REPUBLIQUE TUNISIENNE

****

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

UNIVERSITE DE SFAX

FACULTE DES SCIENCES DE SFAX

******

DEPARTEMENT DE MATHEMATIQUES

MEMOIRE DE PROJET DE FIN D' ETUDES

Pour l'obtention du :

DIPLÔME DE MAITRISE EN MATHEMATIQUES APPLIQUEES

Sujet :

Implantation d'un algorithme pour le complètement des matrices polynomiales multivariées unimodulaires

par

Kamel BOUGHARRIOU

&

Mohamed ABID

Soutenu, le 29 /05/2006 devant le Jury d'Examen:

Mr Imed FEKI	**(Maître assistant FSS)**	**Président**
Mr Ihsen YENGUI	**(Maître de conférences FSS)**	**Encadreur**
Mr Mongi Benhamedou	**(Maître de conférences FSS)**	**Membre**
Mr Slim CHAABENE	**(Maître de conférences FSS)**	**Membre**

Année Universitaire 2005/2006

Remerciements

Nous tenons à remercier toutes les personnes qui ont contribué de prés ou de loin à la réalisation de ce projet.

Il nous est plus particulièrement très agréable d'exprimer notre gratitude et reconnaissance, à Monsieur Ihsen Yengui, Maître de Conférences à la faculté des Sciences de Sfax, pour la chance qu'il nous a offerte afin d'effectuer ce projet de fin d'études et la bienveillance avec laquelle il a suivi notre travail.

Nous tenons aussi à remercier, Monsieur Imed FEKI, Monsieur Mongi Benhamedou et Monsieur Slim CHAABENE pour avoir accepté de faire partie du jury de ce mémoire.

Par la même occasion, nous voudrons remercier tous nos enseignants de la Faculté des Sciences de Sfax pour la qualité de l'enseignement qu'ils nous ont dispensé durant nos études.

Dédicaces

J'ai le plaisir de dédier ce mémoire en témoignage d'affection et de reconnaissance à tous ceux qui m'aiment et que j'aime.

Particulièrement,

A la mémoire de mon père,

Que la mort l'a pris avant d'adresser à ce jour.

A ma mère,

Pour les encouragements et les sacrifices

Qu'elle n'a cessé de me faire

Et de m'offrir les conditions favorables à mes études.

A mes frères et ma sœur,

Pour leur soutien morale et leurs encouragements.

A ma grand mére,

Pour les encouragements Qu'elle n'a cessé de me faire

A mes amis,

Au nom de l'amitié qui nous réunit,

Et au nom de nos souvenirs inoubliables.

Kamel

Dédicaces

Je dédie ce travail,
A mon père, qui n'a jamais reculé devant aucun sacrifice chaque fois qu'il était question de mon éducation et de mon avenir,

A ma mère, qui a toujours eu une confiance aveugle en ce que je pouvais accomplir, à ses efforts colossaux pour que je puisse accomplir autant, à sa patience et à son amour,
A mon frère et ma sœur et leurs époux qui m'ont encouragé et soutenu dans mes projets,

A toute ma famille et mes amis, que j'ai partagé avec eux des souvenirs inoubliables.

Mohamed ABID.

Résumé

Le but de ce projet est d'implanter un algorithme de complètement unimodulaire et de l'appliquer dans le traitement du signal multidimensionnel.

Ce projet s'articule autour de trois chapitres :

Dans le *chapitre1* intitulé " Base de Gröbner et resultant de deux polynômes ", on présente un algorithme de division dans $K[X_1,...,X_n]$ qui généralise l'algorithme de division euclidienne dans $K[X]$.

Ensuite on présente l'algorithme de Buchberger qui permet de construire une base de Gröbner indispensable pour le problème d'appartenance à un idéal.

Le *chapitre 2* est consacré à l'étude d'un algorithme pour le complètement des matrices polynomiales multivariées unimodulaires. Il est bien connu qu' un tel algorithme a un large champs d'application, notamment dans le domaine du traitement du signal multidimensionnel. Par exemple, l'égalisation de canaux MIMO (multi entrées – multi sorties) de télécommunications tel que le réseau GSM, requiert la construction de l'inverse à gauche d'une matrice polynomiale multivariée unimodulaire à coefficients dans le corps des complexes. De multiples problèmes de traitement du signal multidimensionnel sont liés à la paramétrisation, la factorisation et le complètement de matrices polynomiales multivariées unimodulaires.

Dans le *chapitre 3*, nous avons mis les codes Maple implantant l'algorithme de complètement unimodulaire étudié dans le chapitre 2.

CHAPITRE I

Bases de Gröbner et Résultant de deux polynômes

Chapitre 1

Bases de Gröbner et Résultant de deux polynômes

Ce chapitre est en grande partie extraite de [CLO].

1 – Généralités

Définition 1.1.

(i) $(A,+,*)$ est un anneau s'il vérifie les deux conditions suivantes :

- $(A,+)$ est un groupe abélien.
- La deuxième loi " $*$ " est associative et distributive par rapport à la loi " $+$ ".

(ii) $(A,+,*)$ est un anneau commutatif si $(A,+,*)$ est un anneau et la loi " $*$ " est commutative.

(iii) $(A,+,*)$ est un anneau unitaire si la deuxième loi " $*$ " admet un élément neutre.

(iv) $(A,+,*)$ est un anneau intègre si $\forall x, y \in A,\ x * y = 0$ alors $x = 0$ ou $y = 0$.

Définition 1.2.

(i) $(A,+,*)$ est un corps si est seulement si $(A,+,*)$ est un anneau unitaire, et tout élément non nul est inversible.

(ii) $(A,+,*)$ est un corps commutatif si $(A,+,*)$ est un corps et la loi " $*$ " est commutative.

Dans toute la suite K désignera un corps commutatif.

Définition 1.3. Un monôme en $X_1,...,X_n$ est un produit de la forme $X_1^{a_1}\cdots X_n^{a_n}$ avec tous les tous les a_i sont des entiers positifs. Le degré total de ce monôme est la somme des a_i, il est noté $|a|$.

Définition 1.4. Un polynôme f en $X_1,...,X_n$ avec des coefficients dans K est une combinaison linéaire finie de monômes, on écrit $f=\sum_a a_a X^a$; $a_a \in K$.

Définition 1.5. Soit $f=\sum_a a_a X^a$, $a_a \in K$, un polynôme dans $K[X_1,...,X_n]$.

(i) On appelle a_a le coefficient du monôme X^a.

(ii) Si $a_a \neq 0$, alors on appelle $a_a X^a$ un terme de *f*.

(iii) Le degré total noté $\deg(f)$ est le maximum des $|a|$ tel que $a_a \neq 0$.

Définition 1.6. Un ensemble $I \subset K[X_1,...,X_n]$ est un idéal si on a :

(i) $0 \in I$.

(ii) Si f, $g \in I$, alors $f+g \in I$.

*(iii)*Si $f \in I$ et $h \in K[X_1,...,X_n]$ alors $hf \in I$.

Définition 1.7. Soient $f_1,...,f_s$ des polynômes dans $K[X_1,...,X_n]$, alors la famille engendrée par $f_1,...,f_s$ est : $\langle f_1,...,f_s\rangle = \left\{\sum_{i=1}^{s} h_i f_i;\ h_1,...,h_s \in K[X_1,...,X_n]\right\}$.

Lemme 1.1. Si $f_1,...,f_s \in K[X_1,...,X_n]$ alors $\langle f_1,...,f_s\rangle$ est un idéal de $K[X_1,...,X_n]$ appelé l'idéal engendré par $f_1,...,f_s$.

Preuve

(i) Montrons que $0 \in \langle f_1,...,f_s\rangle$; $0=\sum_{i=1}^{s} 0 f_i$, $0 \in K[X_1,...,X_n]$ *alors* $0 \in \langle f_1,...,f_s\rangle$.

(ii) Soit $f, g \in \langle f_1,..., f_s \rangle$ *alors* $f = \sum_{i=1}^{s} p_i f_i$ *avec* $p_i \in K[X_1,..., X_n]$ *et* $g = \sum_{i=1}^{s} q_i f_i$ *avec* $q_i \in K[X_1,..., X_n]$.

On a $f + g = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i = \sum_{i=1}^{s} (p_i + q_i) f_i$ *avec* $p_i + q_i \in K[X_1,..., X_n]$ *puisque* $p_i \in K[X_1,..., X_n]$ *et* $q_i \in K[X_1,..., X_n]$. *Alors* $f + g \in K[X_1,..., X_n]$.

(iii) Soit $h \in K[X_1,..., X_n]$ *on a* $hf = h\sum_{i=1}^{s} p_i f_i = \sum_{i=1}^{s} hp_i f_i = \sum_{i=1}^{s} (hp_i) f_i$ *avec* $hp_i \in K[X_1,..., X_n]$, *alors* $hf \in I$.

Définition 1.8. Soit *f* un polynôme non nul de $K[X]$, $f = a_0 X^m + a_1 X^{m-1} + ... + a_m$ avec $a_i \in K[X]$ et $a_0 \neq 0$, $m = \deg(f)$. On dit que $a_0 X^m$ est le terme dominant de *f*, et on écrit $LT(f) = a_0 X^m$.

Proposition 1.1. Soit *g* un polynôme non nul de $K[X]$. Tout $f \in K[X]$ peut être écrit sous la forme $f = qg + r$ avec $q, r \in K[X]$ et $r = 0$ ou $\deg(r) < \deg(g)$. Les polynômes *q* et *r* sont uniques.

Preuve

Si $f = 0$ *rien à faire.*

Si $f \neq 0$ *on initialise :* $q := 0$; $r := f$;

Si $LT(g)$ *divise* $LT(r)$ *alors*

$q := q + LT(r)/LT(g)$;

$r := r - (LT(r)/LT(g))g$;

On refait tant que $r \neq 0$ *et* $LT(g)/LT(r)$.

Exemple : On prend $g(x)=x^2-1$ et $f(x)=2x^3-x^2+3x-1$. On initialise $q=0$ et $r=f$.

$LT(g)=x^2$ et $LT(r)=2x^3$ d'où $LT(g)/LT(r) \Rightarrow q=2x$ et $r=-x^2+5x-1$.

$LT(g)=x^2$ et $LT(r)=-x^2$ d'où $LT(g)/LT(r) \Rightarrow q=2x-1$ et $r=5x-2$.

$LT(g)$ ne divise pas $LT(r)$ d'où on s'arrête et $f(x)=qg+r=(2x-1)(x^2-1)+5x-2$.

Définition 1.9. Un plus grand commun diviseur des polynômes $f_1,...,f_s \in K[X]$ est un polynôme unitaire *h* tel que :

(i) *h* divise $f_1,...,f_s$,

(ii) Si *p* divise $f_1,...,f_s$ alors *p* divise *h*.

On écrit $h=\Delta(f_1,...,f_s)$.

Proposition 1.2. Soient $f_1,...,f_s$ des polynômes dans $K[X]$ alors :

(i) $\Delta(f_1,...,f_s)$ existe et il est unique.

(ii) $\Delta(f_1,...,f_s)$ est un générateur de l'idéal $\langle f_1,...,f_s\rangle$.

(iii) Pour $s\geq 3$; $\Delta(f_1,...,f_s)=\Delta(f_1,\Delta(f_2,...,f_s))$.

(iv) Il y a un algorithme pour obtenir $\Delta(f_1,...,f_s)$ appelé algorithme d'Euclide.

Preuve

(i) Chaque idéal de $K[X]$ *est principal donc il existe* $h\in K[X]$ *tel que* $\langle f_1,...,f_s\rangle=\langle h\rangle$. *Supposons qu'il existe* $p\in K[X]$ *divisant* $f_1,...,f_s$ *; c'est-à-dire* $f_1=c_1p,...,f_s=c_sp$ *; on a* $h\in K\langle f_1,...,f_s\rangle$ *donc il existe* $A_1,...,A_s$ *tel que :* $h=A_1f_1+...+A_sf_s=(A_1c_1+...+A_sc_s)p$, *et par suite* h/p. *Il vient* $h=\Delta(f_1,...,f_s)$.

Pour montrer 1'unicite, supposons qu'il existe $\tilde{h}$ *un autre* $\Delta(f_1,...,f_s)$. *On a alors* $h/\tilde{h}$ *et* $\tilde{h}/h$ *et par suite il existe* $l \in K^*$ *tel que* $h = l\tilde{h}$.

(ii) $h = \Delta(f_1,...,f_s)$, $h/f_i \Rightarrow f_i \in \langle h\rangle \forall i \Rightarrow \langle f_1,...,f_s\rangle \subset \langle h\rangle$.

L'algorithme d'Euclide implique $h = \sum_{i=1}^{s} h_i f_i, h_i \in K[X]$ *et par suite* $h \in \langle f_1,...,f_s\rangle$. *On conclut que* $\langle f_1,...,f_s\rangle = \langle h\rangle$.

