codes correcteurs

DEA MDFI, Mars 2003.
aucun document autorisé,
durée : 3 heures.

Il est demandé de traiter trois des quatre exercices. Vous avez le choix entre les exercices II et III mais les exercices I et IV sont obligatoires.

I. DÉFINITIONS ET NOTATIONS

Soit n un entier non nul. Tous les codes considérés sont binaires et linéaires. Les notations sont usuelles : $\mathbf{F}_2$ désigne le corps à deux éléments, d_H la métrique de l'espace de Hamming $\mathbf{F}_2^n$, $V_n(r)$ le cardinal d'une boule rayon r, et $B_n(x,r)$ la boule de centre x et rayon r :

$$B_n(x,r) = \{y \in C \mid \mathrm{d}_H(x,y) \leq r\}.$$

Soit C un code de longueur n. On définit la distance d'un mot $x \in \mathbf{F}_2^n$ au code C par

$$d(x,C) = \min_{c \in C} \mathrm{d}_H(x,c)$$

Le *rayon de recouvrement* de C est égal au plus petit entier r tel que l'union des boules de rayon r centrées sur des mots de C recouvre $\mathbf{F}_2^n$. Autrement dit, le rayon de recouvrement de C est égal à

$$\max_{x \in \mathbf{F}_2^n} d(x,C).$$

On rappelle que, si n est impair, on sait construire un code cyclique t-correcteur de longueur n pour tout entier t vérifiant $2t+1 \leq n$, c'est un code $\mathrm{BCH}(t,n)$. Une fois fixé un élément d'ordre n dans une certaine extension L de $\mathbf{F}_2$, on peut prendre l'idéal des polynôme $P(X) \in \mathbf{F}_2[X]/(X^n-1)$ tels que

$$\forall i, \quad 1 \leq i \leq 2t \Leftrightarrow \quad P(\beta^i) = 0.$$

Dans la suite, les entiers $\rho(t,n)$ et $\delta(t,n)$ désigneront respectivement le rayon de recouvrement et la distance minimale du code $\mathrm{BCH}(t,n)$. Quand n est de la forme 2^f-1, le code BCH est dit *primitif*.

On suppose n impair.

[1] Combien y-a-il de codes $\mathrm{BCH}(1,n)$?

[2] Montrer que la distance minimale d'un code BCH primitif 1-correcteur est exactement égale à 3.

[3] Comparer au sens de l'inclusion les codes $\mathrm{BCH}(t,n)$ et $\mathrm{BCH}(t-1,n)$. L'inclusion n'est pas toujours stricte. Donner un exemple d'égalité.

[4] Donner une condition nécessaire et suffisante pour que l'inclusion soit stricte dans le cas particulier $t=2$.

II. RAYON DES CODES BCH

On suppose toujours que n est impair. On considère un $[n,k]$-code C de capacité de correction e et de rayon de recouvrement ρ.

[5] Comparer les ensembles $\mathbf{F}_2^n$, $\bigcup_{c \in C} B(c,\rho)$ et $\bigcup_{c \in C} B(c,e)$ pour obtenir $e \leq \rho$. Traduire cette relation dans le cadre des codes BCH.

[6] Montrer que si C est strictement inclus dans un code C' de distance minimale d alors $d \leq \rho$.

[7] Montrer que si les codes $\mathrm{BCH}(t,n)$ et $\mathrm{BCH}(t-1,n)$ sont distincts alors $\delta(t-1,n) \leq \rho(t,n)$.

Les BCH sont primitifs.

[8] Soit $R \in \mathbf{F}_2[X]/(X^n-1)$. Soit $(u,v) \in L^2$ le "syndrôme" de R par rapport au code BCH 2-correcteur. Par définition, $u = R(\beta)$ et $v = R(\beta^3)$. Montrer que $d(R, \mathrm{BCH}(2,n)) \leq 3$ implique l'existence de trois éléments x, y, z dans L tels que

$$\begin{cases} x+y+z = \alpha \\ x^3+y^3+z^3 = \beta \end{cases} \tag{1}$$

[9] Quelque soit $w \in L$, 'équation $XY(X+Y) = w$ admet au moins une solution dans L^2. Prouver cette affirmation.

