Exercices sur les chapitres « Approximants de Padé et de Padé-Hermite » et « Matrices creuses »

À préparer pour le 25/10/2018

Exercice 1. Montrer, en employant un argument algorithmique, qu'il n'existe aucun approximant de Padé de type $(1,1)$ de $1+X^2$.

Exercice 2 (Lien entre reconstruction rationnelle et approximation de Padé-Hermite)**.** Soit $\mathbb{K}$ un corps, et soient A, B deux polynômes de $\mathbb{K}[X]$, avec $n = \deg(A) > \deg(B)$, et soit $k \in \{1, \dots, n\}$. Montrer que (R, V) est solution du problème de reconstruction rationnelle

$$\deg(R) < k, \quad \deg(V) \le n-k \quad \text{et} \quad R \equiv VB \bmod A$$

si et seulement s'il existe un polynôme $U \in \mathbb{K}[X]$ tel que (R, V, U) soit un approximant de Padé-Hermite de $(-1, B, A)$ de type $(k-1, n-k, n-k-1)$.

Exercice 3 (Probabilité de réussite de l'algorithme de Wiedemann)**.** Soit M une matrice dans $\mathcal{M}_n(\mathbb{K})$, soit b un vecteur de $\mathbb{K}^n \setminus \{0\}$ et soit f le polynôme minimal de la suite $(M^i \cdot b)_{i\ge 0}$.
Le but de l'exercice est d'estimer la probabilité $\mathcal{P}$ que f coïncide avec le polynôme minimal de la suite $({}^t u \cdot M^i \cdot b)_{i \ge 0}$ lorsque u est un vecteur de $\mathbb{K}^n$ dont les coordonnées sont choisies aléatoirement au hasard dans un sous-ensemble fini U de $\mathbb{K}$.

1. Montrer qu'il existe une application $\psi : \mathbb{K}^n \to \mathbb{A} = \mathbb{K}[X]/(f)$, $\mathbb{K}$-linéaire et surjective, telle que pour tout vecteur $u \in \mathbb{K}^n$ on ait

$$f \text{ est le polynôme minimal de } ({}^t u \cdot M^i \cdot b)_{i\ge 0} \iff \psi(u) \text{ est inversible dans } \mathbb{A}.$$

   [Indication : l'application $\phi : \mathbb{K}^n \to \mathbb{K}^{\mathbb{N}}$ définie par $\phi(u) = ({}^t u \cdot M^i \cdot b)_{i\ge 0}$ induit une application linéaire surjective $\mathbb{K}^n \to M_f$, où M_f est l'espace vectoriel des suites de $\mathbb{K}^{\mathbb{N}}$ admettant f comme polynôme annulateur. Par ailleurs, $\mathbb{A}$ et M_f sont isomorphes en tant qu'espaces vectoriels.]

2. Soit d le degré de f. Montrer qu'il existe un polynôme non identiquement nul $R \in \mathbb{K}[X_1, \dots, X_n]$ de degré total au plus d tel que pour tout vecteur $u = {}^t(u_1, \dots, u_n) \in \mathbb{K}^n$ on ait

$$\psi(u) \text{ est inversible dans } \mathbb{A} \text{ si et seulement si } R(u_1, \dots, u_n) \neq 0.$$

   [Indication : utiliser un résultant.]

3. Montrer que R admet au plus $d \cdot |U|^{n-1}$ racines dans U^n. En déduire que la probabilité qu'un élément de U^n dont les coordonnées sont choisies aléatoirement au hasard dans U soit racine de R est bornée par $d/|U|$.

4. Conclure que la probabilité $\mathcal{P}$ vérifie

$$\mathcal{P} \ge 1 - \frac{d}{|U|}.$$