(iii) Soit $h_1 = \Delta(f_1, \Delta(f_2,...,f_s))$. *On a* h_1 *divise* f_1 *et* $\Delta(f_2,...,f_s)$ *donc* h_1 *divise* f_i $\forall 1 \le i \le s$.

(iv) Algorithme d'Euclide pour chercher $\Delta(f_1,...,f_s)$.

On a $\Delta(f_1,...,f_s) = \Delta(f_1, \Delta(f_2,...,f_s))$, *c'est une relation de récurrence donc il suffit de calculer* $\Delta(f_{s-1}, f_s)$ *puis la remplacer par sa valeur et faire le même travail jusqu'à trouver* $\Delta(f_1,...,f_s)$.

$\Delta(f,g)$:

Initialisation $h = f$; $s = g$, soit p une valeur intermédiaire.

$p :=$ reste de la division de h par s;

$h := s$;

$s := p$;

On répète cette étape jusqu'a $s = 0$.

L'algorithme d'Euclide implique $h = \sum_{i=1}^{s} h_i f_i, h_i \in K[X]$ et par suite $h \in \langle f_1,...,f_s\rangle$.

On conclut que $\langle f_1,...,f_s\rangle = \langle h\rangle$.

2 – Algorithme de division dans $K[X_1,...,X_n]$

Q.A.I : Pour $f \in K[X_1,...,X_n]$ et $I = \langle f_1,..., f_s \rangle$ peut-on décider si $f \in I$?

Pour $n=1$, il suffit de calculer $\Delta = \Delta(f_1,..., f_s)$. On a alors :

$$\begin{aligned} \Delta / f &\Leftrightarrow \exists c \in K[X] \ / \ f = c.\Delta \\ &\Leftrightarrow f \in \langle h \rangle \ / h = \Delta(f_1,..., f_s) \\ &\Leftrightarrow f \in I \end{aligned}$$

Cependant, la question est plus difficile à traiter pour $n>2$.

Par exemple, si on veut savoir si X^2Y+Y appartient à $\langle Y^3+8, XY+2 \rangle \subseteq \mathbb{Q}[X,Y]$.

On a $\Delta(Y^3+8, XY+2)=1$ mais $\langle Y^3+8, XY+2 \rangle \neq \langle 1 \rangle = \mathbb{Q}[X,Y]$.

I1 n'y a pas une identité de Bezout entre Y^3+8 et $XY+2$. En effet si $1 = f(X,Y)(Y^3+8)+(XY+2)g(X,Y)$, on aura en prenant $X=1$ et $Y=-2$, $1=0$, ce qui est absurde.

- Le but est de généraliser 1'algorithme d'Euclide dans $K[X]$ à $K[X_1,...,X_n]$ pour $n \geq 2$. Dans $K[X]$ on ordonne les monômes $X^a >_{lex} X^b$ par leurs degrés et on écrit un polynôme dans l'ordre décroissant des monômes.

Dans $K[X_1,...,X_n]$, on notera un monôme $X_1^{a_1} \cdot ... \cdot X_n^{a_n}$ par X^a avec $a = (a_1,..., a_n)$.

Par exemple $X_1^3 X_2^4 X_3 X_5^2 = X^{(3,4,1,0,2)}$.

Définition 2.1. Un ordre monomial dans $K[X_1,...,X_n]$ est une relation $>$ dans l'ensemble des monômes X^a telle que :

(i) $>$ est un ordre total.

(ii) $X^a > X^b$ implique $X^g X^a > X^g X^b$.

(iii) $X^a > 1 \ \forall X^a \in K[X_1,...,X_n]$; $X^0 = 1$.

Exemple 2.1.

(1) L'ordre usuel dans $K[X]$ est $X^3 > X^2 > X > X^0 = 1$.

(2) L'ordre lexicographique : $X^a >_{lex} X^b$ si la première composante à gauche non nulle $a - b$ de est > 0. Par exemple $X_1 X_2^2 X_3^2 >_{lex} X_2^2 X_3 >_{lex} X_2 X_3^2$.

Notons que si on change l'ordre des variables, l'ordre lexicographique obtenu est différent. Par conséquent il y a $n!$ ordres lexicographiques.

(3) L'ordre lexicographique gradué : $X^a >_{greolex} X^b$ si $|a| = \sum_{i=1}^{n} a_i > |b| = \sum_{i=1}^{n} b_i$ ou $|a| > |b|$ et $X^a >_{lex} X^b$. Par exemple $X_1 X_3^2 >_{greolex} X_2 X_3$, $X_1^2 X_2 >_{greolex} X_2 X_3^2$.

(4) L'ordre lexicographique inversé : $X^a >_{revlex} X^b$ si la dernière composante à gauche non nulle de $a - b$ de est < 0. Par exemple $X_1^3 X_2 >_{revlex} X_2^2 X_3$, $X_1^2 X_2 X_3 >_{revlex} X_1 X_2^2 X_3$.

(5) L'ordre lexicographique inversé gradué : $X^a >_{grevlex} X^b$ si $|a| = \sum_{i=1}^{n} a_i > |b| = \sum_{i=1}^{n} b_i$ ou $|a| > |b|$ et la première composante à droite de $a - b$ de est < 0. Par exemple $X_1^3 X_2 >_{grevlex} X_2 X_3$, $X_1 X_2^2 >_{grevlex} X_1 X_3^2$.

Définition 2.2. Soit $>$ un ordre monomial dans $K[X_1, ..., X_n]$.

Pour $h = \sum_{i=0}^{r} C_i X^{a_i} \neq 0, C_i \in K$, écrit dans l'ordre croissant des monômes c'est-à-dire $X^{a_i} > X^{a_j}$ si $i > j$.

(i) Le monôme dominant de *f* est $LM(f) = X^{a_r}$.

(ii) Le coefficient dominant de *f* est $LC(f) = C_r$.

(iii) Le terme dominant de *f* est $LT(f) = C_r X^{a_r}$.

(iv) Le multidegré de *f* est $mdeg(f) = a_r \in \mathbb{N}^n$.

Lemme 2.1. Soient $f, g \in K[X_1,...,X_n]$ deux polynômes non nuls. On a :

(i) $mdeg(fg) = mdeg(f) + mdeg(g)$.

(ii) Si $f + g \neq 0$ alors $mdeg(f+g) \leq \max(mdeg(f), mdeg(g))$.

➢ On a vu comment la division euclidienne est utilisée pour répondre à la (Q.A.I.) dans $K[X]$. On étudie maintenant ce problème lorsqu'on a plusieurs variables. On donnera un algorithme de division pour les polynômes dans $K[X_1,...,X_n]$ qui étend l'algorithme d'Euclide dans $K[X]$.

Théorème 2.1. (Algorithme de division dans $K[X_1,..., X_n]$)

Soient $f_1,..., f_s \in K[X_1,..., X_n]$ muni d'un ordre monomial $>$.

Alors il existe $q_1,..., q_s \in K[X_1,..., X_n]$ $r \in K[X_1,..., X_n]$ tels que $f = q_1 f_1 + ... + q_s f_s + r$, avec $mdeg(f) = mdeg(q_i f_i)$ si $q_i f_i \neq 0$ et $r = 0$ ou aucun terme de r n'est divisible par l'un des $LT(f_i), 1 \leq i \leq s$.

Preuve

Si $f = 0$ *rien à faire* $0 = 0 f_1 + ... + 0 f_s$.

Si $f \neq 0$

Initialisation : $q_1 := 0, q_2 := 0,..., q_s := 0; p := f; r := 0; i := 1$ *où* p *est une variable intermédiaire représentant la division intermédiaire à chaque étape avec* $f = q_1 f_1 + ... + q_s f_s + p + r$,

(p *change à chaque étape. A la dernière étape, on trouve* $p = 0$*)*.

Etape 1 : Si $LT(f_i) \neq LT(p)$ *alors* $i = i + 1$ *et on refait l'étape 1.*

Si $LT(f_i) \mid LT(p)$ *alors* $q_i := q_i + \frac{LT(p)}{LT(f_i)}$, $p := p - \frac{LT(p)}{LT(f_i)} f_i$.

Si $p = 0$, *c'est terminé. Si non, on refait 1'étape 1.*

Si $i > s$ *on passe à 1'étape 2. On n'arrive à cette étape que lorsque* $LT(f_i) \nmid LT(p)$.

Etape 2 : On pose $r := r + LT(p)$, $p := p - LT(p)$.

L'égalité $f = q_1 f_1 + ... + q_s f_s + r$ *est conservée et* $p = 0$ *ou* $mdeg(p)$ *décroît strictement.*

Si $p = 0$, *c'est termine.*

Si $p \neq 0$, *on refait l'étape 1 et ainsi de suite jusqu'a trouver* $p = 0$.

Input : $f_1, ..., f_s, f$.

Output : $q_1, ..., q_s, r$.

$q_1 := 0;\ q_s := 0;\ p := f\ ;\ r := 0;$

while $p = 0$ *do*

$i := 1$

divisionoccured := false

while $i < s$ *and divisionoccured := false do*

if $LT(f_i)$ *divise* $LT(p)$ *then*

$$q_i := q_i + \frac{LT(p)}{LT(f_i)}$$

$$p := p - \frac{LT(p)}{LT(f_i)} f_i$$

divisionoccured := true

else

$i := i + 1$

if divisionoccured = false then

$r := r + LT(p)$

$p := p - LT(p)$

Exemple 2.2. $f_1 = X^2 + 1,\ f_2 = XY - 1 \in K[X,Y]$. On munit $K[X,Y]$ de l'ordre lexicographique. Divisons $f = X^2Y + Y$ par F :

❖ Pour $F = (f_1, f_2)$:

q_1	q_2	p	r
0	0	$X^2Y + Y$	0
Y	0	0	0

D'où le résultat est $X^2Y + Y = Y \cdot (X^2 + 1) + 0 \cdot (XY - 1) + 0$.

❖ Pour $F = (f_2, f_1)$:

q_1	q_2	p	r
0	0	$X^2Y + Y$	0
0	X	$X + Y$	0
0	X	Y	X
0	X	0	$X + Y$

D'où le résultat est $X^2Y + Y = X \cdot (XY - 1) + 0 \cdot (X^2 + 1) + (X + Y)$.

➢ Le premier résultat montre que $f \in \langle f_2, f_1 \rangle$ mais le deuxième calcul donne un reste non nul. On conclut qu'une telle division est insuffisante pour répondre à la Q.A.I. Pour remédier à ceci, on a besoin du concept de Bases de Gröbner**.**

Exemple 2.3. On ouvre une session Maple :

```
> restart; with(Groebner):
> f1 := x^2+1;
```

$$f1 := x^2 + 1$$

```
> f2 := x*y-1;
```

$$f2 := xy - 1$$

```
> f := x^2*y+y;
```

$$f := x^2 y + y$$

```
> normalf(f, [f1,f2], plex(x,y));
```

$$0$$

```
> normalf(f, [f2,f1], plex(x,y));
```

$$y + x$$

Exemple 2.4. Pour $f_1 = x^2 + y$, $f_2 = xy - x \in K[X,Y]$. On munit $K[X,Y]$ de l'ordre lexicographique. On divisons $f = X^2Y^2 + Y$ par (f_1, f_2) puis (f_2, f_1) :

```
> restart; with(Groebner):
> f1 := x^2+y;
```

$$f1 := x^2 + y$$

```
> f2 := x*y-x;
```

$$f2 := xy - x$$

```
> f := x^2*y^2+y;
```

$$f := x^2 y^2 + y$$

```
> normalf(f, [f1,f2], plex(x,y));
```

$$y - y^3$$

```
> normalf(f, [f2,f1], plex(x,y));
```

$$0$$

3 – Bases de Gröbner

Définition 3.1. Fixons un ordre monomial dans $K[X_1,...,X_n]$ et considérons un idéal I de $K[X_1,...,X_n]$.

Soit G une partie finie de $K[X_1,...,X_n]$ et I un idéal engendré par cette partie. On dira que G est une base de Gröbner si $\langle LT(g_1),...,LT(g_s)\rangle = \langle LT(f), f \in I\rangle := LT(I)$.

Proposition 3.1. Si $G = \{g_1,...,g_s\}$ est une base de Gröbner de I alors $I = \langle G\rangle = \langle g_1,...,g_s\rangle$.

Preuve

On a $\langle g_1,..., g_s\rangle \subseteq I$ *car* $g_i \in I$.

Soit $f \in I$. *En divisant par G on obtient :* $f = q_1 f_1 + ... + q_s f_s + r$ *avec* $r = 0$ *ou tous les termes de r ne sont divisibles par aucun des* $LT(g_i)$.

Si $r \neq 0$, *puisque* $r \in I$ *alors* $LT(r) = h_1 LT(g_1) + ... + h_s LT(g_s)$ *avec* $h_i \in K[X_1,..., X_n]$. *Alors le terme dominant de r est divisible par l'un des* $LT(g_i)$ *(voir Lemme 3.1), ce qui est faux. Donc* $r = 0$ *et* $f \in \langle g_1,...g_s\rangle$.

