Mathematical Principles in Vision and Graphics: Solving Polynomial Systems

Ass.Prof. Friedrich Fraundorfer

SS2018

Slides by Vincent Lepetit

May 16, 2018

Polynomial Systems in Computer Vision

Many Computer Vision problems can be solved by finding the roots of a polynomial system:

- camera pose estimation from point correspondences;
- camera relative motion estimation from point correspondences;
- image distortion calibration;
- point triangulation;
- ...

Solving Polynomial Systems

- no general method;

Solving Polynomial Systems

- no general method;
- several mathematical tools exist. For a given problem, a tool can be more adapted than the others.

Gröbner Bases

- introduced in 1965 by Bruno Buchberger (now at the Johannes Kepler University in Linz) in his Ph.D. thesis (named after his advisor Wolfgang Gröbner) to study sets of polynomials

A Polynomial System

Let consider the following polynomial system:

$$\begin{array}{l} L_1 \\ L_2 \\ L_3 \end{array} \left\{ \begin{array}{rcl} 2x^2 + y^2 - 2z + 3z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2 y^2 + y^2 z^2 - 2 & = & 0 \end{array} \right.$$

A Polynomial System

Let consider the following polynomial system:

$$\begin{array}{l} L_1 \\ L_2 \\ L_3 \end{array} \left\{ \begin{array}{rcl} 2x^2 + y^2 - 2z + 3z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2 y^2 + y^2 z^2 - 2 & = & 0 \end{array} \right.$$

Hint: try to remove x from the first equation

A Polynomial System

Let consider the following polynomial system:

$$\begin{array}{l} L_1 \\ L_2 \\ L_3 \end{array} \left\{ \begin{array}{rcl} 2x^2 + y^2 - 2z + 3z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \end{array} \right.$$

Hint: try to remove x from the first equation

Replace L_1 by $L_1 - 2L_2$:

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \end{array} \right.$$

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2 y^2 + y^2 z^2 - 2 & = & 0 \end{array} \right.$$

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \end{array} \begin{cases} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2 y^2 + y^2 z^2 - 2 & = & 0 \end{cases}$$

Hint: try to remove x from the second equation:

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \end{array} \right.$$

Hint: try to remove x from the second equation:

Adding $y^2 L_2 - L_3$:

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \end{array} \right.$$

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \end{array} \right.$$

A Real Polynomial System (continued)

$$
\begin{array}{l}
L_1' \\
L_2 \\
L_3 \\
L_4
\end{array}
\left\{
\begin{array}{rcl}
y^2 - 4z + z^2 + 5 & = & 0 \\
x^2 + z + z^2 & = & 0 \\
x^2 y^2 + y^2 z^2 - 2 & = & 0 \\
y^2 z + 2 & = & 0
\end{array}
\right.
$$

Hint: try to remove y from the first equation

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \end{array} \right.$$

Hint: try to remove y from the first equation

Add $yL_1' - L_4$:

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array} \right.$$

A Real Polynomial System (continued)

$$
\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array}
\left\{
\begin{array}{rcl}
y^2 - 4z + z^2 + 5 & = & 0 \\
x^2 + z + z^2 & = & 0 \\
x^2 y^2 + y^2 z^2 - 2 & = & 0 \\
y^2 z + 2 & = & 0 \\
5z - 4z^2 + z^3 - 2 & = & 0
\end{array}
\right.
$$

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array} \right.$$

Hint: L_5 is a polynomial in z only

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array} \right.$$

Hint: L_5 is a polynomial in z only

$5z - 4z^2 + z^3 - 2 = (z-1)^2(z-2)$

Each possible value for z gives a new polynomial system in x and y only.

Solving a Univariate Polynomial

- closed form up to degree 4;

Solving a Univariate Polynomial

- closed form up to degree 4;
- for higher degrees:
  - the companion matrix method: The *companion matrix* of $p(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$ is

$$\mathbf{C} = \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & -a_2 \\ & & \ddots & & \vdots \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

Solving a Univariate Polynomial

- closed form up to degree 4;
- for higher degrees:
  - the companion matrix method: The *companion matrix* of $p(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$ is

$$\mathbf{C} = \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & -a_2 \\ & & \ddots & & \vdots \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

Its eigenvalues are the roots of $p(z)$ (because $p(z)$ is the characteristic polynomial $\det(z\mathbf{I} - \mathbf{C})$ of $\mathbf{C}$).

Solving a Univariate Polynomial

- closed form up to degree 4;
- for higher degrees:
  - the companion matrix method: The *companion matrix* of $p(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$ is

$$\mathbf{C} = \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & -a_2 \\ & & \ddots & & \vdots \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

    Its eigenvalues are the roots of $p(z)$ (because $p(z)$ is the characteristic polynomial $\det(z\mathbf{I} - \mathbf{C})$ of $\mathbf{C}$).
  - Sturm's bracketing method (slightly less stable but much faster).

Two Gröbner bases

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array} \right.$$

$$\left\{ y^2 - 4z + z^2 + 5, x^2 + z + z^2, x^2y^2 + y^2z^2 - 2, y^2z + 2, 5z - 4z^2 + z^3 - 2 \right\}$$

is a Gröbner basis.

Two Gröbner bases

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array} \right.$$

$$\left\{ y^2 - 4z + z^2 + 5, x^2 + z + z^2, x^2y^2 + y^2z^2 - 2, y^2z + 2, 5z - 4z^2 + z^3 - 2 \right\}$$

is a Gröbner basis.

$$\left\{ y^2 - 4z + z^2 + 5, x^2 + z + z^2, 5z - 4z^2 + z^3 - 2 \right\}$$

is also a Gröbner basis.

A Gröbner basis is a set of polynomials $\{g_1, \ldots, g_t\}$, such that the system

$$\left\{ \begin{array}{rcl} g_1(x_1, \ldots, x_n) & = & 0 \\ & \cdots & \\ g_t(x_1, \ldots, x_n) & = & 0 \end{array} \right.$$

A Gröbner basis is a set of polynomials $\{g_1, \ldots, g_t\}$, such that the system

$$\left\{ \begin{array}{rcl} g_1(x_1, \ldots, x_n) & = & 0 \\ & \ldots & \\ g_t(x_1, \ldots, x_n) & = & 0 \end{array} \right.$$

has the same solutions as the original one,

but with some specific properties that make the new system easier to solve than the original one, OR AT LEAST USEFUL to solve the original one.

Tools

We can create new equations from:

- linear combinations of existing equations.

Tools

We can create new equations from:

- linear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system.

Tools

We can create new equations from:

- linear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system. For example, we can write the system:

$$\begin{cases} 2x^2 + xy + y^2 + 1 & = & 0 \\ x^2 - xy + 2y^2 - 1 & = & 0 \end{cases}$$

  in matrix form:

Tools

We can create new equations from:

- linear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system. For example, we can write the system:

$$\begin{cases} 2x^2 + xy + y^2 + 1 & = & 0 \\ x^2 - xy + 2y^2 - 1 & = & 0 \end{cases}$$

  in matrix form:

$$\begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & -1 & 2 & -1 \end{bmatrix} \begin{bmatrix} x^2 \\ xy \\ y^2 \\ 1 \end{bmatrix} = 0\,.$$

Tools

We can create new equations from:

- linear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system. For example, we can write the system:

$$\begin{cases} 2x^2 + xy + y^2 + 1 & = & 0 \\ x^2 - xy + 2y^2 - 1 & = & 0 \end{cases}$$

  in matrix form:

$$\begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & -1 & 2 & -1 \end{bmatrix} \begin{bmatrix} x^2 \\ xy \\ y^2 \\ 1 \end{bmatrix} = 0\,.$$

  After Gauss-Jordan elimination:

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 \end{bmatrix} \begin{bmatrix} x^2 \\ xy \\ y^2 \\ 1 \end{bmatrix} = 0\,.$$

Tools

We can create new equations from:

- linear combinations of existing equations.
- *algebraic* combinations of existing equations.

Tools

We can create new equations from:

- linear combinations of existing equations.
- *algebraic* combinations of existing equations.
- the remainder of polynomial divisions (used by Buchberger's algorithm).

Notations and Definitions

Fields

A *field* is a set where one can define addition, subtraction, multiplication, and division with the usual properties.

Fields

A *field* is a set where one can define addition, subtraction, multiplication, and division with the usual properties.

For example, the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, the complex numbers $\mathbb{C}$ are fields.

The integers $\mathbb{Z}$ are not a field (division fails).

Fields

A *field* is a set where one can define addition, subtraction, multiplication, and division with the usual properties.

For example, the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, the complex numbers $\mathbb{C}$ are fields.

The integers $\mathbb{Z}$ are not a field (division fails).

The coefficients of polynomials and the variables take their values from a field.

Monomials

Definition. A **monomial** in $x_1, \ldots, x_n$ is a product of the form:

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots \cdot x_n^{\alpha_n},$$

where all the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers, sometimes noted $\mathbf{x}^\alpha$ with $\alpha = (\alpha_1, \ldots, \alpha_n)$.

Examples: x, x^2, $x^2 y$, $x^2 y z^3$

Polynomials

Definition. A **polynomial** f in $x_1, \ldots, x_n$ with coefficients in a field k is a finite linear combination with coefficients in k of monomials. A polynomial is written in the form

$$f = \sum_{\alpha} a_\alpha \mathbf{x}^\alpha, \quad a_\alpha \in k$$

with

- a_α the **coefficient** of the monomial $\mathbf{x}^\alpha$.

