KANE Seyni
ID Etudiant: 22011929

Master 2 ACC / Paris 8
DM Algorithmes arithmétiques II
Prof: Julien Lavauzelle
26 Octobre 2022

Une introduction aux bases de Gröbner

---

1 Objectifs

Le sujet a pour objectif la découverte de la notion de bases de Gröbner, leur calcul effectif, et leur application à la résolution de systèmes polynomiaux.

Notre but sera d'essayer de comprendre le sujet en nous familiarisant avec la nation de bases de Gröbner avec des exemples pratiques. Et avec des implementations des differents algorithmes qui interviennent dans le calcule effectif des bases de Gröbner.

Dans ce qui suit nous allons essayer de repondre au questions qui sont posé dans ce DM.

NB: les algorithmes ne sont pas commenter dans ce fichier. Cependant une version commenté et plus detaillé se trouve dans fichier le .py contenant tous le code de ce DM.

2 Réponses

Soit le systéme d'équation suivant:

$$(E)\begin{cases} 3x^4 + 2xy^2z + xy^2 + 2z^3 - 6x^2 + xy - y + 3 = 0 & (1) \\ x^4 + xy^2z + \ + z^3 - 2x^2 + 1 = 0 & (2) \\ 2x^4 + 2xy^2z + xy^2 + 2z^3 - 4x^2 + xy - y + 2 = 0 & (3) \end{cases}$$

Réponse 1

KANE Seyni
kaneseyni.sn@gmail.com

Nous allons essayer d'isoler une équation qui ne dépend que de x.
En faisant $(1) - (3)$ on obtient:

$$x^4 \; - \; 2x^2 \; + \; 1 \; = \; 0 \qquad (4)$$

Réponse 2

On d'abord résoudre l'équation (4)

On remarque que $1 \; et \; -1$ sont des solutions double de cette équation, alors on peut factoiser $x^4 \; - \; 2x^2 \; + \; 1$ de la façon suivante:

$$x^4 \; - \; 2x^2 \; + \; 1 \; = \; (x \; - \; 1)^2(x \; + \; 1)^2$$

D'oú l'ensemble des solutions de l'équation (4) est : $\{-1 \; , \; 1\}$

En remplaçant la variable x, on obtient:

- Pour $x \; = \; 1$, (E) devient:

$$\begin{cases} \quad y^2 z \; + \; + z^3 \; = 0 & (2) \\ 2y^2 z \; + \; y^2 \; + 2z^3 \; = 0 & (3) \end{cases}$$

  En faisant $(3) - (22)$ on obtient:

$$y^2 \; = \; 0 \; \Rightarrow \; y \; = \; 0$$
$$\text{Et en remplaçant } y \text{ dans } (L2) \; \Rightarrow \; z \; = \; 0$$

  Donc pour $x \; = \; 1$, la solution de (E) est: $(1, 0, 0)$

- Pour $x \; = \; -1$, (E) devient:

$$\begin{cases} \quad -y^2 z \; + z^3 \; = 0 & (2) \\ -2y^2 z \; - \; y^2 \; + 2z^3 \; - 2y \; = 0 & (3) \end{cases}$$

  $(3) - 2(2)$ donnes:

$$-y^2 \; - 2y = \; 0 \; \Rightarrow \; - y(y + 2) \; = \; 0$$
$$\Rightarrow \; y = 0 \text{ où } y = -2$$
$$\text{Et en remplaçant } y = -2 \text{ dans } (2) \; \Rightarrow \; - 4z \; + \; z \; = \; 0$$
$$\Rightarrow \; z = 0 \text{ où } z = \; \pm \; 2$$

  Donc pour $x \; = \; -1$, les solutions de (E) sont: $(-1, 0, 0)$, $(-1, -2, 0)$,$(1, -2, -2)$, $(-1, -2, 2)$.

