Modeling Physics with Differential-Algebraic Equations

Lecture 4

Algebraic Methods: Elimination Theory and Invariant Sets

COMASIC (M2)
January 10, 2018

Khalil Ghorbal
khalil.ghorbal@inria.fr

Outline

- k denotes an algebraically closed field.
- $k[X] = k[X_1, \ldots, X_n]$: the ring of polynomials over k
- $I = (f_1, \ldots, f_s) \subset k[X]$ **ideal** generated by the f_i

$$I := \left\{ f \in k[X] \mid \exists \lambda_1, \ldots, \lambda_s \in k[X],\ f = \sum_{i=1}^{s} \lambda_i f_i \right\}$$

- The **Radical** of I, denoted $\sqrt{I}$, is an ideal of $k[X]$ defined as follows.

$$\sqrt{I} := \{ f \in k[X] \mid \exists m \in \mathbb{N}.\ f^m \in I \}$$

Hilbert Basis Theorem

Every ideal of $k[X]$ is finitely generated.

Definition: **Variety**

Let $I = (f_1, \ldots, f_s)$ be an ideal of $k[X]$. A *variety* $\mathcal{V}(I)$ is a subset of k^n defined as follows.

$$\mathcal{V}(I) := \{x \in k^n \mid f_1(x) = 0, \ldots, f_s(x) = 0\}$$

Definition: **Vanishing ideal**

Let S be a subset of k^n. A *V*anishing ideal $\mathcal{I}(S)$ is an ideal of $k[X]$ defined as follows.

$$\mathcal{I}(S) := \{f \in k[X] \mid \forall x \in S, f(x) = 0\}$$

- A monomial is an element of $k[X]$ of the form $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$.
- Notation: X^α, $\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

Definition: **Monomial Order**

Total order on the set of monomials satisfying:

1. For all $\gamma \in \mathbb{N}^n$, $X^\alpha < X^\beta$ implies $X^\alpha X^\gamma < X^\beta X^\gamma$,
2. For all $\alpha \in \mathbb{N}^n$, $X^\alpha > 1$, so 1 is the minimal element.

Example: Lex Ordering

Extends the lexicographic ordering $X_1 > X_2 > \cdots > X_n$ as follows:

$$X^\alpha > X^\beta \text{ if and only if } \begin{cases} & \alpha_1 > \beta_1 \\ \text{or} & \alpha_1 = \beta_1 \wedge \alpha_2 > \beta_2 \\ \text{or} & \vdots \end{cases}$$

- A monomial is an element of $k[X]$ of the form $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$.
- Notation: X^α, $\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

Definition: **Monomial Order**

Total order on the set of monomials satisfying:

1. For all $\gamma \in \mathbb{N}^n$, $X^\alpha < X^\beta$ implies $X^\alpha X^\gamma < X^\beta X^\gamma$,
2. For all $\alpha \in \mathbb{N}^n$, $X^\alpha > 1$, so 1 is the minimal element.

Example: Lex Ordering

Extends the lexicographic ordering $X_1 > X_2 > \cdots > X_n$ as follows:

$$X^\alpha > X^\beta \text{ if and only if } \begin{cases} & \alpha_1 > \beta_1 \\ \text{or} & \alpha_1 = \beta_1 \wedge \alpha_2 > \beta_2 \\ \text{or} & \vdots \end{cases}$$

Leading Terms, Monomials and Coefficients

For a fixed monomial order ($>$), one can write any polynomial $f \in k[X]$ as follows:

$$f = cX^{\alpha} + \sum_{i=1}^{s} a_i X^{\beta_i}$$

such that $c \neq 0$ and X^{α} is bigger than any other monomial with a nonzero coefficient (formally, for all $i = 1, \ldots, s$: $a_i \neq 0$ implies $X^{\alpha} > X^{\beta_i}$).

Definitions

- $\mathrm{LT}(f) = cX^{\alpha}$: **Leading Term** of f
- $\mathrm{LM}(f) = X^{\alpha}$: **Leading Monomial** of f
- $\mathrm{LC}(f) = c$: **Leading Coefficient** of f

Theorem

Given non zero polynomials $f, f_1, \ldots, f_s \in k[X]$ and a monomial ordering $(>)$, there exists $r, q_1, \ldots, q_s \in k[X]$ such that

- $f = (\sum_1^s q_i f_i) + r$
- No term in r is divisible by any $\mathrm{LT}(f_i)$
- $\mathrm{LT}(f) = \max_> \{\mathrm{LT}(q_i)\mathrm{LT}(f_i) \mid q_i \neq 0\}$

Given I an ideal of $k[X]$, the **leading terms ideal** of I is defined by

$$\mathrm{LT}(I) := (\{\mathrm{LT}(f) \mid f \in I\})$$

That is, the ideal generated by all the LT of all the polynomials in I. By definition the following inclusion of ideals holds

$$(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)) \subset \mathrm{LT}(I)$$

Theorem

Given non zero polynomials $f, f_1, \ldots, f_s \in k[X]$ and a monomial ordering $(>)$, there exists $r, q_1, \ldots, q_s \in k[X]$ such that

- $f = (\sum_1^s q_i f_i) + r$
- No term in r is divisible by any $\mathrm{LT}(f_i)$
- $\mathrm{LT}(f) = \max_> \{\mathrm{LT}(q_i)\mathrm{LT}(f_i) \mid q_i \neq 0\}$

