Slide 1

On the Theories of Triangular Sets

Marc Moreno Maza (NAG)

March 16, 1998

Slide 2

What we would like to have ...

Given a polynomial system $\left\{ \begin{array}{rcl} p_1(x_1,\ldots,x_{\mathbf{n}}) & = & 0 \\ p_2(x_1,\ldots,x_{\mathbf{n}}) & = & 0 \\ & \vdots & \\ p_{\mathbf{m}}(x_1,\ldots,x_{\mathbf{n}}) & = & 0 \end{array} \right.$

with $p_1,\ldots,p_m \in \mathbb{Q}[x_1,\ldots,x_n]$ we want a solution like :

$$\left\{ \begin{array}{rcl} x_1 & = & \alpha_1 \\ x_2 & = & \alpha_2 \\ & \vdots & \\ x_n & = & \alpha_n \end{array} \right. \quad \text{or} \quad \left\{ \begin{array}{rcl} x_1 & = & \beta_1 \\ x_2 & = & \beta_2 \\ & \vdots & \\ x_n & = & \beta_n \end{array} \right. \quad \text{or} \ \ldots$$

where $\alpha_1,\alpha_2,\ldots,\alpha_n,\beta_1,\beta_2,\ldots,\beta_n,\ldots$ are **exact values** like 1, $\frac{355}{113}$, $\frac{1+\imath\sqrt{5}}{2}$.

. . . and cannot always get

Because we may have

- $\begin{cases} x_1^{10^9} = 1 \\ x_2 = x_1 \end{cases}$ or

- $\begin{cases} x_1^5 + a_4 x_1^4 + \cdots + a_1 x_1 + a_0 = 0 \\ x_2 = \alpha_2(x_1) \\ \vdots \\ x_n = \alpha_n(x_1) \end{cases}$ or

- $\mathbf{m < n}$

Slide 3

Slide 4

What can we expect ?

• For $\left\{ \begin{array}{r} x^6 - 2\ x^4 + 3\ x^3 + x^2 - 6\ x - 2 = 0 \\ x^5 - 2\ x^3 - 3\ x^2 + 6 = 0 \end{array} \right.$

the set of solutions is : $S = \{x \ \mid \ x^2 - 2 = 0\}$.

• For $\left\{ \begin{array}{r} x - t^3 = 0 \\ y - t^2 = 0 \\ z - t = 0 \end{array} \right.$

the set of solutions may be the system itself.

• For $\left\{ \begin{array}{r} \left(x^2 - 2\right)\ y^2 + \left(-2\ x^3 + 4\ x\right)\ y + x^4 - 2\ x^2 = 0 \\ x^4 - 5\ x^2 + 6 = 0 \end{array} \right.$

the set of solutions may be given by :

$$\left\{ \begin{array}{r} x^2 - 3 = 0 \\ (y - x)^2 = 0 \end{array} \right. \quad \text{or} \quad \left\{ \ x^2 - 2 = 0 \right.$$

Slide 5

- For $\begin{cases} x^2+y+z=1 \\ x+y^2+z=1 \\ x+y+z^2=1 \end{cases}$

with $\boxed{z<y<x}$ <u>a solution is</u> :

$$\begin{cases} z^6-4z^4+4z^3-z^2=0 \\ 2z^2y+z^4-z^2=0 \\ y^2-y-z^2+z=0 \\ x+y+z^2-1=0 \end{cases}$$

<u>Another solution is</u> :

$$\begin{cases} z &=& 1 \\ y &=& 0 \\ x &=& 0 \end{cases} \text{ or } \begin{cases} z &=& 0 \\ y &=& 1 \\ x &=& 0 \end{cases} \text{ or } \begin{cases} z &=& 0 \\ y &=& 0 \\ x &=& 1 \end{cases} \text{ or }$$

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

Gröbner Bases & Triangular Sets

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$ we want to describe $\mathbf{V}(F)$.

Gröbner Bases

Slide 6

- Rewrites the ideal $\langle F \rangle$ by providing a special set of generators.
- For polynomial system solving (in practise) this is only an intermediate step.
- Computation complexity increases very quickly when $\langle F \rangle$ contains components of different dimensions.
- Output Size may be very big.

Slide 7

Gröbner Bases & Triangular Sets

Triangular Sets Methods

- Decomposes $\sqrt{\langle F \rangle}$ into unmixed-dimensional components, each compnent given by at least n polynomials.
- Different algorithms which do not provide the same kind of decompositions.
- Some algorithms produce redundant decompositions

$\Longrightarrow$ Needs of a unified theory and practical comparison.

