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

Polynomials, Solution sets, Gröbner bases

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

[1]Inria and CryptoNext Security

[2]Sorbonne University, CNRS

First informations

Pedagogical team.

- Jean-Charles Faugère, Inria and CryptoNext Security
  `jean-charles.faugere@inria.fr`
- Vincent Neiger, Sorbonne University
  `vincent.neiger@lip6.fr`
- Mohab Safey El Din, Sorbonne University
  `mohab.safey@lip6.fr`

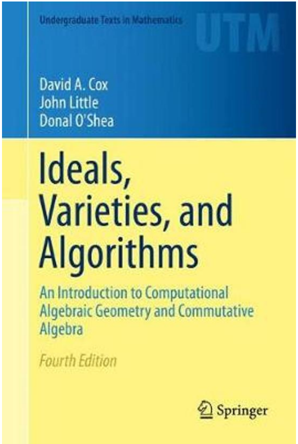
All slides and companion lecture notes (including exercises) will be available at

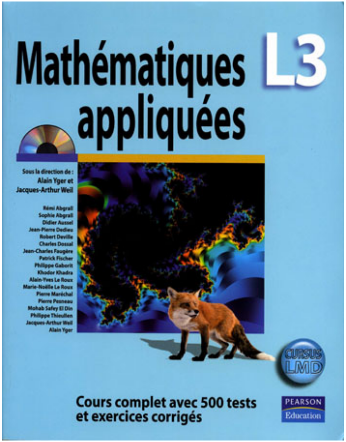
https://www-polsys.lip6.fr/∼jcf/Teaching/index.html

The course is taught in English upon explicit request.

Research internships / PhD positions available on the web. **Contact the teachers asap** if you get interested.

Textbooks





Mathematical background (mainly commutative algebra and some tapas of algebraic geometry) is introduced when needed.

This course is research oriented: it includes new recently published results.

Introduction

What is a polynomial?

What is a polynomial?

A monomial is a tuple $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of $\mathbb{N}^n$. Given two monomials $\boldsymbol{\alpha}, \boldsymbol{\beta}$, one defines the sum $\boldsymbol{\alpha} + \boldsymbol{\beta}$ by taking the sum of the tuples.

What is a polynomial?

A monomial is a tuple $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ of $\mathbb{N}^n$. Given two monomials $\boldsymbol{\alpha}, \boldsymbol{\beta}$, one defines the sum $\boldsymbol{\alpha} + \boldsymbol{\beta}$ by taking the sum of the tuples.

Provided $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ and variables $x_1, \dots, x_n$,

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

Sum of tuples $\boldsymbol{\alpha} + \boldsymbol{\beta} \leftrightarrow$ product $\boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\beta}}$

What is a polynomial?

A monomial is a tuple $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of $\mathbb{N}^n$. Given two monomials $\boldsymbol{\alpha}, \boldsymbol{\beta}$, one defines the sum $\boldsymbol{\alpha} + \boldsymbol{\beta}$ by taking the sum of the tuples.

Provided $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and variables $x_1, \ldots, x_n$,

$$\boldsymbol{\alpha} \text{ encodes } \boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

$$\text{Sum of tuples } \boldsymbol{\alpha} + \boldsymbol{\beta} \leftrightarrow \text{product } \boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\beta}}$$

The total degree of $\boldsymbol{\alpha}$ is the sum $\alpha_1 + \cdots + \alpha_n$.

Univariate monomials ($n = 1$) are naturally ordered by their degree and this order is compatible with multiplication

$$(m_1 \prec m_2 \Rightarrow \forall m \in \mathbb{N}^n, m \times m_1 \prec m \times m_2).$$

What is a polynomial?

A monomial is a tuple $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of $\mathbb{N}^n$. Given two monomials $\boldsymbol{\alpha}, \boldsymbol{\beta}$, one defines the sum $\boldsymbol{\alpha} + \boldsymbol{\beta}$ by taking the sum of the tuples.

Provided $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and variables $x_1, \ldots, x_n$,

$$\boldsymbol{\alpha} \text{ encodes } \boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

$$\text{Sum of tuples } \boldsymbol{\alpha} + \boldsymbol{\beta} \leftrightarrow \text{product } \boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\beta}}$$

The total degree of $\boldsymbol{\alpha}$ is the sum $\alpha_1 + \cdots + \alpha_n$.

Univariate monomials ($n = 1$) are naturally ordered by their degree and this order is compatible with multiplication

$$(m_1 \prec m_2 \Rightarrow \forall m \in \mathbb{N}^n, m \times m_1 \prec m \times m_2).$$

Multivariate monomials ($n > 1$) can be ordered too with orders compatible with the multiplication and extra properties.

What is a polynomial?

A monomial is a tuple $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of $\mathbb{N}^n$. Given two monomials $\boldsymbol{\alpha}, \boldsymbol{\beta}$, one defines the sum $\boldsymbol{\alpha} + \boldsymbol{\beta}$ by taking the sum of the tuples.

Provided $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and variables $x_1, \ldots, x_n$,

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

Sum of tuples $\boldsymbol{\alpha} + \boldsymbol{\beta} \leftrightarrow$ product $\boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\beta}}$

The total degree of $\boldsymbol{\alpha}$ is the sum $\alpha_1 + \cdots + \alpha_n$.

Univariate monomials ($n = 1$) are naturally ordered by their degree and this order is compatible with multiplication

$$(m_1 \prec m_2 \Rightarrow \forall m \in \mathbb{N}^n, m \times m_1 \prec m \times m_2).$$

Multivariate monomials ($n > 1$) can be ordered too with orders compatible with the multiplication and extra properties.

We will define and use such orders which are called admissible orders.

What is a polynomial?

Let $\mathbb{K}$ be a field. We consider the $\mathbb{K}$-vector space E generated by all the monomials of $\mathbb{N}^n$. This is an infinite dimensional vector space, the set of monomials in $\mathbb{N}^n$ is a free basis of E.

What is a polynomial?

Let $\mathbb{K}$ be a field. We consider the $\mathbb{K}$-vector space E generated by all the monomials of $\mathbb{N}^n$. This is an infinite dimensional vector space, the set of monomials in $\mathbb{N}^n$ is a free basis of E.

A polynomial is an element of this $\mathbb{K}$-vector space E. All in all, it is represented as a finite sequence of elements $(c_{\boldsymbol{\alpha}_1}, \ldots, c_{\boldsymbol{\alpha}_\ell})$ of $\mathbb{K}$, indexed by finitely many elements of $\mathbb{N}^n$. Mathematically, it is a finite linear combination of monomials over $\mathbb{K}$.

Equipped with variables $x_1, \ldots, x_n \quad \rightsquigarrow c_{\boldsymbol{\alpha}_1} x_1^{\alpha_{1,1}} \cdots x_n^{\alpha_{1,n}} + \cdots + c_{\boldsymbol{\alpha}_\ell} x_1^{\alpha_{\ell,1}} \cdots x_n^{\alpha_{\ell,n}}$.

What is a polynomial?

Let $\mathbb{K}$ be a field. We consider the $\mathbb{K}$-vector space E generated by all the monomials of $\mathbb{N}^n$. This is an infinite dimensional vector space, the set of monomials in $\mathbb{N}^n$ is a free basis of E.

A polynomial is an element of this $\mathbb{K}$-vector space E. All in all, it is represented as a finite sequence of elements $(c_{\boldsymbol{\alpha}_1}, \ldots, c_{\boldsymbol{\alpha}_\ell})$ of $\mathbb{K}$, indexed by finitely many elements of $\mathbb{N}^n$. Mathematically, it is a finite linear combination of monomials over $\mathbb{K}$.

Equipped with variables $x_1, \ldots, x_n \rightsquigarrow c_{\boldsymbol{\alpha}_1} x_1^{\alpha_{1,1}} \cdots x_n^{\alpha_{1,n}} + \cdots + c_{\boldsymbol{\alpha}_\ell} x_1^{\alpha_{\ell,1}} \cdots x_n^{\alpha_{\ell,n}}$.

The set of polynomials with variables $x_1, \ldots, x_n$ with base field $\mathbb{K}$ is denoted by $\mathbb{K}[x_1, \ldots, x_n]$.

Defining the classical multiplication of polynomials, one equips $\mathbb{K}[x_1, \ldots, x_n]$ with a ring structure.

What is a polynomial?

Let $\mathbb{K}$ be a field. We consider the $\mathbb{K}$-vector space E generated by all the monomials of $\mathbb{N}^n$. This is an infinite dimensional vector space, the set of monomials in $\mathbb{N}^n$ is a free basis of E.

A polynomial is an element of this $\mathbb{K}$-vector space E. All in all, it is represented as a finite sequence of elements $(c_{\boldsymbol{\alpha}_1}, \ldots, c_{\boldsymbol{\alpha}_\ell})$ of $\mathbb{K}$, indexed by finitely many elements of $\mathbb{N}^n$. Mathematically, it is a finite linear combination of monomials over $\mathbb{K}$.

