session 1987

SGE **DEUXIÈME ÉPREUVE DE MATHÉMATIQUES T'** DURÉE : 4 heures

La qualité de la rédaction et de la présentation, la clarté et la précision des raisonnements constitueront un élément important pour l'appréciation des copies.

L'usage des instruments de calcul est autorisé.

Notations et objectif du problème

Dans tout le problème E et F sont deux espaces vectoriels sur un corps K, de dimensions respectives k et n où $0 < k < n$; $b_E = (e_1, e_2, ..., e_k)$ est une base de E et $b_F = (f_1, f_2, ..., f_n)$ une base de F. On suppose donnée une application linéaire injective g de E dans F et on pose $C = g(E)$. Une telle application g est appelée *code* : en effet, les composantes $u_1, u_2, ..., u_k$ d'un élément u de E peuvent être considérées comme les symboles successifs d'un message; les composantes $x_1, x_2, ..., x_n$ de $x = g(u)$ sont les symboles successifs du message codé. Le message codé est transmis et on recueille un élément y de F, dont les composantes $y_1, y_2, ..., y_n$ sont les symboles successifs du message reçu. Le message reçu y peut différer de x à cause d'erreurs de transmission affectant certaines composantes. Le but du problème est d'étudier comment on peut reconstituer x puis u à partir de y.

I. Résultats généraux sur les codes

1. *Distance minimale d'un code.*

Soit W la fonction de F dans $\mathbb{R}$ qui à tout élément de F fait correspondre le nombre de composantes non nulles de cet élément dans la base b_F.

a. Montrer que la fonction Δ de $F \times F$ dans $\mathbb{R}$ définie par : $\Delta(x, y) = W(x - y)$ est une distance sur F.

b. Le nombre d défini par $d = \min_{\substack{u \in C \\ u \neq 0}} W(u)$, est appelé distance minimale du code.

Soit t la partie entière de $\dfrac{d-1}{2}$. Montrer que pour tout élément y de F il existe au plus un élément x de C tel que $\Delta(x, y) \leqslant t$.

2. *Applications de contrôle.*

Soit h une application linéaire de F dans un espace vectoriel F'. On suppose que le noyau de h est C. On dit alors que h est une application de contrôle pour le code g.

a. Déterminer le rang de la famille $(h(f_i))_{1 \leqslant i \leqslant n}$.

b. Soient x un élément non nul de C et J l'ensemble des indices i pour lesquels la composante de x sur f_i est non nulle. Montrer que la famille $(h(f_i))_{i \in J}$ est liée.

c. Montrer qu'il existe une famille de d vecteurs extraite de la famille $(h(f_i))_{1 \leqslant i \leqslant n}$ qui est liée.

d. Montrer que toute famille de $d-1$ vecteurs extraite de la famille $(h(f_i))_{1 \leqslant i \leqslant n}$ est libre.

e. Déduire des questions précédentes que $d \leqslant n - k + 1$.

3. *Un exemple d'application de contrôle.*

a. Montrer qu'il existe une partie P de l'ensemble $\{1, 2, ..., n\}$ ayant $n-k$ éléments telle que la famille $(f_i)_{i \in P}$ soit base d'un supplémentaire D de C dans F. Quitte à permuter éventuellement les éléments de la base b_F on supposera désormais que la partie P ainsi trouvée est la partie $\{k+1, k+2, ..., n\}$.

b. Dans ces conditions, montrer qu'il existe une base b'_E de E telle que la transposée G de la matrice de l'application linéaire g dans les bases b'_E et b_F soit de la forme $G = [I_k \; A]$, où I_k désigne la matrice identité d'ordre k et A est une matrice à $n-k$ colonnes et k lignes.

Tournez la page S. V. P.

c. Soit h l'application linéaire de F dans D qui à tout élément x associe la projection de x sur D parallèlement à C. Montrer que h est une application de contrôle pour g et déterminer la matrice H de h lorsque F est muni de la base b_F et D de la base $(f_{k+1}, \ldots, f_n)$.

d. Correction d'un message.

On suppose que, dans la transmission d'un message, il se produit t erreurs au plus. Soit y un message reçu. On calcule $z = h(y)$. Prouver qu'il existe un élément e de F tel que $h(e) = z$ et $W(e) \leqslant t$. Montrer que $x = y - e$ appartient à C et que x est l'unique élément de C dont la distance à y est minimum. Ainsi, x est le message transmis.

4. ***Étude d'un exemple de code.***

On suppose que K est le corps à deux éléments $\{0, 1\}$.

E est l'espace K^4, F l'espace K^7, ces deux espaces étant munis de leurs bases canoniques respectives. Enfin g est l'application linéaire de E dans F dont la matrice dans les bases indiquées a pour transposée :

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

a. Calculer la matrice H de l'application linéaire h introduite au 3.*c*.

b. Déterminer la valeur de la distance minimale d.

c. Soit $y = (1, 0, 1, 0, 0, 1, 0)$. Calculer $h(y)$.

