

Une approche élémentaire de la programmation linéaire entière

PAR PATRICK TELLER

VERSION révisée juin 2018

Ce problème, dont la nature est algébrique, est ordinairement traité de la manière suivante:

Résolution du problème « relâché » (c'est à dire sans contrainte d'intégrité) puis utilisation de méthodes itératives, destinées à isoler des solutions dans \mathbb{N}^m : méthode de coupes de Gomory, méthode de séparation et évaluation, Branch and Bound.

Ce qui caractérise de ces méthodes est que leur moteur est essentiellement algorithmique; la seule contrainte de type mathématique (ou informatique?) est la capacité à distinguer les entiers parmi les rationnels; la complexité (dans le pire des cas) est exponentielle, même si, comme souvent, les cas rencontrés dans la pratique ne le sont pas.

De son coté l'algèbre commutative a développé les bases de Grobner qui permettent d'étendre la notion de division polynomiale aux anneaux de polynômes en plusieurs indéterminées et des travaux spécifiques à caractère algébrique (Conti-Traverso[1]) ou géométrique (Thomas [2]) ont permis d'exploiter cet environnement pour résoudre (de manière exacte) les problèmes de programmation linéaire en entiers.

Le hic c'est que les bases de Grobner (appelées aussi bases standard) font appel, entre autres, à des notions comme celles d'idéaux, d'anneaux noethériens... ce qui semble leur conférer un degré d'abstraction élevé et présenter en conséquence des obstacles pour leur emploi par des élèves ingénieurs; en réalité, ces notions, dans toute leur abstraction, ne sont pas indispensables, pour l'emploi que nous comptons en faire; et il est possible d'en développer une version linéaire adaptée à des sous-groupes additifs de \mathbb{Z}^p qui suffira largement.

De plus, alors qu'il est établi qu'il n'y a pas lieu d'imposer de conditions de signe sur les coefficients du système [3], le recours à des polynômes imposait dans le cas de coefficients négatifs l'utilisation d'exposants négatifs, et par suite, soit des polynômes de Laurent soit l'introduction d'inconnues supplémentaires traduisant l'inversibilité.

La restriction des bases standard à des sous-groupes de \mathbb{Z}^p va permettre d'étudier de manière bien plus élémentaire l'existence de solutions dans \mathbb{N}^m d'un système linéaire diophantien et, dans l'affirmative, la recherche des (de la) solution(s) qui optimise(nt) une forme linéaire donnée.

Dans ce qui va suivre on trouvera donc une méthode élémentaire qui ne fait appel qu'à des notions de base de l'Algèbre linéaire; bien sûr les techniques réclament une justification, il est donc nécessaire d'inclure des démonstrations, celles-ci seront « indépendantes » de la théorie générale (bien qu'inspirées plus ou moins directement des démonstrations générales); elles ne sont pas indispensables pour la simple mise en pratique de la technique proposée.

Pourquoi les bases standard ?

C'est en fait l'origine de ce travail, les bases de Grobner sont employées dans les domaines se rattachant à la Géométrie Algébrique comme des bases d'idéaux dans des anneaux de polynômes à plusieurs indéterminées, elles permettent d'y étendre la notion de division euclidienne, et surtout celle de reste dans une telle division.

Dans notre cas il sera en fait question d'un semi-sous-groupe \mathcal{A} de \mathbb{Z}^n , engendré par m vecteurs (A_1, \dots, A_m) et d'abord de l'appartenance (ou la non-appartenance) d'un élément de \mathbb{Z}^n à \mathcal{A} ; la difficulté réside dans le fait banal qu'il s'agit d'équations à plusieurs inconnues et que le choix du coefficient éventuel de l'un des A_j peut se révéler inadapté et irrécupérable; l'avantage fourni par les bases standard (qui ne sont pas des « bases » au sens de l'algèbre linéaire mais des familles génératrices suffisamment riches) réside en cela que le reste d'un vecteur modulo cette base sera indépendant de la procédure de combinaison linéaire employée, c'est à dire de l'ordre dans lequel sont traités les éléments de cette base; en d'autres mots tout usage abusif de l'un des A_j peut être corrigé par l'intervention ultérieure d'un autre élément de la base standard.

Dans tout ce qui suit « combinaison linéaire » s'entendra comme combinaison linéaire à coefficients dans \mathbb{Z} ; de même on utilisera indistinctement les expressions p -uplet et vecteur pour des éléments de \mathbb{Z}^p .

1. La matrice-témoin

Soit la matrice $A \in \mathcal{M}_{nm}(\mathbb{N})$ et $B \in \mathcal{M}_{n1}(\mathbb{N})$ on désigne par (*) le système d'équations linéaires $AX=B$.

Définition 1. La matrice témoin d'un système linéaire

Soit une matrice $A \in \mathcal{M}_{nm}(\mathbb{N})$ on appellera matrice témoin du système (*) la matrice

$$\bar{A} = \begin{pmatrix} A & \\ -I_m & \end{pmatrix} = \begin{pmatrix} A_1 & A_2 & \cdot & \cdot & A_m \\ -1 & 0 & 0 & \cdot & 0 \\ 0 & -1 & 0 & \cdot & \cdot \\ \cdot & 0 & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & 0 & -1 \end{pmatrix}.$$

Proposition 2. La matrice témoin du système linéaire $AX=B$ permet de « tracer » la résolution

Soit une matrice $A \in \mathcal{M}_{nm}(\mathbb{N})$ et un vecteur colonne $B \in \mathcal{M}_{n1}(\mathbb{N})$, il existe un vecteur colonne $X = \begin{pmatrix} x_1 \\ \dots \\ x_m \end{pmatrix} \in \mathcal{M}_{m1}(\mathbb{N})$, tel que $AX=B$ si et seulement si, en considérant la matrice

$$\bar{A} = \begin{pmatrix} A & \\ -I_m & \end{pmatrix} = \begin{pmatrix} A_1 & A_2 & \cdot & \cdot & A_m \\ -1 & 0 & 0 & \cdot & 0 \\ 0 & -1 & 0 & \cdot & \cdot \\ \cdot & 0 & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & 0 & -1 \end{pmatrix}, \bar{A}X = \begin{pmatrix} B \\ -X \end{pmatrix}, \text{ ce qui équivaut à } \begin{pmatrix} B \\ 0 \end{pmatrix} = \bar{A}X + \begin{pmatrix} 0 \\ X \end{pmatrix} (**).$$