Polynomials

Definition. A **polynomial** f in $x_1, \ldots, x_n$ with coefficients in a field k is a finite linear combination with coefficients in k of monomials. A polynomial is written in the form

$$f = \sum_{\alpha} a_\alpha \mathbf{x}^\alpha, \quad a_\alpha \in k$$

with

- a_α the **coefficient** of the monomial $\mathbf{x}^\alpha$.
- If $a_\alpha \neq 0$, then we call $a_\alpha \mathbf{x}^\alpha$ a **term** of f.

Notations: $k[x_1, \ldots, x_n]$

Notation. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

Notations: $k[x_1, \ldots, x_n]$

Notation. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

$k[x]$ is the set of polynomials in one variable: $x^2 - x \in k[x]$, $x^3 + 4x \in k[x]$.

Notations: $k[x_1, \ldots, x_n]$

Notation. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

$k[x]$ is the set of polynomials in one variable: $x^2 - x \in k[x]$, $x^3 + 4x \in k[x]$.

$k[x, y]$ is the set of polynomials in two variables: $x^2 - y \in k[x, y]$, $x^3 + 2xy + y^2 \in k[x, y]$.

Ideals

Definition. A subset $I \in k[x_1, \ldots, x_n]$ is an **ideal** if

Ideals

Definition. A subset $I \in k[x_1, \dots, x_n]$ is an **ideal** if

- $\forall f \in I, g \in I \quad f + g \in I$;

Ideals

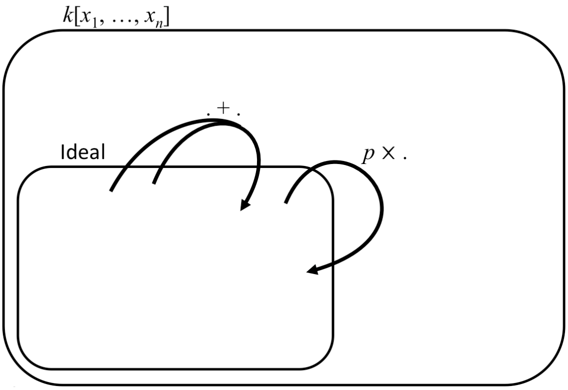
Definition. A subset $I \in k[x_1, \ldots, x_n]$ is an **ideal** if

- $\forall f \in I, g \in I \quad f + g \in I$;
- $\forall f \in I, p \in k[x_1, \ldots, x_n], \quad p \times f \in I$.

Ideals

Definition. A subset $I \in k[x_1, \ldots, x_n]$ is an **ideal** if

- $\forall f \in I, g \in I \quad f + g \in I;$
- $\forall f \in I, p \in k[x_1, \ldots, x_n], \quad p \times f \in I.$



Notations: $\langle \mathbf{f_1}, \ldots, \mathbf{f_s} \rangle$

Definition. Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. $\langle f_1, \ldots, f_s \rangle$ denotes the set:

Notations: $\langle \mathbf{f_1}, \ldots, \mathbf{f_s} \rangle$

Definition. Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. $\langle f_1, \ldots, f_s \rangle$ denotes the set:

$\langle f_1, \ldots, f_s \rangle = \{ p_1.f_1 + \ldots + p_s.f_s \,:\, p_i \in k[x_1, \ldots, x_n]$ for $i = 1, \ldots, s \}$.

Notations: $\langle \mathbf{f_1}, \ldots, \mathbf{f_s} \rangle$

Definition. Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. $\langle f_1, \ldots, f_s \rangle$ denotes the set:

$$\langle f_1, \ldots, f_s \rangle = \{p_1.f_1 + \ldots + p_s.f_s \,:\, p_i \in k[x_1, \ldots, x_n] \text{ for } i = 1, \ldots, s\}\ .$$

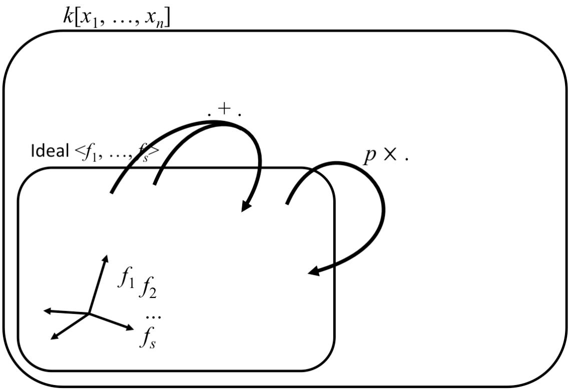
It is easy to show that $\langle f_1, \ldots, f_s \rangle$ *is an ideal.*

Notations: $\langle \mathbf{f_1}, \ldots, \mathbf{f_s} \rangle$

Definition. Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. $\langle f_1, \ldots, f_s \rangle$ denotes the set:

$$\langle f_1, \ldots, f_s \rangle = \{p_1.f_1 + \ldots + p_s.f_s \,:\, p_i \in k[x_1, \ldots, x_n] \text{ for } i = 1, \ldots, s\}\ .$$

It is easy to show that $\langle f_1, \ldots, f_s \rangle$ is an ideal.



Ideal - example

For example, let consider the ideal $I = \langle x - y^2, xy \rangle$.

- Is $x^2 - xy^2 \in I$?

Ideal - example

For example, let consider the ideal $I = \langle x - y^2, xy \rangle$.

- Is $x^2 - xy^2 \in I$? Yes, because $x^2 - xy^2 = x.(x - y^2) + 0.xy$.

Ideal - example

For example, let consider the ideal $I = \langle x - y^2, xy \rangle$.

- Is $x^2 - xy^2 \in I$? Yes, because $x^2 - xy^2 = x.(x - y^2) + 0.xy$.
- Is $x^2 \in I$?

Ideal - example

For example, let consider the ideal $I = \langle x - y^2, xy \rangle$.

- Is $x^2 - xy^2 \in I$? Yes, because $x^2 - xy^2 = x.(x - y^2) + 0.xy$.
- Is $x^2 \in I$? Yes, because $x^2 = x.(x - y^2) + y.xy$.

Ideal - example

For example, let consider the ideal $I = \langle x - y^2, xy \rangle$.

- Is $x^2 - xy^2 \in I$? Yes, because $x^2 - xy^2 = x.(x - y^2) + 0.xy$.
- Is $x^2 \in I$? Yes, because $x^2 = x.(x - y^2) + y.xy$.
- Is $y \in I$?

Ideal - example

For example, let consider the ideal $I = \langle x - y^2, xy \rangle$.

- Is $x^2 - xy^2 \in I$? Yes, because $x^2 - xy^2 = x.(x - y^2) + 0.xy$.
- Is $x^2 \in I$? Yes, because $x^2 = x.(x - y^2) + y.xy$.
- Is $y \in I$? No, there is no $p_1, p_2 \in k[x_1, \ldots, x_n]$ such that $y = p_1.(x - y^2) + p_2.xy$.

Motivation for the Notion of Ideal

If $(a_1, \ldots, a_n) \in k^n$ is such that

$$\forall\, 1 \leq i \leq s \;\; f_i(a_1, \ldots, a_n) = 0\,,$$

Motivation for the Notion of Ideal

If $(a_1, \ldots, a_n) \in k^n$ is such that

$$\forall\, 1 \leq i \leq s \;\; f_i(a_1, \ldots, a_n) = 0\,,$$

then

$$\forall\, p \in \langle f_1, \ldots, f_s \rangle \quad p(a_1, \ldots, a_n) = 0\,.$$

Motivation for the Notion of Ideal

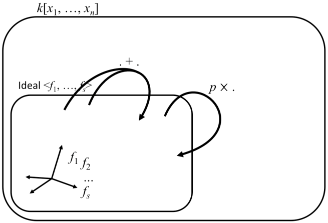
If $(a_1, \ldots, a_n) \in k^n$ is such that

$$\forall\, 1 \leq i \leq s \;\; f_i(a_1, \ldots, a_n) = 0\,,$$

then

$$\forall\, p \in \langle f_1, \ldots, f_s \rangle \;\; p(a_1, \ldots, a_n) = 0\,.$$

In other words, the ideal generated by a polynomial system is made of all the polynomials that can be added to the system without changing the solutions.



Affine Varieties - Sets of Solutions

Definition. The set

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0 \quad \forall\, 1 \leq i \leq s\}.$$

is called the **affine variety** defined by polynomials $f_1, \ldots, f_s$ in $k[x_1, \ldots, x_n]$.

Affine Varieties - Sets of Solutions

Definition. The set

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \,:\, f_i(a_1, \ldots, a_n) = 0 \quad \forall\, 1 \le i \le s\}\,.$$

is called the **affine variety** defined by polynomials $f_1, \ldots, f_s$ in $k[x_1, \ldots, x_n]$.

Examples:

- $\mathbf{V}(x^2 + y^2 - 1)$ is

Affine Varieties - Sets of Solutions

Definition. The set

$$\mathbf{V}(f_1,\ldots,f_s) = \{(a_1,\ldots,a_n) \in k^n : f_i(a_1,\ldots,a_n) = 0 \quad \forall\, 1 \le i \le s\}\,.$$

is called the **affine variety** defined by polynomials $f_1,\ldots,f_s$ in $k[x_1,\ldots,x_n]$.