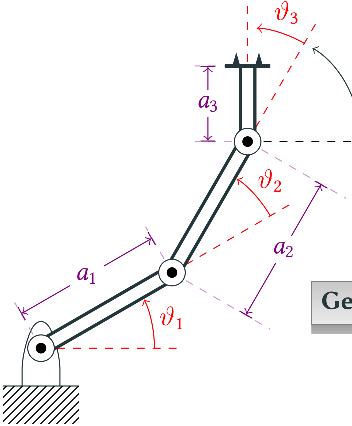
Equipped with variables $x_1, \ldots, x_n \rightsquigarrow c_{\boldsymbol{\alpha}_1} x_1^{\alpha_{1,1}} \cdots x_n^{\alpha_{1,n}} + \cdots + c_{\boldsymbol{\alpha}_\ell} x_1^{\alpha_{\ell,1}} \cdots x_n^{\alpha_{\ell,n}}$.

The set of polynomials with variables $x_1, \ldots, x_n$ with base field $\mathbb{K}$ is denoted by $\mathbb{K}[x_1, \ldots, x_n]$.

Defining the classical multiplication of polynomials, one equips $\mathbb{K}[x_1, \ldots, x_n]$ with a ring structure.

Arithmetic size. A polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ of degree D is encoded with an array of coefficients of length $\binom{n+D}{n}$.

Polynomial systems in engineering sciences (I)

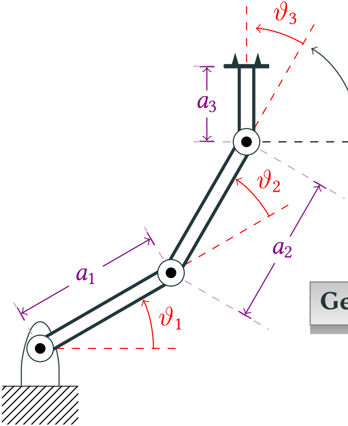


$$\begin{cases} x_{\text{end}} &= a_1\cos(\vartheta_1) + a_2\cos(\vartheta_1+\vartheta_2) + \\ & \quad a_3\cos(\vartheta_1+\vartheta_2+\vartheta_3) \\ y_{\text{end}} &= a_1\sin(\vartheta_1) + a_2\sin(\vartheta_1+\vartheta_2) + \\ & \quad a_3\sin(\vartheta_1+\vartheta_2+\vartheta_3) \\ \psi &= \vartheta_1+\vartheta_2+\vartheta_3 \end{cases}$$

Geometric properties → **kinematic map**

$$\mathscr{K} : SO(2)^n \to E.$$

Polynomial systems in engineering sciences (I)



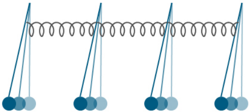
$$
\begin{cases}
x_{\text{end}} = a_1 \cos(\vartheta_1) + a_2 \cos(\vartheta_1 + \vartheta_2) + \\
\qquad\quad a_3 \cos(\vartheta_1 + \vartheta_2 + \vartheta_3) \\
y_{\text{end}} = a_1 \sin(\vartheta_1) + a_2 \sin(\vartheta_1 + \vartheta_2) + \\
\qquad\quad a_3 \sin(\vartheta_1 + \vartheta_2 + \vartheta_3) \\
\psi = \vartheta_1 + \vartheta_2 + \vartheta_3
\end{cases}
$$

Geometric properties → **kinematic map**

$$\mathscr{K} : SO(2)^n \to E.$$

Polynomial systems are ubiquitous in robotics, mechanics, and some areas of biology and chemistry.

Polynomial systems in engineering sciences (II)



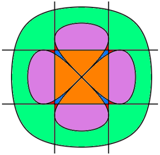
A dynamical system of 4 coupled oscillators: maximal number of equilibria?

$\rightsquigarrow$ Kuramoto model of 4 oscillators

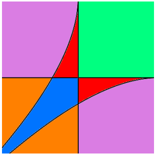
Maximal number of real solutions of

$$\begin{cases} x_{2i-1}^2 + x_{2i}^2 = 1, x_7 = 0, x_8 = 1 \\ \sum_{j=1}^{4} (x_{2i-1}x_{2j} - x_{2i}x_{2j-1}) = y_i, i = 1 \ldots 3 \end{cases}$$

[Xin, Kikkawa, Liu '16] conjectured at most **10** real solutions



Section $y_1 + y_2 + 2y_3 = 0$



Zoom in: **2**, **4**, **6**, **8**, **10**

Definitive answer through polynomial system solvers

Polynomial systems solving in mathematics

Algebraic methods for polynomial system solving and more generally, computer algebra can be used to prove some mathematical results (or disprove mathematical conjectures).

Theorem. Surfaces of degree 3 always contain lines and conics.

Noether–Lefschetz theorem $\Longrightarrow$ surfaces of degree ≥ 4 almost never do.

What about some special surfaces of degree 4? $\cos(t)f + \sin(t)g = 0$

Using the `msolve` library

SORBONNE UNIVERSITÉ

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITY OF OREGON

Polynomial systems in cryptography

Context. A (Alice) wants to send a private message to B (Bob).

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

Let $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ built by B. That will be the public key that B shares with A.

Polynomial systems in cryptography

Context. A (Alice) wants to send a private message to B (Bob).

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

Let $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ built by B. That will be the public key that B shares with A.

The secret is a solution ξ of the system $f_1 = \cdots = f_s = 0$ (which is expected to be known by design of $\boldsymbol{f}$ from B).

Polynomial systems in cryptography

Context. A (Alice) wants to send a private message to B (Bob).

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

Let $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ built by B. That will be the public key that B shares with A.

The secret is a solution ξ of the system $f_1 = \cdots = f_s = 0$ (which is expected to be known by design of $\boldsymbol{f}$ from B).

To send a message $m \in \mathbb{K} \in \mathbb{K}^n$, A picks a matrix M in $R^{n\times s}$ and sends

$$c = m + M \,.\, \boldsymbol{f} \in R^n$$

Decoding amounts to substitute variables in c by ξ.

Polynomial systems in cryptography

Context. A (Alice) wants to send a private message to B (Bob).

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

Let $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ built by B. That will be the public key that B shares with A.

The secret is a solution ξ of the system $f_1 = \cdots = f_s = 0$ (which is expected to be known by design of $\boldsymbol{f}$ from B).

To send a message $m \in \mathbb{K} \in \mathbb{K}^n$, A picks a matrix M in $R^{n\times s}$ and sends

$$c = m + M \,.\, \boldsymbol{f} \in R^n$$

Decoding amounts to substitute variables in c by ξ.

Attacking this cryptocipher amounts to solve $f_1 = \cdots = f_s = 0$.

Polynomial systems in cryptography

Context. A (Alice) wants to send a private message to B (Bob).

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

Let $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ built by B. That will be the public key that B shares with A.

The secret is a solution ξ of the system $f_1 = \cdots = f_s = 0$ (which is expected to be known by design of $\boldsymbol{f}$ from B).

To send a message $m \in \mathbb{K} \in \mathbb{K}^n$, A picks a matrix M in $R^{n \times s}$ and sends

$$c = m + M \,.\, \boldsymbol{f} \in R^n$$

Decoding amounts to substitute variables in c by ξ.

Attacking this cryptocipher amounts to solve $f_1 = \cdots = f_s = 0$.

National Institute of Standards and Technology
U.S. Department of Commerce

Multivariate cryptography and post-quantum cryptography are hot topics

Features of polynomial systems of equations

Linear systems of equations may have

infinitely many solutions or 0 or 1 solution.

Gaussian elimination $\Longrightarrow$ Triangular rewriting $\Longrightarrow$ Solving

Features of polynomial systems of equations

Coordinates lie in the field of the input coefficients

Linear systems of equations may have

infinitely many solutions or 0 or 1 solution.

Gaussian elimination $\Longrightarrow$ Triangular rewriting $\Longrightarrow$ Solving

Features of polynomial systems of equations

Coordinates lie in the field of the input coefficients

Linear systems of equations may have infinitely many solutions or 0 or 1 solution.

Implicit ordering on the variables

Gaussian elimination $\Longrightarrow$ Triangular rewriting $\Longrightarrow$ Solving

Features of polynomial systems of equations

Coordinates lie in the field of the input coefficients

Linear systems of equations may have

Implicit ordering on the variables

infinitely many solutions or 0 or 1 solution.

Gaussian elimination $\Longrightarrow$ Triangular rewriting $\Longrightarrow$ Solving

Non-linear polynomial systems of equations may have

infinitely many solutions $\qquad x_1^2 + x_2^2 - 1 = 0$

0 solution $\qquad x_1 x_2 - 1 = x_1 = 0$

Finitely many solutions $\qquad x_1^2 + x_2^2 - 1 = x_1 - x_2 = 0$

They can have really **a lot of solutions** $\qquad x_1^2 - 2 = \cdots = x_n^2 - 2 = 0$

Features of polynomial systems of equations

Coordinates lie in the field of the input coefficients

Linear systems of equations may have

Implicit ordering on the variables

infinitely many solutions or 0 or 1 solution.

