Introduction au Calcul formel

Algorithmes et complexité

Frédéric Chyzak

frederic.chyzak@inria.fr

http://www.enseignement.polytechnique.fr/profs/informatique/Frederic.Chyzak/

Idéaux

Définition. Un *idéal* I d'un anneau A est un sous-groupe de A stable par multiplication par tout élément de A.

Exemple. Étant donnée une famille $(g_u)_{u\in U}$ d'éléments de A, les combinaisons linéaires finies à coefficients dans A forment un idéal noté $\sum_{u\in U} Ag_u$.

Exemple. L'ensemble des polynômes de $\mathbb{C}[X_1,\ldots,X_n]$ qui s'annulent sur un ensemble donné V de points de $\mathbb{C}^n$:

$$I(V) = \left\{ p \in \mathbb{C}[X_1,\ldots,X_n] \;\middle|\; \forall x = (x_1,\ldots,x_n) \in V,\ p(x) = 0 \right\}.$$

Problème I : description d'un idéal

Un idéal $I \subset k[X_1, \ldots, X_n]$ peut-il être engendré par un nombre fini de générateurs ? Autrement dit, a-t-on toujours

$$I = \sum_{j=1}^{s} k[X_1, \ldots, X_n] p_j \ ?$$

Ce n'est pas évident pour un $I(V)$.

C'est faux pour $A = k[X_1, X_2, \ldots]$:

$$AX_1 \subsetneq AX_1 + AX_2 \subsetneq \cdots \subsetneq AX_1 + \cdots + AX_\ell \subsetneq \cdots$$

Problème II : appartenance à un idéal

Pour un idéal $I \subset A = k[X_1, \ldots, X_n]$ et un polynôme $p \in A$ donnés, déterminer (algorithmiquement) si $p \in I$.

Exemple. $X^3 - 1$ est-il combinaison linéaire (sur $\mathbb{Q}[X, Y, Z]$) de

$$X + Y + Z, \quad XY + YZ + ZX \quad \text{et} \quad XYZ - 1 \ ?$$

Géométriquement, ce problème est relié à la question de savoir si

$$V(I) \subset V(\{p\})$$

pour

$$V(S) = \left\{ x = (x_1, \ldots, x_n) \in k^n \;\middle|\; \forall p \in S,\ p(x) = 0 \right\}.$$

Problème III : résolution de systèmes polynomiaux

Donner toutes les solutions dans k^n d'un système d'équations polynomiales :

$$p_1(x_1, \ldots, x_n) = \cdots = p_s(x_1, \ldots, x_n) = 0.$$

Exemple. Lieu et valeurs des extrema de $(x, y, z) \mapsto x^3 + 2xyz - z^2$ sur la sphère unité $\{ (x, y, z) \mid x^2 + y^2 + z^2 = 1 \}$?

L'ensemble $V\left(\sum_{i=1}^{s} Ap_i\right)$ de ces solutions est noté $V(p_1, \ldots, p_s)$.

Problème annexe : $n = s = 1$, $p_1 = X^2 + 1$; dans $k = \mathbb{C}$, 2 solutions, dans $k = \mathbb{R}$, aucune solution.

Problème IV : équations implicites

Étant donnée une paramétrisation rationnelle

$$x_i = r_i(t_1, \ldots, t_m), \quad i = 1, \ldots, n,$$

d'un ensemble V de points de k^n, trouver un système d'équations polynomiales qui définisse la variété V.

Exemple (cercle)**.**

$$x = \frac{1 - t^2}{1 + t^2} \quad \text{et} \quad y = \frac{2t}{1 + t^2} \implies x^2 + y^2 = 1.$$

Bases de Gröbner, l'idée

Systèmes distingués de générateurs d'un idéal vérifiant une **propriété de divisibilité**.

