codes correcteurs

DESS SSI, février 2003.
Tous documents autorisés,
durée : 3 heures.

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

[1] Quelle est la signification des lettres "B", "C" et "H" ?

[2] Quelle relation vérifient t et $\delta(t,n)$?

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

[4] Comparer au sens de l'inclusion les codes $\textsc{bch}(t,n)$ et $\textsc{bch}(t-1,n)$.

[5] L'inclusion n'est pas toujours stricte. Donner un exemple d'égalité.

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

II. RAYON DES CODES BCH

Soit C un $[n,k]$ code de capacité de correction e et de rayon de recouvrement ρ.

[7†] Comparer les ensembles $\mathbf{F}_2^n$, $\bigcup_{c \in C} B(c,\rho)$ et $\bigcup_{c \in C} B(c,e)$.

[8†] Etablir la relation :

$$V_n(e) \leq 2^{n-k} \leq V_n(\rho).$$

[9] Déduire de ce qui précède une relation entre e et ρ. Traduire cette relation dans le cadre des codes BCH.

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

[11] On suppose les codes $\textsc{bch}(t,n)$ et $\textsc{bch}(t-1,n)$ distincts. Montrer que :

$$\delta(t-1,n) \leq \rho(t,n)$$

Commmenter les réponses des questions [9] et [11].

III. CYCLOTOMIE

Soit K le corps à 32 éléments.

[12] Dresser la liste des classes cyclotomiques modulo 31.

[13‡] Tout polynôme irréductible de degré 5 est primitif. Justifier cette affirmation.

[14†] Prouver l'irréductibilité de $\pi(X) = X^5 + X^2 + 1$.

[15] Soit β une des racines de $\pi(X)$. Déterminer le polynôme minimal de β^{-1}.

[16] Déterminer les racines du polynôme

$$\lambda(X) = X^6 + X^5 + X^3 + X^2 + X + 1.$$

IV. DÉCODAGE

On note $g(X)$ le générateur du code $\textsc{bch}(7,31)$.

[17†] Déterminer le quotient $h(X) = (X^{31}+1)/g(X)$.

[18] Calculer $g(X)$.

[19] Donner une matrice de contrôle du BCH 7 correcteur.

[20‡] On note $R(X)$ un mot reçu. Déterminer le polynôme localisateur d'erreur sachant que

$$R(\beta) = R(\beta^3) = 1, \quad \text{et} \quad R(\beta^5) = R(\beta^7) = R(\beta^{11}) = 0.$$

[21] Quelles erreurs ont affecté le mot transmis?