EXERCICES NUMÉRIQUES SUR LA PARTIE CODAGE DU MODULE DE THORIE DE L'INFORMATION

PHILIPPE LANGEVIN

Traitez un sujet au choix, rédigez vos résultats sans dépasser 4 pages simples au format A4. La clarté des réponses, la qualité de la rédaction et l'originalité du contenu seront prises en considérations pour l'évaluation. Vous devez remettre vos solutions avant le 15 Avril 2006.

1. Matrices Aléatoires

(1) Analyser le résultat renvoyé par un énumérateur de poids quand on lui applique une matrice $k \times n$ ($k \leq n$) de rang strictement inférieur à k.
(2) Modifier un énumérateur de poids pour calculer le rang d'une matrice binaire.
(3) Calculer le rang d'un échantillon de matrices binaires aléatoires de 6 lignes et 32 colonnes. Sur la base de votre expérience, estimez la probabilité d'obtenir une matrice de rang 0, 1, 2, 3, 5, et 6.
(4) Comparer ces estimations avec des résultats théoriques sur le nombre de matrices binaires de rang r que vous trouverez dans la littérature classique ou électronique.

2. Codes Aléatoires

On rappelle que deux codes $[n, k]$ sont équivalents si la matrice de l'un peut être obtenue à partir de celle de l'autre par des permutations de colonnes et des combinaisons linéaires de lignes.

On dit qu'un $[n, k]$-code est normal s'il possède une matrice génératrice de la forme $(I_k A)$ où I_k est la matrice identité $k\times$ et A une matrice $k \times (n-k)$.

(1) Que peut-on dire de la distribution des poids de deux codes équivalents ?
(2) Ecrire une fonction pour construire une matrice normale aléatoire $k \times n$.
(3) Calculer la distribution de poids d'un échantillon de codes binaires normaux 12×24.
(4) Faire une représentation graphique de la distribution de poids moyenne.
(5) Que remarquez vous ?

3. Recherche de mots de petits poids

Soit C un $[n, k]$-code binaire normal dont une matrice génératrice est $G = (I_k A)$ où I_k est la matrice identité $k \times k$ et A une matrice $k \times (n - k)$.

(1) Montrer que si $c \in C$ désigne un mot de poids $w \leq k$ alors c est une combinaison linéaire d'au plus w lignes de G.
(2) Ecrire un programme pour rechercher les mots de poids plus petit que 3 dans un code binaire normal.
(3) Quelle est la complexité de votre algorithme ?
(4) Soit $t \leq k$. Ecrire un programme pour rechercher les mots de poids plus petit que t dans un code binaire normal.
(5) Quelle est la complexité de votre algorithme ?

4. Codes de Gray

On généralise la notion de code de Gray binaire. Soient m et q deux entiers supérieurs à 1 strictement. Un code de Gray q-aire d'ordre m est énumération des q^m mots q-aire de longueur m : $x_1, x_2, \ldots, x_{q^m}$ telle que deux mots conséxcutifs sont distants de 1 au sens de la distance de Hamming.

(1) Comment peut-on construire un code de Gray d'ordre m à partir d'un code de Gray d'ordre $m - 1$?
(2) Ecrire un programme pour construire un code de Gray ternaire d'ordre m.

5. Construction de bons codes

On note $V(n, d)$ le nombre de mots binaires de poids inférieur ou égal d à dans l'espace de Hamming de $\mathbf{F}_2^n$. Un code C est dit maximal lorsque sa distance minimale est plus grande que celle de tous les codes qui le contiennent. En d'autres termes les boules de rayons $d - 1$ centrées sur les mots de C recouvre l'espace de Hamming tout entier et donc

$$2^n \leq V(n, d-1)\, 2^k \tag{1}$$

Soient n, k et d trois entiers. On démontre sans difficulté que si $2^{n-k} > V(n, d - 1)$ alors il existe un $[n, k, d]$ code.

(1) Ecrire une fonction pour calculer $V(n, d)$.
(2) Ecrire un programme pour construire un code aléatoire vérifiant (1).
(3) Donner quelques résultats numériques.

6. Approximation d'une source

Traiter la question 3 du TP 2.