ACGA **2012-2013**

Algèbre commutative et géométrie algébrique
TP : Bases de Gröbner et applications

Ce T.P. sera noté sur 4 points :

- 1 point pour la présentation globale ;
- 1,5 point pour les deux premières parties ;
- 1,5 point pour la dernière partie (deux critères principaux : réussir à résoudre la grille proposée, et que je sois capable d'utiliser facilement le programme proposé pour une autre grille).

Le fichier contenant la feuille de travail Maple (ou autre) est à envoyer à l'adresse **tristan.vaccon@univ-rennes1.fr** avant le **05 avril 2013**. Ce T.P. peut être fait en binôme (et cela est même conseillé), en pensant bien à indiquer dans le nom du fichier les noms des personnes participant au projet.

1 Algorithme de Buchberger

Étape 0. Ordres et monômes.

- Utiliser le package **Groebner**.
- Comprendre les fonctions **LeadingTerm**, **LeadingCoefficient** et **LeadingTerm**, ainsi que les ordres **plex**, **grlex**, **grevlex**.

Exemple 1. Quel est le LT de $X * Y^4 + 7 * X^2$ selon *plex(x,y)* ? Selon *grlex(x,y)* ?

Étape 1. Division

Écrire une fonction **Division(P,F,ordre)** qui calcule la division d'un polynôme P par la famille de polynômes F, selon l'ordre monomial *ordre* (réduction totale).

Indications. Écrire une fonction **IsDivisible(a,b)** qui teste si le monôme a est divisible par le monôme b.

Exemple 2. Quel est le résultat de la division de $f = x^2 * y + x * y^2 + y^2$ par $(y^2 - 1, x * y - 1)$ selon $plex(x, y)$? Quel est le résultat de la division de $f = x * y^2 - x$ par $(xy + 1, y^2 - 1)$? Par $(y^2 - 1, xy + 1)$?

Étape 2. S-polynôme

Écrire une fonction **SPoly(P,Q,ordre)** qui calcule le S-polynôme de P et Q selon l'ordre monomial *ordre*.

Exemple 3. Quel est le S-polynôme de $f = x^3y^2 - x^2y^3 + x$ et $g = 3x^4y + y^2$?

Étape 3. Algorithme de Buchberger

Écrire une fonction **Buchberger(F,ordre)** qui calcule une base de Gröbner de l'idéal engendré par la famille de polynômes F, selon l'ordre monomial *ordre*.

Bonus. Implémenter le critère de sélection de Buchberger sur les paires de polynômes ayant des termes de tête étrangers.

Exemple 4. Donner une base de Gröbner de $I =< y - x^2, z - x^3 >$ pour $plex(y, z, x)$, pour $plex(x, y, z)$, par votre algorithme. Comparer avec $Basis([y-x^2, z-x^3], plex(x, y, z))$ et $Basis([y-x^2, z - x^3], plex(y, z, x))$.

Exemple 5. Cas des polynômes symétriques :

Proposition 1.1. *We consider the ring $k[x_1,\dots,x_n,y_1,\dots,y_n]$ with a monomial ordering such that any monomial involving one of the x_i is greater than all the polynomial of $k[y_1,\dots,y_n]$ (for instance, the lexicographical ordering). Let G be Gröbner basis of $I=\langle\sigma_1-y_1,\dots,\sigma_n-y_n\rangle\subset k[x_1,\dots,x_n,y_1,\dots,y_n]$. Let $f\in k[x_1,\dots,x_n]$, let g be the remainder of the division of f by G, then f is symmetric if and only if $g\in k[y_1,\dots,y_n]$ and then, $f=g(\sigma_1,\dots,\sigma_n)$ is the unique expression of f as a polynomial in the elementary symmetric functions.*

Écrire une fonction **DecompositionSymElem(P)** donnant la décomposition d'un polynôme symétrique $P\in\mathbb{Q}[x_1,\dots,x_n]$ en les polynômes symétriques élémentaires. La tester sur $X^3+3*X^2*Y+3*X^2*Z+3*X*Y^2+6*Z*Y*X+3*X*Z^2+Y^3+3*Y^2*Z+3*Y*Z^2+Z^3+Z^2*Y^2*X^2$.

Indications. On pourra utiliser la fonction **Indets** pour obtenir les variables afin de pouvoir écrire les polynômes symétriques élémentaires.

