Algèbre linéaire sur les entiers

Préparation agrégation, option C

Révision du 02/06

On examine dans ce texte quelques exemples d'algorithmes d'algèbre linéaire sur les entiers, d'une part pour obtenir des formes normales de matrice avec des matrices de passage inversibles dans $\mathbb{Z}$, d'autre part pour obtenir des algorithmes efficaces.

1 Forme normale de Hermite et de Smith, applications

Soit A une matrice à coefficients entiers. On va adapter l'algorithme du réduction dit du pivot de Gauss pour d'une part rester dans $\mathbb{Z}$ et d'autre part effectuer des manipulations "réversibles" dans $\mathbb{Z}$ (ce qui revient à dire que les matrices de passage sont inversibles dans $\mathbb{Z}$). Supposons que nous souhaitions réduire une colonne j à partir de la ligne i, on commence par chercher un pivot $b = A_{i'j}$ non nul, on échange les lignes i et i'. La méthode de Gauss crée alors des zéros par la manipulation $L_k \leftarrow L_k - A_{kj}/bL_i$, opération qui sort de $\mathbb{Z}$. On peut toutefois adapter cette méthode, soit $a = A_{kj}$, on applique l'identité de Bézout :

$$ua + vb = d = gcd(a, b)$$

on effectue alors simultanément les 2 opérations de lignes

$$L_i \leftarrow v * L_i + u * L_k\,, \quad L_k \leftarrow (-a * L_i + b * L_k)/d$$

On montre facilement que cette opération correspond à l'écriture de $A = PA'$ avec $P \in SL(\mathbb{Z})$ et A' a alors un zéro en ligne k colonne j, en effectuant l'algorithme de réduction de Gauss sous-diagonal, on parvient ainsi à écrire A comme produit d'une matrice de $GL(\mathbb{Z})$ par une matrice triangulaire supérieure de rang maximal. C'est la forme normale de Hermite de A.

Lorsqu'on s'autorise aussi à effectuer des opérations élémentaires sur les colonnes, on peut écrire la matrice A sous la forme PBQ où P et Q sont inversibles dans $\mathbb{Z}$ et B est une matrice diagonale, on peut même (quitte à échanger des lignes/colonnes et re-réduire) faire en sorte que les coefficients diagonaux se divisent ($b_{i,i}$ divise $b_{i+1,i+1}$). C'est la forme normale de Smith.

La forme normale de Hermite permet en particulier de calculer une $\mathbb{Z}$-base du noyau de A (opération qui est non triviale même à partir d'une base dans

$\mathbb{Q}$ du noyau de A). La forme normale de Smith permet de calculer les diviseurs élémentaires d'un groupe abélien de type fini (ce sont les coefficients diagonaux d'une forme normale de Smith).

2 Algorithmes efficaces

2.1 L'algorithme de Gauss-Bareiss

Pour créer un zéro en restant dans $\mathbb{Z}$, au lieu d'effectuer la manipulation $L_k \leftarrow L_k - A_{kj}/bL_i$, on pense d'abord à effectuer $L_k \leftarrow bL_k - A_{kj}L_i$. Mais cette opération va faire apparaitre des entiers qui sont de taille plus grande que la taille nécessaire à la réduction dans $\mathbb{Z}$. On peut alors penser à diviser chaque ligne par le pgcd des coefficients de la ligne pour optimiser la taille des entiers utilisés. Mais cette opérations n'est pas optimale en temps. Il existe un moyen terme (qui se généralise par exemple aux polynômes) entre ces deux méthodes qui consiste à diviser par un coefficient calculé à priori (dont on sait à l'avance qu'il divise tous les coefficients). On montre ainsi que l'on peut utiliser le pivot de l'étape précédente (génériquement il s'agit du pivot utilisé pour réduire la colonne précédente) comme diviseur de la ligne $bL_k - A_{kj}L_i$. On obtient ainsi une croissance linéaire (en la taille de la matrice) des coefficients des matrices lors de la réduction.

Cet algorithme est bien adapté aux opérations telles que calcul du noyau dans $\mathbb{Q}$, calcul du déterminant dans $\mathbb{Z}$ (on vérifie que le déterminant est le dernier coefficient diagonal de la réduction), calcul de l'inverse.

2.2 Méthodes modulaires

Pour éviter les problémes de croissance des coefficients intermédiaires, on peut aussi calculer la quantité souhaitée modulo plusieurs nombres premiers, puis la reconstruire en utilisant une borne à priori, le théorème des restes chinois et la représentation symétrique. Par exemple pour le déterminant, on peut utiliser la borne de Hadamard et des nombres premiers dont le produit est supérieur à 2 fois la borne.

