On Triangular Decompositions of Algebraic Varieties

Marc Moreno Maza (NAG, Oxford)

20 June 2000

A short history but an intense activity

[Wu, 1987] [Kalkbrener, 1991], [Lazard, 1991], [Wang, 1993] ...

- Applications in various areas.
  - Computations with algebraic numbers [Rioboo, 1992]. [Gómez-Díaz, 1994] [Dellière, 1999].
  - Decomposition into primes [Shimoyama and Yokoyama, 1996].
  - Algebraic Geometry [Tran, 1998] [Richardson, 1999].
  - Differential Algebra [Boulier, 1995-1997] [Hubert 2000].
- Recent advances.
  - Unification of concepts [Aubry, Lazard, Moreno Maza, 1999].
  - Canonicity issues [Ollivier 1990] [Boulier et Lemaire, 2000].
  - Complexity issues [Szántó, 1999].

Basic Definitions

- $p \in \mathbf{k}[x_1, \ldots, x_n]$ is regular modulo ideal $\mathcal{I}$ if for every prime $\mathcal{P}$ associated with $\mathcal{I}$ we have $p \notin \mathcal{P}$.
- $T \subseteq \mathbf{k}[x_1 < \cdots < x_n]$ is triangular if $T \cap \mathbf{k} = \emptyset$ and if for $i = 1 \cdots n$ there is at most one $t \in T$ with main variable x_i.
- The saturated ideal of T is $\mathbf{Sat}(T) = \mathcal{I}(T) : {h_T}^\infty$ where h_T is the product of the initials of T.
- T is a regular chain if for every $p = h_p x_i^d + \cdots \in T$ the initial h_p is regular modulo $\mathbf{Sat}(T \cap \mathbf{k}[x_1, \ldots, x_{i-1}])$.
- The quasi-component of T is $\mathbf{W}(T) = \mathbf{V}(T) \setminus \mathbf{V}(h_T) \subseteq \mathbf{K}^n$.
  We have: $\overline{\mathbf{W}(T)} = \mathbf{V}(\mathbf{Sat}(T))$.

  [Kalkbrener 91], [Aubry, Lazard, Moreno Maza, 1999].

Fundamental Properties

- If T is a regular chain then
  - T is a characteristic of $\mathbf{Sat}(T)$ (and conversely),
  - $\mathbf{Sat}(T) = \{p \mid \mathsf{prem}(p, T) = 0\}$ (and conversely),
  - if $\mid T \mid = \ell$ then every prime associated with $\mathbf{Sat}(T)$ has height ℓ.
- T, U regular chains. If $\sqrt{\mathbf{Sat}(T)} \subseteq \sqrt{\mathbf{Sat}(U)}$ and $\mid T \mid = \mid U \mid$, then every polynomial regular modulo $\mathbf{Sat}(T)$ is regular modulo $\mathbf{Sat}(U)$.
- For a polynomial p regular modulo $\mathbf{Sat}(T)$ either $\mathbf{Z}(p, T) = \emptyset$ or $\mathsf{dim}(\mathbf{Z}(p, T)) < \mathsf{dim}(\mathbf{Sat}(T))$ where $\mathbf{Z}(p, T) = \mathbf{V}(p) \cap \mathbf{W}(T)$.
- For every prime $\mathcal{P}$ we read T such that $\mathcal{P} = \mathbf{Sat}(T)$ in the lex. base of $\mathcal{P}$; moreover $\mathbf{W}(T)$ corresponds to the generic zeros of $\mathcal{P}$.

$$(\mathcal{P}) = \begin{cases} ax + by - c \\ dx + ey - f \\ gx + hy - i \end{cases} \simeq (T) = \begin{cases} gx + hy - i \\ (hd - eg)\, y - id + fg \\ (ie - fh)\, a + (ch - ib)\, d + (fb - ce)\, g \end{cases}$$