En conclure qu'il existe un élément x de C et un seul tel que $W(x, y) \leqslant 1$. Quel est cet élément x ? Quel est l'élément u de K^4 tel que $x = g(u)$?

II. Étude d'une famille de codes

Dans cette partie le corps de base K est le corps à deux éléments $\{0, 1\}$.

On désigne par m un entier strictement positif et on pose $k = m + 1$. On note E_k l'espace vectoriel K^k et F_k l'espace vectoriel de toutes les fonctions définies sur K^m à valeurs dans K.

1. *Construction d'une base de* F_k *par codage binaire.*

a. Quel est le nombre d'éléments de E_k et de F_k ? Quelle est la dimension de F_k ?

b. Montrer que pour tout $(w_1, w_2, \ldots, w_m)$ de K^m le nombre $\sum_{i=1}^{m} w_i 2^{i-1}$ est dans l'ensemble $\{0, 1, \ldots, 2^m - 1\}$, puis que l'application de K^m dans $\{0, 1, \ldots, 2^m - 1\}$ qui à tout $(w_1, w_2, \ldots w_m)$ de K^m fait correspondre $\sum_{i=1}^{m} w_i 2^{i-1}$ est bijective.

c. Pour tout $(w_1, w_2, \ldots, w_m)$ de K^m notons $\text{supp}(w_1, w_2, \ldots w_m)$ l'ensemble des indices i compris entre 1 et m tels que $w_i \neq 0$. Montrer que l'application de $\{0, 1, \ldots, 2^m - 1\}$ dans l'ensemble des parties de $\{1, 2, \ldots, m\}$ qui, à j écrit sous la forme $j = \sum_{i=1}^{m} w_i 2^{i-1}$, associe $P_j = \text{supp}(w_1, w_2, \ldots, w_m)$ est bijective.

Tournez la page S. V. P.

d. Pour tout élément j de $\{0, 1, ..., 2^m-1\}$ définissons la fonction f_j de K^m dans K par :

$$f_j(v_1, v_2, \ldots, v_m) = \begin{cases} 1 \text{ si supp } (v_1, v_2, \ldots v_m) = P_j \\ 0 \text{ sinon.} \end{cases}$$

Montrer que la famille $b_{F_k} = (f_0, f_1, ..., f_{2^m-1})$ est une base de F_k.

e. Soit U la fonction de K^m dans K constante et égale à 1. Pour tout j, on note V_j la fonction de K^m dans K définie par $V_j(v_1, v_2, ..., v_m) = v_j$, et $\bar{V}_j = U - V_j$.

Prouver que, pour tout j, $$f_j = \prod_{i \in P_j} V_i \prod_{i \notin P_j} \bar{V}_i.$$

f. Montrer que dans la base b_{F_k} la composante sur f_j d'un élément f de F_k s'écrit sous la forme $f(u)$ où u est un élément de K^m qu'on déterminera.

Quelles sont les composantes de la fonction U sur la base b_{F_k} ? Quelles sont celles de V_i ?

Déterminer pour tout i compris entre 1 et m les composantes de V_i sur la base b_{F_k}.

2. *Définition d'une famille de codes.*

On munit désormais E_k de sa base canonique et F_k de la base construite en 1.*d*.

On désigne par g_k l'application linéaire de E_k dans F_k définie par :

$$g_k(u_0, u_1, ..., u_m) = u_0 U + u_1 V_1 + ... + u_m V_m.$$

a. Montrer que g_k est une application linéaire injective.

Nous noterons C_k l'image $g_k(E_k)$ et d_k la distance minimale correspondante.

b. Pour $k = 2$ et $k = 3$ déterminer tous les éléments de C_k (ceux-ci seront donnés par leurs composantes sur la base b_{F_k}). Déterminer d_2 et d_3.

c. Supposons maintenant $k > 2$.

Montrer que $g_k(u_0, u_1, ..., u_{m-1}, 0)$ a ses 2^{m-1} premières composantes sur la base b_{F_k} qui sont les mêmes que ses 2^{m-1} dernières composantes et que ces composantes sont celles sur $b_{F_{k-1}}$ de $g_{k-1}(u_0, u_1, ..., u_{m-1})$.

Montrer que $g_k(u_0, u_1, ..., u_{m-1}, 1)$ a exactement 2^{m-1} composantes non nulles.

En conclure que, pour $k > 2$, $\quad d_k = \min(2d_{k-1}, 2^{m-1})$.

Calculer d_k.

d. Prenons $m = 3$, donc $k = 4$.

Déterminer la matrice G_4 transposée de la matrice de l'application linéaire g_4 lorsque $E_4 = K^4$ est muni de la base canonique et lorsque F_4 est muni de la base b_{F_4}.

Tournez la page S. V. P.