Définition 3.2. Un idéal de $K[X_1,..., X_n]$ non nul est dit monomial s'il est engendre par des monômes (pas nécessairement en nombre fini).

Lemme 3.1. $X^b \in \langle X^a, a \in \Gamma \subseteq \mathbb{N}^n\rangle = I \Leftrightarrow \exists a \in \Gamma$ tel que X^a / X^b.

Preuve

$"\Leftarrow"$ $X^a / X^b \Rightarrow X^b \in I$.

$"\Rightarrow"$ *On a* $X^b = \sum_{i=1}^{s} h_i X^{a(i)}$, $h_i \in K[X_1,..., X_n]$, $a(i) \in \Gamma$. *En écrivant les* h_i *comme somme des termes et en développant le second membre, on déduit que tous les termes du second membre sont divisibles par un certain* $X^{a(i)}$, *donc de même pour* X^b.

Proposition 3.2. (Lemme de Dickson) Tout idéal monomial dans $K[X_1,..., X_n]$ est engendré par un nombre fini de monômes.

Théorème 3.1. Soit I un idéal non nul de $K[X_1,..., X_n]$, alors I possède une base de Gröbner pour n'importe quel ordre monomial.

On vient de voir que tout idéal non nul de $K[X_1,...,X_n]$ possède une base de Gröbner. Dans la suite on va construire effectivement une telle base et montrer qu'avec les bases de Gröbner on peut répondre à la Q.A.I..

Proposition 3.3. Soient $G=\{g_1,...,g_s\}$ une base de Gröbner d'un idéal non nul $I\subseteq K[X_1,...,X_n]$ et $f\in K[X_1,...,X_n]$, alors il existe un unique $r\in K[X_1,...,X_n]$ vérifiant :

(i) $r=0$ ou aucun terme de *r* n'est divisible par l'un des $LT(g_i)$.

(ii) $\exists\, g\in I$ tel que $f=g+r$. En particulier, r est le reste de la division de f par $\{g_1,...,g_s\}$ (indépendamment de l'ordre des g_i).

Preuve

Existence : Par l'algorithme de division.

Unicité : Supposons que $f=g_1+r_1=g_2+r_2$. *Cela implique que* $r_2-r_1\in I$.

Si $r_2\neq r_1$, $LT(r_2-r_1)\in\langle LT(g_1),...,LT(g_s)\rangle$. *Le lemme 4.1 implique qu'il existe i tel que* $LT(g_i)/LT(r_2-r_1)$. *Ce qui est impossible car les termes de* r_1 *et de* r_2 *ne sont pas divisibles par aucun des* $LT(g_i)$. *On a donc* $r_1=r_2$ *et* $g_1=g_2$.

Corollaire 3.1. (Q.A.I) Soient $G=\{g_1,...,g_s\}$ une base de Gröbner d'un idéal non nul $I\subseteq K[X_1,...,X_n]$ et $f\in K[X_1,...,X_n]$. Alors $f\in I\Leftrightarrow$ le reste de la division de *f* par *G* est nul.

Preuve

$"\Rightarrow"$ $f\in I\Rightarrow f=f+0\Rightarrow r=0$ *: Le reste de la division de f par G (par unicité, voir Proposition 3.3).*

$"\Leftarrow"$ *Si* $r=0$, $f\in\langle g_1,...g_s\rangle$.

Definition 3.3. $f, g \in K[X_1,..., X_n] \setminus \{0\}$.

(i) Notons $mdeg(f) = a$ et $mdeg(g) = b$. Posons $g = (g_1,..., g_n)$ avec

$g_i = max(a_i, b_i)$.

On note $X^g = LCM(LM(f), LM(g))$ le plus petit multiple commun de X^a et X^b.

(ii) On définit $S(f,g)$ par $S(f,g) = \frac{X^g}{LT(f)} f - \frac{X^g}{LT(g)} g$.

Remarquons que $mdegS(f,g) < g$. Par le lemme suivant on montrera que c'est une spécificité des S-paires $S(f,g)$.

Lemme 3.2. Supposons que $mdeg\left(\sum_{i=1}^{t} c_i f_i\right)$ avec $c_i \in K$, $f_i \in K[X_1,..., X_n]$ et

$mdeg(f_i) = g \quad \forall 1 \le i \le t$. Alors $\sum_{i=1}^{t} c_i f_i$ est une combinaison linéaire à coefficients dans K

des $S(f_i, f_j)$, $1 \le i, j \le t$.

Preuve

Posons $d_i = LC(f_i)$. *Puisque* $mdeg\left(\sum_{i=1}^{t} c_i f_i\right) < g$, *on a* $\sum_{i=1}^{t} c_i d_i = 0$.

$$\left.\begin{array}{l} mdeg(f_i) = g \\ mdeg(f_j) = g \end{array}\right\} \Rightarrow LCM(LM(f_i), LM(f_j)) = X^g$$

$$\Rightarrow S(fi, fj) = \frac{X^g}{d_i X^g} f_i - \frac{X^g}{d_j X^g} f_j = \frac{f_i}{d_i} - \frac{f_j}{d_j}.$$

Posons $p_i = \frac{f_i}{d_i}$, *on a* $S(f_i, f_j) = p_i - p_j$.

Ainsi

$$\begin{aligned}\sum_{i=1}^{t} c_i f_i &= \sum_{i=1}^{t} c_i d_i p_i \\ &= c_1 d_1 (p_1 - p_2) + (c_2 d_2 + c_1 d_1)(p_1 - p_2) + \ldots + (c_1 d_1 + \ldots + c_{t-1} d_{t-1})(p_{t-1} - p_t) \\ &+ (c_1 d_1 + \ldots + c_{t-1} d_{t-1} + c_t d_t) p_t \\ &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \ldots + (c_1 d_1 + \ldots + c_{t-1} d_{t-1}) S(f_{t-1}, f_t).\end{aligned}$$

Théorème 3.2. (Critère de Buchberger par les S-paires)

Soient I un idéal non nul de $K[X_1,\ldots,X_n]$ et G une base de I $(G=\{g_1,\ldots,g_s\}, I=\langle g_1,\ldots,g_s\rangle)$.

Alors G est une base de Gröbner pour I si et seulement si les restes des divisions des $S(g_i, g_j)$ par G sont tous nuls.

Exemple 3.1. Soit $I=\langle Z^2+X^2, X+Y\rangle$, montrons que $G=\{Z^2+X^2, X+Y\}$ est une base de Gröbner pour I où l'ordre est $>_{lex}$ avec $Y>Z>X$.

$G=\{Z^2+X^2, X+Y\}$,

$LM(Z^2+X^2)=Z^2$,

$LM(X+Y)=Y$,

$LCM(LM(Z^2+X^2), LM(X+Y))=YZ^2$,

$$\begin{aligned}S(Z^2+X^2, X+Y) &= \frac{YZ^2}{Z^2}(Z^2+X^2) - \frac{YZ^2}{Y}(X+Y) \\ &= YZ^2 + YX^2 - Z^2X - YZ^2 = YX^2 - Z^2X.\end{aligned}$$

En effectuant la division de $S\left(Z^2+X^2, X+Y\right)$ par *G* on aura :

$YX^2 - Z^2X = Y\left(Z^2+X^2\right) - Z^2\left(X+Y\right) + 0$, donc *G* est une base de Gröbner de *I.*

Si on suppose que $X > Y > Z$, on aura :

$LM\left(Z^2+X^2\right) = X^2$,

$LM\left(X+Y\right) = X$,

$LCM\left(LM\left(Z^2+X^2\right), LM\left(X+Y\right)\right) = X^2$,

$S\left(Z^2+X^2, X+Y\right) = \frac{X^2}{X^2}\left(Z^2+X^2\right) - \frac{X^2}{X}\left(X+Y\right) = Z^2 - XY$.

On divise $Z^2 - XY$ par *G*, on obtient : $Z^2 - XY = 0\cdot\left(Z^2+X^2\right) - Y\cdot\left(X+Y\right) + Z^2 + Y^2$.

On voit que le reste de la division est différent de zéro, ce qui traduit que *G* n'est pas une base de Gröbner pour *I.*

Théorème 3.3. (Algorithme de Buchberger) Soit $I = \langle f_1, ..., f_s \rangle$ un idéal non nul de $K[X_1, ..., X_n]$ dans lequel on a fixe un ordre monomial. Alors une base de Gröbner de *I* peut être calculée après un nombre fini d'étapes par l'algorithme suivant :

Input : $F = \{f_1, ..., f_t\}$.

Output : *G* une base de Gröbner de *I* avec $F \subset G$.

Etape 0 : Initialisation $G := F$

Etape 1 : $G' := F$ puis on effectue toutes les divisions des G' pour tous $f, g \in G'$.

Si le reste *r* de la division de $S(f, g)$ par G' est non nul on pose $G := G \cup \{r\}$.

Etape 2 : Si $G' = G$, on arrête. Si non on refait l'étape 1.

Notons $\overline{S(p,q)}^G$ le reste de la division de $S(p,q)$ par *G*, l'algorithme s'écrit :

Input : $F = \{ f_1,..., f_t \}$.

Output : G une base de Gröbner pour I, avec $F \subset G$.

$G := F$

REPEAT

$G' := G$ for each pair p, q, $p \neq q$ in G' DO

$S := \overline{S(p,q)}^{G}$ IF $S \neq 0$ THEN $G' := G \cup \{S\}$

UNTIL $G = G'$.

Preuve

Pourquoi $G \subset I$ *?*

A l'initialisation $G = F \subset I$.

A chaque étape i, on élargit G_i *en ajoutant un reste* r_i *de la division d'un certain* $S(f,g)$ *par* G_i.

$f, g \in I \Rightarrow S(f,g) \in \langle f, g \rangle \subset I$. *Comme* $G_i \subset I$, $r_i \in I$ *et* $G_{i+1} \subset I$.

Pourquoi cet algorithme s'arrête-t-il ?

Si a une étape i 1'algorithme ne s'arrête pas c'est qu' on a ajoute a G_i *un reste* r_i *non nul.*

Pour $G_i = \{ g_1,..., g_s \}$, *on note* $\langle LT(G_i) \rangle = \langle LT(g_{t_1},..., g_{t_i}) \rangle$.

Si $LT(r_i)$ *n'est divisible par aucun* $LT(g_{t_1}),..., LT(g_{t_i})$ *alors* $LT(r_i)$ *n'appartient pas à* $\langle LT(g_{t_1}),..., LT(g_{t_i}) \rangle$. *Ce qui implique* $G_{i+1} := G_i \cup \{r\}$ *et* $\langle LT(G_i) \rangle \subset \langle LT(G_{i+1}) \rangle$.

Puisque $K[X_1,..., X_n]$ *est noethérien, l'algorithme doit s'arrêter après un nombre fini d'étapes. En effet, un anneau A est dit noethérien si toute suite croissante d'idéaux et stationnaire (devient constante après un nombre fini d'étapes).*

- Le code Maple suivant implémente l'algorithme de Buchberger :

```
groebnerBasis:= proc( polys::list(polynom), vars::list (name) )
local B, GB, p, h, i, j, f ;
with (grobner, normalf) ; with (grobner, spoly) ;
B := [ seq( seq( [polys [i], polys [j] ], i = 1..j − 1 ), j = 2..nops(polys) ) ] ;
GB:= polys ;
while not B = [] do
        P := B[1] ;
        B:= B[2.. −1] ;
        h := normalf( spoly( p[1], p[2], vars, plex), GB, vars, plex ) ;
        if h <> 0
        then GB:= [op(GB), h] ;
                B:= [op(B), seq( [f,h], f = GB ) ] ;
        fi ;
od ;
GB
end ;
```

Remarque 3.1. On remarque que la partie stable engendrée par les monômes de tête des éléments de G croît strictement à chaque disjonction dans G. En considérant les idéaux engendrés successivement par cette partie stable, on obtient ainsi une suite strictement croissante d'idéaux.

Par exemple si à l'étape i, $G_i = \{g_1,...,g_s\}$, alors pour l'étape suivante les restes resteront non nuls.

Si $G_{i+1} = \{g_1,...,g_{i+1}\}$, on cherche seulement les restes des divisions de $S(g_{i+1}, g_k)$ par G_{i+1} avec $1 \le k \le i$.

4 – Base de Gröbner réduite

Lemme 4.1. Soit G une base de Gröbner pour un idéal non nul I de $K[X_1,...,X_n]$. Soit $p \in G$ tel que $LT(P) \in \langle LT(G \setminus \{p\}) \rangle$, alors $G \setminus \{p\}$ est aussi une base de Gröbner pour I.

Preuve

Soit $f \in I$, *puisque* $\langle LT(I)\rangle = \langle LT(G)\rangle$, $LT(f)$ *est divisible par un certain* $LT(p')$, $p' \in G$.

Si $p' \neq p$, *c'est O.K.*

Si $p' = p, LT(p') = LT(p)$ *est divisible par un certain* $LT(p'')$, $p'' \in G \setminus \{p\}$. *Donc* $\langle LT(I)\rangle = \langle LT(G) \setminus \{p\}\rangle$.