Gaussian elimination $\Longrightarrow$ Triangular rewriting $\Longrightarrow$ Solving

Non-linear polynomial systems of equations may have

infinitely many solutions $\qquad x_1^2 + x_2^2 - 1 = 0$

0 solution $\qquad x_1 x_2 - 1 = x_1 = 0$

Finitely many solutions $\qquad x_1^2 + x_2^2 - 1 = x_1 - x_2 = 0$

They can have really **a lot of solutions** $\qquad x_1^2 - 2 = \cdots = x_n^2 - 2 = 0$

... and their coordinates may lie outside the field generated by the input coefficients.

What does “solving” mean?

Depends a lot on the application and on the base field $\mathbb{K}$

- $\mathbb{K} = \mathbb{Q} \rightsquigarrow$ extract informations on real or complex solutions
- $\mathbb{K}$ is a finite field $\rightsquigarrow$ solutions in $\mathbb{K}$ or an algebraic closure of $\mathbb{K}$

What does "solving" mean?

Depends a lot on the application and on the base field $\mathbb{K}$

- $\mathbb{K} = \mathbb{Q} \rightsquigarrow$ extract informations on real or complex solutions
- $\mathbb{K}$ is a finite field $\rightsquigarrow$ solutions in $\mathbb{K}$ or an algebraic closure of $\mathbb{K}$

Algebraic closure – definition

Let $\mathbb{K}$ be a field. An algebraic closure of $\mathbb{K}$, is a field $\overline{\mathbb{K}}$, containing $\mathbb{K}$ s.t. all univariate polynomials of degree d with coefficients in $\overline{\mathbb{K}}$ have d solutions counted with multiplicities.

What does "solving" mean?

Depends a lot on the application and on the base field $\mathbb{K}$

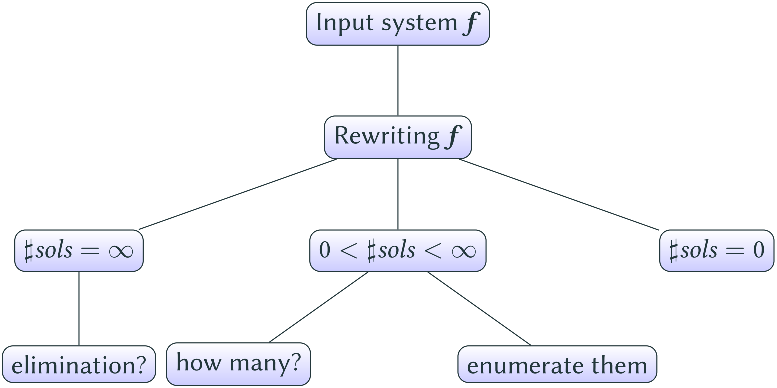
- $\mathbb{K} = \mathbb{Q} \rightsquigarrow$ extract informations on real or complex solutions
- $\mathbb{K}$ is a finite field $\rightsquigarrow$ solutions in $\mathbb{K}$ or an algebraic closure of $\mathbb{K}$

Algebraic closure – definition

Let $\mathbb{K}$ be a field. An algebraic closure of $\mathbb{K}$, is a field $\overline{\mathbb{K}}$, containing $\mathbb{K}$ s.t. all univariate polynomials of degree d with coefficients in $\overline{\mathbb{K}}$ have d solutions counted with multiplicities.

Algebraic methods $\rightarrow$ Triangular rewriting $\rightarrow$ "Solving" over $\overline{\mathbb{K}}$

What does “solving” mean?



Towards Gröbner bases

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

	Linear systems	**Polynomial systems**
Equations	$\ell_1 = \cdots = \ell_s = 0$	$f_1 = \cdots = f_s = 0$
Algebraic object	Vector space $V = \{\sum_i a_i \ell_i \mid a_i \in \mathbb{K}\}$	Ideal generated by the f_i's $I = \{\sum_i q_i f_i \mid q_i \in R\}$
Algorithm	Gaussian elimination (variable ordering)	"Elimination of monomials" (monomial ordering $\rightsquigarrow$ term rewriting)
Output	Triangular basis of V	**Gröbner basis of I**

Gröbner bases and polynomial system solving

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

$$\boldsymbol{f} = (f_1, \ldots, f_s) \subset R.$$

Provided $\prec$, a Gröbner basis G of the ideal generated by $\boldsymbol{f}$ provides a canonical description of it.

Emptiness decision

A non-zero constant $a \in \mathbb{K}$ lies in G.

Gröbner bases and polynomial system solving

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

$$\boldsymbol{f} = (f_1, \dots, f_s) \subset R.$$

Provided $\prec$, a Gröbner basis G of the ideal generated by $\boldsymbol{f}$ provides a canonical description of it.

Emptiness decision

A non-zero constant $a \in \mathbb{K}$ lies in G.

Membership problem

There exists a division algorithm which, given G, $\prec$ and $f \in R$ allows us to decide whether f lies in the ideal generated by $\boldsymbol{f}$.

Gröbner bases and polynomial system solving

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

$$\boldsymbol{f} = (f_1, \ldots, f_s) \subset R.$$

Provided $\prec$, a Gröbner basis G of the ideal generated by $\boldsymbol{f}$ provides a canonical description of it.

Emptiness decision

A non-zero constant $a \in \mathbb{K}$ lies in G.

Membership problem

There exists a division algorithm which, given G, $\prec$ and $f \in R$ allows us to decide whether f lies in the ideal generated by $\boldsymbol{f}$.

- Unique representative of f modulo the ideal (provided $\succ$)
- Allows to compute “modulo” the equations

$\rightsquigarrow$ description of the solutions

Gröbner bases and polynomial system solving

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$, $\prec$ a monomial ordering, $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ and G a Gröbner basis for the ideal generated by $\boldsymbol{f}$ (provided $\prec$).

One can choose $\prec$ such that G has the following shape

$$G = \begin{cases} T_n \subset \mathbb{K}[x_1, \ldots, x_n] \\ \qquad\quad \vdots \\ T_2 \subset \mathbb{K}[x_{n-1}, x_n] \\ T_1 \subset \mathbb{K}[x_n] \end{cases}$$

Gröbner bases and polynomial system solving

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$, $\prec$ a monomial ordering, $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ and G a Gröbner basis for the ideal generated by $\boldsymbol{f}$ (provided $\prec$).

One can choose $\prec$ such that G has the following shape

$$G = \begin{cases} T_n \subset \mathbb{K}[x_1, \ldots, x_n] \\ \qquad \vdots \\ T_2 \subset \mathbb{K}[x_{n-1}, x_n] \\ T_1 \subset \mathbb{K}[x_n] \end{cases}$$

Gröbner bases and polynomial system solving

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$, $\prec$ a monomial ordering, $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R$ and G a Gröbner basis for the ideal generated by $\boldsymbol{f}$ (provided $\prec$).

One can choose $\prec$ such that G has the following shape

$$G = \begin{cases} T_n \subset \mathbb{K}[x_1, \ldots, x_n] \\ \qquad\quad \vdots \\ T_2 \subset \mathbb{K}[x_{n-1}, x_n] \\ T_1 \subset \mathbb{K}[x_n] \end{cases}$$

Shape position

When $s \geq n$, and when the solution set in $\overline{\mathbb{K}}^n$ is finite, G has (most of the time) the following so-called shape position

$$w, x_2 - v_2, \ldots, x_n - v_n \text{ with } w, v_i \in \mathbb{K}[x_1]$$

- Note that, in this case, solutions in $\mathbb{K}^n$ can be recovered

Julia Demo

Basic notions of algebra and geometry

Algebraic sets and ideals

Ideals and solution sets

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

Ideal

An ideal I of R is a non-empty subset of R such that for all f, g in I and $h \in R$, $f + g \in I$ and $hf \in I$.

Ideals and solution sets

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

Ideal

An ideal I of R is a non-empty subset of R such that for all f, g in I and $h \in R$, $f + g \in I$ and $hf \in I$.

Lemma – Definition

Let $S \subset R$. Then

$$\left\{ \sum_{i=1}^{s} q_i f_i \mid q_i \in R, (f_1, \ldots, f_s) \subset S \right\}$$

is an ideal of R. It is called the ideal generated by S, denoted by $\langle S \rangle$.

Ideals and solution sets

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

Ideal

An ideal I of R is a non-empty subset of R such that for all f, g in I and $h \in R$, $f + g \in I$ and $hf \in I$.

Lemma – Definition

Let $S \subset R$. Then

$$\left\{ \sum_{i=1}^{s} q_i f_i \mid q_i \in R, (f_1, \ldots, f_s) \subset S \right\}$$

is an ideal of R. It is called the ideal generated by S, denoted by $\langle S \rangle$.

Remark. Let $\xi \in \overline{\mathbb{K}}^n$ such that $f_i(\xi) = 0$ for $1 \le i \le s$.

Then for all $g \in \langle \boldsymbol{f} \rangle$, $g(\xi) = 0$.

Ideals and solution sets

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

Definition

A $\mathbb{K}$-algebraic set V (also called algebraic variety) of $\overline{\mathbb{K}}^n$ is a subset of $\overline{\mathbb{K}}^n$ such that there exists a subset $S \subset R$ such that

$$V = \{\xi \in \overline{\mathbb{K}}^n \mid \forall f \in S \quad f(\xi) = 0\}$$

Ideals and solution sets

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

Definition

A $\mathbb{K}$-algebraic set V (also called algebraic variety) of $\overline{\mathbb{K}}^n$ is a subset of $\overline{\mathbb{K}}^n$ such that there exists a subset $S \subset R$ such that

$$V = \{\xi \in \overline{\mathbb{K}}^n \mid \forall f \in S \quad f(\xi) = 0\}$$

Remark. for any $f \in \langle S \rangle$ and $\xi \in V$, $f(\xi) = 0$.