Elles nous fournissent :

1. formes canoniques pour les idéaux :

$$\{p_i\} \to \{g_i\} \quad \text{tel que} \quad \sum_i Ap_i = \sum_i Ag_i \ ;$$

2. divisions avec unicité du reste : $p \to \sum_i a_i g_i + r$;

2'. formes canoniques dans l'anneau quotient : $A/\sum_i Ag_i$;

3. élimination polynomiale : $(A = B[X])$

$$\{p_i\} \to \{g_i\} \quad \text{tel que} \quad \sum_i Bg_i = \sum_i Ap_i \cap B.$$

Coefficients et monômes

$$p = \sum_{\text{finie}} p_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} = \sum_{j=1}^{s} c_j m_j \in k[X_1, \ldots, X_n]$$

Définition. $p_{i_1,\ldots,i_n}$ est le coefficient du monôme $X_1^{i_1} \ldots X_n^{i_n}$ dans p.

Les monômes constituent un monoïde commutatif M engendré par les X_i.

Monoïdes

Définition. Un *monoïde* M est un ensemble muni d'une loi interne associative pour laquelle il existe un élément neutre.

Exemple. $(\mathbb{N}^n, +, 0)$:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n).$$

Exemple. L'ensemble noté $[X_1, \ldots, X_n]$ des monômes en des indéterminées X_1, …, X_n, muni du produit usuel.

$$\left(X_1^{a_1} \ldots X_n^{a_n}\right) \times \left(X_1^{b_1} \ldots X_n^{b_n}\right) = X_1^{a_1+b_1} \ldots X_n^{a_n+b_n}.$$

C'est le monoïde commutatif libre sur n générateurs.

Ordre monomial

Un ordre monomial sur M est une relation d'ordre qui est :

- totale sur M : deux monômes peuvent toujours être comparés ;
- compatible avec le produit : $m_1 \prec m_2 \implies m'm_1 \prec m'm_2$;
- un bon ordre : tout ensemble non vide de monômes a un plus petit élément, ou de façon équivalente, toute suite strictement décroissante de monômes termine.

$1 = X_1^0 \dots X_n^0$ est le plus petit élément de M pour tout ordre monomial.

Notations

$$X^{\alpha} = X_1^{\alpha_1} \dots X_n^{\alpha_n}.$$

$$|\alpha| = \alpha_1 + \cdots + \alpha_n.$$

$$f(S) = \{\, f(s) \mid s \in S \,\}.$$

Ordre lexicographique (ordre du dictionnaire)

Définition. $X_1^{\alpha_1} \dots X_n^{\alpha_n} \prec_{\text{lex}} X_1^{\beta_1} \dots X_n^{\beta_n}$ si et seulement si $\alpha_k < \beta_k$ pour $k = \min\{\, i \mid \alpha_i \neq \beta_i \,\}$.

(La première valeur non nulle de la suite $\alpha_1 - \beta_1$, $\alpha_2 - \beta_2$, … est strictement négative.)

$$X_1 \succ X_2 \succ \cdots \succ X_n.$$

Exemple. Pour $n = 3$: $1 \prec X_3 \prec X_3^2 \prec X_3^3 \prec \cdots \prec X_2 \prec X_2X_3 \prec X_2X_3^2 \prec X_2X_3^3 \prec \cdots \prec X_2^2 \prec X_2^2X_3 \prec X_2^2X_3^2 \prec X_2^2X_3^3 \prec \cdots \prec X_1 \prec X_1X_3 \prec X_1X_3^2 \prec X_1X_3^3 \prec \cdots \prec X_1X_2 \prec X_1X_2X_3 \prec X_1X_2X_3^2 \prec X_1X_2X_3^3 \prec \cdots \prec X_1X_2^2 \prec X_1X_2^2X_3 \prec X_1X_2^2X_3^2 \prec X_1X_2^2X_3^3 \prec \cdots$

Ordre lexicographique gradué

Définition. $X^\alpha \prec_{\text{grlex}} X^\beta$ si et seulement si

$$|\alpha| < |\beta| \text{ ou } (|\alpha| = |\beta| \text{ et } X^\alpha \prec_{\text{lex}} X^\beta).$$

