



PRÉPASIMPLE

prepasimple.fr

HEC

Mathématiques 1

2004

Sujet de mathématiques approfondies

Mathématiques approfondies — Prépa ECG

Annales de concours · Sujet

Sur la transmission de messages

Le but de ce problème est de construire un système permettant de détecter et de corriger automatiquement des erreurs apparues lors de la transmission de messages binaires.

Dans tout le problème, m , n et p désignent des entiers naturels non nuls.

Partie I. L'opération Δ sur les parties d'un ensemble

Dans cette partie, on considère un ensemble $E = \{e_1, \dots, e_n\}$ ayant n éléments.

La différence symétrique de deux parties quelconques A et B de E , notée $A\Delta B$, est l'ensemble des éléments de E qui appartiennent à l'une et pas à l'autre. On admet que l'opération Δ est commutative et associative.

On sait que, pour toute partie A de E :

$$A\Delta\emptyset = A, \quad A\Delta A = \emptyset.$$

Pour toutes parties A et B de E , on pose $d(A, B) = \text{Card}(A\Delta B)$.

1) a) Pour une partie A de E , déterminer $d(A, \emptyset)$ et $d(A, E)$.

1) b) Montrer que, pour toutes parties A et B de E , $d(A, B) = d(A\Delta B, \emptyset)$.

2) a) On sait qu'on peut représenter une partie A de E par le n -uplet $(x_1, \dots, x_n)$, en posant, pour tout $i \in \{1, \dots, n\}$, $x_i = 1$ si e_i appartient à A et $x_i = 0$ sinon.

Les parties A , B et $A\Delta B$ étant représentées respectivement par $(x_1, \dots, x_n)$, $(y_1, \dots, y_n)$ et $(z_1, \dots, z_n)$, construire, pour un entier i fixé appartenant à $\{1, \dots, n\}$, une table à deux lignes et deux colonnes donnant les valeurs de z_i en fonction des valeurs de x_i et y_i .

Comparer z_i et $|x_i - y_i|$.

2) b) Montrer que, pour toutes parties A, B et C de E , $d(A, C) \leq d(A, B) + d(B, C)$.

Partie II. Calcul binaire sur des colonnes

On considère l'ensemble $K = \{0, 1\}$. On note $M_{p,n}(K)$ l'ensemble des matrices réelles à p lignes et n colonnes dont tous les coefficients appartiennent à K .

On définit sur les bits l'addition binaire $\oplus$ et le produit ordinaire par les tables suivantes :

$\oplus$	0	1
0	0	1
1	1	0
$\cdot$	0	1
0	0	0
1	0	1

L'addition binaire d'une liste de bits vaut 0 si le nombre de bits égaux à 1 est pair, et 1 sinon. On admet l'associativité et la commutativité de $\oplus$, ainsi que la distributivité du produit de bits par rapport à $\oplus$.

On définit également les opérations suivantes, qui sont des règles de calcul sur des tableaux de bits :

1. Pour $A = (a_{ij})$ et $B = (b_{ij})$ dans $M_{p,n}(K)$, $A \oplus B = (a_{ij} \oplus b_{ij})$.
2. Pour $\varepsilon \in K$ et $A \in M_{p,n}(K)$, $\varepsilon A = O$ si $\varepsilon = 0$, et $\varepsilon A = A$ si $\varepsilon = 1$.
3. Pour $A = (a_{ij}) \in M_{p,n}(K)$ et $B = (b_{ij}) \in M_{n,m}(K)$, on définit $A \odot B = (c_{ij}) \in M_{p,m}(K)$ par $c_{ij} = \bigoplus_{k=1}^n a_{ik} b_{kj}$.

Ainsi, $A \odot B$ s'obtient en calculant le produit matriciel réel AB , puis en remplaçant chaque coefficient entier par son reste dans la division par 2.

On admet que l'addition binaire des matrices est commutative et associative, qu'elle a pour élément neutre la matrice nulle O , et que le produit binaire est distributif par rapport à cette addition. Pour toute matrice binaire A , $A \oplus O = A$ et $A \oplus A = O$.

Ces définitions seront utilisées comme des opérations combinatoires sur des listes de bits. Une somme binaire sans terme vaut O .

On appelle code toute partie non vide $\mathcal{C}$ de $M_{n,1}(K)$ telle que, pour tous $x, y \in \mathcal{C}$, $x \oplus y \in \mathcal{C}$.

