Algorithmes de calcul de la réduction de Hermite d'une matrice à coefficients polynomiaux

Salah LABHALLA Marrakech
Henri LOMBARDI Besançon
Roger MARLIN Nice

Résumé : Nous étudions dans cet article des algorithmes de calcul de la réduction de Hermite d'une matrice à coefficients polynomiaux, qui évitent l'explosion de la taille des objets intermédiaires et ont une bonne complexité séquentielle. Le deuxième et le troisième algorithmes généralisent la méthode des sous-résultants pour le calcul du pgcd de deux polynômes. Le dernier de ces algorithmes semble optimal en ce sens qu'il calcule une réduction de Hermite avec une matrice de passage de degré minimal, en utilisant une méthode progressive et économique. Nous ramenons le calcul de la réduite de Hermite à un problèmes de triangulation progressive de matrices dont les tailles sont bien contrôlées et dont les entrées sont des coefficients des polynômes donnés en entrée. L'algorithme est donc faisable dès qu'on dispose d'une méthode de triangulation en temps polynomial pour les matrices dans le corps des coefficients. Il revient au même de dire que le calcul des déterminants est en temps polynomial dans le corps en question (pour le codage choisi). Les résultats théoriques sont meilleurs que pour les algorithmes connus précédemment, et les résultats pratiques sont encourageants.

Abstract : In this paper, we study some algorithms for computing an Hermite reduction of a matrix with polynomial entries which avoid the swell-up of the size of intermediary objects and have a good sequential complexity. The second and the third algorithms generalize the sub-resultant method for computing the gcd of two polynomials. The last one is optimal in the sense that it computes an Hermite reduction with a minimal degree change of basis matrix. The Hermite reduction with polynomials entries amounts to a linear algebra problem over the coefficient field with a good control of the dimensions. Our problem of linear algebra is a progressive triangulation of matrices. So it is feasible exactly when there exists a polynomial time algorithm computing determinants of matrices with entries in the coefficient field of the polynomials given as input. Theoreticals results are better than for previously known algorithms, and practical results are interesting.

1) Introduction

Nous considérons un anneau de polynômes $\mathbf{A} = \mathbf{K}[X]$ où $\mathbf{K}$ est un corps dans lequel «l'algèbre linéaire est aisée», c.-à-d. dans lequel les calculs de déterminants sont «aisés» (par exemple le corps est codé de manière que ces calculs aient lieu en temps polynomial). Les calculs de déterminants dans $\mathbf{A}$ sont alors eux-mêmes aisés.

Nous appelons $\mathbf{F}$ le corps de fractions de $\mathbf{A}$. Le fait de savoir calculer «aisément» les déterminants dans $\mathbf{A}$ permet de résoudre «aisément» les problèmes d'algèbre linéaire en dimension finie sur $\mathbf{F}$, uniquement avec des calculs dans $\mathbf{A}$. Par contre les problèmes d'algèbre linéaire dans $\mathbf{A}$ 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» (qui recopient 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.

Dans cet article, nous donnons pour ce type de problèmes des algorithmes séquentiels qui évitent l'explosion de la taille des objets intermédiaires.

Nous remarquons comme Kaltofen, Krishnamoorthy et Saunders dans [KKS] que le calcul de la réduction de Hermite d'une matrice à coefficients dans **A** se ramène à un problème d'algèbre linéaire sur **K** avec un bon contrôle de la dimension. Nous formulons tout d'abord un problème d'algèbre linéaire sur **K** , équivalent au calcul de la réduction normale de Hermite de la matrice, dans le même esprit que [KKS].

Nous proposons ensuite deux algorithmes nettement plus simples qui résolvent le problème posé par simple triangulation d'une matrice à coefficients dans **K** , dont la taille est majorée de manière précise. Nous ne calculons plus la réduite normale, mais celle-ci ne présente pas une utilité spécifique bien grande. En outre, elle est facilement calculée à partir d'une réduite arbitraire. Par contre la réduite, non nécessairement normale, que nous calculons est obtenue beaucoup plus facilement. Le deuxième et le troisième algorithmes généralisent la méthode des sous-résultants pour le calcul du pgcd de deux polynômes.

Le premier de ces algorithmes est une pure triangulation de matrice à coefficients dans **K** , particulièrement simple à implanter. La matrice à trainguler est fixée a priori. Après la triangulation de cette matrice, il suffit d'inspecter le résultat pour en déduire une réduite de Hermite de la matrice de départ (à coefficients dans **K**[X]).

Dans le deuxième algorithme, que nous appelons HERMIPOL, nous proposons une triangulation progressive, le nombre de lignes et de colonnes n'étant pas fixé a priori. Ceci permet de majorer la taille de la matrice qui est finalement triangulée non seulement en fonction de la taille des entrées mais aussi en fonction de la taille des sorties. Plus précisément, s'il est possible d'obtenir une réduite de Hermite avec une matrice de passage de faible degré, l'algorithme trouvera le résultat plus rapidement. Non seulement le temps de calcul sera meilleur, mais la taille des coefficients dans la réduite calculée sera mieux majorée a priori.

Ces deux algorithmes sont nettement plus simples, et bien meilleurs en complexité séquentielle que celui proposé dans [KKS]. En outre, l'algorithme HERMIPOL semble a priori optimal.

Nous obtenons précisément le théorème suivant :

Théorème 7 : Soit **K** un corps et M une matrice à s lignes et r colonnes à coefficients dans **K**[X]. Notons $\delta_1 = \deg(M)$ le degré maximum d'un polynôme entrée de M , et $\delta' = \inf(s,(r-1)).\delta_1$. Supposons qu'une réduction minimale de Hermite de M soit obtenue avec une matrice de passage de degré d . (rappelons que nécessairement $d \leq \delta'$)

Lorsqu'on applique l'algorithme HERMIPOL à la matrice M le calcul exécuté est la triangulation sans échange de colonnes d'une matrice à entrées dans **K** dont les caractéristiques sont les suivantes :

- les entrées sont toutes nulles ou égales à des coefficients des polynômes entrées de M
- le nombre de lignes est $\leq s.(1 + \delta_1 + d)$
- le nombre de colonnes est $\leq r.(1 + d)$

De manière générale, nous n'avons pas cherché à présenter les résultats de complexité sous une forme plus détaillée que la description précise du problème d'algèbre linéaire sur **K** auquel nous nous ramenons dans les algorithmes. La manière dont le problème d'algèbre linéaire doit être traité, et la complexité pratique qui en résulte, dépendent au plus haut point de la nature du corps **K** et de la façon dont il est codé. On sait que les problèmes d'algèbre linéaire sont résolubles en temps polynomial dans tout corps “de présentation finie” sur un corps premier, c.-à-d. dans les corps de fonctions des variétés irréductibles définies sur le corps premier. Dans le dernier algorithme il s'agit de savoir trianguler une matrice. On sait que ce problème se résoud en temps polynomial si et seulement si les déterminants se calculent en temps polynomial sur le corps **K** (avec le codage choisi). Dans le cas où le corps apparait comme le corps des fractions d'un anneau intègre **C** dans lequel les divisions exactes sont "faciles" la méthode la plus pratique de triangulation d'une matrice est la méthode de Bareiss. Le calcul d'une triangulation est alors en temps polynomial si et seulement si, d'une part les opérations d'addition, multiplication et division exacte sont en temps polynomial (pour le codage choisi de **C**) et d'autre part la taille des déterminants est polynomialement majorée.

Le travail présenté ici a déjà été exposé au colloque MEGA 92, mais la traduction en anglais de l'article n'a pas été faite à temps pour paraître dans les compte-rendus.

Notons pour terminer cette introduction que le calcul d'une réduction de Smith avec une bonne complexité, est donnée dans [Vil], qui se base sur les algorithmes donnés ici pour la réduite de Hermite.

2) Généralités

Définitions, notations, résultats élémentaires

Nous disons qu'un algorithme est de classe $\mathcal{P}$ lorsqu'il a une complexité en temps polynomiale. Une fonction est dite $\mathcal{P}$-calculable lorsqu'elle peut être calculée par un algorithme de classe $\mathcal{P}$.

La théorie de la réduction de Hermite d'une matrice à coefficients dans un anneau de Bezout est bien connue. Nous conseillons le chapitre II du livre de Schrijver [Sch] pour un exposé de cette théorie dans le cas de l'anneau des entiers avec une étude de complexité.

Nous utiliserons le mot «entrée» à la place du mot «coefficient» lorsqu'il s'agit d'une matrice. Ceci dans le but de réserver le mot «coefficient» aux polynômes.