Given I an ideal of $k[X]$, the **leading terms ideal** of I is defined by

$$\mathrm{LT}(I) := (\{\mathrm{LT}(f) \mid f \in I\})$$

That is, the ideal generated by all the LT of all the polynomials in I. By definition the following inclusion of ideals holds

$$(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)) \subset \mathrm{LT}(I)$$

- $\mathrm{LT}(I)$ is "bigger" than $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s))$
- $X > Y$: $f_1 = X^2 + X$; $f_2 = X^2 + Y$
- $(\mathrm{LT}(f_1), \mathrm{LT}(f_2)) = (X^2, X^2) = (X^2)$
- $f_1 - f_2 = X - Y \in I := (f_1, f_2)$
- $\mathrm{LT}(X - Y) = X$ is in $(\mathrm{LT}(I))$. Clearly $X \notin (X^2)$

Definition: **Gröbner Bases**

Fix the monomial order $(>)$. Let I be an ideal of $k[X]$. G is a *Gröbner Basis* for I with respect to $(>)$ if and only if

$$(\mathrm{LT}(g) \mid g \in G) = (\mathrm{LT}(I)) \ .$$

In words: The leading terms ideal of G is generated by the leading terms of the generators of G.

- $\mathrm{LT}(I)$ is "bigger" than $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s))$
- $X > Y$: $f_1 = X^2 + X$; $f_2 = X^2 + Y$
- $(\mathrm{LT}(f_1), \mathrm{LT}(f_2)) = (X^2, X^2) = (X^2)$
- $f_1 - f_2 = X - Y \in I := (f_1, f_2)$
- $\mathrm{LT}(X - Y) = X$ is in $(\mathrm{LT}(I))$. Clearly $X \notin (X^2)$

Definition: **Gröbner Bases**

Fix the monomial order $(>)$. Let I be an ideal of $k[X]$. G is a *Gröbner Basis* for I with respect to $(>)$ if and only if

$$(\mathrm{LT}(g) \mid g \in G) = (\mathrm{LT}(I)) \ .$$

In words: The leading terms ideal of G is generated by the leading terms of the generators of G.

$G = (g_1, \ldots, g_m)$ is **reduced** if for every $i = 1, \ldots, m$, $\mathrm{LC}(g_i) = 1$ and $\mathrm{LT}(g_i)$ does not divide any term of any g_j, $j \neq i$.

Example

- $G = (X + Y^2, Y)$ is a non reduced Gröbner basis.
- (X, Y) is a reduced Gröbner basis.

Theorem

Every ideal has a unique reduced Gröbner Basis representation (up to the fixed monomial order).

k is algebraically closed.

Theorem: **Hilbert's Nullstellensatz**

- Strong: $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$
- Weak: $\mathcal{V}(I) = \emptyset$ if and only if $1 \in I$

Corollaries: Solvability and Gröbner Bases

I is an ideal of $k[X]$. The following statements are equivalent:

- $I \neq k[X]$
- $1 \notin I$
- $\mathcal{V}(I) \neq \emptyset$
- I has a Gröbner Basis having nonconstant polynomials
- The reduced Gröbner Basis of I is different from $\{1\}$

k is algebraically closed.

Theorem: **Hilbert's Nullstellensatz**

- Strong: $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$
- Weak: $\mathcal{V}(I) = \emptyset$ if and only if $1 \in I$

Corollaries: Solvability and Gröbner Bases

I is an ideal of $k[X]$. The following statements are equivalent:

- $I \neq k[X]$
- $1 \notin I$
- $\mathcal{V}(I) \neq \emptyset$
- I has a Gröbner Basis having nonconstant polynomials
- The reduced Gröbner Basis of I is different from $\{1\}$

The Finiteness Theorem

Let I be an ideal of $k[X]$. The following statements are equivalent.

- $\mathcal{V}(I)$ is finite (finite set of points in k^n)
- $k[X]/I$ is a finite-dimensional vector space over k
- Only a finite number of monomials are not in $\mathrm{LT}(I)$

In addition $\dim_k k[X]/I$ gives exactly the number of solutions (counted with their multiplicities) of the system defined by I.

Example

- $I = (X^2 + 1)$
- $k[X]/I$ is isomorphic, as a vector space, to k^2: elements of $k[X]/I$ are of the form $a + bX$ where $a, b \in k$
- When k is algebraically closed, $X^2 + 1$ has two roots since it is of degree 2

- Gröbner Bases are akin to Standard Bases by Hironaka (1964).
- The name Gröbner was introduced by Buchberger in his thesis (1965) where he gives a procedure to compute such bases.
- The coefficients of the intermediate (S) polynomials computed while generating a basis could be very large, likewise their polynomial degrees can be as large as n^2 if one starts with polynomials of degree n.
- The fastest known implementation if Fougere's F4 and F5 packages (available in Maple), they are however limited in the size of X and the total degrees of the f_i.
- Almost all computer algebra systems have an implementation the Buchberger algorithm (possibly with different optimizations and heuristics).

This classical correspondence between Algebra and Geometry, together with the existence of procedures to compute Gröbner Bases in many practically relevant cases have many applications:

- Solvability of a system of polynomial equations
- Finite solutions test
- Ideal membership test
- Polynomial reduction (division)
- Elimination theory (next section)

Outline

- $k[X, Y] = k[X_1, \ldots, X_s, Y_{s+1}, \ldots, Y_n]$
- A monomial in $k[X, Y]$ has the form $X^\alpha Y^\gamma$
- Let I be an ideal of $k[X, Y]$

Elimination Order

A monomial ordering eliminates X if $X^\alpha > X^\beta$ implies $X^\alpha Y^\gamma > X^\beta Y^\delta$ for every Y^γ and Y^δ. (For instance, the lex monomial ordering is an elimination order.)

