MMA 数学特論 I

Algorithms for polynomial systems: elimination & Gröbner bases

多項式系のアルゴリズム: グレブナー基底 & 消去法

Lecture VII: Elimination and Nullstellensatz

(summary of a full lesson given on the blackboard) **July, 1st, 8th 2010.**

Xavier Dahan

Review on: Elimination and the Nullstellensatz

All fields are infinite in this chapter

- $f_1, \ldots, f_s \subset k[X_1, \ldots, X_n]$ a polynomial system.
- k_1 any field extension $k_1|k$,
- $\mathbf{V}_{k_1}(f_1, \ldots, f_s)$ the set of common solutions in k_1 of the polynomials f_i:

$$\begin{aligned}\mathbf{V}_{k_1}(f_1, \ldots, f_s) &:= \{(x_1, \ldots, x_n) \in k_1^n \mid \forall 1 \leq i \leq s, \quad f_i(x_1, \ldots, x_n) = 0\} \\ &= \mathbf{V}_{k_1}(f_1) \cap \cdots \cap \mathbf{V}_{k_1}(f_s)\end{aligned}$$

Definition 1 *Such sets are called affine varieties defined over k.*

Remark: This depends only of the polynomial system $f_1, \ldots, f_s$ and the field k, not on the field k_1. Indeed, we have:

for any field k_0 such that $k \subset k_0 \subset k_1$, $\quad \mathbf{V}_{k_0}(f_1, \ldots, f_s) = \mathbf{V}_{k_1}(f_1, \ldots, f_s) \cap k_0^n$

Affine variety over field extensions (example)

Algebraic numbers: Let $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$, be the algebraic closure of $\mathbb{Q}$ ($\overline{\mathbb{Q}}$ is called the field of *algebraic numbers*):

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C}, \text{such that } \exists P \in \mathbb{Q}[X],\ P(\alpha) = 0\},$$

$\longrightarrow$ Cf. Lecture II

Example: Let $f_1 = (XY)^2 + Y$ and $f_2 = (Y-1)(Y^2-2)$ a system of 2 equations.

Over $\mathbb{Q}$: $\{Y = 1\}$ is solution of f_2, but $f_1(X, 1) = X^2 + 1$ has no solutions, hence $\mathbf{V}_{\mathbb{Q}}(f_1, f_2) = \emptyset$.

Over $k_1 = \mathbb{Q}(i)$: $\mathbf{V}_{k_1}(f_1, f_2) = \{(i, 1), (-i, 1)\}$,

Over $k_2 = \mathbb{Q}(\sqrt{\sqrt{2}})$: $\mathbf{V}_{k_2}(f_1, f_2) = \{(\pm\frac{\sqrt{2}}{2}, \sqrt{\sqrt{2}})\}$

Over $k_3 = \mathbb{Q}(\sqrt{\sqrt{2}}, i)$: $\mathbf{V}_{k_3}(f_1, f_2) = \mathbf{V}_{k_2}(f_1, f_2) \cup \mathbf{V}_{k_1}(f_1, f_2)$

Affine variety of an ideal

- let $I = \langle f_1, \ldots, f_s \rangle$ an ideal of $k[X_1, \ldots, X_n]$
- for all $f \in I$ and field extension $k_1|k$: $\mathbf{V}_{k_1}(f_1, \ldots, f_s) \subset \mathbf{V}_{k_1}(f)$.
- If $\langle g_1, \ldots, g_t \rangle = \langle f_1, \ldots, f_s \rangle$, then $\mathbf{V}_{k_1}(f_1, \ldots, f_s) = \mathbf{V}_{k_1}(g_1, \ldots, g_t)$.
- $\Rightarrow \mathbf{V}_{k_1}(f_1, \ldots, f_s)$ depends only on the ideal I: we denote $\mathbf{V}_{k_1}(I) = \mathbf{V}_{k_1}(f_1, \ldots, f_s)$.

$$\begin{array}{ccc} \text{Ideals of } k[X_1, \ldots, X_n] & \longrightarrow & \text{Affine varieties defined over } k \\ I & \longmapsto & \mathbf{V}_{k_1}(I) \subset k_1^n \end{array}$$

