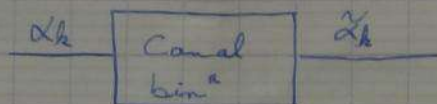


Sujet 5: Codes correcteurs Code de Hamming



$$P_e = \text{Prob}\{x_k \neq x_k'\}$$

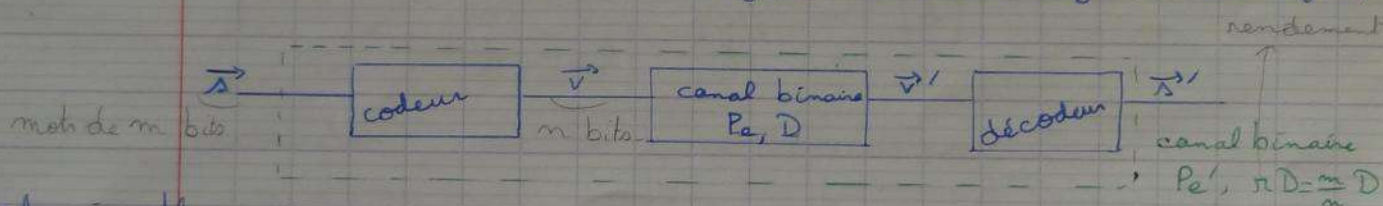
f cours
feuille 3

• Code correcteur :

- corriger ou détecter une erreur en ajoutant de la redondance, donc le débit effectif va diminuer, ainsi que la proba d'erreur. $\hat{A}$ chose qu'avec la valence: $\uparrow$ valence, $\uparrow$ débit bin^a ms avec proba d'erreur
- Procédures $\rightarrow$ BEC - FEC

1. Code de Hamming

Code en block (mot^a de longueur: la source long M, envoi long N)



• code séparable :

$$\vec{V} = (v_1, v_2, \dots, v_7) = \underbrace{(s_1, s_2, s_3, s_4)}_m \underbrace{(v_5, v_6, v_7)}_{k \text{ seq de contrôle}} \quad m+k=n$$

1)

• code linéaire :

$$v_1 = s_1, v_2 = s_2, \dots, v_5 = \text{combi liné}^e \text{ de } s_1, \dots, s_4$$

$$\vec{V} = G \vec{S} = G \times \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} \quad \begin{matrix} G: \text{mat génératrice existe car code} \\ \text{linéaire.} \end{matrix}$$

$(7 \times 1) \quad (4 \times 1) \quad \Rightarrow G (7 \times 4)$

2)

$$\hookrightarrow v_5 = a_1 s_1 + a_2 s_2 + a_3 s_3 + a_4 s_4$$

$$v_6 = b_1 s_1 + \dots + b_4 s_4$$

$$v_7 = c_1 s_1 + \dots + c_4 s_4$$

(On est ds l'algèbre de Bool)
les "a" prennent $[0; 1]$
 $\oplus$: Ou exclusif
 $\otimes$: Et

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \end{pmatrix}$$

2^7 : 128 mots de 7 bits possible

3) A la réceptⁿ de $\vec{v}' = [v'_1 \dots v'_7]$, on vérifie que :

$$\begin{cases} v'_5 = a_1 v'_1 + a_2 v'_2 + a_3 v'_3 + a_4 v'_4 \\ v'_6 = b_1 v'_1 + \dots + b_4 v'_4 \\ v'_7 = c_1 v'_1 + \dots + c_4 v'_4 \end{cases}$$

binaires
addition et
soustraction =

$$\Rightarrow \begin{cases} a_1 v'_1 + a_2 v'_2 + a_3 v'_3 + a_4 v'_4 + v'_5 = 0 \\ \dots + v'_6 = 0 \\ \dots + v'_7 = 0 \end{cases} \Leftrightarrow H \vec{v}' = 0$$

$$\text{Soit : } H = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & 1 & 0 & 0 \\ b_1 & b_2 & b_3 & b_4 & 0 & 1 & 0 \\ c_1 & c_2 & c_3 & c_4 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} v'_1 \\ v'_2 \\ v'_3 \\ v'_4 \\ v'_5 \\ v'_6 \\ v'_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$3 \times 7 \qquad 7 \times 1 \qquad 3 \times 1$

4) $\vec{E}_i = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ la $i^{\text{ème}}$ composante est égale à 1, les autres 0.

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

On considère une erreur sur la $i^{\text{ème}}$ composante de $\vec{v}$
 $\hookrightarrow \vec{v}' = \vec{v} + \vec{E}_i$

5) $H \vec{v}' = \underbrace{H \vec{v}}_{=0} + H \vec{E}_i \Rightarrow$ cad $i^{\text{ème}}$ colonne de H .
 $= z$ le syndrome d'erreur.

6) Conditⁿ p^r qu'une erreur bin^a unique soit identifiable:
 $\hookrightarrow$ il faut que les col. de H soient $\neq$ ^{et} $\vec{v}$ de la col $\begin{pmatrix} 0 \\ 0 \\ \vdots \end{pmatrix}$.

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

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

$$9) \quad V = G \cdot \Delta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

10) $V' = (0111100)^T$, donc $Z = H \cdot V' = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, le syndrome correspond à la 3^e col de H.

$$\text{Donc : } V = V' + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$\Rightarrow$ En gnl les codes séparables par bloc fonctionnent par le calcul d'un syndrome d'erreur de taille k ($n = m + k$).
Chaque erreur possible (n possible) doit être identifiée par un syndrome $\neq$ non nul, $2^k - 1 \neq n$.

$$\text{Donc } 2^k - 1 \geq n$$

11.	k	n	m	$\frac{m}{n}$
	2	3	1	0,33
	3	7	4	0,57
	4	15	11	0,73
	5	31	26	0,83
	6	63	57	0,90

+ le rendement est élevé mieux c'est - Mais + il y a un risque d'erreur.

Par ailleurs le code de Hamming est 1-correcteur, s'il y a 2 erreurs à la correct on en atera une 3^{ème}.

$\Rightarrow$ + k sera gd, + la proba d'erreur sera gde.

2 - Code de Hamming étendu (avec 1 bit de parité)

1. 1-correcteur $\Rightarrow$ 1 à la fois

2. Avec une erreur : $\left\{ \begin{array}{l} \text{syndrome} \neq 0. \\ \text{le contrôle de parité} < 0. \end{array} \right.$
 — 2 — : $\left\{ \begin{array}{l} \text{syndrome} \neq 0 \\ \text{le contrôle de parité} > 0. \end{array} \right.$

$\downarrow$
fait en sorte que la Σ de 1 paire.

Donc on détecte 2 erreurs mais corrige 1.

3- G pr $m=4$ et $n=8$.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ a_1 & a_2 & a_3 & a_4 & 1 \\ b_1 & b_2 & b_3 & b_4 & 1 \\ c_1 & c_2 & c_3 & c_4 & 1 \\ \Sigma & \Sigma & \Sigma & \Sigma & \Sigma \end{pmatrix}$$

$1+a_1+b_1+c_1 \dots 1+a_4+b_4+c_4$

$g = 1 + a_1 + b_1 + c_1$
 $h = 1 + a_2 + b_2 + c_2$

ou avait d'ou

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

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