UFR de Mathématiques et Informatique
Université Bordeaux I
Année 1999–2000

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Corrigé de l'épreuve du 20 janvier 2000

Exercice I

1) Il est clair que $< P, Q >$ est une forme bilinéaire, et que cette forme est symétrique. De plus, $< P, P >= \int_0^1 P(x)^2 A(x)\,dx$ est bien positif ou nul puisque $A(x)$ est positif ou nul sur $[0, 1]$. Le point le plus important est de noter que puisque $P^2(x)A(x)$ est une fonction *continue*, on ne peut avoir $< P, P >= 0$ que si $P^2(x)A(x)$ est identiquement nul sur $[0, 1]$, ce qui n'est pas possible pour un polynôme non identiquement nul. Il en résulte que $< P, P >= 0$ si et seulement si $P = 0$, donc $< P, Q >$ est bien un produit scalaire.

2) a) On a

$$\begin{aligned}P_1(X) &= \frac{c_1}{A(X)}(A(X)X(1-X))' = \frac{c_1}{A(X)}(A(X)(1-2X) + A'(X)X(1-X)) \\ &= c_1\left((1-2X) + \frac{A'(X)}{A(X)}X(1-X)\right) .\end{aligned}$$

Puisque $P_1(X)$ est un polynôme, il en résulte que $X(1-X)A'(X)/A(X)$ est un polynôme. Or soit $\alpha \in \mathbb{C}$ une racine de $A(X)$, et soit m son ordre de multiplicité. On peut donc écrire $A(X) = (X-\alpha)^m B(X)$ et $A'(X) = (X-\alpha)^{m-1}C(X)$, où $B(X)$ et $C(X)$ sont des polynômes non divisibles par $X - \alpha$, donc tels que $B(\alpha) \neq 0$ et $C(\alpha) \neq 0$. Comme $X(1-X)A'(X)/A(X) = X(1-X)C(X)/((X-\alpha)B(X))$ est un polynôme, on a $\alpha(1-\alpha)C(\alpha) = 0$, et puisque $C(\alpha) \neq 0$, on a donc bien $\alpha = 0$ ou $\alpha = 1$, en d'autres termes les racines dans $\mathbb{C}$ de $A(X)$ sont 0 ou 1.

Ceci signifie donc que l'on peut écrire $A(X) = cX^a(1-X)^b$ pour a et b entiers positifs ou nuls, et puisque $A(x) \geq 0$ sur $[0, 1]$ et non identiquement nul, on doit avoir $c > 0$.

b) On a

$$P_n(X) = \frac{c_n}{X^a(1-X)^b}\frac{d^n}{dX^n}(X^{n+a}(1-X)^{n+b}) .$$

Le polynôme $X^{n+a}(1-X)^{n+b}$ est de degré $2n+a+b$ et possède 0 comme racine d'ordre $n+a$ et 1 comme racine d'ordre $n+b$. Il en résulte que sa dérivée n-ième est un polynôme de degré $n+a+b$ qui possède 0 comme racine d'ordre a et 1 comme racine d'ordre b, donc elle est divisible par $X^a(1-X)^b$, et le quotient est donc bien un polynôme, de degré exactement égal à n.

Montrons que les P_n forment une famille de polynômes orthogonaux pour notre produit scalaire. Pour simplifier les notations, posons $S(X) = X^{n+a}(1-X)^{n+b}$ et écrivons D à la place de d/dx. Soit Q un polynôme de degré $m < n$. Par intégration par parties, on obtient

$$\frac{1}{c_n} < P_n, Q >= \int_0^1 D^n S(x)Q(x)\,dx = D^{n-1}S(x)Q(x)\big|_0^1 - \int_0^1 D^{n-1}S(x)DQ(x)\,dx \;.$$