V is the algebraic set associated to $\langle S \rangle$. It is denoted by $V(S)$ or $V(\langle S \rangle)$.

Ideals and solution sets

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $R = \mathbb{K}[x_1, \dots, x_n]$.

Definition

A $\mathbb{K}$-algebraic set V (also called algebraic variety) of $\overline{\mathbb{K}}^n$ is a subset of $\overline{\mathbb{K}}^n$ such that there exists a subset $S \subset R$ such that

$$V = \{\xi \in \overline{\mathbb{K}}^n \mid \forall f \in S \quad f(\xi) = 0\}$$

Remark. for any $f \in \langle S \rangle$ and $\xi \in V$, $f(\xi) = 0$.

V is the algebraic set associated to $\langle S \rangle$. It is denoted by $V(S)$ or $V(\langle S \rangle)$.

- Let I and $\mathcal{J}$ be ideals of R. It holds that $I \subset \mathcal{J}$ iff $V(\mathcal{J}) \subset V(I)$.
- Let I and $\mathcal{J}$ be ideals of R. It holds that $V(I \cap \mathcal{J}) = V(I) \cup V(\mathcal{J})$.

Hilbert's basis theorem

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

Hilbert's basis theorem

Let I be an ideal of R. There exists a **finite** subset $S \subset R$ such that $I = \langle S \rangle$.

Hilbert's basis theorem

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

Hilbert's basis theorem

Let I be an ideal of R. There exists a **finite** subset $S \subset R$ such that $I = \langle S \rangle$.

- Any $\mathbb{K}$-algebraic set of $\overline{\mathbb{K}}^n$ is defined as the solution set (in $\overline{\mathbb{K}}^n$) of a finite polynomial system of equations.

Hilbert's basis theorem

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

Hilbert's basis theorem

Let I be an ideal of R. There exists a **finite** subset $S \subset R$ such that $I = \langle S \rangle$.

- Any $\mathbb{K}$-algebraic set of $\overline{\mathbb{K}}^n$ is defined as the solution set (in $\overline{\mathbb{K}}^n$) of a finite polynomial system of equations.
- Assume we are given some monomial ordering $\prec$ and let $I \subset R$ be an ideal.

  For $f \in I$, denote by $\mathrm{LM}_\prec(f)$ the leading monomial of f (w.r.t. $\prec$).

Hilbert's basis theorem

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

Hilbert's basis theorem

Let I be an ideal of R. There exists a **finite** subset $S \subset R$ such that $I = \langle S \rangle$.

- Any $\mathbb{K}$-algebraic set of $\overline{\mathbb{K}}^n$ is defined as the solution set (in $\overline{\mathbb{K}}^n$) of a finite polynomial system of equations.
- Assume we are given some monomial ordering $\prec$ and let $I \subset R$ be an ideal.

  For $f \in I$, denote by $\mathrm{LM}_\prec(f)$ the leading monomial of f (w.r.t. $\prec$).

  Let $S = \{m \mid \exists f \in I \text{ such that } m = \mathrm{LM}_\prec(f)\}$.

  Then $\langle S \rangle$ is finitely generated.

Hilbert's basis theorem

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

Hilbert's basis theorem

Let I be an ideal of R. There exists a **finite** subset $S \subset R$ such that $I = \langle S \rangle$.

- Any $\mathbb{K}$-algebraic set of $\overline{\mathbb{K}}^n$ is defined as the solution set (in $\overline{\mathbb{K}}^n$) of a finite polynomial system of equations.
- Assume we are given some monomial ordering $\prec$ and let $I \subset R$ be an ideal.

  For $f \in I$, denote by $\mathrm{LM}_\prec(f)$ the leading monomial of f (w.r.t. $\prec$).

  Let $S = \{m \mid \exists f \in I \text{ such that } m = \mathrm{LM}_\prec(f)\}$.

  Then $\langle S \rangle$ is finitely generated.

Algebraic methods $\rightsquigarrow$ **Appropriate bases of ideals**

Noetherianity

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

Ascending chains of ideals

Let $(I_i)_{i \in \mathbb{N}}$ be a sequence of ideals such that

$$I_1 \subset I_2 \subset \cdots \subset I_i \subset I_{i+1} \subset \cdots$$

There exists $k \in \mathbb{N}$ such that for all $\ell \geq k$, $I_k = I_\ell$.

Hilbert's weak Nullstellensatz

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

Hilbert's weak Nullstellensatz

Let $I \subset R$ be an ideal. It holds that $V(I)$ is empty if and only if $1 \in I$.

Hilbert's weak Nullstellensatz

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

Hilbert's weak Nullstellensatz

Let $I \subset R$ be an ideal. It holds that $V(I)$ is empty if and only if $1 \in I$.

- On input $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R \rightsquigarrow$ decide whether $1 \in \langle \boldsymbol{f} \rangle$.

Emptiness decision in $\overline{\mathbb{K}}^n$

Ideal membership problem

Hilbert's weak Nullstellensatz

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

Hilbert's weak Nullstellensatz

Let $I \subset R$ be an ideal. It holds that $V(I)$ is empty if and only if $1 \in I$.

- On input $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R \rightsquigarrow$ decide whether $1 \in \langle \boldsymbol{f} \rangle$.

  Emptiness decision in $\overline{\mathbb{K}}^n$

  Ideal membership problem
- **Example.** Take $f_1 = x_1 x_2 - 1$ and $f_2 = x_1$. Then $1 \in \langle f_1, f_2 \rangle$

  (since $1 = x_2 f_2 - f_1$)

Hilbert's weak Nullstellensatz

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

Hilbert's weak Nullstellensatz

Let $I \subset R$ be an ideal. It holds that $V(I)$ is empty if and only if $1 \in I$.

- On input $\boldsymbol{f} = (f_1, \ldots, f_s) \subset R \rightsquigarrow$ decide whether $1 \in \langle \boldsymbol{f} \rangle$.

  Emptiness decision in $\overline{\mathbb{K}}^n$ | Ideal membership problem

- **Example.** Take $f_1 = x_1 x_2 - 1$ and $f_2 = x_1$. Then $1 \in \langle f_1, f_2 \rangle$

  (since $1 = x_2 f_2 - f_1$)

- Warning: applies to $\overline{\mathbb{K}}$ only.

  Example. Take $\mathbb{K} = \mathbb{R}$ and $I = \langle x_1^2 + x_2^2 + 1 \rangle$.

Ideals associated to sets, Hilbert's Nullstellensatz

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

Definition – Lemma

Let $E \subset \overline{\mathbb{K}}^n$. Consider the subset S of R associated to E defined as

$$S = \{f \in R \mid \forall \xi \in E, \quad f(\xi) = 0\} .$$

It holds that S is an ideal, which is called ideal associated to E and denoted by $\mathrm{Id}(E)$.

Ideals associated to sets, Hilbert's Nullstellensatz

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

Definition – Lemma

Let $E \subset \overline{\mathbb{K}}^n$. Consider the subset S of R associated to E defined as

$$S = \{f \in R \mid \forall \xi \in E, \quad f(\xi) = 0\}\,.$$

It holds that S is an ideal, which is called ideal associated to E and denoted by $\mathrm{Id}(E)$.

- Let $I \subset R$. It holds that $V(I) = V(\mathrm{Id}(V(I)))$ and $I \subset \mathrm{Id}(V(I))$. The latter inclusion may be strict.

Example. Take $I = \langle x_1^2 \rangle$.

Ideals associated to sets, Hilbert's Nullstellensatz

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

Definition – Lemma

Let $E \subset \overline{\mathbb{K}}^n$. Consider the subset S of R associated to E defined as

$$S = \{f \in R \mid \forall \xi \in E, \quad f(\xi) = 0\}\,.$$

It holds that S is an ideal, which is called ideal associated to E and denoted by $\mathrm{Id}(E)$.

- Let $I \subset R$. It holds that $V(I) = V(\mathrm{Id}(V(I)))$ and $I \subset \mathrm{Id}(V(I))$. The latter inclusion may be strict.

  Example. Take $I = \langle x_1^2 \rangle$.

- **Exercise.** Prove that $\mathrm{Id}(\mathbb{R}) = \langle 0 \rangle$.

Ideals associated to sets, Hilbert's Nullstellensatz

We observed that for $I = \langle x_1^2 \rangle$, it holds that

$$x_1 \in \mathsf{Id}(V(I)) \qquad \text{and} \qquad x_1 \notin I.$$

Ideals associated to sets, Hilbert's Nullstellensatz

We observed that for $I = \langle x_1^2 \rangle$, it holds that

$$x_1 \in \mathrm{Id}(V(I)) \qquad \text{and} \qquad x_1 \notin I.$$

In other words, some power of x_1 lies in I.