En multipliant les éléments d'une base de Gröbner de I par des constantes convenables pour rendre leurs $LC = 1$ et en éliminant de G chaque p tel que $LT(p) \in \langle LT(G \setminus \{p\})\rangle$, on arrive à ce qu'on appelle base de Gröbner minimale pour I.

Définition 4.1. Une base de Gröbner minimale pour un idéal I de $K[X_1,...,X_n]$ est une base de Gröbner pour I telle que :

(i) $\forall p \in G,\ LC(p) = 1$.

(ii) $\forall p \in G,\ LT(p) \notin \langle LT(G \setminus \{p\})\rangle$.

Lemme 4.2. Soient G et G' deux bases de Gröbner minimales pour un même idéal I alors $LT(G) = LT(G')$ et G et G' ont le même nombre d'élément.

Preuve

Soit $p \in G$. *On sait qu'il* $\exists\, p' \in G'$ *tel que* $LT(p') / LT(p)$ *et* $\exists\, p'' \in G$ *tel que* $LT(p'') / LT(p)$ *(*car G et G' sont deux bases de Gröbner pour I*).*

Donc $LT(p'') / LT(p)$. *Or* $LT(p) \notin \langle LT(G \setminus \{p\})\rangle$ *par suite* $p'' = p$.

Comme $LT(p') / LT(p)$, $LT(p) / LT(p')$ *et* $LC(p') = LC(p) = 1$ *on a forcément* $LC(p') = LC(p)$, *on déduit alors que* $LT(G) \subseteq LT(G')$.

De même, $LT(G') \subseteq LT(G)$ *donc* $LT(G) = LT(G')$.

Puisque la notion de base de Gröbner minimale n'assure pas son unicité, on introduit la notion de base de Gröbner réduite.

Définition 4.2. Une base de Gröbner réduite pour un idéal I de $K[X_1,...,X_n]$ est une base de Gröbner pour I telle que :

(i) $\forall p \in G,\ LC(p) = 1$.

(ii) $\forall p \in G$, aucun monôme de p n'appartient à $\langle LT(G \setminus \{p\}) \rangle$.

Théorème 4.1. Soient I un idéal non nul de $K[X_1,...,X_n]$ et G une base de Gröbner minimale pour I pour un ordre monomial fixé, alors il existe une unique base de Gröbner réduite pour I.

En introduisant la fonction $remainder(f; g_1,..., g_s) =$ le reste de la division de f par $g_1,..., g_s$, l'algorithme est :

Input : $g_1,..., g_s$.

Output : $\tilde{g}_1,..., \tilde{g}_s$.

IF $s = 1$ THEN $\tilde{g}_1 := g_1$;

ELSE

IF $s = 2$ THEN $\tilde{g}_1 := remainder(g_1; g_2)$; $\tilde{g}_2 := remainder(g_2; \tilde{g}_1)$;

ELSE

$\tilde{g}_1 := remainder(g_1; g_2,..., g_s)$; $\tilde{g}_2 := remainder(g_2; \tilde{g}_1, g_3,..., g_s)$;

$i := 3$;

WHILE $i \le s$ DO $\tilde{g}_i := remainder(g_i; \tilde{g}_1,..., \tilde{g}_{i-1}, g_{i+1}..., g_s)$; $i := i+1$;

Preuve

Existence : Soient $g \in G$ *et* g' *le reste de la division de g par* $G \setminus \{g\}$, *posons* $G' = (G \setminus \{g\}) \cup \{g'\}$.

Lorsqu'on divise g par $G \setminus \{g\}$, $LT(G)$ *va du côté du reste puisque* $LT(g)$ *n'appartient pas à* $\langle LT(G \setminus \{g\}) \rangle$. *Donc* $LT(g) = LT(g')$, $LT(G) = LT(G')$ *et* G' *une base de Gröbner minimale pour I.*

Puisque g' *est le reste de la division de g par* $G \setminus \{g\}$, *aucun monôme de* g' *n'appartient à* $LT(G \setminus \{g\}) = LT(G')$, *on dira que* g' *est réduit pour* G'.

Notons que si g est réduit pour G alors il reste réduit pour n'importe quelle autre base minimale G' *pour I contenant g et tel que* $LT(G') = LT(G)$.

On prend $g_1 \in G$ *et on remplace G par* $G_1 = G \setminus \{g_1\} \cup \{\tilde{g}_1\}$ *avec* g_1 *est le reste de la division de* g_1 *par G. On note que* g_1 *est réduit pour* G_1.

Ensuite on prend $g_2 \in G_1 \setminus \{\tilde{g}_1\}$ *et on pose* $G_2 = G \setminus \{g_2\} \cup \{\tilde{g}_2\}$ *avec* g_2 *est le reste de la division de* g_2 *par* G_1. *On note que* $\tilde{g}_1$ *et* $\tilde{g}_2$ *sont réduits pour* G_2, *et ainsi de suite.*

Puisque $|G|$ *est fini, après un nombre fini d'étapes on arrive à une base de Gröbner réduite pour I.*

Unicité : Supposons que G et G' sont deux bases de Gröbner réduites pour I. D'après le dernier lemme 4.2, on a $LT(G') = LT(G'')$ *et* $|G'| = |G''|$.

Soit $g' \in G'$. *On sait qu'il existe* $g'' \in G''$ *tel que* $LT(g') = LT(g'')$, $g' \in I$ *et* $g'' \in I$. *Ce qui implique* $g' - g'' \in G$ *et par suite le reste de la division de* $g' - g''$ *par g est nul.* (1)

Or $LT(g') = LT(g'')$, *donc aucun monôme de* g' *ni de* g'' *n'est divisible par un élément de* $LT(G \setminus \{g'\}) = LT(G \setminus \{g''\})$. *En outre, dans* $g' - g''$ *où le terme dominant se simplifie, aucun monôme n'est divisible par un élément de* $LT(G') = LT(G'')$, *donc le reste de la division de* $g' - g''$ *par G est égal à* $g' - g''$. (2)

(1) *et* (2) *impliquent que* $g' - g'' = 0$, *c'est-à-dire* $g' = g''$. *Finalement, comme* $G' \subseteq G''$ *et* $|G'| = |G''|$, *on* $G' = G''$.

Exemple 4.1. Exemple de base de Gröbner réduite $G = \{Z, Y^2, XY, X^2 - Y\}$ est une base de Gröbner réduite pour l'idéal $I = \langle G \rangle$. En effet on a :

❖ $S(Z, Y^2) = \frac{ZY^2}{Z} \cdot Z - \frac{ZY^2}{Y^2} \cdot Y^2 = 0$.

$S(Z, XY) = \frac{ZXY}{Z} \cdot Z - \frac{ZXY}{XY} \cdot XY = 0$.

$$S(Z, X^2 - Y) = \frac{ZX^2}{Z} \cdot Z - \frac{ZX^2}{X^2} \cdot (X^2 - Y)$$
$$= YZ = Y \cdot Z + 0 \cdot Y^2 + 0 \cdot XY + 0 \cdot (X^2 - Y) + 0.$$

$S(Y^2, XY) = \frac{XY^3}{Y^2} \cdot Y^2 - \frac{XY^3}{XY} \cdot XY = 0.$

$$S(Y^2, X^2 - Y) = \frac{X^2Y^2}{Y^2} \cdot Y^2 - \frac{X^2Y^2}{X^2} \cdot (X^2 - Y)$$
$$= Y^3 = 0 \cdot Z + Y \cdot Y^2 + 0 \cdot XY + 0 \cdot (X^2 - Y) + 0.$$

$$S(XY, X^2 - Y) = \frac{X^2Y}{XY} \cdot XY - \frac{X^2Y}{X^2} \cdot (X^2 - Y)$$
$$= Y^2 = 0 \cdot Z + 1 \cdot Y^2 + 0 \cdot XY + 0 \cdot (X^2 - Y) + 0.$$

❖ $Z \notin \langle Y^2, XY, X^2 - Y \rangle$ car Z n'est pas divisible par Y^2 ni par XY ni par $X^2 - Y$.

$Y^2 \notin \langle Z, XY, X^2 - Y \rangle$ car Y^2 n'est pas divisible par Z ni par XY ni par $X^2 - Y$.

$XY \notin \langle Z, Y^2, X^2 - Y \rangle$ car XY n'est pas divisible par Z ni par Y^2 ni par $X^2 - Y$.

$X^2 \notin \langle Z, Y^2, XY \rangle$ car X^2 n'est pas divisible par Z ni par Y^2 ni par XY.

$-Y \notin \langle Z, Y^2, XY \rangle$ car $-Y$ n'est pas divisible par Z ni par Y^2 ni par XY.

❖ $LC(Z) = LC(Y^2) = LC(XY) = LC(X^2 - Y) = 1$.

➢ **Exemple 4.2.** On ouvre une session Maple pour calculer une base de Gröbner réduite :

```
> restart; with(Groebner):

> f1 := x^2-z^2;
```

$$f1 := x^2 - z^2$$

```
> f2 := y+z-x;
```

$$f2 := y + z - x$$

```
> f3 := x^2+y^2- z;
```

$$f3 := x^2 + y^2 - z$$

```
> gbasis([f1,f2,f3], plex(x,y,z));
```

$$\left[5z^3 - 6z^2 + z, -z^2 + z + 2yz, y^2 - z^2 - z, -y - z + x\right]$$

D'où $G = \left\{5z^3 - 6z^2 + z, -z^2 + z + 2yz, y^2 - z^2 - z, -y - z + x\right\}$ est une base de Gröbner réduite pour l'idéal $I = \langle G \rangle$.

➢ En particulier, on peut donner un test algorithmique d'appartenance d'un polynôme *f* à un idéal donné présenté par un système fini de générateurs $g_1, ..., g_s$: il suffit de tester la nullité du reste de *f* par réduction, ce qui est résumé comme suit.

Algorithme (Test d'appartenance à un idéal polynômial)

Input : un polynôme *f* et des polynômes non nuls $p_1,...,p_s$ engendrant un idéal *I.*

Output : une variable booléenne indiquant si *f* est un élément de *I.*

(i) Choisir un ordre monomial > sur $K[X_1,...,X_n]$.

(ii) Calculer une base de Gröbner $G=\{g_1,...,g_s\}$ de I pour cet ordre.

(iii) Effectuer la réduction de *p* par *G* .

(iv) Si le reste est nul, répondre VRAI, si non répondre FAUX.

5 – Applications des bases de Gröbner

En plus de répondre à la Q.A.I, les bases de Gröbner sont utilisées pour résoudre d'autres problèmes.

5 – 1 – Résolution des systèmes d'équations polynomiales

En utilisant les bases de Gröbner, on peut réduire le problème de résolution d'un système d'équations polynomiales à trouver les racines d'un polynôme à une variable.

Soit $I=\langle f_1,...,f_s\rangle \subseteq K[X_1,...,X_n]$ ($K=\mathbb{R}$ ou $\mathbb{C}$) et considérons le système d'équations $f_1=...=f_s=0$.

I est dit résoluble s'ils existent $a_1,...,a_n$ dans $\mathbb{C}$ tels que $f_i(a_1,...,a_n)=0 \ \forall i=1,...,s$.

On introduit $G=\{g_1,...,g_t\}$ une base de Gröbner réduite de *I* par rapport à un ordre lexicographique. Alors :

(i) *I* n'a pas de solution si et seulement si $G=\{1\}$.

(ii) *I* a un nombre fini de solution si et seulement si $\forall i=1,...,n$, une puissance pure $X_i^{a_i}$ paraît comme $LM(g_i)$ pour un $j=1,...,k$.

(iii) Si *I* est résoluble avec un nombre fini de solution, alors *G* contient un polynôme *g* à une seule variable.

Après la recherche des racines de *g*, les solutions du système $f_1 = ... = f_s = 0$ peuvent être trouvées en substituant les racines de *g* par celles des polynômes de *G*.

Exemple 5.1.1. Supposons qu'on cherche dans $\mathbb{R}$ les solutions du systeme d'équations suivant :

$$\begin{cases} X^2 - Y = 1 \\ X^3 + 2X^2 + 2X - Y^2 = -1 \end{cases}$$

On définit *I* par $I = \left\langle X^2 - Y - 1, X^3 + 2X^2 + 2X - Y^2 + 1 \right\rangle \subset \mathbb{R}[X, Y]$.

On applique l'algorithme de Buchberger en respectant l'ordre lexicographique $X > Y$.

On obtient une base de Gröbner réduite pour *I* :

$G = \left\{ Y^4 - 5Y^3 - 9Y^2 - 3Y, 12X + Y^3 - 8Y^2 + 3Y + 12 \right\}$.

Comme $G \neq \{1\}$, le système a des solutions dans $\mathbb{C}^2$.

