15 juin 2022
Master 1 M.F., Orsay

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

L'examen est constitué d'un exercice et d'un problème, qui sont indépendants.
Il est autorisé d'admettre le résultat de certaines questions pour traiter les suivantes.
Dans ce sujet plusieurs questions nécessitent à la fois un calcul (à effectuer en `Sage`) et des justifications mathématiques. On veillera bien à écrire sur la copie tous les détails nécessaires, y compris les résultats fournis par `Sage` et l'interprétation qu'on peut en faire.
Lorsqu'on évoque le coût d'un algorithme, on attend toujours une réponse de la forme $O(\ldots)$: déterminer la constante implicite dans le symbole $O(\ldots)$ n'est pas demandé.

Exercice : Ombre portée par un ruban

Dans cet exercice on cherche à déterminer l'ombre portée sur le sol par un ruban suspendu en l'air. On repère un point de l'espace par ses coordonnées $(x, y, z) \in \mathbb{R}^3$, avec $z \geq 0$; le sol est défini par $z = 0$. On suppose que le ruban a pour équation

$$\begin{cases} (x-2)^2 + (y-1)^2 + (z-10)^2 = 50 \\ (x+5)^2 + (y+2)^2 + (z-8)^2 = 30 \end{cases}$$

et que le soleil est situé à l'infini dans la direction du vecteur $(1, 2, 1)$. L'ombre portée sur le sol par le ruban est l'ensemble des points $(x, y, 0)$ du sol pour lesquels le rayon lumineux provenant du soleil et qui aurait pu éclairer ce point est arrêté par le ruban.

1. *Dans cettte question on mènera les calculs avec* `Sage` *et on les expliquera sur la copie.* Démontrer qu'un point de coordonnées $(x, y, 0)$, avec $x, y \in \mathbb{R}$, est dans l'ombre portée par le ruban si et seulement si il existe $t \in \mathbb{R}$ tel que $P(t) = Q(t) = 0$, avec

   $$P(T) = 6T^2 + (2x + 4y - 28)T + x^2 + y^2 - 4x - 2y + 55$$

   et

   $$Q(T) = 6T^2 + (2x + 4y + 2)T + x^2 + y^2 + 10x + 4y + 63.$$

2. En considérant le polynôme $P(T) - Q(T)$, montrer que la question 1 reste vraie si on remplace "il existe $t \in \mathbb{R}$" par "il existe $t \in \mathbb{C}$".
3. En utilisant le résultant et en justifiant précisément, montrer comment obtenir un polynôme $R \in \mathbb{Q}[X, Y]$ tel que l'ombre portée par le ruban soit l'ensemble des points de coordonnées $(x, y, 0)$ avec $x, y \in \mathbb{R}$ tels que $R(x, y) = 0$.
4. $(\star)$ Calculer le polynôme R de la question précédente, et écrire sur la copie la valeur de $R(0, 0)$.

Problème

Dans ce problème, chacune des 4 parties utilise les précédentes, sauf la partie 3 qui est indépendante des parties 1 et 2 et qui porte sur des notions différentes.

Partie 1 : Erreurs en rafale

Etant donné un message envoyé $c \in \mathbb{F}_2^n$, le message reçu $r \in \mathbb{F}_2^n$ peut être différent de c. On note alors $e = r - c = (e_0, \ldots, e_{n-1}) \in \mathbb{F}_2^n$ l'erreur. On dit qu'il s'agit de t *erreurs en rafale*, et on note $r(e) = t$, si t est le plus petit entier pour lequel les bits non nuls de e figurent parmi t positions consécutives lorsqu'on prolonge e par périodicité, en posant $e_n = e_0$, $e_{n+1} = e_1$, ...

Dans toute la suite du problème on adopte la définition précise suivante. Etant donné $e = (e_0, \ldots, e_{n-1}) \in \mathbb{F}_2^n$, on pose $e_{n+i} = e_i$ pour tout $i \in [\![0, n-1]\!]$, et pour tout $j \in [\![0, n-1]\!]$ on note :

$$\ell_e(j) = \min\{k \in [\![0, n]\!],\ e_{j+k} = e_{j+k+1} = \ldots = e_{j+n-1} = 0\}$$

de telle sorte que si $e_{j+n-1} = 1$, l'ensemble à droite est le singleton $\{n\}$ (puisque pour $k = n$ la condition $e_{j+k} = e_{j+k+1} = \ldots = e_{j+n-1} = 0$ est vide, donc vraie) si bien que $\ell_e(j) = n$ dans ce cas ; on a $\ell_e(j) \leq n-1$ si $e_{j+n-1} = 0$.

