CHAMBRE DE COMMERCE ET D'INDUSTRIE DE PARIS
DIRECTION DE L'ENSEIGNEMENT
Direction des Admissions et concours

ECOLE DES HAUTES ETUDES COMMERCIALES
E.S.C.P.-E.A.P.
ECOLE SUPERIEURE DE COMMERCE DE LYON

CONCOURS D'ADMISSION SUR CLASSES PREPARATOIRES

OPTION SCIENTIFIQUE

MATHEMATIQUES I

Année 2004

La présentation, la lisibilité, l'orthographe, la qualité de la rédaction, la clarté et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.
Les candidats sont invités à encadrer dans la mesure du possible les résultats de leurs calculs.
Ils ne doivent faire usage d'aucun document : l'utilisation de toute calculatrice et de tout matériel électronique est interdite.
Seule l'utilisation d'une règle graduée est autorisée.

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, 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 :

$$(\mathcal{G}) \qquad A\Delta\emptyset = A, \quad A\Delta A = \emptyset$$

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

1. (a) Pour une partie A de E, déterminer $d(A, \emptyset)$ et $d(A, E)$.
   (b) Montrer que pour toutes parties A et B de E : $d(A, B) = d(A\Delta B, \emptyset)$.

2. On sait qu'on peut représenter une partie A de E par le n-uplet $(x_1, \dots, x_n)$ en posant :

$$\forall i \in \{1, \dots, n\},\ x_i = 1 \textit{ si } e_i \textit{ appartient à } A \textit{ et } 0 \textit{ sinon.}$$

   (a) Les parties A, B, $A\Delta B$ 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 $|x_i - y_i|$.
   (b) Montrer que pour toutes parties A, B et C de E, $d(A, C) \leqslant d(A, B) + d(B, C)$.

Partie II : Une autre algèbre linéaire

On considère l'ensemble $\mathbb{K} = \{0, 1\}$ et $\mathfrak{M}_{p,n}(\mathbb{K})$ désigne l'ensemble des matrices à p lignes et n colonnes dont les coefficients appartiennent à $\mathbb{K}$.
On définit sur $\mathbb{K}$ l'addition $\dot{+}$ et la multiplication . à l'aide des tables suivantes

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

On remarque que la multiplication sur $\mathbb{K}$ est la multiplication des réels, que ces opérations sont associatives, commutatives et que la multiplication sur $\mathbb{K}$ est distributive par rapport à l'addition sur $\mathbb{K}$; ces propriétés ne sont pas à démontrer.
On définit également

1) la somme $A\dot{+}B$ de deux matrices $A = (a_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant n}}$ et $B = (b_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant n}}$ appartenant à $M_{p,n}(\mathbb{K})$ par :

$$A\dot{+}B = (c_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant n}} \quad \text{où} \quad c_{i,j} = a_{i,j}\dot{+}b_{i,j}$$

2) le produit $\varepsilon.A$ d'une matrice $A = (a_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant n}}$ et d'un élément ε appartenant respectivement à $\mathfrak{M}_{p,n}(\mathbb{K})$ et $\mathbb{K}$ par :

$$\varepsilon.A = (\varepsilon.a_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant n}}$$

3) le produit $A\dot{\times}B$ de deux matrices $A = (a_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant n}}$ et $B = (b_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}$ appartenant respectivement à $M_{p,n}(\mathbb{K})$ et $\mathfrak{M}_{n,m}(\mathbb{K})$ par :

$$A\dot{\times}B = (c_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant m}} \quad \text{où} \quad c_{i,j} = a_{i,1}.b_{1,j}\dot{+}\cdots\dot{+}a_{i,n}.b_{n,j}$$