1) On considère les quatre colonnes

$$x_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad x_4 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

appartenant à $M_{5,1}(K)$, puis l'ensemble

$$\mathcal{C} = \{\varepsilon_1 x_1 \oplus \varepsilon_2 x_2 \oplus \varepsilon_3 x_3 \oplus \varepsilon_4 x_4 : (\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) \in K^4\}.$$

1) a) Montrer que $\mathcal{C}$ est un code. Déterminer tous les éléments de $\mathcal{C}$ à l'aide de x_1, x_2, x_3, x_4 .

1) b) Existe-t-il une famille (a_1, a_2) d'éléments de $\mathcal{C}$ telle que $\{\varepsilon_1 a_1 \oplus \varepsilon_2 a_2 : (\varepsilon_1, \varepsilon_2) \in K^2\}$ soit égal à $\mathcal{C}$?

1) c) Montrer que $\varepsilon_1 x_1 \oplus \varepsilon_2 x_2 \oplus \varepsilon_4 x_4 = O$ implique $\varepsilon_1 = \varepsilon_2 = \varepsilon_4 = 0$.

On dit qu'une famille $(u_1, \dots, u_q)$ d'éléments de $M_{p,n}(K)$ est libre pour l'addition binaire lorsque, pour tout $(\varepsilon_1, \dots, \varepsilon_q) \in K^q$, l'égalité $\bigoplus_{j=1}^q \varepsilon_j u_j = O$ implique $\varepsilon_1 = \dots = \varepsilon_q = 0$. Dans le cas contraire, elle est dite liée pour l'addition binaire.

Une famille $(u_1, \dots, u_q)$ d'éléments d'un code $\mathcal{C}$ est appelée une base binaire de $\mathcal{C}$ si elle est libre pour l'addition binaire et si tout élément de $\mathcal{C}$ est une somme binaire d'éléments de cette famille. La famille vide est libre et constitue une base binaire du code $\{O\}$.

Dans la suite de cette partie, n désigne un entier naturel supérieur ou égal à 2.

2) Pour $x = {}^t(x_1, \dots, x_n)$ et $y = {}^t(y_1, \dots, y_n)$ appartenant à $M_{n,1}(K)$, $d(x, y)$ est le nombre d'entiers $i \in \{1, \dots, n\}$ tels que $x_i \neq y_i$.

2) a) Montrer que, pour tous $x, y \in M_{n,1}(K)$, $d(x, y) = d(x \oplus y, O)$.

2) b) Montrer que, pour tous $x, y, z \in M_{n,1}(K)$, $d(x, z) \leq d(x, y) + d(y, z)$.

3) Soit $\mathcal{C}$ un code non réduit à $\{O\}$.

3) a) Montrer que $\mathcal{C}$ admet une base binaire. On pourra considérer, après avoir justifié son existence, le cardinal maximum d'une famille libre pour l'addition binaire formée d'éléments de $\mathcal{C}$.

3) b) Montrer que, si $(u_1, \dots, u_q)$ est une base binaire d'un code $\mathcal{C}$, alors tout élément de $\mathcal{C}$ s'écrit de manière unique sous la forme $\bigoplus_{j=1}^q \varepsilon_j u_j$, avec $(\varepsilon_1, \dots, \varepsilon_q) \in K^q$. En déduire le cardinal de $\mathcal{C}$ en fonction du cardinal d'une de ses bases binaires.

3) c) Montrer que toutes les bases binaires de $\mathcal{C}$ ont le même cardinal.

3) d) On suppose que q est le cardinal d'une base binaire de $\mathcal{C}$ et que $(v_1, \dots, v_q)$ est une famille libre pour l'addition binaire formée d'éléments de $\mathcal{C}$. Montrer que cette famille est une base binaire de $\mathcal{C}$.

- 4) On suppose dans cette question que $1 \leq p \leq n$. On note I_p la matrice à p lignes et p colonnes dont les coefficients diagonaux valent 1 et les autres 0.

On suppose que $Q \in M_{p,n}(K)$ possède p colonnes égales aux p colonnes distinctes de I_p . On définit $\mathcal{C}_Q = \{x \in M_{n,1}(K) : Q \odot x = O\}$.

- 4) a) Montrer que $\mathcal{C}_Q$ est un code.

