Calculs de Pgcd au-dessus des

Tours d'Extensions Simples et

Rsolution des Systmes

d'quations Algbriques

Marc Moreno Maza

quipe de Calcul Formel

Systmes d'quations Algbriques

- Trouver les x tels que

$$\left\{\begin{array}{ccc} x^6 - 2\,x^4 + 3\,x^3 + x^2 - 6\,x - 2 & = & 0 \\ x^5 - 2\,x^3 - 3\,x^2 + 6 & = & 0 \end{array}\right.$$

- Trouver les (x, y, z) tels que

$$\left\{\begin{array}{ccc} x^2 + y + z & = & 1 \\ x + y^2 + z & = & 1 \\ x + y + z^2 & = & 1 \end{array}\right.$$

- Trouver les $(c_2, s_2, c_1, s_1, b, a)$ tels que

$$\left\{\begin{array}{ccc} c_1 c_2 - s_1 s_2 + c_1 & = & a \\ s_1\ c_2 + c_1\ s_2 + s_1 & = & b \\ c_1^2 + s_1^2 & = & 1 \\ c_2^2 + s_2^2 & = & 1 \end{array}\right.$$

Qu'est-ce que resoudre ?

• Une solution de $\left\{\begin{array}{rcl} x^6-2\,x^4+3\,x^3+x^2-6\,x-2 & = & 0 \\ x^5-2\,x^3-3\,x^2+6 & = & 0 \end{array}\right.$ est :

$$S=\{x \ \mid\ x^2-2=0\}$$

• Une solution de $\left\{\begin{array}{rcl} x^2+y+z & = & 1 \\ x+y^2+z & = & 1 \\ x+y+z^2 & = & 1 \end{array}\right.$

avec $\boxed{z<y<x}$ est :

$$\left\{\begin{array}{rcl} z^6-4z^4+4z^3-z^2 & = & 0 \\ 2z^2y+z^4-z^2 & = & 0 \\ y^2-y-z^2+z & = & 0 \\ x+y+z^2-1 & = & 0 \end{array}\right.$$

Une autre solution est :

$$\left\{\begin{array}{rcl} z & = & 1 \\ y & = & 0 \\ x & = & 0 \end{array}\right. \text{ ou } \left\{\begin{array}{rcl} z & = & 0 \\ y & = & 1 \\ x & = & 0 \end{array}\right. \text{ ou } \left\{\begin{array}{rcl} z & = & 0 \\ y & = & 0 \\ x & = & 1 \end{array}\right. \text{ ou } \left\{\begin{array}{rcl} z^2+2z-1 & = & 0 \\ y & = & z \\ x & = & z \end{array}\right.$$

• Pour $\left\{\begin{array}{rcl} c_1c_2-s_1s_2+c_1 & = & a \\ s_1\ c_2+c_1\ s_2+s_1 & = & b \\ c_1^2+s_1^2 & = & 1 \\ c_2^2+s_2^2 & = & 1 \end{array}\right.$

avec $\boxed{\mathbf{c_2}>\mathbf{s_2}>\mathbf{c_1}>\mathbf{s_1}>b>a}$ on a :

$$\left\{\begin{array}{c} \left(4b^2+4a^2\right)\ \mathbf{s_1}^{\mathbf{2}}+\left(-4b^3-4a^2b\right)\mathbf{s_1}+b^4+2a^2b^2+a^4-4a^2\ =\ 0 \\ \left(4bs_1-2b^2\right)\ \mathbf{c_1}\ =\ 4as_1{}^2-2abs_1+ab^2+a^3-4a \\ 2a\ \mathbf{c_1}\ =\ -2bs_1+b^2+a^2 \\ \mathbf{c_1^2}\ =\ 1-s_1^2 \\ \mathbf{s_2}\ =\ bc_1-as_1 \\ 2\ \mathbf{c_2}\ =\ b^2+a^2-2 \end{array}\right.$$