Indication: dénombrer les polynômes irréductibles de degré 2.

[10] Montrer que le système (**??**) admet toujours des solutions.

Indication: $X = x+u$, $Y = y+u$ *et* $Z = z+u$.

[11] Montrer que le rayon de recouvrement du code BCH primitif 2-correcteur est inférieur ou égal à 3. Est-il égal à 2 ?

III. ISOMÉTRIE

On note μ le caractère additif non trivial du corps $\mathbf{F}_2$. Soit C un code de longueur n. Une application de C dans C qui conserve les distances est une *isométrie* de C. Les isométries de C forment un groupe et nous noterons $\mathrm{aut}(C)$ le sous groupe des isométries **linéaires**.

[12] Soit π une permutation de $\{1,2,\ldots,\}$. Vérifier que l'application $\tilde{\pi}\colon x \mapsto x^\pi = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$ est une isométrie linéaire de $\mathbf{F}_2^n$.

[13] Soit f une isométrie de $\mathbf{F}_2^n$. Montrer que si $f(0) = 0$ alors f est une permutation linéaire du type ci-dessus. Caractériser toutes les isoméries de $\mathbf{F}_2^n$.

[14] Pour $i \in \{1, 2, \ldots, n\}$, on note π_i la i-e forme coordinnée i.e. la forme qui envoie x sur x_i. Exprimer le poids de x en fonction des caractères $\mu \circ \pi_i$.

[15] Soit $f \in \mathrm{aut}(C)$ une isométrie linéaire du code C. Utiliser la relation obtenue dans la question précédente et le lemme de Dedekind (indépendance des caractères) pour montrer que : quelque soit $i \in \{1, 2, \ldots, n\}$, il existe $j \in \{1, 2, \ldots, n\}$ tel que $\mu \circ \pi_i \circ f = \mu \circ \pi_j$.

[16] Déduire de ce qui précède relèvement de $\mathrm{aut}(C)$ dans $\mathrm{aut}(\mathbf{F}_2^n)$, c'est-à-dire un morphisme surjectif

$$\mathrm{aut}(\mathbf{F}_2^n) \longrightarrow \mathrm{aut}(C) \longrightarrow 1$$

IV. Moment des poids

L'espace des applications de $\mathbf{F}_2^n$ dans le corps des nombres réels est muni du produit usuel des fonctions et du produit de convolution noté $*$.

$$f * g(v) = \sum_{x+y=v} f(x)g(y)$$

Pour un entier k et une fonction f, on note $f^{[k]}$ la k-e puissance convolutionnelle de f :

$$f^{[k]} = \underbrace{f * f * \ldots f}_{k \text{ termes}}$$

On identifie $\mathbf{F}_2^n$ avec son dual, de sorte que le coefficient de Fourier de f en v soit :

$$\hat{f}(v) = \sum_{x \in \mathbf{F}_2^n} f(x)\mu(vx).$$

On note σ la fonction indicatrice de la sphère unité :

$$\sigma(x) = \begin{cases} 1, & \text{si } \mathrm{wt}(x) = 1; \\ 0, & \text{sinon.} \end{cases}$$

où $\mathrm{wt}(x)$ désigne le poids de Hamming de x.

[17] Calculer $\sigma^{[2]}(0)$, $\sigma^{[4]}(0)$.

[18] Quelle est la signification combinatoire de $\sigma^{[k]}(y)$?

[19] Calculer le coefficient de Fourier de $f * g$ en fonction de ceux de f et g. Inversement, exprimer le coefficient de Fourier de fg à partir d'un produit de convolution.

[20] Calculer la transformée de Fourier de la fonction $c(x) := 2\mathrm{wt}(x) - n$ en fonction de σ.

[21] Soit k un entier. Utiliser la formule de Poisson pour calculer:

$$\frac{1}{|C|} \sum_{x \in z+C} c(x)^k$$