14 juin 2021
Master 1 M.F., Orsay

Corrigé de l'examen de M.A.O. Calcul Formel

Toutes les fonctions programmées en `Sage` sont disponibles dans le Jupyter Notebook qui accompagne ce pdf (`examen_programmation.ipynb`).

Problème 1

1. Soit $i \in \{1, \dots, d\}$. On a $Q'(X) = \sum_{k=1}^{d} \prod_{j \neq k} (X - \alpha_j)$. Quand on évalue au point α_i, il ne reste que le terme correspondant à $k = i$, et on obtient $Q'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$ ce qui est bien la valeur en α_i de la fraction rationnelle $\frac{Q(X)}{X - \alpha_i}$. En multipliant la relation (1) par $X - \alpha_i$, puis en évaluant en α_i, on obtient alors $\beta_i = \frac{P(\alpha_i)}{Q'(\alpha_i)}$ (ce qui a bien un sens puisque α_i est une racine simple de Q, donc $Q'(\alpha_i) \neq 0$). Comme P et Q sont à coefficients dans $\mathbb{Q}$, on a $\beta_i \in \mathbb{K}$. Enfin P et Q sont premiers entre eux, donc n'ont aucune racine commune d'où $P(\alpha_i) \neq 0$ et $\beta_i \neq 0$.

2. La décomposition en éléments simples (qu'on peut calculer en utilisant la question précédente) est
$$\frac{X}{X^2 - 3} = \frac{1/2}{X - \sqrt{3}} + \frac{1/2}{X + \sqrt{3}}$$
et on a $\mathbb{K} = \mathbb{Q}(\sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}$; ceci donne la primitive
$$\frac{1}{2} \ln(X - \sqrt{3}) + \frac{1}{2} \ln(X + \sqrt{3}).$$
Les deux coefficients β_1 et β_2 sont égaux, donc on peut regrouper les deux termes ce qui donne pour primitive
$$\frac{1}{2} \ln\Big((X - \sqrt{3})(X + \sqrt{3})\Big) = \frac{1}{2} \ln(X^2 - 3)$$
et on a $\mathbb{K}_0 = \mathbb{Q}(1/2) = \mathbb{Q}$.

3. Pour commencer, traitons le cas particulier où $P = cQ'$ pour un certain $c \in \mathbb{C}$ (qui est nécessairement rationnel, et non nul), car ce cas particulier fait exception à la preuve suivante. Dans ce cas on a $R(Y) = \mathrm{Res}(Q(X), (c - Y)Q'(X)) = (c - Y)^d \mathrm{Res}(Q(X), Q'(X))$ avec $\mathrm{Res}(Q(X), Q'(X)) \neq 0$ puisque Q est à racines simples. Donc c est l'unique racine de R. Par ailleurs dans ce cas particulier on a $P/Q = cQ'/Q$ donc la primitive de la relation (4) est simplement $c \ln(Q(X))$ ce qui donne $r = 1$, $c_1 = c$ et $P_1 = Q$: l'unique racine de R est bien c_1.

   Supposons dorénavant que P n'est pas de la forme cQ', et montrons d'abord que tous les c_j sont des racines de R. Soit $j \in \{1, \dots, r\}$; il existe $i \in \{1, \dots, d\}$ tel que $c_j = \beta_i$. D'après la question 1 on a $P(\alpha_i) - c_j Q'(\alpha_i) = 0$, donc α_i est une racine du polynôme $P(X) - c_j Q'(X) \in \mathbb{K}[X]$. Comme α_i est aussi une racine de Q, les polynômes Q et $P - c_j Q'$ ont une racine commune dans $\mathbb{K}$. Cela montre que leur résultant est nul. Or ce résultant est nul, si et seulement si, $R(c_j) = 0$: en effet, l'application de spécialisation $\varphi : \mathbb{Q}[Y] \to \mathbb{K}$ définie par $\varphi(S(Y)) = S(c_j)$ envoie le polynôme $Q(X)$ sur un polynôme de même degré (à savoir $Q(X)$ lui-même, puisque $Q(X)$ ne dépend pas de Y), et on a

$P - c_j Q' \neq 0$ (sinon on est dans le cas particulier traité préalablement). Donc c_j est bien une racine de R.