Plutôt que résoudre le système (*) nous allons rechercher l'existence d'un vecteur $\begin{pmatrix} 0 \\ X \end{pmatrix}$ qui sera le « reste » de $\begin{pmatrix} B \\ 0 \end{pmatrix}$ modulo le semi-sous-groupe de \mathbb{Z}^{n+m} engendré par les vecteurs colonnes $(\bar{A}_1, \dots, \bar{A}_m)$.

Le problème c'est que ce « reste » dépend de la procédure employée, ce qui signifie que, si une réponse positive suffit, une réponse négative ne permet pas de conclure car il n'y a pas unicité du reste; nous allons substituer à la famille $(\bar{A}_1, \dots, \bar{A}_m)$ une base standard associée, pour laquelle nous établirons une telle unicité.

2. Les outils (inspirés des bases de Grobner)

Rappelons de manière succincte les définitions et propriétés des bases standard vectorielles qui ont été définies et établies dans [4]:

Nous désignerons par \preceq la relation d'ordre (partiel) sur \mathbb{N}^p définie comme suit $U = \begin{pmatrix} u_1 \\ \dots \\ u_p \end{pmatrix} \preceq V = \begin{pmatrix} v_1 \\ \dots \\ v_p \end{pmatrix} \iff \forall i \in \{1, \dots, p\}, u_i \leq v_i$; on dira alors que U précède V , lorsque 0 précède U on dira que U est positif.

On désignera par α l'ordre lexicographique qui, lui, est un ordre total; lorsque $\begin{pmatrix} 0 \\ \cdot \\ 0 \end{pmatrix} \alpha \begin{pmatrix} v_1 \\ \dots \\ v_p \end{pmatrix}$ on dira que $\begin{pmatrix} v_1 \\ \dots \\ v_p \end{pmatrix}$ est lex-positif, de même on dira lex-strictement-positif pour lex-positif et non nul.

Définition 3. Soit un p -uplet $U = \begin{pmatrix} u_1 \\ \dots \\ u_p \end{pmatrix}$ on notera, pour chaque i , $u_i^+ = \max\{u_i, 0\}$ et $u_i^- = \max\{0, -u_i\}$, $U^+ = \begin{pmatrix} u_1^+ \\ \dots \\ u_p^+ \end{pmatrix}$ et $U^- = \begin{pmatrix} u_1^- \\ \dots \\ u_p^- \end{pmatrix}$, d'où $U = U^+ - U^-$; lorsque $U \neq 0$ on notera $s(U) = \min\{i \in \llbracket 1, \dots, p \rrbracket, u_i \neq 0\}$ et $U^* = U$ lorsque $u_{s(U)} > 0$ et $U^* = -U$ lorsque $u_{s(U)} < 0$; un p -uplet U non nul, tel que $u_{s(U)} > 0$ sera donc lex-strictement-positif.

On appellera support de U l'ensemble $\text{supp}(U) = \{i, u_i \neq 0\}$ et de même on pourra s'intéresser à $\text{supp}(U^+)$ et $\text{supp}(U^-)$

Par ailleurs on remarquera que si U est non nul alors U^* est nécessairement lex-strictement positif.

Définition 4. Réduction d'un p uplet U par un p uplet V lex-strictement positif.

Soit U et V deux p uplets tels que $V^+ \preceq U^{*+}$, soit $\beta = \max\{k \in \mathbb{N}, 0 \preceq U^{*+} - kV^+\}$, d'où on posera $U = \varepsilon\beta V + W$ (où $\varepsilon = +1$ si $U^* = U$, $\varepsilon = -1$ si $U^* = -U$).

W sera appelé le reste de U modulo V .

Dans le cas $U = 0V + W$ on dira que U est irréductible par V .

Exemple 5.

$$U = \begin{pmatrix} 4 \\ 3 \\ -3 \\ -2 \end{pmatrix}, V = \begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}, U = 1V + W = \begin{pmatrix} 3 \\ 0 \\ -2 \\ 2 \end{pmatrix}, \text{ donc } U \xrightarrow{V} \begin{pmatrix} 3 \\ 0 \\ -2 \\ 2 \end{pmatrix}$$

$$U = \begin{pmatrix} -4 \\ -3 \\ 3 \\ 2 \end{pmatrix}, V = \begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}, U = (-1)V + W = \begin{pmatrix} -3 \\ 0 \\ 2 \\ -2 \end{pmatrix}, \text{ donc } U \xrightarrow{V} \begin{pmatrix} -3 \\ 0 \\ 2 \\ -2 \end{pmatrix}$$

$$U = \begin{pmatrix} 0 \\ -3 \\ 3 \\ 2 \end{pmatrix}, V = \begin{pmatrix} 1 \\ 3 \\ -1 \\ -4 \end{pmatrix}, U^* = \begin{pmatrix} 0 \\ 3 \\ -3 \\ -2 \end{pmatrix} \text{ n'est pas précédé par } V \text{ donc } U \xrightarrow{V} U$$

Proposition 6. Le processus de réduction et les premières coordonnées

Démonstration.

1) Soit $U = \begin{pmatrix} a \\ \dots \\ \dots \end{pmatrix}$, où $a > 0$; il ne peut être réduit que par un vecteur lex-strictement positif $V = \begin{pmatrix} b \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq b \leq a$ et alors $U \xrightarrow{V} \begin{pmatrix} c \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq c \leq a$.