Examples:

- $\mathbf{V}(x^2+y^2-1)$ is the circle of radius 1 centered at the origin;
- $\mathbf{V}(x^2+y^2-1, x)$ is

Affine Varieties - Sets of Solutions

Definition. The set

$$\mathbf{V}(f_1,\ldots,f_s)=\{(a_1,\ldots,a_n)\in k^n : f_i(a_1,\ldots,a_n)=0 \quad \forall\, 1\le i\le s\}\,.$$

is called the **affine variety** defined by polynomials $f_1,\ldots,f_s$ in $k[x_1,\ldots,x_n]$.

Examples:

- $\mathbf{V}(x^2+y^2-1)$ is the circle of radius 1 centered at the origin;
- $\mathbf{V}(x^2+y^2-1,x)$ is the set $\{(0,1),(0,-1)\}$.

Definition - Leading Term $\mathrm{LT}(f)$

Definition. Given a nonzero polynomial $f \in k[x]$, let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m \, ,$$

where $a_i \in k$ and $a_0 \neq 0$.

Definition - Leading Term $\mathrm{LT}(f)$

Definition. Given a nonzero polynomial $f \in k[x]$, let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m \,,$$

where $a_i \in k$ and $a_0 \neq 0$.

$a_0 x^m$ is called the *leading term* of f.

Definition - Leading Term $\mathrm{LT}(f)$

Definition. Given a nonzero polynomial $f \in k[x]$, let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m \,,$$

where $a_i \in k$ and $a_0 \neq 0$.

$a_0 x^m$ is called the *leading term* of f.

We will write $\mathrm{LT}(f) = a_0 x^m$.

Dividing Multivariate Polynomials?

Is there a division for polynomials in several variables?

Dividing Multivariate Polynomials?

Is there a division for polynomials in several variables?

The answer is yes, but we need to decide which term of a polynomial is the leading term.

Dividing Multivariate Polynomials?

Is there a division for polynomials in several variables?

The answer is yes, but we need to decide which term of a polynomial is the leading term.

For example, what is the leading term of $x^2 + xy + y^2$?

Dividing Multivariate Polynomials?

Is there a division for polynomials in several variables?

The answer is yes, but we need to decide which term of a polynomial is the leading term.

For example, what is the leading term of $x^2 + xy + y^2$?

To decide, we will define a *monomial order*.

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

1. $>$ is a total (linear) ordering relation:
   there is only one possible to order in increasing order under $>$ a set of monomials;

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

1. $>$ is a total (linear) ordering relation:
   there is only one possible to order in increasing order under $>$ a set of monomials;
2. $>$ is compatible with multiplication:

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

1. $>$ is a total (linear) ordering relation:
   there is only one possible to order in increasing order under $>$ a set of monomials;
2. $>$ is compatible with multiplication:
   if $x^\alpha > x^\beta$ and x^γ is any monomial, then
   $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^\beta x^\gamma = x^{\beta+\gamma}$;

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

1. $>$ is a total (linear) ordering relation:
   there is only one possible to order in increasing order under $>$ a set of monomials;
2. $>$ is compatible with multiplication:
   if $x^\alpha > x^\beta$ and x^γ is any monomial, then
   $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^\beta x^\gamma = x^{\beta+\gamma}$;
3. $>$ is a well-ordering:

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

1. $>$ is a total (linear) ordering relation:
   there is only one possible to order in increasing order under $>$ a set of monomials;
2. $>$ is compatible with multiplication:
   if $x^\alpha > x^\beta$ and x^γ is any monomial, then
   $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^\beta x^\gamma = x^{\beta+\gamma}$;
3. $>$ is a well-ordering:
   every nonempty set of monomials has a smallest element under $>$.

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

1. $>$ is a total (linear) ordering relation:
   there is only one possible to order in increasing order under $>$ a set of monomials;
2. $>$ is compatible with multiplication:
   if $x^\alpha > x^\beta$ and x^γ is any monomial, then
   $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^\beta x^\gamma = x^{\beta+\gamma}$;
3. $>$ is a well-ordering:
   every nonempty set of monomials has a smallest element under $>$.

Monomial Order on $k[x]$

The only monomial order on $k[x]$ is the degree order, given by:

$$\ldots > x^{n+1} > x^n > \ldots > x^2 > x > 1.$$

Monomial Orders on $k[x_1, \ldots, x_n]$

For polynomials in several variables, there are many choices of monomial orders.

Monomial Orders on $k[x_1, \ldots, x_n]$

For polynomials in several variables, there are many choices of monomial orders.

Let's first define an order on the variables: $x_1 > x_2 > \ldots > x_n$ (this is not a monomial order), and $x > y > z$.

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Lexicographic Order $>_{lex}$

Definition. The lexicographic order: analogous to the ordering of words in a dictionary.

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Lexicographic Order $>_{lex}$

Definition. The lexicographic order: analogous to the ordering of words in a dictionary.

For example, under this order $>_{lex}$:

$$x^2 >_{lex} xy^2 >_{lex} xy >_{lex} x >_{lex} y$$

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Lexicographic Order $>_{lex}$

Definition. The lexicographic order: analogous to the ordering of words in a dictionary.

For example, under this order $>_{lex}$:

$$x^2 >_{lex} xy^2 >_{lex} xy >_{lex} x >_{lex} y$$

Formal definition: $x^\alpha >_{lex} x^\beta$ if in the difference $\alpha - \beta$ (which belongs to $\mathbb{Z}^n$), the leftmost nonzero entry is positive.

Monomial Orders on $k[x_1, \dots, x_n]$ - the Lexicographic Order $>_{lex}$

Definition. The lexicographic order: analogous to the ordering of words in a dictionary.

For example, under this order $>_{lex}$:

$$x^2 >_{lex} xy^2 >_{lex} xy >_{lex} x >_{lex} y$$

Formal definition: $x^\alpha >_{lex} x^\beta$ if in the difference $\alpha - \beta$ (which belongs to $\mathbb{Z}^n$), the leftmost nonzero entry is positive.

$x^2yz^3 >_{lex} x^2z^4$ or $x^2z^4 >_{lex} x^2yz^3$?

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Lexicographic Order $>_{lex}$

Definition. The lexicographic order: analogous to the ordering of words in a dictionary.

For example, under this order $>_{lex}$:

$$x^2 >_{lex} xy^2 >_{lex} xy >_{lex} x >_{lex} y$$

Formal definition: $x^\alpha >_{lex} x^\beta$ if in the difference $\alpha - \beta$ (which belongs to $\mathbb{Z}^n$), the leftmost nonzero entry is positive.

$x^2yz^3 >_{lex} x^2z^4$ or $x^2z^4 >_{lex} x^2yz^3$?

$\rightarrow x^2yz^3 >_{lex} x^2z^4$ because $(2,1,3) - (2,0,4) = (0, \mathbf{1}, -1)$

Monomial Orders on $k[x_1, \dots, x_n]$ - the Graded Reverse Lexicographic Order $>_{grevlex}$

Let x^α and x^β be monomials in $k[x_1, \dots, x_n]$. $x^\alpha >_{grevlex} x^\beta$ if:

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Graded Reverse Lexicographic Order $>_{grevlex}$

Let x^α and x^β be monomials in $k[x_1, \ldots, x_n]$. $x^\alpha >_{grevlex} x^\beta$ if:

- $\sum_i^n \alpha_i > \sum_i^n \beta_i$, or if

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Graded Reverse Lexicographic Order $>_{grevlex}$

Let x^α and x^β be monomials in $k[x_1, \ldots, x_n]$. $x^\alpha >_{grevlex} x^\beta$ if:

- $\sum_i^n \alpha_i > \sum_i^n \beta_i$, or if
- $\sum_i^n \alpha_i = \sum_i^n \beta_i$ and in the difference $\alpha - \beta$, the *rightmost* nonzero entry is *negative*.

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Graded Reverse Lexicographic Order $>_{grevlex}$

Let x^α and x^β be monomials in $k[x_1, \ldots, x_n]$. $x^\alpha >_{grevlex} x^\beta$ if:

- $\sum_i^n \alpha_i > \sum_i^n \beta_i$, or if
- $\sum_i^n \alpha_i = \sum_i^n \beta_i$ and in the difference $\alpha - \beta$, the *rightmost* nonzero entry is *negative*.

Under this order $>_{grevlex}$:

$$xy^2 >_{grevlex} x^2 >_{grevlex} xy >_{grevlex} x >_{grevlex} y$$

$x^2y^2z^2 >_{grevlex} xy^4z$ or $xy^4z >_{grevlex} x^2y^2z^2$?

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Graded Reverse Lexicographic Order $>_{grevlex}$

Let x^α and x^β be monomials in $k[x_1, \ldots, x_n]$. $x^\alpha >_{grevlex} x^\beta$ if:

- $\sum_i^n \alpha_i > \sum_i^n \beta_i$, or if
- $\sum_i^n \alpha_i = \sum_i^n \beta_i$ and in the difference $\alpha - \beta$, the *rightmost* nonzero entry is *negative*.

Under this order $>_{grevlex}$:

$$xy^2 >_{grevlex} x^2 >_{grevlex} xy >_{grevlex} x >_{grevlex} y$$

$x^2y^2z^2 >_{grevlex} xy^4z$ or $xy^4z >_{grevlex} x^2y^2z^2$?