Ideals associated to sets, Hilbert's Nullstellensatz

We observed that for $I = \langle x_1^2 \rangle$, it holds that

$$x_1 \in \mathrm{Id}(V(I)) \qquad \text{and} \qquad x_1 \notin I.$$

In other words, some power of x_1 lies in I.

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $R = \mathbb{K}[x_1, \dots, x_n]$.

Hilbert's Nullstellensatz

Let $f \in R$ and $I \subset R$ be an ideal. If $f \in \mathrm{Id}(V(I))$, then there exists $k \in \mathbb{N}$ such that $f^k \in I$.

Ideals associated to sets, Hilbert's Nullstellensatz

We observed that for $I = \langle x_1^2 \rangle$, it holds that

$$x_1 \in \mathrm{Id}(V(I)) \qquad \text{and} \qquad x_1 \notin I.$$

In other words, some power of x_1 lies in I.

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

Hilbert's Nullstellensatz

Let $f \in R$ and $I \subset R$ be an ideal. If $f \in \mathrm{Id}(V(I))$, then there exists $k \in \mathbb{N}$ such that $f^k \in I$.

Definition/Lemma – radical ideal

Let $I \subset R$ be an ideal. The set

$$\{f \in R \mid \exists k \in \mathbb{N} \text{ such that } f^k \in I\}$$

is an ideal. It is called the radical of I and denoted by $\sqrt{I}$.

Ideal – Variety correspondence

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

- Let $I \subset R$ be an ideal. It holds that

$$\sqrt{I} = \mathsf{Id}(V(I)).$$

- Let $V \subset \overline{\mathbb{K}}^n$ be an algebraic set. It holds that

$$V(\mathsf{Id}(V)) = V.$$

Zariski topology

This slide anticipates our future study of the complexity of Gröbner bases computations (under so-called regularity assumption).

Zariski topology

This slide anticipates our future study of the complexity of Gröbner bases computations (under so-called regularity assumption).

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$ and $n \in \mathbb{N} - \{0\}$

One can equip $\overline{\mathbb{K}}^n$ with a so-called Zariski topology, where the class of closed sets is the class of algebraic sets in $\overline{\mathbb{K}}^n$.
By definition, the open sets, in this topology are complements of algebraic sets.

Zariski topology

This slide anticipates our future study of the complexity of Gröbner bases computations (under so-called regularity assumption).

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$ and $n \in \mathbb{N} - \{0\}$

One can equip $\overline{\mathbb{K}}^n$ with a so-called Zariski topology, where the class of closed sets is the class of algebraic sets in $\overline{\mathbb{K}}^n$.
By definition, the open sets, in this topology are complements of algebraic sets.

- The Zariski closure of a subset W in $\overline{\mathbb{K}}^n$ is the smallest (for the partial order induced by inclusion) algebraic set which contains W.

Zariski topology

This slide anticipates our future study of the complexity of Gröbner bases computations (under so-called regularity assumption).

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$ and $n \in \mathbb{N} - \{0\}$

One can equip $\overline{\mathbb{K}}^n$ with a so-called Zariski topology, where the class of closed sets is the class of algebraic sets in $\overline{\mathbb{K}}^n$.
By definition, the open sets, in this topology are complements of algebraic sets.

- The Zariski closure of a subset W in $\overline{\mathbb{K}}^n$ is the smallest (for the partial order induced by inclusion) algebraic set which contains W.
- The Zariski topology is less fine that the Euclidean topology.
  Example. The open (for the Euclidean topology) disk centered at 0 of radius 1 in $\mathbb{C}$ is not an open set for the Zariski topology. Its Zariski closure is $\mathbb{C}$.

Zariski topology

This slide anticipates our future study of the complexity of Gröbner bases computations (under so-called regularity assumption).

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$ and $n \in \mathbb{N} - \{0\}$

One can equip $\overline{\mathbb{K}}^n$ with a so-called Zariski topology, where the class of closed sets is the class of algebraic sets in $\overline{\mathbb{K}}^n$.
By definition, the open sets, in this topology are complements of algebraic sets.

- The set of polynomials of degree $\leq D$ with coefficients in $\overline{\mathbb{K}}$ is a finite dimensional vector space. It is isomorphic to $\overline{\mathbb{K}}^N$ with $N = \binom{n+D}{D}$. A property $\mathscr{P}$ on polynomials is generic iff there exists a non-empty Zariski open subset $U \subset \overline{\mathbb{K}}^N$ such that $\mathscr{P}$ holds for any $f \in U$.

Geometric "complexity measures"

We need to quantify how difficult it will be to describe $\mathbb{K}$-algebraic sets.

Geometric "complexity measures"

We need to quantify how difficult it will be to describe $\mathbb{K}$-algebraic sets.

- Notion of dimension: measures the number of degrees of freedom when moving on the algebraic set;

Geometric "complexity measures"

We need to quantify how difficult it will be to describe $\mathbb{K}$-algebraic sets.

- Notion of dimension: measures the number of degrees of freedom when moving on the algebraic set;
- Notion of degree: measures how "fat" is an algebraic set.

Geometric "complexity measures"

We need to quantify how difficult it will be to describe $\mathbb{K}$-algebraic sets.

- Notion of dimension: measures the number of degrees of freedom when moving on the algebraic set;
- Notion of degree: measures how "fat" is an algebraic set.

Dimension

Let $V \subset \overline{\mathbb{K}}^n$ be an algebraic set. The dimension of V is the maximum integer d such that there exists $\boldsymbol{\iota} = \{i_1, \ldots, i_d\} \subset \{1, \ldots, n\}$ such that $\pi_{\boldsymbol{\iota}}(V)$ contains a non-empty Zariski open subset of $\overline{\mathbb{K}}^d$.

Geometric "complexity measures"

We need to quantify how difficult it will be to describe $\mathbb{K}$-algebraic sets.

- Notion of dimension: measures the number of degrees of freedom when moving on the algebraic set;
- Notion of degree: measures how "fat" is an algebraic set.

Dimension

Let $V \subset \overline{\mathbb{K}}^n$ be an algebraic set. The dimension of V is the maximum integer d such that there exists $\boldsymbol{\iota} = \{i_1, \ldots, i_d\} \subset \{1, \ldots, n\}$ such that $\pi_{\boldsymbol{\iota}}(V)$ contains a non-empty Zariski open subset of $\overline{\mathbb{K}}^d$.

- By convention, the dimension of the empty set it -1.
- When V is a finite set of points, it has dimension 0.
- A hypersurface (defined by a single polynomial) has dimension $n-1$.

Geometric “complexity measures”

We need to quantify how difficult it will be to describe $\mathbb{K}$-algebraic sets.

- Notion of dimension: measures the number of degrees of freedom when moving on the algebraic set;
- Notion of degree: measures how “fat” is an algebraic set.

Dimension

Let $V \subset \overline{\mathbb{K}}^n$ be an algebraic set. The dimension of V is the maximum integer d such that there exists $\boldsymbol{\iota} = \{i_1, \ldots, i_d\} \subset \{1, \ldots, n\}$ such that $\pi_{\boldsymbol{\iota}}(V)$ contains a non-empty Zariski open subset of $\overline{\mathbb{K}}^d$.

- By convention, the dimension of the empty set it -1.
- When V is a finite set of points, it has dimension 0.
- A hypersurface (defined by a single polynomial) has dimension $n-1$.
- When V has dimension 1, it contains a curve

Example. $x_1^2 + x_2^2 = 0$

Geometric "complexity measures"

We need to quantify how difficult it will be to describe $\mathbb{K}$-algebraic sets.

- Notion of dimension: measures the number of degrees of freedom when moving on the algebraic set;
- Notion of degree: measures how "fat" is an algebraic set.

Dimension

Let $V \subset \overline{\mathbb{K}}^n$ be an algebraic set. The dimension of V is the maximum integer d such that there exists $\boldsymbol{\iota} = \{i_1, \ldots, i_d\} \subset \{1, \ldots, n\}$ such that $\pi_{\boldsymbol{\iota}}(V)$ contains a non-empty Zariski open subset of $\overline{\mathbb{K}}^d$.

- By convention, the dimension of the empty set it -1.
- When V is a finite set of points, it has dimension 0.
- A hypersurface (defined by a single polynomial) has dimension $n-1$.
- When V has dimension 1, it contains a curve

Example. $x_1^2 + x_2^2 = 0$

Other example.

$$(x_1^2 + x_2^2)(x_1 - 1) = (x_1^2 + x_2^2)(x_2 - 1) = 0$$

Geometric "complexity measures"

Let $V \subset \overline{\mathbb{K}}^n$ be a non-empty algebraic set of dimension d.

Lemma

For a generic choice of a $(n-d)$-dimensional affine linear subspace $\mathscr{L}_{n-d}$, $V \cap \mathscr{L}_{n-d}$ has dimension 0.

Geometric "complexity measures"

Let $V \subset \overline{\mathbb{K}}^n$ be a non-empty algebraic set of dimension d.

Lemma

For a generic choice of a $(n-d)$-dimensional affine linear subspace $\mathscr{L}_{n-d}$, $V \cap \mathscr{L}_{n-d}$ has dimension 0.