2) Soit $U = \begin{pmatrix} 0 \\ a \\ \dots \\ \dots \end{pmatrix}$, où $a > 0$; il ne peut être réduit que par un vecteur lex-strictement positif $V = \begin{pmatrix} 0 \\ b \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq b \leq a$ et alors $U \xrightarrow{V} \begin{pmatrix} 0 \\ c \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq c \leq a$.

3) Soit $U = \begin{pmatrix} 0 \\ a \\ \dots \\ \dots \end{pmatrix}$, où $a < 0$; alors $U^* = \begin{pmatrix} 0 \\ -a \\ \dots \\ \dots \end{pmatrix}$ il ne peut être réduit que par un vecteur lex-strictement positif $V = \begin{pmatrix} 0 \\ b \\ \dots \\ \dots \end{pmatrix}$, où $0 \leq b \leq -a$ et alors $U \xrightarrow{V} \begin{pmatrix} 0 \\ c \\ \dots \\ \dots \end{pmatrix}$. \square

Proposition 7.

Le reste d'un vecteur positif modulo un vecteur lex-strictement positif est positif

Démonstration.

Soit $U = \begin{pmatrix} u_1 \\ \dots \\ \dots \\ u_p \end{pmatrix} \succ 0$ et $V = \begin{pmatrix} v_1 \\ \dots \\ \dots \\ v_p \end{pmatrix}$, lex - strictement positif; si U n'est pas irréductible alors $\forall i, v_i > 0, u_i \geq v_i$ et le reste de U par V sera $U - E(\min\{u_i/v_i, v_i > 0\})V$, donc à coordonnées positives. \square

Définition 8. Réduction d'un p uplet U par un ensemble de p uplets lex-strictement positifs S

Soit le $n+m$ -uplet U et un ensemble de p -uplets $S = \{V_i, i \in I\}$ on dira que U est réduit à W modulo S lorsqu'il existe un ensemble d'indices (i_1, \dots, i_q) à valeurs dans I tel que $U \xrightarrow{V_{i_1}} \xrightarrow{V_{i_2}} \dots \xrightarrow{V_{i_q}} W$, où W est irréductible par les différents V_i ; W pourra être appelé « un reste » de U modulo S .

Théorème 9. Algorithme de construction de bases standard associée à un ensemble fini de p -uplets lex-strictement positifs $S = \{V_i, i \in I\}$.

On pose $S := \{V_i, i \in I\}$, $G := \{\{V_i, V_j\}, V_i \neq V_j\}$

tant que $G \neq \emptyset$

on prend $\{V_i, V_j\} \in G$, on pose $G := G - \{V_i, V_j\}, W :=$ une réduction de $(V_i - V_j)$ modulo S

si $W \neq 0$ on pose $G := G \cup \{\{V, W^*\}, V \in S\}, S := S \cup \{W^*\}$

L'algorithme de Buchberger s'arrête en un temps fini.

On désigne par S_∞ la famille obtenue, ce sera une base standard associée à S .

Exemple 10.

On considère les trois uplets $\begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \\ 0 \\ 0 \\ -1 \end{pmatrix}$, l'application de l'algorithme produit les six uplets: $\begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix}$.

Remarque 11.

Voici le détail des calculs:

Maxima 5.37.2 <http://maxima.sourceforge.net>

using Lisp GNU Common Lisp (GCL) GCL 2.6.12

Distributed under the GNU Public License. See the file COPYING.

Dedicated to the memory of William Schelter.

The function `bug_report()` provides bug reporting information.

```
(%i42) a:transpose(matrix([1,2,-1,0,0]));b:transpose(matrix([3,4,0,-1,0]));c:transpose(matrix([2,
```

$$a = \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}, b = \begin{pmatrix} 3 \\ 4 \\ 0 \\ -1 \\ 0 \end{pmatrix}, c = \begin{pmatrix} 2 \\ 5 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

première passe:

```
(%i45) b-a;b-a-a;v1:b-a-a;
```

```
(%o45) 
$$\begin{pmatrix} 2 \\ 2 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

```

```
(%o46) 
$$\begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix}$$

```

```
(%o47) 
$$\begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix}$$

```

```
(%i48) c-a;c-a-a;v2:c-a-a;
```

```
(%o48) 
$$\begin{pmatrix} 1 \\ 3 \\ 1 \\ 0 \\ -1 \end{pmatrix}$$

```

```
(%o49) 
$$\begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}$$

```

$$(\%o50) \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}$$

(%i93) b-c;v3:b-c;

$$(\%o93) \begin{pmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix}$$

$$(\%o94) \begin{pmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix}$$

deuxième passe

(%i53) a-v1;w1:a-v1;

$$(\%o53) \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}$$

(%i53) a-v2;a-v2-v3;

$$(\%o55) \begin{pmatrix} 1 \\ 1 \\ -3 \\ 0 \\ 1 \end{pmatrix}$$

$$(\%o56) \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}$$

(%i78) a-v3;a-v3-v2;w1:a-v3-v2;

$$(\%o78) \begin{pmatrix} 0 \\ 3 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

$$(\%o79) \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}$$

$$(\%o80) \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}$$

(%i60) b-v1;b-v1-2*a;

$$(\%o60) \begin{pmatrix} 2 \\ 4 \\ -2 \\ 0 \\ 0 \end{pmatrix}$$

$$(\%o61) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(%i68) b-v2;b-v2-a;b-v2-a-v3;b-v2-a-v3-a;

$$(\%o68) \begin{pmatrix} 3 \\ 3 \\ -2 \\ -1 \\ 1 \end{pmatrix}$$

$$(\%o69) \begin{pmatrix} 2 \\ 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

$$(\%o70) \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

$$(\%o71) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(%i73) b-v3;b-v3-c;

$$(\%o73) \begin{pmatrix} 2 \\ 5 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

$$(\%o74) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(%i81) c-v1;c-v1-a;c-v1-a-w1;

$$(%o81) \begin{pmatrix} 1 \\ 5 \\ -2 \\ 1 \\ -1 \end{pmatrix}$$

$$(%o82) \begin{pmatrix} 0 \\ 3 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

$$(%o83) \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix} \text{ (deja vu)}$$