$\rightarrow xy^4z >_{grevlex} x^2y^2z^2$ because $1+4+1 = 2+2+2$ and

Monomial Orders on $k[x_1, \dots, x_n]$ - the Graded Reverse Lexicographic Order $>_{grevlex}$

Let x^α and x^β be monomials in $k[x_1, \dots, x_n]$. $x^\alpha >_{grevlex} x^\beta$ if:

- $\sum_i^n \alpha_i > \sum_i^n \beta_i$, or if
- $\sum_i^n \alpha_i = \sum_i^n \beta_i$ and in the difference $\alpha - \beta$, the *rightmost* nonzero entry is *negative*.

Under this order $>_{grevlex}$:

$$xy^2 >_{grevlex} x^2 >_{grevlex} xy >_{grevlex} x >_{grevlex} y$$

$x^2y^2z^2 >_{grevlex} xy^4z$ or $xy^4z >_{grevlex} x^2y^2z^2$?

$\rightarrow xy^4z >_{grevlex} x^2y^2z^2$ because $1+4+1 = 2+2+2$ and $(1,4,1) - (2,2,2) = (-1, 2, \mathbf{-1})$

Monomial Orders

$$x^3y^2z >_{lex} x^2y^6y^8$$

$$x^2y^6y^8 >_{grevlex} x^3y^2z$$

$$x^2y^2z^2 >_{lex} xy^4z$$

$$xy^4z >_{grevlex} x^2y^2z^2$$

Why Several Orders?

Computing Gröbner bases with $>_{grevlex}$ is usually more efficient.

Why Several Orders?

Computing Gröbner bases with $>_{grevlex}$ is usually more efficient.

Computing Gröbner bases with $>_{lex}$ yields a polynomial system that can be easily solved.

Using the Monomial Orders

to decide which term of a polynomial is the leading term:

$\mathrm{LT}_>(f)$ denotes the leading term of f according to order $>$ (or simply $LT(f)$ when there is no ambiguity).

Using the Monomial Orders

to decide which term of a polynomial is the leading term:

$\mathrm{LT}_{>}(f)$ denotes the leading term of f according to order $>$ (or simply $LT(f)$ when there is no ambiguity).

For example, consider $f = 3x^3y^2 + x^2yz^3$.

$$\mathrm{LT}_{>_{lex}}(f) \quad =$$

Using the Monomial Orders

to decide which term of a polynomial is the leading term:

$\mathrm{LT}_>(f)$ denotes the leading term of f according to order $>$ (or simply $LT(f)$ when there is no ambiguity).

For example, consider $f = 3x^3y^2 + x^2yz^3$.

$$\begin{array}{rcl} \mathrm{LT}_{>_{lex}}(f) & = & 3x^3y^2 \\ \mathrm{LT}_{>_{grevlex}}(f) & = & \end{array}$$

Using the Monomial Orders

to decide which term of a polynomial is the leading term:

$\mathrm{LT}_{>}(f)$ denotes the leading term of f according to order $>$ (or simply $LT(f)$ when there is no ambiguity).

For example, consider $f = 3x^3y^2 + x^2yz^3$.

$$\begin{array}{rcl} \mathrm{LT}_{>_{lex}}(f) & = & 3x^3y^2 \\ \mathrm{LT}_{>_{grevlex}}(f) & = & x^2yz^3 \end{array}$$

Division in $k[x_1, \ldots, x_n]$

Let $F = (f_1, \ldots, f_s)$ be an *ordered* s-tuple of polynomials in $k[x_1, \ldots, x_n]$.

Division in $k[x_1, \ldots, x_n]$

Let $F = (f_1, \ldots, f_s)$ be an *ordered* s-tuple of polynomials in $k[x_1, \ldots, x_n]$.

Then every $f \in k[x_1, \ldots, x_n]$ can be written as

$$f = a_1 f_1 + \ldots + a_s f_s + r\,,$$

where

- $a_i, r \in k[x_1, \ldots, x_n]$;

Division in $k[x_1, \ldots, x_n]$

Let $F = (f_1, \ldots, f_s)$ be an *ordered* s-tuple of polynomials in $k[x_1, \ldots, x_n]$.

Then every $f \in k[x_1, \ldots, x_n]$ can be written as

$$f = a_1 f_1 + \ldots + a_s f_s + r\,,$$

where

- $a_i, r \in k[x_1, \ldots, x_n]$;
- $\forall\, i \;\; a_i f_i = 0$ or $\mathrm{LT}_>(f) \geq \mathrm{LT}(a_i f_i)$;

Division in $k[x_1, \ldots, x_n]$

Let $F = (f_1, \ldots, f_s)$ be an *ordered* s-tuple of polynomials in $k[x_1, \ldots, x_n]$.

Then every $f \in k[x_1, \ldots, x_n]$ can be written as

$$f = a_1 f_1 + \ldots + a_s f_s + r \,,$$

where

- $a_i, r \in k[x_1, \ldots, x_n]$;
- $\forall\, i \;\; a_i f_i = 0$ or $\mathrm{LT}_>(f) \geq \mathrm{LT}(a_i f_i)$;
- either $r = 0$, or r is a linear combination of monomials, none of which is divisible by any of $\mathrm{LT}_>(f_1), \ldots, \mathrm{LT}(f_s)$.

Division in $k[x_1, \ldots, x_n]$

Let $F = (f_1, \ldots, f_s)$ be an *ordered* s-tuple of polynomials in $k[x_1, \ldots, x_n]$.

Then every $f \in k[x_1, \ldots, x_n]$ can be written as

$$f = a_1 f_1 + \ldots + a_s f_s + r\,,$$

where

- $a_i, r \in k[x_1, \ldots, x_n]$;
- $\forall\, i \;\; a_i f_i = 0$ or $\mathrm{LT}_>(f) \geq \mathrm{LT}(a_i f_i)$;
- either $r = 0$, or r is a linear combination of monomials, none of which is divisible by any of $\mathrm{LT}_>(f_1), \ldots, \mathrm{LT}(f_s)$.

r is called *a* remainder of f on division by F.

- Notation: $r = \overline{f}^F$;
- there exists an algorithm to compute the a_i's and r.

Division in $k[x_1, \ldots, x_n]$

Let $F = (f_1, \ldots, f_s)$ be an *ordered* s-tuple of polynomials in $k[x_1, \ldots, x_n]$.

$$f = a_1 f_1 + \ldots + a_s f_s + r\,,$$

Reordering F or changing the monomial order can produce different a_i and a different remainder r!

Division in $k[x_1, \dots, x_n]$: Example

Let $f = xy^2 + x^2y + y^2 + x$.

Let $F = (x^2, y)$.

Division in $k[x_1, \ldots, x_n]$: Example

Let $f = xy^2 + x^2y + y^2 + x$.

Let $F = (x^2, y)$.

Using $>_{lex}$:

$$f = y.x^2 + (y + xy).y + x\,.$$

Division in $k[x_1, \ldots, x_n]$: Example

Let $f = xy^2 + x^2y + y^2 + x$.

Let $F = (x^2, y)$.

Using $>_{lex}$:

$$f = y.x^2 + (y + xy).y + x\,.$$

Let now $F = (y, x^2)$.

$$f = (x^2 + y + xy).y + 0.x^2 + x$$

Division in $k[x_1, \ldots, x_n]$: Example

Let $f = xy^2 + x^2y + y^2 + x$.

Let $F = (x^2, y)$.

Using $>_{lex}$:

$$f = y.x^2 + (y + xy).y + x\,.$$

Let now $F = (y, x^2)$.

$$f = (x^2 + y + xy).y + 0.x^2 + x$$

(see `normalf` command in Maple or `PolynomialReduce` in Mathematica)

Using the Polynomial Division

Can we use the division to decide whether a given polynomial $f \in k[x_1, \dots, x_n]$ is a member of a given ideal $I = \langle f_1, \dots, f_s \rangle$, by computing the remainder on division?

- One direction is easy:

Using the Polynomial Division

Can we use the division to decide whether a given polynomial $f \in k[x_1, \ldots, x_n]$ is a member of a given ideal $I = \langle f_1, \ldots, f_s \rangle$, by computing the remainder on division?

- One direction is easy:
  If $r = \overline{f}^F = 0$,

Using the Polynomial Division

Can we use the division to decide whether a given polynomial $f \in k[x_1, \ldots, x_n]$ is a member of a given ideal $I = \langle f_1, \ldots, f_s \rangle$, by computing the remainder on division?

- One direction is easy:
  If $r = \overline{f}^F = 0$, then $f = a_1 f_1 + \ldots + a_n f_n$. By definition, $f \in \langle f_1, \ldots, f_n \rangle$.

Using the Polynomial Division

Can we use the division to decide whether a given polynomial $f \in k[x_1, \dots, x_n]$ is a member of a given ideal $I = \langle f_1, \dots, f_s \rangle$, by computing the remainder on division?

- One direction is easy:
  If $r = \overline{f}^F = 0$, then $f = a_1 f_1 + \ldots + a_n f_n$. By definition, $f \in \langle f_1, \dots, f_n \rangle$.
- On the other hand:

Using the Polynomial Division

Can we use the division to decide whether a given polynomial $f \in k[x_1, \ldots, x_n]$ is a member of a given ideal $I = \langle f_1, \ldots, f_s \rangle$, by computing the remainder on division?

- One direction is easy:
  If $r = \overline{f}^F = 0$, then $f = a_1 f_1 + \ldots + a_n f_n$. By definition, $f \in \langle f_1, \ldots, f_n \rangle$.
- On the other hand:
  there is no guarantee to find $\overline{f}^F = 0$ for every f in $I = \langle f_1, \ldots, f_s \rangle$, with $F = (f_1, \ldots, f_s)$.

