mathbb{N}^n$:



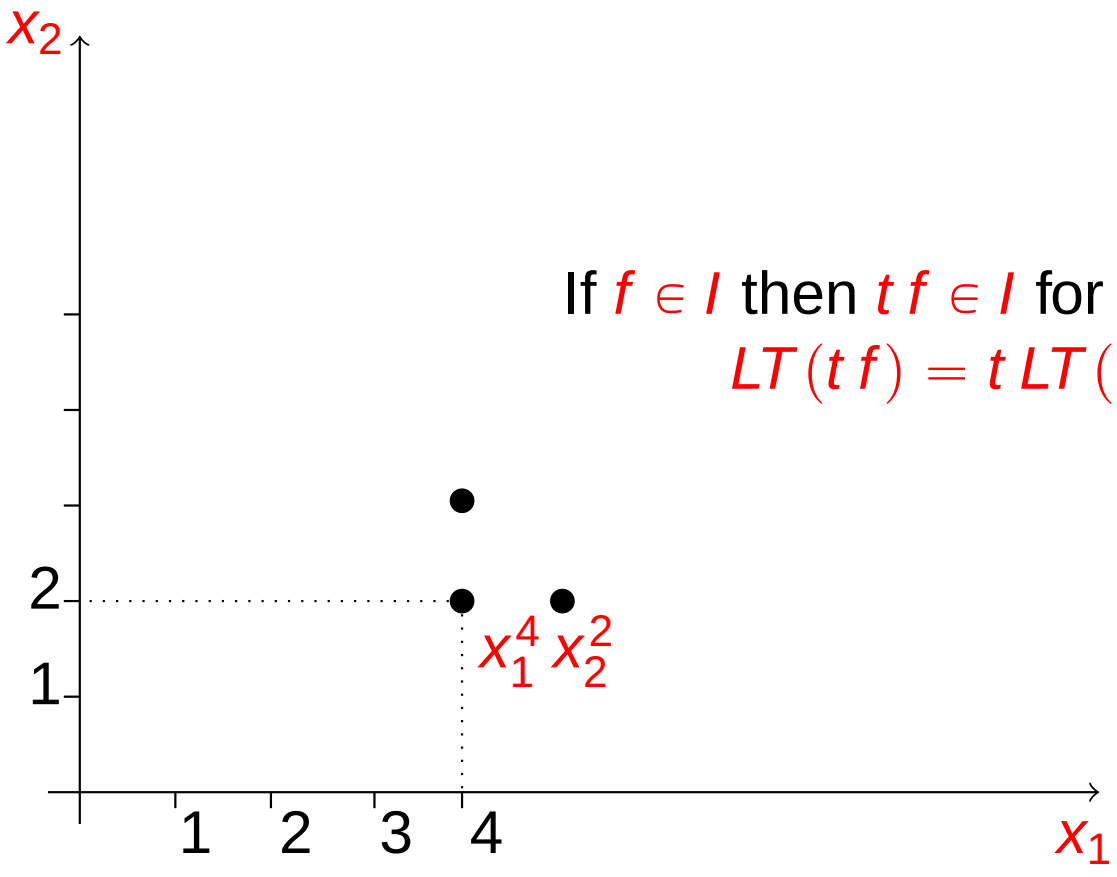
If $f \in I$ then $t\, f \in I$ for all $t \in T$

$$LT(t\, f) = t\, LT(f)$$

The staircase of a Gröbner basis.

Gröbner Bases

For any $f \in I$ we draw the point $\mathrm{LT}(f) \in \mathbb{N}^n$:



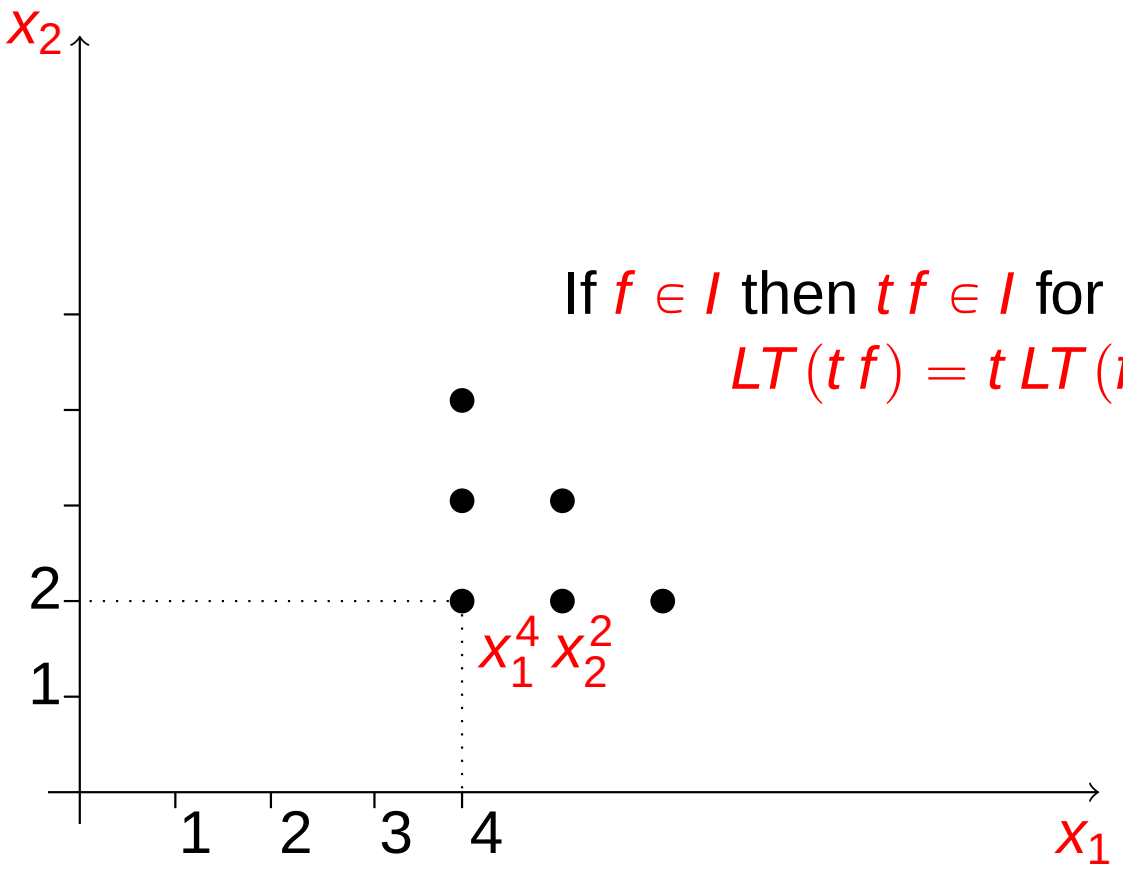
If $f \in I$ then $t\,f \in I$ for all $t \in T$

$$LT(t\,f) = t\,LT(f)$$

The staircase of a Gröbner basis.