- 4) b) Montrer qu'il existe une permutation σ de $\{1, \dots, n\}$ telle que, pour tout $(x_1, \dots, x_n) \in K^n$,

$$Q \odot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (I_p \ P) \odot \begin{pmatrix} x_{\sigma(1)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix},$$

avec $P \in M_{p,n-p}(K)$.

Dans cette notation par blocs, la k -ième ligne de $(I_p \ P)$ est formée de la k -ième ligne de I_p suivie de la k -ième ligne de P . Lorsque $p = n$, le bloc P est vide.

- 4) c) En déduire le nombre d'éléments de $\mathcal{C}_Q$ et le cardinal d'une de ses bases binaires.

- 4) d) On suppose dans cette sous-question que $Q = (B \ I_p)$, avec $B \in M_{p,n-p}(K)$.

Montrer que les colonnes de $\begin{pmatrix} I_{n-p} \\ B \end{pmatrix}$ constituent une base binaire de $\mathcal{C}_Q$; lorsque $p = n$, cette famille est vide.

- 4) e) Si A est une partie non vide de $\mathbb{N}$, $\min A$ désigne son plus petit élément.

On suppose que $r > 1$ est un entier, que toute famille formée de $r - 1$ colonnes de Q prises à des positions distinctes est libre pour l'addition binaire, et qu'il existe une

famille liée pour l'addition binaire formée de r colonnes de Q prises à des positions distinctes. Montrer que, dans ces conditions,

$$r = \min\{d(x, O) : x \in \mathcal{C}_Q \setminus \{O\}\}.$$

Partie III. Un code correcteur d'erreurs

Dans cette partie, on suppose que $p \geq 2$ et on pose $n = 2^p - 1$.

On considère une matrice H dont les colonnes sont les n éléments non nuls de $M_{p,1}(K)$, chacun apparaissant une fois, et on définit $\mathcal{C}_H = \{u \in M_{n,1}(K) : H \odot u = O\}$.

- 1) Déterminer le cardinal des bases binaires de $\mathcal{C}_H$.
- 2) Montrer que $\min\{d(u, v) : u, v \in \mathcal{C}_H, u \neq v\} = 3$.
- 3) Pour tout $v \in M_{n,1}(K)$, on définit $B_v = \{u \in M_{n,1}(K) : d(u, v) \leq 1\}$.
 - 3) a) Déterminer le cardinal de B_v .
 - 3) b) Montrer que, si v et w sont deux éléments distincts de $\mathcal{C}_H$, alors $B_v \cap B_w = \emptyset$.
 - 3) c) Montrer que $\bigcup_{v \in \mathcal{C}_H} B_v = M_{n,1}(K)$.
- 4) Soit $z \in M_{n,1}(K) \setminus \mathcal{C}_H$.
 - 4) a) Montrer qu'il existe un seul élément $v \in \mathcal{C}_H$ tel que $d(z, v) = 1$; cet élément est noté $\Phi(z)$.
 - 4) b) Montrer qu'il existe un seul élément $e \in M_{n,1}(K)$ tel que $d(e, O) = 1$ et $H \odot z = H \odot e$. Comparer $\Phi(z)$ et $z \oplus e$.

- 5) Dans cette question et dans celle-ci uniquement, on suppose que $p = 3$, donc $n = 7$, et on choisit pour H la matrice

$$H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

- 5) a) Montrer que $\mathcal{C}_{H_1}$ a pour base binaire (c_1, c_2, c_3, c_4) , où

$$c_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad c_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad c_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad c_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

- 5) b) On suppose qu'on veut transmettre, par sémaphore, radio ou internet, un message consistant en une suite de quatre symboles égaux à 0 ou 1 : $\eta_1, \eta_2, \eta_3, \eta_4$.

Au lieu de transmettre dans l'ordre ces quatre symboles, on calcule

$y = \eta_1 c_1 \oplus \eta_2 c_2 \oplus \eta_3 c_3 \oplus \eta_4 c_4$ et ce sont les sept éléments de cette colonne qui sont transmis dans l'ordre, de haut en bas.

On suppose que les composantes de la colonne reçue y^* sont, dans l'ordre, 0, 1, 0, 0, 1, 1, 0 et qu'il y a eu une seule erreur dans la transmission, c'est-à-dire qu'une seule composante de y^* est fausse.

