Quelques remarques sur le calcul des réductions de Hermite et de Smith

Résumé : Nous étudions dans cette note le problème du calcul des réductions de Hermite et de Smith pour les matrices non régulières, supposant connu le cas des matrices régulières

Introduction

Cette note est pour l'essentiel un extrait de [LLM]
Nous considérons un anneau principal «discret à division explicite» **A** . (par exemple l'anneau des entiers naturels, ou un anneau de polynomes sur un corps discret explicite)
Nous supposons que les déterminants sont «aisément» calculables dans **A** . Le fait que les déterminants dans **A** soient aisés à calculer est a priori une condition indispensable pour espérer calculer en un temps raisonnable les réduites de Hermite et Smith d'une matrice à coefficients dans **A** .
Nous appelons **F** le corps de fractions de **A** . Le fait de savoir calculer «aisément» les déterminants dans **A** permet de résoudre «aisément» les problèmes d'algèbre linéaire en dimension finie sur **F** , uniquement avec des calculs dans **A** . Par contre les problèmes d'algèbre linéaire dans **A** sont a priori plus difficiles.
Les problèmes d'algèbre linéaire en dimension finie sur **A** se ramènent en fait à des calculs de réductions de Hermite ou de Smith et à des calculs de produits de matrices à coefficients dans **A** (par réduction d'une matrice, nous entendons: calcul de la réduite et calcul de la ou des matrices unimodulaires de changement de base). En particulier la solution des systèmes d'équations linéaires à coefficients et inconnues dans **A** est entièrement claire à partir de la réduction de Hermite des matrices.
Les méthodes «brutales» (recopiant les preuves explicites d'existence de la réduction de Hermite ou de celle de Smith) conduisent en pratique à une explosion de la taille des objets de l'anneau **A** manipulés par l'algorithme.

Les articles parus qui étudient des algorithmes séquentiels évitant l'explosion de la taille des objets intermédiaires ne traitent que le cas des matrices carrées non singulières (et, quelquefois, le cas des matrices rectangulaires dont le rang est égal au nombre de lignes, pour la réduction de Hermite). Cette note rappelle quelques généralités sur les réductions de Smith et Hermite et explique comment le cas général peut être traité à partir du cas des matrices carrées non singulières.

Définitions et notations

Nous nous situons dans le cadre général de la théorie constructive des anneaux principaux discrets (cf. [MRR] chap. IV, V) à division explicite. Un *anneau principal discret à division explicite* (au sens constructif) est un anneau intègre donné dans une présentation où :

l'anneau est discret : le test d'égalité est explicite,
l'anneau est explicite : les lois de compositions sont explicites,
l'anneau est explicitement de Bezout : on sait calculer à partir de a et b arbitraires, des éléments u, v, c, d, g avec :

$$u\,a + v\,b = g\,,\quad g\,d = a,\quad g\,c = b,$$

ce qui donne une matrice carrée de déterminant 1 avec :

$$(a,b)\begin{pmatrix} u & -c \\ v & d \end{pmatrix} = (g,0),$$

l'anneau est à division explicite : le test de divisibilité, et, en cas de réponse positive, le calcul du quotient, sont explicites, en particulier on a un test d'inversibilité et en cas de réponse positive, un calcul explicite de l'inverse,

toute suite décroissante pour la divisibilité contient deux termes consécutifs associés (c.-à-d. divisibles l'un par l'autre) : ceci est la condition de noetheriannité exprimée constructivement.

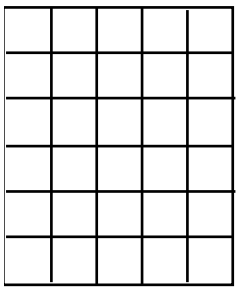
Tant que n'est pas envisagé le problème de la réduite de Smith, la condition de noetheriannité n'intervient aucunement. Si on supprime cette exigence, on dira que l'anneau **A** est un *anneau de Bezout explicite*.