Counter-example

there is no guarantee to find $\overline{f}^F = 0$ for every f in $I = \langle f_1, \ldots, f_s \rangle$.

Example:

Counter-example

there is no guarantee to find $\overline{f}^F = 0$ for every f in $I = \langle f_1, \ldots, f_s \rangle$.

Example:

$p = y$ is in $I = \langle x^2 + 1, xy \rangle$ because

$$p = y(x^2 + 1) + (-x)(xy) .$$

Counter-example

there is no guarantee to find $\overline{f}^F = 0$ for every f in $I = \langle f_1, \ldots, f_s \rangle$.

Example:

$p = y$ is in $I = \langle x^2 + 1, xy \rangle$ because

$$p = y(x^2 + 1) + (-x)(xy) \ .$$

This is *not* a valid division because

$$\mathrm{LT}_{>_{lex}}\left(y(x^2+1)\right) = x^2 y \quad \Big\rangle_{lex} \quad \mathrm{LT}(p) = y$$

Counter-example

there is no guarantee to find $\overline{f}^F = 0$ for every f in $I = \langle f_1, \ldots, f_s \rangle$.

Example:

$p = y$ is in $I = \langle x^2 + 1, xy \rangle$ because

$$p = y(x^2 + 1) + (-x)(xy) \, .$$

This is *not* a valid division because

$$\mathrm{LT}_{>_{lex}}\left(y(x^2 + 1) \right) = x^2 y \quad \Big\rangle_{lex} \quad \mathrm{LT}(p) = y$$

Division:

$$p = 0.(x^2 + 1) + 0.(xy) + \mathbf{y} \, .$$

Gröbner Basis: Definition

Definition. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal.

Gröbner Basis: Definition

Definition. Let $I \subset k[x_1, \dots, x_n]$ be an ideal. A *Gröbner basis* for I is a set of polynomials $G = \{g_1, \dots, g_t\} \subset I$ such that

Gröbner Basis: Definition

Definition. Let $I \subset k[x_1, \dots, x_n]$ be an ideal. A *Gröbner basis* for I is a set of polynomials $G = \{g_1, \dots, g_t\} \subset I$ such that

$$\forall f \in I \backslash \{0\} \;\; \exists\, g \in G \quad \text{such that } \mathrm{LT}(f) \text{ is divisible by } \mathrm{LT}(g)\,.$$

It can be shown that a Gröbner basis always exists for any ideal I and it is indeed a basis for I i.e. $I = \langle g_1, \dots, g_t \rangle$.

Link with the Division in $k[x_1, \ldots, x_n]$

If F is a Gröbner basis for I, then for any $g \in I$, and for any ordering of F, the remainder of the division of g by F is null.

Example

Let

$$I = \left\langle x^2 - y^2 + 1,\ xy - 1 \right\rangle .$$

$\{x^2 - y^2 + 1,\ xy - 1\}$ is *not* a Gröbner basis for I under $>_{lex}$.

Example

Let

$$I = \left\langle x^2 - y^2 + 1,\ xy - 1 \right\rangle .$$

$\{x^2 - y^2 + 1,\ xy - 1\}$ is *not* a Gröbner basis for I under $>_{lex}$.

For example,

$$f = y(x^2 - y^2 + 1) - x(xy - 1) = x + y - y^3$$

is in I.

Example

Let

$$I = \left\langle x^2 - y^2 + 1,\ xy - 1 \right\rangle .$$

$\{x^2 - y^2 + 1,\ xy - 1\}$ is *not* a Gröbner basis for I under $>_{lex}$.

For example,

$$f = y(x^2 - y^2 + 1) - x(xy - 1) = x + y - y^3$$

is in I. However $\mathrm{LT}(f) = x$ is not divisible neither by $\mathrm{LT}(x^2 - y^2 + 1) = x^2$ nor by $\mathrm{LT}(xy - 1) = xy$.

Example

Let

$$I = \left\langle x^2 - y^2 + 1,\ xy - 1 \right\rangle .$$

$\{x^2 - y^2 + 1,\ xy - 1\}$ is *not* a Gröbner basis for I under $>_{lex}$.

For example,

$$f = y(x^2 - y^2 + 1) - x(xy - 1) = x + y - y^3$$

is in I. However $\mathrm{LT}(f) = x$ is not divisible neither by $\mathrm{LT}(x^2 - y^2 + 1) = x^2$ nor by $\mathrm{LT}(xy - 1) = xy$.

A Gröbner basis for I under the $>_{lex}$ order is:

$$\left\langle y^4 - y^2 - 1,\ x - y^3 + y \right\rangle .$$

We can check that $\mathrm{LT}(f) = x$ is divisible by $\mathrm{LT}(x - y^3 + y) = x$.

Remark

For arbitrary bases, combinations of basis elements may have a leading term that is not a multiple of any of the leading terms in the basis.

Remark

For arbitrary bases, combinations of basis elements may have a leading term that is not a multiple of any of the leading terms in the basis.

This is because multiples of leading terms may cancel.

Remark

For arbitrary bases, combinations of basis elements may have a leading term that is not a multiple of any of the leading terms in the basis.

This is because multiples of leading terms may cancel.

That is what happened in the previous example $I = \langle x^2 - y^2 + 1,\ xy - 1 \rangle$. We have:

Remark

For arbitrary bases, combinations of basis elements may have a leading term that is not a multiple of any of the leading terms in the basis.

This is because multiples of leading terms may cancel.

That is what happened in the previous example $I = \langle x^2 - y^2 + 1,\ xy - 1 \rangle$. We have:

$$\begin{aligned} \mathrm{LT}(x^2 - y^2 + 1) &= x^2 \\ \mathrm{LT}(xy - 1) &= xy \end{aligned}$$

Remark

For arbitrary bases, combinations of basis elements may have a leading term that is not a multiple of any of the leading terms in the basis.

This is because multiples of leading terms may cancel.

That is what happened in the previous example $I = \langle x^2 - y^2 + 1,\ xy - 1 \rangle$. We have:

$$\mathrm{LT}(x^2 - y^2 + 1) = x^2$$
$$\mathrm{LT}(xy - 1) = xy$$

but if we multiply $x^2 - y^2 + 1$ by y and $xy - 1$ by $-x$ and sum the results, these leading terms disappear.

Remark

For arbitrary bases, combinations of basis elements may have a leading term that is not a multiple of any of the leading terms in the basis.

This is because multiples of leading terms may cancel.

That is what happened in the previous example $I = \langle x^2 - y^2 + 1,\ xy - 1 \rangle$. We have:

$$\mathrm{LT}(x^2 - y^2 + 1) = x^2$$
$$\mathrm{LT}(xy - 1) = xy$$

but if we multiply $x^2 - y^2 + 1$ by y and $xy - 1$ by $-x$ and sum the results, these leading terms disappear.

The resulting polynomial $f = x + y - y^3$ is in I and its leading term x is not divisible neither by $\mathrm{LT}(x^2 - y^2 + 1) = x^2$ nor by $\mathrm{LT}(xy - 1) = xy$.

Remark (2)

Let's try the same operation on the Gröbner basis $\langle y^4 - y^2 - 1,\ x + y - y^3 \rangle$:

Remark (2)

Let's try the same operation on the Gröbner basis $\langle y^4 - y^2 - 1,\ x + y - y^3 \rangle$:

$$x(y^4 - y^2 - 1) + y^2(x - y^3 + y)$$

Remark (2)

Let's try the same operation on the Gröbner basis $\langle y^4 - y^2 - 1,\ x + y - y^3 \rangle$:

$$\begin{aligned} & x(y^4 - y^2 - 1) + y^2(x - y^3 + y) \\ = \quad & -xy^2 + xy^4 - x + xy^2 + y^3 - y^4 \end{aligned}$$

Remark (2)

Let's try the same operation on the Gröbner basis $\langle y^4 - y^2 - 1,\ x + y - y^3 \rangle$:

$$\begin{aligned} & x(y^4 - y^2 - 1) + y^2(x - y^3 + y) \\ = \; & -xy^2 + xy^4 - x + xy^2 + y^3 - y^4 \\ = \; & -x + xy^4 + y^3 - y^4 \end{aligned}$$

Remark (2)

Let's try the same operation on the Gröbner basis $\langle y^4 - y^2 - 1,\ x + y - y^3 \rangle$:

$$\begin{aligned} & x(y^4 - y^2 - 1) + y^2(x - y^3 + y) \\ = \ & -xy^2 + xy^4 - x + xy^2 + y^3 - y^4 \\ = \ & -x + xy^4 + y^3 - y^4 \end{aligned}$$

the leading term is

Remark (2)

Let's try the same operation on the Gröbner basis $\langle y^4 - y^2 - 1,\ x + y - y^3 \rangle$:

$$\begin{array}{rl} & x(y^4 - y^2 - 1) + y^2(x - y^3 + y) \\ = & -xy^2 + xy^4 - x + xy^2 + y^3 - y^4 \\ = & -x + xy^4 + y^3 - y^4 \end{array}$$

the leading term is xy^4, which is divisible by $\mathrm{LT}(x - y^3 + y) = x$.

Cool

If

- we use the monomial order $>_{lex}$ to compute a Gröbner basis and
- the solution set is finite,

then a univariate polynomial (in the last variable) is in the basis.