2.3 Méthodes p-adiques

Pour les systèmes de Cramer à coefficients entiers, on peut aussi utiliser une méthode p-adique asymptotiquement plus efficace. On calcule d'abord une borne sur les coefficients des fractions solutions de l'équation $Ax = b$ en utilisant les règles de Cramer et la borne d'Hadamard. On calcule ensuite l'inverse de A modulo p (en changeant de p si A n'est pas inversible modulo p), puis, si

$$x = \sum_i x_i p^i, \quad A(\sum_{i<k} x_i p^i) = b \pmod{p^k}$$

on ajoute $x_k p^k$ et on obtient l'équation :

$$Ax_k = \frac{b - \sum_{i<k} x_i p^i}{p^k} \pmod{p}$$

qui détermine x_k. On s'arrête lorsque k est suffisamment grand pour pouvoir reconstruire les fractions à l'aide de l'identité de Bézout (cf. la section 2.4 infra). On peut utiliser cette méthode pour réduire sous forme échelonnée des matrices de rang maximal ayant plus de colonnes que de lignes, on extrait d'abord une sous-matrice inversible à l'aide d'un petit nombre premier, et on traduit l'opération de réduction par une suite de résolution de systèmes de Cramer.

On peut aussi calculer efficacement le déterminant d'une matrice A à coefficients entiers de manière probabiliste. Pour cela, on résoud l'équation $Ax = b$ pour b vecteur aléatoire à coefficients entiers, le dénominateur commun d des composantes de x est en général le dernier facteur invariant de A, en tous cas c'est toujours un diviseur du déterminant de A. On reconstruit alors $\det(A)/d$ par les restes chinois en calculant $\det(A)$ modulo plusieurs nombres premiers. On peut soit utiliser la borne de Hadamard et suffisamment de nombres premiers pour prouver le déterminant, soit s'arrêter lorsqu'on a quelques nombres premiers pour lesquels la reconstruction modulaire n'évolue plus, la valeur du déterminant étant alors probable. Pour des matrices A aléatoires, le calcul de d donne un très gros facteur du déterminant, ce qui permet de limiter le nombre de nombres premiers à utiliser ensuite. La complexité asymptotique du calcul du déterminant prouvé est la même que par une méthode purement modulaire (cf. 2.5), mais la coefficient moyen devant le terme en n^4 est beaucoup plus petit.

2.4 Reconstruction de rationnels

Soit n et a/b une fraction irréductible d'entiers tels que b est premier avec n et $|a| < \sqrt{n}/2$ et $0 \leq b \leq \sqrt{n}/2$. Il s'agit de reconstruire a et b connaissant $x = a \times (b^{-1}) \pmod{n}$ avec $x \in [0, n[$.

Unicité

S'il existe une solution (a, b) vérifiant $|a| < \sqrt{n}/2$ et $0 \leq b \leq \sqrt{n}/2$, soit (a', b') une solution de $x = a \times (b^{-1}) \pmod{n}$ et vérifiant $|a'| < \sqrt{n}$ et $0 \leq b' \leq \sqrt{n}$, alors :

$$ab' = a'b \pmod{n}$$

Comme $|ab'| < n/2$, $|a'b| < n/2$, on en déduit que $ab' = a'b$. Donc $a/b = a'/b'$ donc $a = a'$ et $b = b'$ car a/b et a'/b' sont supposées irréductibles.

Reconstruction lorsqu'on sait qu'il y a une solution

On suit l'algorithme de calcul des coefficients de Bézout pour les entiers n et x. On pose :

$$\alpha_k n + \beta_k x = r_k$$

où les r_k sont les restes successifs de l'algorithme d'Euclide, avec la condition initiale :

$$\alpha_0 = 1, \beta_0 = 0, \alpha_1 = 0, \beta_1 = 1, r_0 = n, r_1 = x$$

et la relation de récurrence :

$$\beta_{k+2} = \beta_k - q_{k+2}\beta_{k+1}, \quad q_{k+2} = \frac{r_k - r_{k+2}}{r_{k+1}}$$

On a $\beta_k x = r_k \pmod{n}$ pour tout rang mais il faut vérifier les conditions de taille sur β_k et r_k pour trouver le couple (a, b). On montre par récurrence que :

$$\beta_{k+1} r_k - r_{k+1}\beta_k = (-1)^k n \tag{1}$$

On vérifie aussi que le signe de β_k est positif si k est impair et négatif si k est pair, on déduit donc de (1) :

$$|\beta_{k+1}| r_k < n$$

(avec égalité si $r_{k+1} = 0$)

Considérons la taille des restes successifs, il existe un rang k tel que $r_k \geq \sqrt{n}$ et $r_{k+1} < \sqrt{n}$. On a alors $|\beta_{k+1}| < n/r_k \leq \sqrt{n}$.

Donc l'algorithme de Bézout permet de reconstruire l'unique couple solution si on sait par ailleurs qu'il existe.

2.5 Exemple de résultats d'efficacité

On peut montrer que si A est une matrice $n \times n$ et b un vecteur dont les coefficients entiers sont de taille inférieure à B, alors la résolution du système $Au = b$ (supposé de Cramer) nécessite au plus

- $O(n^5 \ln(nB)^2)$ opérations par la méthode de Gauss-Bareiss
- $O(n^3(n + \ln(nB)) \ln(nB))$ opérations par une méthode modulaire (avec restes chinois)
- $O(n^3 \ln(nB)^2)$ opérations par une méthode p-adique.

3 Suggestions de développement

- Justification de l'un des algorithmes présentés et illustration sur machine.
- Application des formes normales de Hermite et Smith.
- Comparaison entre algorithmes d'algèbre linéaire sur les entiers. Par exemple Gauss-Bareiss et déterminant modulaire ou Gauss-Bareiss/méthode p-adique pour les systèmes de Cramer.