DEA MDFI

Mars 2001

CODAGE

Exercice 1

On considère un code linéaire C de longueur n et de dimension k sur le corps fini $\mathbf{F}_q$.

Soit $\mathcal{M}$ une matrice dont les lignes sont tous les mots non nuls de C.

1) Calculer le nombre de composantes nulles dans chaque colonne de $\mathcal{M}$ (Utiliser la description des mots de C au moyen des colonnes d'une matrice génératrice de C).

2) En déduire le nombre

$$S = \sum_{x \in C} w(x)$$

où $w(x)$ désige le poids de x.

3) Utiliser le résultat précédent pour trouver une borne supérieure sur le poids minimum de C et donc sur la capacité de correction de C.

4) (Question supplémentaire) Trouver, en utilisant le résultat de 2), tous les codes linéaires C sur $\mathbf{F}_2$ vérifiant les propriétés suivantes :

- Le poids minimum du code orthogonal de C est au moins 3.
- Tous les mots non nuls de C ont le même poids.

Exercice 2

Constuire un code cyclique de longueur 8 sur $\mathbf{F}_3$ corrigeant 2 erreurs et permettant de coder 20 messages.

Fournitures demandées :

- Une matrice génératrice.
- Une matrice de contrôle.

On pourra utiliser le polynôme $x^2 + x + 2$ qui est un polynôme irréductible sur $\mathbf{F}_3$ et primitif.

Exercice 3

Soit m un entier pair, $m = 2t$. On note xy le produit scalaire usuel des deux vecteurs x et y de $\mathbf{F}_2^m$:

$$xy = \sum_{i=1}^{m} x_i y_i,$$

et on écrit $x \perp y$ lorsque $xy = 0$. Pour mémoire, le coefficient de Fourier d'une fonction booléenne f en un point a de $\mathbf{F}_2^m$ vaut

$$\hat{f}(a) = \sum_{x \in \mathbf{F}_2^m} (-1)^{f(x)+a.x}.$$

Une fonction boolénne est dite courbe si tous ses coefficients de Fourier sont de module 2^t. On remarque que si f est courbe alors il existe une fonction booléenne $\tilde{f}$ tel que $\hat{f}(a) = (-1)^{\tilde{f}(a)} 2^t$.

(1) Montrer que $f \mapsto \tilde{f}$ est une involution de l'ensemble des fonctions courbes.
(2) Soit $q(x)$ la forme quadratique $q(x) = \sum_{i=1}^{t} x_i x_{t+i}$. Montrer par un calcul direct de $\hat{q}(a)$ que q est courbe, et préciser la fonction $\tilde{q}$.
(3) Soit g une fonction arbitraire de t variables. Montrer que la fonction booléenne $f \colon x \mapsto q(x) + g(x_1, \ldots, x_t)$ est courbe. Calculer $\tilde{g}$.
(4) Déduire de (3) que pour tout entier $2 \leq s \leq t$, il existe une fonction courbe de degré t.
(5) Soit f une fonction booléenne, v un vecteur de $\mathbf{F}_2^m$ et S un sous-espace vectoriel de dimension k dans $\mathbf{F}_2^m$. Établir la relation

$$2^k \sum_{a \perp S} \hat{f}(a)(-1)^{av} = 2^m \sum_{s \in S} (-1)^{f(s+v)}$$

(6) Montrer que si f est courbe alors le poids de la restriction de f à l'espace affine $v+S$ est pair dès que la codimension de S est inférieure ou égale à t.
(7) Soit f une fonction de degré strictement supérieur à t. Montrer qu'il existe un sous-espace affine V de codimension t tel que la restriction de f à soit de poids impair.
(8) On dit qu'une fonction booléenne f est d'indice r s'il existe un sous-espace affine de dimension r sur lequel f est constante et si r est le plus grand entier satisfaisant à cette propriété.
(9) Montrer que l'indice d'une fonction courbe est au plus t.
(x) Calculer l'indice de la forme quadratique $q(x)$.