Codage linéaire

Un codage linéaire est un application linéaire g

$$\begin{array}{rccc} g: & \mathcal{B}^k & \rightarrow & \mathcal{B}^n \\ & m & \rightarrow & g(m) \end{array}$$

Le code $\mathcal{C} = Im(g)$ est un sous espace vectoriel de dimension k de $\mathcal{B}^n$
Le code est injectif : $Ker(g) = \{\vec{0}\}$

- $g(\vec{o}) = \vec{o}$
  Le mot nul est un mot de code
- $\left(\forall m \in \mathcal{B}^k\right)\left(\forall m' \in \mathcal{B}^k\right) g\left(m \oplus m'\right) = g(m) \oplus g(m')$
  La somme de deux mots de codes est un mot de code

Distance d'un code linéaire

étant donne C un mot du code linéaire $\mathcal{C}$, considérons la translation t_C qui a tout mot de code c_1 associe $c_2 = c_1 \oplus C$

$$t_C(\mathcal{C}) = \mathcal{C}$$

- $t_C(\mathcal{C}) \subset \mathcal{C}$ puisque la somme de deux mots de codes est un mot de code
- $\mathcal{C} \subset t_C(\mathcal{C})$ en effet $(\forall c \in \mathcal{C})(c \oplus C) \oplus C = c$. Comme c et C sont deux mots de codes $c \oplus C$ est aussi un mot de code et $t_c(c \oplus C) = c$

la distance d'un code linéaire est égale au poids du mot de code de plus faible poids

cela provient du fait que d_H est invariante par translation.
soit c_1 et c_2 deux mots de codes tels que la distance du code $d = d_H(c_1, c_2)$ alors

$$\begin{array}{rcl} d & = & d_H(c_1, c_2) \\ & = & w(c_1 \oplus c_2) \\ & = & w((c_1 \oplus c_1) \oplus (c_2 + \oplus c_1)) \\ & = & d_H(c_1 \oplus c_1, c_2 \oplus c_1) \\ & = & d_H(\vec{0}, c_2 \oplus c_1) \end{array}$$

Il existe donc un mot de code ($c = c_2 \oplus c_1$) tel que $d = d_H(\vec{0}, c)$

Matrice génératrice d'un code linéaire

soit $\mathcal{E}_k$ et $\mathcal{E}_n$ des bases respectivement de $\mathcal{B}^k$ et $\mathcal{B}^n$
soit m un mots de $\mathcal{B}^k$ et $[m]_{\mathcal{E}_k}$ sa matrice (horizontale) des coordonnées de m la base $\mathcal{E}_k$

la matrice génératrice du code linéaire g est donnée par

$$G = \begin{pmatrix} [g(e_1)]_{\mathcal{E}_n} \\ [g(e_2)]_{\mathcal{E}_n} \\ \cdots \\ [g(e_k)]_{\mathcal{E}_n} \end{pmatrix}$$

Si on note $C_m = g(m)$ alors

$$[C_m]_{\mathcal{E}_n} = [m]_{\mathcal{E}_k} G$$

Matrice génératrice d'un code linéaire : forme systématique

$$g : m_1 m_2 \cdots m_k \longrightarrow C_m = \underbrace{m_1 m_2 \cdots m_k}_{k \text{ bits informatifs}} \mid \underbrace{c_1 c_2 \cdots c_{n-k}}_{n-k \text{ bits de contrôle}}$$

Relativement aux base canoniques la matrice G peut se mettre sous la forme

la matrice génératrice du code linéaire g est donnée par
$$G = \left(I_{kxk} \quad P_{kx(n-k)}\right)$$

la matrice génératrice du code linéaire g est donnée par
$$C_m = mG$$
$$C_m = m|mP$$

exemple :$k = 3$, $n = 6$

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

les mots de code					
bits informatifs			bits de contrôle		
0	0	0	0	0	0
0	0	1	1	1	0
0	1	0	1	0	1
0	1	1	1	1	0
1	0	0	0	1	1
1	0	0	1	0	1
1	1	0	1	1	0
0	1	1	0	0	0

Matrice génératrice d'un code linéaire : forme systématique

Exercice :

1. si on considère $k = 3$ autrement si les message en entrée du codage canal sont de longueur, quelle doit être la longueur minimale des mots de code pour que le code corrige une erreur de façon certaine.
2. soit le code dont la matrice génératrice est

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

   1. quelle est la distance du code, combien d'erreur peut-on être sûr de détecter, de corriger ?
   2. donner la matrice P de parité
   3. comment est codé le message $m = 101$? identifier les parties informative et de parité