Gröbner Bases

For any $f \in I$ we draw the point $\mathrm{LT}(f) \in \mathbb{N}^n$:



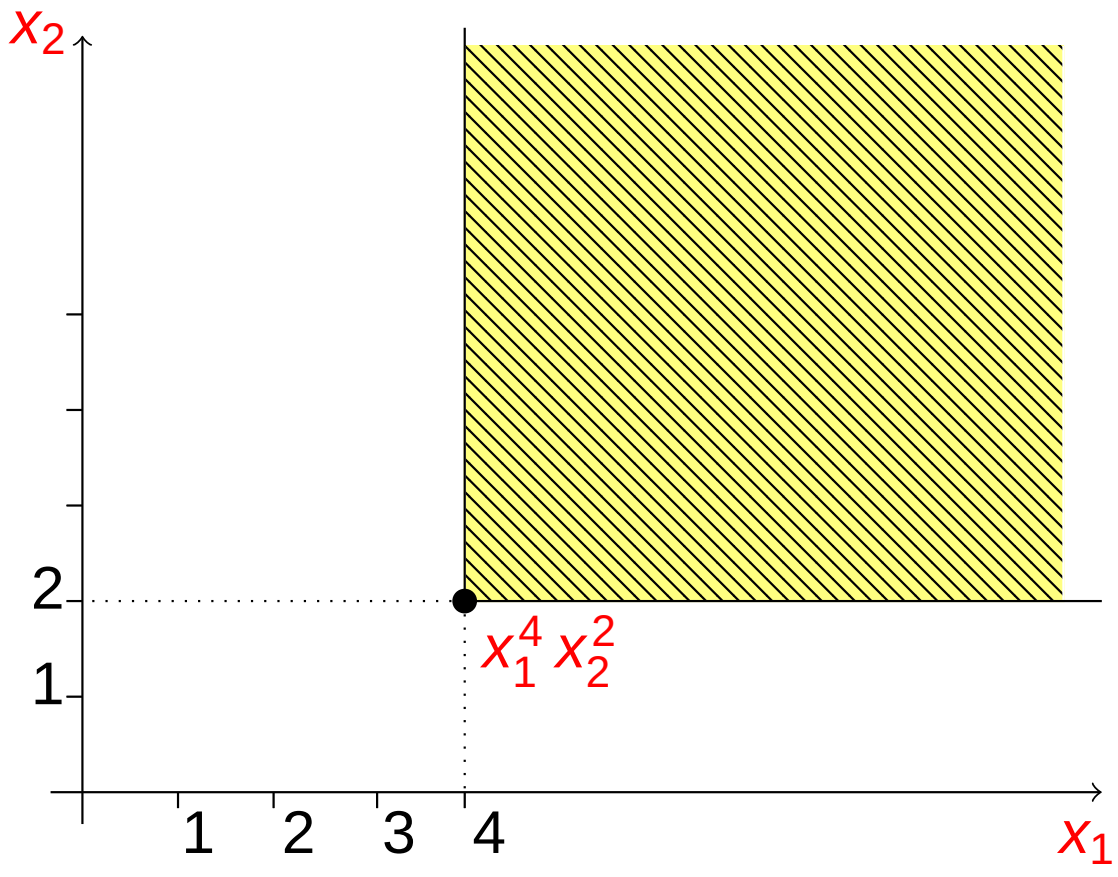
If $f \in I$ then $t\, f \in I$ for all $t \in T$

$$LT(t\, f) = t\, LT(f)$$

The staircase of a Gröbner basis.

Gröbner Bases

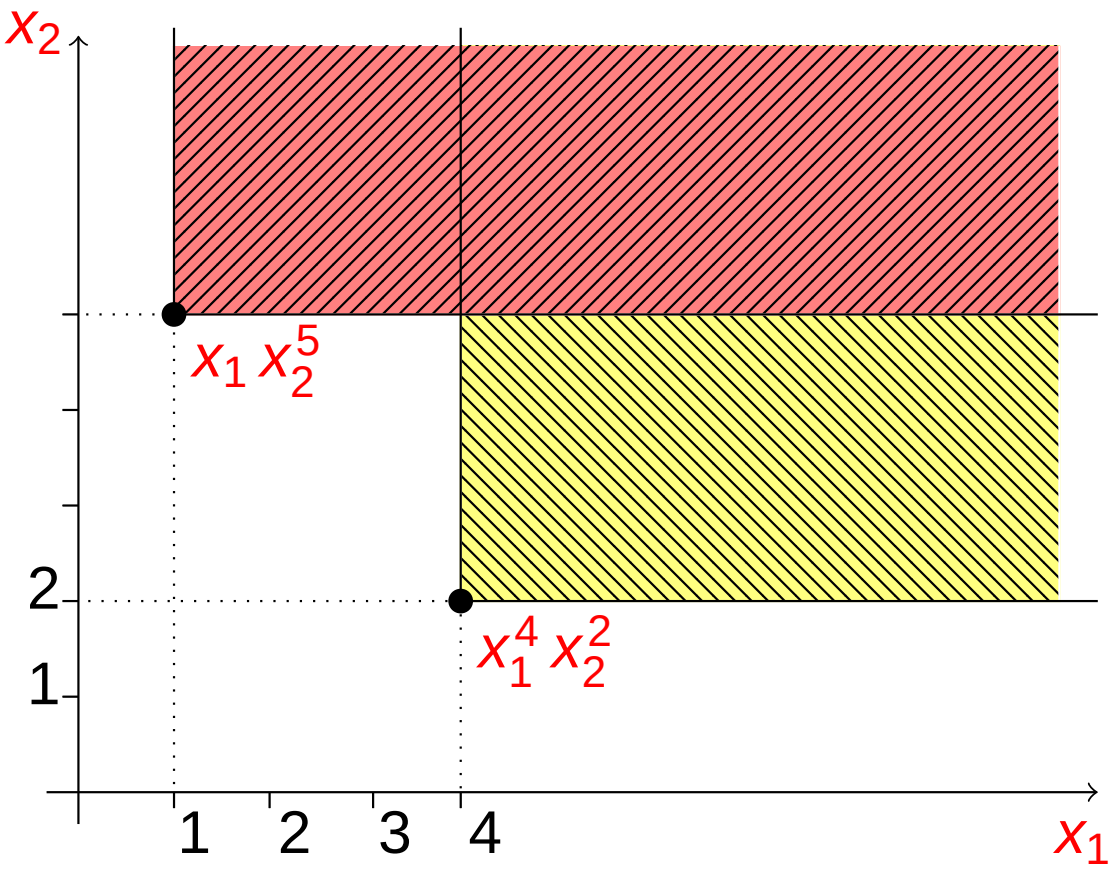
For any $f \in I$ we draw the point $\mathrm{LT}(f) \in \mathbb{N}^n$:



The staircase of a Gröbner basis.