Lemma – Definition

There exists $\delta \in \mathbb{N}$ such that, for a generic choice of a $(n-d)$-dimensional affine linear subspace $\mathscr{L}_{n-d}$, $V \cap \mathscr{L}_{n-d}$ has dimension 0 and cardinality δ. We call δ the degree of V and we denote it by $\deg(V)$.

Geometric "complexity measures"

Let $V \subset \overline{\mathbb{K}}^n$ be a non-empty algebraic set of dimension d.

Lemma

For a generic choice of a $(n-d)$-dimensional affine linear subspace $\mathscr{L}_{n-d}$, $V \cap \mathscr{L}_{n-d}$ has dimension 0.

Lemma – Definition

There exists $\delta \in \mathbb{N}$ such that, for a generic choice of a $(n-d)$-dimensional affine linear subspace $\mathscr{L}_{n-d}$, $V \cap \mathscr{L}_{n-d}$ has dimension 0 and cardinality δ. We call δ the degree of V and we denote it by $\deg(V)$.

- By convention, the degree of the empty set is 0.

Bézout's theorem

Bézout theorem

Let V and W be two algebraic sets in $\overline{\mathbb{K}}^n$. Then

$$\deg(V \cap W) \leq \deg(V)\deg(W)$$

Gröbner bases

Definitions and first properties

Reminder of motivation

$\boxed{\text{Ideal membership problem}}$

Hilbert's weak Nullstellensatz.

Rewriting input polynomial systems

Reminder of motivation

Ideal membership problem

Hilbert's weak Nullstellensatz.

Rewriting input polynomial systems

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1} + x_2 - 1$

$f_2 = \boxed{x_1} - x_2 + 1$

$\boxed{f_1 - f_2} = 2x_2 - 2$

Reminder of motivation

Ideal membership problem

Hilbert's weak Nullstellensatz.

Rewriting input polynomial systems

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1} + x_2 - 1$

$f_2 = \boxed{x_1} - x_2 + 1$

$\boxed{f_1 - f_2} = 2x_2 - 2$

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1^2} + x_2^2 - 1$

$f_2 = \boxed{x_1^2} - x_2^2 + 1$

Reminder of motivation

Ideal membership problem

Hilbert's weak Nullstellensatz.

Rewriting input polynomial systems

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1} + x_2 - 1$

$f_2 = \boxed{x_1} - x_2 + 1$

$\boxed{f_1 - f_2} = 2x_2 - 2$

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1^2} + x_2^2 - 1$

$f_2 = \boxed{x_1^2} - x_2^2 + 1$

$\boxed{g = f_1 - f_2} = 2x_2^2 - 2$

$\boxed{f_1 - \frac{1}{2}g} = x_1^2$

Reminder of motivation

Ideal membership problem

Hilbert's weak Nullstellensatz.

Rewriting input polynomial systems

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1} + x_2 - 1$

$f_2 = \boxed{x_1} - x_2 + 1$

$\boxed{f_1 - f_2} = 2x_2 - 2$

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1^2} + x_2^2 - 1$

$f_2 = \boxed{x_1^2} - x_2^2 + 1$

$\boxed{g = f_1 - f_2} = 2x_2^2 - 2$

$\boxed{f_1 - \frac{1}{2}g} = x_1^2$

What about ?

$f_1 = x_1^2 + x_2^2 + x_1x_2 - 1$

$f_2 = x_1^2 - x_2^2 - 2x_1x_2 + 1$

Reminder of motivation

Ideal membership problem

Hilbert's weak Nullstellensatz.

Rewriting input polynomial systems

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1} + x_2 - 1$

$f_2 = \boxed{x_1} - x_2 + 1$

$\boxed{f_1 - f_2} = 2x_2 - 2$

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1^2} + x_2^2 - 1$

$f_2 = \boxed{x_1^2} - x_2^2 + 1$

$\boxed{g = f_1 - f_2} = 2x_2^2 - 2$

$\boxed{f_1 - \frac{1}{2}g} = x_1^2$

What about ?

$f_1 = x_1^2 + x_2^2 + x_1x_2 - 1$

$f_2 = x_1^2 - x_2^2 - 2x_1x_2 + 1$

We need more ingredients

Monomial orderings

Admissible monomial orderings

Let $\prec$ be a total order over $\mathbb{N}^n$. We say that $\prec$ is an admissible monomial ordering if the following holds:

- $\mathbf{0} \preceq \boldsymbol{\alpha}$ for all $\boldsymbol{\alpha} \in \mathbb{N}^n$;
- if $\boldsymbol{\alpha} \prec \boldsymbol{\beta}$ then for any $\boldsymbol{\gamma} \in \mathbb{N}^n$ it holds that $\boldsymbol{\alpha} + \boldsymbol{\gamma} \prec \boldsymbol{\beta} + \boldsymbol{\gamma}$

  $\prec$ is compatible with multiplication
- there is no infinitely decreasing sequence $(\boldsymbol{\alpha}_i)_{i \in \mathbb{N}}$

There are many different ways to define admissible monomial orderings, which may have additional properties.

Some examples (I)

Lexicographical monomial ordering

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec_{lex} \boldsymbol{\beta} \iff \exists i \text{ such that } \begin{cases} \alpha_j = \beta_j \text{ for } j < i \\ \alpha_i < \beta_i \end{cases}$$

Some examples (I)

Lexicographical monomial ordering

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec_{lex} \boldsymbol{\beta} \iff \exists i \text{ such that } \begin{cases} \alpha_j = \beta_j \text{ for } j < i \\ \alpha_i < \beta_i \end{cases}$$

This ordering eliminates variables at first. It compares first the exponent of x_1, in case of equality it compares the exponent of x_2, and so on.

Examples

- $x_3^{10} \prec_{lex} x_2^3 \prec_{lex} x_1$
- $1 \prec_{lex} x_2 \prec_{lex} x_2^2 \prec_{lex} x_2^{1000} \prec_{lex} x_1 \prec_{lex} x_1 x_2 \prec_{lex} x_1^2$

Some examples (II)

Graded lexicographical monomial ordering

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec_{grlex} \boldsymbol{\beta} \iff \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \text{ or } \begin{cases} \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \\ \text{ and there exists } i \text{ such that} \\ \alpha_j = \beta_j \text{ for } j < i \\ \alpha_i < \beta_i \end{cases}$$

This ordering first filters monomials w.r.t. their degrees and next applies the lexicographical ordering.

Some examples (II)

Graded lexicographical monomial ordering

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec_{grlex} \boldsymbol{\beta} \Longleftrightarrow \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \text{ or } \begin{cases} \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \\ \text{ and there exists } i \text{ such that} \\ \alpha_j = \beta_j \text{ for } j < i \\ \alpha_i < \beta_i \end{cases}$$

This ordering first filters monomials w.r.t. their degrees and next applies the lexicographical ordering.

Feature. All monomials are preceded by a finite number of other monomials.

- $1 \prec_{grlex} x_3 \prec_{grlex} x_2 \prec_{grlex} x_1 \prec_{grlex} x_3^2 \prec_{grlex} x_2 x_3 \prec_{grlex} x_2^2 \prec_{grlex} x_1 x_3 \prec_{grlex} x_1 x_2 \prec_{grlex} x_1^2$

Some examples (III)

Graded reverse lexicographical monomial ordering

Let $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec_{grevlex} \boldsymbol{\beta} \iff \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \text{ or } \begin{cases} \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \\ \text{ and there exists } i \text{ such that} \\ \alpha_j = \beta_j \text{ for } j > i \\ \alpha_i > \beta_i \end{cases}$$

Some examples (III)

Graded reverse lexicographical monomial ordering

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec_{grevlex} \boldsymbol{\beta} \iff \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \text{ or } \begin{cases} \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \\ \text{ and there exists } i \text{ such that} \\ \alpha_j = \beta_j \text{ for } j > i \\ \alpha_i > \beta_i \end{cases}$$

Feature. All monomials are preceded by a finite number of other monomials.

Some examples (III)

Graded reverse lexicographical monomial ordering

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec_{grevlex} \boldsymbol{\beta} \iff \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \text{ or } \begin{cases} \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \\ \text{ and there exists } i \text{ such that} \\ \alpha_j = \beta_j \text{ for } j > i \\ \alpha_i > \beta_i \end{cases}$$

Feature. All monomials are preceded by a finite number of other monomials.

- $1 \prec_{grevlex} x_3 \prec_{grevlex} x_2 \prec_{grevlex} x_1 \prec_{grevlex} x_3^2 \prec_{grevlex} x_2x_3 \prec_{grevlex} x_1x_3 \prec_{grevlex} x_2^2 \prec_{grevlex} x_1x_2 \prec_{grevlex} x_1^2$

Some examples (II)

Block orderings

Let $\prec_1$ and $\prec_2$ be two admissible monomial orderings over $\mathbb{N}^i$ and $\mathbb{N}^j$ with $n = i + j$.

Let $\boldsymbol{\alpha} = (\underbrace{\alpha_1, \ldots, \alpha_i}_{\boldsymbol{\alpha}_1}, \underbrace{\alpha_{i+1}, \ldots, \alpha_n}_{\boldsymbol{\alpha}_2})$ in $\mathbb{N}^n$.