Lex Base:

$$\begin{cases} xa + yb - c & xd + ye - f & \boxed{xg + yh - i} \\ yae - ydb - af + dc & yah - ygb - ai + gc & \boxed{ydh - yge - di + gf} \\ \boxed{aei - ahf - dbi + dhc + gbf - gec} & & \end{cases}$$

$$\begin{aligned} \mathbf{V}(\mathcal{P}) \quad = \quad & \mathbf{W}(T) \cup \mathbf{W} \begin{cases} dx + ey - f \\ hy - i \\ (ie - fh)\, a + (-ib + ch)\, d \\ g \end{cases} \cup \mathbf{W} \begin{cases} gx + hy - i \\ (ha - bg)\, y - ia + cg \\ hd - eg \\ ie - fh \end{cases} \\ & \cup \mathbf{W} \begin{cases} x \\ (hd - eg)\, y - id + fg \\ fb - ce \\ ie - fh \end{cases} \cup \mathbf{W} \begin{cases} ax + by - c \\ hy - i \\ d \\ g \\ ie - fh \end{cases} \cup \cdots \end{aligned}$$

Splitting into Quasi-Components

- Let $W, , \ldots, W_i, \ldots, W_{i,j}, \ldots \subseteq \mathbf{K}^n$.
  - $W \longrightarrow_K (W_1, \ldots, W_\ell) \iff \overline{W} = \cup_{i=1}^{\ell} \overline{W_i}$.
  - $W \longrightarrow_L (W_1, \ldots, W_\ell) \iff W \subseteq \cup_{i=1}^{\ell} W_i \subseteq \overline{W}$.
- If $W \longrightarrow_L (W_1, \ldots, W_\ell)$ and $V \cap W_i \longrightarrow_L (W_{i,1}, \ldots, W_{i,n_i})$, where $V = \overline{V}$, then

$$V \cap W \longrightarrow_L (W_{1,1}, \ldots, W_{1,n_1}, \ldots, W_{\ell,1}, \ldots, W_{\ell,n_\ell}).$$

- t, a, b with main variable x_{i+1} such that $T \cup t$ regular chain, $\mathsf{prem}(t, a) \in \mathbf{Sat}(T) \cap \mathbf{k}[x_1, \ldots, x_i]$, $b = \mathsf{pquo}(t, a)$ and the initial h_a of a is regular modulo $\mathbf{Sat}(T)$. Then we have:

(a) $\mathbf{W}(T \cup t) \longrightarrow_K (\mathbf{W}(T \cup a), \mathbf{W}(T \cup b))$,

(b) $\mathbf{W}(T \cup t) \longrightarrow_L (\mathbf{W}(T \cup a), \mathbf{W}(T \cup b), \mathbf{Z}(h_a, T \cup t))$.

Kalkbrener's Algorithm

• Given $F \subseteq \mathbf{k}[x_1, \ldots, x_n]$ computes regular chains $T_1, \ldots, T_\ell$ such that

$$\mathbf{V}(F) = \cup_{i=1}^{\ell} \overline{\mathbf{W}(T_i)}.$$

• bottom-up elimination: the algorithm relies on $\mathsf{decompose}_n$ defined with $\mathsf{decompose}_{n-1}$.

• *non-generic* zeros may be hidden.

• $\overline{\mathbf{W}(T_i)}$ may be contained in $\overline{\mathbf{W}(T_j)}$.

• Kalkbrener's decompositions can be obtained by Szántó's algorithm with sequential complexity $deg^{O(n^2(dim+1))}$
and parallel complexity $(n \log(deg))^{O(1)}$.

[Kalkbrener, 1991-1998], [Szántó, 1999], [Aubry, 1999].

Lazard's Algorithm

• Given $F \subseteq \mathbf{k}[x_1, \ldots, x_n]$ computes regular chains with additional strong properties $T_1, \ldots, T_\ell$ such that

$$\mathbf{V}(F) = \cup_{i=1}^{\ell} \mathbf{W}(T_i).$$

• incremental elimination: the algorithm eliminates one polynomial after another.

• All zeros *generic or not* are explicitly in the decomposition.

• $\mathbf{W}(T_i)$ and $\mathbf{W}(T_j)$ are not comparable but intermediate redundant components occur.

• Lazard's regular chains may be expensive to compute.

[Lazard, 1991] [Moreno Maza, 1997].

Related approaches: [Gómez-Díaz, 1994], [Wang, 1998], [Dellière, 1999].