Une autre solution est :

$$\left\{\begin{array}{c}
\left(4b^2+4a^2\right)\ \mathbf{s_1}^{\mathbf{2}} + \left(-4b^3-4a^2b\right)\mathbf{s_1} + b^4+2a^2b^2+a^4-4a^2 \ = \ 0 \\
2a\ \mathbf{c_1} \ = \ -2bs_1+b^2+a^2 \\
2a\ \mathbf{s_2} \ = \ -\left(2b^2-2a^2\right)s_1+b^3+a^2b \\
2\ \mathbf{c_2} \ = \ b^2+a^2-2 \\
(b^2+a^2)\neq 0 \\
a\neq 0
\end{array}\right.$$

$$\text{ou}\ \left\{\begin{array}{rcl}
2\mathbf{s_1} & = & b \\
4\mathbf{c_1}^{\mathbf{2}} & = & -b^2+4 \\
\mathbf{s_2} & = & bc_1 \\
2\mathbf{c_2} & = & b^2-2 \\
\mathbf{a} & = & 0
\end{array}\right. \quad \text{ou}\ \left\{\begin{array}{rcl}
\mathbf{c_1}^2 & = & -{s_1}^2+1 \\
\mathbf{s_2} & = & 0 \\
\mathbf{c_2} & = & -1 \\
\mathbf{b} & = & 0 \\
\mathbf{a} & = & 0
\end{array}\right.$$

Plan

1. Scinder pour rsoudre
   - Pgcd et produit de corps
   - Produit de corps et tours
   - Tours et pgcd
   - Algorithme modifi des sous-rsultants
2. Rsoudre avec des ensembles triangulaires
   - Dcompositions de Wu
   - Les chanes rgulires de Kalkbrener
   - Les ensembles de Lazard
   - Pgcd et dcomposition de Lazard
3. Comparaison exprimentale des mthodes
   - Pourquoi, comment et qui comparer ?
   - L'implantation
   - Deux applications
   - Conclusions

1.1 Pgcd et produit de corps

$\mathbf{A}$: anneau.

$\mathbf{reg}(\mathbf{A})$ ses lements rguliers.

$\mathbf{fr}(\mathbf{A}) = (\mathbf{reg}(\mathbf{A}))^{-1}\mathbf{A}$.

<u>**Dfinition**</u>

Pour $p_1, p_2, g \in \mathbf{A}[X]$, g est un **pgcd** de $p1, p_2$ si:

$$\langle p_1, p_2 \rangle_{\mathbf{fr}(\mathbf{A})[X]} = \langle g \rangle_{\mathbf{fr}(\mathbf{A})[X]}$$

<u>**Proposition**</u>

$$\left.\begin{array}{r} \mathbf{A} \cong \mathbf{A}_1 \times \cdots \times \mathbf{A}_n \\ (p)_i \text{ et } (q)_i \text{ ont un pgcd } \in \mathbf{A}_i[X] \end{array}\right\} \Rightarrow p, q \text{ ont un pgcd } \in \mathbf{A}[X]$$

$\rightsquigarrow$ Quand $\mathbf{A}$ est-il un tel produit ?

1.2 Produits de corps et tours

Proposition (Principe D5 reformul)

$$\begin{array}{c} \mathbf{A} \text{ prod corps} \\ p \in \mathbf{A}[X] \setminus \mathbf{A} \text{ unitaire} \\ \langle p, \frac{d\,p}{d\,X} \rangle = \langle 1 \rangle \end{array} \Rightarrow \left\{ \begin{array}{c} \langle p \rangle \text{ radical} \\ \\ \mathbf{fr}(\mathbf{A}[X]) \text{ et } \mathbf{A}[X]/\langle p \rangle \text{ prod corps} \end{array} \right.$$

Dfinition

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

$(\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_n)$ **tour d'extensions simples de** $\mathbf{k}$ si

$$\begin{array}{c} \mathbf{A}_i = \mathbf{fr}(\mathbf{A}_{i-1}[X_i]) \\ \text{ou} \\ \exists p_i \in \mathbf{A}_{i-1}[X_i] \left\{ \begin{array}{l} p_i \text{ unitaire} \\ \mathbf{A}_i = \mathbf{fr}(\ \mathbf{A}_{i-1}[X_i]/\langle p_i \rangle) \end{array} \right. \end{array}$$

Proposition

p_i sans carrs $\Rightarrow$ $\forall p, q \in \mathbf{A}_i[X_{i+1}]$ p, q ont un pgcd.