Nous considérons donc un anneau $\mathbf{A} = \mathbf{K}[X]$ et une matrice M de type s*r (s lignes et r colonnes) à entrées dans **A** . Nous appelons **F** le corps de fractions de **A** . Nous notons :

$\mathcal{L}$ le module libre $\mathbf{A}^s$,

e_1 , ..., e_s la base canonique de $\mathcal{L}$,

pour k = 1, ..., s ; $\mathcal{F}_k$ est le sous-**A**-module de $\mathcal{L}$ engendré par e_k , ..., e_s

Π_k : $\mathcal{L}$h **A** la k-ème forme coordonnée

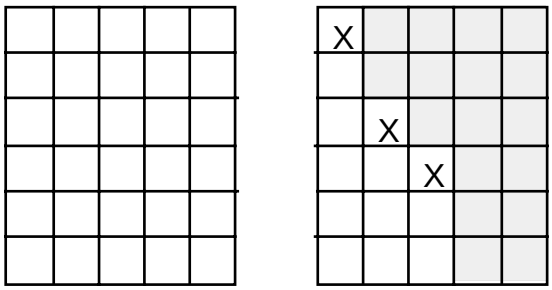
V_1 , ... , V_r les vecteurs colonnes de M (considérés comme des éléments de $\mathcal{L}$),

$\mathcal{E}$ le sous-**A**-module de $\mathcal{L}$ engendré par V_1 , ... , V_r

$\mathfrak{E}_k = (\mathfrak{E} i \mathfrak{F}_k)$
$\mathfrak{E}'_k = \Pi_k(\mathfrak{E}_k)$ qui est un idéal de **A**

Nous disons qu'une matrice carrée est **unimodulaire** si son déterminant est un élément non nul de **K** c.-à-d. 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 $\mathfrak{E}$ 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*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.

Le problème qui nous préoccupe ici est que ce calcul est en général trop coûteux, parce que chacune des matrices de Bezout successives dépend des précédentes et qu'en conséquence sa taille est mal contrôlée.

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** . Les problèmes d'algèbre linéaire dans **A** sont a priori plus difficiles. Il est cependant facile de constater que 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.

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** peut se faire 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** .

Les propositions qui suivent sont bien connues.

Proposition 1 : On reprend les notations ci-dessus concernant la matrice M .

Soient W_1 , ... , W_t avec $W_i \in \mathcal{E}_{k_i}$, $w_i = \Pi_{k_i}(W_i)$.

On suppose que les conditions suivantes sont vérifiées :

- la suite k_i (i = 1, ... , t) est strictement croissante
- w_i (i=1, ... , t) est non nul de degré minimum dans $\mathcal{E}'_{k_i}$
- $\mathcal{E}'_k = \{0\}$ pour tout k distinct des k_i

Alors la matrice M' dont les t premiers vecteurs colonnes sont les W_i et dont les derniers vecteurs colonnes sont nuls est une réduite de Hermite de M .

Proposition 2 : Etant données deux réduites de Hermite M' et M'' d'une même matrice M de type $s*r$, il existe une matrice Q de type $r*r$, 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 d'une 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 ...

Réduite normale.

On définit une **forme normale** pour la réduite de Hermite en imposant les conditions supplémentaires suivantes :

- les w_i sont des polynômes unitaires
- toute entrée à gauche d'un w_i est un polynôme de degré < deg(w_i)

Il est clair que la réduite de Hermite sous forme normale est unique.

On peut calculer une réduite de Hermite sous forme normale à partir d'une réduite de Hermite ordinaire comme suit :

- multiplier chaque W_i par l'inverse du coefficient dominant de w_i
- pour i de t à 2 : remplacer chaque W_j (pour $j < i$) par $W_j - q_{i,j} W_i$, où $q_{i,j}$ est le quotient dans la division euclidienne de l'entrée numéro k_i de W_j par w_i

On remarquera que du point de vue de la taille des objets intermédiaires, ce processus est acceptable parce que les $q_{i,j}$ peuvent être tous calculés directement sur la matrice à normaliser.

Le résultat suivant se déduit immédiatement de la proposition 1 .

Proposition 3 : (toujours les mêmes notations)

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 , ... , 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 , $w_i = \Pi_{k_i}(W_i)$.

i) Si M' est une réduite normale de Hermite de M , les conditions suivantes sont vérifiées :
- la suite k_i (i = 1, ... , t) est strictement croissante
- w_i (i = 1, ... , t) est unitaire et de degré minimum dans $\mathcal{E}'_{k_i}$
- toute entrée à gauche d'un w_i est un polynôme de degré < deg(w_i)
- $\mathcal{E}'_k = \{0\}$ pour tout k distinct des k_i

ii) Réciproquement, si les W_i sont dans $\mathcal{E}$ et si les conditions ci-dessus sont vérifiées, la matrice M' est la réduite normale de Hermite de M .

De la réduite de Hermite générale à la réduction de Hermite

Certains algorithmes de calculs de réduites de Hermite fonctionnent uniquement pour les matrices carrées non singulières, d'autres 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*r et calculons une réduite de Hermite N' de N . Elle est constituée d'une matrice M' de type s*r et d'une matrice de type r*r collée en dessous. 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*r à entrées dans **A** telles que : N U = N' et N' V = N. D'où on tire facilement que U V = I_r . Donc M U = M' , avec U unimodulaire, égale à la matrice collée en dessous de M' dans N'. Par ailleurs, la matrice M' est bien en forme triangulaire de Hermite.

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

Algorithmes efficaces: méthodes et résultats connus

Cas des matrices à coefficients entiers

Les méthodes modulaires sont étudiées dans [Fru1], [Fru2], [Fru3], [Sch], [DKT], [Ili1], [Ili2] et [HM]. Des méthodes plus directes sont données dans [KB] et [CC].

Ce genre d'algorithme, appliqué au cas des anneaux de polynômes, permet de majorer convenablement les degrés, mais non les coefficients, des polynômes entrées des matrices intermédiaires.

Cas des matrices à coefficients polynomiaux

Dans le cas de matrices ayant pour entrées des polynômes à coefficients rationnels, Kannan utilise un algorithme récursif du même genre que dans [KB], mais s'arrange pour remplacer les polynômes pivots dont la taille des coefficients menace d'exploser par les polynômes primitifs proportionnels, qui sont de taille convenable. Le fait que de tels polynômes proportionnels de taille convenable existent, résulte d'arguments qui ne semblent pas s'étendre à tout corps où les déterminants sont calculables en temps polynomial.

Kaltofen-Krishnamoorthy-Saunders proposent une méthode qui commence par calculer en parallèle les degrés des éléments diagonaux de la réduite normale dans $\mathbf{K}[X]$, ce qui est légitime du point de vue de la complexité parallèle, mais très lourd du point de vue de la complexité séquentielle. L'idée essentielle est que la réduction de Hermite dans $\mathbf{K}[X]$ se ramène à un problème d'algèbre linéaire sur $\mathbf{K}$.

3) Calcul d'une réduction de Hermite pour une matrice polynomiale par des méthodes de sous-résultants généralisés

Un calcul de réduite de Hermite peut être compris comme un «gros» calcul de pgcd.

On sait que l'algorithme d'Euclide appliqué brutalement dans un anneau de polynômes est a priori mal contrôlé du point de vue de la taille des coefficients. Par exemple, il y a de fortes présomptions qu'un calcul de pgcd par l'algorithme d'Euclide dans $\mathbb{Q}[X]$ puisse conduire à une taille du résultat exponentielle en la taille des données (cf. [Lom]).

Aussi le calcul du pgcd de deux polynômes P et Q par divisions successives est classiquement remplacé par un calcul de «sous-résultants» qui sont des polynômes proportionnels aux restes successifs de l'algorithme d'Euclide, et dont les coefficients sont des mineurs extraits de la matrice de Sylvester (cf. [Loo], [GLRR]). Quant au fond, on a remplacé un algorithme récursif dans $\mathbf{K}[X]$ par un calcul d'algèbre linéaire sur $\mathbf{K}$.

Nous proposons ici trois méthodes relevant purement de l'algèbre linéaire en dimension finie (bien contrôlée) sur le corps des coefficients. La première est à peu près celle donnée dans [KKS]. les deux autres peuvent être qualifiées de méthodes de sous-résultants généralisés.

Une première méthode: par résolution d'un grand système linéaire

L'unicité est un atout

Dans beaucoup de problèmes mathématiques et en particulier dans les problèmes de complexité, le fait qu'un problème a été mis sous une forme où la solution est unique est souvent un grand avantage[1].