Or comme ci-dessus, le polynôme $S(X)$ possède 0 et 1 comme racines d'ordre supérieur ou égal à n. Il en résulte que toutes ses dérivées jusqu'à l'ordre $n-1$ s'annulent en 0 et 1, donc le terme tout intégré est nul, et on a donc

$$\frac{1}{c_n} < P_n, Q >= -\int_0^1 D^{n-1}S(x)DQ(x)\,dx \;.$$

En effectuant des intégrations par parties successives, on en déduit que pour tout entier k tel que $0 \le k \le n$ on a

$$\frac{1}{c_n} < P_n, Q >= (-1)^k \int_0^1 D^{n-k}S(x)D^kQ(x)\,dx \;,$$

et donc en particulier

$$\frac{1}{c_n} < P_n, Q >= (-1)^n \int_0^1 S(x)D^nQ(x)\,dx \;.$$

Comme on a supposé que le degré de $Q(X)$ est strictement inférieur à n, on a $D^nQ(X) = 0$, donc $< P_n, Q >= 0$. Appliquant ceci à $Q = P_m$, on en déduit bien que les P_n forment une famille de polynômes orthogonaux.

Enfin, pour que les P_n soient unitaires (auquel cas la famille est unique), il suffit d'ajuster convenablement la constante c_n, comme nous allons le faire maintenant.

c) Reprenant les notations ci-dessus, le terme dominant de $S(X)$ est $(-1)^{n+b}X^{2n+a+b}$. Le terme dominant de sa dérivée n-ième est donc égal à

$$(-1)^{n+b}(2n+a+b)(2n+a+b-1)\ldots(n+a+b+1)X^{n+a+b} = (-1)^{n+b}\frac{(2n+a+b)!}{(n+a+b)!}X^{n+a+b} \;.$$

Par ailleurs, le terme dominant de $X^a(1-X)^b$ est égal à $(-1)^bX^{a+b}$. On en déduit que le terme dominant de $P(X)$ est égal à

$$(-1)^n c_n \frac{(2n+a+b)!}{(n+a+b)!}X^n \;.$$

Pour que ceci soit égal à X^n il est donc nécéssaire et suffisant que

$$c_n = (-1)^n \frac{(n+a+b)!}{(2n+a+b)!} \;.$$

3) Les coefficients de X^n dans les deux membres de l'équation de récurrence sont égaux puisque les P_n sont unitaires. En identifiant les coefficients de X^{n-1}, on obtient $\lambda_n = \lambda_{n-1} + a_n$, d'où

$$a_n = \lambda_n - \lambda_{n-1} \; .$$

De même, en identifiant les coefficients de X^{n-2}, on obtient $\mu_n = \mu_{n-1} + a_n\lambda_{n-1} + b_n$, d'où

$$b_n = \mu_n - \mu_{n-1} - a_n\lambda_{n-1} = \mu_n - \mu_{n-1} - \lambda_{n-1}(\lambda_n - \lambda_{n-1}) \; .$$

4) a) On a par récurrence

$$\frac{d^n}{dX^n}X^m = m(m-1)\dots(m-n+1)X^{m-n} = \frac{m!}{(m-n)!}X^{m-n} \; .$$

b) D'après 2c), on a tout d'abord $c_n = (-1)^n(n+3)!/(2n+3)!$. D'autre part, pour calculer $D^n(A(X)X^n(1-X)^n)$, il ne faut surtout pas appliquer la formule de Leibnitz donnant la dérivée n-ième d'un produit. Beaucoup plus simplement, on remplace $A(X)$ par sa valeur et on obtient par la formule du binôme :

$$\begin{aligned} S(X) = A(X)X^n(1-X)^n &= X^{n+2}(1-X)^{n+1} \\ &= (-1)^{n+1}X^{n+2}(X^{n+1} - (n+1)X^n + \frac{n(n+1)}{2}X^{n-1} + \cdots) \\ &= (-1)^{n+1}(X^{2n+3} - (n+1)X^{2n+2} + \frac{n(n+1)}{2}X^{2n+1} + \cdots) \; . \end{aligned}$$

Il résulte du a) que

$$D^nS(X) = (-1)^{n+1}\left(\frac{(2n+3)!}{(n+3)!}X^{n+3} - (n+1)\frac{(2n+2)!}{(n+2)!}X^{n+2} + \frac{n(n+1)}{2}\frac{(2n+1)!}{(n+1)!}X^{n+1} + \cdots\right) ,$$

d'où

$$\begin{aligned} c_nD^nS(X) &= -\left(X^{n+3} - (n+1)\frac{n+3}{2n+3}X^{n+2} + \frac{n(n+1)}{2}\frac{(n+2)(n+3)}{(2n+2)(2n+3)}X^{n+1} + \cdots\right) \\ &= -\left(X^{n+3} - \frac{(n+1)(n+3)}{2n+3}X^{n+2} + \frac{n(n+2)(n+3)}{4(2n+3)}X^{n+1} + \cdots\right) \; . \end{aligned}$$