Pour toute matrice A appartenant à $\mathfrak{M}_{p,n}(\mathbb{K})$ et toute colonne X appartenant à $\mathfrak{M}_{n,1}(\mathbb{K})$, le produit $A\dot{\times}X$ est ainsi bien défini.
On admet que la loi $\dot{+}$ ainsi définie sur $\mathfrak{M}_{p,n}(\mathbb{K})$ est une opération commutative, associative, qu'elle admet un élément neutre à savoir la matrice nulle ayant p lignes et n colonnes et dont tous les éléments sont nuls ; on note O cette matrice et cela quelles que soient les valeurs de n et p. On admet également que $\dot{\times}$ est distributive par rapport à $\dot{+}$.
Dans leur copie les candidats pourront omettre les points sur les signes $\dot{+}$ et $\dot{\times}$. On remarque que pour toute matrice A appartenant à $M_{p,n}(\mathbb{K})$:

$$(\mathcal{G}') \qquad A\dot{+}O = A, \qquad A\dot{+}A = O$$

On appelle **code** toute partie non vide $\mathcal{C}$ de $\mathfrak{M}_{n,1}(\mathbb{K})$ telle que :

$$\forall (x, y) \in \mathcal{C}^2, \quad x\dot{+}y \in \mathcal{C}$$

1. On considère les quatre colonnes

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

appartenant à $\mathfrak{M}_{5,1}(\mathbb{K})$ puis l'ensemble

$$\mathcal{C} = \{\varepsilon_1.x_1\dot{+}\varepsilon_2.x_2\dot{+}\varepsilon_3.x_3\dot{+}\varepsilon_4.x_4, \quad (\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) \in \mathbb{K}^4\}$$

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

(b) Existe-t-il une famille (u_1, u_2) d'éléments de $\mathcal{C}$ telle que $\{\varepsilon_1.u_1 \dot{+} \varepsilon_2.u_2, (\varepsilon_1, \varepsilon_2) \in \mathbb{K}^2\}$ soit égal à $\mathcal{C}$?

(c) Montrer que : $\varepsilon_1.x_1 \dot{+} \varepsilon_2.x_2 \dot{+} \varepsilon_4.x_4 = O \Rightarrow \varepsilon_1 = \varepsilon_2 = \varepsilon_4 = 0$.

On dit qu'une famille $(u_1, \ldots, u_q)$ d'éléments de $\mathfrak{M}_{p,n}(\mathbb{K})$ est $\mathbb{K}$-libre lorsque :

$$\forall (\varepsilon_, \ldots, \varepsilon_q) \in \mathbb{K}^q, \qquad \varepsilon_1.u_1 \dot{+} \cdots \dot{+} \varepsilon_q.x_q = O \Rightarrow \varepsilon_1 = \cdots = \varepsilon_q = 0$$

Dans le cas contraire, on dit que la famille $(u_1, \ldots, u_q)$ est $\mathbb{K}$-liée. On dit qu'une famille $(u_1, \ldots, u_p)$ dont les éléments appartiennent à un code $\mathcal{C}$ est une $\mathbb{K}$-base de $\mathcal{C}$ lorsqu'elle est une famille $\mathbb{K}$-libre et lorsque pour tout élément x de $\mathcal{C}$ il existe $\varepsilon_1, \ldots, \varepsilon_p)$ appartenant à $\mathbb{K}^p$ tel que $x = \varepsilon_1.u_1 \dot{+} \cdots \dot{+} \varepsilon_p.u_p$ (Dans leur copie, les candidats pourront omettre la lettre $\mathbb{K}$ dans les expressions manipulées $\mathbb{K}$-libre, $\mathbb{K}$- base, sans en oublier le sens particulier.)
Dans la suite de cette partie n désignera un entier naturel supérieur ou égal à 2.

2. Pour tout $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ appartenant à $\mathfrak{M}_{n,1}(\mathbb{K})$, $d(x, y)$ est le nombre d'entiers i appartenant à $\{1, \ldots, n\}$ tels que $x_i \neq y_i$.

   (a) Montrer que : $\forall (x, y) \in (\mathfrak{M}_{n,1}(\mathbb{K}))^2, \quad d(x, y) = d(x \dot{+} y, O)$.

   (b) Montrer que : $\forall (x, y, z) \in (\mathfrak{M}_{n,1}(\mathbb{K}))^3, \quad d(x, z) \leqslant d(x, y) + d(y, z)$.

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

   (a) Montrer que $\mathcal{C}$ admet une $\mathbb{K}$-base. On pourra considérer, après avoir justifié son existence, le cardinal maximum d'une famille $\mathbb{K}$-libre formée d'éléments de $\mathcal{C}$.