(Degré total raffiné par $\prec_{\text{lex}}$.)

$$X_1 \succ X_2 \succ \cdots \succ X_n.$$

Exemple. Pour $n = 3$: $1 \prec X_3 \prec X_2 \prec X_1 \prec X_3^2 \prec X_2X_3 \prec X_2^2 \prec X_1X_3 \prec X_1X_2 \prec X_1^2 \prec X_3^3 \prec X_2X_3^2 \prec X_2^2X_3 \prec X_2^3 \prec X_1X_3^2 \prec X_1X_2X_3 \prec X_1X_2^2 \prec X_1^2X_3 \prec X_1^2X_2 \prec X_1^3 \prec \cdots$

Ordre lexicographique renversé

Définition. $X_1^{\alpha_1} \dots X_n^{\alpha_n} \prec_{\text{revlex}} X_1^{\beta_1} \dots X_n^{\beta_n}$ si et seulement si $\alpha_k > \beta_k$ pour $k = \max\{\, i \mid \alpha_i \neq \beta_i \,\}$.

(La dernière valeur non nulle de la suite $\alpha_1 - \beta_1$, $\alpha_2 - \beta_2$, … est strictement positive.)

$$X_1 \succ X_2 \succ \cdots \succ X_n.$$

Exemple. Pour $n = 3$:

$\cdots \prec X_1^3X_2^2X_3 \prec X_1^2X_2^2X_3 \prec X_1X_2^2X_3 \prec X_2^2X_3 \prec \cdots \prec X_1^3X_2X_3 \prec X_1^2X_2X_3 \prec X_1X_2X_3 \prec X_2X_3 \prec \cdots \prec X_1^3X_3 \prec X_1^2X_3 \prec X_1X_3 \prec X_3 \prec \cdots \prec X_1^3X_2^2 \prec X_1^2X_2^2 \prec X_1X_2^2 \prec X_2^2 \prec \cdots \prec X_1^3X_2 \prec X_1^2X_2 \prec X_1X_2 \prec X_2 \prec \cdots \prec X_1^3 \prec X_1^2 \prec X_1 \prec 1.$

Ordre lexicographique renversé gradué

Définition. $X^\alpha \prec_{\text{grevlex}} X^\beta$ si et seulement si

$$|\alpha| < |\beta| \text{ ou } (|\alpha| = |\beta| \text{ et } X^\alpha \prec_{\text{revlex}} X^\beta).$$

(Degré total raffiné par $\prec_{\text{revlex}}$.)

$$X_1 \succ X_2 \succ \cdots \succ X_n.$$

Exemple. Pour $n = 3$: $1 \prec X_3 \prec X_2 \prec X_1 \prec X_3^2 \prec X_2X_3 \prec X_1X_3 \prec X_2^2 \prec X_1X_2 \prec X_1^2 \prec X_3^3 \prec X_2X_3^2 \prec X_1X_3^2 \prec X_2^2X_3 \prec X_1X_2X_3 \prec X_1^2X_3 \prec X_2^3 \prec X_1X_2^2 \prec X_1^2X_2 \prec X_1^3 \prec \cdots$

Remarques sur les ordres monomiaux

L'ordre $\prec_{\text{revlex}}$ n'est pas un ordre monomial.

Les ordres $\prec_{\text{lex}}$, $\prec_{\text{grlex}}$, $\prec_{\text{grevlex}}$ sont des ordres monomiaux.

Les ordres monomiaux $\prec_{\text{lex}}$ et $\prec_{\text{grevlex}}$ seront les plus employés, ainsi que d'autres ordres pondérés et d'élimination de bloc.

On utilisera la notation $\prec_{\text{lex}(X_{\sigma(1)},\ldots,X_{\sigma(n)})}$, etc, pour éviter de renommer les indéterminées. Ainsi, $\prec_{\text{lex}(X_1,\ldots,X_n)} = \prec_{\text{lex}}$, etc.

