Une démonstration de la décomposition de Dunford inspiré de l'algorithme de Newton.

1 Introduction

À un candidat qui avait donné la démonstration usuelle, sur $\mathbb{C}$, de la décomposition de Dunford,

$$u = d + n,$$

un membre du jury a posé, sans succés, la question suivante :

Peut-on calculer d et n sans connaître les valeurs propres de u ?

Il s'avère que oui ! En fait, une adaptation de la méthode de Newton pour l'approximation des racines conduit à une démonstration effective (i.e. transformable, en un algorithme qui a le bon gout d'être très rapide).

2 Algorithme de Newton

L'algorithme de Newton est un algorithme itératif sensé converger vers une solution d'une équation du type $f(x) = 0$ avec f dérivable et de dérivé jamais nulle. On définit une suite par récurence par la fomule :

$$x_{n+1} = x_n - f(x_n)/f'(x_n).$$

Dans les bons cas x_n converge ; la limite est alors une (la) solution de $f(x) = 0$.

3 Décomposition de Dunford

On a l'énoncé suivant:

Théorème 1. *Soit E un espace vectoriel de dimension finie et u un endomorphisme de E dont le polynôme caractéristique est scindé. On suppose que la caractéristique du corps de base est nulle.*

Alors, il existe un unique couple (d, n) d'endomorphismes de E tels que d est diagonalisable, n est nilpotent, d et n commutent et $u = d + n$.

De plus, d et n sont des polynômes en u.

Démonstration. Commençons par montrer l'existence. Pour cela on va exhiber une « équation » satisfaite par d et vérifier que l'algorithme de Newton converge pour cette équation.

Le point de départ est donc la constation que les racines du polynôme minimal de d sont simples et sont les valeurs propres de u. Notons P_u le polynôme carctéristique de u. Posons :

$$Q = \frac{P_u}{P_u \wedge P_u'}.$$

On aura

$$Q(d) = 0.$$

Considérons donc la suite d'endomorphismes suivante :

$$\begin{aligned} &u_0 = u, \\ &u_{n+1} = u_n - Q(u_n) * Q'(u_n)^{-1}. \end{aligned}$$

Remarquons qu'il faut justifier que $Q'(u_n)$ est bien inversible. On montre en fait par une même récurence sur n les trois propriétés suivantes:

1. $u_n \in k[u]$;
2. $Q'(u_n)$ est inversible pour tout n; et
3. $Q(u_n) \in Q(u)^{2^n} k[u]$, en particulier $Q(u_n)$ est nilpotent.

Pour $n = 0$, Q' est premier avec le polynôme minimal de u (caractéristique zéro) donc $Q'(u)$ est inversible. Supposons l'hypothèse satisfaite pour u_n: ceci implique que u_{n+1} est bien défini. Comme l'inverse d'un endomorphisme inversible v appartient à $k[v]$, $u_{n+1} \in k[u]$. D'après le lemme 2 appliqué dans l'anneau $k[u]$, il suffit de montrer que $Q'(u_{n+1}) - Q'(u_n)$ est nilpotent pour avoir l'inversibilité de $Q'(u_{n+1})$. Or le lemme 3 implique que $Q'(u_{n+1}) - Q'(u_n) \in (u_{n+1} - u_n)k[u]$. Or, la formule de récurence montre que $(u_{n+1} - u_n)k[u] \subset Q(u_n)k[u]$. Par récurence, $Q(u_n)$ est nilpotent; et l'inversibilité de $Q'(u_{n+1})$ suit.

Écrivons

$$Q(u_{n+1}) = Q(u_n + y),$$

avec $y = -\frac{q(u_n)}{q'(u_n)}$. Le lemme 4 montre alors qu'il existe $v \in \mathbb{C}[u]$ tel que

$$Q(u_{n+1}) = Q(u_n) + yQ'(u_n) + y^2 v.$$

Or $Q(u_n) + yQ'(u_n) = 0$ et $y^2 \in Q'(u_n)^2\mathbb{C}[u]$. Ainsi

$$Q(u_{n+1}) \in Q'(u_n)^2\mathbb{C}[u] \subset Q'(u)^{2^{n+1}}\mathbb{C}[u].$$

La dernière assertion de la récurrence est démontrée.

La dernière assertion montre que $Q(u_n) = 0$ pour n asser grand. Remarquons que $n \geq \ln_2(\dim E)$ suffit. Ainsi, à partir de cette valeur u_n statione.

Notons d l'endomorphisme sur lequel u_n stationne. On a $Q(d) = 0$; donc d est diagonalisable.

Il nous reste à voir que $u - d$ est nilpotente. Or, d'après ce qui précède, $u - d = (u_0 - u_1) + (u_1 - u_2) + \cdots + (u_{n-1} - u_n)$ (si $d = u_n$) appartient à $Q(u).k[u]$. On en déduit qu'il est nilpotent. $\square$

Voici les énoncés des lemmes que nous avons utilisés:

Lemme 2. *Soit A un anneau commutatif unitaire. Soit a un élément inversible de A et n un élément nilpotent.*

Alors, $a + n$ est inversible.

Proof.

$\square$

Lemme 3. *Pour tout polynôme R il existe un polynôme en deux variables S tel que :*

$$R(Y) - R(X) = (Y - X)S(X, Y).$$

Proof. L'ensemble des polynômes R qui vérifient le lemme est un sous-espace vectoriel de l'espace des polynômes. Or la formule

$$Y^d - X^d = (Y - X)(Y^{d-1} + Y^{d-2}X + \dots X^{d-1}),$$

montre que $R = X^d$ appartient à cet ev. Le lemme en découle. $\square$

Lemme 4. *Pour tout polynôme R il existe un polynôme en deux variables S tel que :*

$$R(X + Y) = R(X) + YR'(X) + Y^2 S(X, Y).$$

Proof. Même preuve que le lemme précédent avec la formule

$$(X + Y)^d = X^d + YdX^{d-1} + Y^2(\cdots).$$

$\square$

4 Implémentation

Il s'agit ici d'implémenter l'algorithme et de comparer ses performances à Maple. Voici les étapes de l'algo:

1. Calculer P_u, puis Q et Q'.
2. Calculer u_n pour $2^n \leq \dim(E)$.
3. Conclure.

5 Suggestions de développements

1. Démontrer les lemmes 2, 3 et 4.
2. Améliorer la borne pour laquelle $u_n = d$.
3. Implémenter l'algorithme.
4. Tester votre implémentation: on a besoin de produire des matrices de grande taille et de décomposition de Dunford non triviale.
5. Que pouvez-vous dire si u est donné par une matrice à coefficients réels, rationels.
6. Ecrire un (plusieurs) algorithme de calcul des puissances de A. Les comparer...