Slide 8

Contents

Slide 9

Triangular Sets

1 A recursive view of Polynomials

2 Triangular Sets

3 Regular Zeros and Saturated Ideals

Slide 10

A recursive view of Polynomials

Notations

- $\mathbf{k}$ a field and $x_1 < \cdots < x_n$ variables.
- $p, q \in \mathbf{k}[x_1, \ldots, x_n]$ with $q \notin \mathbf{k}$.
- $\mathsf{mvar}(q)$ the gratest variable of q.
- $\mathsf{prem}(p, q)$ pseudo-remainder of p by q w.r.t. $\mathsf{mvar}(q)$.

Definition

$$\mathsf{mvar}(q) = x_i \quad \Longrightarrow \quad q = \mathsf{init}(q)\ {x_i}^{\mathsf{mdeg}(q)} + \mathsf{tail}(q)$$

$$\text{where} \begin{cases} \mathsf{init}(q) \in \mathbf{k}[x_1, \ldots, x_{i-1}] \\ \mathsf{mdeg}(q) = \mathsf{deg}(q, x_i) \\ \mathsf{deg}(\mathsf{tail}(q), x_i) < \mathsf{mdeg}(q) \end{cases}$$

Example

$$\left.\begin{array}{c} p = x_2^2 + x_1 x_2 + x_1^2 \\ q = x_1 x_2 - 1 \end{array}\right\} \Longrightarrow \begin{cases} \mathsf{init}(q) = x_1 \\ \mathsf{mdeg}(q) = 1 \\ \mathsf{tail}(q) = -1 \\ \mathsf{prem}(p, q) = x_1^4 + x_1^2 + 1 \end{cases}$$

Slide 11

Triangular Sets

Definition

$T \subseteq \mathbf{k}[x_1, \ldots, x_n]$ is a *triangular set* iff

(i) $T \cap \mathbf{k} = \emptyset$,

(ii) $(\forall p, q \in T)\ p \neq q \implies \mathsf{mvar}(p) \neq \mathsf{mvar}(q)$.

Notations

$\mathsf{prem}(p, T) ==$

$T = \emptyset =>$ **return** p

$t :=$ the $p \in T$ with maximum $\mathsf{mvar}(p)$

return $\mathsf{prem}(\mathsf{prem}(p, t), T \setminus \{t\})$

- $\mathsf{red}_{\mapsto 0}(T) = \{p \in \mathbf{k}[x_1, \ldots, x_n] \mid \mathsf{prem}(p, T) = 0\}$.

Example 1

If $T = \{x_1(x_1 - 1), x_1 x_2 - 1\}$ and $p = x_2^2 + x_1 x_2 + x_1^2$

$$\mathsf{prem}(p, T) = \mathsf{prem}(\mathsf{prem}(p,\ T_{x_2}),\ T_{x_1}) = 2\ x_1 + 1.$$

Slide 12

Regular Zeros and Saturated Ideals (I)

Notations

- $h(T)$ the product of the $\mathsf{init}(t)$ for $t \in T$.
- $\mathbf{K}$ an algebraic closure of $\mathbf{k}$.
- For $W \subseteq \mathbf{K}^n$, the Zariski closure of W w.r.t. $\mathbf{k}$ is $\overline{W}$:

$$\overline{W} = \bigcap_{\substack{F \subseteq \mathbf{k}[x_1, \ldots, x_n] \\ W \subseteq \mathbf{V}(F)}} \mathbf{V}(F)$$

Definition

The *Regular Zero Set* of T is:

$$\mathbf{W}(T) = \mathbf{V}(T) \setminus \mathbf{V}(h(T)).$$

The *Saturated Ideal* of T is:

$$\mathsf{sat}(T) = \{p \in \mathbf{k}[x_1, \ldots, x_n] \mid (\exists e \in \mathbb{N})\ h(T)^e p \in \langle T \rangle\}.$$

Slide 13

Regular Zeros and Saturated Ideals (II)

Example 1

$$T = \{x_1(x_1-1), x_1x_2-1\} \Rightarrow \begin{cases} \mathsf{sat}(T) = \langle x_1 - 1, x_2 - 1\rangle \\ \mathbf{W}(T) = \mathbf{V}(x_1 - 1, x_2 - 1) \end{cases}$$

$$\left.\begin{array}{c} p = (x_1 - 1)(x_1x_2 - 1) \\ q = -(x_1 - 1)x_1x_2 \end{array}\right\} \Rightarrow \begin{cases} p, q \in \mathsf{red}_{\mapsto 0}(T) \\ p + q \notin \mathsf{red}_{\mapsto 0}(T) \end{cases}$$

