 

# Examen de M.A.O. Calcul Formel  Durée : 3 heures

14 juin 2021
Master 1 M.F., Orsay

Les deux problèmes sont indépendants et peuvent être abordés dans un ordre quelconque. Il est autorisé d'admettre le résultat de certaines questions pour traiter les suivantes. Lorsqu'on évoquera le coût d'un algorithme, il s'agira toujours de son coût en nombre d'opérations arithmétiques et on attendra toujours une réponse de la forme $O(\ldots)$ : déterminer la constante implicite dans le symbole $O(\ldots)$ n'est pas demandé.

**Problème 1**

Soient $P$ et $Q$ deux polynômes à coefficients dans $\mathbb{Q}$. On suppose que $Q$ est non constant, unitaire et séparable. On pose $d = \deg Q$ et on note $\alpha_1, \ldots, \alpha_d$ les racines complexes de $Q$ (qui sont donc simples), si bien que $Q(X) = \prod_{i=1}^{d}(X - \alpha_i)$. On suppose aussi $\deg P < d$ et $\operatorname{pgcd}(P, Q) = 1$. Il existe alors un unique développement en éléments simples de la fraction rationnelle $P/Q$, qui s'écrit

$$\frac{P(X)}{Q(X)} = \sum_{i=1}^{d} \frac{\beta_i}{X - \alpha_i} \quad \text{avec } \beta_1, \ldots, \beta_d \in \mathbb{C}. \tag{1}$$

On note $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ le sous-corps de $\mathbb{C}$ engendré sur $\mathbb{Q}$ par $\alpha_1, \ldots, \alpha_d$ ; il s'agit d'un corps de décomposition de $Q$ sur $\mathbb{Q}$.

1. Démontrer les propriétés suivantes pour tout $i \in \{1, \ldots, d\}$ :
   - La valeur en $\alpha_i$ de la fraction rationnelle $\frac{Q(X)}{X - \alpha_i}$ est $Q'(\alpha_i)$.
   - On a
   $$\beta_i = \frac{P(\alpha_i)}{Q'(\alpha_i)}$$
   - Le nombre complexe $\beta_i$ appartient à $\mathbb{K}$ et est non nul.

Dans la formule (1) il peut arriver que certains coefficients $\beta_i$ soient égaux ; on peut alors regrouper les termes correspondants et on obtient

$$\frac{P(X)}{Q(X)} = \sum_{j=1}^{r} c_j \frac{P_j'(X)}{P_j(X)} \text{ avec } 1 \leq r \leq d,\ c_1, \ldots, c_r \in \mathbb{K},\ \text{ et }\ P_1, \ldots, P_r \in \mathbb{K}[X] \text{ unitaires.} \tag{2}$$

Précisément, on a $\{c_1, \ldots, c_r\} = \{\beta_1, \ldots, \beta_d\}$ avec $c_1, \ldots, c_r$ deux à deux distincts, et pour tout $j$ tel que $1 \leq j \leq r$ on a

$$P_j(X) = \prod_{\substack{1 \leq i \leq d \\ \beta_i = c_j}} (X - \alpha_i).$$

Notons $\mathbb{K}_0 = \mathbb{Q}(c_1, \ldots, c_r)$ le sous-corps de $\mathbb{C}$ engendré sur $\mathbb{Q}$ par $c_1$, …, $c_r$. Le but de ce problème est de calculer le développement (2) directement, en faisant seulement des calculs dans $\mathbb{K}_0$, alors que si on le déduit de (1) on doit travailler dans $\mathbb{K}$ (qui peut être beaucoup plus grand).

2. En considérant l'exemple où $P(X) = X$ et $Q(X) = X^2 - 3$, montrer qu'on peut avoir $\mathbb{K}_0 = \mathbb{Q}$ et $\mathbb{K} \neq \mathbb{Q}$ ; on explicitera les formules (1) et (2) dans ce cas. *Il est demandé de présenter une réponse complète à cette question sur la copie. Les calculs à mener sont suffisamment simples pour être menés sans utiliser d'ordinateur, même si évidemment ce n'est pas interdit tant que la copie contient une réponse complète.*

On note alors $R(Y) \in \mathbb{Q}[Y]$ le résultant des polynômes $Q(X)$ et $P(X) - YQ'(X)$, vus dans $(\mathbb{Q}[Y])[X]$ (c'est-à-dire comme des polynômes en $X$ à coefficients dans $\mathbb{Q}[Y]$).