Elimination Ideal

$I \cap k[Y]$ is the *elimination ideal* of I that eliminates X.

Elimination Theorem

Let G be a Gröbner basis of I for a monomial order $(>)$ that eliminates X. Then $G \cap k[Y]$ is a Gröbner Basis of the elimination ideal $I \cap k[Y]$ for the monomial order on $k[Y]$ induced by $(>)$.

- $k[X, Y] = k[X_1, \ldots, X_s, Y_{s+1}, \ldots, Y_n]$
- A monomial in $k[X, Y]$ has the form $X^\alpha Y^\gamma$
- Let I be an ideal of $k[X, Y]$

Elimination Order

A monomial ordering eliminates X if $X^\alpha > X^\beta$ implies $X^\alpha Y^\gamma > X^\beta Y^\delta$ for every Y^γ and Y^δ. (For instance, the lex monomial ordering is an elimination order.)

Elimination Ideal

$I \cap k[Y]$ is the *elimination ideal* of I that eliminates X.

Elimination Theorem

Let G be a Gröbner basis of I for a monomial order $(>)$ that eliminates X. Then $G \cap k[Y]$ is a Gröbner Basis of the elimination ideal $I \cap k[Y]$ for the monomial order on $k[Y]$ induced by $(>)$.

- $k[X, Y] = k[X_1, \ldots, X_s, Y_{s+1}, \ldots, Y_n]$
- A monomial in $k[X, Y]$ has the form $X^\alpha Y^\gamma$
- Let I be an ideal of $k[X, Y]$

Elimination Order

A monomial ordering eliminates X if $X^\alpha > X^\beta$ implies $X^\alpha Y^\gamma > X^\beta Y^\delta$ for every Y^γ and Y^δ. (For instance, the lex monomial ordering is an elimination order.)

Elimination Ideal

$I \cap k[Y]$ is the *elimination ideal* of I that eliminates X.

Elimination Theorem

Let G be a Gröbner basis of I for a monomial order $(>)$ that eliminates X. Then $G \cap k[Y]$ is a Gröbner Basis of the elimination ideal $I \cap k[Y]$ for the monomial order on $k[Y]$ induced by $(>)$.

Given the coordinates $x_1, \ldots, x_s, y_{s+1}, \ldots, y_n$, let

$$\pi_s : \mathbb{A}^n \to \mathbb{A}^{n-s}$$

denote the projection onto the last $n - s$ coordinates.

Variety of Partial Solutions

$$\pi_s(\mathcal{V}(I)) \subseteq \mathcal{V}(I \cap k[Y]) \ .$$

Moreover, $\mathcal{V}(I \cap k[Y])$ is the Zariski Closure of the projection, that is the *s*mallest variety containing the set $\pi_s(\mathcal{V}(I))$.

Example

$I = (XY - 1, Z - Y)$, with respect to the lex order $(X > Y > Z)$, the generator of I form a Gröbner Basis. Thus $I \cap k[Y, Z] = (Z - Y)$. So $(y, z) = (0, 0)$ is in $\mathcal{V}(I \cap k[Y])$ but not in $\pi_s(\mathcal{V}(I))$.

Given the coordinates $x_1, \ldots, x_s, y_{s+1}, \ldots, y_n$, let

$$\pi_s : \mathbb{A}^n \to \mathbb{A}^{n-s}$$

denote the projection onto the last $n - s$ coordinates.

Variety of Partial Solutions

$$\pi_s(\mathcal{V}(I)) \subseteq \mathcal{V}(I \cap k[Y]) \ .$$

Moreover, $\mathcal{V}(I \cap k[Y])$ is the Zariski Closure of the projection, that is the *s*mallest variety containing the set $\pi_s(\mathcal{V}(I))$.

Example

$I = (XY - 1, Z - Y)$, with respect to the lex order $(X > Y > Z)$, the generator of I form a Gröbner Basis. Thus $I \cap k[Y, Z] = (Z - Y)$. So $(y, z) = (0, 0)$ is in $\mathcal{V}(I \cap k[Y])$ but not in $\pi_s(\mathcal{V}(I))$.

Solving by Triangulation

- $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$
- Use the lex order $X_1 > \cdots > X_n$ which is an elimination order for each X_i
- Compute a Gröbner Basis G with respect to that order
- Then $G \cap k[X_n]$ is a principal ideal, thus one gets a univariate polynomial in X_n to solve
- Now compute $G \cap k[X_{n-1}, X_n]$, knowing the X_n, this gives a univariate polynomial in X_{n-1} alone
- Keep iterating till solving the entire system

Order $X > Y > Z$.

Original System

$$f_1 = X^2 + Y + Z - 1$$
$$f_2 = X + Y^2 + Z - 1$$
$$f_3 = X + Y + Z^2 - 1$$

Gröbner Basis

$$g_1 = X + Y + Z^2 - 1$$
$$g_2 = Y^2 - Y - Z^2 + Z$$
$$g_3 = 2YZ^2 + Z^4 - Z^2$$
$$g_4 = Z^6 - 4Z^4 + 4Z^3 - Z^2$$

Elimination Ideals

$$I_1 = G \cap k[Z] = (g_4)$$
$$I_2 = G \cap k[Y, Z] = (g_2, g_3, g_4)$$
$$I_3 = G \cap k[X, Y, Z] = (g_1, g_2, g_3, g_4)$$

Outline

Given a polynomial ordinary differential equation $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$.

