Algèbre linéaire sur un corps

Karim Belabas

version du 04/02/2022, 14:00

Soit K un corps, et E, F deux K-ev de dimension finie.

- $\dim E = n$, on fixe une base (e_i), $i \leqslant n$;
- $\dim F = m$, on fixe une base (f_j), $j \leqslant m$.

On a alors des isomorphismes « canoniques » :

$$\begin{aligned} K^n &\xrightarrow{\sim} E \\ (x_i) &\longmapsto \sum_{i=1}^{n} x_i e_i \end{aligned} \qquad \begin{aligned} K^m &\xrightarrow{\sim} F \\ (y_j) &\longmapsto \sum_{j=1}^{m} y_j f_j \end{aligned}$$

$$\begin{aligned} M_{m\times n}(K) = K^{m\times n} &\xrightarrow{\sim} \mathrm{Hom}_K(E, F) \\ (a_{i,j}) &\longmapsto \left(e_j \mapsto \sum_i a_{i,j} f_i\right) \end{aligned}$$

(coordonnées et représentation matricielle *dense*)

Cas particulier : $E = F$.

Dans ce cas $\mathrm{Hom}_K(E, E) =: \mathrm{End}_K(E)$ est un anneau et même une K-algèbre (multiplication matricielle). Et $\mathrm{GL}(E) = \mathrm{End}_K(E)^\times$ est un groupe.

Complexité algébrique des opérations matricielles

$\dim_K E = n$, $\dim_K F = m$, $\dim_K G = \ell$. Soit $\alpha \in \mathrm{Hom}_K(F, G)$, $\beta \in \mathrm{Hom}_K(E, F)$, représentés par les matrices A et B.

1. Pour $x = (x_i) \in E$, $\alpha(x) = Ax$ se calcule en $O(mn)$ opérations dans K.
2. $\alpha \circ \beta$ associé à $A \times B$ se calcule en $O(mn\ell)$ opérations dans K.

Matrice échelonnée

Une matrice $A = (a_{i,j}) \in M_{m\times n}(K)$ est échelonnée en lignes si le nombre de zéros sur chaque ligne avant la première valeur non nulle (pivot) augmente strictement ligne par ligne : il existe un entier r et une fonction $f : \{1, \ldots, r\} \to \{1, \ldots, n\}$ strictement croissante telle que pour $1 \leqslant i \leqslant r$

- $a_{i,j} = 0$ pour tout $j < f(i)$,
- $a_{i,f(i)} \neq 0$.
- $a_{i,j} = 0$ pour tout $i > r$.

A est de rang r ; A est échelonnée réduite si $a_{i,f(i)} = 1$ pour tout $i \leqslant r$.

Théorème

Soit $A \in M_{m\times n}(K)$. Il existe $U \in \mathrm{GL}_m(K)$ tel que $C = UA$ soit échelonnée.

L'algorithme du pivot de Gauss trouve U et $C = UA$ en utilisant $O(m^2 n)$ opérations dans K.

Applications

1. Rang $= \dim_K(\operatorname{Im} A)$: c'est r.
2. Image $\operatorname{Im} A = \{Ax\colon\ : x \in K^n\}$: une K-base est donnée par les colonnes de A contenant un pivot après réduction sous forme échelonnée, les $A_{f(i)}$.
3. Noyau $\operatorname{Ker} A = \{x \in K^n\colon Ax = 0\} = \operatorname{Ker} UA$. La solution de $Cx = 0$ est facile : soit (e_i) la base canonique de K^n, $C = (c_{i,j})$, une base du noyau est constituée des

$$e_j - \sum_{i\colon f(i)<j} c_{i,j} e_{f(i)},$$

où $j \notin \{f(1), \dots f(r)\}$. On retrouve le théorème du rang : $\dim \operatorname{Im} A + \dim \operatorname{Ker} A = n$.

4. Systèmes linéaires : $Ax = b$, $b \in K^m$. Soit $Cx = Ub$ et la résolution du système échelonné est facile en considérant les coordonnées d'indice décroissant : on obtient une solution particulière x_0 et la solution générale est l'espace affine $x_0 + \operatorname{Ker} A$.

Complexité

$O(m^2 n)$ opérations dans K. Soit $O(n^3)$ pour des matrices carrées.

