UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2000–2001

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Corrigé de la session de septembre 2001

Exercice I

1) Il est clair que $< P, Q >$ est une forme bilinéaire, que $< P, P > \geq 0$, et que $< 0, 0 >= 0$. Il faut montrer que $< P, P >= 0$ implique que $P = 0$. Or $< P, P >= 0$ équivaut à $\int_0^1 P'(x)^2\, dx = 0$ et $P(0) = 0$. Or, comme d'habitude on utilise le fait que si l'intégrale d'une fonction positive ou nulle *et continue* est nulle, la fonction est identiquement nulle. Il en résulte que le polynôme P' a une infinité de racines, donc est identiquement nul (attention, une fonction continue arbitraire pourrait être nulle sur $[0, 1]$ sans être identiquement nulle).

Il en résulte que P est un polynôme constant, et puisque $P(0) = 0$, que cette constante est nulle, donc $P = 0$.

2) Comme P_0 est de degré 0 et unitaire, on a $P_0(x) = 1$. Comme $P_0(0) = 1$ et que $P_0'(x) = 0$, un polynôme Q est orthogonal à P_0 si et seulement si $Q(0) = 0$, c'est à dire si Q n'a pas de terme constant. Il en résulte que l'on doit avoir $P_1(X) = X$. D'autre part on voit sur la définition qu'un polynôme Q est orthogonal à $P_1(X) = X$ si et seulement si $\int_0^1 Q'(x)\, dx = 0$, c'est à dire si et seulement si $Q(1) = Q(0)$, et donc Q est orthogonal à P_0 et à P_1 si et seulement si $Q(1) = Q(0) = 0$. Il en résulte que l'on doit avoir $P_2(X) = X^2 - X$. Enfin pour la même raison on a $P_3(X) = X^3 + aX^2 + bX$ avec $P_3(1) = a + b + 1 = 0$, donc $b = -a - 1$ et $P_3(X) = X^3 + aX^2 - (a + 1)X$, où a est déterminé par $< P_3, P_2 >= 0$. Comme on sait déjà que $< P_2, P_1 >=< P_2, X >= 0$, on écrit simplement que $< X^3 + aX^2, P_2 >= 0$, ce qui donne tous calculs faits $a = -3/2$, d'où $P_3(X) = X^3 - (3/2)X^2 + X/2$.

3) a) Il est clair que $(X(1-X))^{n+1}$ est un polynôme de degré égal à $2n+2$ et de terme de plus bas degré X^{n+1}. Il en résulte que sa dérivée n-ième est un polynôme de degré égal à $n + 2$ et de terme de plus bas degré $(n + 1)!X$, et en particulier $Q_n(0) = 0$.

b) Comme $Q_n(0) = 0$, on a $Q_n(0)A(0) = 0$. Il en résulte par intégration par parties que l'on a (en notant D l'opérateur de dérivation)

$$
\begin{aligned}
< Q_n, A > &= \int_0^1 DA(x)\, D^{n+1}((x(1-x))^{n+1})\, dx \\
&= DA(x) D^n((x(1-x))^{n+1})\Big|_0^1 - \int_0^1 D^2A(x)\, D^n((x(1-x))^{n+1})\, dx\ .
\end{aligned}
$$

Comme 0 et 1 sont racines d'ordre $n+1$ de $(x(1-x))^{n+1}$, le terme tout intégré est nul. Il en sera de même ultérieurement puisque l'ordre de dérivation sera même inférieur. Par récurrence, on en déduit que

$$
< Q_n, A >= (-1)^k \int_0^1 D^{k+1}A(x) D^{n+1-k}((x(1-x))^{n+1})\, dx\ .
$$

En particulier, appliquant ceci à $k = n+1$, on voit que si A est un polynôme de degré inférieur ou égal à $n+1$, la dérivée $n+2$-ième de A étant nulle on a bien $< Q_n, A >= 0$.

c) Supposons par récurrence $P_0, \ldots, P_{n-1}$ construits. Le polynôme P_n est l'unique polynôme unitaire de degré n et orthogonal aux P_j pour $j < n$. D'après ce que nous venons de voir, Q_{n-2} est orthogonal aux P_j pour $j < n$, et c'est un polynôme de degré exactement égal à n. Si on pose $c_n = 1/d_n$, où d_n est le coefficient de degré n de Q_{n-2}, le polynôme $c_n Q_{n-2}(X)$ répond à toutes les conditions, et donc par unicité on a $P_n(X) = c_n Q_{n-2}(X)$.