Gröbner Bases

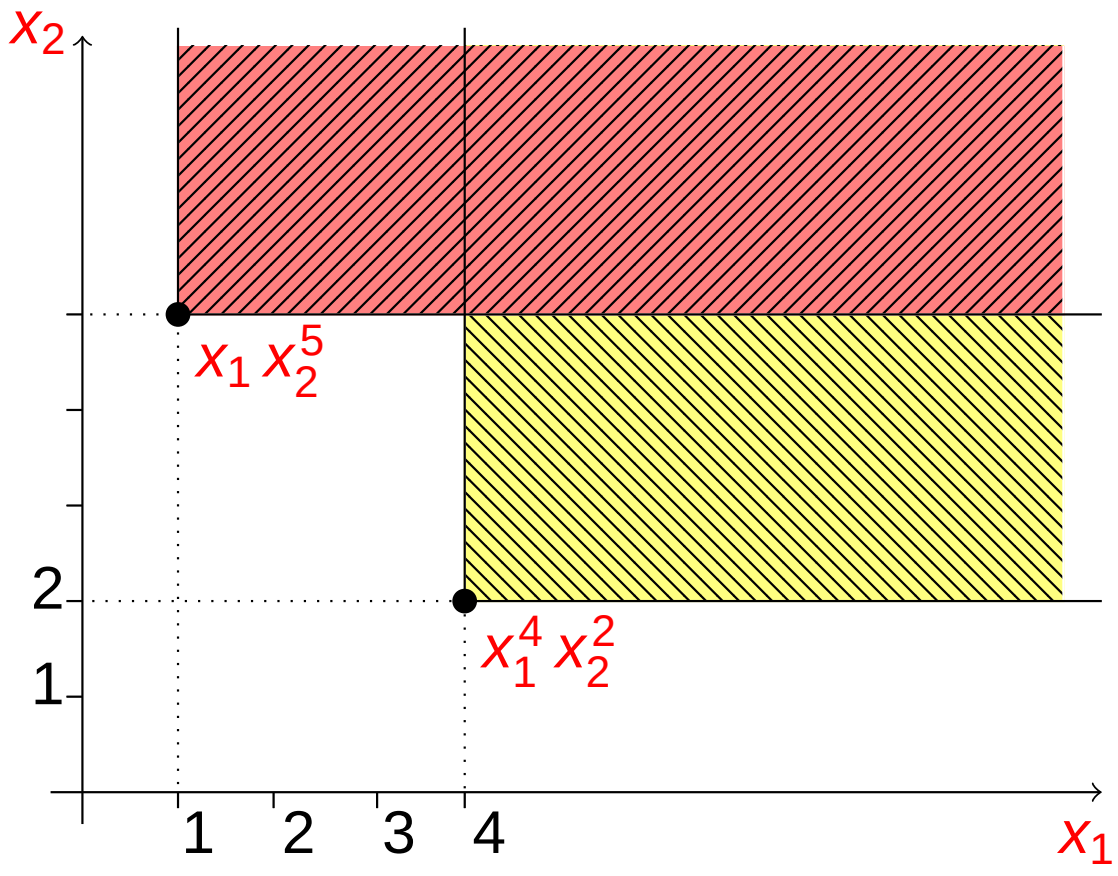
For any $f \in I$ we draw the point $\mathrm{LT}(f) \in \mathbb{N}^n$:



The staircase of a Gröbner basis.

Gröbner Bases

For any $f \in I$ we draw the point $\mathrm{LT}(f) \in \mathbb{N}^n$:



The staircase of a Gröbner basis.

Remark

The elements in a Gröbner basis are the **minimal** elements (for the division relation).

Gröbner Bases

Theorem

We fix a monomial order $<$. Any ideal I has a finite Gröbner basis G.

Theorem (Buchberger)

Let $G = [g_1, \ldots, g_k] \subset \mathbb{K}[x_1, \ldots, x_n]$ and $<$ a monomial ordering .
The two conditions are equivalents:

(i) *G is a Gröbner basis of $\mathrm{Id}(g_1, \ldots, g_k)$ for $<$.*

(ii) $\textsc{Reduction}(p, G) = 0$ *if and only if* $p \in \mathrm{Id}(G)$.

Normal Form

Theorem (Buchberger)

$G = [g_1, \ldots, g_k]$ Gröbner basis of $\mathrm{Id}(g_1, \ldots, g_k)$ wrt a fixed monomial ordering $<$.
Then, the result of FullReduction(p, G) *is unique and does not depend on the order of the elements in G).*

We give a new name to this FullReduction function:

Definition Normal Form

$G = (g_1, \ldots, g_k)$ be a Gröbner basis of I wrt $<$

For any polynomial f:

$$\mathrm{NF}(f, G, <) := \text{the result of the function FullReduction}(f, G).$$

Buchberger Algorithm

Describe a very simple version of the **Buchberger** algorithm:

Algorithm (Buchberger)

Input: $\begin{cases} F = [f_1, \ldots, f_s] \text{ a list of polynomials} \\ < \text{ admissible ordering} \end{cases}$

Output: G a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$.

$G := F$ and $m := s$

$P := \{(f_i, f_j) \mid 1 \leqslant i < j \leqslant m\}$ *the list of critical pairs*

while $P \neq \emptyset$ **do**

  Select and remove from P a critical pair (f, g)

  $f_{m+1} := \mathrm{Spol}(f, g)$

  $f_{m+1} :=$ REDUCTION(f_{m+1}, G)

  if $f_{m+1} \neq 0$ **then**

    $m := m + 1$

    $P := P \cup \{(f_i, f_m) \mid 1 \leqslant i < m\}$

    $G := G \cup \{f_m\}$

return G

Buchberger Algorithm

Remark

We have several degree of freedom to implement the algorithm: in the main loop we can choose any critical pair.
In practice, it is very important to select the critical pairs in the right order (see selection strategies).

Theorem

Buchberger's algorithm terminates.

Proof.

. . .

□

Remark

This is a non constructive proof of the algorithm and consequently we cannot deduce any complexity bound.

Polynomial Reduction : the algorithm

Algorithm (REDUCTION)

Input: $\begin{cases} p \text{ a polynomial} \\ F = [f_1, \ldots, f_m] \text{ a list of polynomials} \\ < \text{ monomial (admissible) ordering} \end{cases}$

Output: a reduced polynomial.

for $i := 1$ **to** m **and** $q = p$ **do**

  if $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ **then**

    return REDUCTION$\left(p - \frac{\mathrm{LM}(p)}{\mathrm{LM}(f_i)} f_i, F, <\right)$

return p

Buchberger Algorithm

Algorithm (Buchberger)

Input: $\begin{cases} F = [f_1, \ldots, f_s] \text{ a list of polynomials} \\ < \text{ admissible ordering} \end{cases}$

Output: G a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$.