Puisque Y^4 est le monôme dominant du premier élément de *G* et *X* du deuxième, le système a un nombre fini de solutions. Le premier polynôme de *G* étant à une seule variable, on peut déterminer ses racines réelles qui sont 0 , -1, $3+2\sqrt{3}$ et $3-2\sqrt{3}$. On remplace ces valeurs dans le premier polynôme. On obtient :

$$\begin{cases} Y = 0 \\ 12X + 12 = 0 \end{cases}, \begin{cases} Y = -1 \\ 12X = 0 \end{cases}, \begin{cases} Y = 3+2\sqrt{3} \\ 12X - 12\left(1+\sqrt{3}\right) = 0 \end{cases} \text{ et } \begin{cases} Y = 3-2\sqrt{3} \\ 12X - 12\left(1-\sqrt{3}\right) = 0 \end{cases}.$$

$$\Rightarrow \begin{cases} Y = 0 \\ X = -1 \end{cases}, \begin{cases} Y = -1 \\ X = 0 \end{cases}, \begin{cases} Y = 3+2\sqrt{3} \\ X = 1+\sqrt{3} \end{cases} \text{ et } \begin{cases} Y = 3-2\sqrt{3} \\ X = 1-\sqrt{3} \end{cases}.$$

Par suite, il y a quatre solutions pour le système d'équations donné qui sont $(0,-1)$, $(-1,0)$, $\left(3+2\sqrt{3}, 1+\sqrt{3}\right)$ et $\left(3-2\sqrt{3}, 1-\sqrt{3}\right)$.

Exemple 5.1.2. Résolution du système à trois variables :

Soit

$$\begin{cases} -x^2 + y + z^2 = -2 \\ x^2 + y^2 - z = 3 \\ x^2 - y + z = 2 \end{cases}$$

On résout dans $\mathbb{C}^3$ ce système par la même méthode que l'exemple 6.1.1. en ouvrant la session Maple suivante :

```
> restart; with(Groebner):
```

```
> f1 := -x^2+y+z^2+2;
```

$$f1 := -x^2 + y + z^2 + 2$$

```
> f2 := x^2+y^2-z-3;
```

$$f2 := x^2 + y^2 - z - 3$$

```
> f3 := x^2-y+z-2;
```

$$f3 := x^2 - y + z - 2$$

```
> G:=gbasis([f1,f2,f3], plex(x,y,z));
```

$$G := \left[z + z^2,\ y^2 - 2z - 1 + y,\ x^2 - y + z - 2 \right]$$

```
> g1:=op(1,G);
```

$$g1 := z + z^2$$

```
> g2:=op(2,G);
```

$$g2 := y^2 - 2z - 1 + y$$

```
> g3:=op(3,G);
```

$$g3 := x^2 - y + z - 2$$

```
> s:=solve(g1);
```

$$s := 0, -1$$

Premier cas : pour z = 0

```
> z:=s[1];
```

$$z := 0$$

```
> expand(g2);
```

$$y^2 - 1 + y$$

```
> ys:=solve(g2);
```

$$ys := -\frac{1}{2} + \frac{\sqrt{5}}{2}, -\frac{1}{2} - \frac{\sqrt{5}}{2}$$

Pour y=y1

```
> y:=ys[1];
```

$$y := -\frac{1}{2} + \frac{\sqrt{5}}{2}$$

```
> expand(g3);
```

$$x^2 - \frac{3}{2} - \frac{\sqrt{5}}{2}$$

```
> x:=solve(g3);
```

$$x := \frac{\sqrt{5}}{2} + \frac{1}{2}, -\frac{1}{2} - \frac{\sqrt{5}}{2}$$

Pour y=y2

```
> x:='x'; y:='y';
```

$$x := x$$
$$y := y$$

```
> y:=ys[2];
```

$$y := -\frac{1}{2} - \frac{\sqrt{5}}{2}$$

```
> expand(g3);
```

$$x^2 - \frac{3}{2} - \frac{\sqrt{5}}{2}$$

```
> x:=solve(g3);
```

$$x := -\frac{1}{2} + \frac{\sqrt{5}}{2}, \frac{1}{2} - \frac{\sqrt{5}}{2}$$

Deuxième cas : pour z = -1

```
> x:='x'; y:='y'; z:='z'; ys:='ys';
```

$$x := x$$
$$y := y$$
$$z := z$$
$$ys := ys$$

```
> z:=s[2];
```

$$z := -1$$

```
> expand(g2);
```

$$y^2 + 1 + y$$

```
> ys:=solve(g2);
```

$$ys := -\frac{1}{2}+\frac{1}{2}I\sqrt{3}, -\frac{1}{2}-\frac{1}{2}I\sqrt{3}$$

Pour y=y1

```
> y:=ys[1];
```

$$y := -\frac{1}{2}+\frac{1}{2}I\sqrt{3}$$

```
> expand(g3);
```

$$x^2 - \frac{5}{2} - \frac{1}{2}I\sqrt{3}$$

```
> x:=solve(g3);
```

$$x := \frac{\sqrt{10+2I\sqrt{3}}}{2}, -\frac{\sqrt{10+2I\sqrt{3}}}{2}$$

Pour y=y2

```
> x:='x'; y:='y';
```

$$x := x$$
$$y := y$$

```
> y:=ys[2];
```

$$y := -\frac{1}{2}-\frac{1}{2}I\sqrt{3}$$

```
> expand(g3);
```

$$x^2 - \frac{5}{2} + \frac{1}{2}I\sqrt{3}$$

```
> x:=solve(g3);
```

$$x := \frac{\sqrt{10-2I\sqrt{3}}}{2}, -\frac{\sqrt{10-2I\sqrt{3}}}{2}$$

➢ D'après le session Maple ci-dessus on obtient deux solutions pour *z* et pour chacune de ces valeurs on obtient deux solutions pour *y*, et de même on obtient pour chacune de ces dernières deux solutions pour *x*.

Ce qui nous donnes les huit solutions suivantes : $\left(\frac{\sqrt{5}}{2}+\frac{1}{2}, -\frac{1}{2}+\frac{\sqrt{5}}{2}, 0\right)$,

$\left(-\frac{1}{2}-\frac{\sqrt{5}}{2}, -\frac{1}{2}+\frac{\sqrt{5}}{2}, 0\right)$, $\left(-\frac{1}{2}+\frac{\sqrt{5}}{2}, -\frac{1}{2}-\frac{\sqrt{5}}{2}, 0\right)$, $\left(\frac{1}{2}-\frac{\sqrt{5}}{2}, -\frac{1}{2}-\frac{\sqrt{5}}{2}, 0\right)$,

$$\left(\frac{\sqrt{10+2I\sqrt{3}}}{2},-\frac{1}{2}+\frac{1}{2}I\sqrt{3},-1\right),\left(-\frac{\sqrt{10+2I\sqrt{3}}}{2},-\frac{1}{2}+\frac{1}{2}I\sqrt{3},-1\right),$$

$$\left(\frac{\sqrt{10-2I\sqrt{3}}}{2},-\frac{1}{2}-\frac{1}{2}I\sqrt{3},-1\right) \text{ et } \left(-\frac{\sqrt{10-2I\sqrt{3}}}{2},-\frac{1}{2}-\frac{1}{2}I\sqrt{3},-1\right).$$

6 – Résultant de deux polynômes

Définition 3.1. [3] Soient $f_1 = a_0X^l + a_1X^{l-1} + ... + a_l,\ a_0 \neq 0,\ a_i \in R$

$$f_2 = b_0X^m + b_1X^{m-1} + ... + b_m,\ b_0 \neq 0,\ b_i \in R,\ R = K[X_1,...,X_n]$$

Le résultant de f_1 et f_2 noté $Res_X(f_1, f_2)$ est le déterminant de la matrice $(m+l)\times(m+l)$ suivante appelée matrice de Sylvester :

$$Syl(f_1, f_2, X) = \begin{pmatrix} a_0 & & & & b_0 & & & & \\ a_1 & a_0 & & & b_1 & b_0 & & & \\ a_2 & a_1 & \ddots & & \vdots & b_1 & \ddots & & \\ \vdots & & \ddots & a_0 & b_m & & \ddots & \ddots & \\ a_l & \vdots & & a_1 & & b_m & & \ddots & b_0 \\ & a_l & & \vdots & & & \ddots & & b_1 \\ & & \ddots & \vdots & & & & \ddots & \vdots \\ & & & a_l & & & & & b_m \end{pmatrix}.$$

Proposition 6.1. Il existe $g_1,\ g_2 \in R[X]$ tel que $g_1f_1 + g_2f_2 = Res_X(f_1, f_2) \in R$ avec $deg(g_1) \leq m-1$ et $deg(g_2) \leq l-1$.

Preuve

$f_1 = a_0X^l + a_1X^{l-1} + ... + a_l,\ a_0 \neq 0,\ a_i \in R$.

$f_2 = b_0X^m + b_1X^{m-1} + ... + b_m,\ b_0 \neq 0,\ b_i \in R$.

On a les égalités suivantes :

$$
\begin{aligned}
&X^{m-1} f_1 = a_0 X^{l+m-1} + \ldots + a_l X^{m-1} && (1)\\
&X^{m-2} f_1 = a_0 X^{l+m-2} + \ldots + a_l X^{m-2} && (2)\\
&\vdots\\
&X f_1 = a_0 X^{l+1} + \ldots + a_l X && (m-1)\\
&X^0 f_1 = a_0 X^{l} + \ldots + a_l && (m)\\
&X^{l-1} f_2 = b_0 X^{m+l-1} + \ldots + b_m X^{l-1} && (m+1)\\
&\vdots\\
&X^0 f_2 = b_0 X^{m} + \ldots + b_m && (m+l)
\end{aligned}
$$

Notons $a_1, \ldots, a_{m+l}$ *les cofacteurs de* $Syl(f_1, f_2, X)$ *obtenus en développant selon la* $(l+m)^{ème}$ *ligne.*

En multipliant chaque égalité (i) *par* a_i *et en faisant la somme, on obtient :*

$$
\begin{aligned}
&\left(a_1 X^{m-1} + a_2 X^{m-2} + \ldots + a_m\right) f_1 + \left(a_{m+1} X^{l-1} + a_{m+2} X^{l-2} + \ldots + a_{m+l}\right) f_2\\
&= \underbrace{\left(a_m a_l + a_{m+l} b_m\right)}_{Res_X(f_1, f_2)} + \underbrace{\left(a_{m-1} a_l + a_m a_{l-1} + \ldots + a_{m+l-1} b_m + a_{m+l} b_{m-1}\right)}_{b_1} X + \ldots + \underbrace{\left(a_1 a_0 + a_{m+1} b_0\right)}_{b_{m+l-1}} X^{m+l-1}.
\end{aligned}
$$

On a $b_1 = \begin{vmatrix} & & & & & \\ \cdots & a_l & a_{l-1} & \cdots & b_m & b_{m-1} \\ \cdots & a_l & a_{l-1} & \cdots & b_m & b_{m-1} \end{vmatrix} = 0.$

De même tous les autres b_i, $2 \le i \le m + l - 1$, *sont nuls car ils correspondent à un déterminant d'une matrice ayant deux lignes identiques* $L_{m+l} = L_{m+l-i}$.

Posons :

$$g_1 = a_1 X^{m-1} + a_2 X^{m-2} + \ldots + a_m,$$

$$g_2 = a_{m+1} X^{l-1} + a_{m+2} X^{l-2} + \ldots + a_{m+l},$$

On obtient $g_1 f_1 + g_2 f_2 = Res_X(f_1, f_2)$.

Le résultant est l' outil le plus décisif pour éliminer les variables :

$Res_X(f_1, f_2) \in \langle f_1, f_2 \rangle \cap R$.

Proposition 6.2. Soient $f_1, f_2, b, d \in R[X]$ et $r = Res_X(f_1, f_2)$. Alors il existe

$B \in \mathrm{SL}_2(R[X])$ tel que : $B\begin{pmatrix} f_1(B) \\ f_2(B) \end{pmatrix} = \begin{pmatrix} f_1(b+rd) \\ f_1(b+rd) \end{pmatrix}$.

En plus de détails, soient $g_1, g_2 \in R[X]$ tels que :

$$g_1 f_1 + g_2 f_2 = Res_X(f_1, f_2) = r,$$

et $s_1, s_2, t_1, t_2 \in R[X, Y, Z]$ des polynômes définis par :

$f_1(X + YZ) = f_1(X) + Ys_1(X, Y, Z)$,

$f_2(X + YZ) = f_2(X) + Ys_2(X, Y, Z)$,

$g_1(X + YZ) = g_1(X) + Yt_1(X, Y, Z)$,

$g_2(X + YZ) = g_2(X) + Yt_2(X, Y, Z)$.

On définit :

$B_{11} = 1 + s_1(b, r, d) \cdot g_1(b) + t_2(b, r, d) \cdot f_2(b)$,

$B_{12} = s_1(b, r, d) \cdot g_2(b) - t_2(b, r, d) \cdot f_1(b)$,

$B_{21} = s_2(b, r, d) \cdot g_1(b) - t_1(b, r, d) \cdot f_2(b)$,

$B_{22} = 1 + s_2(b, r, d) \cdot g_2(b) + t_1(b, r, d) \cdot f_1(b)$.