Nous considérons donc un anneau de Bezout explicite **A** et une matrice M de type $s \times r$ (s lignes et r colonnes) à entrées dans **A**. Nous appelons **F** le corps de fractions de **A**. Nous notons :

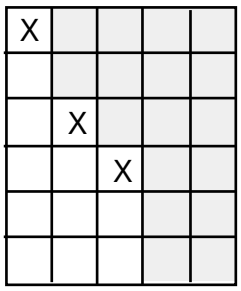
L le module libre $\mathbf{A}^s$,
$e_1, \ldots, e_s$ la base canonique de L,
pour $k = 1, \ldots, s$; F_k est le sous-**A**-module de L engendré par $e_k, \ldots, e_s$
$\Pi_k : L \longrightarrow \mathbf{A}$ la k-ème forme coordonnée
$V_1, \ldots, V_r$ les vecteurs colonnes de M (considérés comme des éléments de L),
E le sous-**A**-module de L engendré par $V_1, \ldots, V_r$
$E_k = E \cap F_k$
$E'_k = \Pi_k(E_k)$ qui est un idéal de **A**

Nous dirons qu'une matrice carrée est **unimodulaire** si son déterminant est inversible dans l'anneau **A** (il revient au même de dire que la matrice est inversible dans l'anneau des matrices carrées $\mathbf{M_r}(\mathbf{A})$).

Une **réduite de Hermite** de la matrice M est par définition une matrice M' de mêmes dimensions que M, dont les vecteurs colonnes engendrent le même sous-**A**-module E et qui de plus est «sous-triangulaire» au sens que les colonnes de M' successives contiennent de plus en plus de zéros au dessus de la première entrée non nulle. (voir figure).



matrice M



réduite de Hermite M'

Les croix représentent des entrées non nulles, les **pivots** de la matrice M', et la partie grisée représente des zéros : le nombre de zéros au dessus de la première entrée non nulle est strictement croissant tant que la colonne n'est pas entièrement nulle.

Une **réduction de Hermite** de la matrice M est donnée par une réduite de Hermite M' de M et une matrice unimodulaire P de type $r \times r$ vérifiant : $M.P = M'$

u	0	**-c**	0	0
0	1	0	0	0
v	0	**d**	0	0
0	0	0	1	0
0	0	0	0	1

Une réduction de Hermite de M peut être calculée en multipliant M à droite par des «matrices de Bezout» (une partie 2×2 du type Bezout, et le restant égal à la matrice identité : voir figure, avec $ud + vc = 1$) de manière à rendre nulles les entrées convenables les unes après les autres. Par exemple la matrice ci-contre, par multiplication à droite, produit une manipulation des colonnes 1 et 3, qui permet de remplacer, sur une ligne donnée, les coefficients a et b par g et 0. Dans l'exemple dessiné

au dessus, on peut obtenir M' à partir de M en la multipliant par 9 matrices de Bezout successives.

Remarque : Une **manipulation élémentaire de colonnes** est un échange de colonnes ou le remplacement de la $i^{ème}$ colonne C_i par $C_i + a\,C_j$ avec $j \neq i$. Une **matrice de manipulation élémentaire** est obtenue en faisant subir une manipulation élémentaire de colonne à la matrice I. Faire une manipulation élémentaire de colonnes (resp. de lignes) sur une matrice revient à la multiplier à droite (resp. à gauche) par une matrice de manipulation élémentaire. Dans un anneau euclidien, les matrices de Bezout peuvent s'écrire comme produit de matrices de manipulations élémentaires. On en déduit que dans un anneau euclidien une matrice unimodulaire peut s'écrire comme produit d'une matrice unimodulaire diagonale et de matrices de manipulations élémentaires.