(%i85) c-v2;c-v2-2*a;

$$(%o85) \begin{pmatrix} 2 \\ 4 \\ -2 \\ 0 \\ 0 \end{pmatrix}$$

$$(%o86) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(%i90) c-v3;c-v3-a;c-v3-a-v2;

$$(%o90) \begin{pmatrix} 1 \\ 6 \\ 0 \\ 1 \\ -2 \end{pmatrix}$$

$$(%o91) \begin{pmatrix} 0 \\ 4 \\ 1 \\ 1 \\ -2 \end{pmatrix}$$

$$(%o92) \begin{pmatrix} 0 \\ 3 \\ -1 \\ 1 \\ -1 \end{pmatrix} \text{ (qui menera à w1 comme plus haut);}$$

voila la troisième passe

(%i95) a-w1;

$$(\%o95) \begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix} (\text{deja vu})$$

(%i99) b-w1;b-w1-a;b-w1-a-2*v1;

$$(\%o99) \begin{pmatrix} 3 \\ 2 \\ 3 \\ -2 \\ 0 \end{pmatrix}$$

$$(\%o100) \begin{pmatrix} 2 \\ 0 \\ 4 \\ -2 \\ 0 \end{pmatrix}$$

$$(\%o101) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(%i108) c-w1;c-w1-a;c-w1-a-v1;c-w1-a-v1-v2;

$$(\%o108) \begin{pmatrix} 2 \\ 3 \\ 3 \\ -1 \\ -1 \end{pmatrix}$$

$$(\%o109) \begin{pmatrix} 1 \\ 1 \\ 4 \\ -1 \\ -1 \end{pmatrix}$$

$$(\%o110) \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}$$

$$(\%o111) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(%i113) v1-w1;v1-w1-v1;

$$(\%o113) \begin{pmatrix} 1 \\ -2 \\ 5 \\ -2 \\ 0 \end{pmatrix}$$

$$(\%o114) \begin{pmatrix} 0 \\ -2 \\ 3 \\ -1 \\ 0 \end{pmatrix} \text{ (dont * sera w1)}$$

$$(\%i124) \text{ -(v2-w1);z1:w1-v2;}$$

$$(\%o124) \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix}$$

$$(\%o125) \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix}$$

$$(\%i126) \text{ v3-w1;v3-w1-v1;}$$

$$(\%o126) \begin{pmatrix} 1 \\ -3 \\ 3 \\ -2 \\ 1 \end{pmatrix}$$

$$(\%o127) \begin{pmatrix} 0 \\ -3 \\ 1 \\ -1 \\ 1 \end{pmatrix}$$

$$(\%i129) \text{ a-z1;a-z1-v1;}$$

$$(\%o129) \begin{pmatrix} 1 \\ 1 \\ 4 \\ -1 \\ -1 \end{pmatrix}$$

$$(\%o130) \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix} \text{ (deja vu)}$$

$$(\%i144) \text{ b-z1;b-z1-a;b-z1-a-2*v1;}$$

$$(\%o144) \begin{pmatrix} 3 \\ 3 \\ 5 \\ -2 \\ -1 \end{pmatrix}$$

$$(\%o145) \begin{pmatrix} 2 \\ 1 \\ 6 \\ -2 \\ -1 \end{pmatrix}$$

$$(\%o146) \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix} \text{ (deja vu)}$$

(%i150) c-z1;t1:c-z1-2*a;

$$(\%o150) \begin{pmatrix} 2 \\ 4 \\ 5 \\ -1 \\ -2 \end{pmatrix}$$

$$(\%o151) \begin{pmatrix} 0 \\ 0 \\ 7 \\ -1 \\ -2 \end{pmatrix}$$

(%i153) v1-z1;v1-z1-v1;

$$(\%o153) \begin{pmatrix} 1 \\ -1 \\ 7 \\ -2 \\ -1 \end{pmatrix}$$

$$(\%o154) \begin{pmatrix} 0 \\ -1 \\ 5 \\ -1 \\ -1 \end{pmatrix} \text{ (* sera z1)}$$

(%i155) v2-z1;

$$(\%o155) \begin{pmatrix} 0 \\ 0 \\ 7 \\ -1 \\ -2 \end{pmatrix} \text{ (deja vu)}$$

(%i157) v3-z1;v3-z1-v1;

$$(\%o157) \begin{pmatrix} 1 \\ -2 \\ 5 \\ -2 \\ 0 \end{pmatrix}$$

$$(\%o158) \begin{pmatrix} 0 \\ -2 \\ 3 \\ -1 \\ 0 \end{pmatrix} (* \text{ sera } w1)$$

(%i159) w1-z1;

$$(\%o159) \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix} (\text{deja vu})$$

quatrième passe

(%i161) a-t1;a-t1-a;

$$(\%o161) \begin{pmatrix} 1 \\ 2 \\ -8 \\ 1 \\ 2 \end{pmatrix}$$

$$(\%o162) \begin{pmatrix} 0 \\ 0 \\ -7 \\ 1 \\ 2 \end{pmatrix} (* \text{ sera } t1)$$

(%i163) b-t1;

(%i164) b-t1;b-t1-b;

$$(\%o164) \begin{pmatrix} 3 \\ 4 \\ -7 \\ 0 \\ 2 \end{pmatrix}$$

$$(\%o165) \begin{pmatrix} 0 \\ 0 \\ -7 \\ 1 \\ 2 \end{pmatrix} (\text{idem})$$

(%i167) c-t1;c-t1-c;

$$(\%o167) \begin{pmatrix} 2 \\ 5 \\ -7 \\ 1 \\ 1 \end{pmatrix}$$

$$(\%o168) \begin{pmatrix} 0 \\ 0 \\ -7 \\ 1 \\ 2 \end{pmatrix} \text{ (idem)}$$

(%i172) v1-t1;v1-t1-v3;v1-t1-v3-z1;

$$(\%o172) \begin{pmatrix} 1 \\ 0 \\ -5 \\ 0 \\ 2 \end{pmatrix}$$

$$(\%o173) \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix}$$

$$(\%o174) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(%i175) v2-t1;

$$(\%o175) \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix} \text{ (idem)}$$