$X^\alpha \prec_{\text{revlex}(X_1,\ldots,X_n)} X^\beta \iff X^\alpha \succ_{\text{lex}(X_n,\ldots,X_1)} X^\beta$.

Exercice. Prouver les deux premiers et le dernier points.

Coefficients, monômes et termes de tête

Définition. On fixe un ordre monomial $\prec$ sur M. Le monôme de tête d'un polynôme p non nul est

$$\mathrm{mt}(p) := \max\{\, m \mid m \in M,\ \text{coeff. de } m \text{ dans } p \neq 0 \,\}.$$

Le coefficient de tête d'un polynôme p non nul est le coefficient $\mathrm{ct}(p)$ de son monôme de tête. Le terme de tête d'un polynôme p non nul est le produit $\mathrm{tt}(p) := \mathrm{ct}(p)\mathrm{mt}(p)$.

Exemple. $p = -30X_1X_2^2 - 210X_2^2X_3 + 3X_1^2 + 35X_2^2 + 30X_1X_3 - 105X_3^2 + 140X_2X_4 - 21X_5$.

Pour grevlex$(X_1, \ldots, X_5)$ et grlex$(X_1, \ldots, X_5)$: $-30X_1X_2^2$.

Pour lex$(X_1, \ldots, X_5)$: $3X_1^2$.

Pour lex$(X_5, \ldots, X_1)$: $-21X_5$.

Réduction

Un polynôme f non nul est réductible par un polynôme g non nul si et seulement si $\mathrm{mt}(g)$ divise $\mathrm{mt}(f)$.

Un polynôme f non nul est réductible par une famille $\{g_i\}_{i\in\{1,\ldots,s\}}$ de polynômes non nuls si et seulement si f est réductible par l'un des g_i.

En une unique indéterminée, f est réductible par g si et seulement si $\deg f \geq \deg g \geq 0$.

Division en plusieurs indéterminées

ENTRÉE : un polynôme f et des polynômes non nuls $g_1, \ldots, g_s$

SORTIE : des polynômes $r, q_1, \ldots, q_s$ tels que $f = q_1 g_1 + \cdots + q_s g_s + r$ et tel qu'aucun monôme de r ne soit réductible par $\{g_i\}$

1. $r \leftarrow 0$; pour i de 1 à s, faire $q_i \leftarrow 0$
2. tant que $f \neq 0$, faire
   - si $\mathrm{mt}(g_i)$ divise $\mathrm{mt}(f)$ pour un certain i, choisir un tel i et faire

     $$q_i \leftarrow q_i + \mathrm{tt}(g_i)^{-1}\mathrm{tt}(f) \quad \text{et} \quad f \leftarrow f - \mathrm{tt}(g_i)^{-1}\mathrm{tt}(f)g_i$$

   - sinon, faire $r \leftarrow r + \mathrm{tt}(f)$ et $f \leftarrow f - \mathrm{tt}(f)$
3. renvoyer $r, q_1, \ldots, q_s$

Non déterminisme de la division

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

$$\begin{aligned}
&(\underline{X^2Y} + XY^2 + Y^2) + 0 \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
&\quad = (\underline{XY^2} + X + Y^2) + X \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
&\quad = (\underline{Y^2} + Y) + (X + Y) \times (XY - 1) + 0 \times (Y^2 - 1) + X \\
&\quad = 0 + (X + Y) \times (XY - 1) + 1 \times (Y^2 - 1) + (X + Y + 1)
\end{aligned}$$

$$\begin{aligned}
&(\underline{X^2Y} + XY^2 + Y^2) + 0 \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
&\quad = (\underline{XY^2} + X + Y^2) + X \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
&\quad = \underline{Y^2} + X \times (XY - 1) + X \times (Y^2 - 1) + 2X \\
&\quad = 0 + X \times (XY - 1) + (X + 1) \times (Y^2 - 1) + (2X + 1)
\end{aligned}$$

Parties stables du monoïde des monômes

Partie stable S de M engendrée par une famille $\{s_i\}_{i\in I}$:

$$S = \{\, ms_i \in M \mid m \in M,\ i \in I \,\} = \bigcup_{i\in I} M s_i.$$

Stabilité par multiplication par tout élément du monoïde M.