Pour ce qui est des problèmes de complexité, lorsque la solution est unique, sa taille permet souvent de contrôler a priori la taille des calculs intermédiaires. Dans le cas d'une infinité de solutions au contraire, il y a des solutions de taille arbitrairement grandes, et une stratégie spécifique est souvent nécessaire pour obtenir des solutions de taille raisonnable.

Dans le cas de la forme normale pour la réduite de Hermite, nous allons voir :

– d'une part qu'elle est de taille raisonnable (si les déterminants sont de taille raisonnable dans le corps $\mathbf{K}$),

1 Par exemple, le fait d'avoir mis une matrice sous forme de Hermite permet de particulariser une solution du système linéaire avec second membre, solution unique dans le corps des fractions (si elle existe) dont l'existence (dans l'anneau) controle la compatibilité du système. Avec la matrice initiale par contre, le fait qu'une solution particulière soit dans le corps des fractions sans être dans l'anneau ne permettait pas de conclure à l'incompatibilité du système (dans l'anneau) sauf evidemment si la solution était unique.

– d'autre part qu'elle peut être trouvée par des méthodes générales d'algèbre linéaire sur **K** , ce qui conduit à une solution dans la classe $\mathfrak{P}$ lorsque les déterminants dans **K** sont calculables dans la classe $\mathfrak{P}$.

Le système linéaire à résoudre

Nous supposons que $s \geq r$ et que la matrice M est de rang r . Ceci n'est pas restrictif, et constitue même la situation standard, où on cherche à calculer non seulement une réduite de Hermite mais une réduction de Hermite. (cf. le § «de la réduite de Hermite générale à la réduction de Hermite» dans la section (2)).

Ensuite, nous rappelons que la forme des réduites de Hermite de M (au sens de : la forme de la partie grisée dans M', c.-à-d. encore : la suite des k_i dans la proposition 1) est donnée par une triangulation de M dans le corps des fractions de $\mathbf{K}[X]$.

Notation : Si A est une matrice polynomiale, nous notons deg(A) pour le plus grand des degrés des entrées de A

Nous considérons alors la matrice Q obtenue en ne gardant dans M que les lignes k_1 , ..., k_r . Nous notons : $\delta_1 = \deg(Q)$.
Nous connaissons det(Q) : la triangulation de M dans le corps $\mathbf{K}(X)$ en vue de déterminer la matrice extraite Q a donné ce résultat comme sous produit .
Posons : $\delta = \deg(\det(Q))$. (on a $\delta \leq r.\delta_1$)
Soit Q' la réduite de Hermite normale de Q .
On doit avoir Q P = Q' avec P inversible dans $\mathbf{M_r}(\mathbf{K}[X])$. D'où :

$\det(P).\det(Q) = \det(Q') = w_1 \ldots w_r$ (les w_i sont les éléments diagonaux de Q') avec det(P) un élément non nul de **K** .

Appelons d_i le degré de w_i , on a donc :

$$\delta = \deg(\det(Q)) = \deg(\det(Q')) = d_1 + d_2 \ldots + d_r$$

Nous notons Q^* la matrice adjointe de Q .
Le degré de la matrice Q^* est majoré par : $(r-1)\,\delta_1$
L'égalité Q P = Q' donne alors :

$$\det(Q)\,P = Q^*\,Q' \qquad (1)$$

Donc $\deg(P) \leq \deg(Q^*) + \deg(Q') - \deg(\det(Q)) \leq \deg(Q^*)$ (2)
Ainsi on a :

Proposition 4 : Soit M une matrice polynomiale de type s*r dont les vecteurs colonnes sont notés V_i . Notons $\delta_1 = \deg(M)$ le degré maximum d'un polynôme entrée de M .

a) Si le rang de M est égal à r , (son nombre de colonnes), les vecteurs $X^j.V_i$ avec $j \leq (r-1)\,\delta_1$ engendrent un **K**-espace vectoriel qui contient les vecteurs colonnes de la réduite de Hermite normale de la matrice M .

b) Dans le cas général, l'affirmation précédente reste vraie en remplaçant $(r-1)\,\delta_1$ par $\delta' = \inf(s,(r-1)).\delta_1$.

preuve> La première affirmation résulte clairement de l'inégalité (2). Pour la dernière affirmation, considérer la matrice obtenue en collant dessous M une matrice identité de type r*r et appliquez le raisonnement précédent à cette matrice. ❑

Supposons connaître les degrés d_i *des polynômes pivots* w_i .

Nous allons voir comment alors calculer la réduite normale de Hermite Q' de Q en résolvant un grand système linéaire à coefficients et inconnues dans **K** .

Dans la réduite de Hermite normale, toutes les entrées ont un degré majoré par :

$$\sup_{i=1,...,r} (d_i)$$

En utilisant l'inégalité (2) ci dessus, nous pouvons majorer les degrés des polynômes entrées de la matrice P par $(r - 1) \delta_1$, et même par :

$$\delta_2 = (r - 1) \delta_1 + \sup_{i=1,...,r} (d_i) - \delta .$$

Nous considérons alors la matrice Q' et la matrice P comme données par les coefficients (dans **K**) des polynômes entrées de Q' et de P .

Pour les entrées de P les degrés sont majorés par δ_2 .

Dans Q' les entrées à droite de la diagonale sont nulles, les degrés sont égaux à d_1, d_2 , ... , d_r sur la diagonale, et strictement majorés par d_2 , ... , d_r sur les lignes 2, ..., r à gauche de la diagonale.

Cela fait donc en tout (sans compter les coefficients dominants égaux à 1 pour les polynômes sur la diagonale de Q') :

$d_1 + 2 d_2 + 3 d_3 + ... + r d_r$ coefficients dans **K** pour la matrice Q'

$r^2 [1 + \delta_2]$ coefficients dans **K** pour la matrice P

Nous considérons tous ces coefficients comme les inconnues pour le système linéaire à coefficients et inconnues dans **K** qui signifie : Q P = Q' .

Ce système linéaire contient une équation pour chaque élément de **K** obtenu comme coefficient d'un polynôme calculé lorsqu'on explicite toutes les entrées du produit de matrices Q P en fonction des entrées de P et Q .

La plupart de ces coefficients doivent être nuls (partie droite de la matrice Q', ou coefficients de degrés trop élevés dans la partie gauche de Q'), r d'entre eux doivent être égaux à 1 , et $d_1 + 2 d_2 + 3 d_3 + ... + r d_r$ d'entre eux doivent être égaux aux «inconnues» choisies pour décrire Q'. On voit en particulier que ces dernières équations peuvent être omises du calcul principal, qui est celui de la matrice P : après le calcul de P on peut passer directement à celui de M" = M P , qui contient Q' comme matrice extraite.

Notez que la proposition 3 garantit l'existence et l'unicité de la matrice Q' en tant que matrice triangulaire de la forme Q P avec des polynômes unitaires ayant les bons degrés sur la diagonale et avec les bonnes majorations de degrés sous la diagonale (ceci sans avoir à supposer P inversible). Là est la clé de la question : cela garantit l'unicité de P et son inversibilité dans $\mathbf{M_r}(\mathbf{K}[X])$, alors que nous n'avons pas exprimé directement cette condition d'inversibilité (elle conduirait à des équations et une inéquation non linéaires).

Estimation de la complexité du calcul lorsqu'on connait les degrés des pivots

Résumons nos résultats dans une proposition (la lecture de cette proposition fait référence aux notations introduites précédemment)

Proposition 5 : Soit M une matrice polynomiale de type s*r dont les vecteurs colonnes sont notés V_i . Notons $\delta_1 = \deg(M)$ le degré maximum d'un polynôme entrée de M . Lorsqu'on a déterminé les indices k_i donnant les lignes des pivots et qu'on a extrait de M la matrice Q correspondant à ces lignes, si on connaît les degrés d_i des polynômes pivots w_i , le calcul de la matrice de passage P qui permet d'obtenir la réduite normale de Hermite pour M demande la solution d'un *système linéaire à coefficients et inconnues dans* **K** dont les caractéristiques

sont les suivantes :

– coefficients : ce sont des coefficients des polynômes entrées de Q

– nombre d'inconnues : $r^2 [1 + \delta_2] \leq r^2 [1 + (r-1)\delta_1]$

– nombre d'équations : $\leq r^2 [1 + \delta_1 + \delta_2] - [d_1 + 2d_2 + 3d_3 + ... + r\,d_r] \leq r^2 (1 + r\,\delta_1)$

Ceci garantit la taille raisonnable des entrées de la matrice P et par suite la taille raisonnable du calcul de P puis de M' = M.P .