Our Algorithm

- Given $F \subseteq \mathbf{k}[x_1, \ldots, x_n]$ computes regular chains $T_1, \ldots, T_\ell$ such that

$$\mathbf{V}(F) = \cup_{i=1}^{\ell} \mathbf{W}(T_i).$$

- elimination in order of decreasing dimension. Hence redundant components can be removed as soon as possible.

- Each T_i can be replaced by Lazard's regular chains.

- We have efficient criteria to compare $\mathbf{W}(T_i)$ and $\mathbf{W}(T_j)$. If there is a doubt we can convert to Lazard's regular chains.

- We can restrict our algorithm to compute Kalkbrener's decompositions.

Delayed Splits

- $F, F_1, \ldots, F_d, T, T_1, \ldots, T_d \subseteq \mathbf{k}[x_1, \ldots, x_n]$. T, T_i regular chains.
We put $\mathbf{Z}(F,T) := \mathbf{V}(F) \cap \mathbf{W}(T)$ and define
$\mathbf{Z}(F,T) \longrightarrow_D (\mathbf{Z}(F_1,T_1), \ldots, \mathbf{Z}(F_d,T_d))$ if we have:

(D_1) $\mathbf{Z}(F_i,T_i) \prec \mathbf{Z}(F,T)$,

(D_2) $\mathbf{Z}(F,T) \subseteq \mathbf{Z}(F_1,T_1) \cup \cdots \cup \mathbf{Z}(F_d,T_d)$,

(D_3) $\mathbf{Sat}(T) \subseteq \mathbf{Sat}(T_i)$,

(D_4) $F_i \neq \emptyset \implies F \subseteq F_i$,

(D_5) $F_i = \emptyset \implies \mathbf{W}(T_i) \subseteq \mathbf{V}(F)$.

This implies:

$$\mathbf{V}(F) \cap \mathbf{W}(T) \subseteq \mathbf{Z}(F_1,T_1) \cup \cdots \cup \mathbf{Z}(F_d,T_d) \subseteq \mathbf{V}(F) \cap \overline{\mathbf{W}(T)}.$$

- $\mathbf{W}(T \cup t) \longrightarrow_D (\mathbf{W}(T \cup a), \mathbf{W}(T \cup b), \mathbf{Z}(h_a, T \cup t))$.

Decomposing by means of Delayed Splits

- For $p \notin \mathbf{Sat}(T)$ $\mathsf{decompose}(p, T) = ([F_1, T_1], \ldots, [F_d, T_d])$ such that

(i) $\mathbf{Z}(p, T) \longrightarrow_D \; ([F_1, T_1], \ldots, [F_d, T_d])$,

(ii) $\mathsf{dim}(T_i) < \mathsf{dim}(T) \implies F_i \neq \emptyset$.

$\mathsf{solve}(F \subseteq \mathbf{k}[x_1, \ldots, x_n])$: L-split of $\mathbf{V}(F)$ by regular chains ==
  $Tasks := [[F, \emptyset]]$
  while $Tasks \neq [\,]$ **repeat**
    choose and remove a process $[F_1, T_1]$ from $Tasks$
    $F_1 = \emptyset \implies$ **output** T_1
    choose and remove a polynomial p Ritt-minimal in F_1
    $p \in \mathbf{Sat}(T_1) \implies Tasks := \mathsf{cons}\ ([F_1, T_1], Tasks)$
    for $[G, U] \in \mathsf{decompose}(p, T_1)$ **repeat**
      $Tasks := \mathsf{cons}\ ([F_1 \cup H, U], Tasks)$

Lifting Delayed Splits

- If $p \in \mathbf{k}[x_1, \ldots, x_i]$, computing a delayed split of $\mathbf{Z}(p, T)$ will require projecting $\mathbf{W}(T)$ in $\mathbf{k}[x_1, \ldots, x_i]$ and then a way to lift.
  - Does not happen in Kalkbrener's algorithm.
  - Happens in Lazard's algorithm but the difficulty is overcome by the strong properties of Lazard's regular chains.