Cool

If

- we use the monomial order $>_{lex}$ to compute a Gröbner basis and
- the solution set is finite,

then a univariate polynomial (in the last variable) is in the basis.

For example, the Gröbner basis for $\langle x^2 - y^2 + 1,\ xy - 1\rangle$ is $\langle y^4 - y^2 - 1,\ x - y^3 + y\rangle$.

Cool

If

- we use the monomial order $>_{lex}$ to compute a Gröbner basis and
- the solution set is finite,

then a univariate polynomial (in the last variable) is in the basis.

For example, the Gröbner basis for $\langle x^2 - y^2 + 1,\ xy - 1\rangle$ is $\langle y^4 - y^2 - 1,\ x - y^3 + y\rangle$.

The system

$$\begin{cases} x^2 - y^2 + 1 & = & 0 \\ xy - 1 & = & 0 \end{cases}$$

has the same solutions as the system:

$$\begin{cases} y^4 - y^2 + -1 & = & 0 \\ x - y^3 + y & = & 0 \end{cases}$$

but the latter is much simpler to solve.

A More Ugly Example

A Gröbner basis for

$$\left\{ \begin{array}{ccc} x^2 - 2xz + 5 & = & 0 \\ xy^2 + yz + 1 & = & 0 \\ 3y^2 - 8xz & = & 0 \end{array} \right.$$

under $>_{lex}$ is

A More Ugly Example

A Gröbner basis for

$$\begin{cases} x^2 - 2xz + 5 & = & 0 \\ xy^2 + yz + 1 & = & 0 \\ 3y^2 - 8xz & = & 0 \end{cases}$$

under $>_{lex}$ is

$$\{-81 + 4320z - 86400z^2 + 766272z^3 - 2513488z^4 - 295680z^5 - 242496z^6 + 61440z^8, -2472389942760 + 1450790919y + 987224793696000z - 1312504296363936z^2 + 575639991700688z^3 + 711670127441280z^4 + 549519027506496z^5 - 103266809856000z^6 - 139421921341440z^7, 6503592729600 + 1450790919x - 257416379643438z + 3400639490020320z^2 - 1485707991955148 0z^3 - 1835782187164800z^4 - 1418473727285760z^5 + 263479449600000z^6 + 359882180198400z^7\}$$

Algorithms to Compute a Gröbner basis

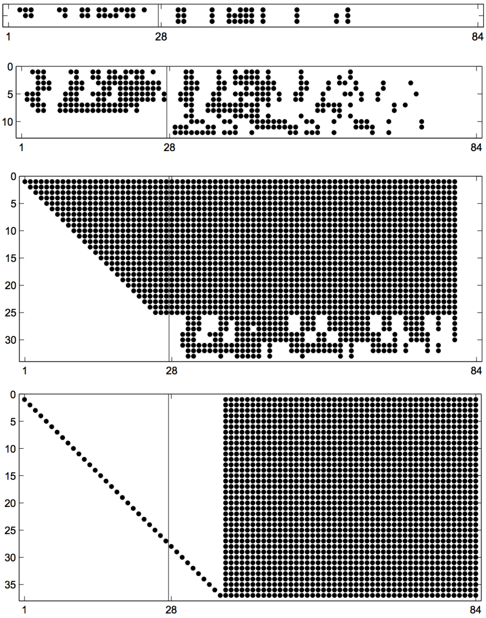
First algorithm to compute a Gröbner basis: the Buchberger algorithm.

More recent algorithms are more efficient ($F4$ and $F5$ algorithms by Faugère).

In [**?**]:

1. Start with $d \leftarrow 1$;
2. Multiply each equation of the current system by every possible monomial of degree d;
3. Simplify the system with Gauss-Jordan elimination;
4. If not a Gröbner basis, set $d \leftarrow d+1$, and iterate from 1.

Computation Steps for [?]



Damnit

Unfortunately, computation of Gröbner bases under the lexicographic ordering ($>_{lex}$) is often intractable for real problems.

Using the graded reverse lexicographical ordering ($>_{grevlex}$) usually yields more tractable computations.

Unfortunately, the resulting polynomial system is not necessarily easy to solve.

Fortunately, other properties of Gröbner bases can be used to find the solutions.

$>_{lex}$ versus $>_{grevlex}$: Example

Computing a Gröbner basis for

$$\left\{ \begin{array}{rcl} d_1^2 + A d_1 d_2 + d_2^2 - F^2 & = & 0 \\ d_1^2 + B d_1 d_3 + d_3^2 - F^2 & = & 0 \\ d_2^2 + C d_2 d_3 + d_3^2 - G^2 & = & 0 \\ d_2^2 + D d_2 d_4 + d_4^2 - F^2 & = & 0 \\ d_3^2 + E d_3 d_4 + d_4^2 - F^2 & = & 0 \end{array} \right.$$

under $>_{grevlex}$: less than a second (but 130 polynomials in a 96Kb text file).

under $>_{lex}$: more than a week

Rings and Ideals

A *ring* is a set with addition and multiplication operations.

For example,

Rings and Ideals

A *ring* is a set with addition and multiplication operations.

For example, $\mathbb{Z}$,

Rings and Ideals

A *ring* is a set with addition and multiplication operations.

For example, $\mathbb{Z}$, $k[x_1, \ldots, x_n]$ are rings.

Let consider an ideal I in a ring R.

Rings and Ideals

A *ring* is a set with addition and multiplication operations.

For example, $\mathbb{Z}$, $k[x_1, \ldots, x_n]$ are rings.

Let consider an ideal I in a ring R.

We can define an *equivalence relation* (denoted $\sim$) between elements of R:

$$a \sim b \text{ iff } a - b \in I\,.$$

Rings and Ideals

A *ring* is a set with addition and multiplication operations.

For example, $\mathbb{Z}$, $k[x_1, \ldots, x_n]$ are rings.

Let consider an ideal I in a ring R.

We can define an *equivalence relation* (denoted $\sim$) between elements of R:

$$a \sim b \text{ iff } a - b \in I \,.$$

For every element $a \in R$, we can define an *equivalence class*, or *coset* as:

$$[a] = \{ b \in R \,|\, a \sim b \} \,.$$

We have

$$a \sim b \Leftrightarrow [a] = [b] \Leftrightarrow a - b \in I$$

Rings and Ideals: Example

$\mathbb{Z}$ is a ring.

$n\mathbb{Z}$, the set of multiples of n is an ideal in $\mathbb{Z}$

Rings and Ideals: Example

$\mathbb{Z}$ is a ring.

$n\mathbb{Z}$, the set of multiples of n is an ideal in $\mathbb{Z}$ (stable under addition and multiplication by any $z \in \mathbb{Z}$).

Rings and Ideals: Example

$\mathbb{Z}$ is a ring.

$n\mathbb{Z}$, the set of multiples of n is an ideal in $\mathbb{Z}$ (stable under addition and multiplication by any $z \in \mathbb{Z}$).

With $n = 7$:

$$0 \sim 7 \sim 14 \sim 21 \sim \ldots$$

$$[0] = [7] = [14] = \{0, 7, 14, \ldots\}$$

Rings and Ideals: Example

$\mathbb{Z}$ is a ring.

$n\mathbb{Z}$, the set of multiples of n is an ideal in $\mathbb{Z}$ (stable under addition and multiplication by any $z \in \mathbb{Z}$).

With $n = 7$:

$$0 \sim 7 \sim 14 \sim 21 \sim ...$$

$$[0] = [7] = [14] = \{0, 7, 14, ...\}$$

$$1 \sim 8 \sim 15 \sim 22 \sim ...$$

$$[1] = [8] = [15] = \{1, 8, 15, ...\}$$

etc.

Rings and Ideals: Example

$\mathbb{Z}$ is a ring.

$n\mathbb{Z}$, the set of multiples of n is an ideal in $\mathbb{Z}$ (stable under addition and multiplication by any $z \in \mathbb{Z}$).

With $n = 7$:

$$0 \sim 7 \sim 14 \sim 21 \sim ...$$

$$[0] = [7] = [14] = \{0, 7, 14, ...\}$$

$$1 \sim 8 \sim 15 \sim 22 \sim ...$$

$$[1] = [8] = [15] = \{1, 8, 15, ...\}$$

etc.

The remainder of z divided by 7 is a standard representative of its class $[z]$.

$$[z] = [\text{remainder}(z/7)] \, .$$

Quotient Ring

If we define addition and multiplication between equivalence classes:

$$[a] + [b] = [a + b] \text{ and}$$

$$[a] \times [b] = [a \times b]\,,$$

Quotient Ring

If we define addition and multiplication between equivalence classes:

$$[a] + [b] = [a + b] \text{ and}$$

$$[a] \times [b] = [a \times b],$$

the set of equivalence classes is a ring.

Quotient Ring

If we define addition and multiplication between equivalence classes:

$$[a] + [b] = [a + b] \text{ and}$$

$$[a] \times [b] = [a \times b],$$

the set of equivalence classes is a ring.

It is called a *Quotient ring*, and is denoted R/I.

Example:

$$\mathbb{Z}/7\mathbb{Z} \quad = \quad \{[0], [1], [2], .., [6]\}$$

Quotient Ring

If we define addition and multiplication between equivalence classes:

$$[a] + [b] = [a + b] \text{ and}$$

$$[a] \times [b] = [a \times b],$$

the set of equivalence classes is a ring.

It is called a *Quotient ring*, and is denoted R/I.

