Une formule explicite réalisant la décomposition de Jordan-Chevalley-Dunford effective

Jean-François Burnol, 14 (et 15) avril 2017

« *Ce qui se conçoit bien s'énonce clairement - Et les mots pour le dire arrivent aisément* » n'est qu'une grosse arnaque, car on n'a JAMAIS FINI DE BIEN CONCEVOIR. Zut à la fin.

Soit $\mathbf{K}$ un corps de caractéristique nulle, et A un endomorphisme d'un $\mathbf{K}$-espace vectoriel V de dimension finie p, et P son polynôme caractéristique unitaire.

Notre objectif est de calculer concrètement la décomposition de Jordan-Chevalley-Dunford qui m'obsède un peu trop ces derniers temps. Il s'agit de trouver un polynôme $D \in \mathbf{K}[X]$ tel que :

— $D(A)$ est diagonalisable sur une clôture algébrique,

— et $A - D(A)$ est nilpotent.

Le D, comme polynôme, n'est unique que modulo le polynôme minimal de A, que nous ne connaissons pas, donc nous nous contentons de chercher l'unique D qui fonctionne pour la multiplication par X sur $V = \mathbf{K}[X]/(P)$ et donc pour tous les A de polynôme caractéristique P (la diagonalisabilité de $D(A)$ se reconnaît par $Q(D(A)) = 0$).

Soient $\lambda_1, \ldots, \lambda_q$ les racines distinctes de P dans une clôture algébrique $\overline{\mathbf{K}}$. Soit $Q = \prod(X - \lambda_j)$. On l'obtient par la formule $P/\mathrm{pgcd}(P, P')$ qui montre $Q \in \mathbf{K}[X]$. Lorsque $q := \deg Q$ vaut 1, la solution est $D = \lambda_1 = -Q(0)$, indépendamment de la multiplicité de l'unique valeur propre λ_1. Nous supposerons par la suite $\boxed{q \geqslant 2}$.

Le polynôme D est la solution sur la clôture algébrique des congruences

$$\begin{aligned} D &\equiv \lambda_1 \pmod{(X-\lambda_1)^{m_1}} \\ &\cdots \\ D &\equiv \lambda_q \pmod{(X-\lambda_q)^{m_q}} \end{aligned} \tag{$\mathcal{D}$}$$

pour $P = \prod(X - \lambda_j)^{m_j}$. Il s'agit de résoudre concrètement ce problème sans avoir à manipuler numériquement les λ_j où toute autre irrationalité par rapport au corps $\mathbf{K}$.

Je l'ai déjà abordé à de multiples reprises ces derniers jours :

— http://jf.burnol.free.fr/agreg170406Dunford_NewAlgo.pdf

— http://jf.burnol.free.fr/agreg170408NewDun.pdf

— http://jf.burnol.free.fr/agreg170410NewtonSchroederDunford.pdf

— http://jf.burnol.free.fr/agreg170413DunfordLineaire.pdf

Tous les algorithmes donnent des méthodes donnant les solutions pour $\max(m_j) \leqslant N$.

Ici, je vais extraire de la preuve incluse dans la dernière fiche une *formule explicite* et elle aura de plus l'avantage de ne pas traiter principalement les $P = Q^N$ mais de donner aussi une solution spécifique à tout P de polynôme réduit Q quelles que soient les multiplicités.

Théorème 1. *Soit P le polynôme caractéristique unitaire de A,*

$$S \coloneqq \operatorname{pgcd}(P, P') \qquad \textit{et} \qquad Q \coloneqq P/S$$

On considère les q polynômes ($q = \deg Q$) :

$$Z_0 \coloneqq 1,\ Z_1 \coloneqq \int_0^X S\,dX,\ Z_2 \coloneqq \int_0^X XS\,dX,\ \dots,\ Z_{q-1} \coloneqq \int_0^X X^{q-2} S\,dX$$