Porperties:

- $\mathbf{V}(\,.\,)$ is decreasing: $I \subset J \Rightarrow \mathbf{V}(J) \subset \mathbf{V}(I)$.
- If $1 \in I$, then $\mathbf{V}(I) = \emptyset$ (1 has no solution)
- $\mathbf{V}(\,.\,)$ is not one-one: $\mathbf{V}_{\mathbb{C}}((X-1)^2) = \mathbf{V}_{\mathbb{C}}(X-1) = \{1\}$, but $\langle (X-1)^2 \rangle \subsetneq \langle X-1 \rangle$.

Ideal of a set. Field of definition of a variety

• Let $S \subset k^n$

$$\mathbf{I}_k(S) := \{f \in k[X_1, \ldots, X_n] \mid f(x_1, \ldots, x_n) = 0, \ \forall (x_1, \ldots, x_n) \in S\}.$$

This is an ideal of $k[X_1, \ldots, X_n]$ the vanishing ideal of S.

• Let $V \subset k^n$ be an affine variety.

$\iff \exists I \subset k[X_1, \ldots, X_n]$ ideal, such that $V = \mathbf{V}_k(I)$.

Let k_0 be the **smallest** field such that:

$$\exists g_1, \ldots, g_s \in k_0[X_1, \ldots, X_n], \text{ and } \langle g_1, \ldots, g_s \rangle = I.$$

Definition 2 *The field k_0 is called the field of definition of V.*

It follows that V is defined over k_0.

Example: $n = 1$. The field of definition of $\{\sqrt{2}\}$ is $\mathbb{Q}(\sqrt{2})$. But the field of definition of $\{\pm\sqrt{2}\}$ is $\mathbb{Q}$.

Properties of vanishing ideals

$$\begin{array}{ccc} \text{Affine varieties (defined over } k_0) & \longrightarrow & \text{Ideals of } k_0[X_1, \ldots, X_n] \\ V & \longmapsto & \mathbf{I}(V) \end{array}$$

- Do not care too much about the field k where is $V \subset k^n$...
- What is important is its field of definition k_0.
- $\mathbf{I}(\,.\,)$ is a decreasing map: $V \subset W \Rightarrow \mathbf{I}(W) \subset \mathbf{I}(V)$.

Lemma 1 *Given an ideal $I \subset k[X_1, \ldots, X_n]$, holds: $I \subset \mathbf{I}(\mathbf{V}(I))$ (not equal in general).*

Proof: *(on the blackboard, with examples ...)*

Lemma 2 *Let V and W be 2 affine varieties, then: $V \subset W \Leftrightarrow \mathbf{I}(W) \subset (V)$. It follows that the map $\mathbf{I}(\,.\,)$ is one-one: $V \neq W \Rightarrow \mathbf{I}(V) \neq \mathbf{I}(W)$*

Proof: *(on the blackboard)*

Elimination ideal

Let $S \subset k^n$.

For $\ell = 1, \ldots, n-1$, and $s = (s_1, \ldots, s_n) \in S$ let $\pi_\ell(s) := (s_{\ell+1}, \ldots, s_n)$.

$\pi_\ell(S) := \{\pi_\ell(s),\ s \in S\} \rightarrow$ projection that eliminates the first ℓ coordinates.

! If V is an affine variety, then $\pi_\ell(V)$ is not an affine variety in general.

Definition 3 *Let $I \subset k[X_1, \ldots, X_n]$ be an ideal. Let $0 \leq \ell \leq n-1$.*

ℓ-th elimination ideal of I: $E_\ell(I) := I \cap k[X_{\ell+1}, \ldots, X_n]$

$E_0(I) = I, \quad E_{\ell+1}(I) = E_1(E_\ell(I))$ $\qquad$ ($E_1(.)$ eliminates the first variable).