Il suffit de prendre $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$.

CHAPITRE II

Applications au traitement du signal

Chapitre 2

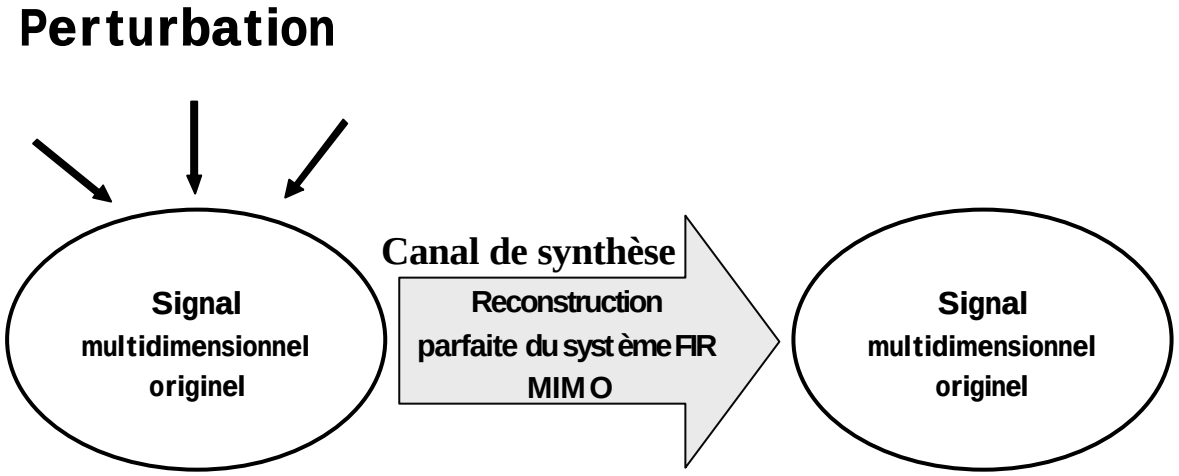
Applications au traitement du signal

1 – Introduction

Ce chapitre vise à montrer comment le traitement du signal à temps discret est lié à l'algèbre linéaire sur les anneaux de polynômes et comment les méthodes du calcul formel peuvent être employées naturellement pour différents problèmes du traitement du signal multidimensionnel. On commence par voir les concepts de base du traitement du signal, et faire le lien entre le traitement du signal à temps discret et 1'algèbre linéaire sur des anneaux de polynômes de Laurent. Une importance est accordée au problème du complètement unimodulaire des matrices à coefficients dans un anneau de polynômes de Laurent. On expliquera comment ce problème est lié au problème de paramétrisation de la synthèse des systèmes à reconstruction parfaite (PR) et réponse d'impulsion finie. Il convient de noter que beaucoup de chercheurs, Faugère, Selsnick, Lebrun et Vetterli, et autres, ont réussi à utiliser le calcul formel pour les systèmes multidimensionnels et le traitement du signal. Ceci est rendu possible essentiellement parce que beaucoup de problèmes de traitement de signal peuvent être modélisés sous forme d'équations polynomiales, qui peuvent être résolues par des méthodes de calcul formel, notamment les bases de Gröbner.

Ce chapitre est en grande partie extraite de [LY] et [P].

Problématique



2 – Concepts de base du traitement du signal

2 – 1 – Signaux à temps discret 1D

Définition 2.1.1.

(i) Un signal unidimensionnel à temps discret $(1D)$ est une suite de réels, c'est-à-dire $(a_n)_{n\in\mathbb{Z}} = (...,a_{-2},a_{-1},a_0,a_1,a_2,...)$, avec $a_n \in \mathbb{R}$ et il existe $N \in \mathbb{Z}$ tels que $a_n = 0$ pour tout $n < N$.

(ii) On note l'ensemble des signaux a temps discret 1D par **S**.

Remarque 2.1.

(1) La définition ci-dessus est formelle. Dans la pratique, un signal à temps discret 1D signifie souvent une suite à carré sommable. L'ensemble de telles suites est noté $l_2(\mathbb{Z})$.

(2) Un signal 1D $(a_n)_{n\in\mathbb{Z}}$ sera noté (a_n).

L'ensemble **S** des signaux à temps discret 1D est un $\mathbb{R}$-espace vectoriel avec les opérations de la superposition (addition) et de la multiplication par un scalaire.

Définition 2.1.2. Convolution des signaux à temps discret : la convolution de deux signaux donnés (a_n) et (c_n), $(b_n)=(a_n)*(c_n)$, est définie par $b_n=\sum_{i+j=n} a_i c_j$.

Définition 2.1.3. Soit $(c_n)\in \mathbf{S}$. On définit l'opérateur $L_{(c_n)}$ sur l'ensemble **S** des signaux à temps discret par $L_{(c_n)}((a_n))=(a_n)*(c_n)$.

On note que 1'application $L_{(c_n)}:\mathbf{S}\to\mathbf{S}$ est une application linéaire. L'ensemble **S** des signaux à temps discret muni des deux opérations de la superposition(addition) et de la convolution forme un anneau commutatif avec l'identité $(d_{n,0})$ définie par $d_{0,0}=1$ et $d_{n,0}=0,\ \forall n\neq 0$.

2 – 2 – Systèmes linéaires à temps invariant

Définition 2.2.1. On dit qu'une application linéaire $L:\mathbf{S}\to\mathbf{S}$ est à temps invariant si pour tout *i*, $L((a_n))=(b_n)$ implique $L((a_{n+i}))=(b_{n+i})$.

Un tel opérateur peut être décrit par le système de sortie unique d'entrée unique (SISO) suivant :

$$\underset{\rightarrow}{(...,a_{-2},a_{-1},a_0,a_1,a_2,...)} \boxed{L} \underset{\rightarrow}{(...,b_{-2},b_{-1},b_0,b_1,b_2,...)}.$$

Lemme 2.2.1. Une application $L:\mathbf{S}\to\mathbf{S}$ est $\mathbb{R}$-linéaire et à temps invariant si et seulement si L est $\mathbf{S}$-linéaire.

Corollaire 2.2.1. Si une application $L:\mathbf{S}\to\mathbf{S}$ est linéaire et à temps invariant sur $\mathbf{S}$, alors elle peut être représentée par une convolution, c'est-à-dire, il existe un signal à temps discret unique $(c_n)\in\mathbf{S}$ tel que $L=L_{(c_n)}$.

Dans ce cas, (c_n) s'appelle le signal de modulation de L ou la réponse d'impulsion de L.

Si $L=L_{(c_n)}$ avec $(c_n)=0$, $\forall n<0$, alors L s'appelle un système causal. Dans ce cas, on vérifie facilement que b_n est complètement déterminé par les a_i avec $i\le n$. Ceci signifie que la valeur donnée dans le signal de sortie ne dépend pas de celle dans le signal d'entrée.

Si $L=L_{(c_n)}$ et (c_n) est un signal à temps discret de durée finie, c'est-à-dire, une suite finie, alors L s'appelle un système FIR.

Définition 2.2.2. Soient $\mathbf{S}$ l'anneau des signaux à temps discret, et $p, q\in\mathbb{N}$. Alors un $\mathbf{S}$-module homomorphisme $A:\mathbf{S}^p\to\mathbf{S}^q$ s'appelle un système linéaire à temps invariant multi-entrée multi-sortie (MIMO).

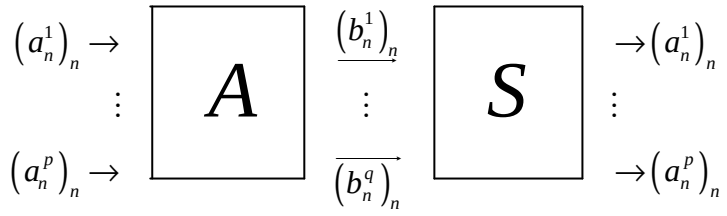
Remarque 2.2. Pour comprendre cette définition, on considère une application $A:\mathbf{S}^p\to\mathbf{S}^q$ qu'on voit comme application entre $\mathbb{R}$-espaces vectoriels. On peut montrer que si A est linéaire et à temps invariant sur $\mathbb{R}$, alors c'est un S-module homomorphisme.

Un système MIMO $A:\mathbf{S}^p\to\mathbf{S}^q$ peut être décrit par la figure suivante :

$$\begin{array}{rcl} \left(a_n^1\right)_n \to & & \to\left(b_n^1\right)_n \\ \vdots & \boxed{A} & \vdots \\ \left(a_n^p\right)_n \to & & \to\left(b_n^q\right)_n \end{array}$$

Un tel système linéaire p-entrée q-sortie à temps invariant est un opérateur du module $\mathbf{S}^p$ au module $\mathbf{S}^q$ défini par des convolutions avec de divers signaux fixés.

2 – 3 – Reconstruction parfaite des signaux



Soient A un système MIMO p-entrée q-sortie et S un système MIMO q-entrée p-sortie. Supposons que quand un signal entrant entre dans A et sa sortie est introduite dans S, la sortie résultante de S est identique au signal d'entrée original de A. Si ceci est vrai pour n'importe quelle entrée, alors la combinaison du système global fait de A et S est une conservation des entrées.

Pour un système MIMO p-entrée q-sortie A, s'il existe un système MIMO q-entrée p-sortie S tels que le système global $\left(\text{fait de } A \text{ et } S\right)$ conserve complètement les entrées, alors on dit que A a la propriété de reconstruction parfaite. Dans ce cas, on dit que A et S font un système PR, et A $\left(\text{respectivement}, S\right)$ s'appelle la partie analyse (respectivement, synthèse) du système global.

3 – Formulation algébrique

3 – 1 – La Z-transformation

Dans la section précédente, on a établi que l'ensemble $\mathbf{S}$ des signaux à temps discret 1D muni des opérations de la superposition et de la convolution forme un anneau commutatif. Cet anneau $\mathbf{S}$ est isomorphe à l'anneau $\mathbb{C}\left[\left[z^{-1}\right]\right]_{z^{-1}}$, une localisation de

l'anneau des séries entières formelles $\mathbb{C}\left[\left[z^{-1}\right]\right]_{z^{-1}}$ par rapport à la correspondance suivante :

$$(a_n) \mapsto \sum_{n=-\infty}^{\infty} a_n z^n .$$

Cette application s'appelle habituellement en littérature de traitement du signal une Z-transformation . Un système SISO peut être vu en tant qu'opérateur sur $\mathbb{C}\left[\left[z^{-1}\right]\right]_{z^{-1}}$.

$$\sum a_n z^n \xrightarrow{\quad \boxed{f} \quad} \sum b_n z^n$$

Si f est un système linéaire à temps invariant, alors il est une multiplication par une série entière dans $\mathbb{C}\left[\left[z^{-1}\right]\right]_{z^{-1}}$ et le système causal est une multiplication par une série entière dans $\mathbb{C}\left[\left[z^{-1}\right]\right]$.

Si *f* est un système FIR, alors il est une multiplication par un polynôme de Laurent dans $\mathbb{C}\left[\left[z^{-1}\right]\right]_{z^{-1}} = \mathbb{C}\left[\left[z^{-1}\right]\right]$, et donc, un système causal FIR est une multiplication par un polynôme dans $\mathbb{C}\left[z^{-1}\right]$.

Ceci est généralise à un système $\left(\text{linéaire à temps invariant}\right)$ multi-entrée multi-sortie, c'est-à-dire, un système linéaire à temps invariant multi-entrée multi-sortie FIR $A: \left(\mathbb{C}\left[z^{\pm 1}\right]\right)^p \to \left(\mathbb{C}\left[z^{\pm 1}\right]\right)^q$ est une multiplication par une matrice, c'est-à-dire $A \in M_{qp}\left(\mathbb{C}\left[z^{\pm 1}\right]\right)$.

Cette matrice *A* est parfois appelée la matrice de transfert du système MIMO.

3 – 2 - Reconstruction parfaite dans le domaine de la Z-transformation

On considère un système p-entrée q-sortie MIMO dont la représentation par la Z-transformation est une matrice *A* de taille $q \times p$. Dans ce cas, le système global que *A* et *S* forment est un système PR, et *A* $\left(\text{respectivement}, S\right)$ est la partie analyse (respectivement, synthèse) du système global.

Remarque 3.1. Dans la littérature sur le traitement du signal, on dit souvent que le système MIMO représentés par une matrice A de taille $q \times p$ dont les coefficients sont des polynômes de Laurent $q \geq p$, a la propriété PR s'il y a une matrice *S* de taille $q \times p$ dont les coefficients sont des polynômes de Laurent et un entier *d*, tels que $SA = z^d I_p$.

Dans ce contexte, le nombre entier $|d|$ s'appelle un retard si *d* est négatif, et s'appelle une avance si *d* est positif.

On note que ces deux définitions de PR sont identiques : c'est-à-dire, si $SA = z^d I_p$, alors $z^{-d} S$ est l'inverse a gauche de *A*.