Example:

$$\begin{aligned} \mathbb{Z}/7\mathbb{Z} &= \{[0], [1], [2], .., [6]\} \\ &= \{[\text{remainder}(z/7)] \mid z \in \mathbb{Z}\} \end{aligned}$$

Quotient Ring $k[x_1, \ldots, x_n]/I$

$k[x_1, \ldots, x_n]$ is a ring. If I is an ideal in $k[x_1, \ldots, x_n]$, $k[x_1, \ldots, x_n]/I$ is a quotient ring.

Quotient Ring $k[x_1, \ldots, x_n]/I$

$k[x_1, \ldots, x_n]$ is a ring. If I is an ideal in $k[x_1, \ldots, x_n]$, $k[x_1, \ldots, x_n]/I$ is a quotient ring.

By definition:

$$[f] = [g] \Leftrightarrow f \sim g \Leftrightarrow f - g \in I\,.$$

Quotient Ring $k[x_1, \ldots, x_n]/I$

$k[x_1, \ldots, x_n]$ is a ring. If I is an ideal in $k[x_1, \ldots, x_n]$, $k[x_1, \ldots, x_n]/I$ is a quotient ring.

By definition:

$$[f] = [g] \Leftrightarrow f \sim g \Leftrightarrow f - g \in I\,.$$

If $G = (g_1, \ldots, g_t)$ is a Gröbner basis, and $f \in k[x_1, \ldots, x_n]$:

$$[f] = [\overline{f}^G]$$

with $\overline{f}^G$ the remainder of the division of f by G. (because $f = h_1.g_1 + \ldots + h_t.g_t + \overline{f}^G \Rightarrow f - \overline{f}^G \in I \Rightarrow [f] = [\overline{f}^G]$)

Quotient Ring $k[x_1, \ldots, x_n]/I$

$k[x_1, \ldots, x_n]$ is a ring. If I is an ideal in $k[x_1, \ldots, x_n]$, $k[x_1, \ldots, x_n]/I$ is a quotient ring.

By definition:

$$[f] = [g] \Leftrightarrow f \sim g \Leftrightarrow f - g \in I\,.$$

If $G = (g_1, \ldots, g_t)$ is a Gröbner basis, and $f \in k[x_1, \ldots, x_n]$:

$$[f] = [\overline{f}^G]$$

with $\overline{f}^G$ the remainder of the division of f by G. (because $f = h_1.g_1 + \ldots + h_t.g_t + \overline{f}^G \Rightarrow f - \overline{f}^G \in I \Rightarrow [f] = [\overline{f}^G]$)
and

$$k[x_1, \ldots, x_n]/I = \left\{ \left[\overline{f}^G\right] \middle| f \in k[x_1, \ldots, x_n] \right\}.$$

(does not depend on G, because the remainder does not depend on the Gröbner basis)

Finiteness Theorem

Theorem. Let's consider

- an ideal I in $\mathbb{C}[x_1, \ldots, x_n]$, and
- the corresponding quotient ring $A = \mathbb{C}[x_1, \ldots, x_n]/I$

$\dim(A)$ is finite $\Leftrightarrow$ $\mathbf{V}(I)$ is finite (i.e. the number of solutions is finite)

Finiteness Theorem

Theorem. Let's consider

- an ideal I in $\mathbb{C}[x_1, \ldots, x_n]$, and
- the corresponding quotient ring $A = \mathbb{C}[x_1, \ldots, x_n]/I$

$\dim(A)$ is finite $\Leftrightarrow$ $\mathbf{V}(I)$ is finite (i.e. the number of solutions is finite)

Counter-example: $I =< x >\in \mathbb{C}[x, y]$, and
$A = \mathbb{C}[x, y]/I = \{[1], [x], [y], [y^2], [\sum_\alpha a_\alpha y^\alpha]\}$

Action Matrix

Let's consider

- an ideal I in $\mathbb{C}[x_1, \ldots, x_n]$,

Action Matrix

Let's consider

- an ideal I in $\mathbb{C}[x_1, \ldots, x_n]$,
- the corresponding quotient ring $A = \mathbb{C}[x_1, \ldots, x_n]/I$,

Action Matrix

Let's consider

- an ideal I in $\mathbb{C}[x_1, \ldots, x_n]$,
- the corresponding quotient ring $A = \mathbb{C}[x_1, \ldots, x_n]/I$,
- a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$,

Action Matrix

Let's consider

- an ideal I in $\mathbb{C}[x_1, \ldots, x_n]$,
- the corresponding quotient ring $A = \mathbb{C}[x_1, \ldots, x_n]/I$,
- a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$,
- the function m_f defined as:

Action Matrix

Let's consider

- an ideal I in $\mathbb{C}[x_1, \dots, x_n]$,
- the corresponding quotient ring $A = \mathbb{C}[x_1, \dots, x_n]/I$,
- a polynomial $f \in \mathbb{C}[x_1, \dots, x_n]$,
- the function m_f defined as:

$$\begin{aligned} m_f \quad : \quad & A \to A \\ & m_f(g) = [f][g] = [f.g] \end{aligned}$$

Then

Action Matrix

Let's consider

- an ideal I in $\mathbb{C}[x_1, \ldots, x_n]$,
- the corresponding quotient ring $A = \mathbb{C}[x_1, \ldots, x_n]/I$,
- a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$,
- the function m_f defined as:

$$\begin{aligned} m_f \quad : \quad & A \to A \\ & m_f(g) = [f][g] = [f.g] \end{aligned}$$

Then m_f is linear: $[f][ag_1 + g_2] = [f]([ag_1] + [g_2]) = a[f][g_1] + [f][g_2]$

Action Matrix

Let's consider

- an ideal I in $\mathbb{C}[x_1, \dots, x_n]$,
- the corresponding quotient ring $A = \mathbb{C}[x_1, \dots, x_n]/I$,
- a polynomial $f \in \mathbb{C}[x_1, \dots, x_n]$,
- the function m_f defined as:

$$\begin{aligned} m_f \quad : \quad & A \rightarrow A \\ & m_f(g) = [f][g] = [f.g] \end{aligned}$$

Then m_f is linear: $[f][ag_1 + g_2] = [f]([ag_1] + [g_2]) = a[f][g_1] + [f][g_2]$

If the number of solutions is finite, $\dim(A)$ is finite, and m_f can be written as a matrix $\mathbf{M}_f$, which is called an *action matrix*.

wow

Theorem. For $\lambda \in \mathbb{C}$, the two statements are equivalent:

Theorem. For $\lambda \in \mathbb{C}$, the two statements are equivalent:

- λ is an eigenvalue of the action matrix $\mathbf{M}_f$;

Theorem. For $\lambda \in \mathbb{C}$, the two statements are equivalent:

- λ is an eigenvalue of the action matrix $\mathbf{M}_f$;
- $\exists\,(a_1, \ldots, a_n) \in \mathbf{V}(I)$ such that $f(a_1, \ldots, a_n) = \lambda$.

wow

Theorem. For $\lambda \in \mathbb{C}$, the two statements are equivalent:

- λ is an eigenvalue of the action matrix $\mathbf{M}_f$;
- $\exists\,(a_1, \ldots, a_n) \in \mathbf{V}(I)$ such that $f(a_1, \ldots, a_n) = \lambda$.

If we take $f = x_i$,

Theorem. For $\lambda \in \mathbb{C}$, the two statements are equivalent:

- λ is an eigenvalue of the action matrix $\mathbf{M}_f$;
- $\exists\,(a_1, \ldots, a_n) \in \mathbf{V}(I)$ such that $f(a_1, \ldots, a_n) = \lambda$.

If we take $f = x_i$, then $f(a_1, \ldots, a_n) = a_i$.

WOW

Theorem. For $\lambda \in \mathbb{C}$, the two statements are equivalent:

- λ is an eigenvalue of the action matrix $\mathbf{M}_f$;
- $\exists\,(a_1, \ldots, a_n) \in \mathbf{V}(I)$ such that $f(a_1, \ldots, a_n) = \lambda$.

If we take $f = x_i$, then $f(a_1, \ldots, a_n) = a_i$.

In other words, the eigenvalues of $\mathbf{M}_{x_i}$ are the possible values for x_i!

WOW

Theorem. For $\lambda \in \mathbb{C}$, the two statements are equivalent:

- λ is an eigenvalue of the action matrix $\mathbf{M}_f$;
- $\exists\,(a_1,\ldots,a_n) \in \mathbf{V}(I)$ such that $f(a_1,\ldots,a_n) = \lambda$.

If we take $f = x_i$, then $f(a_1,\ldots,a_n) = a_i$.

In other words, the eigenvalues of $\mathbf{M}_{x_i}$ are the possible values for x_i!

Computing the Action Matrix

We need to identify a basis for the set of remainders.

The monomials in the basis of the set of remainders are the monomials that are not multiples of the leading terms of the polynomials in the Gröbner basis.

Computing the Action Matrix (continued)

The monomials in the basis B of the set of remainders are the monomials that are not multiples of the leading terms of the polynomials in the Gröbner basis.

Example: The Gröbner basis G under $>_{grevlex}$ for

$$\begin{cases} x^2 - 2xz + 5 & = & 0 \\ xy^2 + yz + 1 & = & 0 \\ 3y^2 - 8xz & = & 0 \end{cases}$$

Computing the Action Matrix (continued)

The monomials in the basis B of the set of remainders are the monomials that are not multiples of the leading terms of the polynomials in the Gröbner basis.