Dessins en escaliers.

Bases de Gröbner, axiome fondamental de la théorie

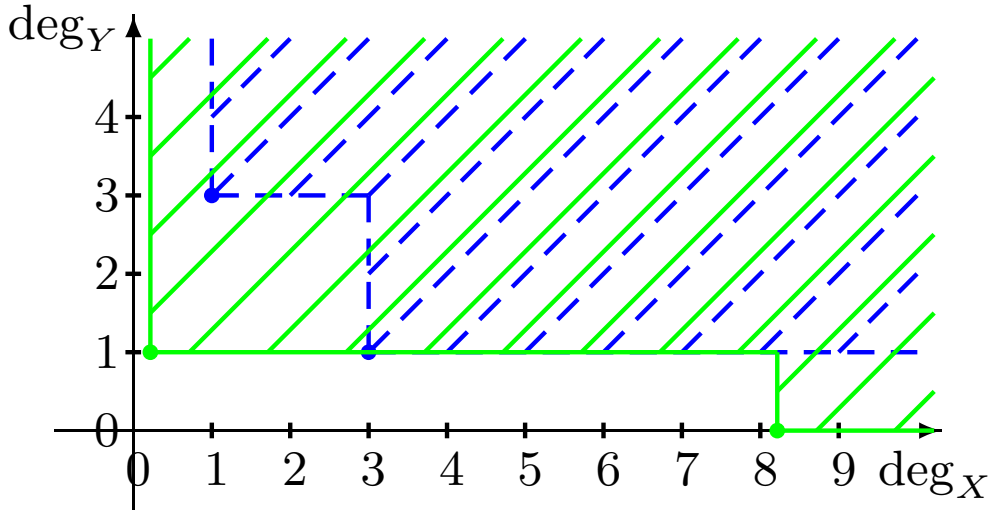
Le monôme de tête d'un produit est le produit des monômes de tête :

$$\mathrm{mt}(fg) = \mathrm{mt}(f)\mathrm{mt}(g).$$

Conséquence : $\mathrm{mt}(I) := \mathrm{mt}(I \setminus \{0\})$ est une partie stable.

Exercice. Démontrer cette propriété de $k[X_1, \ldots, X_n]$.

Bases de Gröbner, le problème



Étant donné

$$I = A(\underline{XY^3} - 1) + A(\underline{X^3Y} + 1),$$

on veut découvrir (pour l'ordre $\mathrm{lex}(Y, X)$)

$$\mathrm{mt}(I) = MY \cup MX^8,$$

$$I = A(\underline{Y} + X^5) + A(\underline{X^8} + 1).$$

Bases de Gröbner, la définition

Définition. Soit I un idéal de $A = \mathbb{C}[X_1, \ldots, X_n]$ et $\prec$ un ordre monomial. Un ensemble fini $G \subseteq I$ est une base de Gröbner de I pour l'ordre $\prec$ si l'une quelconque des propriétés équivalentes est vérifiée :

1. la partie stable de M engendrée par $\mathrm{mt}(G)$ est $\mathrm{mt}(I)$;
2. $\mathrm{mt}(G)$ et $\mathrm{mt}(I)$ engendrent le même idéal ;
3. tout $f \in I$ non nul est réductible par G ;
4. pour tout $f \in A$, il existe un unique $r \in A$ tel que $f - r \in I$ et dont aucun monôme n'est divisible par un monôme de $\mathrm{mt}(G)$;
5. pour tout $f \in I$, le reste de la division de f par G est nul.

Remarques sur la définition des bases de Gröbner

r est le reste de la division de f par G.

G est un système de générateurs de I dans A : $I = \sum_{g \in G} Ag$.

On peut toujours remplacer un élément d'une base de Gröbner par le reste de sa division par les autres éléments.