(qui sont de degrés $< \deg P$), ainsi que leurs réductions modulo Q :

$$W_j \coloneqq Z_j \bmod Q \qquad (0 \leqslant j \leqslant q-1)$$

Le $D \in \mathbf{K}[X]$, $\deg D < \deg P$, de la décomposition de Chevalley-Dunford *est donné par la* formule explicite *suivante* :

$$D = \Big[Z_0 \,|\, Z_1 \,|\, \cdots \,|\, Z_{q-1}\Big] \cdot \Big[W_0 \,|\, W_1 \,|\, \cdots \,|\, W_{q-1}\Big]^{-1} \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Autrement dit, D est l'unique combinaison linéaire $\sum_{0 \leqslant k \leqslant q-1} u_k Z_k$ congrue à X modulo Q. Dans la formule ci-dessus, les polynômes sont considérés comme les colonnes de leurs coefficients dans les bases $(1, X, \dots, X^{\deg P - 1})$ et $(1, X, \dots, X^{q-1})$ respectivement.

Trouver D explicitement comme somme de monômes revient donc, une fois S et Q connus, à faire des opérations qui ont un coût linéaire en $p = \deg P$: q fois $\mathcal{O}(p)$ pour les intégrales, puis q fois $\mathcal{O}(qp)$ pour les réductions modulo Q (en utilisant les algorithmes « de l'École »). Puis la résolution d'un système avec q inconnues, comptons $\mathcal{O}(q^2)$ (par méthode des pivots « de l'École »), et finalement une combinaison linéaire au coût qp. Sauf erreur cela donne donc un coût total en $\mathcal{O}(q^2 p)$. Si $P = Q^N$, on obtient donc $\mathcal{O}(q^3 N)$.

Pour la démonstration je commence par :

Lemme 1. *Les congruences $\mathcal{D}$ sont équivalentes aux deux conditions :*

$$D \equiv X \pmod{Q} \tag{1a}$$

$$D' \equiv 0 \pmod{S} \tag{1b}$$

Preuve. Si D est solution des congruences associées aux valeurs propres, alors certainement $D - X$ s'annule en chaque λ_j, donc déjà $D \equiv X \bmod Q$. De plus $D - \lambda_j$ a en λ_j un zéro de multiplicité au moins $m_j \geqslant 1$. Si $m_j > 1$, la dérivée D' aura en λ_j un zéro de multiplicité au moins $m_j - 1$. Donc D' est divisible par $\prod_j (X - \lambda_j)^{m_j - 1}$ qui n'est autre que $P/Q = S$.

Réciproquement si $D' \equiv 0 \pmod{S}$ alors en un λ_j avec $m_j > 1$, D' a un zéro de multiplicité au moins $m_j - 1$, donc $D - D(\lambda_j)$ a un zéro de multiplicité au moins m_j. Mais $D \equiv X \pmod{Q}$ donc $D(\lambda_j) = \lambda_j$. Ainsi $D \equiv \lambda_j \bmod (X - \lambda_j)^{m_j}$. Ceci est vrai aussi si $m_j = 1$, puisque $D \equiv X \bmod Q$. Il en résulte que D est solution des congruences associées aux valeurs propres. □

Lemme 2. *Le morphisme $\psi : \mathbf{K} \times \mathbf{K}_{q-2}[X] \to \mathbf{K}_{q-1}[X]$ (avec $\mathbf{K}_n[X]$ l'espace vectoriel des polynômes de degrés au plus égaux à n) défini par la formule :*

$$\psi(u, M) = u + \int_0^X MS\, dX \mod Q$$

est un isomorphisme.

Preuve. Supposons que $\psi(u, M)$ est nul. Cela veut dire que $\int_0^X MS\, dX = -u + QY$ pour un certain polynôme Y.