Dual d'un code linéaire

Notation : soit $x = x_1 x_2 \cdots x_n$ et $y = y_1 y_2 \cdots y_n$ deux vecteurs de $\mathcal{B}^n$

$$< x, y >= x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n$$

Soit $\mathcal{C}$ un $[n,k]$-code,
$\mathcal{C}^{\perp} = \{x \in \mathcal{B}^n tq \forall c \in \mathcal{C} < x, , c >= 0\}$
est appelé code dual de $\mathcal{C}$

d'après les résultats d'algèbre linéaire

- $\mathcal{C}^{\perp} = \left\{x \in \mathcal{B}^n \ tq \ Gx^t = 0\right\}$
- $dim(\mathcal{C}) = k \Longrightarrow dim\left(\mathcal{C}^{\perp}\right) = n - k$
- $\mathcal{C}^{\perp\perp} = \mathcal{C}$
  $\mathcal{C} = \left\{y \in \mathcal{B}^n tq \ \forall x \in \mathcal{C}^{\perp}, < y, x >= 0\right\}$
  si H est une matrice génératrice du code dual : $\mathcal{C} = \left\{y \in \mathcal{B}^n \ tq \ yH^t = 0\right\}$

Dual d'un code linéaire : Exemple

soit le [7,3]-code de matrice génératrice systématique

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

- recherche de $\mathcal{C}^{\perp}$:
  on cherche les mots $abcdefg \in \mathcal{B}^7$ tel que $G.(abcdefg)^t = 0$. On obtient le système d'équations linéaires homogènes

$$\begin{cases} a \oplus d \oplus e & = & 0 \\ b \oplus e \oplus g & = & 0 \\ c \oplus d \oplus f \oplus g & = & 0 \end{cases}$$

  ce système est de rang 3,prenons a, b, c comme inconnues principales,et d, e, f, g comme paramètres

$$\begin{cases} a & = & d \oplus e \\ b & = & e \oplus g \\ c & = & d \oplus f \oplus g \end{cases}$$

  on a donc

$$\begin{array}{rcl} \mathcal{C}^{\perp} & = & \{(d \oplus e)(e \oplus g)(d \oplus f \oplus g)defg | defg \in \mathcal{B}^4\} \\ & = & \{d(1011000) \oplus e(1100100) \oplus f(0010010) \oplus g(0110001) | defg \in \mathcal{B}^4\} \\ & = & Vec\{1011000; 1100100; 0010010; 0110001\} \end{array}$$

  une matrice génératrice du code dual est

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} P^t & I_4 \end{pmatrix}$$

Dual d'un code linéaire : Exemple

- $\mathcal{C} = \mathcal{C}^{\perp\perp}$ se traduit par la recherche des solutions du système $abcdefg \cdot H^t = 0$

$$\begin{cases} a \oplus c \oplus d & = & 0 \\ a \oplus b \oplus e & = & 0 \\ c \oplus f & = & 0 \\ b \oplus c \oplus g & = & 0 \end{cases}$$

Le code est ainsi défini comme l'intersection d'hyperplans

Matrice de contrôle de parité

Soit G une matrice génératrice d'un $(n,k]$-code linéaire $\mathcal{C}$.
On appelle matrice de contrôle de parité toute matrice H génératrice du code dual $\mathcal{C}^{\perp}$

Une matrice H de contrôle de parité d'un $[n,k]$- code est une matrice $(n-k) \times n$ définie par

$$GH^T = O_{k\times(n-k)}$$

Dans le cas où G est écrite sous forme systématique $G = \begin{pmatrix} I_k & P_{k\times(n-k)} \end{pmatrix}$

$$H = \begin{pmatrix} P^t_{k\times(n-k)} & I_{n-k} \end{pmatrix}$$

un mot $m \in \mathcal{B}^n$ est un mot de code si et seulement si

$$mH^t = 0_{1\times(n-k)}$$

Syndrome

Un codage linéaire est un application linéaire g

$$\begin{array}{rccc} \sigma : & \mathcal{B}^n & \rightarrow & \mathcal{B}^n \\ & & \rightarrow & \sigma(x) = x.H^t \end{array}$$

- σ est linéaire
- $Ker(\sigma) = \mathcal{C}$

Soit $m = i|p$ un mot en sortie de canal .
Son syndrome est

$$\begin{array}{rcl} \sigma(m) & = & i|p \cdot H^T \\ & = & i|p \begin{pmatrix} P \\ I \end{pmatrix} \\ & = & iP \oplus p \end{array}$$

iP est la partie de contrôle du mot de code associé à la partie informative i, p est la partie de contrôle reçue.
Le syndrome de m est donc le vecteur d'erreur de la partie contrôle lorsqu'on suppose la partie informative exacte
Exemple :

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

1. combien y -a-t-il de syndromes ?
2. donner la liste des syndromes des mots de poids 1 .
3. pour les autres syndromes déterminer les mots de plus faible poids dont ils sont le syndrome

Syndrome

syndromes			mots associés				
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	1
0	1	0	0	0	0	1	0
0	1	1	0	1	0	0	0
1	0	0	,0	0	1	0	0
1	0	1	1	0	0	0	0
1	1	0	1	1	0	0	0
1	1	1	1	0	0	1	0