Réciproquement, soit c une racine complexe de R. Le même argument de spécialisation montre que le résultant de Q et $P - cQ'$ est nul. Ces polynômes ont donc une racine commune dans $\mathbb{C}$, puisque Q est scindé sur $\mathbb{C}$ (on pourrait faire le même raisonnement en restant dans l'extension finie $\mathbb{K}$). Cette racine est l'un des α_i, et on a donc $P(\alpha_i) - cQ'(\alpha_i) = 0$ ce qui donne $c = \frac{P(\alpha_i)}{Q'(\alpha_i)} = \beta_i$ d'après la question 1 : c est bien l'un des c_j.

Une autre méthode (plus efficace) est la suivante. Il est clair que R est aussi le résultant de $Q(X)$ et $P(X) - YQ'(X)$ vus dans $(\mathbb{C}[Y])[X]$. Or Q est unitaire et scindé sur $\mathbb{C}$, donc sur $\mathbb{C}[Y]$, avec pour racines $\alpha_1, \ldots, \alpha_d$. On a donc $R(Y) = \prod_{i=1}^{d}(P(\alpha_i) - YQ'(\alpha_i))$: ses racines complexes sont exactement les $y \in \mathbb{C}$ pour lesquels il existe i tel que $P(\alpha_i) = yQ'(\alpha_i)$. Ce sont bien les c_j.

4. Les polynômes P_j et $\operatorname{pgcd}(Q, P - c_j Q')$ sont unitaires, scindés et à racines simples sur $\mathbb{K}$ (car Q l'est), donc pour montrer qu'ils sont égaux il suffit de montrer qu'ils ont les mêmes racines. Tout d'abord, soit α une racine de P_j : il existe $i \in \{1, \ldots, d\}$ tel que $c_j = \beta_i$ et $\alpha = \alpha_i$. Alors $P(\alpha_i) - c_j Q'(\alpha_i) = 0$ d'après la question 1, donc α est bien une racine commune de Q et $P - c_j Q'$. Réciproquement, si α est une racine commune de Q et $P - c_j Q'$ alors α est l'un des α_i, et la relation $P(\alpha_i) - c_j Q'(\alpha_i) = 0$ montre que $c_j = \beta_i$, donc α est bien une racine de P_j.
5. Comme Q et $P - c_j Q'$ sont à coefficients dans $\mathbb{K}_0$, leur pgcd aussi. Le coût du calcul de Q' à partir de Q (dont on connaît les coefficients) est $O(d)$: une multiplication par coefficient. Ensuite on a $\deg Q = d$ et $\deg(P - c_j Q') \leq d - 1$ donc le coût du calcul de P_j par l'algorithme d'Euclide est $O(d(d-1)) = O(d^2)$ opérations arithmétiques dans $\mathbb{K}_0$.
6. ($\star$) On obtient
$$\frac{P}{Q} = 9\frac{P_1'}{P_1} - \frac{15}{2}\frac{P_2'}{P_2} - 5\frac{P_3'}{P_3}$$
avec $P_1 = X^7 + X + 1$n $P_2 = X^2 - 2$ et $P_3 = X + 1$.
7. ($\star$) On en déduit qu'une primitive est donnée (sur tout intervalle où elle est bien définie) par
$$X \longmapsto 9\ln\left(X^7 + X + 1\right) - \frac{15}{2}\ln\left(X^2 - 2\right) - 5\ln(X + 1).$$