   (b)
   - Montrer que si $(u_1, \ldots, u_p)$ est une $\mathbb{K}$-base d'un code $\mathcal{C}$, alors tout élément de $\mathcal{C}$ s'écrit de manière unique sous la forme $\varepsilon_1.u_1 \dot{+} \cdots \dot{+} \varepsilon_p.u_p$.
   - En déduire le cardinal de $\mathcal{C}$ en fonction du cardinal d'une de ses $\mathbb{K}$-bases.

   (c) Montrer que toutes les $\mathbb{K}$-bases de $\mathcal{C}$ ont le même cardinal.

   (d) On suppose que p est le cardinal d'une $\mathbb{K}$-base de $\mathcal{C}$ et que $(v_1, \ldots, v_p)$ est une famille $\mathbb{K}$-libre de $\mathcal{C}$, montrer que $(v_1, \ldots, v_p)$ est une $\mathbb{K}$-base de $\mathcal{C}$.

4. On suppose dans cette question que $1 \leqslant p \leqslant n$ et on note I_p la matrice à p lignes et p colonnes dont tous les éléments sont nuls excepté les éléments diagonaux qui sont égaux à 1.
On suppose également que Q est une matrice appartenant à $\mathfrak{M}_{p,n}(\mathbb{K})$ telle que p colonnes de Q sont égales aux p colonnes distinctes de I_p.
On définit l'ensemble $\mathcal{C}_Q = \{x \in \mathfrak{M}_{n,1}(\mathbb{K}), Q \dot{\times} x = O\}$.

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

   (b) Montrer que pour tout $(x_1, \ldots, x_n)$ appartenant à $\mathbb{K}^n$ il existe une permutation σ de $\{1, \ldots, n\}$ telle que :

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

   où P est une matrice appartenant à $\mathfrak{M}_{p,n-p}(\mathbb{K})$.
   (Dans la notation habituelle d'une matrice par blocs utilisée ci-dessus, la k-ième ligne de $(I_p \quad P)$ est formée de la k-ième ligne de I_p suivie de la k-ième ligne de P.)

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

(d) On suppose dans cette sous-question que Q est la matrice $(B \quad I_p)$ où B est une matrice appartenant à $\mathfrak{M}_{p,n-p}(\mathbb{K})$. Montrer que les colonnes de la matrice $\begin{pmatrix} I_{n-p} \\ B \end{pmatrix}$ constituent une base de $\mathcal{C}_Q$.

(e) Si A est une partie non vide de $\mathbb{N}$, $\min A$ désigne le plus petit élément de A. On suppose que r est un entier strictement supérieur à 1, que toute famille formée de $r-1$ colonnes de Q est une famille $\mathbb{K}$-libre de $\mathfrak{M}_{p,1}(\mathbb{K})$ et qu'il existe une famille $\mathbb{K}$-liée formée de r colonnes de Q.
Montrer que dans ces conditions $r = \min\{d(x,O), x \in \mathcal{C}_Q \backslash \{O\}\}$.

Partie III : Un code correcteur d'erreurs

Dans cette partie, on suppose que l'entier p est supérieur ou égal à 2 et on pose $n = 2^p - 1$.
On considère une matrice H dont les colonnes sont les n éléments non nuls de $\mathfrak{M}_{p,1}(\mathbb{K})$ et on définit :

$$\mathcal{C}_H = \{u \in \mathfrak{M}_{n,1}(\mathbb{K}), H \dot{\times} u = O\}$$

1. Déterminer le cardinal des $\mathbb{K}$-bases de $\mathcal{C}_H$.

2. Montrer que : $\min\{d(u,v), (u,v) \in \mathcal{C}_H^2 \quad \text{et} \quad u \neq v\} = 3$.

3. Pour tout v appartenant à $M_{n,1}(\mathbb{K})$, on définit $B_v = \{u \in \mathfrak{M}_{n,1}(\mathbb{K}), d(u,v) \leqslant 1\}$.

   (a) Déterminer le cardinal de B_v.

   (b) Montrer que si v et w sont deux éléments distincts de $\mathcal{C}_H$, alors $B_v \cap B_w = \emptyset$.

   (c) Montrer que $\bigcup_{v \in \mathcal{C}_H} B_v = \mathfrak{M}_{n,1}(\mathbb{K})$.