Initial Value Problem

$$\mathbf{x}(t), t \in U \text{ solution of the Cauchy problem } \left(\frac{d\mathbf{x}(t)}{dt} = \mathbf{f}(\mathbf{x}), \mathbf{x}(0) = \mathbf{x}_0 \right)$$

Orbit

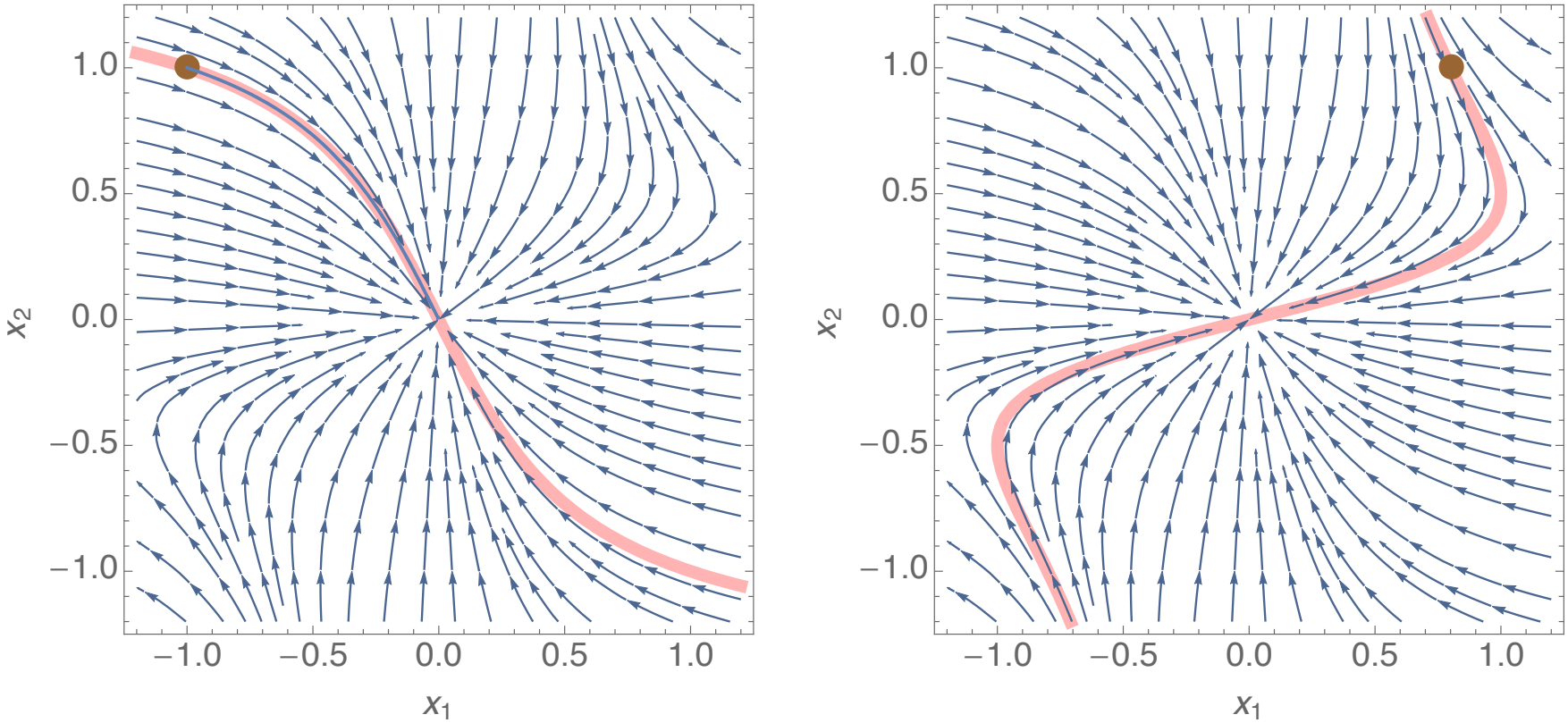
$$\mathcal{O}_{\mathbf{x}_0} := \{\mathbf{x}(t) \mid t \in U\} = \{\mathbf{x} \in \mathbb{R}^n \mid \exists t \in \mathbb{R}, \mathbf{x} = \varphi_t(\mathbf{x}_0)\} \subset \mathbb{R}^n$$

Invariant Region $S \subset \mathbb{R}^n$

$$\forall \mathbf{x}_0 \in S, \forall t \in U, \mathbf{x}(t) \in S$$

Algebraic Invariant Equations

$$\mathbf{f} = (-x_1 - 2x_1^2 x_2, -x_2),$$



$$p(x_1, x_2) = (x_2(0) - x_1(0)x_2(0)^2)x_1 - x_1(0)(x_2 - x_1 x_2^2) = 0$$

Gradient

$$\nabla p := \left(\frac{\partial p}{\partial x_1}, \ldots, \frac{\partial p}{\partial x_n} \right)$$