1.3 Tours et pgcd

Problme

$(\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_n)$ tour

$p, q \in \mathbf{A}_n[x_{n+1}]$

Comment calculer un pgcd de p et q ?

Avant

(1) algorithme des sous-rsultants dans $(\mathbf{k}[x_1, \ldots, x_n])[x_{n+1}]$

(2) proprit de spcialisation des sous-rsultants

$\Rightarrow$ coefficients (polynomiaux) trop gros

Maintenant [Moreno Maza, Rioboo 1994]

(1) algorithme MODIFI des sous-rsultants dans $\mathbf{A}_n[x_{n+1}]$

(2) NORMALISATION des coefficients dominants

$\Rightarrow$ nouveaux problmes accessibles

1.4 Algorithme modifi

NewSubResGcd(p_1,p_2,$\boxed{f\text{:}(\mathbf{reg(A)} \mapsto \mathbf{reg(A)})}$) ==

if deg(p_2) $>$ deg(p_1) **then** $(p_1,p_2) := (p_2,p_1)$

$\delta :=$ deg(p_1) - deg(p_2)

$\psi' :=$ -1 ; $\beta' := -1^{\delta+1}$

$\boxed{p_2 := f(\mathsf{lc}(p_2))^* p_2}$

$\alpha' :=$ lc(p_2)

while (deg(p_2) > 0) **repeat**

  $p_3 :=$ prem(p_1,p_2) exquo β'

  $\boxed{p_3 := f(\mathsf{lc}(p_3))^* p_3}$

  if $\delta > 0$ **then**

    $\psi' := (-\alpha')^\delta$ exquo ${\psi'}^{\delta-1}$

  $(p_1 \; , p_2) := (p_2 \; , p_3)$

  if (deg(p_2) > 0) **then**

    $\delta :=$ deg(p_1) - deg (p_2)

    $\beta' :=$ -$\alpha' \, {\psi'}^{\delta}$

    $\alpha' :=$ lc(p_2)

if $p_2 = 0$ **then return** p_1 **else return** p_2

1.4 Un exemple

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$: notre tour

$p = x^3 + \sqrt{2}x^2 + \sqrt{3}x + 1$

$q = 3x^2 + 2\sqrt{2}x + \sqrt{3}$

```
(26) ->internalSubResList(p,q,x+->1)$Pack1

  3    +-+ 2    +-+           2     +-+      +-+
[x  + \|2 x  + \|3 x + 1, 3x  + 2\|2 x + \|3 ,
    +-+           +-+ +-+            +-+       +-+     +-+
(6\|3  - 4)x - \|2 \|3  + 9, (- 18\|2  + 12)\|3  + 8\|2  + 21]

Time: 0.05 (IN) + 10.07 (EV) + 0.27 (OT) + 4.50 (GC) = 14.88 sec


(27) ->internalSubResList(p,q,x+->quasiRecip(x))$Pack1

  3    +-+ 2    +-+           2     +-+      +-+
[x  + \|2 x  + \|3 x + 1, 3x  + 2\|2 x + \|3 ,
            +-+       +-+     +-+
 46x + (- 2\|2  + 27)\|3  - 9\|2  + 18, 1090585871]

Time: 0.03 (IN) + 8.35 (EV) + 0.22 (OT) + 2.80 (GC) = 11.40 sec
```

2.1 Dcompositions de Wu

Notation

$p \in \mathbf{k}[x_1, \ldots, x_n]$ avec $x_1 < \cdots < x_n$

$$p = \mathsf{init}(p)\ \mathsf{mvar}(p)^{\mathsf{mdeg}(p)}\ +\ \mathsf{tail}(p)$$

Dfinition

$T = \{t_1, \ldots, t_s\} \subseteq \mathbf{k}[x_1, \ldots, x_n]$ *triangulaire* si

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

$(ii)\ \ i \neq j \implies \mathsf{mvar}(t_i) \neq \mathsf{mvar}(t_j)$

$h = \mathsf{init}(t_1) \times \cdots \times \mathsf{init}(t_s)$.