Une matrice D est dite sous forme **réduite de Smith** si ses seuls coefficients non nuls sont les d_i en position (i,i) pour $i = 1,\ldots, k \leq \inf(r,s)$, et si en outre $d_1 \mid d_2 \mid \ldots \mid d_k$.
Une **réduction de Smith** de la matrice M de type $s \times r$ est donnée par une matrice D sous forme réduite de Smith et deux matrices unimodulaires P de type $r \times r$ et Q de type $s \times s$ vérifiant : Q.M.P = D.
La réduite D est unique modulo la multiplication des d_i par des inversibles.
On peut calculer une réduction de Smith de M comme suit. On calcule une réduction de Hermite M_1 par manipulations élémentaires de colonnes, puis une réduction de Hermite de la transposée de M_1 par manipulations élémentaires de lignes de M_1, ce qui donne une matrice M_2. On recommence le processus jusqu'à obtenir une matrice diagonale. On termine ensuite facilement le passage de la forme diagaonale à la forme de Smith.
Remarque: dans l'anneau de Bezout non noethérien de tous les entiers algébriques, toute matrice admet une réduction de Smith. Il semble qu'on ignore toujours si une réduction de Smith existe pour toute matrice dans tout anneau de Bezout. (Kaplanski [Kap] montre que dans un anneau de Bezout toute matrice admet une réduction de Smith si et seulement si toute matrice triangulaire 2×2 en admet une)

De la réduction de Hermite à la résolution des systèmes linéaires

Si nous voulons résoudre un système linéaire *à coefficients et inconnues dans* **A**, nous l'écrivons sous la forme : M X = B. Si une réduction de Hermite pour M est M P = M' avec P V = I_r, on considère le système auxiliaire M' Y = B.
Si on teste la compatibilité du système auxiliaire, on a par là-même un test de compatibilité du système initial.
Et si en cas de réponse positive on détermine une solution particulière avec second membre et la solution générale sans second membre pour le système auxiliaire, on récupèrera les résultats analogues pour le premier système en multipliant à gauche par la matrice V inverse de P.
Soit t le rang de la matrice M', c.-à-d. le nombre de colonnes non nulles. Le test de compatibilité revient à chercher la solution particulière Y_0 où les $r - t$ dernières coordonnées sont nulles. On voit apparaître alors deux types de conditions de compatibilité. Le premier type est fourni par l'existence d'une solution Y_0 dans le corps des fractions de **A**, et les conditions correspondantes sont l'annulation de certains déterminants construits à partir des entrées de M' et de B. Le deuxième type de condition est fourni par les relations de divisibilité entre certains déterminants, relations de divisibilité qui font que la solution particulière Y_0 dans le corps des fractions est en fait une solution dans **A**.

5				
3				
4	3			
2	7	12		
6	2	1		
5	8	-13		

Prenons l'exemple de la réduite de Hermite ci contre avec l'anneau Z et le second membre B avec des entrées b_i indéterminées. Les conditions du premier type sont :

$$\begin{pmatrix} 5 & b_1 \\ 3 & b_2 \end{pmatrix} = 0$$

$$\begin{pmatrix} 5 & 0 & 0 & b_1 \\ 4 & 3 & 0 & b_3 \\ 2 & 7 & 12 & b_4 \\ 6 & 2 & 1 & b_5 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 0 & b_1 \\ 4 & 3 & 0 & b_3 \\ 2 & 7 & 12 & b_4 \\ 5 & 8 & -13 & b_6 \end{pmatrix} = 0$$

Les conditions du deuxième type sont :

$$5 \text{ divise } b_1 \,,\ \begin{pmatrix} 5 & 0 \\ 4 & 3 \end{pmatrix} \text{ divise } \begin{pmatrix} 5 & b_1 \\ 4 & b_3 \end{pmatrix} \,,\ \begin{pmatrix} 5 & 0 & 0 \\ 4 & 3 & 0 \\ 2 & 7 & 12 \end{pmatrix} \text{ divise } \begin{pmatrix} 5 & 0 & b_1 \\ 4 & 3 & b_3 \\ 2 & 7 & b_4 \end{pmatrix}$$