En effectuant la division euclidienne de ceci par $A(X) = X^2(1-X) = -(X^3 - X^2)$, on obtient finalement :

$$P_n = X^n - \frac{n(n+2)}{2n+3}X^{n-1} + \frac{(n-1)n(n+2)}{4(2n+3)}X^{n-2} + \cdots \; .$$

On a donc

$$\lambda_n = -\frac{n(n+2)}{2n+3} \quad \text{et} \quad \mu_n = \frac{(n-1)n(n+2)}{4(2n+3)} \; .$$

c) D'après la question 3), on a

$$a_n = \lambda_n - \lambda_{n-1} = -\frac{2n^2+4n+3}{(2n+1)(2n+3)}$$

et

$$b_n = \mu_n - \mu_{n-1} - a_n\lambda_{n-1} = -\frac{(n-1)(n+2)}{4(2n+1)^2} \; .$$

Exercice II

1) a) Le polynôme caractéristique de A est égal à

$$P(X) = (X - z)(X - \overline{z}) + t\overline{t} = X^2 - 2aX + a^2 + b^2 + c^2 + d^2 \ .$$

Il en résulte que les valeurs propres de A sont

$$\lambda_1 = a + i\sqrt{b^2 + c^2 + d^2} \quad \text{et} \quad \lambda_2 = a - i\sqrt{b^2 + c^2 + d^2} \ .$$

Comme $b^2 + c^2 + d^2 \geq 0$, on a clairement $\lambda_2 = \overline{\lambda_1}$, et donc si nous écrivons $\lambda = \lambda_1$, les valeurs propres sont les deux nombres conjugués λ et $\overline{\lambda}$.

b) On ne peut avoir $\lambda = \overline{\lambda}$ que si $b^2 + c^2 + d^2 = 0$, donc $b = c = d = 0$, et dans ce cas $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ est égale à a fois la matrice identité. Il en résulte que soit les valeurs propres sont distinctes, auquel cas la matrice est diagonalisable, soit la matrice est déjà sous forme diagonale, et même scalaire, donc A est toujours diagonalisable.

c) On vérifie immédiatement que AA^* est égale à N fois la matrice identité, avec $N = a^2 + b^2 + c^2 + d^2$. Si A est la matrice nulle, elle est clairement diagonalisable. Sinon, on en déduit que $A/\sqrt{N}$ est une matrice unitaire, et d'après un théorème du cours une telle matrice est diagonalisable.

2) On vérifie immédiatement que si λ_i est une valeur propre, le vecteur propre associé dont la première coordonnée est t vaut $(t, \lambda_i - z)^t$. Il en résulte que les deux vecteurs propres souhaités sont $(t, \lambda - z)^t$ et $(t, \overline{\lambda} - z)^t$, d'où la diagonalisation $A = PDP^{-1}$ avec

$$D = \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} t & t \\ \lambda - z & \overline{\lambda} - z \end{pmatrix} \ .$$

On calcule de plus que

$$P^{-1} = \frac{1}{t(\lambda - \overline{\lambda})} \begin{pmatrix} z - \overline{\lambda} & t \\ \lambda - z & -t \end{pmatrix} \ .$$

3) Il en résulte que $\exp(A) = P \exp(D) P^{-1}$, donc

$$\exp(A) = \frac{1}{t(\lambda - \overline{\lambda})} \begin{pmatrix} t & t \\ \lambda - z & \overline{\lambda} - z \end{pmatrix} \begin{pmatrix} e^{\lambda} & 0 \\ 0 & e^{\overline{\lambda}} \end{pmatrix} \begin{pmatrix} z - \overline{\lambda} & t \\ \lambda - z & -t \end{pmatrix} \ .$$

