TD : Codes-correcteurs

Christophe Ritzenthaler

Codes non linéaires

1. *Calculer la distance de Hamming entre* (1001001) *et* (1011100).

2. On considère le code binaire

$$C = \{(0000101), (0011101), (1111100), (1111111), (0101011)\}.$$

On suppose que la probabilité d'erreur de transmission pour chaque symbole est $p = 1/4$. Si $r = (1101001)$ et $s = (0110101)$ sont transmis, *décoder* r *et* s *selon le principe de maximum de vraisemblance.*

3. Soit A un alphabet à q symboles. On pose

$$A_q(n, d) = \sup\{\#C, C \subset A^n, d(C) = d\}.$$

Montrer que $A_q(n, 1) = q^n$ *et* $A_q(n, n) = q$.

Codes linéaires

1. Soit C le code engendré par la matrice

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

   (a) *Déterminer le nombre de mots de code de* C.

   (b) *Calculer une matrice de contrôle.*

   (c) *Calculer la distance de* C.

   (d) *Déterminer le nombre d'erreurs que* C *peut corriger.*

2. Soit C le code de matrice de contrôle

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

(a) *Donner une matrice génératrice pour C.*

(b) *Décoder par syndrome $r = (11101)$ et $s = (11011)$.*

3. Soit C un code binaire de type $[n, k, d]$.

   (a) Soit s la moitié de la somme des distances entre deux mots distincts de C. *Montrer que $s \geq \binom{2^k}{2} d$.*

   (b) On place les mots de code de C en ligne dans une matrice A. Soit x_i le nombre de 1 dans la colonne i de A. *Montrer que $s = \sum_{i=1}^{n} x_i(2^k - x_i)$.*

   (c) *Montrer que (borne de Plotkin)*

$$d \leq \frac{n2^{k-1}}{2^k - 1}.$$

Codes de Hamming

On appelle *code de Hamming* de paramètre $r \geq 2$ un code binaire de longueur $2^r - 1$ ayant pour matrice de contrôle une matrice $H(r)$ de r lignes et $2^r - 1$ colonnes dont toutes les colonnes sont distinctes et non nulle.
A équivalence près on peut supposer que la i-ème colonne de $H(r)$ représente l'écriture binaire de l'entier i.

1. *Construire $H(2)$ et $H(3)$.*

2. *Donner une matrice génératrice pour ces codes.*

3. *Montrer que les codes de Hamming sont de distance* 3.

4. *Montrer que ce sont des codes parfaits, i.e. l'union des boules de centre les mots du code et de rayon e (ici $e = 1$) est égale à $\{0, 1\}^{2^r-1}$.*

Ces codes sont très faciles à décoder. *Montrer qu'on peut toujours choisir pour leaders les mots ayant un seul* 1 *à la place i pour les 2^r classes.*

Codes BCH

On considère un code BCH de longueur $2^r - 1$ et de distance prescrite 3. *Montrer que son polynôme générateur est le polynôme minimal de α sur $\mathbb{F}_2$ (pour α une racine primitive $2^r - 1$-ème de l'unité). En déduire que la dimension du code est $2^r - 1 - r$ est que ce code est équivalent au code de Hamming $H(r)$.*

Remarque 1. *Plus généralement les codes BCH peuvent s'interpréter comme des sous-codes de Hamming : on rajoute des conditions (i.e. des lignes à la matrice de contrôle) qui ont pour effet de diminuer la dimension du code, mais d'augmenter la distance.*