— 4 —

3. *Introduction d'une structure euclidienne.*

Soit A_k le $\mathbb{R}$-espace vectoriel des fonctions définies sur K^m à valeurs dans $\mathbb{R}$, muni du produit scalaire qui à tout couple (φ, ψ) d'éléments de A_k associe

$$(\varphi \mid \psi) = \sum_{w \in K^m} \varphi(w)\, \psi(w).$$

D'autre part, pour tout couple (v, w) d'éléments de K^m, où $v = (v_1, v_2, \ldots, v_m)$ et $w = (w_1, w_2, \ldots, w_m)$, posons $< v, w > = \sum_{i=1}^{m} v_i w_i$, où la somme est calculée dans K.

Pour tout élément v de K^m définissons la fonction χ_v de K^m dans $\mathbb{R}$ par : $\chi_v(w) = (-1)^{< v, w >}$.

a. Soit v un élément de K^m. Montrer que, pour tout couple (w, w') d'éléments de K^m,

$$\chi_v(w + w') = \chi_v(w)\, \chi_v(w').$$

b. Inversement, soit χ un élément de A_k tel que, $\chi(0) = 1$ et que, pour tout couple (w, w') d'éléments de K^m,

$$\chi(w + w') = \chi(w)\, \chi(w').$$

Montrer qu'il existe un élément v et un seul de K^m tel que $\chi_v = \chi$. Pour cela, on pourra d'abord prouver que, pour tout w, $[\chi(w)]^2 = 1$, et introduire les valeurs de χ sur les éléments de la base canonique de K^m.

c. Montrer que si, v est un élément non nul de K^m, il existe un élément s de K^m tel que $\chi_v(s) = -1$. En déduire que $(\chi_v \mid \chi_0) = 0$; pour cela, on pourra observer que pour tout élément φ de A_k,

$$\sum_{w \in K^m} \varphi(w) = \sum_{w \in K^m} \varphi(w + s).$$

d. Prouver finalement que la famille $\left(\frac{1}{2^{m/2}}\, \chi_v\right)$, où v parcourt K^m, est une base orthonormale de l'espace euclidien A_k. Pour cela, on pourra utiliser le résultat de *c.* en observant que $\chi_v \chi_{v'} = \chi_{v+v'}$.

e. Montrer que si v est différent de 0, l'ensemble des éléments w de K^m tels que $< v, w > = 0$ a le même nombre d'éléments que l'ensemble des w de K^m tels que $< v, w > = 1$. Retrouver ainsi le résultat du *c.*

f. Transformation de Fourier sur K^m.

Pour tout élément φ de A_k, on note $\hat{\varphi}$ l'élément de A_k qui, à tout élément v de K^m, associe : $\hat{\varphi}(v) = (\varphi \mid \chi_v)$.

Établir que, pout tout élément φ de A_k,

(1) $$\varphi = \frac{1}{2^m} \sum_{v \in K^m} \hat{\varphi}(v)\, \chi_v.$$

(2) $$(\hat{\varphi} \mid \hat{\varphi}) = 2^m (\varphi \mid \varphi).$$

(3) $$\hat{\hat{\varphi}} = 2^m \varphi.$$

Soit enfin $\mathcal{F}$ l'endomorphisme de A_k qui, à tout élément φ, associe $\frac{1}{2^{m/2}}\, \hat{\varphi}$. Énoncer les propriétés de $\mathcal{F}$ traduisant les relations (2) et (3). Déterminer l'image par $\mathcal{F}$ de la base $\left(\frac{1}{2^{m/2}}\, \chi_v\right)$.

Tournez la page S. V. P.

4. *Application au décodage.*

À toute fonction f de F_k on associe la fonction φ_f de K^m dans $\mathbb{R}$ définie par $\varphi_f(w) = (-1)^{f(w)}$.

a. Montrer que, pour tout i compris entre 1 et m, il existe un élément unique v de K^m que l'on déterminera tel que $\varphi_{V_i} = \chi_v$. En déduire $\widehat{\varphi_{V_i}}$. Déterminer enfin $\widehat{\varphi_U}$.

b. Montrer que, pour tout élément $v = (v_1, v_2, \ldots v_m)$ de K^m et tout élément f de F_k, $\varphi_f(v)$ est égal au nombre de composantes nulles de la fonction $f + \sum_{i=1}^{m} v_i V_i$ sur la base b_{F_k} diminué du nombre de ses composantes non nulles sur cette base.

En conclure que :

$$\Delta\left(f, \sum_{i=1}^{m} v_i V_i\right) = \frac{1}{2}\left(2^m - \widehat{\varphi}_f(v)\right).$$

Par un calcul analogue montrer que :

$$\Delta\left(f, U + \sum_{i=1}^{m} v_i V_i\right) = \frac{1}{2}\left(2^m + \widehat{\varphi}_f(v)\right).$$

c. Reprenons l'exemple où $m = 3$.

Soit f la fonction qui sur la base $(f_0, f_1, \ldots, f_7)$ admet (0, 0, 1, 1, 1, 1, 1, 0) pour composantes.

Calculer pour chaque élément v de K^3 la valeur de $\widehat{\varphi}_f(v)$.

En déduire l'élément x de C_4 le plus proche de f au sens de la distance Δ.

Déterminer l'élément u de E_4 tel que $g_4(u) = x$.

• • •
•