TD. Codes correcteurs

1 Concepts fondamentaux

1. Si on expédie des bits sur un canal binaire symétrique à raison de 512 bits toutes les millisecondes, avec une probabilité d'erreur de 1%, quel est le nombre de bits faux expédiés au bout de 3h ? (*on assimilera probabilité et fréquence*).
   Solution : $512.10^3.3600.3 = 5529600000$ bits envoyés en 3 heures. On a donc $55296000/100 = 55296000$ bits erronés.

2. Dans un code de dimension k, et de longueur n, combien faut-il connaître de bits pour définir le codage ?
   Solution : Il faut donner le mot de code de taille n pour chaque mot de longueur k. Il faut donc $n2^k$ bits.

3. Dans le cas où $k = 2$ et $r = 1$, faire la liste de tous les codages systématiques possibles.
   Solution : Il y en a $2^4 = 16$: en prenant les bits de contrôle des 4 mots, de toutes les façons possibles.

4. Les valeurs de r et de k étant fixées, combien y a-t-il de codages systématiques différents ?
   Solution : Pour chaque mot de longueur k on peut ajouter n'importe quel mot de longueur r en tant que bits de contrôle. On a donc 2^k choix à faire et à chaque fois, on peut choisir parmi 2^r. On a donc 2^{r2^k} codages systématiques différents.

5. A partir d'un code $[n, k, d]$, on construit un nouveau code de longueur $n + 1$ en ajoutant le bit 1 à la fin des anciens mots de code. Quelle est la distance minimale de ce nouveau code ?
   Solution : Deux mots qui étaient séparés par la distance d le sont encore : la distance minimale ne change pas.

6. On fabrique un code $[2k, k]$ en collant, à la fin de chaque bloc, le complément du bloc. Quelle est la distance minimale du bloc ?
   Solution : La distance minimale est de 2 car si deux mots sont différents sur un bit, leur complémentaire est différent sur un bit.

7. Dans un code $[5, 2]$, quelle peut être la plus grande valeur de d ? Donner un exemple.
   Solution : Inégalité de Hamming : $C_5^0 + C_5^1 \leq 2^3 < C_5^0 + C_5^1 + C_5^2$ car $6 \leq 8 < 16$. On a donc $t = 1$, donc au mieux $d = 3$. Par exemple, le code dont les mots de code sont 00000, 01101, 10011, 11110]

2 Codes linéaires

1. Soit k quelconque. On code un bloc de k bits en lui ajoutant un bit de contrôle choisi de façon que le nombre de 1 dans le mot de code soit toujours pair. Démontrer que ce code est linéaire. Déterminer sa distance minimale. Permet-il de corriger des erreurs ? Pourquoi ?
   Solution :
   Preuve de linéarité : soient x, y, z trois mots de longueur k tels que $x = y \oplus z$. Si le nombre de 1 dans z et y a la même parité alors x a un nombre pair de 1. En effet, $w(x) = w(y) + w(z) - 2p(x, y)$ où $p(x, y)$ est le nombre de 1 qui sont à la même position dans y et z. Il en suit que le code de x : $\phi(x)$ est égal à $x.0$ qui est bien égal à soit à $y.1 \oplus z.1$ ou bien à $y.1 \oplus z.1$.

   Pour la même raison, si les nombres de 1 ont des parités différentes dans z et y alors x a un nombre impair de 1. Il en suit que le code de x : $\phi(x)$ est égal à $x.1$ qui est bien égal à soit à $y.0 \oplus z.1$, ou bien à $y.1 \oplus z.0$.

   La distance minimale est de 2 car deux mots différents de code ne peuvent être à distance 1. En effet, cela impliquerait que l'un des deux aurait un nombre impair de 1 (poids impair).

   Il est impossible de corriger les erreurs car on ne sait pas où elles se trouvent.

2. Le code à répétition d'ordre n code un bloc de 1 bit en le répétant n fois. Démontrer qu'il s'ait d'un code linéaire. Déterminer sa matrice génératrice, sa matrice de contrôle, son tableau standard, sa liste de syndromes, sa distance minimale.
   Solution :
   Linéarité immédiate car on a que deux mots de code : 0^n et 1^n.
   Matrice génératrice = une matrice ligne constituée de n bits à 1.
   Matrice de contrôle = première colonne a $n - 1$ bits 1 accolée à la matrice unité d'ordre $n - 1$.

Tableau standard : 2 colonnes et 2^{n-1} lignes : dans la première ligne, il y a le mot binaire 0..0, et le mot 1..1. Dans chaque ligne, on trouve côte à côte un mot binaire et son complément.
La distance minimale est n. $p(\text{faux après correction}) = \frac{p^n}{1-(1-p)^n}$

3. On définit un code systématique $[7,4]$ de la façon suivante : si le bloc à coder est $b_1b_2b_3b_4$, alors les bits de contrôles $c_1c_2c_3$ sont tels que :

$$c_1 = b_1 \oplus b_2 \oplus b_3$$
$$c_2 = b_1 \oplus b_2 \oplus b_4$$
$$c_3 = b_1 \oplus b_3 \oplus b_4$$

   (a) Montrer que ce codage est linéaire
   Solution : Il est facile de vérifier que pour ce codage systématique ϕ on a toujours $\phi(x) \oplus \phi(y) = \phi(x \oplus y)$.

   (b) Déterminer sa matrice génératrice, les mots de code et la distance minimale de ce code.

   Solution :
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$
   et $d = 3$

   (c) Que peut-on dire de plus à propos de ce code ?
   Solution : C'est un code de Hamming

4. Déterminer la distance minimale du code défini par la matrice génératrice :
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

   Mots de code = 0000000,1000111,0101011, 0011101, 1101100, 1011010, 0110110, 1110001

   (a) Coder tous les blocs de 3 bits. Quelle est la distance minimale du code ?
   Solution : $d = 4$

   (b) Corriger les messages suivants : 1111100, 0111000, 1110101, 1111101, 1100111, et 0100000
   Solution : On obtient : 1101100, 1110001, 1110001, 0011101, 1000111, 0000000