Zros rguliers de T :

$$\mathbf{W}(T) := \mathbf{V_K}(t_1, \ldots, t_s) \setminus \mathbf{V_K}(h)$$

Thorme + algorithme [Wu Wen-Tsün, 87]

$$\mathbf{V_K}(F) \;=\; \mathbf{W}(T_1) \cup \cdots \cup \mathbf{W}(T_\ell)$$

△ Cependant, on peut avoir :

- composantes vides i.e. $\mathbf{W}(T_i) = \emptyset$
- redondance i.e. $\bigcup_{j \neq i} \mathbf{W}(T_j) = \bigcup_j \mathbf{W}(T_j)$
- manque de canonicit

2.2 Chanes rgulires de Kalkbrener

Kalkbrener (1991) :

- notion de chane rgulire, ensemble triangulaire encodant les tours d'extensions simples,
- algorithme de dcomposition de $\sqrt{\langle p_1, \ldots, p_m \rangle}$.

Aubry, Lazard, Moreno Maza (1996-1997) :

- point de vue global et unificateur.

<u>Dfinition</u>

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

$$\overline{\mathbf{W}(T)} = \mathbf{V_K}(\mathsf{sat}(T))$$

<u>Thorme</u>

$$\begin{gathered} \text{T chane rgulire} \\ \Updownarrow \\ \mathsf{init}(t_i) \text{ inversible dans } \mathbf{A}_{i-1} \\ \Updownarrow \\ \langle \mathsf{sat}(T) \rangle = \{p \mid \mathsf{prem}(p, T) = 0\} \\ \Updownarrow \\ T \text{ ensemble caracteristique de Ritt de } \mathsf{sat}(T) \end{gathered}$$

$$\mathbf{V_K}(F) = \overline{\mathbf{W}(T_1)} \cup \cdots \cup \overline{\mathbf{W}(T_\ell)}$$

$\triangle$ redondances possibles, pas de composantes vides.

2.3 Ensembles de Lazard

Dfinition

$T = \{t_{d+1}, \ldots, t_n\} \subseteq \mathbf{k}[x_1, \ldots, x_d, \mathbf{x_{d+1}}, \ldots, \mathbf{x_n}]$

T normalis si :

$$
\begin{aligned}
t_{d+1} &= \mathbf{x_{d+1}^{e_{d+1}}} + \frac{p_{d+1}(x_1,\ldots,x_d,\mathbf{x_{d+1}})}{q_{d+1}(x_1,\ldots,x_d)} \\
t_{d+2} &= \mathbf{x_{d+2}^{e_{d+2}}} + \frac{p_{d+2}(x_1,\ldots,x_d,\mathbf{x_{d+1}},\mathbf{x_{d+1}})}{q_{d+1}(x_1,\ldots,x_d)} \\
&\ldots \\
t_n &= \mathbf{x_n^{e_n}} + \frac{p_{d+1}(x_1,\ldots,x_d,\mathbf{x_{d+1}},\ldots,\mathbf{x_n})}{q_{d+1}(x_1,\ldots,x_d)}
\end{aligned}
$$

T ensemble de Lazard si normalis et t_i est sans carrs dans $\mathbf{A}_{i-1}$

$\triangle$ si $d = 0$ alors $q_i \in \mathbf{k}$

Thorme + mthode [Lazard, 1991]

$$\mathbf{V_K}(F) \;=\; \mathbf{W}(T_1) \cup \cdots \cup \mathbf{W}(T_\ell)$$

Dcomposition sans redondances et canonique

$\mathbf{fr}(\ \mathbf{k}[x_1, \ldots, x_n]/\mathsf{sat}(T_i))$ produit de corps.