On notera que tous les déterminants qui interviennent dans ce calcul sont, ou bien des formes linéaires (à coefficients dans **A**) par rapport à B, ou bien, (pour les dénominateurs des fractions qui doivent être égales à des éléments de **A**) des constantes (des déterminants extraits de M' et ne dépendant donc pas de B).
Quant à la solution générale Y_g sans second membre du système auxiliaire, elle est fournie par tous les vecteurs colonnes ayant leurs t premières coordonnées nulles.
La solution générale du premier système est alors $X = V(Y_0 + Y_g)$ avec $r - t$ degrés de liberté.
La morale de ces considérations est, que, une fois calculée une réduction de Hermite de la matrice M, on aura un calcul de la compatibilité du système linéaire $MX = B$, et, en cas de réponse positive, un calcul de ses solutions, qui utilise seulement les calculs de déterminants dans **A**, les tests de divisibilité dans **A**, les divisions exactes dans **A** et les produits de matrices dans **A**. En pratique, cela signifie que la complexité du calcul total est du même ordre de grandeur que celle du calcul de la seule réduction de Hermite de la matrice M.

Algèbre linéaire sur **A** et algèbre linéaire sur **F**

Nous supposons que les déterminants sont «aisément» calculables dans **A** (par exemple par la méthode de Bareiss ou celle de Berkovitz-Samuelson), ce qui revient grosso modo à dire que les opérations d'addition, soustraction, multiplication sont «aisées» et que les déterminants sont convenablement majorés en taille (pour la méthode de Bareiss, il faut aussi que les divisions exactes sont «aisées»).
Le fait de savoir calculer «aisément» les déterminants dans **A** permet de résoudre «aisément» les problèmes d'algèbre linéaire en dimension finie sur **F**, uniquement avec des calculs dans **A**. Par contre les problèmes d'algèbre linéaire dans **A** sont a priori plus difficiles.

Dans la suite nous parlons de « triangulation dans **F** d'une matrice M » lorsque nous calculons des matrices M' et P avec :

> $M' = M.P$, P inversible dans **F** *mais pas nécessairement dans* **A**, et M' sous forme triangulaire de Hermite comme expliqué au paragraphe précédent.

En pratique, cette triangulation dans **F** se fait par la méthode de Bareiss ou celle de Berkovitz-Samuelson, méthodes qui impliquent uniquement des calculs dans l'anneau des entrées de M. Toutes les entrées non nulles de M' sont alors égales à des déterminants extraits de M.
En résumé : une triangulation dans **F** ne signifie pas que les calculs ont lieu dans **F** (ils ont lieu dans **A**) mais que la matrice inversible P est a priori seulement inversible dans **F**.

Une caractérisation algébrique «abstraite» des réduites de Hermite

Proposition : On reprend les notations du début du a).
On considère un entier $t \leq r$ et une matrice M' dont les t premières colonnes sont non nulles et les $r-t$ dernières nulles. On note $W_1, \ldots, W_t$ les t premiers vecteurs colonnes de M', k_i (i=1, ... , t) le numéro de la première entrée non nulle de W_i, w_i l'entrée en question.
i) Si M' est une réduite de Hermite de M, les conditions suivantes sont vérifiées :
- la suite k_i (i=1, ... , t) est strictement croissante
- w_i (i=1, ... , t) engendre l'idéal E'_{k_i}
- $E'_k = \{0\}$ pour tout k distinct des k_i

ii) Réciproquement, si les W_i sont dans E et si les trois conditions ci-dessus sont vérifiées, la matrice M' est une réduite de Hermite de M .

Corollaire : Etant données deux réduites de Hermite M' et M" d'une même matrice M de type $s \times r$, il existe une matrice Q de type $r \times r$, sous-triangulaire et avec des inversibles sur la diagonale telle que M'.Q = M" . En particulier toute réduite de Hermite de M provient d'une réduction de Hermite de M (c.-à-d. est de la forme M.P avec P unimodulaire).