Problème 2

1. Comme $a_0 = 1$, on a $u_n = u_{n+d} + \sum_{i=1}^{d-1} a_i u_{n-1}$ (on rappelle que $1 = -1$ puisqu'on travaille dans $\mathbb{F}_2$) ce qui permet de calculer u_n à partir de u_{n+1}, u_{n+2}, $\ldots$, u_{n+d}. Par ailleurs il y a une infinité d'entiers $i \geq 0$, alors que le vecteur $V_i \in \mathbb{F}_2^d$ ne peut prendre qu'un nombre fini de valeurs, donc il existe i et j, avec $i \neq j$, tels que $V_i = V_j$. Quitte à permuter i et j, on peut supposer $j > i$. On obtient alors par une récurrence immédiate que $V_n = V_{n+j-i}$ pour tout $n \geq i$. On démontre ensuite que cette propriété est encore vraie pour tout n compris entre 0 et i en procédant par récurrence descendante : on exprime chaque u_n à partir de u_{n+1}, u_{n+2}, $\ldots$, u_{n+d} (ce qui revient à utiliser le fait que la matrice M est inversible, puisque 0 n'est pas racine de son polynôme caractéristique qui est P).

2. Si $a_0 = P(0) = 0$, la suite définie par $u_0 = 1$ et $u_n = 0$ pour tout $n \geq 1$ vérifie la relation de récurrence (5) mais n'est pas périodique.
3. ($\star$) On conjecture que $p = 7$.
4. Par définition de p on a $V_p = V_0$. Si il existait un entier k tel que $1 \leq k < p$ et $V_k = V_0$, une récurrence immédiate montre qu'on aurait $u_{n+k} = u_n$ pour tout $n \geq 0$ (ce serait vrai pour $0 \leq n \leq d-1$ par hypothèse, et ensuite on utilise la relation de récurrence satisfaite par (u_n)). Cela contredirait la minimalité de p.
5. Supposons qu'il existe i, j tels que $0 \leq i < j \leq p-1$ tels que $V_i = V_j$. Alors comme à la question 1 on montre que $j - i$ est une période de la suite (u_n). Comme $0 < j - i < p$, cela contredit la définition de p. Donc les V_i, pour $0 \leq i \leq p-1$, sont des éléments deux à deux distincts de l'ensemble $\mathbb{F}_2^d \setminus \{0\}$ qui est de cardinal $2^d - 1$, ce qui donne $p \leq 2^d - 1$.
6. On part de V_0, et pour tout entier $k \geq 1$ on calcule V_k à partir de V_{k-1}. La formule $V_k = MV_{k-1}$ pourrait laisser croire que $O(d^2)$ opérations arithmétiques dans $\mathbb{F}_2$ sont nécessaires pour chaque valeur de k, mais ce n'est pas le cas puisque la plupart des coefficients de M sont nuls. En fait le seul calcul à faire est celui de u_{k+d-1} à partir des d termes précédents, en utilisant la relation (5). Ce calcul coûte $O(d)$ opérations arithmétiques dans $\mathbb{F}_2$ pour chaque valeur de k. On s'arrête dès que $V_k = V_0$, et alors on a $p = k$. Le coût du test pour savoir si $V_k = V_0$ est considéré comme négligeable, puisqu'on compte seulement les opérations arithmétiques. Finalement le coût est de $O(pd)$ opérations arithmétiques dans $\mathbb{F}_2$, ce qui montre que cet algorithme est plus rapide quand p est petit. Mais comme on ne connaît pas p a priori, et que l'énoncé demande une estimation en fonction de d seulement, on utilise la majoration $p \leq 2^d - 1$ de la question précédente pour montrer que le coût est en $O(d \cdot 2^d)$ opérations arithmétiques dans $\mathbb{F}_2$.
7. ($\star$)
8. Par une récurrence immédiate on voit que $V_n = M^n V_0$ pour tout $n \geq 0$. La question 4 montre donc que p est le plus petit entier $k \geq 1$ tel que $M^k V_0 = V_0$. Comme $V_0 \neq 0$ (puisque la suite (u_n) n'est pas identiquement nulle), p est le plus petit entier $k \geq 1$ tel que V_0 soit un vecteur propre de M^k associé à la valeur propre 1.
9. (a) Comme P est irréductible de degré d, on a $[\mathbb{K} : \mathbb{F}_2] = d$ et $\operatorname{Card} \mathbb{K} = 2^d$. Le corps de rupture $\mathbb{K}$ est aussi un corps de décomposition de P : le polynôme P est scindé sur $\mathbb{K}$. Comme $\mathbb{K}$ est un corps fini (donc parfait), P est séparable car il est irréductible.
   (b) Soient x_1 et x_2 deux racines de P dans $\mathbb{K}$. Notons φ le morphisme de Frobenius relatif à $\mathbb{F}_2$, défini par $\varphi(y) = y^2$. Alors il existe un entier $i \leq d-1$ tel que $x_2 = \varphi^i(x_1)$. En notant ω l'ordre de x_1 dans le groupe multiplicatif $\mathbb{K}^*$, la relation $x_1^\omega = 1$ donne $x_2^\omega = 1$ quand on applique i fois le morphisme de corps φ. Cela montre que l'ordre de x_2 divise celui de x_1. Comme x_1 et x_2 jouent des rôles symétriques, on en déduit qu'ils ont le même ordre ω.
   (c) On sait que P est le polynôme caractéristique de M, et que P est scindé à racines simples sur $\mathbb{K}$. Donc M est diagonalisable sur $\mathbb{K}$, et pour tout k les valeurs propres de M^k sont exactement les puissances k-ièmes des valeurs propres de M. Comme toutes les racines de P sont d'ordre ω dans le groupe multiplicatif $\mathbb{K}^*$, on en déduit que les entiers k tels que 1 soit valeur propre de M sont exactement les multiples de ω. Or la question 8 montre que 1 est valeur propre de M^p, donc ω divise p. Par ailleurs