2.4 Dcompositions de Lazard

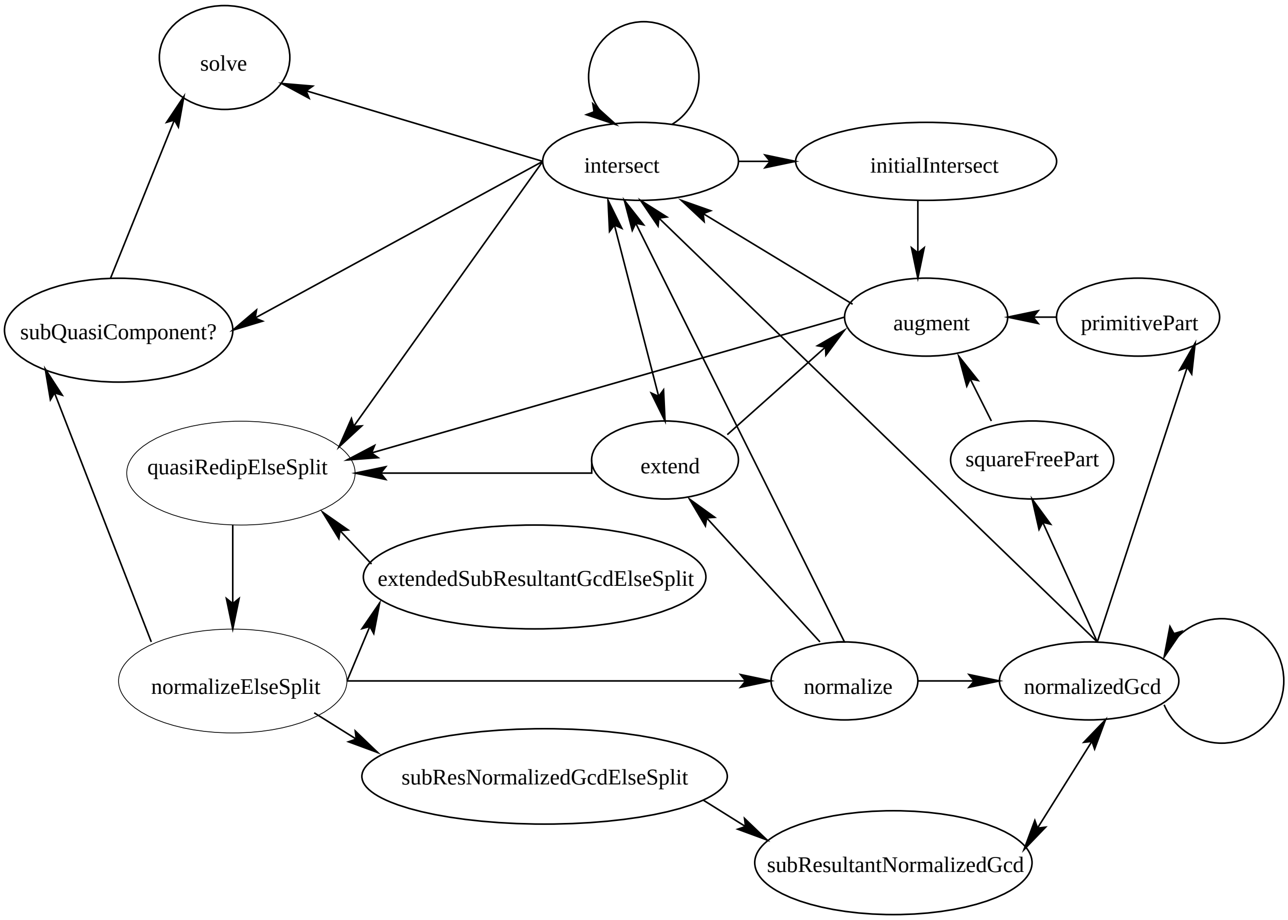
Principe incrmental

$p \in \mathbf{k}[x_1, \ldots, x_n]$

$T \subseteq \mathbf{k}[x_1, \ldots, x_n]$ ensemble de Lazard

$\mathsf{intersect}(p, T)$ retourne $\{S_1, \ldots, S_\ell\}$ tel que

$$\mathbf{V}(p) \cap \mathbf{W}(T) \ \subseteq\ \cup_1^\ell \mathbf{W}(S_i) \ \subseteq\ \overline{\mathbf{V}(p) \cap \mathbf{W}(T)}$$



Graphe des appels : ne boucle pas !

3.1 Pourquoi, comment et qui ?

Pourquoi ?

