DESS, Codage.

lundi 15 février 2004

La précision et la clarté de votre rédaction sont *fondamentales*. Cours et TD sont autorisés. Durée 3h00. Le barème indiqué est *approximatif*.

Exercice 1. [3 pts] Dans $\mathbf{F}_2[X]$, l'anneau des polynômes à coefficients dans le corps à deux éléments.

1. [2pt] Construire une registre à décalage qui réalise la division d'un polynôme $a(X) = a_0 + a_1X + \ldots + a_nX^n$ par le polynôme $X^3 + X^1 + 1$.

2. [1pt] Utiliser ce registre pour obtenir le reste de la division de $X^2 + X^4 + X^5$ par $X^3 + X^1 + 1$.

Exercice 2. [7 pts] Un système de Steiner $2-(v,3)$ est la donnée d'un ensemble X de cardinal v et d'un ensemble de triples (parties à trois éléments) T_1, T_2, ..., T_r tels que toute paire de points soit incluse dans un et un seul triple. On rappelle que le support d'un mot binaire x de longueur n est $\{i \mid x_i = 1\}$.

1. [1pt] Montrer que l'existence d'un sustème de Steiner implique

$$r = \frac{v(v-1)}{6}$$

2. [1pt] Donner une définition d'un code parfait e-correcteur.

3. [1pt] Montrer que les supports des mots de poids trois d'un code parfait 1-correcteur forment une système de Steiner.

4. [1pt] Déterminer de deux façons différentes le nombre de mots poids minimaux du code de Hamming de longueur $2^s - 1$.

5. [1pt] Construire un système de Steiner pour l'ensemble $X = \{1, 2, \ldots, 7\}$.

6. [1pt] L'ensemble des triples obtenus possède une propriété géométrique remarquable. Laquelle ? Faire une représentation graphique.

7. [1pt] Construire un système de Steiner pour l'ensemble $X = \{1, 2, \ldots, 7\}$.

Exercice 3. [6 pts]

L'étendu d'un code linéaire binaire $C[n,k]$ est égal à l'ensemble, noté $\hat{C}$, des mots de longueur $n+1$ obtenus en ajoutant un bit de parité sur chacun des mots de C. En d'autres termes,

$$(c_1, c_2, \ldots, c_n, c_\infty) \in \hat{C} \Longleftrightarrow (c_1, c_2, \ldots, c_n) \in C \quad \sum_{i=1}^{n} c_i = c_\infty$$

1. [1pt] L'étendu de C est linéaire. Pourquoi ? Quelle est la dimension de $\hat{C}$?

2. [1pt] Comparer les distances minimales d'un code et de son étendu.

3. [1pt] Donner une condition nécessaire et suffisante pour que les codes C et $\hat{C}$ n'aient pas la même distance minimale.

4. [1pt] Donner un mot non nul de l'orthogonal de $\hat{C}$.

5. [1pt] Préciser les dimensions des matrices de contrôles de C et $\hat{C}$. Comment construire une matrice de de contrôle de $\hat{C}$ à partir d'une matrice de contrôle H de de C ?

6. [1pt] Construire un code de paramètre $[8, 4, 4]$. Quelle est sa capacité de correction ? S'agit il d'un code parfait ?

Exercice 4. [5 pts]

Soient $C[n, k_1, d_1]$ et $D[n, k_2, d_2]$ deux codes binaires. On suppose que D est inclus dans C et on construit l'ensemble $C \mid C + D$ des mots de la forme

$$(u_1, u_2, \ldots, u_n, u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)$$

avec $u \in C$ et $v \in D$.

1. [1pt] Montrer que l'ensemble $C \mid C + D$ est un code linéaire.

2. [1pt] Préciser sa dimension.

3. [2pt] Montrer que la distance minimale de $C \mid C + D$ est plus grande que $\min(2d_1, d_2)$.

4. [1pt] Construire un code binaire $[16, 5, 8]$.

Exercice 5. [8 pts] Soit v un nombre premier impair. Soit β une racine d'ordre v dans une extension convenable de $\mathbf{F}_2$. On note R le groupe des résidus quadratiques modulo v et N l'ensemble des non résidus.

1. [1pt] Déterminer R et N pour $v = 17$. Décrire la décomposition en facteurs irréductible de $X^{17} + 1$.

2. [1pt] Rappeler la définition du code résidu quadratique binaire de longueur v définit par la racine

3. [1pt] Soit $E(X) = \sum_{r \in R} X^r$. Montrer E est un idempotent, c'est-à-dire que

$$E^2(X) \equiv E(X) \mod X^v - 1.$$

4. [1pt] Montrer que si γ est une racine v-ième alors $E(\gamma) = 0$ ou bien $E(\gamma) = 1$.

5. [1pt] Soit $E(X) = \sum_{r \in R} X^r$. Montrer si $n \in N$ alors

$$1 + E(X) + E(X^n) \equiv 1 + X + \ldots + X^{v-1} \mod X^v - 1$$

En déduire qu'il existe une racine γ d'ordre v telle que $E(\gamma) = 0$.

6. [1pt] On suppose que $E(\beta) = 0$. Calculer le PGCD de $X^{17} + 1$ et de $E(X)$.

7. [1pt] En déduire un facteur irréductible de degré 8 de $X^{17} + 1$.

8. [1pt] Montrer que le RQ-code de longueur 17 est un $[17, 9, 5]$.