On recent advances on regular chains.

Marc Moreno Maza

LIFL, University of Lille 1

Characteristic sets, triangular sets and regular chains

- Characteristic sets
  - (i) of prime ideals [Ritt, 1932]
  - (ii) (or representations) of differential ideals [Boulier, Lazard, Ollivier & Petitot, 1995-1997], [Morrison, 1999], [Hubert, 2000]
  - (iii) of finite polynomial sets [Wu, 1987] [Chou & Gao, 1990] [Gallo & Mishra, 1990] [Wang, 1992]

- Triangular sets
  - (i) with #equations = #unknowns and *monic* polynomials [Lazard, 1992] [D5, 1985]
  - (ii) with *monic* and *square-free* polynomials [Lazard, 1991]

- Regular chains
  - introduced in [Kalkbrener, 1991] [Yang & Zhang, 1994]
  - compared with other notions in [Aubry, Lazard & Moreno Maza, 1999]
  - adapted to differential algebra [Boulier & Lemaire, 2000] [Lemaire, 2002]

The *as many polynomials as unknowns* case.

- In [Lazard, 1992] a subset

  $$T = \{T_1, \ldots T_n\} \subseteq \mathbf{k}[x_1 < \cdots < x_n]$$

  is a triangular set if for $i = 1 \cdots n$

  $$T_i = 1\,\mathbf{x_i^{d_i}} + a_{i-1}\,\mathbf{x_i^{d_i-1}} + \cdots + a_1\,\mathbf{x_i} + a_0$$

  with

  $$a_{i-1}, \ldots, a_1, a_0 \in \mathbf{k}[x_1, \ldots, x_{i-1}].$$

- Algorithmic properties. Let $p \in \mathbf{k}[x_1, \ldots, x_n]$ with $\deg(p, x_n) > 0$ and define $\mathcal{I} = (T)$.
  - One can decide whether $p \in \mathcal{I}$. Indeed T is a Gr. basis of $\mathcal{I}$ w.r.t. $x_1 < \cdots < x_n$.
  - One can decide whether $p^{-1} \mod \mathcal{I}$ exists. Indeed, . . .

(1) For $n = 1$ by computing $\gcd(p, T_1)$. This may split T_1 into 2 factors.

(2.1) For $n = 2$ one can try to compute $\gcd(p, T_2)$ modulo T_1 (by running the Eucl. algo as if $\mathbf{k}[x_1]/(T_1)$ was a field).

(2.2) Then, for $n = 2$ one can search for $p^{-1} \mod \mathcal{I}$ (by trying to compute $\gcd(p, T_2)$).

If p is not invertible mod. $\mathcal{I}$ then triang. sets T', T'' appear s.t. $\sqrt{\mathcal{I}} = \sqrt{\mathcal{I}'} \cap \sqrt{\mathcal{I}''}$.

- For $p_1, p_2 \in \mathbf{k}[x_1, \ldots, x_n][y]$ one can compute $g_1, \ldots, g_s \in \mathbf{k}[x_1, \ldots, x_n][y]$ and triangular sets $T_1, \ldots, T_s \subseteq \mathbf{k}[x_1, \ldots, x_n]$ s.t.

(1) a Bézout relation $\cdots p_1 + \cdots p_2 = g_i$ holds modulo T_i.

(2) g_i is *monic* ($\mathrm{lc}(g_i, y)$ is inv. mod $\mathcal{I}_i$).

(3) $\sqrt{\mathcal{I}} = \cap_i \sqrt{\mathcal{I}_i}$.

- Generalisation to non-monic T_i's

(2) For $n = 2$

$$T = \begin{cases} \mathbf{x_1^{d_1}} + \cdots + a_1\,\mathbf{x_1} + a_0 \\ h_2\,\mathbf{x_2^{d_2}} + \cdots + b_1\,\mathbf{x_2} + b_0 \end{cases}$$

is a triangular set if h_2^{-1} exists modulo T_1. Then the previous properties remain valid by changing $\mathcal{I}$ to $(T) : {h_2}^{\infty}$.

(3) For $n = 3$

$$T = \begin{cases} \mathbf{x_1^{d_1}} + \cdots + a_1\,\mathbf{x_1} + a_0 \\ h_2\,\mathbf{x_2^{d_2}} + \cdots + b_1\,\mathbf{x_2} + b_0 \\ h_3\,\mathbf{x_3^{d_3}} + \cdots + c_1\,\mathbf{x_3} + c_0 \end{cases}$$

is a triangular set if h_2^{-1} exists modulo T_1 and h_3^{-1} exists modulo $(\{T_1, T_2\}) : {h_2}^{\infty}$. Here $\mathcal{I}$ changes to $(T) : (h_2\,h_3)^{\infty}$.