Si A est carrée, on peut obtenir le déterminant en calculant $\det U$ au cours de l'algorithme puis $\det UA / \det U$: $O(n^3)$. Les formules de Cramér pour la résolution d'un système utilisent $O(n^4)$ opérations.

Factorisation LU

Cas particulier des matrices carrées $A \in M_n(K)$. Calcul de l'inverse ou résolution de $Ax = b$ pour *plusieurs* second membres b.

Théorème

Il existe

- *P une matrice de permutation associée à $\sigma \in S_n$: si $x = (x_i)$, Px a pour coordonnées $(x_{\sigma(i)})$. Donc $p_{\sigma(i),i} = 1$ pour $i = 1, \dots, n$ et des 0 ailleurs.*
- *U triangulaire supérieure,*
- *L triangulaire inférieure avec une diagonale de 1,*

telles que $PA = LU$.

On peut prendre $P = \operatorname{Id}$ si et seulement si les mineurs principaux $(= \det(A[1..i, 1..i])$ pour $i = 1, \dots n)$ ne s'annulent pas ; L et U sont alors uniques.

Algorithme récursif dans le cas A inversible

Par blocs. On choisit Q matrice de permutation telle que $a_{k,1} \neq 0$ (sur $\mathbb{R}$ ou $\mathbb{C}$ de module maximal dans la colonne) :

$$QA = \begin{pmatrix} a_{k,1} & {}^t w \\ v & A' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v/a_{k,1} & \operatorname{Id} \end{pmatrix} \begin{pmatrix} a_{k,1} & {}^t w \\ 0 & A' - v\,{}^t w/a_{k,1} \end{pmatrix}$$

On trouve récursivement P', L', U' telles que $P'(A' - v\,{}^t w/a_{k,1}) = L'U'$.

$$\begin{aligned}
\begin{pmatrix} 1 & 0 \\ 0 & P' \end{pmatrix} QA &= \begin{pmatrix} 1 & 0 \\ P'v/a_{k,1} & P' \end{pmatrix} \begin{pmatrix} a_{k,1} & {}^t w \\ 0 & P'^{-1}L'U' \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ P'v/a_{k,1} & \operatorname{Id} \end{pmatrix} \begin{pmatrix} a_{k,1} & {}^t w \\ 0 & L'U' \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ P'v/a_{k,1} & L' \end{pmatrix} \begin{pmatrix} a_{k,1} & {}^t w \\ 0 & U' \end{pmatrix}
\end{aligned}$$

qui est bien de la forme $PA = LU$!

Complexité

$O(n^3)$ opérations dans K

Applications

1. Déterminant : $\det A = \varepsilon(\sigma) \det U$, car $\det P = \varepsilon(\sigma)$.
2. Système linéaire $Ax = b \Leftrightarrow LUx = Pb$. On résoud successivement $Ly = Pb$ puis $Ux = y$

$Ly = Pb$

$$\begin{aligned} y_1 &= b_{\sigma(1)} \\ l_{2,1}y_1 + y_2 &= b_{\sigma(2)} \\ &\dots \\ l_{n,1}y_1 + \cdots + y_n &= b_{\sigma(n)} \end{aligned}$$

Soit pour $i = 1, 2, \ldots, n$:

$$y_i = b_{\sigma(i)} - \sum_{1 \leqslant j < i} l_{i,j} y_j \ .$$

$Ux = y$

$$\begin{aligned} u_{1,1}x_1 + u_{1,2}x_2 + \cdots + u_{1,n}x_n &= y_1 \\ &\dots \\ u_{n-1,n-1}x_{n-1} + u_{n-1,n}x_n &= y_{n-1} \\ u_{n,n}x_n &= y_n \end{aligned}$$

Soit pour $i = n, n-1, \ldots, 1$:

$$x_i = \left(y_i - \sum_{j > i} u_{i,j} y_j \right) / u_{i,i} \ .$$

Complexité

- $PA = LU$: $O(n^3)$ opérations dans K.
- $Ly = Pb$, $Ux = y$: $O(n^2)$.
- Système linéaire complet : $O(n^3)$.
- Inverse A^{-1} : $O(n^3) + nO(n^2) = O(n^3)$.