Étape 4. Bases de Gröbner réduites et minimales :

- Écrire une fonction **MinGröbner(F,ordre**) qui calcule une base de Gröbner de l'idéal engendré par la famille F pour l'ordre *ordre* qui soit **minimale**.
- Écrire une fonction **RedGröbner(F,ordre)** qui calcule une base de Gröbner **réduite** de l'idéal engendré par la famille F pour l'ordre *ordre*.

Exemple 6. Calculer une base de Gröbner minimale de $I=<x^3-2xy,x^2y-2y^2+x>$ selon **grlex(x,y)**. En donner une base de Gröbner réduite.

2 Applications au calcul effectif sur les idéaux

Étape 5. Appartenance à un idéal

Écrire une fonction **IsInIdeal(P,F,ordre)** qui teste si P est dans l'idéal engendré par F, en passant par un calcul d'une base de Gröbner de F selon l'ordre monomial *ordre*

Exemple 7. Est-ce que $f=-4x^2y^2z^2+y^6+3z^5$ est dans $I=<xz-y^2,x^3-z^2>$?

Étape 6. Calcul de l'union

Écrire une fonction **Union(F,G,ordre)** qui calcule une base de Gröbner de l'idéal engendré par l'union des familles F et G, selon l'ordre monomial *ordre*.

Exemple 8. Que donne **Union**([X^2*Y],[$X*Y^2$],**plex(X,Y)**) ?

Étape 7. Calcul d'idéaux d'élimination :

- Écrire une fonction **AppartientElimSet(P,S)** qui retourne **True** si le polynôme P est dans $k[S^c]$ où S est un ensemble de variables, et **True** sinon.
- Écrire une fonction **ElimSet(F,S,ordre)** qui calcule une base de Gröbner de $<F>\cap k[S^c]$ (ceci est l'élimination des variables S).

Exemple 9. On considère $I=<x^2+y+z-1,x+y^2+z-1,x+y+z^2-1>$ dans $\mathbb{C}[x,y,z]$. Donner une base de Gröbner de $I\cap\mathbb{C}[y,z]$ et de $I\cap\mathbb{C}[z]$.

Exemple 10. Combien de solutions dans $\mathbb{Q}^3$ possède le système suivant ?

$$\begin{aligned} x^2+y^2+z^2 &= 4\\ x^2+2y^2 &= 5\\ xz &= 1 \end{aligned}$$

Étape 8. Calcul d'intersection de deux idéaux :

Écrire une fonction **Intersection(F,G,ordre)** qui calcule une base de Gröbner de l'intersection de F et G selon l'ordre monomial *ordre*.

Exemple 11. Que donne **Intersection**([X^2*Y],[$X*Y^2$],**plex(X,Y)**) ?

Et **Intersection**([$(x+y)^4(x^2+y)^2(x-5*y)$],[$(x+y)(x^2+y)^3(x+3y)$],**plex(X,Y)**) ?

3 Résolution de sudoku par bases de Gröbner

3.1 Présentation du problème

On se propose d'écrire un algorithme de résolution de sudoku fondé sur des calculs de bases de Gröbner.

Le principe du sudoku est de remplir une matrice $M = (M_{i,j}) \in M_9(\mathbb{Z})$ par des chiffres de $[\![1, 9]\!]$ tels que :

- sur chaque ligne, les neuf chiffres apparaissent (ou encore, les éléments de la ligne sont tous distincts) ;
- même contrainte sur chaque colonne ;
- chacune des 9 sous-matrices $(M_{i+3k_1,j+3k_2})_{i,j\in[\![1,3]\!]}$ pour $k_1, k_2 \in [\![0, 2]\!]$ a tout ses coefficients distincts (les 9 chiffres apparaissent sur chacune de ces sous-matrices) ;
- de plus, les matrices que l'on regarde peuvent avoir déjà certains chiffres fixés.

Le principe de la résolution que nous proposons sera de déterminer une base de Gröbner de l'idéal des contraintes sur les coefficients, et ainsi, si cette idéal définit bien une unique solution, en réduisant $M_{i,j}$ modulo l'idéal de ces relations, on obtiendra la seule valeur possible pour ce coefficient.

3.2 Contraintes

[1]

Contrainte 1.