Remarque sur les coefficients pivots de la réduite de Hermite. Le produit à droite par une matrice unimodulaire ne change pas le pgcd des mineurs d'ordre m extraits sur m lignes fixées d'une matrice. En conséquence, nous avons :

w_1 = pgcd des coefficients de la ligne numéro k_1 de M (à un inversible près)
$w_1 w_2$ = pgcd des mineurs d'ordre 2 extraits sur les lignes numéro k_1 et k_2 de M
$w_1 w_2 w_3$ = pgcd des mineurs d'ordre 3 .... etc ...

Remarque sur la triangulation dans F de la matrice M.
Une triangulation de M dans **F** sans échange de ligne n'est rien d'autre que le calcul d'une réduite de Hermite de la matrice M , lorsque l'anneau considéré est le corps **F** (qui, étant un corps explicite, est a fortiori un anneau de Bezout explicite). Notez que la triangulation dans **F** de la matrice M fournit la «forme» de la réduite de Hermite dans **A** , c.-à-d. le rang de la matrice et les numéros k_i des lignes des pivots.

Cas des entiers naturels

Lorsque l'anneau **A** est Z , on peut définir, parmi toutes les réduites de Hermite d'une matrice M , une **réduite normale**. C'est celle où les pivots sont positifs, et les coefficients à gauche du pivot w_i sont réduits modulo w_i (on peut choisir quelle réduction modulo w_i on utilise, ce qui modifie la réduite normale). Lorsque le type de «réduction modulo» est fixé, la réduite normale est unique, et elle est alors de taille «raisonnable». Il a néanmoins fallu attendre [KB] pour avoir un algorithme qui calcule la réduite normale en évitant l'explosion exponentielle de la taille des coefficients intermédiaires. A noter que Frumkin (références [Fru]) donne auparavant une méthode modulaire en temps polynomial pour la résolution des systèmes linéaires en entiers, sans traiter la réduction des matrices en tant que telle.

De la réduite de Hermite générale à la réduction de Hermite

Certains algorithmes de calculs de réduites de Hermite fonctionnent sans restriction aucune sur la matrice. Voyons comment le fait de savoir calculer rapidement une réduite de Hermite (pour une matrice M arbitraire) permet de calculer rapidement une réduction de Hermite.

Considérons en effet la matrice N obtenue à partir de M en «collant» en dessous une matrice identité de type $r \times r$ et calculons une réduite de Hermite N' de N. Elle est constituée d'une matrice M' de type $s \times r$ avec collée en dessous une matrice P de type $r \times r$. Comme les colonnes de N et celles de N' engendrent le même sous-**A**-module de $\mathbf{A}^{s+r}$ il existe deux matrices U et V de type $r \times r$ à entrées dans **A** telles que : $N\,U = N'$ et $N'\,V = N$. D'où on tire facilement que $U = P$ et $P\,V = I_r$. Donc $M\,P = M'$, avec P unimodulaire. Et la matrice M' est bien de la forme voulue.

$$\begin{bmatrix} M \\ I_r \end{bmatrix} \cdot \boxed{U} = \boxed{N'} = \begin{bmatrix} M' \\ U \end{bmatrix} \quad , \quad \boxed{N'} \cdot \boxed{V} = \begin{bmatrix} M'.V \\ U.V \end{bmatrix} = \begin{bmatrix} M \\ I_r \end{bmatrix}$$

De la réduite de Hermite non singulière à la réduction de Hermite générale

Certains algorithmes de calcul des réduites de Hermite ne fonctionnent bien que dans le cas d'une matrice carrée non singulière. Dans ce paragraphe, nous indiquons comment, à partir de ce cas, on peut traiter le cas général

Premier cas, matrice carrée non singulière

Soit M' la réduite de Hermite de M, on cherche P, unimodulaire, tel que $M' = M\,P$.
Comme la solution est unique et automatiquement unimodulaire, elle se calcule par les algorithmes d'algèbre linéaire dans le corps des fractions **F**.