Tous calculs faits, on obtient

$$\exp(A) = \frac{1}{\lambda - \overline{\lambda}} \begin{pmatrix} (z - \overline{\lambda})e^{\lambda} - (z - \lambda)e^{\overline{\lambda}} & t(e^{\lambda} - e^{\overline{\lambda}}) \\ \dfrac{(z - \lambda)(z - \overline{\lambda})}{t}(e^{\overline{\lambda}} - e^{\lambda}) & (z - \overline{\lambda})e^{\overline{\lambda}} - (z - \lambda)e^{\lambda} \end{pmatrix} \ .$$

Or, comme $\exp(A)$ est également somme de la série $A^n/n!$ et qu'on vérifie que la forme de la matrice A est conservée par addition et multiplication, $\exp(A)$ doit être encore de la forme $\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}$ pour certains nombres complexes u et v. On vérifie que ceci est bien correct pour les éléments diagonaux (en notant que $\lambda - \overline{\lambda}$ ainsi que $z - \lambda$ et $z - \overline{\lambda}$ sont des imaginaires purs). Pour les éléments qui ne sont pas sur la diagonale, ceci entraine nécessairement que le terme où figure un t au dénominateur doit se simplifier. Et de fait, d'après l'équation du second degré vérifié par λ, on a $(z-\lambda)(z-\overline{\lambda})/t = \overline{t}$, donc finalement

$$\exp(A) = \frac{1}{\lambda - \overline{\lambda}} \begin{pmatrix} (z-\overline{\lambda})e^{\lambda} - (z-\lambda)e^{\overline{\lambda}} & t(e^{\lambda} - e^{\overline{\lambda}}) \\ \overline{t}(e^{\overline{\lambda}} - e^{\lambda}) & (z-\overline{\lambda})e^{\overline{\lambda}} - (z-\lambda)e^{\lambda} \end{pmatrix} .$$

Exercice III

1) Utilisons d'abord la première méthode. On a

$$\|A\| = \sup_{\|X\|=1} \|AX\| .$$

Comme nous sommes en dimension 2, si $\|X\| = 1$ on peut écrire $X = (\cos\theta, \sin\theta)^t$ pour un certain angle θ. On a donc

$$\begin{aligned} \|AX\|^2 &= (a\cos\theta + b\sin\theta)^2 + c^2\sin^2\theta \\ &= a^2\cos^2\theta + (b^2+c^2)\sin^2\theta + 2ab\cos\theta\sin\theta \\ &= \frac{1}{2}(a^2(1+\cos 2\theta) + (b^2+c^2)(1-\cos 2\theta) + 2ab\sin 2\theta) \\ &= \frac{1}{2}(a^2+b^2+c^2 + (a^2-b^2-c^2)\cos 2\theta + 2ab\sin 2\theta) . \end{aligned}$$

Or soit $f(x)$ une fonction du type $f(x) = u + v\cos x + w\sin x$. On a $f'(x) = -v\sin x + w\cos x$, qui s'annule donc pour les valeurs de x telles que $\operatorname{tg} x = w/v$. Pour de telles valeurs, on a $\cos^2 x = 1/(1+\operatorname{tg}^2 x) = v^2/(v^2+w^2)$, donc $\cos x = \varepsilon v/\sqrt{v^2+w^2}$ pour $\varepsilon = \pm 1$, et donc $\sin x = \cos x \operatorname{tg} x = \varepsilon w/\sqrt{v^2+w^2}$. Il résulte de ceci que les extrémums de $f(x)$ sur $\mathbb{R}$ sont les deux valeurs $u + \varepsilon\sqrt{v^2+w^2}$ pour $\varepsilon = \pm 1$, et donc le maximum de $f(x)$ est égal à $u + \sqrt{v^2+w^2}$ (ceci est utilisé constamment en physique). Appliquant ceci à notre fonction, on en déduit que

$$\|A\|^2 = \frac{1}{2}\left(a^2+b^2+c^2 + \sqrt{(a^2-b^2-c^2)^2 + 4a^2b^2}\right) .$$

Utilisons maintenant la deuxième méthode. Soit $A = UDV^t$ une décomposition en valeurs singulières de A. Puisque U et V sont des matrices orthogonales, on a $\|A\| = \|D\|$, et il est clair que la norme d'une matrice diagonale à coefficients diagonaux positifs ou nuls est égal au plus grand de ces coefficients. En d'autres termes, la norme de A est égale à sa plus grande valeur singulière.