(%i177) v3-t1;v3-t1-v3;

$$(\%o177) \begin{pmatrix} 1 \\ -1 \\ -7 \\ 0 \\ 3 \end{pmatrix}$$

$$(\%o178) \begin{pmatrix} 0 \\ 0 \\ -7 \\ 1 \\ 2 \end{pmatrix} \text{ (* sera t1)}$$

(%i180) w1-t1;w1-t1-w1;

$$(\%o180) \begin{pmatrix} 0 \\ 2 \\ -10 \\ 2 \\ 2 \end{pmatrix}$$

$$(\%o181) \begin{pmatrix} 0 \\ 0 \\ -7 \\ 1 \\ 2 \end{pmatrix} (\text{idem})$$

(%i183) z1-t1;z1-t1-z1;

$$(\%o183) \begin{pmatrix} 0 \\ 1 \\ -12 \\ 2 \\ 3 \end{pmatrix}$$

$$(\%o184) \begin{pmatrix} 0 \\ 0 \\ -7 \\ 1 \\ 2 \end{pmatrix} (\text{idem})$$

(%i185)

Théorème 12.

Soit un ensemble fini de p uplets $S = \{V_i, i \in I\}$ et une base standard $S_\infty = \{W_j, j \in J\}$ associée à S ; un p -uplet V appartient au sous-groupe engendré par S si et seulement il est réduit modulo S_∞ .

Théorème 13. Unicité du reste d'un p -uplet modulo S_∞

Soit V un p -uplet positif, le reste de V modulo S_∞ est unique (indépendant de la réduction appliquée).

3. Application aux systèmes d'équations linéaires

Nous allons commencer par le cas des systèmes linéaires de la forme $AX=B$, où $A \in \mathcal{M}_{nm}(N)$ et $B \in \mathcal{M}_{n1}(N)$.

Rappelons

Définition 14. La matrice témoin d'un système linéaire

Soit une matrice $A \in \mathcal{M}_{nm}(N)$ on appellera matrice témoin du système la matrice

$$\bar{A} = \begin{pmatrix} A & B \\ -I_m & 0 \end{pmatrix} = \begin{pmatrix} A_1 & A_2 & \dots & A_m \\ -1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & \dots \\ \dots & 0 & -1 & \dots & \dots \\ \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}.$$

Proposition 15. La matrice témoin du système linéaire $AX=B$ permet de « tracer » la résolution

Soit une matrice $A \in \mathcal{M}_{nm}(N)$ et un vecteur colonne $B \in \mathcal{M}_{n1}(N)$, il existe un vecteur colonne $X = \begin{pmatrix} x1 \\ \dots \\ xm \end{pmatrix} \in \mathcal{M}_{m1}(N)$, tel que $AX=B$ si seulement si, en considérant la matrice

$$\bar{A} = \begin{pmatrix} A & \\ -I_m & \end{pmatrix} = \begin{pmatrix} A1 & A2 & \dots & Am \\ -1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & \dots \\ \dots & 0 & -1 & \dots & \dots \\ \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}, \bar{A}X = \begin{pmatrix} B \\ -X \end{pmatrix}, \text{ ce qui équivaut à } \begin{pmatrix} B \\ 0 \end{pmatrix} = \bar{A}X + \begin{pmatrix} 0 \\ X \end{pmatrix} (*).$$

Si on considère une base standard S_∞ associée à l'ensemble des colonnes $\bar{A}_1, \dots, \bar{A}_m$, l'égalité (*) est équivalente au fait que le reste de $\begin{pmatrix} B \\ 0 \end{pmatrix}$ modulo S_∞ est de la forme $\begin{pmatrix} 0 \\ X \end{pmatrix}$.

Or il a été montré plus haut (proposition 8) que le reste de $\begin{pmatrix} B \\ 0 \end{pmatrix}$ modulo S_∞ est nécessairement un $n+m$ uplet à coordonnées positives; donc la question se résume à savoir si les n premières coordonnées du reste sont nulles ou pas; l'unicité du reste modulo S_∞ nous conduit donc à

Théorème 16.

Soit $\mathcal{F} = \{W_1, \dots, W_t\}$ une base standard du sous-groupe engendré par $\left\{ \begin{pmatrix} A_1 \\ -1 \\ 0 \\ \dots \\ 0 \end{pmatrix}, \begin{pmatrix} A_2 \\ 0 \\ -1 \\ \dots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} A_m \\ 0 \\ \dots \\ \dots \\ -1 \end{pmatrix} \right\}$ et $V := \begin{pmatrix} B \\ 0 \end{pmatrix} \in \mathcal{M}_{n+m,1}(\mathbb{N})$.

$V' := V$

tant que $V' \neq 0$

s'il existe un $i \in \{1, \dots, t\}$ $W_i^+ \preceq V'$, prendre $j = \min\{i, W_i^+ \preceq V'\}$

alors si $V' \xrightarrow{W_j} R, V' := R$

Le reste de $\begin{pmatrix} B \\ 0 \end{pmatrix}$ modulo S_∞ est le $n+m$ uplet R ; si $R = \begin{pmatrix} 0 \\ X \geq 0 \end{pmatrix}$ X est solution (dans \mathbb{N}^m) du système $AX=B$, si dans R les n premières coordonnées ne sont pas nulles le système $AX=B$ ne possède pas de solution dans \mathbb{N}^m .

Remarque 17.

On comparera avec le point de vue polynomial de Conti-Traverso.