(n) $\mathcal{I}$ changes to $\mathbf{Sat}(T) = (T) : (h_2 \cdots, h_n)^{\infty}$.

Regular chains

- The subset $T \subseteq \mathbf{k}[x_1 < \cdots < x_n]$ is a regular chain if
  - either $T = \emptyset$
  - or $T = T' \cup \{t\}$ where T' is a regular chain and
    - $t = h_t \, \mathbf{x_i^{d_i}} + a_{i-1} \, \mathbf{x_i^{d_i-1}} + \cdots + a_1 \, \mathbf{x_i} + a_0$
    - $T', \{h_t \, a_{i-1}, \ldots, a_1, a_0\} \subseteq \mathbf{k}[x_1, \ldots, x_{i-1}]$.
    - h_t is regular modulo **Sat**(T').
- Notations
  - Let h be the product of the initials of T and s be the product of the separants of T.

- ◦ Let $X = \{x_1, \ldots, x_n\}$, A the set of the $x \in X$ s.t. x is the greatest variable of some $t \in T$. Define $B = X \setminus A$.

- Reduction to dimension zero.

  - ◦ For every prime $\mathcal{P}$ associated with **Sat**(T) dim$(\mathcal{P}) = n - m$ and $\mathcal{P} \cap \mathbf{k}[B] = \{0\}$.

  $\Rightarrow$ Every non-zero $p \in \mathbf{k}[B]$ is regular modulo **Sat**(T).

  $\Rightarrow$ T can be viewed as a triangular set in $\mathbf{k}(B)[A]$.

  - ◦ For every prime $\mathcal{P}$ associated with $\mathcal{J} = (T) : s^\infty$ we have

    dim$(\mathcal{P}) = n - m$ and $\mathcal{P} \cap \mathbf{k}[B] = \{0\}$.

    Moreover $\mathcal{J}$ is radical (Lazard's Lemma).

Characteristic sets

- Notations. Let $F \subseteq \mathbf{k}[x_1 < \cdots < x_n]$ s.t. $F \cap \mathbf{k} \subseteq \{0\}$. Let $C \subseteq F$ s.t.
  - two different polynomials in C have different greatest variables,
  - C is (algebraically) auto-reduced.
- Definition The subset C is a characteristic set of F if every $f \in F$ reduced w.r.t. C is zero.
- Properties. If C char. set of an ideal $\mathcal{I}$ then for all $p \in \mathcal{I}$ we have $\text{prem}(p, C) = 0$. Moreover,

$$\mathbf{Sat}(C) = \{p \mid \text{prem}(p, C) = 0\}$$
$$\Updownarrow$$
$$C \quad \text{regular chain}$$
$$\Updownarrow$$
$$C \quad \text{characteristic set of } \mathbf{Sat}(C)$$

Regular differential chains

- Notations. Let $R = \mathbf{k}\{U\}$ a ring of differential polynomials. Let $C \subseteq R$ such that
  - two different polynomials in C have different greatest leaders (variables),
  - C is (differentially) auto-reduced and coherent.

- Definition. The subset C is a regular differential chain if C is a regular chain such that **Sat**(C) is radical.

- Properties.

$$[C] : (h\,s)^\infty = \{p \mid \text{full-rem}(p, C) = 0\}$$
$$\Updownarrow$$
$$C \quad \text{regular differential chain}$$
$$\Updownarrow$$
$$C \quad \text{characteristic set of } [C] : (h\,s)^\infty$$

Canonicity of regular chains

- Let $T \subseteq \mathbf{k}[X]$ be a regular chain with $A \subseteq X$ as the set of the leading variables of T. Define $B = X \setminus A$.

- Canonicity. Assume that
  - T is auto-reduced,
  - for every $t \in T$ we have $h_t \in \mathbf{k}[B]$,
  - every $t \in T$ is primitive as a polynomial in $(\mathbf{k}[B])[A]$.

  Then T depends only on **Sat**(T) and the ordering on the variables.