Example: The Gröbner basis G under $>_{grevlex}$ for

$$\left\{ \begin{array}{rcl} x^2 - 2xz + 5 & = & 0 \\ xy^2 + yz + 1 & = & 0 \\ 3y^2 - 8xz & = & 0 \end{array} \right.$$

is $\{ \begin{array}{l} 3y^2 - 8xz,\ x^2 - 2xz + 5, \\ 160z^3 - 160xz + 415yz + 12x - 30y - 224z + 15, \\ 240yz^2 - 9xy + 1600xz + 18yz + 120z^2 - 120x + 240z, \\ 16xz^2 + 3yz - 40z + 3,\ 40xyz - 3xy + 6yz + 40z^2 \end{array} \}$

with leading terms $\{y^2, x^2, z^3, yz^2, xz^2, xyz\}$.

The monomials in B are the monomials that are not divisible by the leading terms: 1, x, y, z, xy, xz, yz, z^2

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G =$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G =$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G = x$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G = x$$

$$\overline{x.x}^G =$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G = x$$
$$\overline{x.x}^G = \overline{x^2}^G =$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G = x$$

$$\overline{x.x}^G = \overline{x^2}^G = -5 + 2xz$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G = x$$

$$\overline{x.x}^G = \overline{x^2}^G = -5 + 2xz$$

$$\overline{x.y}^G = \overline{xy}^G = xy$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G = x$$

$$\overline{x.x}^G = \overline{x^2}^G = -5 + 2xz$$

$$\overline{x.y}^G = \overline{xy}^G = xy$$

$$\overline{x.z}^G = \overline{xz}^G = xz$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\begin{aligned}
\overline{x.1}^G &= \overline{x}^G = x \\
\overline{x.x}^G &= \overline{x^2}^G = -5 + 2xz \\
\overline{x.y}^G &= \overline{xy}^G = xy \\
\overline{x.z}^G &= \overline{xz}^G = xz \\
\overline{x.(xy)}^G &= \overline{x^2y}^G = -5y + \tfrac{3}{20}xy - \tfrac{2}{10}yz - 2z^2
\end{aligned}$$

Computing the Action Matrix $\mathbf{M}_x$

The basis B is $\{[1], [x], [y], [z], [xy], [xz], [yz], [z^2]\}$

The coefficients of $\mathbf{M}_x$ are the coordinates of these cosets after multiplication by $[x]$:

$$\overline{x.1}^G = \overline{x}^G = x$$

$$\overline{x.x}^G = \overline{x^2}^G = -5 + 2xz$$

$$\overline{x.y}^G = \overline{xy}^G = xy$$

$$\overline{x.z}^G = \overline{xz}^G = xz$$

$$\overline{x.(xy)}^G = \overline{x^2y}^G = -5y + \tfrac{3}{20}xy - \tfrac{2}{10}yz - 2z^2$$

etc.

(I used the Mathematica `PolynomialReduce` function to compute these remainders)

Computing the Action Matrix $\mathbf{M}_x$ (continued)

$$
\begin{aligned}
&[x.1] = [x] \\
&[x.x] = -5[1] + 2[xz] \\
&[x.y] = [xy] \\
&[x.z] = [xz] \\
&[x.(xy)] = -5[y] + \tfrac{3}{20}[xy] - \tfrac{2}{10}[yz] - 2[z^2]
\end{aligned}
$$

etc.

Computing the Action Matrix $\mathbf{M}_x$ (continued)

$$
\begin{aligned}
&[x.1] = [x] \\
&[x.x] = -5[1] + 2[xz] \\
&[x.y] = [xy] \\
&[x.z] = [xz] \\
&[x.(xy)] = -5[y] + \tfrac{3}{20}[xy] - \tfrac{2}{10}[yz] - 2[z^2] \\
&\text{etc.}
\end{aligned}
$$

and:

Computing the Action Matrix $\mathbf{M}_x$ (continued)

$$
\begin{aligned}
&[x.1] = [x] \\
&[x.x] = -5[1] + 2[xz] \\
&[x.y] = [xy] \\
&[x.z] = [xz] \\
&[x.(xy)] = -5[y] + \tfrac{3}{20}[xy] - \tfrac{2}{10}[yz] - 2[z^2] \\
&\text{etc.}
\end{aligned}
$$

and:

$$
\mathbf{M}_x = \begin{array}{c}
\begin{matrix} 1 & x & y & z & xy & xz & yz & z^2 \end{matrix} \\
\begin{bmatrix}
0 & -5 & 0 & 0 & 0 & & & \\
1 & 0 & 0 & 0 & 0 & & & \\
0 & 0 & 0 & 0 & -5 & & & \\
0 & 0 & 0 & 0 & 0 & : & : & : \\
0 & 0 & 1 & 0 & \frac{3}{20} & : & : & : \\
0 & 2 & 0 & 1 & 0 & & & \\
0 & 0 & 0 & 0 & -\frac{2}{10} & & & \\
0 & 0 & 0 & 0 & -2 & & &
\end{bmatrix}
\end{array}
\begin{matrix} \\ 1 \\ x \\ y \\ z \\ xy \\ xz \\ yz \\ z^2 \end{matrix}
$$

Computing the Possible Values for x

$$\mathbf{M}_x = \begin{bmatrix} 0 & -5 & 0 & 0 & 0 & -\frac{3}{8} & 0 & -\frac{3}{16} \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{5}{2} \\ 0 & 0 & 1 & 0 & \frac{3}{20} & 0 & \frac{3}{40} & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{2}{10} & -\frac{3}{8} & -\frac{3}{20} & -\frac{3}{16} \\ 0 & 0 & 0 & 0 & -2 & 0 & -1 & 0 \end{bmatrix}$$

Computing the Possible Values for x

$$\mathbf{M}_x = \begin{bmatrix} 0 & -5 & 0 & 0 & 0 & -\frac{3}{8} & 0 & -\frac{3}{16} \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{5}{2} \\ 0 & 0 & 1 & 0 & \frac{3}{20} & 0 & \frac{3}{40} & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{2}{10} & -\frac{3}{8} & -\frac{3}{20} & -\frac{3}{16} \\ 0 & 0 & 0 & 0 & -2 & 0 & -1 & 0 \end{bmatrix}$$

The real eigenvalues for $\mathbf{M}_x$ are $-1.10137..$ and $0.9660..$, which are the possible values for x.

Computing the Complete Solution

The real eigenvalues for $\mathbf{M}_x$ are $-1.10137..$ and $0.9660..$, which are the possible values for x.

Computing the Complete Solution

The real eigenvalues for $\mathbf{M}_x$ are $-1.10137..$ and $0.9660..$, which are the possible values for x.

We still have to find the corresponding values for y and z.

Possible strategies:

Computing the Complete Solution

The real eigenvalues for $\mathbf{M}_x$ are $-1.10137..$ and $0.9660..$, which are the possible values for x.

We still have to find the corresponding values for y and z.

Possible strategies:

1. do the same with $\mathbf{M}_y$ and $\mathbf{M}_z$, and check for every possible combination $(x, , y, z)$ if it is a valid solution.

Computing the Complete Solution

The real eigenvalues for $\mathbf{M}_x$ are $-1.10137..$ and $0.9660..$, which are the possible values for x.

We still have to find the corresponding values for y and z.

Possible strategies:

1. do the same with $\mathbf{M}_y$ and $\mathbf{M}_z$, and check for every possible combination $(x, , y, z)$ if it is a valid solution.
2. for each possible value for x, plug it in the system and solve the resulting system (which is now only in y and z).

The first option is more stable numerically.

In Practice [Kukelova08]

Offline

input: polynomial system with random coefficients

↓

output: "elimination template" operations to apply to the system to obtain a Gröbner basis

Online

input: actual coefficients of the system

1. apply the elimination template to compute the coefficients of the Gröbner basis:

2. compute the action matrix(ces)

3. compute the solutions using the action matrix(ces)

The offline computations are done in $\mathbb{Z}/p\mathbb{Z}$ with p a large prime number. It speeds up the computations, and avoids numerical instability (can easily determine when a coefficient becomes null).

See Automatic solver software on
`http://cmp.felk.cvut.cz/minimal/`

Further Reading and References I

- M. Byröd, K. Josephson, and K. Åström.
  Fast and Stable Polynomial Equation Solving and its Application to Computer Vision.
  2009.
- D.A. Cox, J.B. Little, and D. O'Shea.
  Using Algebraic Geometry.
  Springer, 2005.
- D.A. Cox, J.B. Little, and D. O'Shea.
  Ideals, Varieties, and Algorithms.
  Springer, 2007.
- Z. Kukelova, M. Bujnak, and T. Pajdla.
  Automatic Generator of Minimal Problem Solvers.
  In *European Conference on Computer Vision*, 2008.

Further Reading and References II

Z. Kukelova, M. Bujnak, and T. Pajdla.
Polynomial Eigenvalue Solutions to Minimal Problems in Computer Vision.
IEEE Transactions on Pattern Analysis and Machine Intelligence, 2012.

H. Li and R. Hartley.
Five-Point Motion Estimation Made Easy.
In *International Conference on Pattern Recognition*, 2006.

D. Nister.
An Efficient Solution to the Five-Point Relative Pose Problem.
IEEE Transactions on Pattern Analysis and Machine Intelligence, 2004.

H. Stewénius, F. Schaffalitzky, and D. Nistér.
How Hard Is Three-View Triangulation Really?
In *International Conference on Computer Vision*, 2005.