3. Démontrer que $c_1$, …, $c_r$ sont exactement les racines complexes (deux à deux distinctes) de $R$. *On ne demande pas d'étudier si ce sont des racines simples ou multiples.*
4. Démontrer que pour tout $j \in \{1, \ldots, r\}$ on a
$$P_j = \operatorname{pgcd}(Q, P - c_j Q').$$
5. En déduire que les polynômes $P_j$ sont à coefficients dans $\mathbb{K}_0$. Si on fixe un entier $j$ et qu'on suppose $c_j$ connu, quel est le coût du calcul de $P_j$ (en opérations arithmétiques dans $\mathbb{K}_0$) ?
6. ($\star$) En appliquant la méthode décrite dans ce problème, développer sous la forme (2) la fraction rationnelle
$$\frac{43X^9 + 48X^8 - 116X^7 - 126X^6 - 11X^3 - 26X^2 - 23X - 8}{(X^2 - 2)(X + 1)(X^7 + X + 1)}.$$
*On inscrira le développement trouvé sur la copie, et on détaillera les différentes étapes dans la feuille de calcul* `Sage`. *Il n'est pas demandé de programmer une fonction qui traite le cas où $P$ et $Q$ sont quelconques.*
7. ($\star$) En déduire une primitive de la fraction rationnelle en question 6. Vérifiez avec `Sage` votre résultat.

**Problème 2**

Dans ce problème on fixe un entier $d \geq 1$ et un polynôme de degré $d$ à coefficients dans $\mathbb{F}_2$, de coefficient constant non nul, noté
$$P(X) = X^d + \sum_{i=0}^{d-1} a_i X^i \in \mathbb{F}_2[X], \qquad \text{avec } a_0 = 1.$$
On se donne une suite $(u_n)_{n \geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ d'éléments de $\mathbb{F}_2$, vérifiant
$$u_{n+d} = \sum_{i=0}^{d-1} a_i u_{n+i} \text{ pour tout } n \geq 0. \tag{3}$$

On considère la matrice compagnon

$$M = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{d-1} \end{bmatrix}.$$

On pourra utiliser sans démonstration le fait que $P(X) = X^d + \sum_{i=0}^{d-1} a_i X^i$ est le polynôme caractéristique de $M$. En notant

$$V_n = \begin{bmatrix} u_n \\ \vdots \\ u_{n+d-1} \end{bmatrix},$$

la relation de récurrence (3) s'écrit sous la forme :

$$V_{n+1} = MV_n \text{ pour tout } n \geq 0.$$

1. Démontrer les propriétés suivantes :
   - La relation (3) permet de calculer $u_n$ à partir de $u_{n+1}$, $u_{n+2}$, …, $u_{n+d}$.
   - Il existe deux entiers $i$ et $j$, avec $i \neq j$, tels que $V_i = V_j$.
   - La suite $(u_n)_{n\geq 0}$ est périodique, c'est-à-dire qu'il existe un entier $p \geq 1$ tel que pour tout $n \in \mathbb{N}$ on ait $u_{n+p} = u_n$.
2. Montrer que si on autorisait le coefficient constant $a_0 = P(0)$ à être nul, il existerait des suites $(u_n)_{n\geq 0}$ non périodiques vérifiant la relation de récurrence (3). *C'est pourquoi on supposera toujours* $a_0 = 1$.