- Among the T such that $\mathcal{P} = \mathbf{Sat}(T)$ which one is the one ?

$$\mathcal{P} = \begin{cases} x^{31} - x^6 - x - y \\ x^8 - z \\ x^{10} - t \end{cases} \qquad \text{with } x > y > z > t.$$

$$(T_1) = \begin{cases} \left(t^4 - t\right) x - ty - z^2 \\ tzy^2 + 2z^3 y - t^8 + 2t^5 + t^3 - t^2 \\ z^5 - t^4 \end{cases}$$

$$(T_2) = \begin{cases} \left(t^4 - t\right) x - ty - z^2 \\ t^3 y^2 + 2t^2 z^2 y + \left(-t^6 + 2t^3 + t - 1\right) z^4 \\ z^5 - t^4 \end{cases}$$

- Push the *non-algebraic* variables down, normalize the initials and clear.

Regular chains and prime ideals

- Every prime ideal $\mathcal{P}$ in a polynomial ring $\mathbf{k}[x_1, \ldots, x_n]$ may be given by a regular chain.

$$\mathcal{P} = \begin{cases} ax + by - c \\ dx + ey - f \\ gx + hy - i \end{cases}$$

$$\Updownarrow$$

$$T = \begin{cases} gx + hy - i \\ (hd - eg)\, y - id + fg \\ (ie - fh)\, a + (ch - ib)\, d + (fb - ce)\, g \end{cases}$$

- The relation between both is $\mathcal{P} = \mathbf{Sat}(T)$.

- The lex. basis is

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

- The common zeros of every polynomial system can be decomposed into finitely many triangular sets

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

where $\mathbf{W}(T)$ denotes the zeros of T that do not cancel its initials. Note that we have $\overline{\mathbf{W}(T)} = \mathbf{V}(\mathbf{Sat}(T))$.

- For $F \subseteq \mathbf{k}[X]$ one can compute decompositions of the form

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

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

Ranking conversions

• For $\mathcal{R} = x > y > z > s > t$ and $\overline{\mathcal{R}} = t > s > z > y > x$ we have:

$$\text{palgie}(\left\{\begin{array}{l} x - t^3 \\ y - s^2 - 1 \\ z - s\,t \end{array}\right., \mathcal{R}, \overline{\mathcal{R}})$$

$$=$$

$$\left\{\begin{array}{l} s\,t - z \\ (x\,y + x)s - z^3 \\ z^6 - x^2y^3 - 3x^2y^2 - 3x^2y - x^2 \end{array}\right.$$

• For $\mathcal{R} = \cdots > v_{xx} > v_{xy} > \cdots > u_{xy} > u_{yy} > v_x > v_y > u_x > u_y > v > u$ and $\overline{\mathcal{R}} = \cdots u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v$ we have:

$$\text{pardi}(\left\{\begin{array}{l} v_{xx} - u_x \\ 4\,u\,v_y - (u_x\,u_y + u_x\,u_y\,u) \\ u_x^2 - 4\,u \\ u_y^2 - 2\,u \end{array}\right. \mathcal{R}, \overline{\mathcal{R}})$$

$$=$$

$$\left\{\begin{array}{l} u - v_{yy}^2 \\ v_{xx} - 2\,v_{yy} \\ v_y\,v_{xy} - v_{yy}^3 + v_{yy} \\ v_{yy}^4 - 2\,v_{yy}^2 - 2\,v_y^2 + 1 \end{array}\right.$$

PARDI, PODI, PALGIE

Input: In $\mathbf{k}[X]$

- two rankings $\mathcal{R}, \overline{\mathcal{R}}$ over X,
- a $\mathcal{R}$-triangular C set such that $\mathbf{Sat}(C)$ is prime.

Output: a $\overline{\mathcal{R}}$-triangular set $\overline{C}$ such that de $\mathbf{Sat}(C) = \mathbf{Sat}(\overline{C})$.

PALGIE: *Prime ALGebraic IdEal* implemented in Aldor, C and Maple,

PODI: *Prime Ordinary Differential Ideal*, implemented in C,

PARDI: *Prime pARtial Differential Ideal*, implemented in Maple.

□

Si tu veux arriver à temps, ménage ta monture

- The main difficulty while computing triangular decompositions is the generation of superfluous components.

- If we could generate components by decreasing order of dimension we could remove superfluous components as soon as they appear by inclusion test.

- However while we are building a large component we may have to consider special cases and then build small components.

- Hence we need to be able to delay some parts of each computation (gcd, regularity-test, enlarging a triangular set).

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 triangular sets.
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:

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

Decomposing by means of Delayed Splits

• For $p \notin \textbf{Sat}(T)$ decompose$(p, T) = ([F_1, T_1], \ldots, [F_d, T$
such that

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

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

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