On calcule que $AA^t = \begin{pmatrix} a^2+b^2 & bc \\ bc & c^2 \end{pmatrix}$ dont le polynôme caractéristique est égal à $X^2 - (a^2+b^2+c^2)X + a^2c^2$. Il en résulte que les valeurs singulières de A sont les racines carrées des racines (non nulles) de ce polynôme, c'est à dire de

$$\frac{1}{2}\left(a^2+b^2+c^2 \pm \sqrt{(a^2+b^2+c^2)^2 - 4a^2c^2}\right) .$$

On a donc

$$\|A\|^2 = \frac{1}{2}\left(a^2+b^2+c^2 + \sqrt{(a^2+b^2+c^2)^2 - 4a^2c^2}\right) ,$$

et il est immédiat de vérifier que ceci est bien la même expression que celle trouvée par l'autre méthode.

2) a) Il y a plusieurs manières de faire ceci. On peut par exemple calculer A^{-1} et remarquer que c'est aussi une matrice triangulaire supérieure, puis appliquer le résultat ci-dessus. Plus simplement peut-être, si $A = UDV^t$ est une SVD de A alors $A^{-1} = (V^t)^{-1}D^{-1}U^{-1}$ est une SVD de A^{-1}, donc $\|A^{-1}\|$ est égal au plus grand élément diagonal de D^{-1}, donc à l'inverse du plus petit élément diagonal de D, alors que $\|A\|$ est égal au plus grand. On en déduit que

$$\frac{\|A\|}{\|A^{-1}\|} = \det(D) = \det(A) = ac$$

donc que

$$\|A^{-1}\| = \frac{\|A\|}{ac} .$$

b) Soit $c(A)$ le conditionnement de A. On a

$$c(A) = \|A\|\|A^{-1}\| = \frac{\|A\|^2}{ac} .$$

Il en résulte que à a et c fixés, le conditionnement de A est minimum lorsque $\|A\|^2$ est minimum. D'après la deuxième formule trouvée ci-dessus pour ceci, puisque $a^2+b^2+c^2$ est une fonction croissante de b^2, il en résulte que le conditionnement est minimum lorsque b^2 est le plus petit possible, c'est à dire égal à 0.

Exercice IV

1) On a

$$AA^t = \begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix} .$$

Le polynôme caractéristique de cette matrice est $X^2 - 10X$, dont les racines sont $X = 10$ et $X = 0$. Il en résulte que

$$D = \begin{pmatrix} \sqrt{10} & 0 \\ 0 & 0 \end{pmatrix} .$$

D'autre part, la matrice U est la matrice orthogonale dont les colonnes sont les vecteurs propres normalisés de la matrice symétrique AA^t (dans le même ordre que les valeurs propres correspondantes). Un calcul immédiat donne comme vecteurs propres $(1,2)^t$ pour la valeur propre 10 et $(-2,1)^t$ pour la valeur propre 0, donc

$$U = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} .$$

Il est important de noter que cette matrice n'est pas unique puisqu'on peut changer les vecteurs propres en leurs opposés.

La matrice V peut s'obtenir comme la matrice U, mais cette fois-ci avec les vecteurs propres de la matrice $A^tA = \begin{pmatrix} 5 & 5 \\ 5 & 5 \end{pmatrix}$, qui sont clairement $(1,1)^t$ et $(1,-1)^t$. Toutefois, il serait prématuré d'écrire

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

puisque on peut changer les vecteurs propres en leurs opposés. Un calcul immédiat montre toutefois qu'on a bien $UDV^t = A$. Cela n'aurait bien sûr plus été le cas si on avait par exemple changé V en $-V$.

2) Si $A = UDV^t$ est une SVD, on sait que $A^\dagger = VD^\dagger U^t$ avec $D^\dagger = \begin{pmatrix} 1/\sqrt{10} & 0 \\ 0 & 0 \end{pmatrix}$. On trouve

$$A^t = \frac{1}{10} \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} .$$

On trouverait bien sûr le même résultat en utilisant la caractérisation donnée dans le texte.