Comment calculer les degrés d_i ?

Dans l'article [KKS], la méthode suivante est proposée, qui est légitime du point de vue de la complexité parallèle, mais lourde du point de vue de la complexité séquentielle.

Pour chacun des indices $i = 1, ..., r$ et pour chaque degré $d = 0, 1, ..., (r-1)\delta_1$ on teste la compatibilité du système linéaire qui traduit le fait suivant :

il existe un vecteur colonne W de degré $\leq (r-1)\delta_1$ tel que M.W ait ses coordonnées n° 1, ..., i–1 égales à 0 et sa coordonnée n°i égale à un polynôme unitaire de degré d .

Une deuxième méthode, par triangulation d'une grande matrice

Dans ce paragraphe, nous allons voir comment on peut se passer de la connaissance des degrés d_i , et ne pas résoudre en entier le système linéaire précédent.

En effet, reprenons les notations de la proposition 1 (avec de nouveau M et non Q).

Nous disposons avec la proposition 4 de majorations sur les degrés des polynômes intervenant comme coefficients des combinaisons linéaires des V_j égales aux W_i . Nous sommes donc ramenés à un problème en dimension finie bien contrôlée sur **K** . Voyons ceci plus en détail.

Quelques notations supplémentaires

Nous complétons les notations données au début de la section (2) . Nous notons :

$\mathcal{F}_{k,d}$ le **K**-espace formé par les éléments de $\mathcal{F}_k$ dont toutes les coordonnées (sur la base $e_k , ..., e_s$) sont de degré $\leq d$

$\mathcal{L}_d = \mathcal{F}_{1,d}$

$\mathcal{B}_d$ la base de $\mathcal{L}_d$ formée des $X^n.e_k$ ordonnée comme suit :
$X^d.e_1 , \ldots, X.e_1 , e_1 , X^d.e_2 , \ldots, X.e_2 , e_2 , \ldots , X^d.e_s , \ldots, X.e_s , e_s$.

$\delta_1 = \deg(M)$ = degré maximum d'une entrée de la matrice M

$\delta' = \inf(s,(r-1)).\delta_1$

$\mathcal{V}$ = la liste des V_j (vecteurs colonnes de M) ordonnée par indices croissants

$\mathcal{V}^{(d)}$ = la liste des $X^n.V_j$ avec $n \leq d$, ordonnée selon la définition récurrente :
$\mathcal{V}^{(0)} = \mathcal{V}$, $\mathcal{V}^{(d+1)} = X.\mathcal{V}^{(d)} * \mathcal{V}$ ($*$ représente la concaténation des listes)

$M^{(d)}$ = la matrice à entrées dans **K** ayant pour liste de vecteurs colonnes la liste $\mathcal{V}^{(d)}$ exprimée sur la base $\mathcal{B}_{d+\delta_1}$

$\mathcal{E}^{(d)}$ le **K**-espace engendré par $\mathcal{V}^{(d)}$.
on a : $\mathcal{E}^{(d+1)} = X.\mathcal{E}^{(d)} + \mathcal{E}^{(0)} = X^{d+1}.\mathcal{E}^{(0)} + \ldots + X.\mathcal{E}^{(0)} + \mathcal{E}^{(0)} = X.\mathcal{E}^{(d)} + \mathcal{E}^{(d)}$
(attention ! $\mathcal{E}^{(d)}$ est contenu dans $\mathcal{E} \cap \mathcal{L}_{d+\delta_1}$, mais l'inclusion est en général stricte, même du coté des bas degrés)

$\mathcal{E}_k^{(d)} = \Pi_k(\mathcal{E}^{(d)} \cap \mathcal{F}_k)$ qui est un sous **K**-espace de **K**[X] (notez également que $\mathcal{E}_k^{(d)}$ n'engendre pas nécessairement l'idéal $\mathcal{E}'_k = \Pi_k(\mathcal{E} \cap \mathcal{F}_k)$)

NB : nous parlons «en parallèle» de la base e_1 , ..., e_s du **A**-module $\mathfrak{L}$ (les coordonnées d'un vecteur W sur cette base sont les polynômes $\Pi_i(W)$), et de la base $\mathfrak{B}_d$ du **K**-espace vectoriel $\mathfrak{L}_d$, base formée de vecteurs $X^n.e_k$. Nous espérons que le contexte permet à chaque fois de faire la différence. L'expression «coordonnée numéro k» fait référence à la première base.

Par la proposition 1, on sait qu'un W_i convient comme vecteur colonne d'une réduite de Hermite de M dès qu'il est dans l'espace vectoriel (de dimension infinie) $\mathfrak{E}_{k_i}$ et que :

$$\deg(\Pi_{k_i}(W_i)) = \text{degré minimum d'un polynôme non nul dans } \mathfrak{E}'_{k_i}$$

La proposition 4 nous dit alors exactement que de tels W_i peuvent être calculés par triangulation d'une matrice représentant le **K**-espace (de dimension finie) $\mathfrak{E}^{(\delta')}$.

Considérons donc la matrice $M^{(\delta')}$ et faisons lui subir une triangulation dans **K** par manipulations de colonnes sans échange de lignes. Des W_i convenables sont automatiquement calculés par cette triangulation :

L'indice k_1 est simplement le plus petit k pour lequel une des coordonnées $\Pi_k(V_j)$ est non nulle.

Le vecteur W_i est le dernier vecteur colonne de la triangulée appartenant à $\mathfrak{F}_{k_i,\delta'+\delta_1}$ mais n'appartenant pas à $\mathfrak{F}_{i+k_i,\delta'+\delta_1}$.

L'indice k_{i+1} est le plus petit indice k pour lequel le vecteur immédiatement après W_i (dans la matrice triangulée) a une coordonnée numéro k non nulle.

On notera que cette méthode ne calcule pas directement la réduite normale, mais la réduite normale ne présente pas une utilité spécifique bien grande. En outre, elle est facilement calculée à partir d'une réduite arbitraire.

Par contre il y a trois avantages immédiats en comparaison de la première méthode :

1) il n'est pas nécessaire de calculer préalablement la suite des indices k_i
2) il n'est pas nécessaire non plus de calculer préalablement les degrés d_i
3) la triangulation proposée est de toute manière plus courte que la résolution du grand système linéaire de la première méthode (cf. estimation de complexité ci-après)

Rappelons que la réduction de Hermite est calculée en même temps que la réduite si on a pris soin de placer la matrice I_r en dessous de la matrice dont on cherche une réduite, et de faire tourner l'algorithme de triangulation sur la matrice à entrées dans **K** correspondant à cette plus grande matrice.

Estimation de la complexité du calcul

Nous résumons les résultats obtenus

Proposition 6 : Soit M une matrice polynomiale de type s*r . Notons $\delta_1 = \deg(M)$ le degré maximum d'un polynôme entrée de M , et $\delta' = \inf(s,(r-1)).\delta_1$. Le calcul d'une réduite de Hermite de M peut être obtenu par une triangulation sans échange de lignes d'une matrice à coefficients dans **K** dont les caractéristiques sont les suivantes :

- les entrées sont toutes nulles ou égales à des coefficients des polynômes entrées de M
- le nombre de lignes est $\le s.(1 + \delta_1 + \delta') \le s.(1 + r\,\delta_1)$,
- le nombre de colonnes est $\le r.(1 + \delta') \le r.[1 + (r-1)\,\delta_1]$

On constate en fin de compte que le détour par la réduite normale a surtout eu un role pédagogique, pour les auteurs tout au moins.

Cette deuxième méthode, moins coûteuse que la première, est cependant un peu trop gourmande. Il y a moyen de trianguler progressivement, des matrices de plus en plus grandes, en faisant augmenter les degrés n dans les $X^n.V_j$, jusqu'au moment où on est assuré que des W_i convenables ont été trouvés. C'est l'objet du paragraphe suivant d'expliquer comment on peut contrôler un tel processus.

Une triangulation mieux contrôlée: l'algorithme HERMIPOL

Une méthode analogue à celle que nous présentons maintenant est exposée dans [Lom] pour le cas d'une matrice à une seule ligne de polynômes. La réduite de Hermite est alors tout simplement le pgcd de la liste des polynômes. Rappelons brièvement ce qui se passe dans ce cas. On démarre avec un espace vectoriel de dimension finie (≥ 2) $\mathcal{H} \subset \mathbf{K}[X]_d$ (l'espace vectoriel des polynômes de degré $\leq d$).