Exemple 18. $A = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 4 & 5 \end{pmatrix} B = \begin{pmatrix} 12 \\ 19 \end{pmatrix}$

On a vu plus haut une base standard associée à l'ensemble $\left\{ \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \\ 0 \\ 0 \\ -1 \end{pmatrix} \right\}$

$\left\{ \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ -3 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -5 \\ 1 \\ 1 \end{pmatrix} \right\}$

Pour résoudre le système $AX=B$ on part de $V' = \begin{pmatrix} 12 \\ 19 \\ 0 \\ 0 \\ 0 \end{pmatrix}$:

$$1) \begin{pmatrix} 12 \\ 19 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 9 \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 9 \\ 0 \\ 0 \end{pmatrix} \text{ d'où } V' := \begin{pmatrix} 3 \\ 1 \\ 9 \\ 0 \\ 0 \end{pmatrix}$$

$$2) \begin{pmatrix} 3 \\ 1 \\ 9 \\ 0 \\ 0 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 5 \\ 1 \\ 0 \end{pmatrix} \text{ d'où } V' := \begin{pmatrix} 1 \\ 1 \\ 5 \\ 2 \\ 0 \end{pmatrix}$$

$$3) \begin{pmatrix} 1 \\ 1 \\ 5 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 3 \\ 3 \\ 0 \end{pmatrix} \text{ d'où } V' := \begin{pmatrix} 0 \\ 1 \\ 3 \\ 3 \\ 0 \end{pmatrix}$$

$$4) \begin{pmatrix} 0 \\ 1 \\ 3 \\ 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ -1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 3 \\ 1 \end{pmatrix}$$

donc une solution est $\begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix}$.

Si les réductions sont réalisées dans un autre ordre, ce qui est possible, on pourra vérifier qu'on obtient quand même le reste $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 3 \\ 1 \end{pmatrix}$.

Remarque 19.

Le cas où A et/ou B contiennent des coefficients négatifs se ramène au cas précédent de la manière suivante:

Si la coordonnée b_i est strictement négative on remplace la i -ème équation L_i par $-L_i$; en conséquence il n'y a plus de condition de signe sur B.

Si l'un des coefficients de A est négatif on se reportera à [3] qui permet de transformer le système en un système où la matrice est à coefficients positifs.

4. Optimisation entière

Définition 20. *Optimisation entière*

Soient $A \in \mathcal{M}_{nm}(\mathbb{N})$ et un vecteur $B \in \mathcal{M}_{n1}(\mathbb{N})$ et une fonction de cout (linéaire) $f: X \mapsto {}^tCX$.

On cherche un m -uplet X_1 à coordonnées dans \mathbb{N} tel que

$$\begin{cases} AX_1 = B \\ {}^tCX_1 = \min \{ {}^tCX, AX = B \} \end{cases} \quad (***) .$$

Nous supposons désormais que le polyèdre d'équation $AX=B$ est borné (nous désignerons ce polyèdre par P), que le système possède des solutions (X_0); déterminer une (la) solution optimale revient à déterminer un élément du noyau de A qui permette de diminuer au mieux le coût.

4.1 Détermination d'une famille génératrice du noyau de A

Définition 21. $\text{Ker}(A)$

On désignera sous le nom de noyau de A (noté $\text{Ker}(A)$) l'ensemble des m -uplets X (à coordonnées dans Z) tels que $AX=0$; c'est un sous-groupe discret, on utilise aussi le mt réseau.

Proposition 22. La recherche d'une base standard pour le sous-groupe engendré par les colonnes de la matrice \bar{A} fournit une famille génératrice du noyau de A .

Démonstration.

Lors de la détermination de la base standard S_∞ associée à la famille des $(\bar{A}_1, \dots, \bar{A}_m)$ ont apparu des $n+m$ uplets de la forme $\begin{pmatrix} 0 \\ Z \end{pmatrix}$, où $Z \in \mathcal{M}_{m,1}(\mathbb{Z})$, qui appartiennent au sous-groupe \mathcal{A} engendré par les $\bar{A}_1, \dots, \bar{A}_m$; de l'égalité $\begin{pmatrix} A \\ -I \end{pmatrix} X = \begin{pmatrix} AX \\ -X \end{pmatrix}$ il découle que, si $\begin{pmatrix} U \\ V \end{pmatrix}$ appartient à la base standard, V appartient à $\text{Ker}(A)$ si et seulement si $U=0$.

Inversement soit un élément N du noyau de A alors $\begin{pmatrix} 0 \\ N \end{pmatrix}$ appartient au sous-groupe \mathcal{A} , et d'après le lemme 13 de [4] c'est une combinaison linéaire d'éléments de la base standard dont les n premières coordonnées sont nulles

Conclusion les éléments de la base standard de la forme $\begin{pmatrix} 0 \\ Z \end{pmatrix}$ constituent une partie génératrice de $\text{Ker}(A)$. \square

4.2 Une base standard associée au noyau

Comme on le verra au 4.3 le rôle des vecteurs du noyau sera de faire baisser le coût tout en maintenant le respect des contraintes mais ils ne sont pas organisés pour permettre la recherche pas à pas d'une diminution du coût; nous avons donc besoin d'un autre type de réduction.

Dans ce paragraphe nous considérons \mathbb{Z}^m

Définition 23. la relation d'ordre total \triangleleft

$$\text{Sur } \mathbb{Z}^m \quad U \triangleleft V \iff \begin{cases} f(U) < f(V) \\ \text{ou} \\ f(U) = f(V) \text{ et } U \alpha V \end{cases}$$

Définition 24. \triangleleft -réduction de X par Y , où $f(Y) > 0$

Soient X et Y , on appellera \triangleleft -réduction de X par Y l'égalité $X = \beta Y + Z$, où $\beta = \max \{k \in \mathbb{N}, 0 \triangleleft X - kY\}$; Z sera le \triangleleft reste de X modulo Y .

$$\text{notation: } X \xrightarrow{\triangleleft Y} Z$$

Dans le cas $\beta = 0$ on dira que X est \triangleleft -irréductible par Y .

