Devoir GI 3ème année - Mercredi 9 juin - 8h-10h

Exercice

Réduction d'une matrice en changeant l'ordre des indices

1) Soit G le graphe associé à la matrice A :

$$A = \begin{pmatrix} 8 & 6 & 0 & 0 & 4 & 0 \\ 8 & 6 & 0 & 0 & 2 & 0 \\ 0 & 0 & 3 & 0 & 9 & 0 \\ 7 & 1 & 1 & 4 & 0 & 5 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 2 & 2 & 4 & 5 & 7 \end{pmatrix}$$

c'est à dire le graphe simple dont les sommets sont les indices $i = 1, 2, 3, 4, 5, 6$ avec un arc de i vers j si et seulement si le coefficient a_{ij} est non nul. Représenter G par un dessin.
2) Répartir les 6 indices par composantes fortement connexes de G ; déterminer son graphe réduit R. Répartir les composantes par niveaux de R et tracer le graphe des niveaux.
3) Déduire une matrice de permutation Q telle que $Q^t AQ$ soit diagonale par blocs ; calculer $Q^t AQ$.

Problème

Construction du code de Hamming de longueur 7 : 1ère méthode

On se place dans $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. Soit C le code de matrice génératrice

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

et soit H la matrice suivante

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

Rappel : C est formé des mots binaires $Y = (y_1 y_2 .. y_7)$ de longueur 7 à coefficients dans $\mathbb{Z}_2$ pour lesquels $HY^T = 0$.

1) Vérifier que H est bien une matrice de contrôle du code. Montrer que H est de rang plein. Préciser l'image de l'application linéaire qui à Y associe

HY^T. Calculer la dimension de C et son cardinal.
2) Montrer que deux colonnes quelconques de H sont linéairement indépendantes, en déduire que C permet de corriger une erreur et que d la distance minimale du code est ≥ 3. C peut-il corriger 2 erreurs ?
Montrer que C contient des mots de poids 3 et en déduire que $d = 3$.
3) Calculer la dimension et le cardinal de l'ensemble C^+ des mots pairs de C. Déterminer une matrice de vérification de parité pour C^+. Que peut-on dire des distances minimales des codes C et C^+ ? Ces codes permettent-ils de détecter deux erreurs ?
4) Supposons que l'on reçoit $c^\star = (0100001)$. Corriger $c^\star$ en supposant que l'on fait au plus une erreur lors de la transmission.
5) Ce code est-il parfait ?

Construction du code de Hamming de longueur 7 : 2ème méthode

Soit C un code linéaire de longueur n. On dit que ce code est **cyclique** si, quel que soit l'élément du code $(c_1..c_n) \in C$, $(c_n c_1..c_{n-1})$ appartient aussi à C.

0) Le code précédent est-il cyclique ?

On identifie un code linéaire C de longueur n à un sous-ensemble de $\mathbb{Z}_2[X]/(X^n-1)$ de la manière suivante : à chaque élément de C, $(c_0..c_{n-1})$, on associe la classe du polynôme $c_0+c_1X+..+c_{n-1}X^{n-1}$ dans $\mathbb{Z}_2[X]/(X^n-1)$. On notera C l'image de C par ce plongement, confondant ainsi un élément du code avec le polynôme qui lui est associé. On peut alors utiliser la structure d'anneau de $\mathbb{Z}_2[X]/(X^n-1)$ pour caractériser un code cyclique. En effet, on la proposition suivante :

Proposition 0.1 *: Un code linéaire C de longueur n est cyclique ssi le sous-espace vectoriel qu'il constitue est un idéal de $\mathbb{Z}_2[X]/(X^n-1)$.*

Un code cyclique de longueur n est donc un idéal de $\mathbb{Z}_2[X]/(X^n-1)$ et on peut montrer qu'il est parfaitement déterminé par la donnée d'un générateur de cet idéal. Dans ce cas, soit g son générateur, supposé de degré r ; il correspond au polynôme non nul de plus petit degré contenu dans C. Alors le code est de dimension $n-r$, tout élément du code correspond à un multiple de g modulo (X^n-1) et une base du code sera $\{g, gX, .., X^{n-r-1}g\}$.
Combien peut-on espérer corriger d'erreurs avec un tel code et comment ? La connaissance des racines du générateur va nous permettre de répondre dans certains cas. C'est le propos du résultat suivant :

Proposition 0.2 *Soit α un élément primitif d'un corps $\mathbb{K}$ et g le générateur du code cyclique C. Si g possède parmi ses racines dans ce corps les éléments α^a, α^{a+1}, .., α^{a+b-2}, alors la distance minimale du code est supérieure ou*

égale à b.

Le but de ce problème est de construire un code cyclique, code de BCH de longueur $n = 7$, de dimension 4 et 2-correcteur. Le principe est donc le suivant : on choisit un polynôme g qui va engendrer un idéal et donc un code vérifiant les propriétés requises.

1) Montrer que $P = X^3 + X + 1$ est un polynôme irréductible sur $\mathbb{Z}_2[X]$.
On se place maintenant dans $\mathbb{K} = \mathbb{Z}_2[X]/(X^3 + X + 1)$. C'est un corps à 2^3=8 éléments, engendré par la classe de X que l'on notera α. α est racine de P.
2) Donner une base de $\mathbb{K}$ et la table des puissances successives de α. En déduire une représentation de $\mathbb{K}$ sous forme d'un ensemble des puissances successives d'un générateur.
3) Montrer que puisque l'on travaille dans $\mathbb{Z}_2[X]$, si α est racine d'un polynôme m alors α^2 est aussi racine de ce polynôme.
On cherche maintenant un polynôme g diviseur de $X^7 - 1$ et de racine α.
4) Déduire de la question précédente que g a pour racines α, et α^2.
Posons alors $g = X^3+X+1$. Le code construit est alors l'idéal de $\mathbb{Z}_2[X]/(X^7-1)$ engendré par g.
5) Vérifier grâce à la proposition 0.2 que sa distance minimale est supérieure à 3 et qu'il corrigera 1 erreur.

On veut construire une matrice de contrôle du code. Nous allons procéder de la manière suivante : soient $\rho_1, .., \rho_3$ les racines de g dans un corps de décomposition. (Le corps de décomposition est un corps plus gros que $\mathbb{K}$ et le contenant.)

6) Soit $c = (c_0..c_{n-1})$ un mot du code. En identifiant c est son polynôme associé, vérifier que l'on a l'équivalence

$$c \in C \Leftrightarrow g|c \Leftrightarrow \forall i = 1..3,\ c(\rho_i) = 0$$

Soit

$$H = \begin{pmatrix} 1 & \rho_1 & .. & \rho_1^6 \\ 1 & \rho_2 & .. & \rho_2^6 \\ 1 & \rho_3 & .. & \rho_3^6 \end{pmatrix}$$

On dit que H est la **matrice de Vandermonde** associée à $(\rho_1, .., \rho_3)$.
7) Vérifier que

$$c \in C \Leftrightarrow H \begin{pmatrix} c_0 \\ c_1 \\ .. \\ c_{n-1} \end{pmatrix} = 0$$

8) Que peut-on en déduire pour la matrice H ?