Forme normale de Hermite

François Thomasset
INRIA

23 août 2001

1 La forme normale de Hermite

Définitions

- Une matrice carrée C est unimodulaire si $\mid det(C) \mid = \pm 1$
- Une matrice carrée H $(m \times m)$ est une matrice de Hermite si :
  - H est à coefficients entiers ;
  - H est triangulaire inférieure : $h_{ij} = 0$ si $i < j$;
  - $h_{ii} > 0$ pour $i = 1, \ldots, m$;
  - $h_{ij} \leq 0$ et $\mid h_{ij} \mid < h_{ii}$, si $i > j$.

Théorème 1 Soit A une matrice $m \times n$ de rang m ; il existe une matrice unimodulaire C, et une matrice carrée H telles que :

- H est une matrice de Hermite ;
- $AC = (H, 0)$;
- $H^{-1}A$ est à coefficients entiers.

La preuve résultera de l'analyse de l'algorithme donné plus loin.

Transformations élémentaires Ces transformations sur une matrice quelconque A sont équivalentes à la multiplication à droite par des matrices unimodulaires appropriées (execrice) :

- échanger deux colonnes ;
- multiplier une colonne par -1 ;
- pour un entier $\lambda \in Z$ donné, ajouter $\lambda\times$ colonne j à la colonne k.

Proposition 2 Soient $a_1, \ldots, a_n$ les colonnes de A, s et t des numéros de colonne avec $s < t$. Soit r le pgcd de a_{is} et a_{it} : il existe des entiers p et q premiers entre eux, tels que $pa_{is} + qa_{it} = r$. Il existe une matrice unimodulaire entière C telle que $AC = A'$, où :

$$\begin{array}{rcl} a'_l & = & a_l \ (l \neq s,t) \\ a'_s & = & pa_s + qa_t \\ a'_t & = & -\dfrac{a_{it}}{r}a_s + \dfrac{a_{is}}{r}a_t \end{array}$$

Démonstration : Prendre pour C une matrice différant de l'identité uniquement dans les colonnes s et t :

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 & \ldots & \\ 0 & 1 & 0 & 0 & & & & \\ \vdots & 0 & 1 & & & & & \\ \vdots & & & p & \ldots & -\frac{a_{it}}{r} & 0 & \ldots \\ & & & 0 & & \vdots & & \\ & & & q & \ldots & \frac{a_{is}}{r} & 0 & \ldots \\ & & & 0 & & & 1 & \ldots \\ \vdots & & & & \ldots & & 0 & 1 \end{pmatrix}$$

- dans la colonne s : $c_{ss} = p$, $c_{ts} = q$, et $c_{is} = 0$ pour $i \neq s, t$;
- dans la colonne t : $c_{st} = -\frac{a_{it}}{r}$, $c_{tt} = \frac{a_{is}}{r}$, et $c_{it} = 0$ pour $i \neq s, t$.

$\diamond$

Algorithme Hermite

Initialisation : $i \leftarrow 1, H' \leftarrow A$

1 : Transformations sur la ligne i : si $i > m$, stop. Sinon on pose $j \leftarrow i + 1$

2 : Si $h'_{ij} \neq 0$:
Calculer p, q, r tels que $r = \text{pgcd}(h'_{ii}, h'_{ij})$, $ph'_{ii} + qh'_{ij} = r$, p et q premiers entre eux (algorithme d'Euclide).
C = matrice unimodulaire donnée par la proposition 2 ($s = i, t = j$).
$H' \leftarrow H'C$
Si $j < n$
$j \leftarrow j + 1$
retourner en **2**
sinon aller en **3**

3 : Si $h'_{ii} < 0$: $H' \leftarrow H'C$, où C multiplie la colonne h'_i par -1.
Ensuite continuer à transformer la ligne i, pour les colonnes $j < i$:
$j \leftarrow 1$, aller en **4**.

4 : Si $j = i - 1$
$i \leftarrow i + 1$; aller en **1**.

sinon

Soit C la matrice unimodulaire remplaçant la colonne h'_j par $h'_j - \lceil \frac{h'_{ij}}{h'_{ii}} \rceil h'_i$

$H' \leftarrow H'C$

$j \leftarrow j+1$; aller en **4**.