Déterminer la valeur exacte des quatre nombres $\eta_1, \eta_2, \eta_3, \eta_4$. On utilisera le produit

$$H_1 \odot y^*.$$

- 5) c) On suppose qu'ayant transmis une colonne $z \in \mathcal{C}_{H_1}$, on a reçu la colonne z^* comportant deux erreurs. Montrer que le calcul de $H_1 \odot z^*$ permet de s'apercevoir qu'il y a eu des erreurs, mais ne permet pas de connaître les deux composantes qui sont fausses.

Partie IV. Distinguere falsum vero

Dans cette partie, on utilise les mêmes notations que dans la partie III; en particulier, $p \geq 2$ et $n = 2^p - 1$.

- 1) Pour tout $k \in \{1, \dots, n\}$, on considère l'écriture de k en base deux :

$$k = \sum_{i=1}^p \varepsilon_{ik} 2^{i-1}.$$

On prend pour matrice H la matrice $H_2 = (\varepsilon_{ik})_{1 \leq i \leq p, 1 \leq k \leq n}$.

On considère $n - p$ éléments $\eta_1, \dots, \eta_{n-p}$ de K . On veut transmettre le message formé par la ligne $(\eta_1 \ \dots \ \eta_{n-p})$. Comme dans la question précédente, on commence par calculer la colonne $y = \bigoplus_{j=1}^{n-p} \eta_j d_j$, où $(d_1, \dots, d_{n-p})$ est une base binaire de $\mathcal{C}_{H_2}$, et c'est cette colonne qui est transmise.

On désigne le message reçu par la colonne y^* et on suppose qu'il y a eu une seule erreur pendant la transmission. On calcule alors $H_2 \odot y^* = {}^t(x_1, \dots, x_p)$ et on pose

$$k = \sum_{i=1}^p x_i 2^{i-1}.$$

Montrer que l'erreur s'est produite à la composante numéro k de y .

- 2) On suppose dans cette question que $p = 3$ et $n = 7$.

2) a) On pose

$$d_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad d_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad d_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad d_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Déterminer la matrice H_2 et montrer que (d_1, d_2, d_3, d_4) est une base binaire de $\mathcal{C}_{H_2}$.

2) b) Les deux célèbres mathématiciens Primus et Secundus concourent au calcul d'une nouvelle constante universelle qu'ils appellent ζ . Primus pense avoir trouvé les trois premiers chiffres significatifs x, y et z , en base dix, de ζ et s'empresse de les transmettre à Secundus. Afin de minimiser les risques d'erreur au cours de la transmission et de s'assurer la possibilité de les détecter et de les corriger, Primus et Secundus adoptent la démarche suivante.

Chaque chiffre de 0 à 9 a été écrit en base deux à quatre positions. Ainsi, 5 est représenté par 0101 et 9 par 1001. Le chiffre x est écrit $x_4x_3x_2x_1$, le chiffre y est écrit $y_4y_3y_2y_1$ et le chiffre z est écrit $z_4z_3z_2z_1$; par exemple, $x = x_1 + 2x_2 + 2^2x_3 + 2^3x_4$.

Primus transmet les trois colonnes $x_1d_1 \oplus x_2d_2 \oplus x_3d_3 \oplus x_4d_4$, $y_1d_1 \oplus y_2d_2 \oplus y_3d_3 \oplus y_4d_4$ et $z_1d_1 \oplus z_2d_2 \oplus z_3d_3 \oplus z_4d_4$. Les colonnes d_1, d_2, d_3, d_4 définies ci-dessus sont bien connues de Secundus.

Primus ne se trompe pas dans ses calculs, mais la transmission est sujette à erreurs : on a constaté dans la pratique qu'il y a une erreur au plus par colonne transmise.

Secundus réceptionne une liste où les trois colonnes reçues sont écrites bout à bout, soit le message suivant :

111011010000110010111.

Quel est probablement le nombre que Primus et Secundus semblent en fait sur le point de découvrir ?

- 2) c) Secundus décide d'écrire un programme en Python qui permet de retrouver, à partir des colonnes reçues, les chiffres envoyés par Primus. Comment peut-il procéder ?

En Python, pour un entier a , l'expression `a % 2` renvoie son reste dans la division par 2. Pour des tableaux NumPy à coefficients entiers, `% 2` s'applique coefficient par coefficient. La syntaxe `int(texte)` convertit une chaîne représentant un entier en cet entier, et `int(a)` convertit un entier NumPy en entier Python.