On définit $\mathcal{H}_n$ par $\mathcal{H}_n = X^n.\mathcal{H}+X^{n-1}.\mathcal{H}+\ldots+X.\mathcal{H}+\mathcal{H} \subset \mathbf{K}[X]_{d+n}$.

On a nécessairement $\dim(\mathcal{H}_{n+1}) \geq 1 + \dim(\mathcal{H}_n)$, parce que $\mathcal{H}_{n+1}$ contient $\mathcal{H}_n$ et un polynôme de degré strictement supérieur à tous ceux de $\mathcal{H}_n$.

Si $\dim(\mathcal{H}_{n+1}) = 1 + \dim(\mathcal{H}_n)$, alors la même situation se reproduit pour tous les $n' \geq n$ de sorte que le degré minimum d'un polynôme est le même dans $\mathcal{H}_n$, et dans $\mathcal{H}_n$, ce qui montre qu'un polynôme de $\mathcal{H}_n$ est de degré minimum dans l'idéal $\mathcal{H}.\mathbf{K}[X]$.

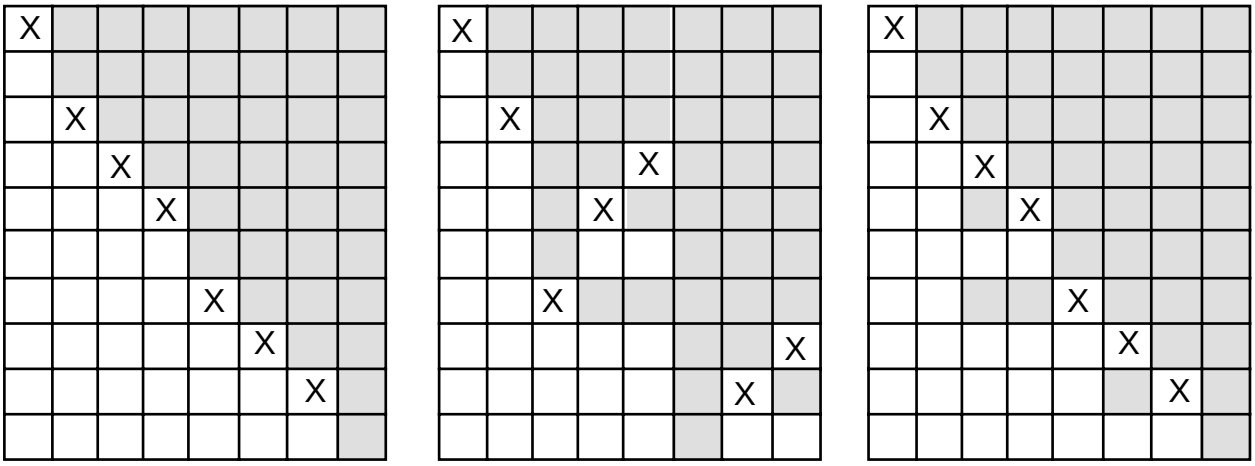
Par ailleurs, tant que $\dim(\mathcal{H}_{n+1}) \geq 2 + \dim(\mathcal{H}_n)$, la différence $\dim(\mathbf{K}[X]_{d+n}) - \dim(\mathcal{H}_n)$ décroit strictement à chaque étape, et ceci fait que le nombre des étapes est majoré par $1 + d - \dim(\mathcal{H})$.

Pour trouver un polynôme de degré minimum dans $\mathcal{H}_n$ il suffit de trianguler une matrice à entrées dans $\mathbf{K}$ dont les colonnes représentent des générateurs de $\mathcal{H}_n$ exprimés sur la base des X^i avec i décroissant de $n + d$ à 0 . Enfin, si on veut procéder de proche en proche en profitant à chaque étape des calculs faits à l'étape précédente, il faut faire une triangulation sans échange de colonnes.

La description de notre troisième algorithme, que nous appelons HERMIPOL, et la preuve de sa correction seront plus claires si nous voyons tout d'abord sur un exemple le comportement de la triangulation envisagée maintenant. Il s'agit d'une triangulation dans $\mathbf{K}$ sans échange de colonne. Il faudra donc des échanges de lignes pour obtenir une forme triangulaire. Ces échanges seront en fait seulement simulés et non affichés, d'où l'aspect pas tout à fait triangulaire des matrices obtenues. Un petit dessin permettra de mieux voir la différence et la similitude des résultats entre triangulation sans échange de ligne et triangulation sans échange de colonnes (les échanges de lignes n'étant pas affichés).

les nouvelles colonnes proviennent
des anciennes ayant pour numéros

1 2 5 4 3 8 7 6



triangulée sans
échange de lignes

triangulée sans
échange de colonnes

la même avec
permutation de
colonnes pour terminer

Exemple

Nous considérons une matrice 3×3 formée de polynômes de degrés 2 ou 3 :

$$\begin{pmatrix} X^2 + 4X + 4 & X^2 + 2X & X^2 + 3X + 2 \\ X^3 + 3X^2 + 5X + 6 & X^3 + 2X^2 + 3X + 3 & X^3 + 2X^2 + 4X + 3 \\ 2X^3 + 3X^2 + 6X + 9 & 2X^3 + X^2 + 4X + 5 & 2X^3 + 2X^2 + 5X + 5 \end{pmatrix}$$

Les premiers pivots dans la réduite de Hermite sont de degrés «exceptionnellement grands», à savoir 1 et 2 au lieu de 0 et 0 (pour une matrice «prise au hasard», tous les pivots, sauf le dernier, dans la réduite de Hermite sont des constantes).

Comme le degré maximum des entrées est 3 et que la matrice est de rang 3 , l'application aveugle de l'algorithme de la deuxième méthode conduirait à trianguler la matrice $M^{(6)}$. En fait, nous sommes fixés sur la réduction de Hermite dès la triangulation de la matrice $M^{(1)}$. Nous bénéficions ici d'une situation exceptionnelle, car il existe une réduction de Hermite avec matrice de passage de degré 1 , au lieu du degré 6 attendu (c'est à mettre en relation avec les grands degrés des premiers pivots).

Nous voudrions cependant insister sur le fait qu'une situation qui peut paraître «exceptionnelle» au regard d'une mesure de probabilité apparemment raisonnable peut très bien être une situation «courante» lorsqu'on ne résout pas des problèmes qui tombent du ciel, mais des problèmes issus de situations «géométriques» concrètes.

Nous donnons ci-dessous les trois matrices à coefficients entiers $M^{(0)}$, $M^{(1)}$, $M^{(2)}$ qui correspondent à la matrice de polynôme donnée, en dessous de laquelle on a rajouté une matrice identité.

matrice $M^{(0)}$

```
 1  1  1
 4  2  3  zone 1
 4  0  2
---------
 1  1  1
 3  2  2  zone 2
 5  3  4
 6  3  3
---------
 2  2  2
 3  1  2  zone 3
 6  4  5
 9  5  5
---------
 1  0  0  zone 4
---------
 0  1  0  zone 5
---------
 0  0  1  zone 6
```

matrice $M^{(1)}$

```
 1  1  1  .  .  .
 4  2  3  1  1  1
 4  0  2  4  2  3
 .  .  .  4  0  2
------------------
 1  1  1  .  .  .
 3  2  2  1  1  1
 5  3  4  3  2  2
 6  3  3  5  3  4
 .  .  .  6  3  3
------------------
 2  2  2  .  .  .
 3  1  2  2  2  2
 6  4  5  3  1  2
 9  5  5  6  4  5
 .  .  .  9  5  5
------------------
 1  0  0  .  .  .
 .  .  .  1  0  0
------------------
 0  1  0  .  .  .
 .  .  .  0  1  0
------------------
 0  0  1  .  .  .
 .  .  .  0  0  1
```

matrice $M^{(2)}$

```
 1  1  1  .  .  .  .  .  .
 4  2  3  1  1  1  .  .  .
 4  0  2  4  2  3  1  1  1   zone 1
 .  .  .  4  0  2  4  2  3
 .  .  .  .  .  .  4  0  2
--------------------------
 1  1  1  .  .  .  .  .  .
 3  2  2  1  1  1  .  .  .
 5  3  4  3  2  2  1  1  1   zone 2
 6  3  3  5  3  4  3  2  2
 .  .  .  6  3  3  5  3  4
 .  .  .  .  .  .  6  3  3
--------------------------
 2  2  2  .  .  .  .  .  .
 3  1  2  2  2  2  .  .  .
 6  4  5  3  1  2  2  2  2   zone 3
 9  5  5  6  4  5  3  1  2
 .  .  .  9  5  5  6  4  5
 .  .  .  .  .  .  9  5  5
--------------------------
 1  0  0  .  .  .  .  .  .
 .  .  .  1  0  0  .  .  .   zone 4
 .  .  .  .  .  .  1  0  0
--------------------------
 0  1  0  .  .  .  .  .  .
 .  .  .  0  1  0  .  .  .   zone 5
 .  .  .  .  .  .  0  1  0
--------------------------
 0  0  1  .  .  .  .  .  .
 .  .  .  0  0  1  .  .  .   zone 6
 .  .  .  .  .  .  0  0  1
```

Montrons maintenant ce que donne sur la matrice $M^{(2)}$ la triangulation sans échange de colonnes. Cela donne des numéros de lignes des pivots successifs un peu erratiques (pour «voir» une forme sous-triangulaire, on pourrait terminer par une permutation de colonnes).