M^ω est la matrice identité, donc la question 8 montre que $p \leq \omega$. Finalement, on a donc $p = \omega$.

10. Soit $d \geq 1$. Il existe un corps $\mathbb{K}$ de cardinal 2^d ; c'est une extension de $\mathbb{F}_2$. Notons x un générateur du groupe cyclique $\mathbb{K}^*$; on a alors $\mathbb{K} = \mathbb{F}_2(x)$. Notons P le polynôme minimal de x sur $\mathbb{F}_2$. Alors P est un polynôme de degré d à coefficients dans $\mathbb{F}_2$, irréductible, et une de ses racines dans $\mathbb{K}$ est d'ordre $\operatorname{Card} \mathbb{K}^* = 2^d - 1$. D'après la question précédente, les suites non identiquement nulles vérifiant (5) sont de période $p = 2^d - 1$.
11. Si $d = 1$, le résultat est évident. Sinon la suite (u_n) est de période $p = 2^d - 1 > 1$ donc (u_n) n'est pas identiquement nulle. D'après la question 8 le vecteur V_0 est un vecteur propre de la matrice M^p. Pour tout entier $k \geq 1$ le vecteur V_k est aussi un vecteur propre de cette matrice, en appliquant la question 8 à la suite décalée $(u_{n+k})_{n\geq 0}$. Or tout vecteur non nul $\mathbb{F}_2^d$ s'écrit sous la forme V_k d'après la question 5 (puisque $p = 2^d - 1$), donc M^p est la matrice identité. Le polynôme $X^p - 1$ est un polynôme annulateur de M, et il est scindé à racines simples sur $\mathbb{F}_{2^d}$ (ses racines sont les $2^d - 1$ éléments non nuls de $\mathbb{F}_{2^d}$). Donc M est diagonalisable sur $\mathbb{F}_{2^d}$, et ses valeurs propres figurent parmi les racines de ce polynôme. Soit x une valeur propre de M dans $\mathbb{F}_{2^d}$, c'est-à-dire une racine de P. Notons ω l'ordre de x dans le groupe multiplicatif $\mathbb{F}_{2^d}^*$; on a $\omega \leq \operatorname{Card}\mathbb{F}_{2^d}^* = p$. Alors $1 = x^\omega$ est valeur propre de M^ω, et $1 \in \mathbb{F}_2$ donc il existe un vecteur propre $V \in \mathbb{F}_2^d$ associé. On a $V = V_k$ pour un certain k, et d'après la question 8 la période de la suite décalée $(u_{n+k})_{n\geq 0}$ est inférieure ou égale à ω. Comme cette période est p, on a finalement $\omega = p$: il existe un générateur x du groupe $\mathbb{F}_{2^d}^*$ tel que $P(x) = 0$. Notons Q le polynôme minimal de x sur $\mathbb{F}_2$. Alors P et Q sont unitaires, Q divise P, et $\deg Q = [\mathbb{F}_2(x) : \mathbb{F}_2] = [\mathbb{F}_{2^d} : \mathbb{F}_2] = d = \deg P$ donc $P = Q$. Cela prouve que P est irréductible et possède une racine d'ordre $2^d - 1$ dans une extension de $\mathbb{F}_2$.