- coexistence d'algorithmes voisins,
- de complexit non connue,
- souvent illustrs uniquement par des temps de calcul.
- + unification des concepts

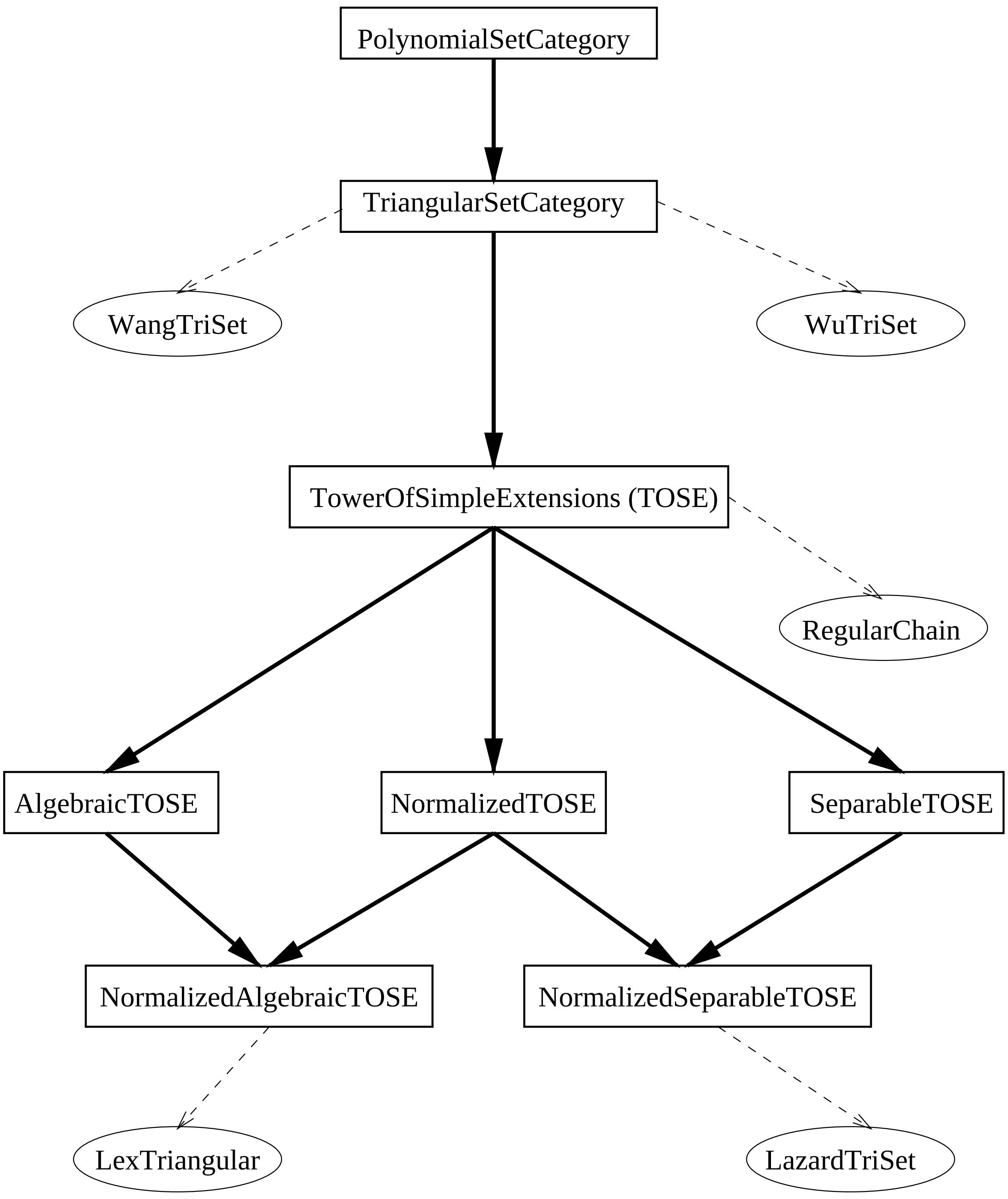
Comment ?

- un homme, une machine, un programme,
- vrification des calculs,
- dpouillement des rsultats.