$G := F$ and $m := s$

$P := \{(f_i, f_j) \mid 1 \leqslant i < j \leqslant m\}$ the list of critical pairs

while $P \neq \emptyset$ **do**

  Select and remove from P a critical pair (f, g)

  $f_{m+1} := \mathrm{Spol}(f, g)$

  $f_{m+1} :=$ REDUCTION(f_{m+1}, G)

  if $f_{m+1} \neq 0$ **then**

    $m := m + 1$

    $P := P \cup \{(f_i, f_m) \mid 1 \leqslant i < m\}$

    $G := G \cup \{f_m\}$

return G

Buchberger Algorithm

Remark

We have several degree of freedom to implement the algorithm: in the main loop we can choose any critical pair.
In practice, it is very important to select the critical pairs in the right order (see selection strategies).

Theorem

Buchberger's algorithm terminates.

Remark

This is a non constructive proof of the algorithm and consequently we cannot deduce any complexity bound.

Characterizations of Gröbner Bases

Characterizations of Gröbner Bases

Useful characterizations of Gröbner bases.

Definition (t-representation)

Let $P = [p_1, \ldots, p_k]$ be a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$, $0 \neq f \in \mathbb{K}[x_1, \ldots, x_n]$, and $t \in T$. Assume that there exists $(g_1, \ldots, g_k) \in \mathbb{K}[x_1, \ldots, x_n]^k$ such that:

$$f = \sum_{i=1}^{k} g_i \, p_i$$

We say that it is a *$t-$representation* of f wrt P if $t \geqslant \mathrm{LT}(g_i p_i)$ for all $1 \leqslant i \leqslant k$. We denote by $f = O_P(t)$ this property.
We note $f = o_P(t)$ when there exists $t' \in T$ such that $t' < t$ and $f = O_P(t')$.

Characterizations of Gröbner Bases

Proposition

If f, g are polynomials and , t is a term, P a finite subset of polynomials, then

$$\begin{array}{llll} f = O_P(t) & g = O_P(t) & \text{implies} & f + g = O_P(t) \\ f = o_P(t) & g = o_P(t) & \text{implies} & f + g = o_P(t) \\ f = O_P(t) & u \in T & \text{implies} & u\ f = O_P(u\,t) \\ f = o_P(t) & u \in T & \text{implies} & u\,f = o_P(u\,t) \end{array}$$

Proposition (R)

If $\textsc{Reduction}(p, P) = 0$ *or* $p \xrightarrow[P]{*} 0$ *then* $p = O_P(\mathrm{LT}(p))$.

Proof.

Easy exercise. □

Characterizations of Gröbner Bases

Theorem

G is a Gröbner basis if and only if $\forall 0 \neq f \in \mathrm{Id}(G)$, $f = O_G(\mathrm{LT}(f))$.

Proof.

...

□

and what happen when

$$f \neq O_G(\mathrm{LT}(f)) \ ?$$

Sum of polynomials

$$f \in I = \mathrm{Id}\,(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

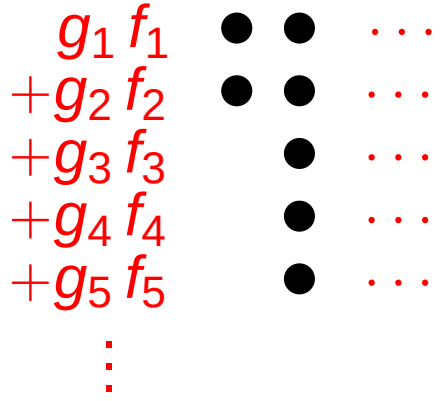
Sum of polynomials

$$f \in I = \mathrm{Id}\,(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

Not a unique representation !



Sum of polynomials

$$f \in I = \mathrm{Id}\,(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

Not a unique representation !

$$\begin{array}{rccc} g_1\, f_1 & \bullet & \bullet & \cdots \\ +g_2\, f_2 & \bullet & \bullet & \cdots \\ +g_3\, f_3 & & \bullet & \cdots \\ +g_4\, f_4 & & \bullet & \cdots \\ +g_5\, f_5 & & \bullet & \cdots \\ \vdots & & & \\ \hline = & 0 & 0 & \bullet \cdots \end{array}$$

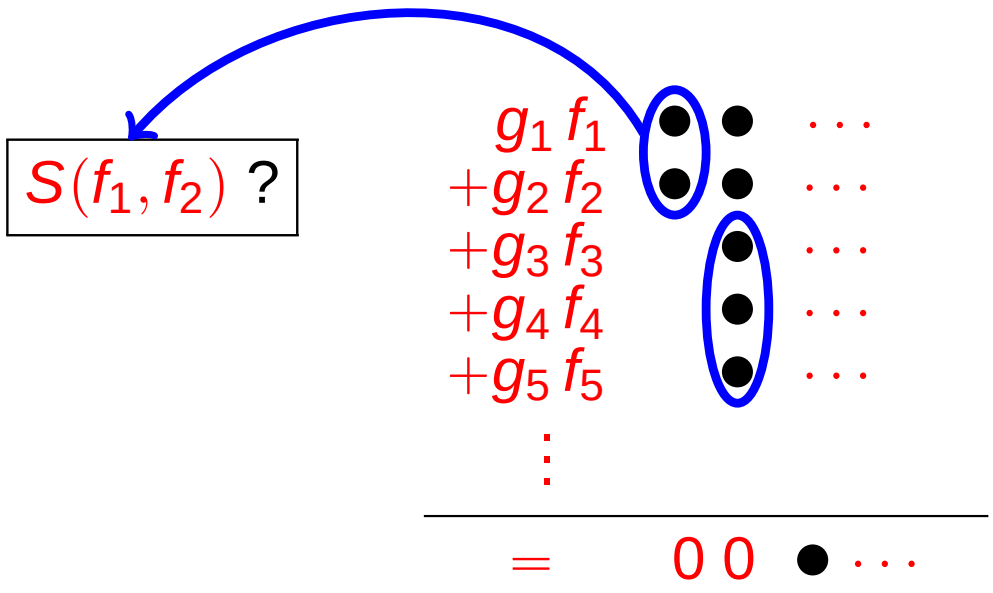
Sum of polynomials

$$f \in I = \mathrm{Id}(f_1, \cdots, f_m)$$

By definition:

$$f = g_1 f_1 + \cdots + g_m f_m$$

Not a unique representation !



Characterizations of Gröbner Bases

Theorem

G is a Gröbner basis if and only if $\forall 0 \neq f \in \mathrm{Id}(G)$, $f = O_G(\mathrm{LT}(f))$.