Lemma 3 *Let $V = \mathbf{V}(I)$ the affine variety defined by the ideal $I \subset k[X_1, \ldots, X_n]$. The inclusion $\pi_\ell(V) \subset \mathbf{V}(E_\ell(I))$ holds.*

Proof: *(on the balckboard, with counterexamples to equality)*

Elimination theorem

Theorem 1 *Let $\prec$ be the monomial order $lex(X_1, \ldots, X_n)$, and $I \subset k[X_1, \ldots, X_n]$ an ideal.*

Let G be a Gröbner basis of I for $\prec$.

Define for $0 \leq \ell \leq n-1$ the set $$G_\ell = G \cap k[X_{\ell+1}, \ldots, X_n].$$

Then $\langle G_\ell \rangle = E_\ell(I) \quad (= I \cap k[X_{\ell+1}, \ldots, X_n])$.

Important remark:

Let $I = \langle A, B \rangle \subset k[X, Y] \rightarrow$ system of 2 polynomials A, B, 2 unknowns X, Y.

Then $E_1(I) = I \cap k[Y]$ verifies: $$\boxed{E_1(I) = \langle \mathsf{Res}_X(A, B) \rangle}$$

$\longrightarrow$ Lex. GB. generalizes resultants.

Basic solving

Fact: $x \succ_{lex} y \succ_{lex} z$ Gröbner bases eliminate variables; it looks like:

$$
x \begin{cases}
g_s(z,y)x^{c_s} + \cdots x^{c_s-1} + \cdots \mathit{terms\ of\ deg}(x) < c_s - 1 \\
\qquad \ddots \qquad \qquad \vdots \\
g_t(z,y)x^{c_t} + \cdots \mathit{terms\ of\ deg}(x) < c_t
\end{cases}
$$

$$
G_1 \qquad y \begin{cases}
\vdots \\
g_u(z)y^{c_u} + \cdots \mathit{terms\ of\ deg}(y) < c_u \\
\ddots
\end{cases}
$$

$$
G_2 \qquad z \begin{cases}
z^{c_\ell} + \cdots z^{c_\ell - 1} + \cdots \mathit{terms\ of\ deg}(z) < c_\ell \\
\qquad \ddots \qquad \qquad \vdots \\
z^{c_1} + \cdots \mathit{terms\ of\ deg}(z) < c_1
\end{cases}
$$

Basic solving

Fact: $x \succ_{lex} y \succ_{lex} z$ Gröbner bases eliminate variables; it looks like:

$$x \left\{ \begin{array}{l} g_s(z,y)x^{c_s} + \cdots x^{c_s-1} + \cdots \mathit{terms\ of\ deg}(x) < c_s - 1 \\ \qquad\qquad \ddots \qquad\qquad\qquad\qquad \vdots \\ \qquad\qquad g_t(z,y)x^{c_t} + \cdots \mathit{terms\ of\ deg}(x) < c_t \end{array} \right.$$

$$G_1 \qquad y \left\{ \begin{array}{l} \qquad\qquad\qquad \vdots \\ g_u(z)y^{c_u} + \cdots \mathit{terms\ of\ deg}(y) < c_u \\ \qquad\qquad\qquad \ddots \end{array} \right.$$

$$G_2 \qquad\qquad z \left\{ z^{c_1} + \cdots \mathit{terms\ of\ deg}(z) < c_1 \right.$$

$G_2 = G \cap k[z] \Rightarrow G_2$ can be generated by **one** polynomial

Basic solving

Fact: $x \succ_{lex} y \succ_{lex} z$ Gröbner bases eliminate variables; it looks like:

$$
x \left\{ \begin{array}{c} g_s(z,y)x^{c_s} + \cdots x^{c_s-1} + \cdots terms\ of\ deg(x) < c_s - 1 \\ \ddots \qquad\qquad\qquad\qquad \vdots \\ g_t(z,y)x^{c_t} + \cdots terms\ of\ deg(x) < c_t \end{array} \right.
$$

$$
G_1 \qquad y \left\{ \begin{array}{c} \vdots \\ g_u(z)y^{c_u} + \cdots terms\ of\ deg(y) < c_u \\ \ddots \end{array} \right.
$$

Case $E_2(I) = I \cap k[z] = \langle 0 \rangle \Rightarrow G_2 = \emptyset$

Basic solving

Strategy:

- Solving univariate polynomials only:

  first, in z

  second, in y

  third, in x

- finding roots of univariate polynomials:

  efficient numerical algorithm (like Newton-Raphson or another).