L'avantage décisif est que, comme il n'y a jamais aucun échange de colonnes, la triangulation de la matrice $M^{(0)}$ est une partie inchangée de la triangulation de la matrice $M^{(1)}$, qui est elle-même une partie inchangée de la triangulation de la matrice $M^{(2)}$ (et ainsi de suite...). En conséquence, une triangulation «progressive», jusqu'au moment où la solution est atteinte, est facile à programmer. Et aucun «calcul inutile» n'a eu lieu.

Degré 2 Départ matrice $M^{(2)}$	fin (triangulation sans échange de colonnes)
1 1 1 . . . . . . 4 2 3 1 1 1 . . . 4 0 2 4 2 3 1 1 1 . . . 4 0 2 4 2 3 . . . . . . 4 0 2	1 • • • • • • • • 4 -2 • • • • • • • 4 **-4** • 2 • • • • • zone 1 . . . 4 • • 2 • • . . . . . . 4 • •
1 1 1 . . . . . . 3 2 2 1 1 1 . . . 5 3 4 3 2 2 1 1 1 6 3 3 5 3 4 3 2 2 . . . 6 3 3 5 3 4 . . . . . . 6 3 3	1 0 • 0 • • 0 • • 3 **-1** 1 • • • • • • 5 **-2** **0** 2 2 • • • • 6 **-3** **3** 2 0 • 2 2 • zone 2 . . . 6 6 • 2 0 • . . . . . . 6 6 •
2 2 2 . . . . . . 3 1 2 2 2 2 . . . 6 4 5 3 1 2 2 2 2 9 5 5 6 4 5 3 1 2 . . . 9 5 5 6 4 5 . . . . . . 9 5 5	2 **0** **0** 0 0 • 0 0 • 3 **-2** **0** 1 2 1 • • • 6 **-2** **0** 2 0 **0** 1 2 1 9 **-4** **4** 2 0 **0** 2 0 0 zone 3 . . . 9 10 **1** 2 0 0 . . . . . . 9 10 1
1 0 0 . . . . 1 0 0 . . . . 1 0 0	1 **-1** **1** -1 -2 **-1** 0 0 0 . . . 1 0 **-1** -1 -2 -1 zone 4 . . . . . . 1 0 -1
0 1 0 . . . . 0 1 0 . . . . 0 1 0	0 **1** **1** 0 0 **0** 0 0 0 . . . 0 2 **0** 0 0 0 zone 5 . . . . . . 0 2 0
0 0 1 . . . . 0 0 1 . . . . 0 0 1	0 **0** **-2** 1 2 **1** 0 0 0 . . . 0 0 **2** 1 2 1 zone 6 . . . . . . 0 0 2

Commentaires :

Nous avons mis des points légers « . » pour les 0 correspondant à des calculs qui n'ont jamais à être faits, et des points plus gros « • » pour les 0 qui apparaissent du fait du traitement des pivots. (ce serait la partie au dessus des pivots si on avait fait les échanges de lignes). Les pivots de la triangulation sont mis en relief. Les colonnes correspondant à la solution calculée sont mises en gras.

Nous pouvons être sûrs que les colonnes 2, 3 et 6 dans cette triangulation sans échange de colonnes fournissent la réduction de Hermite de la matrice initiale, ceci dès qu'est apparue la colonne 6 , c.-à-d. dès la fin de la triangulation de la matrice $M^{(1)}$. En effet, lorsqu'on passe de $M^{(1)}$ à $M^{(2)}$, un nouveau pivot apparaîtra nécessairement dans chacune des zones 1, 2, 3 puisqu'un vecteur ayant comme première entrée non nulle un polynôme du degré minimum précédemment trouvé se trouve de nouveau dans l'espace vectoriel engendré par les colonnes. Les trois colonnes introduites sont donc entièrement absorbées par la nécessité de reproduire dans la triangulation ces degrés minimums précédemment trouvés, et donc les degrés minimums fourni par la triangulation de la matrice $M^{(2)}$ ne sont pas meilleurs que les précédents. Comme le même raisonnement est valable pour les degrés suivants, on est sûr d'avoir atteint la réduite de Hermite. Dans le cas traité en exemple, on a donc obtenu la réduite de Hermite :

$$\begin{pmatrix} -2X - 4 & 0 & 0 \\ -X^2 - 2X - 3 & X^2 + 3 & 0 \\ -2X^2 - 2X - 4 & 4 & X^3 + 1 \end{pmatrix}$$

avec la matrice de passage :

$$\begin{pmatrix} -1 & 1 & -X-1 \\ 1 & 1 & 0 \\ 0 & -2 & X+2 \end{pmatrix}$$

Nous terminons l'article par des précisions sur l'algorithme, une preuve plus complète de sa correction et une estimation de complexité.

L'algorithme HERMIPOL

L'algorithme que nous proposons est donc le suivant :

Entrée de l'algorithme : ce sont les vecteurs V_1 , ... , V_r dont les entrées sont des polynômes. On ne suppose pas que le système est de rang r . Néanmoins, si on désire obtenir, non seulement la réduite de Hermite mais aussi la matrice de passage, on colle en dessous de la matrice des V_i (présentés en colonne) la matrice I_r auquel cas, les nouveaux vecteurs colonnes forment un système de rang r .

Nous continuons à appeler V_i les vecteurs colonnes (même si on a rajouté la matrice I_r).

L'algorithme est divisé en étapes. L'étape numéro $d+1$ calcule la matrice M'_d ayant pour colonnes les colonnes non nulles de la triangulée sans échange de colonnes d'une matrice $M^{(d)\bullet}$ extraite de la matrice $M^{(d)}$ (on ne garde que les colonnes réellement utiles). Les matrices $M^{(d)\bullet}$ et leurs triangulées sont considérées comme divisées en zones horizontales, chaque zone correspondant aux vecteurs de base $X^n.e_k$ pour une valeur fixée de l'indice k .

A chaque étape certains vecteurs V_j sont éventuellement «tués», c.-à-d. réduits au vecteur nul par le processus de triangulation (ceci n'arrive que si le $\mathbf{K}[X]$-module $\mathcal{E}$ engendré par les V_j est de rang inférieur à r).

A chaque étape également sont éventuellement repérés des nouveaux vecteurs «candidats pour la réduite de Hermite».

Hypothèse implicite : Il n'y a pas de vecteur nul dans la liste de départ (sinon on la raccourcit).

Etape n°1 : On a $d = 0$. On pose $M^{(0)\bullet} = M^{(0)}$. On triangule sans échange de colonnes la matrice $M^{(0)\bullet}$. On obtient une matrice M'_0 .

Transition de l'étape n°d+1 à l'étape n°d+2 : La matrice M'_d vient d'être calculée par triangulation de la matrice $M^{(d)\bullet}$ sans échange de colonnes. On supprime les colonnes éventuellement nulles dans M'_d ainsi que les colonnes correspondantes dans $M^{(d)\bullet}$. Les vecteurs V_j correspondants sont rajoutés à la liste des vecteurs morts.

Etape n°d+2 : Construire $M^{(d+1)\bullet}$ à partir de $M^{(d)\bullet}$ en rajoutant une ligne de 0 en bas de chacune des zones, puis en rajoutant à gauche les vecteurs V_i qui sont encore vivants.

La matrice M'_d , à condition de rajouter une ligne de 0 en bas de chaque zone, représente le début du calcul de la triangulée M'_{d+1} de $M^{(d+1)\bullet}$: il ne reste à traiter que les colonnes nouvellement ajoutées.