Deuxième cas, matrice de rang égal à son nombre de colonnes

Une triangulation dans **F** de la matrice M donne les numéros des lignes des pivots. On extrait de M la matrice N correspondant à ces lignes. On calcule la réduction de Hermite $N' = N\,P$, on a la réduction de Hermite de M en faisant $M' = M\,P$.

Troisième cas, matrice de rang égal à son nombre de lignes (cf. [KB])

La matrice M est une matrice de type $s \times r$, de rang s avec $r > s$.
Par triangulation dans **F** de la matrice, on détermine une permutation de colonnes qui permet de ramener s colonnes indépendantes en première position.

Nous supposons désormais que la matrice est de ce type.
($\det(M_1) \neq 0$)

$$\begin{array}{|c|c|} \hline M_1 & M_2 \\ \hline \end{array}$$

On considère alors la matrice M_3 non singulière égale à :

$$\begin{array}{|c|c|} \hline M_1 & M_2 \\ \hline 0 & I_{r-s} \\ \hline \end{array}$$

Une réduite de Hermite de M_3 est une matrice
$T = M_3 . P$ avec P unimodulaire

T_1	0
U	T_2

Alors $T' =$ | T_1 | 0 | est une réduite de Hermite de M puisque $T' = M . P$.

Cas général

Supposons maintenant le rang de M strictement inférieur à r .
On commence, par une triangulation dans **F** de la matrice M (sans échange de lignes) à calculer les indices k_1 , ..., k_t des lignes des pivots.
On décompose la matrice en blocs successifs de manière à séparer les lignes portant des pivots, des autres. Par exemple, avec $s = 8$, $r = 6$, $k_1 = 1$, $k_2 = 2$, $k_3 = 4$, $k_4 = 5$, $k_5 = 8$, on a les 5 blocs ci-contre.

M =

M_1
M_2
M_3
M_4
M_5

On conserve uniquement les blocs portant les pivots, et on obtient une matrice N qui rentre dans le troisième cas examiné :

N =

M_1
M_3
M_5

Soit alors $N.P = T'$ une réduction de Hermite de N . On décompose P en blocs verticaux de manière à faire apparaître dans le produit les blocs triangulaires $M_i.P_i$ sur la diagonale :