Proposition 1 *Let $1 \leq i \leq n$. Let $F \subseteq \mathbf{k}[x_1, \ldots, x_i]$. Let $C \cup D$ be a regular chain such that $C \subseteq \mathbf{k}[x_1, \ldots, x_i]$ and $D \cap \mathbf{k}[x_1, \ldots, x_i] = \emptyset$.*

$$
\begin{array}{ccc}
\boxed{\mathbf{Z}(F, C \cup D)} & \longrightarrow_D & \boxed{(\mathbf{Z}(F_i, C_{i,j}))} \\
\mathbf{Z}(F, C) & & \uparrow \\
\downarrow D & & h_C \text{ regular modulo } C_{i,j} \\
(\mathbf{Z}(F_i, C_i)) & \mathbf{W}(C_i \cup D) \longrightarrow_D & (\mathbf{W}(C_{i,j}))
\end{array}
$$

Lifting Triangular Sets

- Assume $\mathsf{regular?}(p, T) = (T_1, \ldots, T_d)$ such that

(i) $\mathbf{W}(T) \longrightarrow_D (\mathbf{W}(T_1), \ldots, \mathbf{W}(T_d))$,

(ii) $p \notin \mathbf{Sat}(T_i) \implies p$ regular modulo T_i.

- $T \subseteq \mathbf{k}[x_1, \ldots, x_i]$ regular chain. p polynomial with $\mathsf{mvar}(p) = x_{i+1}$.

Then $\mathsf{extend}(T, p)$ returns regular chains $T_1, \ldots, T_d$ such that $\mathbf{W}(T \cup p) \longrightarrow_D (\mathbf{W}(T_1), \ldots, \mathbf{W}(T_d))$.

$\mathsf{extend}(T, p) ==$
  for $T_i \in \mathsf{regular?}(h_p, T)$ **repeat**
    $h_p \in \mathbf{Sat}(T_i) \implies$ **iterate**
    $\mathsf{dim}(T_i) = \mathsf{dim}(T) \implies$ **output** $T_i \cup p$
    for $T_{i,j} \in \mathsf{regular?}(h_T\, h_p, T_i)$ **repeat**
      $h_T\, h_p \notin \mathbf{Sat}(T_{i,j}) \implies$ **output** $T_{i,j} \cup p$

Gcd Modulo Regular Chains

- $T \subseteq \mathbf{k}[x_1, \ldots, x_i]$. t, p, g polynomials with main variable x_{i+1}.
Assume (i) $T \cup t$ regular chain, (ii) h_p regular modulo $\mathbf{Sat}(T)$.
Then g is regular gcd of t and p modulo T if

(G_1) $\mathsf{lc}(g, x_{i+1})$ is regular modulo T,

(G_2) $\exists\, u, v \in \mathbf{k}[x_1, \ldots, x_{i+1}]$ such that $ut + vp - g \in \mathbf{Sat}(T)$,

(G_3) if $\mathsf{mvar}(g) = x_{i+1}$ then $t, p \in \mathbf{Sat}(T \cup g)$.

Proposition 2 *If* $\mathsf{mvar}(g) = x_{i+1}$ *then*

$$\mathbf{Z}(p, T \cup t) \longrightarrow_D (\mathbf{W}(T \cup g), \mathbf{Z}(\{h_g, p\}, T \cup t)).$$

With a weaker condition than (G_2) as in [Moreno Maza, 1997], there's one term more: $\mathbf{Z}(p, T \cup \mathsf{pquo}(t, g))$.

- Assume $\mathsf{regularGcd}(t, p, T) = ([g_1, T_1], \ldots, [g_d, T_d])$ such that

(i) $\mathbf{W}(T) \longrightarrow_D (\mathbf{W}(T_1), \ldots, \mathbf{W}(T_d))$,

(ii) $\mathsf{dim}(T_i) = \mathsf{dim}(T) \Longrightarrow g_i$ is regular gcd of t and p modulo T_i.

$$\boxed{\begin{array}{l}
\mathsf{decompose}(p, T \cup t) == \\
\quad \textbf{for } [g_i, T_i] \in \mathsf{regularGcd}(t, p, T) \textbf{ repeat} \\
\quad\quad \mathsf{dim}(T_i) < \mathsf{dim}(T) \Longrightarrow \\
\quad\quad\quad \textbf{for } T_{i,j} \in \mathsf{extend}(T_i, h_T t) \textbf{ output } [p, T_{i,j}] \\
\quad\quad g_i \in \mathbf{k} \Longrightarrow \textbf{iterate} \\
\quad\quad \mathsf{mvar}(g_i) < x_{i+1} \Longrightarrow \textbf{output } [\{g_i, p\}, T_i \cup t] \\
\quad\quad \mathsf{mdeg}(g_i) = \mathsf{mdeg}(t) \Longrightarrow \textbf{output } [\emptyset, T_i \cup t] \\
\quad\quad \textbf{output } [\emptyset, T_i \cup g_i] \\
\quad\quad \textbf{output } [\{h_g, p\}, T_i \cup t]
\end{array}}$$