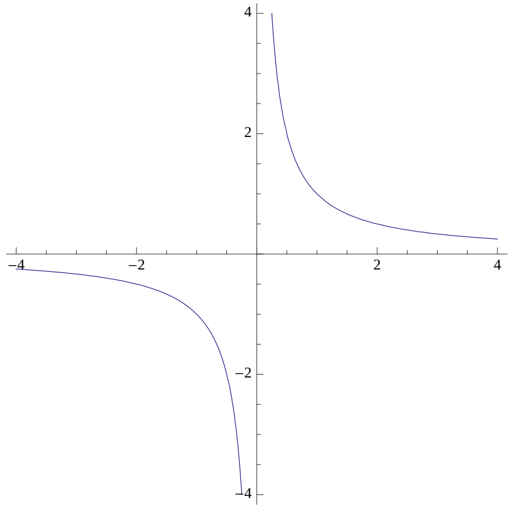
Remark: In practice, works well if the Gröbner basis is “purely” triangular,

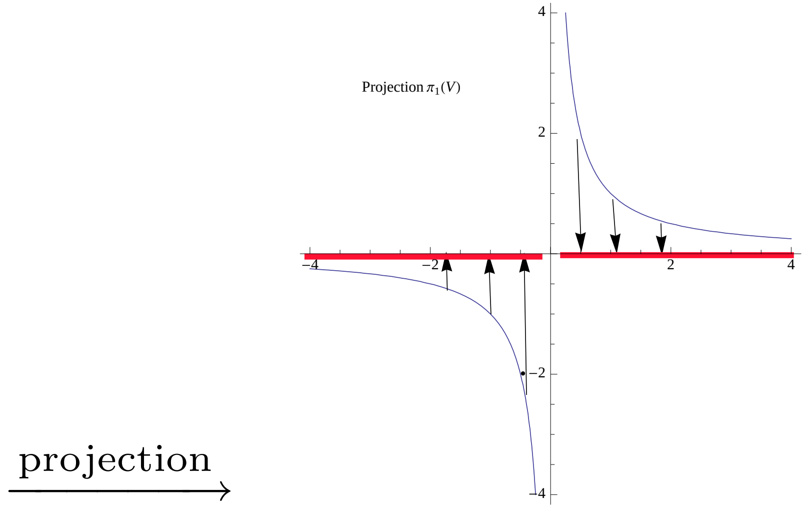
$$
\begin{array}{lr}
\text{one polynomial in } x & x^c + f_{c-1}(z,y)x^{c-1} + \cdots \\
\text{one polynomial in } y & y^b + g_{b-1}(z)y^{b-1} + \cdots \\
\text{one polynomial in } z & z^a + h_{a-1}z^{a-1} + \cdots
\end{array}
$$

and there are no multiplicities…

Extension theorem (on a toy example)

The problem:





$\boxed{f(x,y) = yx - 1}$ is a Gröbner basis of $I = \langle f \rangle$ for $lex(y,x)$.

Clearly, $E_1(I) = \langle f \rangle \cap k[x] = \langle 0 \rangle$. $\mathbf{V}_{\mathbb{C}}(E_1(I)) = \mathbb{C}$.

But $\pi_1(V) = \mathbb{C} - \{0\} \Rightarrow \pi_1(V) \subsetneq \mathbf{V}(E_1(I))$ $\Rightarrow$ 0 is a useless solution.

Let us write $f(x,y) = a_1(x)y + a_0(x)$, $a_1(x) = x$, and $a_0(x) = -1$.

We have that 0 is a root of $a_1(x) = x$. We have $\boxed{\mathbf{V}(E_1(I)) = \pi_1(V) \cup \mathbf{V}(a_1)}$.

Extension theorem (in general)

Generalization: Let $I = \langle f_1, \ldots, f_s \rangle \subset k[X_1, \ldots, X_n]$.