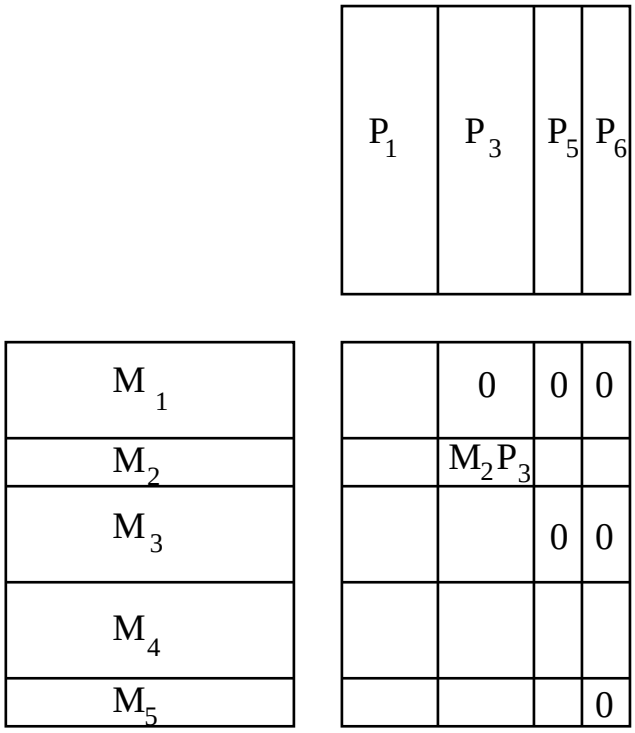
P_1	P_3	P_5	P_6

M_1
M_3
M_5

M_1P_1	0	0	0
M_3P_1	M_3P_3	0	0
			0

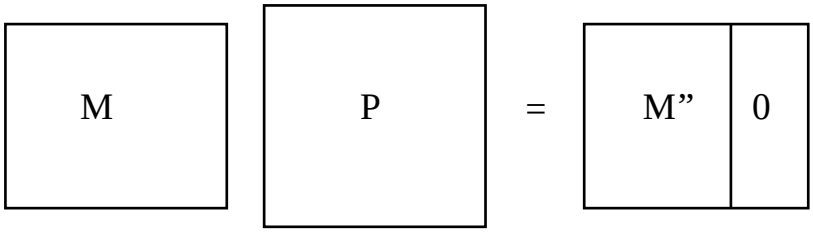
Montrons alors que M.P = T" est une réduction de Hermite de M

Puisque P est unimodulaire, il suffit de montrer que la matrice T" est de la forme voulue, ce qui revient à dire que des blocs tels que $M_2.P_3$ sont nuls.
Si $M_2.P_3$ n'était pas nulle, comme M_1P_3 = une matrice nulle, il y aurait une combinaison linéaire qui annulerait les colonnes de M_1 sans annuler celles de M_2 . Cela revient à dire qu'il y a un hyperplan qui contient les lignes de M_1 mais ne contient pas toutes les lignes de M_2 , c.-à-d. encore que la matrice obtenue en mettant M_1 au dessus de M_2 aurait un rang supérieur au rang de M_1 , mais ceci contredit la triangulation de M dans **F** .

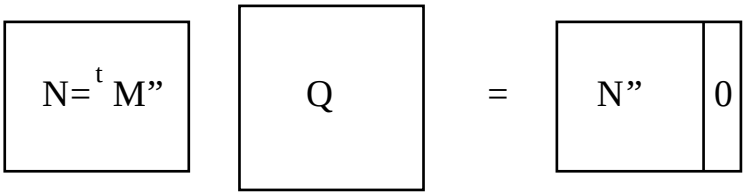


Des réductions de Hermite et de Smith non singulière à la réduction de Smith générale

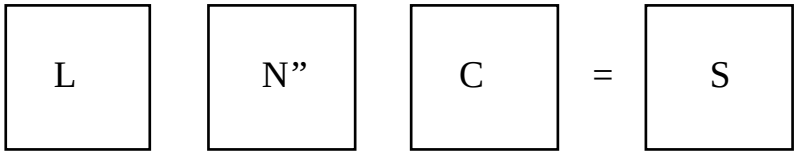
Nous supposons avoir un algorithme convenable (en temps polynomial par exemple) pour la réduction de Hermite et un autre pour la réduction de Smith dans le cas des matrices carrées non singulières. Nous obtenons la réduction de Smith en enchainant deux réductions de Hermite et une réduction de Smith non singulière. (nous ne rappelons ici pas la définition bien connue de la réduction de Smith)
Soit en effet M une matrice rectangle ou carrée singulière, et M.P = M' une réduction de Hermite. Si M" est la matrice extraite de M' en ne conservant que les colonnes non nulles, il est clair qu'il suffit de calculer une réduction de Smith de M".