4 – Prolongements aux dimensions plus élevées

Définition 4.1. Un *m*-D signal à temps discret est une suite d'indices multiples de réels, c'est-à-dire, $\left(a_{i_1 \ldots i_m}\right)_{(i_1 \ldots i_m) \in \mathbb{Z}^m}$, avec $a_{i_1 \ldots i_m} \in \mathbb{R}$ et il existe $N \in \mathbb{Z}$ tels que $a_{i_1 \ldots i_m} = 0$ pour tout $i_i < N$ pour un certain *i*.

On peut définir la superposition et la convolution de signaux à temps discret *m*-D comme dans le cas 1D. Les systèmes linéaires à temps invariant *m*-D sont définis de la même manière. On vérifie que l'ensemble des signaux à temps discret *m*-D forment un anneau commutatif avec ces deux opérations. Cet ensemble est isomorphe à l'anneau

$\mathbb{C}\left[\left[z_1^{-1},...,z_m^{-1}\right]\right]_{z_1^{-1},...,z_m^{-1}}$, une localisation de 1'anneau des séries entières formelles à plusieurs variables $\mathbb{C}\left[\left[z_1^{-1},...,z_m^{-1}\right]\right]$ par rapport à la Z-transformation suivante :

$$\left(a_{i_1\ldots i_m}\right)_{i_1\ldots i_m} \mapsto \sum_{(i_1\ldots i_m)\in\mathbb{Z}^m} a_{i_1\ldots i_m} z_1^{-i_1}\ldots z_m^{-i_m} .$$

Tous les concepts introduits pour les signaux 1D dans les sections précédentes peuvent être prolonges aux signaux *m*-D. Par exemple, pour la Z-transformtion, un système *m*-D FIR MIMO est décrit par une matrice dont les entrées sont des polynômes de Laurent en m variables, c'est-à-dire des éléments de $\mathbb{C}\left[\left[z_1^{\pm 1},...,z_m^{\pm 1}\right]\right]$. La méthode de représentation de polyphases peut être prolongée aux filtres multidimensionnels.

5 – Unimodularité et reconstruction parfaite

Définition 5.1. Une matrice $U \in A^{q\times p}$ avec $q \geq p$ et A un anneau, est dite unimodulaire si l'idéal engendré par les mineurs maximaux $\left(\text{de taille } p\times q\right)$ contient 1. En particulier, si $U = \begin{pmatrix} U_1 \\ \vdots \\ U_q \end{pmatrix} \in A^{q\times 1}$, U est unimodulaire si $1 \in \left\langle U_1,\ldots,U_q \right\rangle$.

Théorème 5.1. Une matrice de taille $q\times p$ dont les coefficients sont des polynômes de Laurent a un inverse à gauche si et seulement si elle est unimodulaire.

Corollaire 5.1. Un système p-entrée q-sortie FIR MIMO est une partie de l'analyse d'un système PR FIR MIMO si et seulement si sa représentation par la Z-transformation est une matrice unimodulaire dont les coefficients sont des polynômes de Laurent.

- Ce corollaire nous permet de voir l'étude des systèmes linéaires à temps invariant PR FIR MIMO comme l'étude des matrices unimodulaires dont les coefficients sont des polynômes de Laurent.

Exemple 5.1. On considère un système FIR MIMO dont la représentation par la Z-transformation est donnée par :

$$U=\begin{pmatrix} \frac{3}{z}-2z-2+2z^2 & \frac{6}{z}+25-16z^2+20z^3 \\ \frac{3}{z}-2z & \frac{6}{z}+29-4z-20z^2 \\ 2z & 2+4z+20z^2 \end{pmatrix}$$

Déterminons si ce système permet la reconstruction parfaite PR des signaux d'entrées arbitraires.

Solution : Les trois mineurs maximaux de U sont -1, $-4+\frac{6}{z}-2z+2z^2$, $\frac{6}{z}-2z$. Notons que $\mathbb{C}\left[z,z_1^{-1}\right]=\mathbb{C}[z,u]\backslash\langle uz-1\rangle$. En calculant une base de Gröbner réduite G de $\langle -1,-4+u-2z+2z^2,u-2z,uz-1\rangle$, on trouve $G=\langle 1\rangle$. Ce qui montre que -1, $\frac{6}{z}-2z$, $-4+\frac{6}{z}-2z+2z^2$ engendrent l'idéal unité. Par conséquent le système donné permet la PR des signaux d'entrées arbitraires.

6 – Construction de la matrice de synthèse

Considérons une matrice unimodulaire A de taille $q\times p$, dont les coefficients sont des polynômes de Laurent. Par Le Théorème 5.1, A représente un système PR MIMO, et il existe une matrice S de taille $p\times q$ telle que $SA=I_p$. Dans le cas 1D, une telle matrice S $\left(\text{non unique sauf pour } p=q\right)$ peut être facilement calculée en utilisant un analogue de l'algorithme de division euclidienne pour les polynômes de Laurent.

Exemple 6.1. On considère encore le système FIR MIMO de l'exemple 5.1. On a montré que ce système permet la PR des signaux d'entrées arbitraires. Explicitement, construisons une synthèse du système qui reconstruira les entrées originales.

En utilisant l'analogue de l'algorithme de division euclidienne pour les polynômes de Laurent, on peut appliquer successivement des opérations élémentaires pour avoir

$$EU = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \text{ avec}$$

$$E = \begin{pmatrix} \frac{z}{18}\left(-18-125z-188z^2-252z^3-215z^4-178z^5+6z^6\right) & \frac{z}{3}\left(-2-27z+30z^2+z^3\right) & \frac{1}{6}\left(-12-89z+51z^2-62z^3-2z^4\right) \\ \frac{z}{6}\left(3+19z-32z^2-23z^3-9z^4-8z^5-6z^6\right) & z\left(4-3z-z^2+z^3\right) & \frac{9}{2}-4z+\frac{3z^2}{2}-z^3-z^4 \\ z\left(-4z+23\frac{z^2}{3}-5z^3+z^4+8\frac{z^5}{3}-2z^6\right) & 2z\left(-3-2z+z^2-z^3\right) & -6+6z-z^2-2z^3-2z^4 \end{pmatrix}.$$

Les deux premières lignes de cette matrice représentent l'inverse à gauche de *U*. Cependant, dans le cas *m*-D cette méthode pour le cas d'une seule variable n'est plus applicable puisque 1'algorithme de la division euclidienne n'est plus valable, et le calcul de *S* est plus difficile.

7 – Travail sur les anneaux de polynômes de Laurent

Plusieurs des méthodes connues pour les matrices unimodulaires sont développés principalement sur les anneaux de polynômes. Par exemple, déterminer l'unimodularité

d'une matrice $A \in M_{pq}\left(K\left[X_1,...,X_n\right]\right)$ sur $K\left[X_1,...,X_n\right]$ est équivalent à déterminer l'idéal engendré par les mineurs maximaux de *A*. Ce problème peut être efficacement résolu par le calcul d'une base de Gröbner réduite. Dans le cas d'un vecteur formé par des polynômes de Laurent, il suffit de faire un changement de variables pour avoir un vecteur formé par des polynômes telle que l'unimodularité du premier vecteur est équivalente à celle du second.

8 – Cas spécial 1-entrée p-sortie

On considère un système multidimensionnel 1-entrée p-sortie FIR $(p>1)$ dont la représentation par la Z-transformation est une matrice de taille p x 1 dont les coefficients sont des polynômes de Laurent

$$v\left(z_1,...,z_n\right)=\begin{pmatrix} f_1\left(z_1,...,z_n\right) \\ \vdots \\ f_p\left(z_1,...,z_n\right) \end{pmatrix}.$$

On suppose qu'il existe un changement bijectif des variables, $\left(z_1,...,z_n\right)\leftrightarrow\left(z'_1,...,z'_n\right)$, tel que *v*, exprime en fonction des nouvelles variables $z'_1,...,z'_n$ représente un système causal avec un inverse causal. Ceci signifie que tout les f_i deviennent des polynômes en $z'^{-1}_1,...,z'^{-1}_n$ et il y a un vecteur de synthèse

$$w=\left(g_1\left(z'_1,...,z'_n\right),...,g_p\left(z'_1,...,z'_n\right)\right)$$

tel que les g_i sont des polynômes en $z'^{-1}_1,...,z'^{-1}_n$ et $g_1 f_1+...+g_p f_p=1$.

En appliquant l'algorithme pour le complètement unimodulaire on trouve une matrice *E* tel que

$$Ev={}^t\left(1,0,...,0\right).$$

Il est immédiat que le premier vecteur $w_1(z_1,...,z_n)$ de E satisfait $w_1 v = 1$, et définit une synthèse du système qui, avec 1'analyse du système défini par *v*, font un système P.R. Une question naturelle concernant le rôle des autres vecteurs $w_2,...,w_p$ de E surgit ici.

On note que $Ev = {}^t(1,0,...,0)$ implique

$$w_2 v = ... = w_p v = 0 .$$

Par conséquent, pour tous polynômes de Laurent $t_2,...,t_p$, on a :

$$\left(w_1 + t_2 w_2 + ... + t_p w_p\right) v = 1,$$

et cette formule donne une famille paramétrée

$$w = w_1 + t_2 w_2 + ... + t_p w_p$$

d'inverses à gauche de *v* en termes de $p-1$ paramètres de polynômes de Laurent $t_2,...,t_p$. La paramétrisation est complète dans le sens que n'importe quel inverse a gauche de *v* peut être écrit sous une telle forme, et elle est canonique dans le sens que l'expression d'une synthèse d'un système en termes des paramètres ci-dessus est unique. Pour la preuve voir.

9 – Systèmes généraux 1-entrée p-sortie

9 – 1 – Vue d'ensemble : Algorithme Causal de Conversion

Les résultats de la section précédente fonctionnent seulement pour le cas spécial des systèmes 1-entrée p-sortie, c'est-à-dire, les systèmes dont les Z-transformations deviennent des vecteurs de polynôme inversibles en fonctions des nouvelles variables. Dans cette section, on utilise lalgorithme de Park qui transforme un vecteur colonne de polynôme de Laurent $v(X_1,...,X_m) \in \left(K\left[X_1^{\pm 1},...,X_m^{\pm 1}\right]\right)^p$ en un vecteur colonne de polynômes $\hat{v}(Y_1,...,Y_m) \in \left(K[Y_1,...,Y_m]\right)^p$ en conservant l'unimodularité.

On conclut que la recherche d'un inverse w FIR pour une analyse v FIR donnée est équivalent à la recherche d'un inverse causal $\hat{w}$ pour le système causal $\hat{v}$.

En utilisant la section 8 on trouve une famine paramètre complète d'inverses a gauche de $\hat{v}$. Une fois qu'un inverse à gauche $\hat{w}$ de $\hat{v}$ est trouvé, $w = \hat{v}T$ est un inverse à gauche (pas nécessairement causal) de *v*, produisant une paramétrisation complète des paires PR FIR pour l'analyse *v* donnée.

CHAPITRE III

Implantation avec Maple de l'algorithme de complètement unimodulaire

Chapitre 3

Implantation avec Maple de l'algorithme de complètement unimodulaire.

1 – Algorithmes pour le complètement unimodulaire

Pour tout anneau B, on dira qu'une matrice $N \in \mathrm{M}_n(B)$ appartient à $\mathrm{SL}_2(B)$ si elle s'écrit sous la forme :

$$\begin{pmatrix} N' & 0 & \dots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

avec $N' \in \mathrm{SL}_2(B)$.

Un algorithme pour le complètement unimodulaire (Algorithme de Lombardi-Yengui) :

Input: Un vecteur $V = {}^t(V_1(X,Y), V_2(X,Y), V_3(X,Y))$ unimodulaire tel que $V_i(X,Y) \in \mathbb{Q}[X,Y]$ et V_1 unitaire en X (V unimodulaire si est seulement si $1 \in \langle V_1, V_2, V_3 \rangle \Leftrightarrow G_{red}\{V_1, V_2, V_3\} = \{1\}$.

Output : Une matrice B dans $\mathrm{SL}_3(\mathbb{Q}[X,Y])$ tels que $BV = V(0,Y)$.

Etape 1 : Pour $1 \le i \le l = \deg_X v_1 + 1$, soit $w_i := v_2 + (i-1)v_3$, calculer $r_i := \mathrm{Res}_X(v_1, w_i)$, $r_i \in \mathbb{Q}[Y]$ et trouver $a_1, \dots, a_l \in \mathbb{Q}[X,Y]$ tels que $a_1 r_1 + \dots + a_l r_l = 1$.

Pour $1 \le i \le l$, calculer $f_i, g_i \in \mathbb{Q}[X,Y]$ tels que $f_i V_1 + g_i w_i = r_i$.

Etape 2 : Poser

$b_l := 0$,

$b_{l-1} := a_l r_l X$,

$b_{l-2} := b_{l-1} + a_{l-1} r_{l-1} X$,

$\vdots$

$b_0 := b_1 + a_1 r_1 X = X$ $\left(\text{ceci implique que } X = \sum_{i=1}^{l} a_i r_i X\right)$.