Theorem

Let G be a finite subset of polynomials. If for all g_1, g_2 in G, we have $\mathrm{Spol}(g_1, g_2) = 0$ or $\mathrm{Spol}(g_1, g_2) = o_G(\mathrm{lcm}(g_1, g_2))$, then G is a Gröbner basis.

Proof.

We need to proof a lemma first . . . □

Proof of the theorem: lemma

Lemma

Let $f_1, \ldots, f_k$ *be nonzero polynomials in* $\mathbb{K}[x_1, \ldots, x_n]$ *and* $t \in T$. *Consider* $f = O_P(t) = \sum_{i=1}^{k} c_i \mathbf{x}^{\alpha_i} f_i$, *where* $c_i \in \mathbb{K}^*$ *such that*

$$t = \mathbf{x}^{\alpha_1} LT(f_1) = \cdots = \mathbf{x}^{\alpha_k} LT(f_k).$$

If $LT(f) < t$, *then* $k > 1$ *and* f *can be rewritten:*

$$f = \sum_{i=1}^{k-1} b_i \frac{t}{\tau_i} S(f_i, f_{i+1}) \text{ with } b_i \in \mathbb{K}, \tag{1}$$

where $\tau_i = lcm(f_i, f_{i+1})$. *Furthermore*

$$\frac{t}{\tau_i} LT(S(f_i, f_{i+1})) < t, \text{ for all } i = 1, \ldots, k-1.$$

Characterizations of Gröbner Bases

Corollary (Buchberger)

Let G be a finite subset of polynomials . G is a Gröbner basis if and only if $\mathrm{Spol}(f,g) \xrightarrow{*} 0$ for all $(f,g) \in G^2$.

Corollary (Buchberger)

Let G be a finite subset of polynomials . G is a Gröbner basis if and only if $\textsc{Reduction}(\mathrm{Spol}(f,g),G) = 0$ for all $(f,g) \in G^2$.

Proof.

Let $(f,g) \in G^2$, $f \neq g$. Put $t = \mathrm{LT}(\mathrm{Spol}(f,g)) < \mathrm{lcm}(f,g)$
If $\textsc{Reduction}(\mathrm{Spol}(f,g),G) = 0$ then from proposition (R) :
$\mathrm{Spol}(f,g) = O_G(\mathrm{LT}(\mathrm{Spol}(f,g))) = O_G(t) = o_G(\mathrm{lcm}(f,g))$and we can apply the theorem. □

Buchberger Algorithm

Very simple version of the **Buchberger** algorithm:

Algorithm (Buchberger)

Input: $\begin{cases} F = [f_1, \ldots, f_s] \text{ a list of polynomials} \\ < \text{ admissible ordering} \end{cases}$

Output: G a finite subset of $\mathbb{K}[x_1, \ldots, x_n]$.

$G := F$ and $m := s$

$P := \{(f_i, f_j) \mid 1 \leqslant i < j \leqslant m\}$ *the list of critical pairs*

while $P \neq \emptyset$ **do**

  Select and remove from P a critical pair (f, g)

  $f_{m+1} := \mathrm{Spol}(f, g)$

  $f_{m+1} :=$ REDUCTION(f_{m+1}, G)

  if $f_{m+1} \neq 0$ **then**

    $m := m + 1$

    $P := P \cup \{(f_i, f_m) \mid 1 \leqslant i < m\}$

    $G := G \cup \{f_m\}$

return G

First application: Elimination Theorem

For an appropriate monomial ordering, Gröbner bases can be used to eliminate variables:

Theorem (Elimination Theorem)

Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, and $k \in \{1, \ldots, n\}$. If G is a Gröbner basis wrt the lexicographical ordering then $G_k = G \cap \mathbb{K}[x_k, \ldots, x_n]$ is a Gröbner basis of $I_k = I \cap \mathbb{K}[x_k, \ldots, x_n]$.

First application: Elimination Theorem

Theorem (Elimination Theorem)

Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, and $k \in \{1, \ldots, n\}$. If G is a Gröbner basis wrt the lexicographical ordering then $G_k = G \cap \mathbb{K}[x_k, \ldots, x_n]$ is a Gröbner basis of $I_k = I \cap \mathbb{K}[x_k, \ldots, x_n]$.

Remark

We can apply the previous in the specific case $k = n$: hence $G \cap \mathbb{K}[x_n]$ is a Gröbner basis of $I_n = I \cap \mathbb{K}[x_n]$ in $\mathbb{K}[x_n]$.
Since I_n is a principal ideal, it is generated by one polynomial $P_n(x_n)$ (may be 0).

First application: Elimination Theorem

Theorem (Elimination Theorem)

Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, and $k \in \{1, \ldots, n\}$. If G is a Gröbner basis wrt the lexicographical ordering then $G_k = G \cap \mathbb{K}[x_k, \ldots, x_n]$ is a Gröbner basis of $I_k = I \cap \mathbb{K}[x_k, \ldots, x_n]$.

In practice, it is much more efficient to avoid the lexicographical ordering. To this end, we need to introduce the following definition:

Definition (Elimination ordering)

A monomial ordering $<$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_s]$ is an elimination ordering wrt the block $[y_1, \ldots, y_s]$ if

$$\forall f \in \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_s],$$
$$\mathrm{LT}_<(f) \in \mathbb{K}[y_1, \ldots, y_s] \text{ implies } f \in \mathbb{K}[y_1, \ldots, y_s]$$

First application: Elimination Theorem

Theorem (Elimination Theorem)

Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, and $k \in \{1, \ldots, n\}$. If G is a Gröbner basis wrt the lexicographical ordering then $G_k = G \cap \mathbb{K}[x_k, \ldots, x_n]$ is a Gröbner basis of $I_k = I \cap \mathbb{K}[x_k, \ldots, x_n]$.

Definition (Elimination ordering)

A monomial ordering $<$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_s]$ is an elimination ordering wrt the block $[y_1, \ldots, y_s]$ if

$$\forall f \in \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_s],$$
$$\mathrm{LT}_<(f) \in \mathbb{K}[y_1, \ldots, y_s] \text{ implies } f \in \mathbb{K}[y_1, \ldots, y_s]$$

Example

A block ordering $<_{\mathrm{DRL,DRL}}\ [x_1, \ldots, x_{k-1}] \gg [x_k, \ldots, x_n]$ is an elimination ordering wrt $[x_k, \ldots, x_n]$).

First application: Elimination Theorem

Theorem (Elimination Theorem)

Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, and $k \in \{1, \ldots, n\}$. If G is a Gröbner basis wrt an elimination ordering wrt $[x_k, \ldots, x_n]$ then $G_k = G \cap \mathbb{K}[x_k, \ldots, x_n]$ is a Gröbner basis of $I_k = I \cap \mathbb{K}[x_k, \ldots, x_n]$.