Qui ?

- des mthodes fondes sur des principes communs,
- pouvant partager les mmes structures de donnes et routines de bas niveau,
- et ne se raccrochant pas une autre

3.2 Catgories et domaines AXIOM



3.3 Catgories et domaines AXIOM

PolynomialSetCategory

- exporte et implante des oprations sur les ensembles, les idaux, les varits, comme

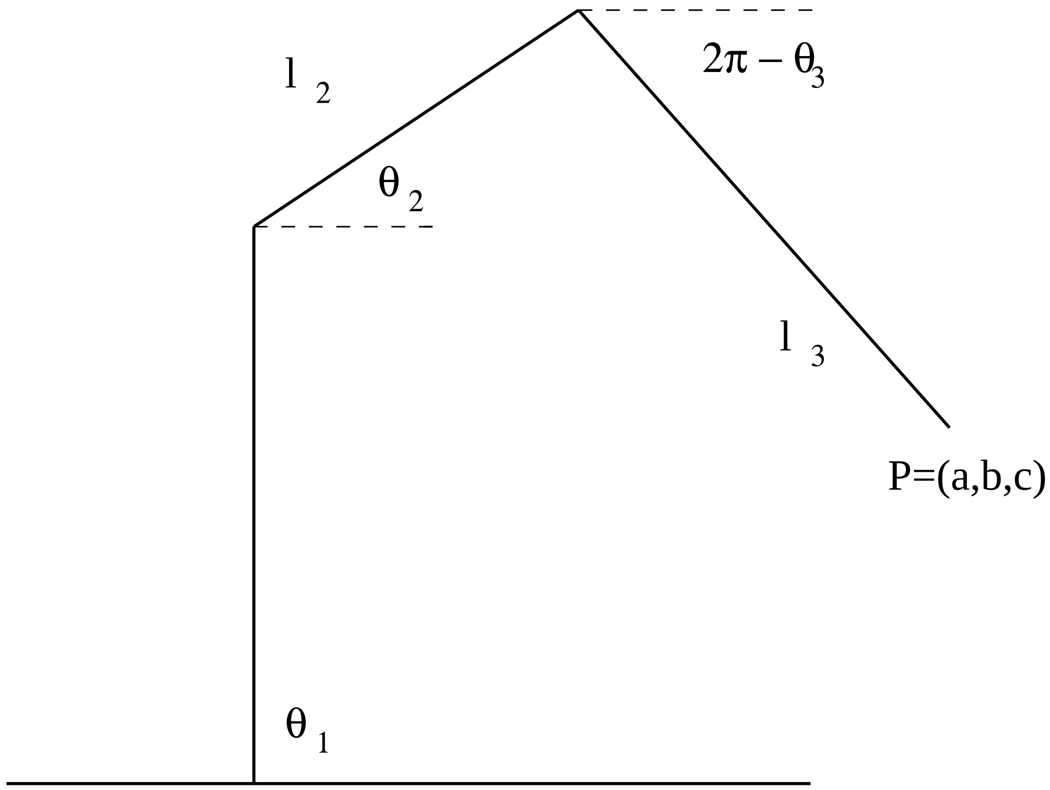
$$\begin{aligned} (I,J) &\longmapsto I \cap J \\ (I,p) &\longmapsto I : p^{\infty} \end{aligned}$$

- oprations fondes sur les bases de Gröbner et la connexion AXIOM $\leftrightarrow$ GB [Faugre, 94]

TriangularSetCategory

- exporte et implante des oprations de bas niveau comme $(p,T) \longmapsto \mathsf{prem}(p,T)$,
- exporte (sans implanter) des oprations sophistiques comme $F \longmapsto \mathsf{zeroSetSplit}(F) = \{T_1, \ldots, T_u\}$
- exporte et implante des oprations sophistiques comme $(F, \{T_1, \ldots, T_u\}) \longmapsto$ $\mathbf{equal?}(\mathbf{V}(F), \bigcup_{j=1}^{u} \overline{\mathbf{W}(T_j)})$