Example 2

If $T = \{x_2^2 - x_1, x_3^2 - 2x_2x_3 + x1, (x_3 - x_2)x_4\}$ then:

$$\mathbf{V}(T) \neq \emptyset \ \text{ but } \ \mathbf{W}(T) = \emptyset.$$

Proposition

- $\mathsf{red}_{\mapsto 0}(T) \subseteq \mathsf{sat}(T)$.
- $\mathsf{red}_{\mapsto 0}(T)$ is not necessarily an ideal of $\mathbf{k}[x_1, \ldots, x_n]$.
- $\overline{\mathbf{W}(T)} = \mathbf{V}(\mathsf{sat}(T))$

Characteristic Sets

Slide 14

1 Characteristic Sets

2 Characteristic Sets and Gröbner Bases

3 Characteristic Sets of Prime ideals

Slide 15

Characteristic Sets

Definition

The triangular set T is called *fine* if:

$$T \neq \emptyset \quad \text{and} \quad (\forall t \in T)\ \mathsf{prem}(\mathsf{init}(t), T) \neq 0.$$

Definition

Let $\mathcal{I}$ be an ideal of $\mathbf{k}[x_1, \ldots, x_n]$. A subset $T \subseteq \mathcal{I}$ is a *characteristic set* of $\mathcal{I}$ if:

(i) either $\mathcal{I} = \langle 1 \rangle$ and $T = \{1\}$,

(ii) or T is a fine triangular set and $\mathcal{I} \subseteq \mathsf{red}_{\mapsto 0}(T)$.

$\triangle$ This is not the original definition (Ritt, 1932).

Slide 16

Characteristic Sets and Gröbner Bases

Theorem

Assume $\mathcal{I} \neq \langle 1 \rangle$. The reduced lexicographical Gröbner basis G of $\mathcal{I}$ **contains** exactly one characteristic set of $\mathcal{I}$ called the *median set* of $\mathcal{I}$ and denoted by $\mathcal{M}(\mathcal{I})$.

Example 3

Assume $\mathcal{I} = \langle F \rangle$ with $F = \{x_1x_2, x_2x_3, x_3x_4\}$.
Then we have $G = F$ and $\mathcal{M}(\mathcal{I}) = \{x_1x_2, x_3x_4\}$.

Example 2

Assume $\mathcal{I} = \langle F \rangle$ with
$F = \{x_2^2 - x_1, x_3^2 - 2x_2x_3 + x1, (x_3 - x_2)x_4\}$.
Then we have $G = F$ and $\mathcal{M}(\mathcal{I}) = F$.

Example 4

With $F = \{x_1^2 - 2, x_2^2 - 2, (x_1 - x_2)x_3, (x_1 + x_2)x_4\}$.
Then we have $G = F \cup \{x_3x_4\}$ and $\mathcal{M}(\mathcal{I}) = F$.
$\mathcal{I}$ is radical but $\mathbf{W}(F) = \emptyset$.

Slide 17

Characteristic Sets of Prime Ideals

Theorem

Assume $\mathcal{P}$ is a prime ideal with $\mathcal{P} \neq \langle 1 \rangle$. Then we have:

(i) $\mathcal{P} = \mathsf{red}_{\mapsto 0}(\mathcal{M}(\mathcal{P}))$,

(ii) $\mathbf{V}(\mathcal{P}) = \overline{\mathbf{W}(\mathcal{M}(\mathcal{P}))}$,

(iii) $\mathcal{P} = \mathsf{sat}(\mathcal{M}(\mathcal{P}))$,

(iv) $\mathbf{W}(\mathcal{M}(\mathcal{P})) \neq \emptyset$.

Slide 18

Regular Chains

Definition

The triangular set $T \subseteq \mathbf{k}[x_1, \ldots, x_n]$ is a *regular chain* if

(i) $T = \emptyset$

(ii) For every $t \in T$, with $x_i = \mathsf{mvar}(t)$, the initial $\mathsf{init}(t)$ of t does not belong to any of the prime ideals associated with $\mathsf{sat}(T \cap \mathbf{k}[x_1, \ldots, x_{i-1}])$.