Let $\boldsymbol{\beta} = (\underbrace{\beta_1, \ldots, \beta_i}_{\boldsymbol{\beta}_1}, \underbrace{\beta_{i+1}, \ldots, \beta_n}_{\boldsymbol{\beta}_2})$ in $\mathbb{N}^n$.

Some examples (II)

Block orderings

Let $\prec_1$ and $\prec_2$ be two admissible monomial orderings over $\mathbb{N}^i$ and $\mathbb{N}^j$ with $n = i + j$.

Let $\boldsymbol{\alpha} = (\underbrace{\alpha_1, \ldots, \alpha_i}_{\boldsymbol{\alpha}_1}, \underbrace{\alpha_{i+1}, \ldots, \alpha_n}_{\boldsymbol{\alpha}_2})$ in $\mathbb{N}^n$.

Let $\boldsymbol{\beta} = (\underbrace{\beta_1, \ldots, \beta_i}_{\boldsymbol{\beta}_1}, \underbrace{\beta_{i+1}, \ldots, \beta_n}_{\boldsymbol{\beta}_2})$ in $\mathbb{N}^n$.

$$\boldsymbol{\alpha} \prec \boldsymbol{\beta} \iff \begin{cases} \boldsymbol{\alpha}_1 \prec_1 \boldsymbol{\beta}_1 \\ \text{or} \\ \boldsymbol{\alpha}_1 = \boldsymbol{\beta}_1 \text{ and} \\ \boldsymbol{\alpha}_2 \prec_2 \boldsymbol{\beta}_2 \end{cases}$$

Some more comments on monomial orderings

- The lexicographical ordering is the one which will enable triangular rewritings of the input system.
  However, its direct use is usually less efficient.

Some more comments on monomial orderings

- The lexicographical ordering is the one which will enable triangular rewritings of the input system.
  However, its direct use is usually less efficient.
- Graded orderings enjoy some interesting feature: any monomial is preceded by finitely many other monomials.

> The *grevlex* ordering is better suited to computing Gröbner bases as it is related to some intrinsic complexity measures for polynomial ideals (notions of regularity that will appear later in the course).

Bayer/Stillmann'87

Some more comments on monomial orderings

- The lexicographical ordering is the one which will enable triangular rewritings of the input system.
  However, its direct use is usually less efficient.
- Graded orderings enjoy some interesting feature: any monomial is preceded by finitely many other monomials.

  The *grevlex* ordering is better suited to computing Gröbner bases as it is related to some intrinsic complexity measures for polynomial ideals (notions of regularity that will appear later in the course).

Bayer/Stillmann'87

Change of ordering algorithms?

Leading monomials, coefficients and terms (I)

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

and $\prec$ be an admissible monomial ordering over R.

Leading monomials, coefficients and terms (I)

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

and $\prec$ be an admissible monomial ordering over R.

Recall that $f \in R$ is a finite sequence of coefficients in $\mathbb{K}$ (indexed by monomials of $\mathbb{N}^n$)

Assume $f \neq 0$ $\rightsquigarrow (c_{\boldsymbol{\alpha}_1}, \ldots, c_{\boldsymbol{\alpha}_t}) \in \mathbb{K} - \{0\}^t$.

Definition

Let $f \in R - \{0\}$. Let $1 \leq i \leq t$ be such that $\boldsymbol{\alpha}_j \prec \boldsymbol{\alpha}_i$ for all $1 \leq j \leq t$, $j \neq i$.

Leading monomials, coefficients and terms (I)

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

and $\prec$ be an admissible monomial ordering over R.

Recall that $f \in R$ is a finite sequence of coefficients in $\mathbb{K}$ (indexed by monomials of $\mathbb{N}^n$)

Assume $f \neq 0$ $\rightsquigarrow (c_{\boldsymbol{\alpha}_1}, \ldots, c_{\boldsymbol{\alpha}_t}) \in \mathbb{K} - \{0\}^t$.

Definition

Let $f \in R - \{0\}$. Let $1 \leq i \leq t$ be such that $\boldsymbol{\alpha}_j \prec \boldsymbol{\alpha}_i$ for all $1 \leq j \leq t$, $j \neq i$.

- The leading monomial of f w.r.t. $\prec$, denoted by $\mathsf{LM}_{\prec}(f)$, is $\boldsymbol{x}^{\boldsymbol{\alpha}_i}$.

Leading monomials, coefficients and terms (I)

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

and $\prec$ be an admissible monomial ordering over R.

Recall that $f \in R$ is a finite sequence of coefficients in $\mathbb{K}$ (indexed by monomials of $\mathbb{N}^n$)

Assume $f \neq 0$ $\rightsquigarrow (c_{\boldsymbol{\alpha}_1}, \ldots, c_{\boldsymbol{\alpha}_t}) \in \mathbb{K} - \{0\}^t$.

Definition

Let $f \in R - \{0\}$. Let $1 \leq i \leq t$ be such that $\boldsymbol{\alpha}_j \prec \boldsymbol{\alpha}_i$ for all $1 \leq j \leq t$, $j \neq i$.

- The leading monomial of f w.r.t. $\prec$, denoted by $\mathrm{LM}_{\prec}(f)$, is $\boldsymbol{x}^{\boldsymbol{\alpha}_i}$.
- The leading term of f w.r.t. $\prec$, denoted by $\mathrm{LT}_{\prec}(f)$, is $c_{\boldsymbol{\alpha}_i}\boldsymbol{x}^{\boldsymbol{\alpha}_i}$.

Leading monomials, coefficients and terms (I)

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

and $\prec$ be an admissible monomial ordering over R.

Recall that $f \in R$ is a finite sequence of coefficients in $\mathbb{K}$ (indexed by monomials of $\mathbb{N}^n$)

Assume $f \neq 0$ $\rightsquigarrow (c_{\boldsymbol{\alpha}_1}, \ldots, c_{\boldsymbol{\alpha}_t}) \in \mathbb{K} - \{0\}^t$.

Definition

Let $f \in R - \{0\}$. Let $1 \leq i \leq t$ be such that $\boldsymbol{\alpha}_j \prec \boldsymbol{\alpha}_i$ for all $1 \leq j \leq t$, $j \neq i$.

- The leading monomial of f w.r.t. $\prec$, denoted by $\mathrm{LM}_{\prec}(f)$, is $\boldsymbol{x}^{\boldsymbol{\alpha}_i}$.
- The leading term of f w.r.t. $\prec$, denoted by $\mathrm{LT}_{\prec}(f)$, is $c_{\boldsymbol{\alpha}_i}\boldsymbol{x}^{\boldsymbol{\alpha}_i}$.
- The leading coefficient of f w.r.t. $\prec$, denoted by $\mathrm{LC}_{\prec}(f)$, is $c_{\boldsymbol{\alpha}_i}$.

Leading monomials, coefficients and terms (II)

Consider again

$$f_1 = x_1^2 + 2x_2^2 + 5x_1x_2 - 1$$

$$f_2 = x_1^2 - 3x_2^2 - 2x_1x_2 + 1$$

Leading monomials, coefficients and terms (II)

Consider again

$$f_1 = x_1^2 + 2x_2^2 + 5x_1x_2 - 1$$
$$f_2 = x_1^2 - 3x_2^2 - 2x_1x_2 + 1$$

Consider $\prec_{lex}$, $\prec_{grlex}$ and $\prec_{grevlex}$.
Compute the leading monomials, terms and coefficients of f_1, f_2.

Leading monomials, coefficients and terms (II)

Consider again

$f_1 = x_1^2 + 2x_2^2 + 5x_1x_2 - 1$

$f_2 = x_1^2 - 3x_2^2 - 2x_1x_2 + 1$

Consider $\prec_{lex}$, $\prec_{grlex}$ and $\prec_{grevlex}$.
Compute the leading monomials, terms and coefficients of f_1, f_2.

We choose now $\prec_{grevlex}$.

Leading monomials, coefficients and terms (II)

Consider again

$$f_1 = x_1^2 + 2x_2^2 + 5x_1x_2 - 1$$
$$f_2 = x_1^2 - 3x_2^2 - 2x_1x_2 + 1$$

Consider $\prec_{lex}$, $\prec_{grlex}$ and $\prec_{grevlex}$.
Compute the leading monomials, terms and coefficients of f_1, f_2.

We choose now $\prec_{grevlex}$.

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \end{aligned} \quad \rightsquigarrow \quad \begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 &= f_1 - f_2 = \boxed{7x_1x_2} + 5x_2^2 \end{aligned}$$

Leading monomials, coefficients and terms (II)

Consider again

$$f_1 = x_1^2 + 2x_2^2 + 5x_1x_2 - 1$$
$$f_2 = x_1^2 - 3x_2^2 - 2x_1x_2 + 1$$

Consider $\prec_{lex}$, $\prec_{grlex}$ and $\prec_{grevlex}$.
Compute the leading monomials, terms and coefficients of f_1, f_2.

We choose now $\prec_{grevlex}$.

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \end{aligned} \quad \rightsquigarrow \quad \begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 = f_1 - f_2 &= \boxed{7x_1x_2} + 5x_2^2 \end{aligned}$$

Observe that $g_1 \in \langle f_1, f_2 \rangle$ brings a new information:
$\mathsf{LM}_{grevlex}(g_1) \notin \langle \mathsf{LM}_{grevlex}(f_1), \mathsf{LM}_{grevlex}(f_2) \rangle$
What could be the next steps?