12. ($\star$) Il suffit de tester si P est irréductible, et si c'est le cas si ses racines sont d'ordre $2^d - 1$ dans $\mathbb{F}_{2^d}$.
13. Les vecteurs $V_0, \ldots, V_{p-1}$ sont deux à deux distincts et appartiennent à $\mathbb{F}_2^d \setminus \{0\}$. Si $p = 2^d - 1$, il y a autant de V_i que d'éléments dans $\mathbb{F}_2^d \setminus \{0\}$ donc chaque élément est obtenu une et une seule fois. Autrement dit, chaque mot de longueur d formé avec les lettres 0 et 1, sauf le mot nul formé uniquement de 0, apparaît une et une seule fois à l'intérieur du long mot formé par les lettres $u_0, \ldots, u_{2^d-2}$. Comme il y a 2^{d-1} tels mots qui commencent par un 1, et $2^{d-1} - 1$ qui commencent par un 0, on en déduit que parmi les $2^d - 1$ éléments $u_0, \ldots, u_{2^d-2}$ il y en a 2^{d-1} qui valent 1, et $2^{d-1} - 1$ qui valent 0. C'est une répartition presque parfaite (en fait trop parfaite pour une suite aléatoire !). La corrélation entre termes consécutifs ressemble aussi à celle d'une suite aléatoire : par exemple il y a autant de suites 01, 10 et 11 dans le long mot formé par $u_0, \ldots, u_{2^d-2}$, et juste une suite 00 de moins (à condition que $d \geq 2$). Toutes ces propriétés sont particulièrement bien vérifiées si on prend exactement une période ; pour obtenir une suite de 1000 bits on peut prendre $d = 10$ ce qui donne $p = 1023$, et omettre les 23 derniers termes. Il est à noter que le choix des d termes initiaux de la suite n'importe pas vraiment (sauf bien sûr qu'ils ne doivent pas être tous nuls). Pour obtenir un polynôme qui vérifie les conditions de la question précédente, on peut procéder par exemple en tirant un polynôme de degré d aléatoirement jusqu'à en trouver un qui vérifie la condition.
14. On peut choisir aléatoirement un polynôme P et plusieurs conditions initiales, et faire calculer par `Sage` les périodes des suites associées, jusqu'à trouver un contre-exemple.

On peut aussi considérer des polynômes P qui sont "très loin" d'être irréductibles avec des racines de grand ordre : considérons P tel que $P(1) = 0$. Alors 1 est valeur propre de M ; notons V un vecteur propre associé. Si $V_0 = V$ alors la question 8 montre que la période vaut 1 : la suite (u_n) est constante. En revanche, si $d \geq 2$ la matrice M n'est pas l'identité, donc il existe aussi V' tel que $MV' \neq V'$. Si $V_0 = V'$ alors la question 8 montre que la période ne vaut pas 1. Donc pour un tel polynôme, les suites (u_n) vérifiant (5) n'ont pas toutes la même période.