Définition 25. \triangleleft -réduction de X par un ensemble fini S d'éléments Y_i , où $\forall i, 0 \triangleleft Y_i$

Soit X et un ensemble fini $S = \{Y_i\}$ tels que $\forall i, 0 \triangleleft Y_i$, on dira que X est \triangleleft -réduit à Z modulo S lorsqu'il existe un ensemble d'indices (i_1, \dots, i_q) à valeurs dans I tel que $X \xrightarrow{\triangleleft Y_{i_1}} \xrightarrow{\triangleleft Y_{i_2}} \dots \xrightarrow{\triangleleft Y_{i_q}} Z$, où Z est \triangleleft -irréductible par les différents Y_i ; Z pourra être appelé « un \triangleleft -reste » de X modulo S .

Définition 26.

Pour tout $Y \in \mathbb{Z}^m$ tel que $f(Y) \neq 0$ on désignera par Y^* celui, parmi Y et $-Y$, dont l'image par f est positive.

Pour tout $Y \in \mathbb{Z}^m$ tel que $f(Y)=0$ on désignera par Y^* celui, parmi Y et $-Y$, qui est lex-positif.

Théorème 27. (d'après le théorème de Buchberger)

On suppose donné un ensemble fini $S = \{Y_i, i \in I\} \subset \mathbb{N}^m$, où $\forall i, 0 \triangleleft Y_i$

On pose $S := \{Y_i, i \in I\}$, $G := \{\{Y_i, Y_j\}, Y_i \neq Y_j\}$

tant que $G \neq \emptyset$

on prend $\{Y_i, Y_j\} \in G$, on pose $G := G - \{Y_i, Y_j\}$, $Z :=$ une \triangleleft -réduction de $(Y_i - Y_j)^*$ modulo S

si $Z \neq 0$ on pose $G := G \cup \{\{V, Z^*\}, V \in S\}$, $S := S \cup Z^*$.

L'algorithme de Buchberger s'arrête en un temps fini.

Démonstration.

Pour montrer que l'algorithme s'achève en un temps fini il faut d'abord remarquer que les vecteurs de coût nul appartiennent au treillis d'équation $\begin{cases} AX = 0 \\ f(X) = 0 \end{cases}$ qui possède un nombre fini d'éléments lex-positifs minimaux.

D'autre part si $X \xrightarrow{\triangleleft Y} Z$, soit $f(Z)=0$ soit $0 < f(Z) < f(Y)$ donc au fur et à mesure de l'exécution les coûts strictement positifs, qui vont apparaître dans les réductions, décroissent strictement, par suite l'algorithme fournira un nombre fini d'éléments de coût strictement positif.

Par suite, comme plus haut, on trouvera un état final de S , S_∞ qui par sa construction contient S et les ensembles S et S_∞ engendrent le même sous-groupe additif.

S_∞ sera appelé une \triangleleft -base standard associée à S . □

Théorème 28. Le rôle des \triangleleft -bases standard

Soit un ensemble fini $S = \{Y_i, i \in I\} \subset \mathbb{Z}^m$ et une \triangleleft -base standard $S_\infty = \{Z_j, j \in J\}$ associée à S ; un élément $V \in \mathbb{Z}^m$ appartient au sous-groupe engendré par S si et seulement la \triangleleft -réduction modulo S_∞ de V est nulle; par suite le reste modulo S_∞ ne dépendra pas de l'ordre des réductions opérés.

Démonstration. analogue à la démonstration de ces propriétés dans [3] □

4.3 Recherche de la solution optimale

Une solution X_0 du système $AX=B$ est connue ainsi qu'une \triangleleft -base standard du noyau \mathcal{N} de A ; celle-ci est composée de m -uplets à coordonnées dans \mathbb{Z} , de coût supérieur ou égal à zéro.

Comme la solution optimale s'écrit $X_0 - N$, où N appartient au noyau, avec $0 \leq f(N)$, N s'écrit donc comme une combinaison linéaire $\sum m_i N_i$ (les m_i sont des entiers, les N_i dans la \triangleleft -base standard du noyau), comme nous avons affaire à une base standard nous ne dépendons pas de l'ordre dans lequel les éléments seront considérés, d'où l'idée de chercher chaque fois une translation qui permette de diminuer strictement le coût sans quitter le domaine admissible.

Théorème 29. Algorithme de recherche d'un point optimal

On suppose connues une solution X_0 et une \triangleleft -base standard du noyau $\mathcal{N} = \{N_i, i \in I\}$.

On pose $X := X_0$, $Y := X$; $\mathcal{N} = \{N_i, i \in I\}$

tant que $\mathcal{N} \neq \emptyset$

on prend $N_i \in \mathcal{N}$, on pose $\mathcal{N} := \mathcal{N} - \{N_i\}$, $\beta := \max\{k \in \mathbb{N}, 0 \triangleleft (X - kN_i) \wedge 0 \preceq (X - kN_i)\}$, $X := X - \beta N_i$.

Exemple 30. Recherche d'une solution du système $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix} X = \begin{pmatrix} 10 \\ 15 \end{pmatrix}$ qui optimise le coût $\begin{pmatrix} 1 & 3 & 14 & 17 \end{pmatrix} X$.

Une base standard de \mathcal{A} est :

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

Une première solution est $X_0 = \begin{pmatrix} 5 \\ 0 \\ 0 \\ 5 \end{pmatrix}$.

Une famille génératrice du noyau est $N_1 = \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix}, N_2 = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, N_3 = \begin{pmatrix} 0 \\ -1 \\ 2 \\ -1 \end{pmatrix}$.

L'étape suivante consiste à essayer de construire une base standard du noyau; on verra que ces 3 vecteurs constituent cette base standard.