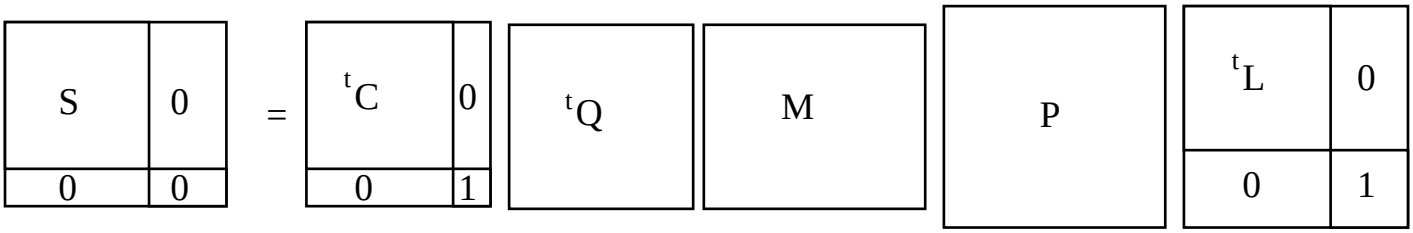
Si M" est carrée donc non singulière on sait par hypothèse calculer cette réduction de Smith (cela signifiait pour M que son rang était celui de son nombre de lignes).
Sinon, soit N la matrice transposée de M" et soit N.Q = N' une réduction de Hermite de N . Soit enfin N" la matrice extraite de N' en ne gardant que les colonnes non nulles.



Cette fois-ci, N" est non singulière, et on sait calculer une réduction de Smith.



Ce qui donne la réduction de Smith de M :



Notons enfin que si le rang de M est égal à son nombre de colonnes, on fait le calcul ci dessus avec la transposée de M ce qui évite la deuxième réduction de Hermite.

Salah LABHALLA Marrakech
Henri LOMBARDI Besançon
Roger MARLIN Nice

Bibliographie, références

[**Bar**] Bareiss E. H. : *Sylvester's Identity and Multistep Integer-Preserving Gaussian Elimination.* Math. Comp. 22 565-578 (1968) .

[**Ber**] Berkovitz S. J. : *On computing the determinant in small parallel time using a small number of processors*. Information Processing Letters 18 numéro 3 147-150 (1984) .

[**CC**] Chou T.-W., Collins G. : *Algorithms for the solution of systems of lineardiophantine equations.* Siam J. on Computing 11 (4) 687-708 (1982)

[**DKT**] Domich D., Kannan R., Trotter L. : Hermite normal form computation using modulo determinant arithmetic, Math. Oper. Res., 12, pp. 50-59 (1987)

[**Fru1**] Frumkin M.: *An application of modular arithmetic to the construction of algorithms solving systems of liear equations.* Soviet. Math. Dokl., 17, pp. 1165-1169. (1976)

[**Fru2**] Frumkin M.: *Polynomial time algorithms in the theory of linear diophantine equations.* In Fundamentals of computation theory, M. Karpinsky ed. LNCS 56. pp. 386-392. (1977)

[**Fru3**] Frumkin M.: *Complexity questions in number theory.* J. Soviet. Mat., 29, pp. 386-392 (1985)

[**HM**] Hafner J., McCurley K. : Asymptotically fast triangularization of matrices over rings.Siam J. Comput., 20 (6), 1068-1083 (1991)

[**Kap**] Kaplanski I. : *Elementary divisors and modules.* Transactions of the A.M.S., vol 66, (1949), 464-491.

[**Ili1**] Iliopoulos C. : *Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrice.* Siam J. on Computing 18 numéro 4 658-669 (1989)

[**Ili2**] Iliopoulos C. : *Worst-case complexity bounds on algorithms for computing the canonical structure of infinite abelian groups and solving systems of linear diophantine equations.* Siam J. on Computing 18 (4) 670-678 (1989)

[**KB**] Kannan R., Bachem A. : *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix.* Siam J. on Computing 8 (4) 499-507 (1979)

[**LLM**] Labhalla L., Lombardi H., Marlin R. : *Algorithmes modulaires de calcul des réductions de Hermite et de Smith* . Rapport technique avril 92

[**MRR**] R. Mines, F. Richman, W. Ruitenburg : *A Course in Constructive Algebra* (Springer-Verlag; Universitext; 1988) .

[**Sam**] Samuelson P. A. : *A method for determining explicitly the coefficients of the characteristic equation* . Ann. Math. Stat. 13 (1942) 424-429.

[**Sch**] Schrijver A.: *Theory of integer and linear programming*. John Wiley. New-York. (1985)