Ainsi les solutions de (E) sont: $(-1, 0, 0)$, $(-1, -2, 0)$,$(1, -2, -2)$, $(-1, -2, 2)$, $(1, 0, 0)$

Réponse 3

Nous allons classer dans l'ordre décroissance pour $>_{lex}$ et pour $>_{grevlex}$ les monômes suivants:

$$\{x, x^2y, y^9, xyz, yz^4, xz, xy, x^2z\}$$

En considérant les monômes dans $\mathbb{F}[x, y, z]$ on a :

- Pour $>_{lex}$:
  Comme l'ordre lexicographique à pour l'exposant de x qui domine, puis celui de y et afin celui de z dans $\mathbb{F}[x, y, z]$, alors les monômes se classent comme suit:
  $$x^2y >_{lex} x^2z >_{lex} xyz >_{lex} xy >_{lex} xz >_{lex} x >_{lex} y^9 >_{lex} yz^4$$
- Pour $>_{grevlex}$:

  Comme l'ordre lexicographique renversé gradué àle degré totale qui domine, et si y'a égalité la puissance inférieure de z domine(suivi de y et enfin de x) x qui domine dans $\mathbb{F}[x, y, z]$, alors les monômes se classent comme suit:
  $$y^9 >_{grevlex} yz^4 >_{grevlex} x^2y >_{grevlex} x^2z >_{grevlex} xyz >_{grevlex} xy >_{grevlex} xz >_{grevlex} x$$

Réponse 4

Montrons que l'ordre lexicographique,$>_{lex}$ est un ordre monomial.
D'après le **Lemme 2.3** du DM il suffit de montrer que toute suite strictement décroissante de $\mathbb{N}^n$

$$u_0 >_{lex} u_1 >_{lex} \cdots >_{lex} u_k >_{lex} \cdots$$

est finie.

Ce equivant a dire que l'ordre lexicographique,$>_{lex}$ n'est pas un ordre monomial si et seulement si il existe une suite strictement décroissante de $\mathbb{N}^n$

$$u_0 >_{lex} u_1 >_{lex} \cdots >_{lex} u_k >_{lex} \cdots$$

infinie.

$\Longrightarrow$ Supposons que $>_{lex}$ n'est pas un ordre monomial et montrons qu'il existe une suite strictement décroissante de $\mathbb{N}^n$ infini.
$>_{lex}$ n'est pas un ordre monomial d'après la **Définition 2.1** $>_{lex}$ n'est pas une relation d'ordre totale sur $\mathbb{N}^n$, donc il existe un sous ensemble non vide $E \subseteq N^n$ n'admettant pas un plus petis elements selon $>_{lex}$.
En effet soit $u_0 \in E$, vue que u_0 n'est pas le plus petit element de E on peut trouver $u_1 \in E$ tel que $u_0 >_{lex} u_1$. Ensuite vue que u_1 n'est pas le plus petit element de E on peut trouver $u_2 \in E$ tel que $u_1 >_{lex} u_2$. Ainsi de suite, on obtent finalement une suite strictement décroissante de $\mathbb{N}^n$

$$u_0 >_{lex} u_1 >_{lex} \cdots >_{lex} u_k >_{lex} \cdots$$

infie.

- Inversement etant donné une suite strictement décroissante de $\mathbb{N}^n$ infini

$$u_0 >_{lex} u_1 >_{lex} \cdots >_{lex} u_k >_{lex} \cdots$$

n'admetant pas de plus petit elements cette suite $\{u_i\}_{i\geq 0} \notin \mathbb{N}^n$.
Par conséquant $>_{lex}$ n'est pas une relation d'ordre totale sur N^n. D'oú n'est pas un ordre monomial.

Réponse 5

Exécutons à la main l'algorithme de division polynomiale

1.) $P = xy^3 + x$ **,** $G = [G_1, G_2]$ **avec** $G_1 = y^2 + x$ **et** $G_2 = xy$

Posons : $F = xy^3 + x$ alors:

En utilisant l'ordre $>_{lex}$ on a:

$$LT(F) = xy^3,\ LT(G_1) = x,\ LT(G_2) = xy.$$

Comme $F \neq 0$ alors determinons $LT(F)$ et $LT(G_1)$

$$\begin{cases} LT(F) = xy^3 \\ LT(G_1) = x \end{cases} \Rightarrow LT(G_1) \mid LT(F)\ et\ LT(F) \mid LT(G_1) = y^3$$

Donc $Q_1 = y^3$ et $F := F - G_1 * y^3 = x - y^5 \neq 0$.
Comme $F \neq 0\ et\ LT(G_1) \mid LT(F)$ alors determinons $LT(F)$ et $LT(G_1)$

$$\begin{cases} LT(F) = x \\ LT(G_1) = x \end{cases} \Rightarrow LT(G_1) \mid LT(F)\ et\ LT(F) \mid LT(G_1) = 1$$