Maxima 5.37.2 <http://maxima.sourceforge.net>
 using Lisp GNU Common Lisp (GCL) GCL 2.6.12
 Distributed under the GNU Public License. See the file COPYING.
 Dedicated to the memory of William Schelter.
 The function bug_report() provides bug reporting information.

```
(%i43) N1:matrix([1], [-2], [1], [0]); N2:matrix([1], [-1], [-1], [1]); N3:matrix([0], [-1], [2], [-1]); C:matrix([1, 3, 14, 17]);
```

```
(%o43)  $\begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix}$ 
```

```
(%o44)  $\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$ 
```

```
(%o45)  $\begin{pmatrix} 0 \\ -1 \\ 2 \\ -1 \end{pmatrix}$ 
```

```
(%o46) ( 1 3 14 17 )
```

```
(%i36) N2-N1;
```

```
(%o36)  $\begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}$  (deja vu)
```

(%o37) -8

(%i71) N1-N3;

$$(%o71) \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} \text{(deja vu)}$$

(%i90) N3-N2;C.(N3-N2-7*N2);

$$(%o90) \begin{pmatrix} -1 \\ 0 \\ 3 \\ -2 \end{pmatrix}$$

(%o91) 0

(%i76

(%i78)

$f(N_1)=9, f(N_2)=1, f(N_3)=8$

(on remarquera que, suivant la procédure proposée, N_3 est choisi lex-négatif car la « consigne » est $f(N) > 0$).

0) $f(X)=90$.

1) $X := \begin{pmatrix} 5 \\ 0 \\ 0 \\ 5 \end{pmatrix}$ rien avec N_1 , avec N_2 $k=5$ convient $X := \begin{pmatrix} 5 \\ 0 \\ 0 \\ 5 \end{pmatrix} - 5 \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \\ 5 \\ 0 \end{pmatrix}$; $f(X)=85$

2) $X := \begin{pmatrix} 0 \\ 5 \\ 5 \\ 0 \end{pmatrix}$, seul N_3 convient avec $k=2$ $X := \begin{pmatrix} 0 \\ 5 \\ 5 \\ 0 \end{pmatrix} - 2 \begin{pmatrix} 0 \\ -1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \\ 1 \\ 2 \end{pmatrix}$; $f(X)=69$

3) $X := \begin{pmatrix} 0 \\ 7 \\ 1 \\ 2 \end{pmatrix}$ aucun des N_i ne convient, donc l'optimum est atteint.

Conclusion

La méthode ici proposée a été inspirée par une lecture attentive de la démarche de Conti-Traverso qui adoptait le point de vue du reste modulo un idéal engendré par les contraintes du système; les binômes introduits par cette méthode algébrique ont été d'une certaine manière transformés en bipoints par R.Thomas, ouvrant la voie à une approche géométrique; celle-ci s'appuyait en un certain sens sur une vision affine des objets utilisés.

En fait l'aspect affine était lui aussi superflu pour la résolution des programmes linéaires en entiers.

On trouvera ici une illustration de ce caractère superflu:

Au lieu d'un binôme $a^2x^3y - b^0z^3t^2$ nous écrivons $\begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \\ -3 \\ -2 \end{pmatrix}$ et au lieu de $ay^2z - b^2x^2t^3$ nous écrivons $\begin{pmatrix} 1 \\ -2 \\ -2 \\ 2 \\ 1 \\ -3 \end{pmatrix}$ (avec l'ordre $a > b > x > y > z > t$).

Le calcul du S-polynome associé passe par le ppcm des monomes a^2x^3y et ay^2z qui est $a^2x^3y^2z$, puis $yz(a^2x^3y - b^0z^3t^2) - ax^3(ay^2z - b^2x^2t^3) = -a^0b^0yz^4t^2 + ab^2x^5t^3 - t^2(-a^0b^0yz^4t^0 + ab^2x^5z^0t)$, où l'on simplifie par le facteur commun en invoquant les propriétés de l'idéal d'un treillis, d'où le vecteur

$$\begin{pmatrix} 1 \\ 2 \\ 5 \\ -1 \\ -4 \\ 1 \end{pmatrix}.$$

Tandis qu'en soustrayant simplement les vecteurs on obtient directement

$$\begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \\ -3 \\ -2 \end{pmatrix} - \begin{pmatrix} 1 \\ -2 \\ -2 \\ 2 \\ 1 \\ -3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 5 \\ -1 \\ -4 \\ 1 \end{pmatrix}.$$

D'une part les deux méthodes conduisent au même résultat, d'autre part l'introduction du ppcm se traduit par une translation, puis la simplification par une nouvelle translation-retour. Notre méthode évite les deux translations, les calculs correspondants et diminue la taille des entiers (exposants des polynomes) utilisés et, par suite, la place dans la mémoire.

Les méthodes appliquant les bases de Grobner, tout comme les autres méthodes citées dans l'introduction, sont a priori de complexité exponentielle et la place occupée en mémoire constitue aussi un problème; il est difficile d'évaluer la complexité des deux constructions de bases standard et le bénéfice que pourrait éventuellement apporter la présentation vectorielle par rapport à la forme classique (polynomiale).

Les aspects originaux de notre étude concernent la **matrice témoin**, ainsi que la traduction vectorielle des notions polynômiales qui constituent une simplification conceptuelle tout autant que technique [4].

Ce travail doit aussi à Guy Chevalier qui m'a fait prendre conscience d'incohérences entre la relation d'ordre \triangleleft et la première version de l'algorithme du Théorème 29, qui ignorait tout simplement l'esprit de ce prapraphe.

Bibliographie :

[1] P.Conti et C.Traverso (1991), Buchberger algorithm and integer programming, pp. 130-139 in Proceedings AAEECC-9 (New-Orleans), Springer, LNCS 539

[2] R.R. Thomas (1995), A geometric Buchberger Algorithm for integer programming, Math.Operations Research 20, pp.864-884

[3] P. Teller (novembre 2016), Une question de signes, www.lalgebrisant.fr

[4] P. Teller (décembre 2016), Une version vectorielle des bases standard, www.lalgebrisant.fr