Lie Derivation

$$\mathfrak{D}_{\mathbf{f}}(p) := \frac{dp(\mathbf{x}(t))}{dt} = \nabla p \cdot \mathbf{f} \qquad (\dot{\mathbf{x}} = \mathbf{f})$$

Closure (Zariski Topology)

$$\bar{\mathcal{O}}_{\mathbf{x}_0} := \mathcal{V}(\mathcal{I}(\mathcal{O}_{\mathbf{x}_0}))$$

Proposition1: Dimension and Integrability

$\mathcal{O}_{\mathbf{x}_0} \subset \bar{\mathcal{O}}_{\mathbf{x}_0}$

Proposition2: Stability under Lie derivation

$\mathcal{I}(\mathcal{O}(\mathbf{x}_0))$ is a (proper) *differential ideal* for $\mathfrak{D}_\mathbf{f}$, that is, $\mathfrak{D}_\mathbf{f}(p) \in \mathcal{I}(\mathcal{O}(\mathbf{x}_0))$ for all $p \in \mathcal{I}(\mathcal{O}(\mathbf{x}_0))$

Example: Zariski Dense Varieties

$\dot{x} = x \rightsquigarrow \mathcal{O}(\mathbf{x}_0) = [0, \infty[\rightsquigarrow I = \langle 0 \rangle \rightsquigarrow \bar{\mathcal{O}}_{\mathbf{x}_0} = \mathcal{V}(\mathcal{I}(\mathcal{O}(\mathbf{x}_0))) = \mathbb{R}$

Definition: Differential Order

The *differential order* of $p \in \mathbb{R}[\mathbf{x}]$ denotes the length of the chain of ideals

$$\langle p \rangle \subset \langle p, \mathfrak{D}_{\mathbf{f}}(p) \rangle \subset \cdots \subset \left\langle p, \mathfrak{D}_{\mathbf{f}}(p), \ldots, \mathfrak{D}_{\mathbf{f}}^{(N_p-1)}(p) \right\rangle =: \partial p.$$

$N_p = \text{card}(\partial p)$ ($< \infty$ since $\mathbb{R}$ is Notherian).

Characterizing Elements of $\mathcal{I}(\mathcal{O}(\mathbf{x}_0))$

Definition: Differential Order

The *differential order* of $p \in \mathbb{R}[\mathbf{x}]$ denotes the length of the chain of ideals

$$\langle p \rangle \subset \langle p, \mathfrak{D}_{\mathbf{f}}(p) \rangle \subset \cdots \subset \left\langle p, \mathfrak{D}_{\mathbf{f}}(p), \ldots, \mathfrak{D}_{\mathbf{f}}^{(N_p-1)}(p) \right\rangle =: \partial p.$$

$N_p = \mathrm{card}(\partial p)$ ($< \infty$ since $\mathbb{R}$ is Notherian).

Theorem

The polynomial p is in $I(\mathcal{O}(\mathbf{x}_0))$ if and only if $\mathfrak{D}_{\mathbf{f}}^{(i)}(p)(\mathbf{x}_0) = 0$, for all $i = 0, \ldots, N_p - 1$.

Definition: Differential Order

The *differential order* of $p \in \mathbb{R}[\mathbf{x}]$ denotes the length of the chain of ideals

$$\langle p \rangle \subset \langle p, \mathfrak{D}_{\mathbf{f}}(p) \rangle \subset \cdots \subset \left\langle p, \mathfrak{D}_{\mathbf{f}}(p), \ldots, \mathfrak{D}_{\mathbf{f}}^{(N_p-1)}(p) \right\rangle =: \partial p.$$

$N_p = \text{card}(\partial p)$ ($< \infty$ since $\mathbb{R}$ is Notherian).

Theorem

The polynomial p is in $I(\mathcal{O}(\mathbf{x}_0))$ if and only if $\mathfrak{D}_{\mathbf{f}}^{(i)}(p)(\mathbf{x}_0) = 0$, for all $i = 0, \ldots, N_p - 1$.

Proof Sketch

$\leftarrow$: Since $\mathbf{x}(t)$ is analytic, $p(\mathbf{x}(t))$ is also analytic. Thus for a nonempty open neighborhood $V \subset U$ around 0, the null Taylor series of $p(t)$ is equal to p, thus $p = 0$ for all U.

Corollary1

An algebraic set $\mathcal{V}(\langle p \rangle)$ is invariant for $\mathbf{f}$ if and only if

$$\partial p \subset \mathcal{I}(\mathcal{V}(\langle p \rangle)) \ .$$

Corollary2

For each $\mathbf{x}_0$, there exists a unique (up to multiplication by a constant and rearrangement of its factors) $p \in \mathbb{R}[\mathbf{x}]$ such that

$$\partial p = \mathcal{I}(\mathcal{O}(\mathbf{x}_0)) \ .$$

Decidability: $\partial p \subset \mathcal{I}(\mathcal{V}(\langle p \rangle))$

Given $\mathbf{f}$ and $p \in \mathbb{R}[\mathbf{x}]$, the invariance of $\mathcal{V}(\langle p \rangle)$ is decidable.

$$\mathfrak{D}_{\mathbf{f}}^{(N_p)}(p) = \sum_{i=0}^{N_p-1} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p)\ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge\ p = 0 \rightarrow \bigwedge_{i=1}^{N_p-1} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\cdots$$

$$\mathfrak{D}_{\mathbf{f}}^{(3)}(p) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p)\ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge\ p = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}^{(2)}(p) = \lambda_0 p + \lambda_1 \mathfrak{D}_{\mathbf{f}}(p)\ (\lambda_i \in \mathbb{R}[\mathbf{x}]) \ \wedge\ p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}(p) = \lambda p\ (\lambda \in \mathbb{R}[\mathbf{x}])$$