Donc $Q_1 = y^3 + 1$ et $F := F - G_1 * 1 = -y^5 - y^2 \neq 0$.
Comme $F \neq 0$ alors determinons $LT(F)$ et $LT(G_1)$

$$\begin{cases} LT(F) = -y^5 \\ LT(G_1) = x \end{cases} \Rightarrow LT(G_1) \nmid LT(F)$$

Comme $LT(G_1) \nmid LT(F)$ alors determinons $LT(F)$ et $LT(G_2)$,

KANE Seyni
kaneseyni.sn@gmail.com

$$\begin{cases} LT(F) = & -y^5 \\ LT(G_2) & = \ xy \end{cases} \Rightarrow \ LT(G_2) \nmid LT(F)$$

Donc $R := LT(F) = -y^5$ et $F := F - LT(F) = -y^5 - y^2 - (-y^5) = -y^2 \neq 0$.

Comme $F \neq 0$, alors determinons $LT(F)$ et $LT(G_1)$

$$Ona \begin{cases} LT(F) = & -y^2 \\ LT(G_1) & = \ x \end{cases} \Rightarrow \ LT(G_1) \nmid LT(F)$$

Comme $LT(G_1) \nmid LT(F)$ Determinons $LT(F)$ et $LT(G_2)$

$$Ona \begin{cases} LT(F) = & -y^2 \\ LT(G_2) & = \ xy \end{cases} \Rightarrow \ LT(G_1) \nmid LT(F)$$

Donc $R := LT(F) = -y^5 - y^2$ et $F := F - LT(F) = -y^2 - (-y^2) \iff 0$.

Ce qui termine l'algorithme avec $Q_1 = y^3 + 1$, $Q_2 = 0$ et $R = -y^5 - y^2$
2.) $P = xy^3 + x$ **,** $G = [G_1, G_2]$ **avec** $G_2 = y^2 + x$ **et** $G_1 = xy$

Posons : $F = xy^3 + x$ alors:

En utilisant l'ordre $>_{lex}$ on a:

$$LT(F) = xy^3,\ LT(G_1) = xy,\ LT(G_2) = x.$$

Comme $F \neq 0$ alors determinons $LT(F)$ et $LT(G_1)$

$$Ona \begin{cases} LT(F) = \ xy^3 \\ LT(G_1) \ = \ xy \end{cases} \Rightarrow \ LT(G_1) \mid LT(F) \ et \ LT(F) \mid LT(G_1) = y^2$$

Donc $Q_1 = y^2$ et $F := F - G_1 * y^2 = x \neq 0$.
Comme $F \neq 0 \ et \ LT(G_1) \mid LT(F)$ alors determinons $LT(F)$ et $LT(G_1)$

$$\begin{cases} LT(F) = \ x \\ LT(G_1) \ = \ xy \end{cases} \Rightarrow \ LT(G_1) \nmid LT(F) \ et \ LT(F) \mid LT(G_1) = 1$$

Comme $LT(G_1) \nmid LT(F)$ alors determinons $LT(F)$ et $LT(G_2)$,

$$\begin{cases} LT(F) = x \\ LT(G_2) = x \end{cases} \Rightarrow LT(G_2) \mid LT(F)$$

Donc $Q_2 = 1$ et $F := F - G_2 * 1 = -y^2 \neq 0$.

Comme $F \neq 0$, alors determinons $LT(F)$ et $LT(G_1)$

$$Ona \begin{cases} LT(F) = -y^2 \\ LT(G_1) = xy \end{cases} \Rightarrow LT(G_1) \nmid LT(F)$$

Comme $LT(G_1) \nmid LT(F)$ Determinons $LT(F)$ et $LT(G_2)$

$$Ona \begin{cases} LT(F) = -y^2 \\ LT(G_2) = x \end{cases} \Rightarrow LT(G_2) \nmid LT(F)$$

Donc $R := LT(F) = -y^2$ et $F := F - LT(F) = -y^2 - (-y^2) \iff 0$.