Eliminating terms – towards critical pairs

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \end{aligned} \rightsquigarrow \begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 = f_1 - f_2 &= \boxed{7x_1x_2} + 5x_2^2 \end{aligned}$$

Eliminating terms – towards critical pairs

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \end{aligned} \quad \rightsquigarrow \quad \begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 = f_1 - f_2 &= \boxed{7x_1x_2} + 5x_2^2 \end{aligned}$$

Remark that x_1g_1, x_2f_1 and x_2f_2 share the same leading monomial.

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 &= f_1 - f_2 = \boxed{7x_1x_2} + 5x_2^2 \\ g_2 &= 7x_2f_1 - x_1g_1 = \boxed{30x_1x_2^2} + 14x_2^3 - 7x_2 \\ g_3 &= x_1g_1 - 7x_2f_2 = \boxed{-19x_1x_2^2} - 21x_2^3 - 7x_2 \end{aligned}$$

Eliminating terms – towards critical pairs

$$
\begin{aligned}
f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\
f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1
\end{aligned}
\quad \rightsquigarrow \quad
\begin{aligned}
f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\
f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\
g_1 &= f_1 - f_2 = \boxed{7x_1x_2} + 5x_2^2
\end{aligned}
$$

Remark that x_1g_1, x_2f_1 and x_2f_2 share the same leading monomial.

$$
\begin{aligned}
f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\
f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\
g_1 &= f_1 - f_2 = \boxed{7x_1x_2} + 5x_2^2 \\
g_2 &= 7x_2f_1 - x_1g_1 = \boxed{30x_1x_2^2} + 14x_2^3 - 7x_2 \\
g_3 &= x_1g_1 - 7x_2f_2 = \boxed{-19x_1x_2^2} - 21x_2^3 - 7x_2
\end{aligned}
$$

No new information ($g_3 \in \langle f_1, f_2 \rangle$ and
$\mathrm{LM}_{grevlex}(g_3) \in \langle \mathrm{LM}_{grevlex}(f_1), \mathrm{LM}_{grevlex}(f_2), \mathrm{LM}_{grevlex}(g_1) \rangle$)

Eliminating terms – towards critical pairs

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \end{aligned} \quad \rightsquigarrow \quad \begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 &= f_1 - f_2 = \boxed{7x_1x_2} + 5x_2^2 \end{aligned}$$

Remark that x_1g_1, x_2f_1 and x_2f_2 share the same leading monomial.

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 &= f_1 - f_2 = \boxed{7x_1x_2} + 5x_2^2 \\ g_2 &= 7x_2f_1 - x_1g_1 = \boxed{30x_1x_2^2} + 14x_2^3 - 7x_2 \\ g_3 &= x_1g_1 - 7x_2f_2 = \boxed{-19x_1x_2^2} - 21x_2^3 - 7x_2 \end{aligned}$$

No new information ($g_3 \in \langle f_1, f_2 \rangle$ and
$\mathrm{LM}_{grevlex}(g_3) \in \langle \mathrm{LM}_{grevlex}(f_1), \mathrm{LM}_{grevlex}(f_2), \mathrm{LM}_{grevlex}(g_1) \rangle$) apparently.

Eliminating terms – towards critical pairs

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \end{aligned} \quad \rightsquigarrow \quad \begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 = f_1 - f_2 &= \boxed{7x_1x_2} + 5x_2^2 \end{aligned}$$

Remark that x_1g_1, x_2f_1 and x_2f_2 share the same leading monomial.

$$\begin{aligned} f_1 &= \boxed{x_1^2} + 2x_2^2 + 5x_1x_2 - 1 \\ f_2 &= \boxed{x_1^2} - 3x_2^2 - 2x_1x_2 + 1 \\ g_1 &= f_1 - f_2 = \boxed{7x_1x_2} + 5x_2^2 \\ g_2 &= 7x_2f_1 - x_1g_1 = \boxed{30x_1x_2^2} + 14x_2^3 - 7x_2 \\ g_3 &= x_1g_1 - 7x_2f_2 = \boxed{-19x_1x_2^2} - 21x_2^3 - 7x_2 \end{aligned}$$

No new information ($g_3 \in \langle f_1, f_2 \rangle$ and $\mathrm{LM}_{grevlex}(g_3) \in \langle \mathrm{LM}_{grevlex}(f_1), \mathrm{LM}_{grevlex}(f_2), \mathrm{LM}_{grevlex}(g_1) \rangle$) apparently.

$\rightsquigarrow$ $g_2 - g_3$ brings a new important one.

Remember the ascending chains of ideals theorem...

Summary

Admissible monomial orders

Mimic degree extension step in Euclidean divison

New specific question: ideal membership for monomial ideals

More is needed...

S-polynomials (I)

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

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ be two monomials of R. The least common multiple of $\boldsymbol{\alpha}, \boldsymbol{\beta}$ ($\mathrm{lcm}(\boldsymbol{\alpha}, \boldsymbol{\beta})$) is the monomial $(\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n))$.

S-polynomials (I)

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

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ be two monomials of R. The least common multiple of $\boldsymbol{\alpha}, \boldsymbol{\beta}$ ($\mathrm{lcm}(\boldsymbol{\alpha}, \boldsymbol{\beta})$) is the monomial $(\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n))$.

- Back to a notation with variables, it generates $\langle \boldsymbol{x}^{\alpha} \rangle \cap \langle \boldsymbol{x}^{\boldsymbol{\beta}} \rangle$.

S-polynomials (I)

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

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ be two monomials of R.
The least common multiple of $\boldsymbol{\alpha}, \boldsymbol{\beta}$ ($\mathsf{lcm}(\boldsymbol{\alpha}, \boldsymbol{\beta})$) is the monomial $(\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n))$.

- Back to a notation with variables, it generates $\langle \boldsymbol{x}^{\alpha} \rangle \cap \langle \boldsymbol{x}^{\boldsymbol{\beta}} \rangle$.
- For f, g in $R - \{0\}$, we define $\mathsf{lcm}_{\prec}(f, g) = \mathsf{lcm}(\mathsf{LM}_{\prec}(f), \mathsf{LM}_{\prec}(g))$.

S-polynomials (II)

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

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

S-polynomials (II)

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

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

- $\mathsf{spol}_{\prec}(f, g) \in \langle f, g \rangle$

S-polynomials (II)

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

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

- $\mathrm{spol}_{\prec}(f, g) \in \langle f, g \rangle$
- As illustrated in the previous example, S-polynomials play a prominent role in discovering new relevant polynomials g in some polynomial ideal $\langle f_1, \ldots, f_s \rangle$.

S-polynomials (II)

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

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

- $\mathsf{spol}_{\prec}(f, g) \in \langle f, g \rangle$
- As illustrated in the previous example, S-polynomials play a prominent role in discovering new relevant polynomials g in some polynomial ideal $\langle f_1, \ldots, f_s \rangle$.

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

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

Ideal membership problem for monomial ideals

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

Monomial ideals

Let $I \subset R$ be an ideal. One says that I is a monomial ideal iff there exists a subset S of monomials such that $I = \langle S \rangle$.

Note that we do not assume S to be finite. Hilbert's basis theorem implies that I is finitely generated by elements of R, not by monomials.

Lemma

Let $I \subset R$ be a monomial ideal and $S \subset R$ be a set of monomial generators for I. Let $\boldsymbol{x}^{\boldsymbol{\alpha}}$ be a monomial. The following holds:

$$\boldsymbol{x}^{\boldsymbol{\alpha}} \in I \iff \boldsymbol{x}^{\boldsymbol{\alpha}} \text{ is divisible by some monomial in } S$$

Ideal membership problem for monomial ideals

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

Monomial ideals

Let $I \subset R$ be an ideal. One says that I is a monomial ideal iff there exists a subset S of monomials such that $I = \langle S \rangle$.

Note that we do not assume S to be finite. Hilbert's basis theorem implies that I is finitely generated by elements of R, not by monomials.

Lemma

Let $I \subset R$ be a monomial ideal and $S \subset R$ be a set of monomial generators for I. Let $\boldsymbol{x}^{\boldsymbol{\alpha}}$ be a monomial. The following holds:

$$\boldsymbol{x}^{\boldsymbol{\alpha}} \in I \iff \boldsymbol{x}^{\boldsymbol{\alpha}} \text{ is divisible by some monomial in } S$$

Dickson's Lemma

Let $I \subset R$ be a monomial ideal. It holds that I has a finite monomial basis.

Hilbert series (I)

Let $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_s} \rangle$

We define the Hilbert function as follows:

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

Hilbert series (I)

Let $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_s} \rangle$

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

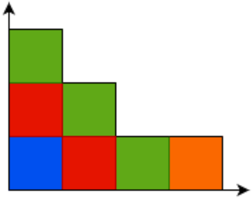
Hilbert series (I)

Let $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_s} \rangle$

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



Take $I = \langle x_1^4, x_1^2 x_2, x_1 x_2^2, x_2^3 \rangle$

$$\mathrm{HS}_I(t) = 1 + 2t + 3t^2 + t^3$$