$V(\langle p \rangle)$ is an invariant algebraic set

- Existence of λ_i: Gröbner Basis
- $p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$: (Universal) Quantifier Elimination

Decidability: $\partial p \subset \mathcal{I}(\mathcal{V}(\langle p \rangle))$

Given $\mathbf{f}$ and $p \in \mathbb{R}[\mathbf{x}]$, the invariance of $\mathcal{V}(\langle p \rangle)$ is decidable.

$$\mathfrak{D}_{\mathbf{f}}^{(N_p)}(p) = \sum_{i=0}^{N_p-1} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \bigwedge_{i=1}^{N_p-1} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\cdots$$

$$\mathfrak{D}_{\mathbf{f}}^{(3)}(p) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}^{(2)}(p) = \lambda_0 p + \lambda_1 \mathfrak{D}_{\mathbf{f}}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}(p) = \lambda p \; (\lambda \in \mathbb{R}[\mathbf{x}])$$

$V(\langle p \rangle)$ is an invariant algebraic set

- Existence of λ_i: Gröbner Basis
- $p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$: (Universal) Quantifier Elimination

Decidability: $\partial p \subset \mathcal{I}(\mathcal{V}(\langle p \rangle))$

Given $\mathbf{f}$ and $p \in \mathbb{R}[\mathbf{x}]$, the invariance of $\mathcal{V}(\langle p \rangle)$ is decidable.

$$\mathfrak{D}_{\mathbf{f}}^{(N_p)}(p) = \sum_{i=0}^{N_p-1} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \bigwedge_{i=1}^{N_p-1} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\cdots$$

$$\mathfrak{D}_{\mathbf{f}}^{(3)}(p) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}^{(2)}(p) = \lambda_0 p + \lambda_1 \mathfrak{D}_{\mathbf{f}}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}(p) = \lambda p \; (\lambda \in \mathbb{R}[\mathbf{x}])$$

$V(\langle p \rangle)$ is an invariant algebraic set

- Existence of λ_i: Gröbner Basis
- $p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$: (Universal) Quantifier Elimination

Decidability: $\partial p \subset \mathcal{I}(\mathcal{V}(\langle p \rangle))$

Given $\mathbf{f}$ and $p \in \mathbb{R}[\mathbf{x}]$, the invariance of $\mathcal{V}(\langle p \rangle)$ is decidable.

$$\mathfrak{D}_{\mathbf{f}}^{(N_p)}(p) = \sum_{i=0}^{N_p-1} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \bigwedge_{i=1}^{N_p-1} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\dots$$

$$\mathfrak{D}_{\mathbf{f}}^{(3)}(p) = \sum_{i=0}^{2} \lambda_i \mathfrak{D}_{\mathbf{f}}^{(i)}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \bigwedge_{i=1}^{2} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}^{(2)}(p) = \lambda_0 p + \lambda_1 \mathfrak{D}_{\mathbf{f}}(p) \; (\lambda_i \in \mathbb{R}[\mathbf{x}]) \; \wedge \; p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p) = 0$$

$$\mathfrak{D}_{\mathbf{f}}(p) = \lambda p \; (\lambda \in \mathbb{R}[\mathbf{x}])$$

$V(\langle p \rangle)$ is an invariant algebraic set

- Existence of λ_i: Gröbner Basis
- $p = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0$: (Universal) Quantifier Elimination

Outline

1. Gröbner Bases
2. Applications (Elimination Theory)
3. Algebraic Characterization of Invariant Varieties
4. Differential Algebra

Summary

- Gröbner Bases are central objects in Computer Algebra Systems
- Elimination Theory generalizes Gaussian elimination (BLT Forms)
- Qualitative Analysis of ODE via their algebraic invariant sets

This Lecture

- Differential Algebra (Quick Introduction)
- Hybrid Aspects: Challenges

R denotes a commutative unitary ring.

- $a \in R$ is a zero divisor if and only if there exists $b \in R$, $b \neq 0$ such that $ab = 0$.
- 0 is a trivial zero divisor.
- Domains are rings where the only zero divisor is zero.
- Quotient of a ring R by an ideal I: R/I.
- $\bar{f}$ (or f) is zero in R/I if and only if f is in the ideal I.
- R/I, residue class ring (not necessarily a domain).
- M is a multiplicatively closed subset of R if and only if $m_1 m_2 \in M$ for all m_1, m_2 in M.

The zero divisors of the residue class ring are important.

Prime Ideals

The ideal $\mathfrak{p}$ is said to be *prime* if and only if

- $R/\mathfrak{p}$ is a domain.
- $R/\mathfrak{p}$ does not have nontrivial zero divisors.
- $ab \in \mathfrak{p}$ if and only if either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Primary Ideals

The ideal $\mathfrak{q}$ is said to be *primary* if and only if

- all zero divisors of $R/\mathfrak{q}$ are nilpotent.
- $ab \in \mathfrak{q}$ if and only if either $a^m \in \mathfrak{q}$ or $b^m \in \mathfrak{q}$ for some positive natural number m.

The radical of a primary ideal, $\sqrt{\mathfrak{q}}$, is a prime ideal.