Remarks

- For every $[F_i, T_i] \in \mathsf{decompose}(p, T)$ such that $\mathsf{dim}(T_i) < \mathsf{dim}(T)$ we have $F_i \neq \emptyset$.
- Moreover if $F_i \neq \emptyset$ and $\mathsf{dim}(T_i) = \mathsf{dim}(T)$ then $\mathsf{dim}(\mathbf{Z}(F_i, T_i)) < \mathsf{dim}(T)$.
- Hence solve can generate the output regular chains in order of decreasing dimension and remove the redundant ones asap.
- It is very unlucky that regular?(p, T) generates T_i such that $\mathsf{dim}(T_i) < \mathsf{dim}(T)$.

Experimental Results

• Although we compute all zeros generic or not, timings are comparable with those of Kalkbrener's algorithm.

• We obtain much better timings than our implementation of Lazard's algorithm, especially in positive dimension.

• On most non trivial examples, many tasks (typically 100) could be run in parallel.

[Aubry and Moreno Maza, 1999] [AXIOM2.2]

• Today very few examples solvable in the $\longrightarrow_K$ sense remain unsolvable in the $\longrightarrow_L$ sense.

[Aldor]

Conclusions

- Significant improvements in the management of the redundant components during triangular decompositions.
- Our algorithm is naturally parallel.
- We have preserved the incremental philosophy of Lazard's algorithm while reaching the practical efficiency of Kalkbrener's algorithm.
- We provide routines to move from decompositions into general regular chains to decompositions into Lazard's regular chains.
- The gap between $\longrightarrow_K$ solving and $\longrightarrow_L$ solving has been greately reduced.

Rappelons que $\mathbf{V}(F)$ est singulière en M si l'espace tangent à $\mathbf{V}(F)$ en M n'est pas de dimension maximal.

Tout système F de polynômes peut se décomposer forme

(1) $\mathbf{V}(F) = \mathbf{W}(T_1) \cup \cdots \cup \mathbf{W}(T_d)$,

(2) où chaque point singulier de $\mathbf{V}(T_i)$ n'appartient pas à $\mathbf{W}(T_i)$ et est en fait *chassé* dans un $\mathbf{W}(T_j)$ tel que $\mathsf{dim}(T_j) < \mathsf{dim}(T_i)$.

Ceci est rendu possible :

- grâce à une propriété de ensembles triangulaires,
- et par l'algorithme incrémental décrit plus loin.

Pour $F = \{x_3^2 - x_2^2\, x_1\}$, le parapluie de Withney, on a :

$$\mathbf{V}(F) = \mathbf{W}(x_1\, x_2\, (x_3^2 - x_2^2\, x_1)) \cup \mathbf{W}(\{x_2, x_3\}) \cup \mathbf{W}(\{x_1, x_3\}).$$

On veut tester si $\mathbf{W}(T_1)$ admet des points à coordonnées toutes réelles. Supposons que T_1 compte m polynômes de $\mathbf{k}[x_1, \ldots, x_n]$. Donc $m \leq n$ et l'espace tangent en un point $M \in \mathbf{W}(T_1)$ est de dimension $n - m$.

(1) On se donne un point $A \notin \mathbf{W}(T_1)$ au hasard.

(2) On cherche l'ensemble E_A des points $M \in \mathbf{W}(T_1)$ à distance minimale de A. En effet $\mathbf{W}(T_1) \cap \mathbb{R}^n \neq \emptyset \Longrightarrow E_A \cap \mathbb{R}^n \neq \emptyset$.

(3) Si E_A n'est pas fini alors retourner en (1). En effet les points A *malchanceux* forment un ensemble de mesure nulle.