d) Le terme dominant de $(X(1-X))^{n+1}$ est $(-1)^{n+1}X^{2n+2}$. Il en résulte que la dérivée n-ième de ce terme dominant, qui est le terme dominant de $Q_n(X)$, est égal à $d_{n+2}X^{n+2}$ avec

$$
d_{n+2} = (-1)^{n+1}(2n+2)(2n+1)\cdots(2n+2-n+1) = (-1)^{n+1}\frac{(2n+2)!}{(n+2)!}\ .
$$

On a donc $d_n = (-1)^{n-1}(2n-2)!/n!$, donc

$$
c_n = \frac{1}{d_n} = (-1)^{n-1}\frac{n!}{(2n-2)!}\ .
$$

4) a) Comme P_n et P_{n+1} sont unitaires, en regardant les termes de degré $n+1$ on constate que $u_n = 1$.

b) D'après la formule du binôme, on a

$$
X^{n+1}(1-X)^{n+1} = \sum_{0\le k\le n+1} (-1)^k \binom{n+1}{k} X^{n+1+k}\ ,
$$

et puisque pour $m \ge n$ la dérivée n-ième de X^m est égale à $m!/(m-n)!X^{m-n}$, on obtient

$$
\begin{aligned}
Q_n(X) &= \sum_{0\le k\le n+1} (-1)^k \frac{(n+1)!(n+1+k)!}{k!(k+1)!(n+1-k)!} X^{k+1} \\
&= \sum_{1\le k\le n+2} (-1)^{k-1} \frac{(n+1)!(n+k)!}{(k-1)!k!(n+2-k)!} X^k\ .
\end{aligned}
$$

On obtient donc

$$P_n(X) = c_n Q_{n-2}(X) = \sum_{1\leq k\leq n} (-1)^{k+n} \frac{(n-1)!n!(n-2+k)!}{(2n-2)!(k-1)!k!(n-k)!} X^k \ .$$

c) Le coefficient de X^n dans P_{n+1} vaut par définition a_{n+1}. Il n'y a pas de coefficient de X^n dans P_{n-1}, et le coefficient de X^n dans $(X+v_n)P_n(X)$ est égal à $a_n + v_n$. On a donc

$$v_n = a_{n+1} - a_n \ .$$

De même, le coefficient de X^{n-1} dans P_{n+1} vaut par définition b_{n+1}, et le coefficient de X^{n-1} dans $(X+v_n)P_n(X) + w_n P_{n-1}(X)$ est égal à $b_n + v_n a_n + w_n$, d'où

$$w_n = b_{n+1} - b_n - a_n v_n = b_{n+1} - b_n - a_n(a_{n+1} - a_n) \ .$$

d) Le coefficient a_n s'obtient en prenant $k = n-1$ et b_n en prenant $k = n-2$ dans la formule explicite pour P_n trouvée ci-dessus. On obtient donc tous calculs faits $a_n = -n/2$ et $b_n = n(n-1)(n-2)/(4(2n-3))$. On en déduit que $v_n = -1/2$, et que $w_n = -n(n-2)/(4(2n-1)(2n-3))$.

On obtient donc la récurrence

$$P_{n+1}(X) = \left(X - \frac{1}{2}\right) P_n(X) - \frac{n(n-2)}{4(2n-1)(2n-3)} P_{n-1}(X) \ .$$

Attention, cette récurrence n'est valable que pour $n \geq 2$, puisque l'on a utilisé la formule $P_n = c_n Q_{n-2}$ qui n'est valable que pour $n \geq 2$. De fait, une vérification montre qu'elle est bien valable pour $n = 2$ (heureusement!), mais pas pour $n = 1$.