Definition (Elimination ordering)

A monomial ordering $<$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_s]$ is an elimination ordering wrt the block $[y_1, \ldots, y_s]$ if

$$\forall f \in \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_s],$$
$$\mathrm{LT}_<(f) \in \mathbb{K}[y_1, \ldots, y_s] \text{ implies } f \in \mathbb{K}[y_1, \ldots, y_s]$$

Example

A block ordering $<_{\mathrm{DRL,DRL}}\ [x_1, \ldots, x_{k-1}] \gg [x_k, \ldots, x_n]$ is an elimination ordering wrt $[x_k, \ldots, x_n]$).

Application: Implicit equation

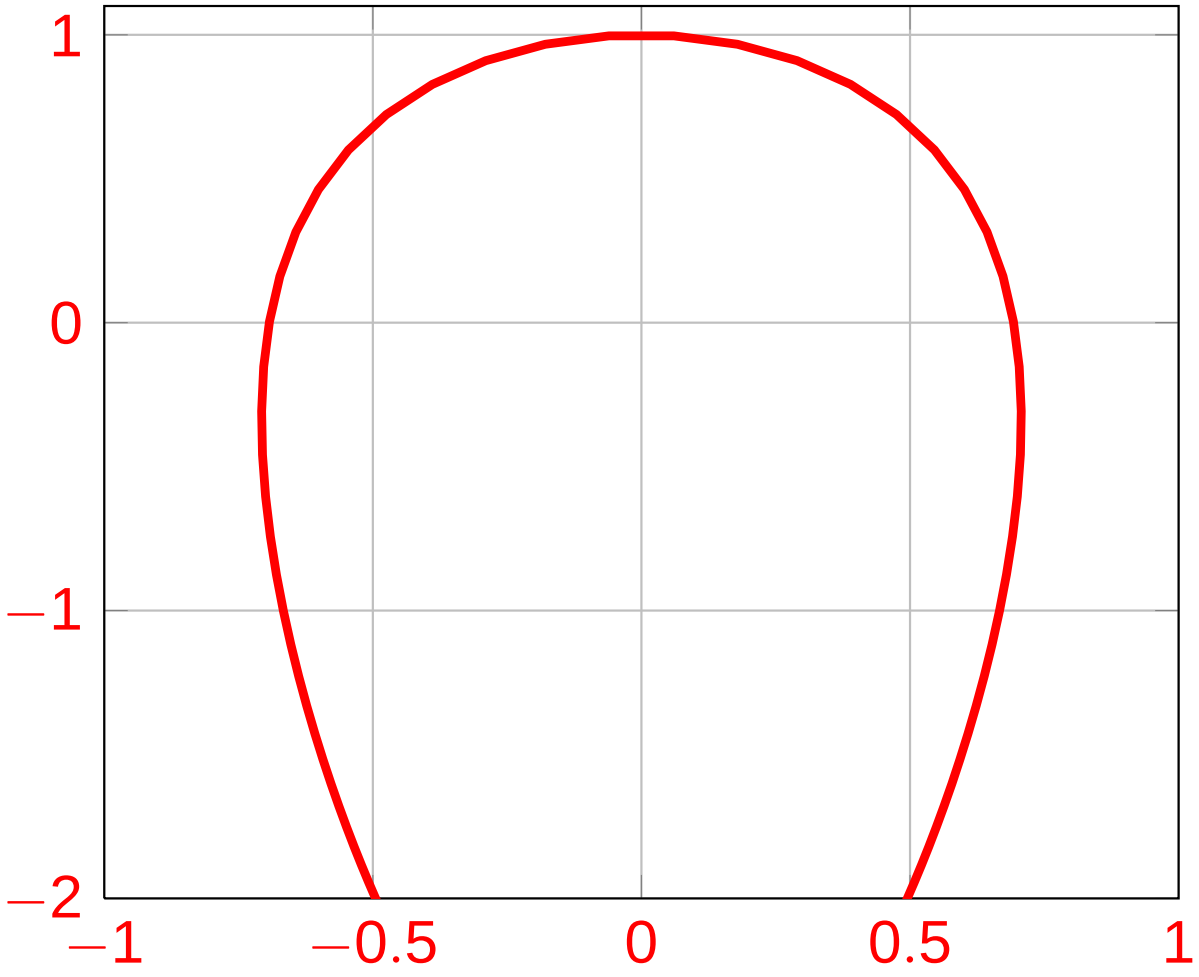
Draw the curve for $t \in [-2, 2]$:

$$\begin{cases} x(t) = \frac{2t}{1+2t^2} \\ y(t) = \frac{1-3t^2}{1+t^2} \end{cases}$$

Application: Implicit equation

Draw the curve for $t \in [-2, 2]$:

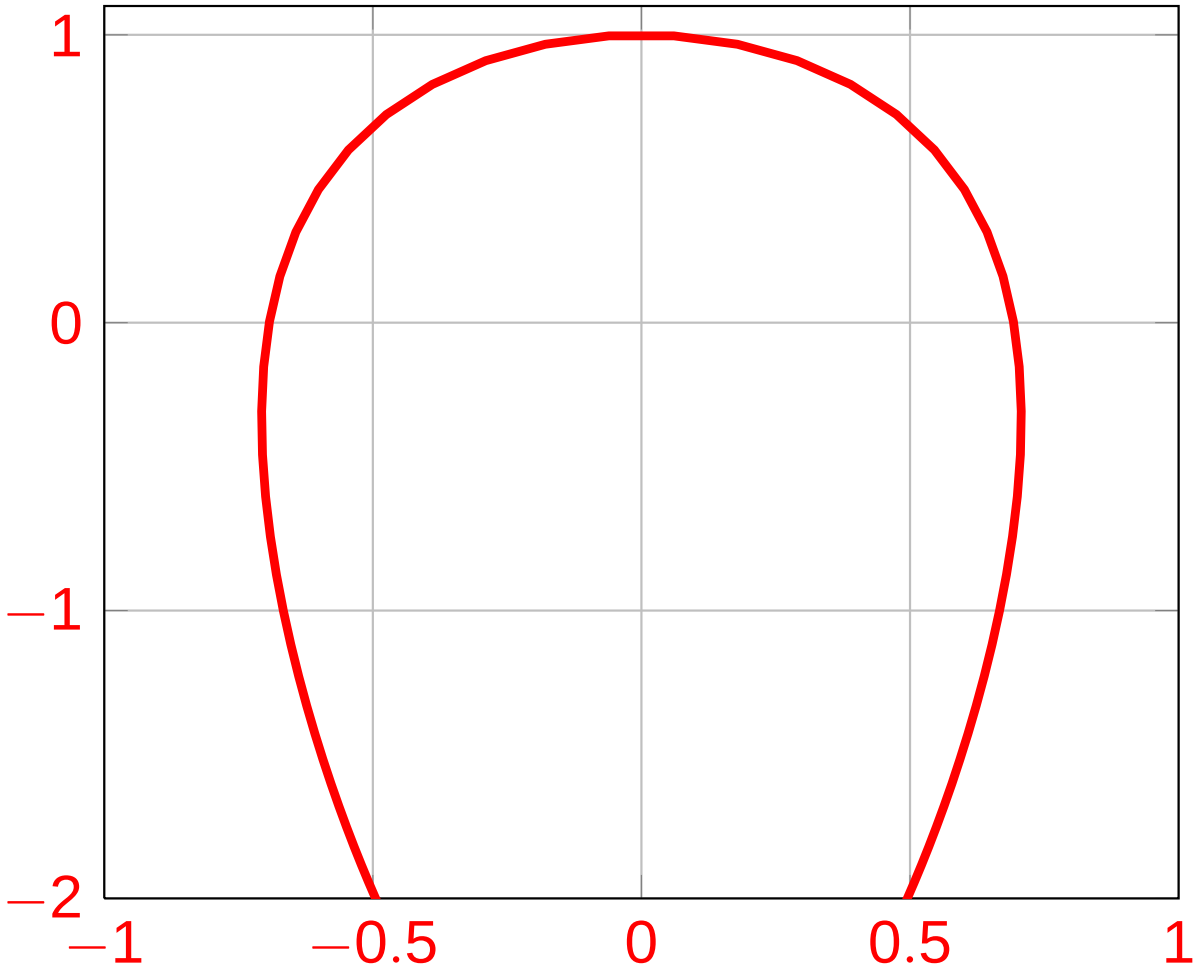
$$\begin{cases} x(t) = \frac{2t}{1+2t^2} \\ y(t) = \frac{1-3t^2}{1+t^2} \end{cases}$$