- Any maximal ideal is prime, the converse is not true.
- For a ring R, (X) is a prime ideal of $R[X]$ but it is not maximal ($(X) \subset (X, Y)$).
- Intuition: points of a given affine space are not the only *irreducible* varieties – this will be given a precise meaning later. Lines and circles are also irreducible.

- One constructs the ring R_M (or $M^{-1}R$), the ring R localized at M, with elements of the form $\frac{r}{m}$ where $r \in R$ and $s \in M$.
- For $\frac{r_1}{m_1}$, $\frac{r_2}{m_2}$ in R_M, the "+" composition law is defined by $\frac{m_2 r_1 + m_1 r_2}{m_1 m_2}$.
- Let φ_M denote the ring homomorphism $R \to R_M$, then

$$\varphi_M^{-1}[(\varphi_M(I))] = I : M$$

Let I be an ideal of R and M a multiplicatively closed subset of R. Then

$$I : M \;=\; \{f \in R \mid \exists m \in M \;,\; mf \in I\} \;.$$

is a *Saturation* ideal.

Let $\mathfrak{q}$ be a primary ideal.

- If $M \cap I \neq \emptyset$ then $I : M = R$.
- If $M \cap \mathfrak{q} = \emptyset$ then $\mathfrak{q} : M = \mathfrak{q}$.

Suppose one has a primary decomposition of I: $I = \cap_{i=1}^{s} \mathfrak{q}_i$, then

$$I : M = \bigcap_{\mathfrak{q}_i \cap M = \emptyset} \mathfrak{q}_i$$

- $f = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$
- $g = b_e X^e + b_{e-1} X^{e-1} + \cdots + b_1 X + b_0$
- $(d, e) \neq (0, 0)$

The Sylvester Matrix of f and g is the following $(d + e)$ square matrix.

$$S(f,g) = \begin{pmatrix} a_d & 0 & \cdots & 0 & b_e & 0 & \cdots & 0 \\ a_{d-1} & a_d & \cdots & 0 & b_{e-1} & b_e & \cdots & 0 \\ a_{d-2} & a_{d-1} & \ddots & 0 & b_{e-2} & b_{e-1} & \ddots & 0 \\ \vdots & \vdots & \ddots & a_d & \vdots & \vdots & \ddots & b_e \\ \vdots & \vdots & \cdots & a_{d-1} & \vdots & \vdots & \cdots & b_{e-1} \\ a_0 & a_1 & \cdots & a_{d-2} & b_0 & b_1 & \cdots & \vdots \\ 0 & a_0 & \ddots & \vdots & 0 & b_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_1 & \vdots & \vdots & \ddots & b_1 \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

$$\begin{aligned} f &= X^2 - X + 1 \\ g &= X - 2 \end{aligned}$$

$$\begin{pmatrix} 1 & 1 & 0 \\ -1 & -2 & 1 \\ 1 & 0 & -2 \end{pmatrix}$$

$$\begin{aligned} f &= X^4 + 3X^3 - 1 \\ g &= -1 \end{aligned}$$

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

R is a domain. Let f and g be two polynomials in $R[X]$. The resultant of f and g, $\mathrm{res}(f, g)$, is the determinant of the Sylvester matrix of f and g.

Properties

- f and g have a common root (on an algebraic field extension of R) if and only if $\mathrm{res}(f, g) = 0$.
- $\mathrm{res}(f, g) = (f, g)$. That is, there exists polynomials u and v of respective degrees less that e and d, such that $\mathrm{res}(f, g) = uf + vg$.

Derivation

A *derivation* δ on R is a map $R \to R$ satisfying:

- $\delta(a+b) = \delta(a) + \delta(b)$
- $\delta(ab) = \delta(a)b + a\delta(b)$

- Notation: δa is often used instead of $\delta(a)$.
- δ_1 and δ_2 commute if and only if $\delta_1\delta_2 a = \delta_2\delta_1 a$ for all $a \in R$.
- **High-order** derivatives δ^h are inductively defined as $\delta(\delta^{h-1}a)$.
- **Ordinary** differential ring has a single derivation.
- **Partial** differential ring has a family $\Delta = \{\delta_1, \ldots, \delta_m\}$ of pairwise commuting derivations.
- Same definitions apply for a field k.

$c \in R$ is a **constant** if and only if $\delta c = 0$ for all $\delta \in \Delta$.
If k if a differential field, then the set of constants is a subfield of k.

Differential Ideal

A *differential* ideal $\mathfrak{a}$ of a Δ-ring R is an ideal of R such that

$$\forall \delta \in \Delta,\ \forall a \in \mathfrak{a},\ \delta a \in \mathfrak{a}\ .$$

- The intersection of an arbitrary number of differential ideals is a differential ideal
- The finite sum of differential ideals is also a differential ideal
- $[S]$ denotes the differential ideal generated by $S \subset R$.