Parmi les nouveaux vecteurs colonnes qui apparaissent, certains donnent lieu à des vecteurs candidats pour la réduite de Hermite. Plus précisément, il y a deux cas. Premier cas : si le premier coefficient non nul d'un nouveau vecteur colonne de la triangulée se trouve dans une zone qui n'avait pas encore été atteinte (une zone est déclarée atteinte lorsqu'un vecteur de la triangulée a une coordonnée non nulle dans cette zone et ses coordonnées dans les zones supérieures toutes nulles, notez que les zones atteintes ne le sont pas nécessairement dans l'ordre croissant), et si le degré correspondant est minimum parmi les vecteurs dans la même situation, le vecteur, transformé en un vecteur de polynômes, est déclaré candidat. Deuxième cas : si le premier coefficient non nul d'un vecteur colonne de la triangulée se trouve dans une zone qui avait déjà été atteinte, mais si le degré correspondant est inférieur à celui du candidat précédemment retenu, et si

le degré correspondant est minimum parmi les vecteurs dans la même situation, le vecteur en question, transformé en un vecteur de polynômes, remplace l'ancien candidat (moins méritant).

Fin de l'algorithme : L'algorithme s'arrête lorsque, à la fin d'une étape, on constate que le nombre de vecteurs restant en vie est égal au nombre de vecteurs candidats pour la réduite de Hermite.

Les candidats sont alors reçus à l'examen avec les félicitations du jury (c.-à-d. que la matrice formée de ces vecteurs, en ordre convenable, complétée par le nombre convenable de colonnes nulles, est bien une réduite de Hermite de la matrice M).

Preuve de la correction de l'algorithme

Reprenons les notations introduites au début de la deuxième méthode. La matrice $M^{(d)}$ a pour vecteurs colonnes ceux de la liste $\mathcal{V}^{(d)}$ exprimée sur la base $\mathcal{B}_{d+\delta_1}$. Notons alors $\mathcal{V}^{(d)\bullet}$ la liste extraite de $\mathcal{V}^{(d)}$ en supprimant les vecteurs qui dépendent linéairement (sur $\mathbf{K}$) des vecteurs qui les précèdent dans la liste. Comme $\mathcal{V}^{(d+1)} = X.\mathcal{V}^{(d)} * \mathcal{V}$ et que la multiplication par X ne change pas la dépendance linéaire sur $\mathbf{K}$, on a nécessairement

$$\mathcal{V}^{(d+1)\bullet} = X.\mathcal{V}^{(d)\bullet} * \mathcal{V}_{d+1}$$

avec $\mathcal{V}_{d+1} \subset \mathcal{V}$. On a de plus $\mathcal{V}_{d+1} t \mathcal{V}_d$ parce que « $V_j \notin \mathcal{V}_d$ » signifie

$$V_j \in <V_1 , \ldots, V_{j-1} > + X.\mathcal{E}^{(d-1)}$$

ce qui implique

$$V_j \in <V_1 , \ldots, V_{j-1} > + X.\mathcal{E}^{(d)}$$

Il est alors clair, par récurrence sur $d \geq 1$, que la matrice $M^{(d)\bullet}$ construite au début de l'étape $d+1$ correspond à la la liste $X.\mathcal{V}^{(d)\bullet} * \mathcal{V}_d$ et qu'elle est remplacée, lors de la transition à l'étape $d+2$ par la matrice correspondant à la liste $\mathcal{V}^{(d+1)\bullet} = X.\mathcal{V}^{(d)\bullet} * \mathcal{V}_{d+1}$.

Donc chaque matrice M'_d est (aux colonnes nulles près) la triangulée sans échange de colonnes de la matrice $M^{(d)}$.

Nous allons en déduire que l'instruction d'arrêt est correcte.

Comme $\mathcal{E}^{(d+1)} = X.\mathcal{E}^{(d)} + \mathcal{E}^{(d)}$, on a $\mathcal{E}_k^{(d+1)} \subset X.\mathcal{E}_k^{(d)} + \mathcal{E}_k^{(d)}$. Les espaces $\mathcal{E}_k^{(d)}$ non nuls correspondent aux zones atteintes lors des étapes $1, \ldots, d+1$. Si $\mathcal{E}_k^{(d)}$ est non nul, l'inclusion $\mathcal{E}_k^{(d+1)} \subset X.\mathcal{E}_k^{(d)} + \mathcal{E}_k^{(d)}$ implique $\dim_{\mathbf{K}}(\mathcal{E}_k^{(d+1)}) \geq 1 + \dim_{\mathbf{K}}(\mathcal{E}_k^{(d)})$.

Par ailleurs $\dim_{\mathbf{K}}(\mathcal{E}^{(d)}) = \mathrm{card}(\mathcal{V}^{(d)\bullet}) = \sum_k \dim_{\mathbf{K}}(\mathcal{E}_k^{(d)})$.

Donc, si à la fin de l'étape $d+1$ il reste en vie un nombre de vecteurs égal au nombre de zones atteintes, on a nécessairement :

- $\dim(\mathcal{E}_k^{(d+1)}) = 1 + \dim(\mathcal{E}_k^{(d)})$ pour les indices k des zones atteintes,
- $\mathcal{V}_{d+1} = \mathcal{V}_d$, et
- $\mathcal{E}^{(d+1)}$ est la somme directe de $X.\mathcal{E}^{(d)}$ et des droites $\mathbf{K}.W_{k_i}$ (les candidats retenus).

Si on continuait l'algorithme avec des valeurs d' supérieures, on ne changerait donc ni les zones atteintes, ni les vecteurs vivants, ni les polynômes non nuls de degré minimum dans chacun des $\mathcal{E}_k^{(d')}$ non nuls.

Nous allons montrer maintenant que l'instruction d'arrêt se produit après un nombre d'étapes en un certain sens minimal. Plus précisément, nous posons la définition suivante.

Définition : Nous disons qu'une **réduction de Hermite** d'une matrice polynomiale M est **minimale** lorsque la matrice de passage correspondante est de degré minimum.

Nous affirmons que l'algorithme s'arrête dès qu'une réduite de Hermite minimale est calculée, donc forcément pour $d \leq \delta' = (r-1).\delta_1$.

Tout d'abord lorsque la matrice M est de rang r, aucun vecteur ne peut être tué en cours de route parce que r zones doivent être en fin de compte atteintes. Par ailleurs, dès que l'espace $\mathcal{E}^{(d)}$ contient les r vecteurs colonnes d'une réduite de Hermite de M, la triangulation de $M^{(d)}$ calcule de tels vecteurs, et donc l'algorithme s'arrête puisque le nombre de zones atteintes est alors égal au nombre de vecteurs en vie.

Notez que si on sait a priori être dans le cas du rang égal à r (par exemple dans le cas où on a collé sous la matrice à traiter la matrice identité, pour obtenir simultanément la matrice de passage), l'écriture de l'algorithme peut être simplifiée parce qu'il n'y a pas à gérer la question des vecteurs morts, et l'algorithme termine dès que r zones ont été atteintes.

Le raisonnement est à peine plus subtil si le rang de la matrice est strictement plus petit que r. On considère la matrice N de rang r obtenue en collant la matrice I_r en dessous de M. On remarque qu'une réduction de Hermite minimale pour N en fournit une pour M et vice versa. On remarque aussi que l'algorithme avec l'entrée M produit comme calculs une partie des calculs exécutés avec l'entrée N. Soit t le rang de M et d le degré minimal d'une matrice de passage de N à une réduite de Hermite N'. Lors de l'étape d+1, et avec l'entrée N, l'algorithme calcule une triangulée de $N^{(d)}$. Toutes les zones correspondant à des lignes des pivots de N' sont atteintes, et parmi elles $r-t$ zones sont en dessous de $M^{(d)}$. Donc la triangulation de $M^{(d)}$ tue nécessairement les $r-t$ vecteurs correspondants. Ainsi, lorsque l'algorithme traite l'entrée M, l'instruction d'arrêt fonctionne au plus tard à l'étape $d+1$.

Il semble par contre difficile de préciser exactement l'étape où il s'arrête. Tous les vecteurs d'une réduite de Hermite de M peuvent en effet apparaître pour la première fois dans un espace $\mathcal{E}^{(d')}$ avec $d' < d$. Et il semble que selon les cas de figure, l'algorithme puisse s'arrêter dès l'étape $d'+1$ ou poursuivre plus loin, par exemple jusqu'à l'étape $d+1$.