Ce qui termine l'algorithme avec $Q_1 = y^2$, $Q_2 = 1$ et $R = -y^2$
3.) $P = xy^3 + x$ **,** $G = [G_1, G_2]$ **avec** $G_1 = y^2 + x$ **et** $G_2 = xy$

Posons : $F = xy^3 + x$ alors:

En utilisant l'ordre $>_{grevlex}$ on a:

$$LT(F) = xy^3, LT(G_1) = y^2, LT(G_2) = xy.$$

Comme $F \neq 0$ alors determinons $LT(F)$ et $LT(G_1)$

$$Ona \begin{cases} LT(F) = xy^3 \\ LT(G_1) = y^2 \end{cases} \Rightarrow LT(G_1) \mid LT(F) \; et \; LT(F) \mid LT(G_1) = y^2$$

Donc $Q_1 = xy$ et $F := F - G_1 * xy = x - x^2y \neq 0$.
Comme $F \neq 0 \; et \; LT(G_1) \mid LT(F)$ alors determinons $LT(F)$ et $LT(G_1)$

$$\begin{cases} LT(F) = x^2y \\ LT(G_1) = y^2 \end{cases} \Rightarrow LT(G_1) \nmid LT(F)$$

Comme $LT(G_1) \nmid LT(F)$ alors determinons $LT(F)$ et $LT(G_2)$,

$$\begin{cases} LT(F) &= x + x^2y \\ LT(G_2) &= xy \end{cases} \Rightarrow LT(G_2) \mid LT(F)$$

Donc $Q_2 = -x$ et $F := F - G_2 * (-x) = x \neq 0$.
Comme $F \neq 0$ alors determinons $LT(F)$ et $LT(G_1)$

$$\begin{cases} LT(F) &= x \\ LT(G_1) &= y^2 \end{cases} \Rightarrow LT(G_1) \nmid LT(F)$$

Comme $LT(G_1) \nmid LT(F)$ alors determinons $LT(F)$ et $LT(G_2)$,

$$\begin{cases} LT(F) &= x \\ LT(G_2) &= xy \end{cases} \Rightarrow LT(G_2) \nmid LT(F)$$

Donc $R := LT(F) \ = \ x$ et $F := F - LT(F) = x - x \iff 0$.

Ce qui termine l'algorithme avec $Q_1 = xy$, $Q_2 = -x$ et $R = x$

Réponse 6

```python
def funcDivisionPolynomial(P, Gs, RING):
    F = RING(P)
    l = len(Gs)
    Qs = l*[RING(0)]
    R = RING(0)
    while F != 0:
        i = 0
        test_division = False
        while i < l and test_division== False:
            if Gs[i].lt().divides(F.lt()):
                q= F.lt()//Gs[i].lt()
                Qs[i] += q
                F = F - q * Gs[i]
                test_division = True
            else:
                i += 1
        if test_division == False:
            r = F.lt()
            R += r
            F -= r
    return Qs, R
```

KANE Seyni
kaneseyni.sn@gmail.com

Réponse 7: Donnons un contre-exemple à l'inclusion réciproque définis à la partie 3.1 du dm.

Soit $I = < f_1, f_2 >$ avec $f_1 = x^3 - xy$ et $f_2 = x^2y - y^2 + x$.

On a :

$$x(\ x^2y\ -\ y^2\ +\ x)\ -\ y(\ x^3\ -\ xy)\ =\ x^2$$

$$Donc \begin{cases} x^2 \ \in \ I \ et \ LT(x^2) \ = \ x^2 \ \in < LT(I) > \\ x^2 \notin < LT(f_1), LT(f_2) > \ = \ < x^3, x^2y > \end{cases} \Rightarrow \ < LT(I) > \ \neq \ < LT(f_1), LT(f_2) >$$

Réponse 8

Soit I l'idéal engendré par $G = \{G1 \ = \ x + y^2, G2 \ = \ xy\}$ que l'on a introduit à la Question 5. Démontrons que $G' \ = \ \{G'1 \ = \ x \ + \ y^2, G'2 \ = \ y^3\}$ est une base de Gröbner de cet idéal I, pour l'ordre lexigographique. Pour cela, on calculons explicitement $< LT(I) >$.

$$LT(I) \ = \ \{a_{\alpha\beta}x^\alpha y^\beta \ | \ \exists f \in I \ avec \ LT(f) \ = \ a_{\alpha\beta}x^\alpha y^\beta\}$$