Application: Implicit equation

Draw the curve for $t \in [-2, 2]$:

$$\begin{cases} x(t) = \frac{2t}{1+2t^2} \\ y(t) = \frac{1-3t^2}{1+t^2} \end{cases}$$



Find an implicit equation $f(x, y) = 0$?

Implicit Equation

Compute a Gröbner basis of

$$\begin{cases} (1+2t^2)x - 2t, \\ (1+t^2)y - 1 + 3t^2 \end{cases}$$

for a monomial ordering such that $t \gg [x, y]$

Implicit Equation

Compute a Gröbner basis of

$$\begin{cases} (1+2t^2)x - 2t, \\ (1+t^2)y - 1 + 3t^2 \end{cases}$$

for a monomial ordering such that $t \gg [x, y]$ the resulting Gröbner basis:

$$\begin{cases} x^2y^2 - 10x^2y + 25x^2 + 4y^2 + 8y - 12, \\ 2ty + 6t + xy - 5x, \\ 16tx + x^2y - 5x^2 + 4y - 4 \end{cases}$$

Implicit Equation

Compute a Gröbner basis of

$$\begin{cases} (1+2t^2)x - 2t, \\ (1+t^2)y - 1 + 3t^2 \end{cases}$$

for a monomial ordering such that $t \gg [x, y]$ the resulting Gröbner basis:

$$\begin{cases} x^2y^2 - 10x^2y + 25x^2 + 4y^2 + 8y - 12, \\ 2ty + 6t + xy - 5x, \\ 16tx + x^2y - 5x^2 + 4y - 4 \end{cases}$$

The implicit equation is

$$\boxed{f(x,y) = x^2y^2 - 10x^2y + 25x^2 + 4y^2 + 8y - 12 = 0}$$

Application: Implicit equation

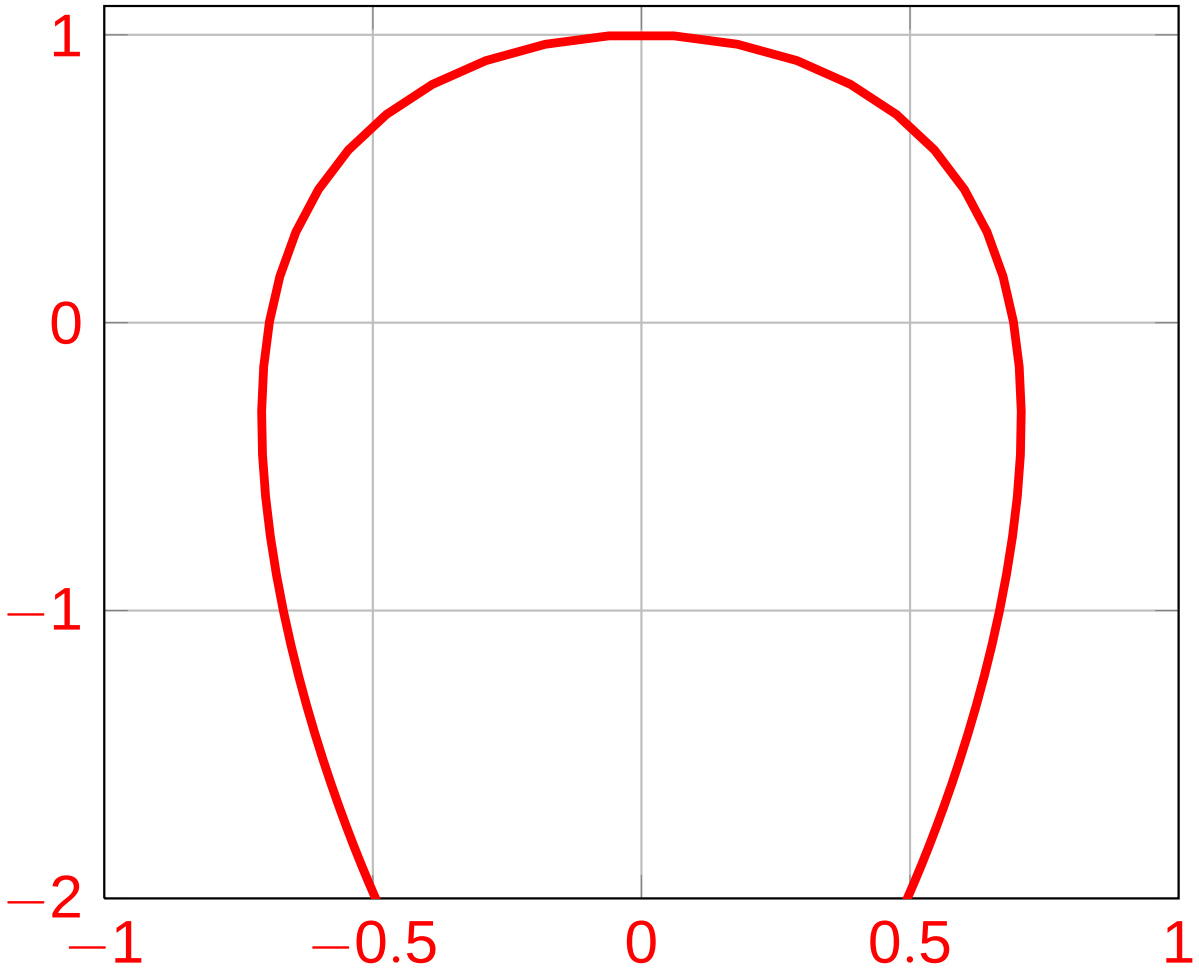
Draw the curve for $t \in [-2, 2]$:

$$\begin{cases} x(t) = \frac{2t}{1+2t^2} \\ y(t) = \frac{1-3t^2}{1+t^2} \end{cases}$$