Let $E_1(I) = I \cap k[X_2, \ldots, X_n]$ (1st elimination ideal of I, eliminate X_1)

We write:

$\forall\, 1 \leq i \leq s,\ f_i = a_i(X_2, \ldots, X_n){X_1}^{N_i} + \cdots$ *terms of degree in* $X_1 < N_i$,
where $a_i \neq 0$.

Let $(x_2, \ldots, x_n) \in \mathbf{V}_{\bar{k}}(E_1(I))$ be a partial solution.

Theorem 2 *Suppose that* $(x_2, \ldots, x_n) \notin \mathbf{V}_{\bar{k}}(a_1, \ldots, a_s)$.

Then there exists $x_1 \in \bar{k}$ *such that the partial solution can be extended to a whole solution* $(x_1, \ldots, x_n) \in V = \mathbf{V}_{\bar{k}}(I)$.

$$\iff \big((x_2, \ldots, x_n) \notin \mathbf{V}_{\overline{k}}(a_1, \ldots, a_s) \Rightarrow (x_2, \ldots, x_n) \in \pi_1(V)\big)$$

$$\iff \boxed{\mathbf{V}_{\overline{k}}(E_1(I)) = \pi_1(V) \cup \mathbf{V}_{\overline{k}}(a_1, \ldots, a_s)}$$

Extension theorem (3 comments)

- The equality $\boxed{\mathbf{V}_{\overline{k}}(E_1(I)) = \pi_1(V) \cup \mathbf{V}_{\overline{k}}(a_1, \ldots, a_s)}$ is true only over an algebraically closed field (like $\mathbb{C}$) $\longrightarrow$ we used $\overline{k}$ and not k
- Link with resultant: (Lect. VI, Part 2, Prop. 3)

$$\begin{aligned} A(X,Y) &= a_m(X)Y^m + a_{m-1}(X)Y^{m-1} + \cdots + a_1(X)Y + a_0(X) \\ B(X,Y) &= b_n(X)Y^n + b_{n-1}(X)Y^{n-1} + \cdots + b_1(X)Y + b_0(X) \end{aligned}$$

Let $r(X) = \mathsf{Res}_Y(A,B)$, the resultant that eliminates Y.

$x \in \overline{k},\ r(x) = 0 \iff \big(\exists y \in \overline{k}, A(x,y) = B(x,y) = 0 \quad \text{or } a_m(x) = b_n(x) = 0\big)$

$\iff \boxed{\mathbf{V}_{\overline{k}}(E_1(A,B)) = \mathbf{V}_{\overline{k}}(r) = \pi_1(V) \cup \mathbf{V}_{\overline{k}}(a_m, b_n)}$, with $\cup$ **disjoint**.

- **!!** In **Theorem 2**, the union $\cup$ is **not disjoint** in general. **!!**

But, the union $\cup$ **is disjoint** if $f_1, \ldots, f_s$ is a lex GB. (PROOF: *points in* $\mathbf{V}(a_1, \ldots, a_s)$ *are solutions at the infinity... requires projective tools...*)

Weak Nullstellensatz

Fundamental Theorem of Algebra: Any non-constant polynomial $P(X) \in \mathbb{C}[X]$ has at least one root.

P is not constant $\iff$ $\big(1 \notin \langle P \rangle \subset \mathbb{C}[X]\ \big)$

P has at least one root $\iff$ $\mathbf{V}_{\mathbb{C}}(P) \neq \emptyset$.

Weak Nullstellensatz: Let $f_1, \ldots, f_s$ be a polynomial system in $\mathbb{C}[X_1, \ldots, X_n]$.

Theorem 3 $\boxed{1 \notin \langle f_1, \ldots, f_s \rangle \iff \mathbf{V}(f_1, \ldots, f_s) \neq \emptyset}$

Or, the polynomial system $f_1 \ldots, f_s$ has a solution if and only if the ideal $\langle f_1, \ldots, f_s \rangle$ has no constant.

Nullstellensatz (1/2): radical ideal

Let $I \subset k[X_1, \ldots, X_n]$ be an ideal.