Soit $m \ \in LT(I) \ \Rightarrow \ \exists a_{\alpha\beta} \in \mathbb{F}, \ \alpha \ , \beta \ \in \mathbb{N} \ et \ f \ \in \ I \min LT(f) \ = \ a_{\alpha\beta}x^\alpha y^\beta \Longleftrightarrow \exists X \ , Y \ \in \mathbb{F}[x, y] \ | \ LT(X * (x + y^2) + Y * (y^3)) \ = \ a_{\alpha\beta}x^\alpha y^\beta \ \Rightarrow$

$$\begin{cases} a_{\alpha\beta}x^\alpha y^\beta \ = \ X * x \\ a_{\alpha\beta}x^\alpha y^\beta \ = \ Y * (y^3) \end{cases} \Rightarrow \ < LT(I) > \ \subseteq \ < x \ , \ y^3 > \ = \ < LT(G'1), LT(G'2) >$$

Or D'apres la Définition 3.1 on a toujours $< LT(G'1), LT(G'2) > \ \subseteq \ < LT(I) >$ d'où $< LT(G'1), LT(G'2) > \ = \ < LT(I) >$

D'où G' est une base de Grobner de l'iéal I

Réponse 9

```
def funcMcm(P, Q, RING):
    u = P.lm().degrees()
    v = Q.lm().degrees()
    w = []
    for i in range (0, len(u)):
        w.append(max(u[i], v[i]) )
    A = x^w[0]*y^w[1]*z^w[2]
    return A
```

KANE Seyni
kaneseyni.sn@gmail.com

```
def funcSpolynome(P, Q, RING):
    p = funcMcm(P.lt(), Q.lt(), RING)
    S = (p.quo_rem(P.lt())[0])*P - (p.quo_rem(Q.lt())[0])*Q
    return S
```

Réponse 10

```
def funcBuchberger(Gs, RING):
    l = len(Gs)
    i = 0
    j = 0
    for i in [0 .. l - 2]:
        for j in [i + 1 .. l - 1]:
            S = funcSpolynome(Gs[i],Gs[j], RING)
            R = funcDivisionPolynomial(S, Gs, RING)[1]
            if R != 0:
                return funcBuchberger(Gs + [R], RING)
    return Gs
```

Réponse 11

```
def funcReduction(Gs, RING):
    Gsc = copy ( Gs )
    Gs1 = []

    while len(Gsc) > 0:
        d = min(p.degree() for p in Gsc)
        P = RING(0)
        for p in Gsc:
            if p.degree() == d:
                P = p
                break
        Gs1.append(P)
        Gscc = []
        for G in Gsc:
            if G.lm().quo_rem(P.lm())[1] != 0:
                Gscc.append(G)
        Gsc = Gscc

    Gs2 = []
    Gs11 = []
    for G in Gs1:
        if G not in Gs:
            Gs11.append(G)
    for G in Gs1:
```

```
        R = funcDivisionPolynomial(G, Gs11, RING)[1]
        Gs2.append(R)
    return Gs2
```

Réponse 12: Calculer une base de Gröbner réduite avec nos progammes pour les idéaux suivants :

---

1. Pour $I =< y^2 + x, xy >$ avec $>_{lex}$: notre programme donne le résultat suivant:
$$\mathcal{G} = \{x + y^2, xy, y^3\}$$
2. Pour $I =< y^2 + x, xy >$ avec $>_{grevlex}$: notre programme donne le résultat suivant:
$$\mathcal{G} = \{x + y^2, xy, x^2\}.$$
3. Pour $I =< x^2 + y^2 - 1, xy - \frac{1}{2} >$ avec $>_{grevlex}$: notre programme donne le résultat suivant:
$$\mathcal{G} = \{x^2 + y^2 - 1, xy - \frac{1}{2}, \frac{1}{2}x + y^3 - y, -2 * y^4 + 2 * y^2 - \frac{1}{2}\}.$$

Réponse 13

Conclusion

Ce DM a été riche en apprentissage tant sur le plan téorique que sur le plan pratique. L'objectif au debut était de nous faire decouvrire les base de bases de Gröbner, leur calcul effectif, et leur application à la résolution de systèmes polynomiaux. On peut dire qu'il est atteind. Car ce DM nous a permit de nous familiariaser avec la notion de base de Gröbner les calculs dans l'anneau $\mathbb{K}[x_1 \ldots, x_2]$ ainsi leurs manupulation sur des logiciel de calcul formelle comme **Sage**.