Application: Implicit equation

Draw the curve for $t \in [-2, 2]$:

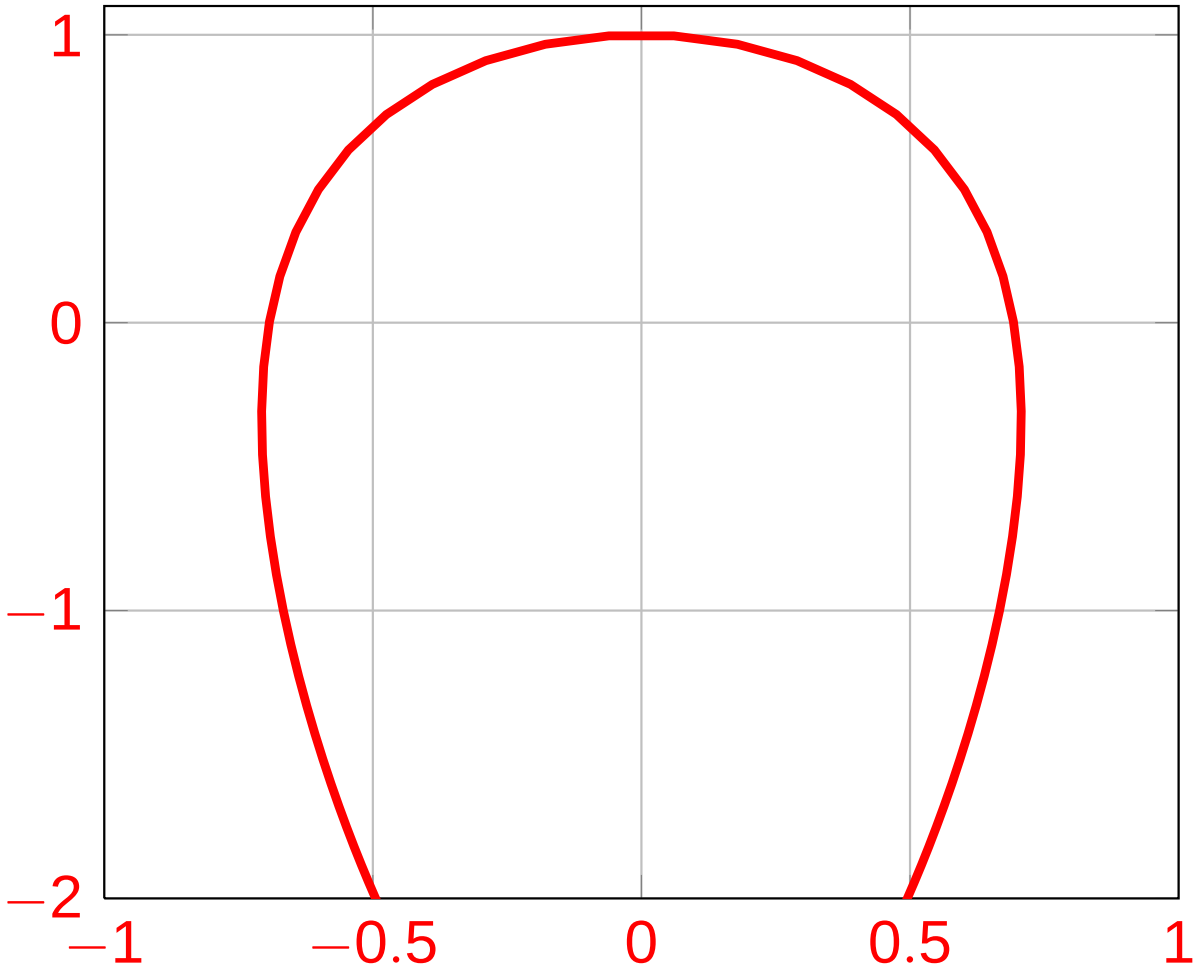
$$\begin{cases} x(t) = \frac{2t}{1+2t^2} \\ y(t) = \frac{1-3t^2}{1+t^2} \end{cases}$$



Application: Implicit equation

Draw the curve for $t \in [-2, 2]$:

$$\begin{cases} x(t) = \frac{2t}{1+2t^2} \\ y(t) = \frac{1-3t^2}{1+t^2} \end{cases}$$



Find an implicit equation $f(x, y) = 0$?

Implicit Equation

Compute a Gröbner basis of

$$\begin{cases} (1+2t^2)x - 2t, \\ (1+t^2)y - 1 + 3t^2 \end{cases}$$

for a monomial ordering such that $t \gg [x, y]$

Implicit Equation

Compute a Gröbner basis of

$$\begin{cases} (1+2t^2)x - 2t, \\ (1+t^2)y - 1 + 3t^2 \end{cases}$$

for a monomial ordering such that $t \gg [x, y]$ the resulting Gröbner basis:

$$\begin{cases} x^2y^2 - 10x^2y + 25x^2 + 4y^2 + 8y - 12, \\ 2ty + 6t + xy - 5x, \\ 16tx + x^2y - 5x^2 + 4y - 4 \end{cases}$$

Implicit Equation

Compute a Gröbner basis of

$$\begin{cases} (1+2t^2)x - 2t, \\ (1+t^2)y - 1 + 3t^2 \end{cases}$$

for a monomial ordering such that $t \gg [x, y]$ the resulting Gröbner basis:

$$\begin{cases} x^2y^2 - 10x^2y + 25x^2 + 4y^2 + 8y - 12, \\ 2ty + 6t + xy - 5x, \\ 16tx + x^2y - 5x^2 + 4y - 4 \end{cases}$$

The implicit equation is

$$\boxed{f(x,y) = x^2y^2 - 10x^2y + 25x^2 + 4y^2 + 8y - 12 = 0}$$

Références I

B. Buchberger.
An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal.
Journal of Symbolic Computation, 41(3-4):475–511, 3 2006.

Buchberger B.
Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.
PhD thesis, Innsbruck, 1965.

Buchberger B.
An Algorithmical Criterion for the Solvability of Algebraic Systems.
Aequationes Mathematicae, 4(3):374–383, 1970.
(German).

Références II

Bayer D. and Stillman M.
A theorem on refining division orders by the reverse lexicographic orders.
Duke J. Math., 55:321–328, 1987.

Cox D., Little J., and O'Shea D.
Ideals, Varieties and Algorithms.
Springer Verlag, New York, 1992.