Exercice. Prouver le dernier point.

Lemme de Dickson

Toute partie stable S de $[X_1, \ldots, X_n]$ est finiment engendrée.

Preuve par récurrence sur n. (Dans le cas $S = \mathrm{mt}(I)$, les éléments minimaux pour $\prec$ constituent un système de générateurs fini.)

Existence des bases de Gröbner

Pour tout ordre monomial $\prec$, tout idéal I non nul admet une base de Gröbner (et donc un système fini de générateurs).

Preuve : considérer un système fini de générateurs de $\mathrm{mt}(I)$ et le relever en un système d'éléments de I, qui s'avère être une base de Gröbner de I pour $\prec$.

Solution I : description d'un idéal

Un idéal $I \subset k[X_1, \ldots, X_n]$ peut-il être engendré par un nombre fini de générateurs ? Autrement dit, a-t-on toujours

$$I = \sum_{j=1}^{s} k[X_1, \ldots, X_n] p_j \ ?$$

Oui, c'est le théorème de Hilbert.

Preuve : considérer une base de Gröbner pour un ordre monomial quelconque.

La réduction, une spécialisation de la division

ENTRÉE : un polynôme f et des polynômes non nuls $g_1, \ldots, g_s$

SORTIE : le polynôme r, reste de la division de f par $G = \{g_i\}$

1. $r \leftarrow 0$
2. tant que $f \neq 0$, faire
   - si $\mathrm{mt}(g_i)$ divise $\mathrm{mt}(f)$ pour un certain i, choisir un tel i et faire
   $$f \leftarrow f - \mathrm{tt}(g_i)^{-1}\mathrm{tt}(f)g_i$$
   - sinon, faire $r \leftarrow r + \mathrm{tt}(f)$ et $f \leftarrow f - \mathrm{tt}(f)$
3. renvoyer r

$\Rightarrow$ Procédure de mise sous forme canonique si G est base de Gröbner.

Solution II : appartenance à un idéal

Pour un idéal $I \subset A = k[X_1, \ldots, X_n]$ et un polynôme $f \in A$ donnés, déterminer (algorithmiquement) si $f \in I$.

ENTRÉE : un polynôme f et des polynômes non nuls $p_1, \ldots, p_s$ engendrant l'idéal I

SORTIE : une valeur booléenne indiquant si $f \in I$

1. choisir un ordre monomial $\prec$ sur $M = [X_1, \ldots, X_n]$
2. calculer une base de Gröbner $G = \{g_1, \ldots, g_s\}$ de I pour cet ordre
3. effectuer la réduction de f par G
4. si le reste est nul, répondre VRAI, sinon répondre FAUX

Exemple en *Magma*

Création d'un anneau de polynômes de rang 3 :

```
> Q:=RationalField();
> A<X,Y,Z>:=PolynomialRing(Q,3);
```

Un polynôme et un idéal de l'anneau :

```
> f:=X^3-1;
> I:=ideal<A|X+Y+Z,X*Y+Y*Z+Z*X,X*Y*Z-1>;
```

Calcul d'une première base de Gröbner, implicitement pour l'ordre $\prec_{\text{lex}}$:

```
> Basis(I);
[
    X + Y + Z,
    X*Y + X*Z + Y*Z,
    X*Y*Z - 1
]
> Groebner(I);
> Basis(I);
[
    X + Y + Z,
    Y^2 + Y*Z + Z^2,
    Z^3 - 1
]
```

```
> NormalForm(f,I);
0
> f in I;
true
> Coordinates(I,f);
[
    X^2 - X*Y - X*Z + Y^2 + 2*Y*Z + Z^2,
    -Y - 2*Z,
    1
]
```

```
> NormalForm(f+1,I);
1
> f+1 in I;
false
> Coordinates(I,f+1);

>> Coordinates(I,f+1);
               ^
Runtime error in 'Coordinates': Argument 2 is not
in argument 1
```

Élimination

L'intersection d'un idéal I de $A = \mathbb{C}[X_1, \ldots, X_n]$ avec la sous-algèbre $A_k = \mathbb{C}[X_{k+1}, \ldots, X_n]$ est un idéal de A_k.