Exercice II

2) a) On calcule que $A^t A = 98J$ où

$$J = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \ .$$

Comme U est orthogonale, on en déduit que $98J = VD^2V^t$. Les valeurs propres de $98J$ sont trivialement 0 (double) et $98 \cdot 3 = 294$ (simple), d'où

$$D = \begin{pmatrix} 7\sqrt{6} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \ .$$

Pour obtenir une matrice V, il faut chercher une *base orthonormée* de vecteurs propres de $A^t A$ (n'importe quelle base ne conviendrait pas). Un vecteur propre pour la valeur propre 294 est le vecteur $(1,1,1)^t$, d'où on doit prendre $v_1 = (1/\sqrt{3})(1,1,1)^t$. Une base de vecteurs propres pour la valeur propre nulle est par exemple formée des vecteurs $(1,-1,0)^t$ et $(1,0,-1)^t$, qui sont automatiquement orthogonaux à v_1 (savez-vous pourquoi ?). Appliquant le procédé de Gram–Schmidt à cette base pour trouver une base orthonormée (et pas seulement orthogonale), on trouve $v_2 = (1/\sqrt{2})(1,-1,0)^t$ et $v_3 = (1/\sqrt{6})(1,1,-2)$, d'où

$$V = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{2} & \sqrt{3} & 1 \\ \sqrt{2} & -\sqrt{3} & 1 \\ \sqrt{2} & 0 & -2 \end{pmatrix} .$$

D'autre part, on calcule que

$$AA^t = \begin{pmatrix} 3 & 12 & 27 \\ 12 & 48 & 108 \\ 27 & 108 & 243 \end{pmatrix} .$$

Nous savons déjà que les valeurs propres de cette matrice sont 0 (double) et 294 (simple). Un vecteur propre correspondant à 294 est $(1,4,9)^t$, d'où $u_1 = (1/(7\sqrt{2}))(1,4,9)^t$ est le premier vecteur propre normalisé.

Une base de vecteurs propres pour la valeur propre nulle est par exemple formée des vecteurs $u_2' = (9,0,-1)^t$ et $u_3' = (4,-1,0)^t$, qui sont automatiquement orthogonaux à u_1. Aavant d'appliquer Gram–Schmidt directement, ce qui conduirait à des calculs un peu plus compliqués, on remplace u_2' par $2u_2' - 3u_3' = (6,3,-2)^t$ qui a l'avantage d'être de norme entière (égale à 7). Appliquant maintenant Gram–Schmidt à ce vecteur et u_3', on trouve $u_2 = (1/7)(6,3,-2)^t$ et $u_3 = (1/(7\sqrt{2}))(5,-8,3)^t$, d'où

$$U = \frac{1}{7\sqrt{2}} \begin{pmatrix} 1 & 6\sqrt{2} & 5 \\ 4 & 3\sqrt{2} & -8 \\ 9 & -2\sqrt{2} & 3 \end{pmatrix} .$$

Noter que les matrices U et V trouvées ci-dessus donnent *une* décomposition SVD, mais ne sont pas uniques, donc dans un autre corrigé on aurait pu prendre d'autres matrices. Seules les valeurs singulières (les éléments diagonaux de D) sont uniques.

b) La norme de A est égale à la plus grande valeur singulière, donc à $\sqrt{294} = 7\sqrt{6}$.

3) Par définition, $A^\dagger = VD^\dagger U^t$, où

$$D^\dagger = \begin{pmatrix} 1/(7\sqrt{6}) & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

Tous calculs faits, on trouve que

$$A^\dagger = \frac{1}{294} \begin{pmatrix} 1 & 4 & 9 \\ 1 & 4 & 9 \\ 1 & 4 & 9 \end{pmatrix} .$$

On voit que ce n'est autre que la transposée de A divisée par 294. Ceci aurait pu se voir sans calculs. En effet, on sait que $A^\dagger$ est caractérisée par le fait que $AA^\dagger$ et $A^\dagger A$ sont des matrices symétriques, ce qui est clair quand $A^\dagger$ est proportionelle à A^t, et telles que $AA^\dagger A = A$ et $A^\dagger AA^\dagger = A^\dagger$, ce qui se vérifie immédiatement.

Exercice III

1) Il est clair que $\omega^2 = \omega - 3$ et que $\overline{\omega} = 1 - \omega$.