$\triangle$ This is not the original definition (Kalkebrener, 1991)

Proposition

If T is a regular chain with s elements, then T is consistent and Sat(T) is an unmixed-dimensional ideal of dimension $n - s$ (Kalkebrener, 1991).

Slide 19

Regular Sets

1 Towers of Simple Extensions

2 Towers and Affine varieties

3 Regular Sets

Slide 20

Towers of Simple Extensions

Definition

$\mathbf{k} = \mathbf{A}_0 \subseteq \mathbf{A}_1 \subseteq \cdots \subseteq \mathbf{A}_n$

$(\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_n)$ *tower of simple extensions* $\mathbf{k}$ if either

$$\mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[X_i])$$

or

$$\exists t_i \in \mathbf{A}_{i-1}[X_i] \begin{cases} t_i \text{ monic} \\ \mathbf{A}_i = \mathbf{fr}(\ \mathbf{A}_{i-1}[X_i]/\langle t_i \rangle) \end{cases}$$

$$\begin{array}{ccccc} \mathbb{Q} & \longmapsto & \mathbb{Q}(\sqrt{2}) & \longmapsto & \mathbb{Q}(\sqrt{2})(\sqrt{3}) \\ & & \| & & \| \\ & & \mathbb{Q}[x_2] \ / \ \langle x_2^2 - 2 \rangle & & \mathbb{Q}(\sqrt{2})[x_1] \ / \ \langle x_1^2 - 3 \rangle \end{array}$$

$$\begin{array}{ccccc} \mathbb{Q} & \longmapsto & \mathbb{Q}(x_2) & \longmapsto & \mathbb{Q}(x_2)(\sqrt{x_2}) \\ & & \| & & \| \\ & & \mathsf{fr}(\mathbb{Q}[x_2]) & & \mathbb{Q}(x_2)[x_1] \ / \ \langle x_1^2 - x_2 \rangle \end{array}$$

Slide 21

Motivations

All t_i irreducible $\Rightarrow \exists \mathcal{P}$ such that:

$$\mathbf{A}_n \equiv \mathbf{fr}(\mathbf{k}[x_1, \ldots, x_n]/\mathcal{P}).$$

$\mathcal{P}$ prime $\Rightarrow \mathbf{A}_i = \mathbf{A}_{(i-1)}(\zeta_i)$ où

$$\begin{cases} \mathbf{A}_0 = \mathbf{k} \\ \mathbf{A}_i = \mathbf{fr}(\mathbf{k}[x_1, \ldots, x_i]/\mathcal{P} \cap \mathbf{k}[x_1, \ldots, x_i]) \\ \zeta_i = x_i/\mathbf{A}_i \end{cases}$$

$\Rightarrow$ **Affine varieties can be described by the towers (of the prime ideals) of their irreducible components.**

Slide 22

Regular Sets

The triangular set $T = \{\ldots, t_i, \ldots\} \subseteq \mathbf{k}[x_1, \ldots, x_n]$ is a *regular set associated with the tower* $\mathbf{k} = \mathbf{A}_0 \subseteq \mathbf{A}_1 \subseteq \cdots \subseteq \mathbf{A}_n$ if:

- $T = \emptyset$ and $\mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[x_i])$
- $T \cap \mathbf{k}[x_1, \ldots, x_{n-1}]$ is a regular set associated with $\mathbf{k} = \mathbf{A}_0 \subseteq \mathbf{A}_1 \subseteq \cdots \subseteq \mathbf{A}_{n-1}$ and:
  - either T has no polnomial in x_n and $\mathbf{A}_n = \mathbf{fr}(\mathbf{A}_{n-1}[x_n])$
  - or T has a polnomial t_n in x_n which is monic in $\mathbf{A}_{n-1}[x_n]$ and $\mathbf{A}_n = \mathbf{fr}(\ \mathbf{A}_{n-1}[x_n]/\langle t_n \rangle)$

Slide 23

The Unification Theorem

Theorem (Aubry, Lazard, Moreno Maza, 1997):

$$\text{T regular chain}$$
$$\Updownarrow$$
$$\text{T regular set}$$
$$\Updownarrow$$
$$\mathsf{sat}(T) = \{p \mid \mathsf{prem}(p, T) = 0\}$$
$$\Updownarrow$$
$$T \ \text{characteristic set of } \mathsf{sat}(T)$$

Remarks

- I've told you four times the same thing this morning.
- The case where $\mathsf{sat}(T)$ is prime is not hard to check.
- $(i) \iff (ii)$ and $(ii) \iff (iii)$ are not easy to prove in the general case.