*Dans toute la suite de ce problème on note $p$ la période de la suite $(u_n)_{n\geq 0}$, qui est le plus petit entier $k \geq 1$ tel que pour tout $n \in \mathbb{N}$ on ait $u_{n+k} = u_n$.*

3. ($\star$) Dans cette question seulement, on étudie l'exemple suivant :

   $$d = 3, \quad P(X) = X^3 + X + 1, \quad u_0 = u_1 = u_2 = 1.$$

   Faire afficher par `Sage` la valeur de $u_n$ pour $0 \leq n \leq 30$, et conjecturer la valeur de $p$. Afficher aussi les vecteurs $V_n$ pour $0 \leq n \leq 10$.
4. Montrer que $p$ est le plus petit entier $k \geq 1$ tel qu'on ait : $V_k = V_0$.
5. Démontrer que $V_0$, $V_1$, …, $V_{p-1}$ sont deux à deux distincts, et en déduire que $p \leq 2^d - 1$.
6. Déduire des questions précédentes un algorithme qui prend en entrée le polynôme $P$ et les premiers termes $u_0$, …, $u_{d-1}$, et détermine la période $p$ ; calculer le coût de cet algorithme en nombre d'opérations arithmétiques dans $\mathbb{F}_2$. *La réponse attendue est de la forme $O(\dots)$ où la quantité … dépend seulement de $d$, et pas de $p$.*

7. (⋆) Implémenter l'algorithme précédent en une fonction `Sage` qui prend en entrée le polynôme $P$ et les premiers termes $u_0, \ldots, u_{d-1}$, et renvoie la période $p$. Appliquer cette fonction à la suite de la question 3, et en déduire une preuve de la conjecture émise à cette question.
8. Démontrer que si la suite $(u_n)_{n\geq 0}$ n'est pas identiquement nulle, alors $p$ 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. Dans cette question on suppose $P$ irréductible dans $\mathbb{F}_2[X]$ et on considère un corps de rupture $\mathbb{K}$ de $P$ sur $\mathbb{F}_2$.
   (*a*) Rappeler combien valent $[\mathbb{K} : \mathbb{F}_2]$ et $\operatorname{Card} \mathbb{K}$ ; le polynôme $P$ est-il scindé sur $\mathbb{K}$ ? Est-il séparable ?
   (*b*) Démontrer que toutes les racines de $P$ dans $\mathbb{K}$ ont le même ordre dans le groupe multiplicatif $\mathbb{K}^*$, noté $\omega$.
   (*c*) Déduire des questions précédentes (et de la question 8) que si $P$ est irréductible et si la suite $(u_n)_{n\geq 0}$ n'est pas identiquement nulle, alors $p = \omega$ (où $\omega$ a été défini à la question précédente).
10. En utilisant la question précédente, démontrer que pour tout $d \geq 1$ il existe un polynôme $P$ tel que les suites non identiquement nulles vérifiant (3) soient de période $p = 2^d - 1$.
11. Réciproquement, démontrer que si il existe une suite $(u_n)$ vérifiant (3) qui est de période $p = 2^d - 1$, alors $P$ est irréductible et possède une racine d'ordre $2^d - 1$ dans une extension de $\mathbb{F}_2$.
12. Expliquer pourquoi les suites vérifiant (3) et ayant une période $p = 2^d - 1$ peuvent être utilisées pour simuler des suites aléatoires. Quelle valeur de $d$ choisiriez-vous pour constuire une suite pseudo-aléatoire de 1000 éléments de $\mathbb{F}_2$ ?
13. (⋆) En utilisant les questions précédentes, programmer une fonction `Sage` qui prend en entrée un polynôme $P$ et renvoie `True` si les suites non identiquement nulles vérifiant (3) sont de période $p = 2^d - 1$, et `False` sinon. *Il est autorisé d'utiliser n'importe quelle fonction de* `Sage`. Tester cette fonction sur le polynôme $P$ de la question 3.
14. (⋆) En utilisant la fonction de la question précédente, programmer une fonction `Sage` qui prend en entrée un entier $d \geq 1$, et affiche une suite pseudo-aléatoire de $2^d - 1$ éléments de $\mathbb{F}_2$.
15. Donner un exemple de polynôme $P$ pour lequel les suites $(u_n)$ vérifiant (3) n'ont pas toutes la même période. *On pourra résoudre cette question, au choix, par un argument théorique ou par un exemple trouvé et/ou justifié par* `Sage`. *Dans le deuxième cas, on devra impérativement écrire sur la copie le polynôme $P$, les premiers termes $u_0, \ldots, u_{d-1}$ de deux suites, et leurs périodes respectives.*