Polynôme caractéristique

Lemme

Soit $A \in M_n(K)$, $\lambda_1, \ldots, \lambda_n$ ses valeurs propres dans $\overline{K}$. Alors, pour tout $j \geqslant 0$, on a

$$\operatorname{Tr} A^j = \lambda_1^j + \cdots + \lambda_n^j \ .$$

Supposons $\operatorname{car} K = 0$ ou $\operatorname{car} K > n$: pour calculer χ_A le polynôme caractéristique de A, il suffit de calculer ses sommes de Newton $T_0, \ldots, T_n$ grâce au Lemme et les formules de Newton donnent ses coefficients : $n \times O(n^3)$ pour calculer les A^j, les traces et les formules de Newton sont d'un ordre de grandeur plus faible :

Complexité

$O(n^4)$ opérations dans K.

Moindres carrés linéaires

Ici $K = \mathbb{R}$. On suppose que y dépend de x par une équation de type

$$y = f(x, \beta) := \sum_{j=1}^{n} \beta_j \varphi_j(x),$$

où les β_j sont inconnus et les fonctions φ_j connues, données par un modèle (y et x sont des scalaires ou des vecteurs). A partir de N couples (x_i, y_i), on veut déterminer le « meilleur » paramètre β au sens des moindres carrés : il doit minimiser $S = \sum_{i \leqslant N} \left(y_i - f(x_i, \beta)\right)^2$.

Points critiques : pour tout $k \leqslant n$ on a

$$0 = \frac{\partial S}{\partial \beta_k} = -2 \sum_{i \leqslant N} \Big(y_i - \sum_{j=1}^{n} \beta_j X_{i,j}\Big) X_{i,k} \ ,$$

avec $X_{i,j} := \varphi_j(x_i)$, $X \in M_{N,n}(K)$. si et seulement si $\left({}^t XX\right)\beta = {}^t XY$
Solution unique si ${}^t XX \in \mathrm{GL}_n(\mathbb{R})$.

Théorème

Soit $B \in \mathrm{GL}_n(\mathbb{R})$. Alors $B = QR$ où $Q \in O_n(\mathbb{R})$ et R est triangulaire supérieure. La décomposition est unique si on suppose les termes diagonaux de R positifs.

La démonstration est constructive. Soit (b_i) une base d'un espace euclidien $(E, \langle \cdot, \cdot \rangle)$ de dimension n. On construit une base orthogonale (b_i^*) telle que pour tout $i \leqslant n$, on ait $\mathrm{Vect}(b_1, \ldots, b_i) = \mathrm{Vect}(b_1^*, \ldots, b_i^*)$:

Procédé de Gram-Schmidt

$b_1^* \leftarrow b_1$
Pour $j = 2, \ldots, n$, on pose

$$b_j^* \leftarrow b_j - \sum_{i<j} \mu_{i,j} b_i^*, \quad \text{où} \quad \mu_{i,j} = \frac{\langle b_j, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle} \ .$$

En posant $b_j' := b_j^* / |b_j^*|$ on obtient une base *orthonormale*.

Dans ce cas, on obtient

$$b_j = \sum_{i \leqslant j} r_{i,j} b_i' \ ,$$

avec $r_{j,j} = |b_j^*|$ et $r_{i,j} = |b_i^*| \mu_{i,j}$ pour $i < j$.
Si on applique le procédé à l'espace euclidien $\mathbb{R}^n$ muni du produit scalaire usuel et à la matrice B dont les colonnes sont les b_i (qui forment une base de $\mathbb{R}^n$), on obtient $(b_1 | \ldots | b_n) = (b_1' | \ldots | b_n')R$, de la forme $B = QR$.

Complexité

$O(n^3)$ opérations

Applications :

- $|\det B| = |\det R|$.
- Systèmes linéaires : $Bx = y$, $B \in \mathrm{GL}_n(\mathbb{R})$. Alors $QRx = y$ soit $Rx = {}^t Qy$ et on résoud le système linéaire en $O(n^2)$ opérations.
- Inverse : $B^{-1} = R^{-1} \cdot {}^t Q$ soit $O(n^3)$ opérations pour inverser R et $O(n^3)$ pour la multiplication.