Le polynôme $U = \int_0^X MS\, dX + u = QY$ est nul en chaque λ_j. De plus sa dérivée $U' = MS$ s'annule au moins à l'ordre $m_j - 1$ en chaque λ_j (si $m_j = 1$, rien de spécial). Donc U s'annule au moins à l'ordre m_j en chaque λ_j. Par conséquent U est un multiple de P. Donc $Y = U/Q$ est un multiple de S. Si Y n'est pas nul $\deg(QY - u) = \deg(QY) = q + \deg Y$ mais $\deg \int_0^X MS\, dX = 1 + \deg(MS) = 1 + \deg M + \deg S < q + \deg S$ puisque $1 + \deg M \leqslant q - 1$. Ceci donne $\deg Y < \deg S$, contradiction si Y est non nul.

Par conséquent $Y = 0$, puis $\int_0^X MS\, dx = -u$ donc en dérivant $MS = 0$ donc $M = 0$. Donc $u = 0$.

Nous avons prouvé que ψ est injective mais les deux espaces vectoriels ont la même dimension q. Donc ψ est un isomorphisme.

Voici une variante (15 avril) : X s'écrit $\psi(u, M)$ si et seulement si on peut trouver un polynôme D de la forme $u + \int_0^X MS\, dX$, $\deg M < q - 1$, de sorte que $D \equiv X \bmod Q$.

Mais cela signifie exactement que $\deg D < \deg P$, S divise D', et $D \equiv X \bmod Q$. D'après le Lemme 1 (vu sur $\overline{\mathbf{K}}$), ce problème équivaut aux congruences ($\mathcal{D}$) et possède donc exactement une solution sur la clôture algébrique $\overline{\mathbf{K}}$, donc exactement un (u, M) à coefficients dans $\overline{\mathbf{K}}$ convient. Si le noyau de ψ (sur $\mathbf{K}$) n'était pas réduit à $\{(0,0)\}$, on pourrait modifier ce (u, M) et obtenir une autre solution. Donc ψ (sur $\mathbf{K}$) est injective. Bien sûr on peut rédiger différemment cette petite descente. Et aussi on aurait pu avoir démontré préalablement que la solution D aux congruences ($\mathcal{D}$) est en fait définie sur $\mathbf{K}$, donc l'équation $\psi(u, M) = X$ a une et exactement une solution, ce qui prouve que ψ est un isomorphisme au vu des dimensions. □

J'en viens à la preuve du Théorème 1.

Preuve. D'après le Lemme 2, la matrice $q \times q$ des W_j est inversible car $(W_0, W_1, \ldots, W_{q-1})$ est image par ψ de la base $(1, X^0, X^1, \ldots, X^{q-2})$ de $\mathbf{K} \times \mathbf{K}_{q-2}[X]$. Considérons le polynôme D défini par la formule. C'est donc que $D = u_0 + \sum_{j=1}^{q-1} u_j Z_j$ avec les coefficients u_0, u_1, …, u_{q-1} choisis de sorte que $u_0 W_0 + u_1 W_1 + \cdots + u_{q-1} W_{q-1} \equiv X \bmod Q$. Mais cela signifie exactement $D \equiv X \bmod Q$. Par ailleurs $D' = \sum_{j=1}^{q-1} u_j X^{j-1} S \equiv 0 \bmod S$. D'après le Lemme 1 le polynôme D est solution des congruences associées aux racines de P. C'est donc l'unique solution de ces congruences vérifiant $\deg D < \deg P$, c.q.f.d. □

Il serait intéressant d'examiner dans quelle mesure cela peut aider pour des algorithmes numériques de calculs de racines de polynômes complexes. Remarquons que $D(0)$ est donné par le seul u_0 (donc une formule déterminantale) et donc en translatant on peut aussi obtenir des formules à la Cramer pour un $D(t)$. On peut même traiter t comme une indéterminée…

Il n'est pas impossible non plus que je n'aie fait que réinventer la roue dans cette histoire, c'est ce à quoi je m'attends. À titre de faible excuse, toute cette série a été motivée par des considérations pratiques : comment réduire au maximum le coût calculatoire. L'algorithme de cette fiche est tout ce qu'il y a de plus concret ; il repose sur une formule exacte pour D comme somme de monômes et non sur l'aboutissement d'un algorithme itératif.