Déterminer les équations correspondant aux contraintes "$M_{i,j}$ prend ses valeurs dans $[\![1, 9]\!]$".

Indications. Penser au fait que $M_{i,j}$ doit annuler un certain polynôme $P \in k[X]$, et ainsi, écrire $P(M_{i,j}) = 0$. On prendra P unitaire et scindé à racines simples (bien choisies...).

Contrainte 2.

Déterminer les équations correspondant à la contrainte "tous les éléments d'une même colonne sont distincts".

Indications. $Q(X, Y) = \frac{P(X)-P(Y)}{X-Y} \in k[X, Y]$ est bien un polynôme. De plus, $Q(X, Y)$ n'est pas divisible par $X-Y$. Il suffit de poser $X = Y$, on a $Q(X, X) = P'(X)$ qui est non nul dès que P est non constant. Ainsi, si $M_{i,j}, M_{i',j'} \in k$ sont tels que $Q(M_{i,j}, M_{i',j'}) = 0$, $P(M_{i,j}) = 0$, $P(M_{i',j'}) = 0$, alors nécessairement, $M_{i,j} \neq M_{i',j'}$ puisque sinon, $Q(M_{i,j}, M_{i,j}) = P'(M_{i,j}) \neq 0$ puique P est à racines simples.

Les contraintes à regarder sont donc les $Q(M_{i,j}, M_{i',j'})$ pour i, j, i', j' bien choisis.

Contrainte 3.

Faire de même pour les lignes et les sous-matrices $3 * 3$ correspondant aux contraintes sur les 9 carrés.

Contrainte 4.

On suppose que la valeur de $M_{i,j}$ est fixé dans le sudoku de départ à $a_{i,j} \in [\![1, 9]\!]$. Quelle est la contrainte polynomiale sur $M_{i,j}$ correspondante à ajouter à notre liste de contraintes ?

[1] La proposition suivante a l'avantage de bien fonctionner avec le calcul de bases de Gröbner de Maple. Néanmoins, une autre présentation des contraintes est possible. En effet, pour avoir tout les termes sur une colonne distincts et égaux à un élément de $[\![1, 9]\!]$, il suffit d'ajouter l'équation $\prod_{i=1}^{9}(X - m_{i,j}) - \prod_{i=1}^{9}(X - i) = 0$, et de faire de même pour toutes les lignes, colonnes et sous-carrés. Hélas, cette méthode, pourtant très simple, produit un calcul de base de Gröbner bien trop compliqué pour Maple, et c'est la raison de la méthode proposée dans cette partie.

3.3 Résolution

On suppose qu'une grille de sudoku est donnée par une matrice $M = (m_{i,j})$ ayant ses coefficients déjà fixés dans $[\![1, 9]\!]$ et les autres, non encore connus, mis à zéro. On suppose qu'il existe une seule solution à ce sudoku.

Comment connaître la valeur que doit prendre $m_{i,j}$? Que se passe-t-il si la grille proposée n'a pas de solutions ?

Indications. On sait quelles sont les contraintes (polynomiales) à appliquer à $M_{i,j}$...

Appliquer ce qui précède à la grille suivante en écrivant une procédure **SudokuSolve** prenant en entrée une matrice à coefficients dans $[\![0, 9]\!]$ et renvoyant la solution s'il est existe et est unique, et un message d'erreur approprié sinon [2] :

		8	4				3	
				1		8		4
					7			1
7		1	2			4	8	
			6		1			
	2	6			8	5		7
2			3					
9		3		2				
	8				5	2		

Indications. Quelques conseils avant de se lancer dans la résolution du sudoku :

- Bien faire attention aux indices lorsqu'on définit les polynômes ;
- Toujours faire une sauvegarde avant de lancer le calcul d'une base de Gröbner ;
- Pour ce dernier : on peut ajouter l'option **characteristic = 11** dans tout les calculs de bases de Gröbner et de réduction, afin de simplifier l'execution ;
- Préférer l'ordre **grevlex** (donné par **tdeg** dans Maple), plus efficace en général ;
- Faire très attentions aux boucles **for** qui ne seraient pas dans une procédure : leur variable est globale par défaut, ce qui amène nécessairement des bugs. Préférer une approche en définissant des procédures.

[2] Une évaluation du temps pris par le calcul, grâce à la fonction **time** serait bienvenue.