4. Soit z appartenant à $\mathfrak{M}_{n,1}(\mathbb{K}) \backslash \mathcal{C}_H$.

   (a) Montrer qu'il existe un seul élément v appartenant à $\mathcal{C}_H$ tel que $d(z,v) = 1$; cet élément v est noté $\Phi(z)$.

   (b) Montrer qu'il existe un seul élément e appartenant à $\mathfrak{M}_{n,1}(\mathbb{K})$ tel que $d(e,O) = 1$ et $H \dot{\times} z = H \dot{\times} e$.
   Comparer $\Phi(z)$ et $z \dot{+} e$.

5. *Dans cette question uniquement on suppose que $p = 3$, donc $n = 7$, et on choisit pour H la matrice*

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

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

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

   (b) On suppose qu'on veut transmettre (par sémaphore, radio ou internet ...) un message consistant en la suite de quatre symboles égaux à 0 où 1 : η_1, η_2, η_3, η_4. Au lieu de transmettre dans l'ordre ces quatre symboles, on calcule $y = \eta_1.c_1 \dot{+} \eta_2.c_2 \dot{+} \eta_3.c_3 \dot{+} \eta_4.c_4$ 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 y^* reçues sont dans l'ordre: $0,1,0,0,1,1,0$ et qu'il y a 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 η_1, η_2, η_3, η_4, (on utilisera le produit $H_1 \dot{\times} y^*$).

(c) On suppose qu'ayant transmis une colonne z, appartenant à $\mathcal{C}_{H_1}$, on a reçu la colonne z^* comportant deux erreurs.
Montrer que le calcul de $H_1 \dot{\times} z^*$ permet de s'apercevoir qu'il y a effectivement 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 est un entier naturel supérieur ou égal à 2 et $n = 2^p - 1$.

1. Pour tout k appartenant à $\{1, \ldots, n\}$, on considère l'écriture de k en base deux :
$$k = \sum_{i=1}^{p} \varepsilon_{i,k} 2^{i-1}$$
et on prend alors pour matrice H la matrice $H_2 = (\varepsilon_{i,k})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant k \leqslant n}}$.
On considère $n - p$ éléments $\eta_1, \ldots, \eta_{n-p}$ appartenant à $\mathbb{K}$. On veut transmettre le message formé par la ligne $(\eta_1, \ldots, \eta_{n-p})$. Comme dans la question précédente, on commence par calculer la colonne $y = \eta_1.d_1 \dot{+} \cdots \dot{+} \eta_{n-p}.d_{n-p}$ où $(d_1, \ldots, d_{n-p})$ est une base 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 une seule erreur pendant la transmission.
On calcule alors $H_2 \dot{\times} y^* = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ et on pose $k = \sum\limits_{i=1}^{p} x_i 2^{i-1}$.
Montrer que l'erreur s'est produite à la composante numéro k de y.

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

   (a) On pose :
$$d_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, d_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, d_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, d_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$
   Déterminer la matrice H_2 et montrer que (d_1, d_2, d_3, d_4) est une $\mathbb{K}$-base de $\mathcal{C}_{H_2}$.

   (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 les corriger, Primus et Secundus adoptent la démarche suivante

   1) Chacun des chiffres $0, \ldots, 9$ a été écrit en base deux à quatre positions. Ainsi 5 est représenté par 0101 et 9 par 1001. Donc le chiffre x est écrit $x_4x_3x_2x_1$, y est écrit $y_4y_3y_2y_1$, z est écrit $z_4z_3z_2z_1$, ainsi par exemple $x = x_1 + x_2.2 + x_3.2^2 + x_4.2^3$.

   2) Primus transmet les 3 colonnes :
$$x_1.d_1 \dot{+} x_2.d_2 \dot{+} x_3.d_3 \dot{+} x_4.d_4, \qquad y_1.d_1 \dot{+} y_2.d_2 \dot{+} y_3.d_3 \dot{+} y_4.d_4, \qquad z_1.d_1 \dot{+} z_2.d_2 \dot{+} z_3.d_3 \dot{+} z_4.d_4$$
   (d_1, d_2, d_3 et d_4 ont été définies ci-dessus et sont bien sûr connues de Secundus).

   Évidemment 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 ?

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