Proposition 3 *L'algorithme Hermite termine avec des matrices H et C satisfaisant les propriétés de la proposition 2.*

Démonstration Toutes les opérations sur les colonnes sont des multiplications à droite par des matrices unimodulaires ; soit C le produit de ces matrices, et $H' = AC$ la matrice finale.

- Après l'étape **2**, $h'_{ij} = 0$ pour toutes les colonnes $j > i$.
- Après **3**, $h'_{ii} \geq 0$.
- Après **4**, $h'_{ij} < 0$, et $\mid h'_{ij} \mid h'_{ii}$ pour tout $j < i$, sauf si $h'_{ii} = 0$.
- Enfin les valeurs ne sont plus modifiées ensuite, lors du traitement des lignes suivantes.

Il ne reste plus à vérifier qu'après **2**, $\mid h'_{ii} > 0 \mid$.

Supposons que $h'_{jj} > 0$ pour tout $j < i$, mais que $h'_{ii} = 0$.

Soit A_1 la matrice formée des i premières lignes de A. L'algorithme Hermite a produit une matrice unimodulaire C^*, telle que $A_1 C^* = H^*$, avec $h^*_{kj} = 0$ pour tout $k \leq i$ et $j \geq i$: le rang de H^* est $i-1$. Comme C^* est unimodulaire, $\text{rang}(A_1) = \text{rang}(A_1 C^*) = i - 1$, ce qui est contradictoire avec $\text{rang}(A) = m$. $\diamond$

Extensions

1. Si A est une matrice $m \times n$ de rang $k < \min(m,n)$, il existe une matrice unimodulaire entière C, et une matrice de Hermite H $k \times k$, telles que :

$$AC = \begin{pmatrix} H & 0 \\ 0 & 0 \end{pmatrix}$$

2. Forme normale de Smith :
   si A est une matrice $m \times m$ entière non singulière, il existe des matrices unimodulaires entières R et C, telles que :
   (a) $RAC = \Delta$
   (b) Δ est une matrice diagonale ; ses éléments diagonaux δ_i sont des entiers strictement positifs.
   (c) $\delta_1 \mid \delta_2 \mid \ldots \mid \delta_m$
   (d) Δ est unique

2 Application : solutions entières d'un système d'équations

Soit A une matrice $n \times n$, à coefficients entiers ; on s'intéresse à l'existence de solutions du système $Ax = b$.

Soit $S = \{x \in Z^n \ : Ax = b\}$. Soient H et C donnés par le théorème 1 ; on pose $C = (C_1, C_2)$, où C_1 est une matrice $n \times m$, et C_2 une matrice $n \times (n-m)$.

Proposition 4

i. *$S \neq \emptyset$ ssi $H^{-1}b \in Z^m$*

ii. *Si $S \neq \emptyset$, une solution est de la forme :*

$$x = C_1 H^{-1} b + C_2 z, \quad z \in Z^{n-m}$$

Démonstration :

$$\begin{aligned} S &= \{x \in Z^n \ : Ax = b\} \\ &= \{Cw \ : ACw = b, w \in Z^n\} \\ &= \{Cw \ : (H,0)w = b, w \in Z^n\} \\ &= \{C_1 w_1 + C_2 w_2 \ : Hw_1 = b, w_1 \in Z^m, w_2 \in Z^{n-m}\} \\ &= \{C_1 H^{-1} b + C_2 w_2 \ : H^{-1}b \in Z^m, w_2 \in Z^{n-m}\} \end{aligned}$$

$\diamond$

La littérature sur les tests de dépendance désigne quelquefois ce résultat comme *"test du pgcd généralisé"*.

Comme conséquence, voici une version du lemme de Farkas pour les entiers.

Corollaire *$S = \{x \in Z^n \ : Ax = b\} \neq \emptyset$, ou bien il existe $u \in R^m$: $uA \in Z^m$, $ub \notin Z$. Ces deux alternatives ont exclusives.*

Démonstration : Les deux alternatives ne peuvent être vérifiées simultanément, puisque celà entraînerait : $uAx = b$, avec $uAx \in Z$, et $ub \notin Z$.
Si $S = \emptyset$, alors $H^{-1}b \notin Z^m$ d'après la proposition 4. Par exemple le $i-$ème coefficient de $H^{-1}b$ n'est pas entier ; il suffit de prendre pour u la $i-$ème ligne de H^{-1}. $\diamond$

Integer and Combinatorial Optimization
George Nemhauser, Laurence Wolsey. J. Wiley and sons, 1999
J1303