Estimation de la complexité de l'algorithme HERMIPOL

Nous résumons l'étude précédente dans un théorème :

Théorème 7 : Soit $\mathbf{K}$ un corps et M une matrice à s lignes et r colonnes à coefficients dans $\mathbf{K}[X]$. Notons $\delta_1 = \deg(M)$ le degré maximum d'un polynôme entrée de M, et $\delta' = \inf(s,(r-1)).\delta_1$. Supposons qu'une réduction minimale de Hermite de M soit obtenue avec une matrice de passage de degré d. (rappelons que nécessairement $d \leq \delta'$)

Lorsqu'on applique l'algorithme HERMIPOL à la matrice M le calcul exécuté est la triangulation sans échange de colonnes d'une matrice à entrées dans $\mathbf{K}$ dont les caractéristiques sont les suivantes :

- les entrées sont toutes nulles ou égales à des coefficients des polynômes entrées de M
- le nombre de lignes est $\leq s.(1 + \delta_1 + d)$
- le nombre de colonnes est $\leq r.(1 + d)$

Remarques complémentaires :

1) La méthode retenue pour la triangulation doit être choisie en fonction des circonstances. Si les coefficients des polynômes sont dans un corps fini, on utilisera le pivot de

Gauss classique. S'ils sont dans un anneau intègre avec division efficace (lorsqu'elle est exacte) on utilisera la méthode de Bareiss, ou dans certains cas favorables une méthode modulaire. Sinon on utilisera la méthode de Berkovitz-Samuelson : l'avantage de celle-ci est aussi de pouvoir s'appliquer au cas d'un anneau «non encore entièrement précisé» quotient intègre d'un anneau par un idéal premier non encore précisé. Ce sera le cas par exemple si on travaille dans une extension de corps cadrée à la D5 (cf. [DD] et [DDD].)

2) On obtient une réduite de Hermite «presque normale» (les degrés à gauche d'un pivot sont inférieurs ou égaux au degré du pivot, au lieu d'être strictement inférieurs) si on poursuit l'algorithme une étape de plus et si on retient comme candidats les derniers vecteurs calculés. Il est alors facile de calculer la réduite normale.

3) Les matrices que l'on traite contiennent relativement beaucoup de zéros, et peu de coefficients distincts. Sans doute serait-il utile d'explorer les possibilités de simplification que cela introduit dans les divers algorithmes de triangulation. Rappelons que l'algorithme des sous-résultants gagne un ordre de grandeur en nombre d'opérations arithmétiques dans le cas le plus simple, qui correspond à une matrice avec une ligne et deux colonnes de polynômes.

4) La complexité de l'algorithme dépend de la taille de l'entrée mais est améliorée si la qualité de la sortie est “bonne” : matrice de passage de degré relativement petit (on peut voir que ce sera le cas notamment si les degrés des pivots sont relativement grands). En ce sens, c'est un bon algorithme, car il permet d'avoir des calculs relativement courts dans les cas qu'on peut estimer les plus intéressants.

5) Le fait de garder les vecteurs candidats lors de leur première apparition (en tant que «vecteur de polynômes ayant sa coordonnée pertinente de degré minimum parmi les vecteurs analogues») permet de minimiser a priori la taille des coefficients des entrées de la réduite de Hermite, puisque cela revient à minimiser la taille des déterminants auxquels ces coefficients sont égaux. En particulier, on aura en général des coefficients plus petits en taille que ceux des polynômes de la réduite normale, qui n'est pas nécessairement une réduite minimale.

4) Résultats expérimentaux

L'algorithme Hermipol a été, en particulier, implémenté par Gilles Villard (IMAG, Université de Grenoble) en MapleV.3 (avec le pgcd de deux polynômes comme opération de base). Gilles Villard a ensuite effectué une comparaison en utilisant alternativement dans des programmes Maple cet algorithme d'une part, l'algorithme de triangulation standard de Maple d'autre part. La comparaison a été effectuée sur un Sun5, en relançant une session Maple pour chaque essai.

Nous remercions Gilles Villard poura voir réalisé cette expérimentation et nous avoir communiqué les résultats.

Première série d'essais :

- les coefficients des matrices sont des polynômes de degré 3, à coefficients en valeur absolue inférieurs ou égaux à 9, générés aléatoirement, les dimensions des matrices varient de 4 à 9, les temps sont exprimés en secondes :

	Standard	Hermipol	Rapport
dim = 4	13	3	4,3
dim = 5	172	12	14,3
dim = 6	1795	40	44,8
dim = 7	12770	113	109
dim = 8	70882	321	221
dim = 9	????	753	

Comparaison des temps d'exécution exprimés en secondes

Concernant la mémoire, Maple donne deux quantités, la mémoire totale utilisée au cours de l'exécution (cumul), et la mémoire utilisée à un instant t donné, ici la fin de l'exécution (allocation effective à l'instant t) l'unité est le MégaMot :

	Standard	Hermipol
total dim 8	594,0	26,0
t=fin dim 8	27,3	3,7

Comparaison des espaces mémoire utilisés

Deuxième série d'essais :

- les coefficients des matrices sont des polynômes de degré 8, les matrices sont de dimension 3, les coefficients sont générés aléatoirement dans des bornes de plus en plus grandes, les temps sont exprimés en secondes :

	Standard	Hermipol	Rapport
$\|coeff\| \leq 9$	16,55	36,42	2,6
$\|coeff\| \leq 99$	86,3	15,15	5,7
$\|coeff\| \leq 999$	195	26,35	7,4
$\|coeff\| \leq 9999$	337	44,36	7,6
$\|coeff\| \leq 99999$	518	60	8,53
$\|coeff\| \leq 999999$	818	89	9,2

Comparaison des temps d'exécution exprimés en secondes

allocation en MégaMots :

	Standard	Hermipol
total 999999	18,5	5,3
t=fin 999999	2,8	1,5

Comparaison des espaces mémoire utilisés

Conclusion:

Ces comparaisons montrent une incontestable supériorité d'Hermipol sur l'algorithme standard de triangulation de Maple. Cette supériorité est d'abord due à une forte économie en espace mémoire.

Roger MARLIN
Département de Mathématiques
UFR des Sciences
Université de Nice
06034 NICE Cédex
FRANCE

email :
marlin@sophia.inria.fr

Henri LOMBARDI
Laboratoire de Mathématiques
URA CNRS 741
UFR des Sciences et Techniques
Université de Franche-Comté
25030 BESANCON Cédex
FRANCE
email :
lombardi@math.univ-fcomte.fr

Salah LABHALLA
Dép. de Mathématiques
Université de Marrakech
Bd de SAFI. BP S 15
MARRAKECH
MAROC

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 linear diophantine equations*. Siam J. on Computing 11 numéro 4 687-708 (1982)

[**DD**] Dicrescenzo C., Duval D. : *Algebraic extensions and algebraic closure in Scratchpad.* Symbolic and algebraic computation (ISSAC 88). Lecture Notes in Computer Science 358, p 440-446 (1989). (Springer)

[**DDD**] Della Dora J., Dicrescenzo C., Duval D. : *About a new method for computing in algebraic number fields* Proceedings Eurocal'85. Lecture Notes in Computer Science 204, p 289-290 (1985). (Springer)

[**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)

[**GLRR**] Gonzalez L., Lombardi H., Recio T., Roy M.F.: *Spécialisation de la suite de Sturm et sous-résultants. I* . RAIRO Informatique théorique et Applications vol 24, n°6, 1990, p. 561-588. (Version plus détaillée, dans CALSYF journées du GRECO de Calcul Formel 1989)

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

[**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)

[**Kan**] Kannan R. : *Solving systems of linear equations over polynomials*. Theoretical Computer Science 39 69-88 (1985).

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

[**KKS**] Kaltofen E., Krishnamoorthy M., Saunders B. D. : *Fast parallel computation of Hermite and Smith normal forms of polynomial matrices*. Siam J. on Algebraic and Discrete Methods 8 numéro 4 683-690 (1987)

[**Lom**] Lombardi Henri. : *Sous-résultants, suite de Sturm, spécialisation*. 2ème partie de la thèse soutenue en juin 89 à Nice. Réimpression : Publications Mathématiques de l'Université (Besançon). 88-89. Théorie des Nombres. Fascicule 2.

[**Loo**] Loos R. : *Generalized poynomial remainder sequences*. Dans Computer Algebra, Symbolic and Algebraic Computation 115-138. Edité par Buchberger, Collins, Loos . Springer Verlag 1982.

[**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)

[**Vil**] Villard G.: *computation of Smith normal forms of polynomial matrices.* Rapport technique dec 92. LMC Imag Grenoble