Soit G une base de Gröbner de I pour l'ordre lexicographique.

L'idéal $I \cap A_k$ est engendré par $G \cap A_k$ dans A_k.
$G \cap A_k$ est une base de Gröbner de $I \cap A_k$.

Exercice. Prouver ces points.

Géométriquement, $V(I \cap A_k)$ est (une clôture de) l'image de $V(I)$ par la projection de $\mathbb{C}^n$ sur ses $n - k$ dernières composantes.

Solution III : résolution de systèmes polynomiaux

Donner toutes les solutions dans k^n d'un système d'équations polynomiales :

$$p_1(x_1, \ldots, x_n) = \cdots = p_s(x_1, \ldots, x_n) = 0.$$

Calculer une base de Gröbner pour l'ordre lexicographique fournit (sous de bonnes hypothèses) un système de forme triangulaire :

$$\begin{aligned} g_1(x_1, x_2, \ldots, x_n) &= 0, \\ g_2(x_2, \ldots, x_n) &= 0, \\ &\vdots \\ g_n(x_n) &= 0. \end{aligned}$$

Puis résoudre des polynômes en une seule indéterminée.

Remarques sur la résolution de systèmes

En réalité, on ne calcule pas forcément un unique polynôme en $X_k, \ldots, X_n$, mais plusieurs.

À chaque spécialisation d'une indéterminée par un zéro d'un polynôme, on peut vouloir recalculer une base de Gröbner.

Ce n'est donc pas un moyen économique pour résoudre.

Solution IV : équations implicites

Étant donnée une paramétrisation rationnelle

$$x_i = r_i(t_1, \ldots, t_m), \quad i = 1, \ldots, n,$$

d'un ensemble V de points de k^n, trouver un système d'équations polynomiales qui définisse la variété V.

Méthode = éliminer les T_i tout en évitant les pôles des r_i

Entrée : les fractions $r_i = p_i/q_i$, en les $T_1, \ldots, T_m$, pour $1 \leq i \leq n$

Sortie : système d'équations algébriques implicites décrivant V

1. choisir un ordre monomial $\prec$ sur $M = [X_1, \ldots, X_n, T_1, \ldots, T_m, U]$ qui élimine U et les T_i
2. calculer une base de Gröbner de

$$I = \sum_{i=1}^{n} A \cdot (q_i X_i - p_i) + A \cdot (q_1 \cdots q_n - 1)$$

   pour cet ordre
3. retirer les polynômes qui font intervenir U ou l'un des T_i et renvoyer la famille ainsi obtenue

Exemple en *Magma*

```
> Q:=RationalField();
> A<T,U,X,Y>:=PolynomialRing(Q,4,"elim",[1,2]);
> I:=ideal<A|(1+T^2)*X-(1-T^2),(1+T^2)*Y-2*T,(1+T^2)*U-1>;
> Groebner(I);
> Basis(I);
[
    T*X + T - Y,
    T*Y + X - 1,
    U - 1/2*X - 1/2,
    X^2 + Y^2 - 1
]
> [b:b in Basis(I)|Degree(b,T) eq 0 and Degree(b,U) eq 0];
[
    X^2 + Y^2 - 1
]
```

Nécessité de la variable ajoutée

Sur l'exemple,

$$x = \frac{s^2}{t}, \qquad y = \frac{t^2}{s}, \qquad z = s$$

le calcul sans introduire U ni le polynôme $STU - 1$ renvoie l'équation implicite

$$z(x^2y - z^3) = 0$$

alors qu'avec, le calcul renvoie

$$x^2y - z^3 = 0.$$

Géométriquement, l'évitement des pôles a exclu l'hyperplan d'équation $z = 0$.

Calculs de bases de Gröbner

Par l'algorithme de Buchberger, la semaine prochaine.