On définit alors une application $r : \mathbb{F}_2^n \to \mathbb{N}$ en posant :

$$r(e) = \min\{\ell_e(j),\ j \in [\![0, n-1]\!]\}.$$

Dans les exemples concrets, on notera $e \in \mathbb{F}_2^n$ comme une succession de 0 et de 1, par exemple $e = 010$ pour $(0, 1, 0) \in \mathbb{F}_2^3$.

1. En exhibant à chaque fois une valeur convenable de j, démontrer que $r(00101100100) \leq 7$ et $r(11000001010) \leq 6$. *On vérifiera plus tard, à la question 6, que ces deux majorations sont en fait des égalités.*
2. Déterminer le(s) $e \in \mathbb{F}_2^n$ tel(s) que $r(e) = 0$, puis celui/ceux tel(s) que $r(e) = n$.
3. Proposer un algorithme (même peu efficace) qui à partir de $e \in \mathbb{F}_2^n$ permet de calculer $r(e)$; calculer son coût en nombre d'accès au vecteur e. *Autrement dit, il s'agit de compter le nombre de fois où l'algorithme évalue e_i avec $i \in \mathbb{N}$; comme toujours la réponse attendue est de la forme $O(\ldots)$, où les points de suspension doivent être une fonction explicite de n.*
4. En fonction de n, quel serait le coût minimal imaginable en nombre d'accès au vecteur e, à constante multiplicative près, pour un algorithme qui calcule $r(e)$ à partir de e ? Proposer un algorithme qui ait ce coût, à constante multiplicative près.
5. ($\star$) Implémenter une fonction `Sage` qui prend en entrée un vecteur $e \in \mathbb{F}_2^n$ (qui pourra être vu, au choix, comme une liste ou comme un vecteur ligne), et renvoie $r(e)$; on pourra utiliser un algorithme quelconque, même peu efficace.
6. ($\star$) En utilisant la fonction de la question précédente, démontrer que les majorations de la question 1 sont des égalités.
7. ($\star$) Dans cette question seulement on pose $n = 130$, $e_0 = 0$, et pour tout $i \in [\![1, 129]\!]$ on prend $e_i = 1$ si i est une puissance de 2 ou une puissance de 3, et $e_i = 0$ sinon. En utilisant la fonction de la question 5, calculer $r(e)$.

Partie 2 : Détection et correction d'erreurs en rafale

Dans cette partie on considère un code linéaire C de longueur n et de dimension $k \geq 1$. On rappelle qu'il s'agit d'un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension k. Etant donné un entier $t \geq 1$, on dit que C *détecte t erreurs en rafale* si pour tout $c \in C \setminus \{0\}$ on a $r(c) > t$, où la fonction $r : \mathbb{F}_2^n \to \mathbb{N}$ a été définie dans la partie 1.

On dit aussi que C *corrige t erreurs en rafale* si pour tous $e_1, e_2 \in \mathbb{F}_2^n$ tels que $r(e_1) \leq t$, $r(e_2) \leq t$ et $e_1 + e_2 \in C$, on a $e_1 + e_2 = 0$.

8. Justifier brièvement pourquoi ces définitions signifient qu'en utilisant le code C, on peut détecter (respectivement corriger) t erreurs en rafale.
9. Démontrer que si le code C détecte t erreurs en rafale, alors C est en somme directe avec $\mathbb{F}_2^t \times \{0\}^{n-t}$, et en déduire que $t \leq n - k$; on note ici $\mathbb{F}_2^t \times \{0\}^{n-t}$ l'ensemble des $e = (e_0, \ldots, e_{n-1}) \in \mathbb{F}_2^n$ tels que $e_t = e_{t+1} = \ldots = e_{n-1} = 0$.
10. Démontrer que si le code C est cyclique, alors il détecte $n - k$ erreurs en rafale.
11. Proposer un exemple de situation pratique où il est plausible que les erreurs se produisent en rafale, c'est-à-dire qu'avec un entier t relativement grand, la probabilité d'avoir t erreurs en rafale soit assez grande, alors que la probabilité d'avoir t erreurs réparties aléatoirement est très faible.
12. Démontrer que si le code C corrige t erreurs en rafale, alors $t \leq \lfloor \frac{n-k}{2} \rfloor$.
13. Comparer les résultats des questions 9 et 12 à des propriétés analogues vues en cours ; quel peut être l'intérêt d'utiliser un code cyclique dans une situation comme celle de la question 11 ?