Etape 3 : Pour $1 \le i \le l$, trouver $B_i \in \mathrm{SL}_3\left(\mathbb{Q}[X,Y]\right)$ telle que $B_i V(b_{i-1}) = V(b_i)$.

En plus de détails, considérer g_i de la matrice correspondant à l'opération élémentaire

$L_2 \to L_2 + (i-1) L_3$ c'est-à-dire,

$$g_i := E_{2,3}(i-1).$$

Poser $F_{i,3} := \dfrac{v_3(b_{i-1}) - v_3(b_i)}{b_{i-1} - b_i} = \dfrac{v_3(b_{i-1}) - v_3(b_i)}{a_i r_i X} \in \mathbb{Q}[X,Y]$, de sorte qu'on obtienne

$$\begin{aligned} v_3(b_{i-1}) - v_3(b_i) = a_i r_i X F_{i,3} &= a_i X F_{i,3} f_i(b_{i-1}) v_1(b_{i-1}) + a_i X F_{i,3} g_i(b_{i-1}) w_i(b_{i-1}) \\ &= s_{i,3} v_1(b_{i-1}) + b_{i,3} w_i(b_{i-1}). \end{aligned}$$

Avec

$$s_{i,3} := a_i X F_{i,3} f_i(b_{i-1}),\ b_{i,3} := a_i X F_{i,3} g_i(b_{i-1}) \in \mathbb{Q}[X,Y].$$

Considérer $\Gamma_i \in \mathrm{E}_3\left(\mathbb{Q}[X,Y]\right)$ la matrice correspondant aux opérations élémentaires :

$L_3 \to L_3 - b_{i,3} L_1 - t_{i,3} L_2$,

c'est-à-dire

$$\Gamma_i := E_{3,1}\left(-s_{i,3}\right) E_{3,2}\left(-b_{i,3}\right).$$

Poser

$$B_{i,2} := \Gamma_i g_i(b_{i-1}) \in \mathrm{E}_3\left(\mathbb{Q}[X,Y]\right),$$

de sorte que nous ayons

$$B_{i,2}\boldsymbol{V}(b_{i-1}) = \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \\ v_3(b_i) \end{pmatrix}.$$

Poser

$$s_{i,1}(X,y,z) := \frac{v_1(X+yz)-v_1(X)}{y} \in \mathbb{Q}[X,Y,y,z],$$

$$s_{i,2}(X,y,z) := \frac{w_i(X+yz)-w_i(X)}{y} \in \mathbb{Q}[X,Y,y,z],$$

$$t_{i,1}(X,y,z) := \frac{f_i(X+yz)-f_i(X)}{y} \in \mathbb{Q}[X,Y,y,z],$$

$$t_{i,2}(X,y,z) := \frac{g_i(X+yz)-g_i(X)}{y} \in \mathbb{Q}[X,Y,y,z],$$

$$C_{i,1,1} := 1+s_{i,1}(b_{i-1},r_i,-a_iX)f_i(b_{i-1})+t_{i,2}(b_{i-1},r_i,-a_iX)w_i(b_{i-1}) \in \mathbb{Q}[X,Y].$$

$$C_{i,1,2} := s_{i,1}(b_{i-1},r_i,-a_iX)g_i(b_{i-1})-t_{i,2}(b_{i-1},r_i,-a_iX)v_1(b_{i-1}) \in \mathbb{Q}[X,Y],$$

$$C_{i,2,1} := s_{i,2}(b_{i-1},r_i,-a_iX)f_i(b_{i-1})-t_{i,1}(b_{i-1},r_i,-a_iX)w_i(b_{i-1}) \in \mathbb{Q}[X,Y],$$

$$C_{i,2,2} := 1+s_{i,2}(b_{i-1},r_i,-a_iX)g_i(b_{i-1})+t_{i,1}(b_{i-1},r_i,-a_iX)v_1(b_{i-1}) \in \mathbb{Q}[X,Y],$$

$$C_i := \begin{pmatrix} C_{i,1,1} & C_{i,1,2} \\ C_{i,2,1} & C_{i,2,2} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q}[X,y]).$$

Ici notons que

$$C_i \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ w_i(b_i) \end{pmatrix}.$$

Poser

$$B_{i,1} := g_i(b_i)^{-1} \begin{pmatrix} C_i & 0 \\ 0 & I_1 \end{pmatrix},$$

avec

$$g_i^{-1} = E_{2,3}(-(i-1)).$$

Poser

$$B_i := B_{i,1}B_{i,2} \in \mathrm{SL}_3\left(\mathbb{Q}[X,y]\right),$$

de façon que $B_i \boldsymbol{V}(b_{i-1}) = \boldsymbol{V}(b_i)$.

Etape 4 : $B := B_l \cdots B_1$. $\left(\text{noter que } B\boldsymbol{V}(X,Y) = \boldsymbol{V}(0,Y)\right)$.

2 – Implantation du code Maple

```
> restart; with(linalg):
`expandmatrix`:=proc(B::matrix)
  local i,j;
    with(grobner,normalf);  with(Groebner,spoly);
with(linalg,multiply);
for i from 1 to 3 do for j from 1 to 3 do
B[i,j]:=expand(B[i,j]);od;od;RETURN(B);
;end:
`expandvector`:=proc(V::matrix)
  local i,j;
    with(grobner,normalf);  with(Groebner,spoly);
with(linalg,multiply);
for i from 1 to 3  do  V[i,1]:=expand(V[i,1]);od;RETURN(V);
;end:

Unimod:=proc(f,X::name)
local n,a,b,S,alfa,s,t,d,i,j,u;
n:=nops(f);a[1]:=f[1];b[1]:=f[2];
   for i from 1 to n-2 do
      d[i]:=gcdex(a[i],b[i],X,'s[i]','t[i]');
      a[i+1]:=a[i]*s[i]+b[i]*t[i];b[i+1]:=f[i+2];
   od;
d[n-1]:=gcdex(a[n-1],b[n-1],X,'s[n-1]','t[n-1]');
u[1]:=product(s[j],j=1..n-1);u[n]:=t[n-1];
   for i from 2 to n-1 do
      u[i]:=(product(s[j],j=i..n-1))*t[i-1]
   od;
d[n-1];
[seq(sort(u[j],x),j=1..n)];
end proc:

for i from 1 to 3 do
nprintf("donner le composant numéro %d du vecteur :",i);
V[i,1]:=readstat();
od;

V:=matrix(3,1,[V[1,1],V[2,1],V[3,1]]):
```

```
V1:=V[1,1]:V2:=V[2,1]:V3:=V[3,1]:
with(Groebner):
WL:=[V1,V2,V3]:
GB:=gbasis(WL,plex(x,y)):

L:=degree(V1,x)+1:

for i from 1 to L do
y[i]:=i-1;
w[i]:=expand(V2+y[i]*V3);
r[i]:=expand(resultant(V1,w[i],x));
gcdex(V1,w[i],r[i],x,'s','t'): f[i]:=s; g[i]:=t;
od:

R0:=Vector[row](L):
for i from 1 to L do
R0[i]:=r[i];
od:
R:=convert(R0,'list'):
A:=Unimod(R,y):
for i from 1 to nops(R) do
alfa[i]:=expand(op(i,A));
od:

b[L]:=0:

for i from 1 to L do
b[L-i]:=expand(b[L-i+1]+alfa[L-i+1]*r[L-i+1]*x);
gama[i]:=matrix(3,3,[1,0,0,0,1,y[i],0,0,1]);
od:
for i from 1 to L+1 do
v[3,i-1]:=expand(subs(x=b[i-1],V3));
od:

for i from 1 to L do
alfar[i]:=expand(alfa[i]*r[i]*x);
F[i,3]:=expand((v[3,i-1]-v[3,i])/(alfar[i]));
od:

for i from 1 to L do
sigma[i,3]:=expand(alfa[i]*x*F[i,3]*subs(x=b[i-1],f[i]));
beta[i,3]:=expand(alfa[i]*x*F[i,3]*subs(x=b[i-1],g[i]));
E[3,1,i]:=matrix(3,3,[1,0,0,0,1,0,-sigma[i,3],0,1]);
E[3,2,i]:=matrix(3,3,[1,0,0,0,1,0,0,-beta[i,3],1]);
Gamma[i]:=matrix(multiply(E[3,1,i],E[3,2,i]));
gamab[i]:=subs(y=b[i-1],gama[i]);
od:

with(linalg,multiply):
for i from 1 to L do
B[i,2]:=expandmatrix(multiply(Gamma[i],gama[i]));
```

```
s[i,1]:=expand((subs(x=x+Y*z,V1)-V1)/Y);
s[i,2]:=expand((subs(x=x+Y*z,w[i])-w[i])/Y);
t[i,1]:=expand((subs(x=x+Y*z,f[i])-f[i])/Y);
t[i,2]:=expand((subs(x=x+Y*z,g[i])-g[i])/Y);

sc[i,1]:=subs(x=b[i-1],y=r[i],z=-alfa[i]*x,s[i,1]);
tc[i,2]:=expand(subs(x=b[i-1],y=r[i],z=-alfa[i]*x,t[i,2]));
c[i,1,1]:=1+expand(sc[i,1]*subs(x=b[i-
1],f[i])+tc[i,2]*subs(x=b[i-1],w[i]));
c[i,1,2]:=expand(sc[i,1]*subs(x=b[i-1],g[i])-
tc[i,2]*subs(x=b[i-1],V1));

sc[i,2]:=expand(subs(x=b[i-1],Y=r[i],z=-alfa[i]*x,s[i,2]));
tc[i,1]:=expand(subs(x=b[i-1],Y=r[i],z=-alfa[i]*x,t[i,1]));
c[i,2,1]:=expand(sc[i,2]*subs(x=b[i-1],f[i])-
tc[i,1]*subs(x=b[i-1],w[i]));
c[i,2,2]:=1+expand(sc[i,2]*subs(x=b[i-
1],g[i])+tc[i,1]*subs(x=b[i-1],V1));

C[i]:=matrix(3,3,[c[i,1,1],c[i,1,2],0,c[i,2,1],c[i,2,2],0,0,
0,1]);

gama2[i]:=inverse(gama[i]);
B[i,1]:=expandmatrix(multiply(subs(x=b[i],gama2[i]),C[i]));
B[i]:=expandmatrix(multiply(B[i,1],B[i,2]));
od:

with(linalg,multiply):
B:=expandmatrix(multiply(B[2],B[1]));

print(`On multiplie B et V, si on trouve V(0,y) c'est
correct, et c'est le cas`);

BV:=expandvector(multiply(B,V));
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

donner lecomposant numéro 1 du vecteurm:

```
> x+2*y+1;
```

$$V_{1,1} := x + 2y + 1$$

donner lecomposant numéro 2 du vecteurm:

```
> -x+x*y;
```

$$V_{2,1} := -x + xy$$

donner lecomposant numéro 3 du vecteurm:

```
> x-y^2+2*y+3;
```

$$V_{3,1} := x - y^2 + 2y + 3$$

```
Warning, the name normalf has been redefined
```

$$B := \begin{bmatrix} 1+\frac{8}{7}x-\frac{1}{7}y^2x & \frac{3}{7}x+\frac{1}{7}xy & -\frac{5}{7}x-\frac{2}{7}xy \\ \frac{1}{7}y^2x-\frac{1}{7}y^3x+\frac{8}{7}xy-\frac{8}{7}x & 1-\frac{3}{7}x+\frac{2}{7}xy+\frac{1}{7}y^2x & -\frac{3}{7}xy-\frac{2}{7}y^2x+\frac{5}{7}x \\ -\frac{1}{7}y^2x+\frac{8}{7}x & \frac{3}{7}x+\frac{1}{7}xy & 1-\frac{5}{7}x-\frac{2}{7}xy \end{bmatrix}$$

On multiplie B et V , si ontrouve $V(0,y)$ *c'est correct, et c'est lecas*

$$BV := \begin{bmatrix} 2y+1 \\ 0 \\ -y^2+2y+3 \end{bmatrix}$$

Conclusion

Dans ce projet, nous avons expliqué la correspondance entre le complètement des matrices polynomiales multivariées unimodulaires et le problème de reconstruction parfaite des signaux multidimensionnels à impulsions finies. Un algorithme de complètement unimodulaire (de Lombardi-Yengui) a été étudié et implanté.

Ce qui nous a fasciné, c'est qu'en vue d'applications concrètes et importantes, on a besoin de concepts assez profonds venant de l'algèbre commutative et linéaire. Gràce au progrès considérable dans les logiciels de calcul formel, plusieurs algorithmes ont pu être implanté et appliqués dans plusieurs domaines.

Bibliographie

[LY] H. Lombardi, I. Yengui. *Suslin's algorithms for reduction of unimodular rows.* J. Symb. Comp. **39** (2005), 707-717.

[P] H. Park. *Symbolic computations and signal processing*. J. Symb. Comp. **37** (2004), 209-226.

[CLO] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties and Algorithms*, 2nd edition, New York, Springer-Verlag, 1997.