3.4 Le problme cinmatique inverse



$$\begin{cases} -d\ s_1 - a = 0 \\ d\ c_1 - b = 0 \\ l_2\ c_2 + l_3\ c_3 - d = 0 \\ l_2\ s_2 + l_3\ s_3 - c = 0 \\ {s_1}^2 + {c_1}^2 - 1 = 0 \\ {s_2}^2 + {c_2}^2 - 1 = 0 \\ {s_3}^2 + {c_3}^2 - 1 = 0 \end{cases}$$

avec $c_i = \cos(\theta_i)$ et $s_i = \sin(\theta_i)$

cinmatique inverse $\Rightarrow$

$\mathbf{s_1} > \mathbf{c_1} > \mathbf{s_2} > \mathbf{c_2} > \mathbf{s_3} > \mathbf{c_3} > l_2 > l_3 > a > b > c > d$

$$\left\{\begin{array}{rcl} a^2+b^2-d^2 &=& 0\\ \left(4\ c^2+4\ d^2\right)\ l_3^2\ \mathbf{c_3}^2+\cdots &=& 0\\ 2\ c\ l_3\ \mathbf{s_3}+\cdots &=& 0\\ l_2\ \mathbf{c_2}+\cdots &=& 0\\ 2\ c\ l_2\ \mathbf{s_2}+\cdots &=& 0\\ d\ \mathbf{c_1}-b &=& 0\\ d\ \mathbf{s_1}+a &=& 0 \end{array}\right.$$

$$\left\{\begin{array}{rcl} c^2+d^2 &=& 0\\ a^2+b^2-d^2 &=& 0\\ \left(4\ d\ l_3\ l_2^2-4\ d\ l_3^3\right)\ \mathbf{c_3}+\cdots &=& 0\\ \left(4\ d^2\ l_3\ l_2^2-4\ d^2\ l_3^3\right)\ \mathbf{s_3}+\cdots &=& 0\\ \left(4\ d\ l_2^3-4\ d\ l_3^2\ l_2\right)\ \mathbf{c_2}+\cdots &=& 0\\ \left(4\ d^2\ l_2^3-4\ d^2\ l_3^2\ l_2\right)\ \mathbf{s_2}+\cdots &=& 0\\ d\ \mathbf{c_1}-b &=& 0\\ d\ \mathbf{s_1}+a &=& 0 \end{array}\right.$$

$$\left\{\begin{array}{rcl} a^2+b^2-d^2 &=& 0\\ l_3^2-c^2-d^2 &=& 0\\ l_2 &=& 0\\ \left(c^2+d^2\right)\ \mathbf{c_3}-d\ l_3 &=& 0\\ \left(c^2+d^2\right)\ \mathbf{s_3}-c\ l_3 &=& 0\\ \mathbf{s_2}^2+\mathbf{c_2}^2-1 &=& 0\\ d\ \mathbf{c_1}-b &=& 0\\ d\ \mathbf{s_1}+a &=& 0 \end{array}\right.$$

$\ldots$

3.5 Conclusions de la comparaison

Wu	historiquement la premire, LENTE, SOUVENT CHEC SUR CAS FACILES DCOMPOSITIONS PEU LISIBLES composantes vides redondances
Wang	PARFOIS TRS RAPIDE, CHEC SUR CAS FACILES DCOMPOSITIONS PEU LISIBLES
Kalkbrener	GLOBALEMENT TRS RAPIDE PARFOIS LENT SUR CAS FACILES DCOMPOSITIONS LISIBLES pas de composantes vides redondances DCOMPOSITIONS PARESSEUSE NON UTILISABLES NUMRIQUEMENT
Lazard	GLOBALEMENT RAPIDE PARFOIS LENT SUR CAS FACILES OPTIMISATIONS CONNUES IMPLANTER DCOMPOSITIONS LISIBLES, CANONIQUES UTILISABLES NUMRIQUEMENT PAS DE REDONDANCES

Conclusions

- Aspect logiciel :
  - implantation de deux nouvelles mthodes
  - comparaison avec d'autres
- Aspect algorithmique :
  - pgcd sur tours algbriques
  - pgcd sur tours sprables
- Aspect algbrique :
  - nouvelles notions
  - unification de points de vue
- Merci tous ...