2) Si $\alpha = a + b\omega$ et $\beta = c + d\omega$, il est clair que si α et β sont dans K alors $\alpha - \beta \in K$, et s'ils sont dans A alors $\alpha - \beta \in A$. Il en résulte que K et A sont des sous-groupes additifs de $\mathbb{C}$. De plus, on a $\alpha\beta = ac + (ad + bc)\omega + bd\omega^2$. Mais d'après la question précédente (et c'est le point essentiel), on a $\omega^2 = \omega - 3$, donc $\alpha\beta = (ac - 3bd) + (ad + bc + bd)\omega$, et ceci appartient bien à K si α et β y appartiennent, ou à A si α et β y appartiennent. La multiplication est donc stable, et bien entendu $1 \in A \subset K$, donc A est un sous-anneau de K qui est lui-même un sous-anneau de $\mathbb{C}$. Enfin, pour voir que K est un corps, il faut montrer que tout élement non nul est inversible. En effet si $\alpha = a + b\omega \neq 0$, on a tout d'abord

$$\alpha\overline{\alpha} = (a + b\omega)(a + b\overline{\omega}) = (a + b\omega)(a + b - b\omega) = a(a + b) + b^2\omega - b^2\omega^2 = a^2 + ab + 3b^2$$

d'après la première question. On a donc

$$\frac{1}{\alpha} = \frac{\overline{\alpha}}{\alpha\overline{\alpha}} = \frac{a + b\overline{\omega}}{a^2 + ab + 3b^2} = \frac{a + b}{a^2 + ab + 3b^2} - \frac{b}{a^2 + ab + 3b^2}\omega$$

et ceci est donc bien dans K puisque les coefficients sont dans $\mathbb{Q}$.

3) Nous venons de montrer que $\phi(\alpha) = a^2 + ab + 3b^2$. Mais en considérant b comme la variable prioritaire, on peut aussi écrire $\phi(\alpha) = 3(b + a/6)^2 + 11a^2/12$, ce qui est le résultat demandé.

4) On a $\phi(\alpha - (u + v\omega)) = \phi(\beta)$ avec $\beta = (a - u) + (b - v)\omega$. On a donc

$$\phi(\alpha - (u + v\omega)) = 3(b - v + (a - u)/6)^2 + 11(a - u)^2/12 \ .$$

Comme u est l'entier le plus proche de a, on a $|a - u| \leq 1/2$ donc $(a - u)^2 \leq 1/4$. De même, comme v est l'entier le plus proche de $b + (a - u)/6$, on a $|b + (a - u)/6 - v| \leq 1/2$ donc $(b - v + (a - u)/6)^2 \leq 1/4$. En remplaçant, on obtient

$$\phi(\alpha - (u + v\omega)) \leq 3/4 + 11/48 = 47/48 < 1 \ .$$

5) Soient x et y deux éléments de A avec $y \neq 0$. Comme A est un sous-anneau de K et que K est un corps, $\alpha = x/y$ est un élément de K. D'après la question précédente, si on pose $q = u + v\omega$ on a $\phi(\alpha - q) < 1$ (en fait plus petit ou égal à 47/48). Comme ϕ a la propriété d'être multiplicative (ce qui n'est pas exigé pour un stathme Euclidien), on a donc $\phi(y(\alpha - q)) < \phi(y)$. Or $r = y(\alpha - q) = x - qy \in A$, et bien entendu $q \in A$. On a donc écrit $x = qy + r$ avec q et y dans A et $\phi(r) < \phi(y)$, ce qui montre bien que ϕ est un stathme Euclidien (les autres propriétés sont évidentes). Il en résulte bien que l'anneau A est Euclidien.

Si on prend plus généralement $\omega = (1 + i\sqrt{4k-1})/2$ avec $k \geq 0$ entier, on peut essayer de faire le même raisonnement. On a toujours $\overline{\omega} = 1 - \omega$, et ici $\omega^2 = \omega - k$. L'ensemble K est toujours un corps et A un sous-corps. Toutefois, l'inégalité de la quatrième question devient

$$\phi(\alpha - (u + v\omega)) \leq \frac{4k^2 + 4k - 1}{16k} ,$$

et ceci est strictement inférieur à 1 si et seulement si $k = 1$, 2 et 3, c'est à dire $\omega = (1 + i\sqrt{d})/2$ avec $d = 3$, 7 et 11. Et de fait, pour $k = 4$ par exemple, c'est à dire pour $d = 15$, il n'est pas difficile de voir que l'anneau A n'est pas Euclidien pour le stathme ϕ, car il n'est même pas principal. En effet, on a par exemple

$$15 = 3 \cdot 5 = -(2\omega - 1)^2 ,$$

et on vérifie que les éléments 3, 5 et $2\omega - 1$ sont irréductibles, ne sont pas inversibles ni associés, ce qui est impossible dans un anneau principal.