Lemma 1 says that $I \subset \mathbf{I}(\mathbf{V}(I))\ldots$ What is $\mathbf{I}(\mathbf{V}(I))$?

Definition 4 $\sqrt{I} := \{f \in k[X_1, \ldots, x_n]$ *such that* $\exists n \in \mathbb{N}\ ,\ f^n \in I\}$ *This is an ideal, called the* radical *of* I*.*

For any ideal J*, always holds* $J \subset \sqrt{J}$*. An ideal* J *is* radical*, if* $\sqrt{J} = J$*.*

Remark: Let $f \in k[X]$ a polynomial.

It has a unique factorization, that is, there exist irreducible polynomials (Cf. Lect. II, Definition 5) $P_1, \ldots, P_s \in k[X]$ such that:

$$f = P_1^{e_1} \ldots P_s^{e_s}.$$

The exponent $e_i \in \mathbb{N}$ is called the multiplicity of P_i.

Check that: $\sqrt{\langle f \rangle} = \langle P_1 \ldots P_s \rangle$ (this is the squarefree part of f).

Nullstellensatz (2/2)

Theorem 4 *Let I be an ideal of $k[X_1, \ldots, X_n]$ over an* algebraically closed *field k (like $k = \mathbb{C}$). We have* $\boxed{\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}}$.

PROOF:(on the blacboard...)

Comments:

- True over $\mathbb{C}$, not true over $\mathbb{R}$.
- The radical $\sqrt{I}$ is difficult to compute in general.
- **But**, it is easy to test if $f \in \sqrt{I}$ (when we know $I = \langle f_1, \ldots, f_s \rangle$):

Rabinovitch's trick: $f \in \sqrt{I} \iff 1 \in \langle f_1, \ldots, f_s, 1 - Yf \rangle$, ($Y$ new variable).

Irreducible varieties and prime ideals

Definition 5 *V is irreducible if:* $V = V_1 \cup V_2 \Rightarrow V = V_1$ *or* $V = V_2$

$V = \mathbf{V}(x^2 - y^2)$ is not irreduiclbe because $V = \mathbf{V}(x - y) \cup \mathbf{V}(x + y)$.

Prime ideal: (Lect. II, Def. 6) $\mathfrak{p}$ is a prime ideal if $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Proposition 1 *Let $V \subset k^n$ be an affine variety.*

V is irred. $\iff$ $\mathbf{I}(V)$ *is a prime ideal*.

PROOF:*(on the blackboard...)*

Proposition 2 *Any affine variety V is a finite union of irreducible varieties. There exists irred. varieties $V_1, \ldots, V_s$ such that:*

$$V = V_1 \cup \ldots \cup V_s.$$

PROOF:*(It is an indiction proof, that uses the Noetherian property...)*

Corollary 1 *Over an* algebraically closed *field k, any* radical *ideal $I \neq \langle 1 \rangle$ is a finite intersection of prime ideals:* $I = \cap_{i=1}^{s} \mathfrak{p}_1$

PROOF: *(roughly,* $I = \mathbf{I}(V) = \mathbf{I}(V_1 \cup \cdots \cup V_s) = \mathbf{I}(V_1) \cap \ldots \cap \mathbf{I}(V_s)$*)*

The algebra-geometry dictionnary

ALGEBRA		GEOMETRY
$k[X_1, \ldots, X_n]$		affine spaces k_1^n $(k \subset k_1)$
Ideal I	$\xrightarrow{\mathbf{V}_{k_1}(\,.\,)}$	affine varieties $\mathbf{V}_{k_1}(I) \subset k_1^n$
Radical ideals $I = \sqrt{I}$	$\xleftarrow{\mathbf{I}(\,.\,)}$	
Prime ideals $\mathfrak{p}$	$\longleftrightarrow$	irreducible varieties
Elimination ideals $E_\ell(I)$	$\dashrightarrow$	Projection varieties $\pi_\ell(V)$
$\sqrt{E_\ell(I)}$	$\xleftarrow{\mathbf{I}(\,.\,)}$	
$\sqrt{I \cap J}$	$\longleftrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$