Partie 3 : Intermède sur les diviseurs de $X^n - 1$ dans $\mathbb{F}_q[X]$

Cette partie est indépendante des deux précédentes. On note p un nombre premier, $\alpha \geq 1$ un entier, $q = p^\alpha$, et $\mathbb{F}_q$ un corps de cardinal q. On considère un polynôme $S \in \mathbb{F}_q[X]$ tel que $S(0) \neq 0$. *On pensera à raisonner dans $\mathbb{F}_q[X]/(S)$.*

14. Démontrer qu'il existe un unique entier $n_S \geq 1$ tel que pour tout $n \geq 1$ on ait l'équivalence suivante : $S(X) | X^n - 1 \Leftrightarrow n_S | n$.
15. Démontrer que si S est irréductible, alors n_S divise $q^{\deg S} - 1$ et q est d'ordre $\deg S$ dans le groupe multiplicatif $(\mathbb{Z}/n_S\mathbb{Z})^*$.
16. Montrer que si $S = S_1 S_2 \ldots S_\ell$ avec $S_1, S_2, \ldots S_\ell \in \mathbb{F}_q[X]$ premiers entre eux deux à deux, alors $n_S = \mathrm{ppcm}(n_{S_1}, \ldots, n_{S_\ell})$.
17. ($\star$) Dans cette question seulement, on considère $S(X) = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$. Par une méthode de votre choix que vous expliquerez dans votre copie, vérifier que S est irréductible ; il est conseillé d'utiliser `Sage`, mais il est interdit de faire appel aux fonctions de `Sage` qui donnent immédiatement le résultat, comme `is_irreducible` ou `factor`.
18. En utilisant `Sage` ou bien les questions précédentes, calculer n_S pour le polynôme $S(X) = (X^9 + 1)(X^5 + X^2 + 1) \in \mathbb{F}_2[X]$.

Partie 4 : Un code cyclique particulier

Dans cette dernière partie on étudie un code cyclique $C \subset \mathbb{F}_2^n$ bien adapté à la correction d'erreurs en rafale. On reprend les notations des trois premières parties (avec $q = 2$ concernant la partie 3).

Soit $t \geq 1$ un entier, et $P \in \mathbb{F}_2[X]$ un polynôme irréductible tel que $\deg P \geq t$; on suppose que P ne divise pas $X^{2t-1} - 1$ et on note

$$g(X) = (X^{2t-1} - 1)P(X) \in \mathbb{F}_2[X].$$

On pose $n = n_g$, où n_g est l'entier associé au polynôme $g \in \mathbb{F}_2[X]$ (défini à la question 14, au début de la partie 3).

19. Soit $Q(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}_2[X]$. Montrer que $X^{2t-1} - 1$ divise $Q(X)$ si, et seulement si,
$$\forall \ell \in [\![0, 2t-2]\!] \qquad \sum_{\substack{0 \leq i \leq d \\ i \equiv \ell \bmod 2t-1}} a_i = 0.$$

Dans les questions 20 et 21 on se donne deux polynômes $S, T \in \mathbb{F}_2[X]$, et $j \in [\![0, n-1]\!]$, tels que :

$$S(0) = T(0) = 1, \quad \deg S < t, \quad \deg T < t, \quad \text{et} \quad g | (S - X^j T).$$

20. En utilisant notamment la question 19, démontrer que $2t - 1$ divise j et que $S = T$.
21. En faisant appel (ou pas) à la question 16, déduire de la question précédente que $j = 0$.
22. A partir du résultat démontré dans les questions 20 et 21, démontrer que le code cyclique $C \subset \mathbb{F}_2^n$ de polynôme générateur $g(X)$ corrige t erreurs en rafale.
23. ($\star$) Dans cette question on considère le code cyclique C de polynôme générateur le polynôme $S(X)$ de la question 18, et on pourra (lorsque c'est utile) utiliser toutes les fonctions implémentées dans `Sage`. Déterminer les paramètres de C, c'est-à-dire sa longueur n, sa dimension k, et sa distance d. Démontrer que C corrige 5 erreurs en rafale, et préciser combien il en détecte. Comparer avec le nombre d'erreurs qu'il peut corriger (respectivement détecter) si on ne suppose plus qu'il s'agit d'erreurs en rafale.