Example 1

- $R = \mathbb{Z}[X]$, $\Delta = \left\{ \frac{d}{dX} \right\}$, is a differential ring.
- $\mathfrak{a} = (2, 2X)$ is a differential ideal.
- $[X] = R$ $(\delta X = 1)$

Example 2

- $R = \mathbb{Z}[X, e^X]$, $\Delta = \left\{ \frac{d}{dX} \right\}$, is a differential ring.
- $\mathfrak{a} = (e^X)$ is a differential ideal.
- $[X] = R$ $(\delta X = 1)$

- Θ: free multiplicative monoid generated by $\Delta = \{\delta_1, \ldots, \delta_m\}$.
- $\theta \in \Theta$ has the form $\delta_1^{e_1} \cdots \delta_m^{e_m}$, $e_i \in \mathbb{N}$.
- **order** of θ is defined as $e_1 + \cdots + e_m$.
- Θ acts on R by $\theta a = \delta_1^{e_1} \cdots \delta_m^{e_m} a$

Differential Polynomial Ring (1/2)

- Let R be a Δ-ring.
- $\Theta X = \{X_{\theta,j}\}_{1 \leq j \leq n, \theta \in \Theta}$, $n > 0$, family of indeterminates.
- $R[\Theta X]$ has a unique Δ-ring structure extending the Δ-ring structure of R by $\delta X_{\theta,j} = X_{\delta\theta,j}$, for all $\delta \in \Delta$, $\theta \in \Theta$.
- $R[\Theta X]$, equipped with this structure is called **Differential Polynomial Ring**,
- in the differential indeterminates $X_j = X_{1,j}$.
- $R[\Theta X]$ is denoted by $R\{X_1, \ldots, X_n\}$ or simply $R\{X\}$
- We write $X_{\theta,j}$ by θY_j (partial derivative of Y_j)
- The order of θY_j is defined as the order of θ

Differential Polynomial Ring (2/2)

- A **Differential Monomial** is a finite power product of derivatives of the form θY_j
- $\prod_k (\theta_k Y_{j_k})^{e_k}$, the θ_k (and likewise the Y_{j_k}) are not necessarily distinct
- A differential polynomial is a finite sum of terms aM where $a \in R$ and M is a differential monomial
- $R\{X\}$ has a structure of differential ring with $\Delta = \left\{ \frac{\partial}{\partial(\theta Y_j)} \right\}_{1 \leq j \leq n, \theta \in \Theta}$

- $R\{X_1, X_2\}$, $\Delta = \{\delta_1, \delta_2\}$
- $\theta_1 = \delta_1^4 \delta_2^3$
- $\theta_2 = \delta_2^4$
- $\theta_3 = \delta_1^3 \delta_2$
- $(\theta_1 X_1)(\theta_2 X_1)(\theta_3 X_2)^2 X_2$ is a monomial or order 7 and degree 5

The Wronskian determinant of dimension 2:

$$W = \begin{vmatrix} X_1 & X_2 \\ \delta X_1 & \delta X_2 \end{vmatrix}$$

is a differential polynomial in $R\{X_1, X_2\}$.

- $W = X_1 \delta X_2 - X_2 \delta X_1$
- $\delta W = X_1 \delta^2 X_2 - X_2 \delta^2 X_1$
- The partial derivative of W with respect to δX_2 is X_1

- Given a Δ differential ring R, to each element f of $R\{X\}$, one associates a (partial) differential equation $f = 0$.
- Likewise for a finite subset of $S \subset R\{X\}$, one gets a system of partial differential equations.
- The differential ideal $[S]$ is associated with S and contains all the equations derived from S by addition, multiplication by elements of $R\{X\}$ and differentiation.

As seen in the purely algebraic case, one wants to define a weaker notion of triangular forms suitable for the differential case.
We thus need to define *reduction* and hence ordering over differential monomials.

Triangular Form

A system $S \subset R\{X\}$ is in triangular form if its element can be rearranged as $S_1, S_2, \ldots, S_k, \ldots$ such that each S_k involves at least one derivative $\theta_k X_{j_k}$ which does not appear in $S_1, \ldots, S_{k-1}$. In particular $S_1 \notin R$.

Example

$$S := \begin{array}{ll} S_1: & \delta^2 X_2 + X_2 \\ S_2: & \delta^2 X_2 + X_2^2 + X_3 \\ S_3: & \delta^2 X_2 + X_1 \end{array}$$

S is in triangular form with respect to X_2, X_3, X_1 (or $\delta^2 X_2, X_3, X_1$)

There are other definitions of triangular forms.

Definition

A ranking of $X_1, \ldots, X_n$ is a total ordering on ΘX such that for all $u, v \in \Theta X$ and $\delta \in \Delta$, $u \leq \delta u$, and $u \leq v$ implies $\delta u \leq \delta v$.

- A ranking is said to be *orderly* if $\mathrm{ord}(u) \leq \mathrm{ord}(v)$ implies $u \leq v$.
- A ranking is said to be *unmixed* if for every i, j, $X_i \leq X_j$ implies $\theta X_i \leq X_j$ for every $\theta \in \Theta$.

Pure Algebra	**Differential Algebra**
Monomials	Differential Monomials
Polynomials	Differential Polynomials
Ordering	Ranking
Hilbert Basis Theorem	Ritt-Raudenbush Basis Theorem
Gröbner Bases	Characteristic Sets (Ritt-Kolchin) Coherent Sets (Rosenfeld) Regular Chains (Boulier et al.)

References

- David A. Cox, John Little and Donal O'Shea, *Ideals, Varieties, and Algorithms*, Springer 2007.
- Peter Schauenberg, *A Gröbner-based Treatment of Elimination Theory for Affine Varieties*, Journal of Symbolic Computation, 2007.
- Khalil Ghorbal and André Platzer, *Characterizing Algebraic Invariants by Differential Radical Invariants*, TACAS, 2014.