Code de Hamming (7,4)

- 4 : nombre de bits du <u>message</u>
  3 : nombre de bits de <u>parité</u> } => 7 bits de <u>code</u> $\in \mathbb{F}_2^7$ de base canonique $(e_1, \dots, e_7)$

- $q_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ $\quad q_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \dots \quad q_7 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{F}_2^3$: bits de parité (erreur)

  q_j représente j en base 2.

- L'application linéaire u fait l'extraction de l'<u>erreur</u> :

$$u : \underset{\text{code reçu}}{\mathbb{F}_2^7} \longrightarrow \underset{\text{erreur}}{\mathbb{F}_2^3} \qquad \text{« } u(\text{code}) = \text{erreur} \text{ »}$$
$$e_j \longmapsto q_j$$

La matrice de u est appelée <u>matrice de contrôle</u> :

$$C = \begin{array}{c} \begin{matrix} q_1 & q_2 & q_3 & q_4 & q_5 & q_6 & q_7 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

① Montrer que u est surjective et donner la dimension de $\mathrm{Ker}(u)$:

- $\forall q_j \in \mathbb{F}_2^3$, $q_j = u(e_j)$, donc tout élément de $\mathbb{F}_2^3$ est l'image d'un vecteur de la base canonique, donc u est surjective.
- Par le thm du rang on a :

$$\underbrace{\dim(\mathbb{F}_2^7)}_{7} = \dim(\mathrm{Ker}(u)) + \underbrace{\dim(\mathrm{Im}(u))}_{\substack{= \dim(\mathbb{F}_2^3) \text{ car } u \text{ surjective} \\ = 3}}$$

$$\Rightarrow \dim(\mathrm{Ker}(u)) = 4.$$

- <u>Remarque</u>: $H = \mathrm{Ker}(u) = \left\{ x \in \mathbb{F}_2^7 \mid u(x) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$
  $= \{\text{codes sans erreur}\}$

On va chercher $\gamma : \mathbb{F}_2^4 \longrightarrow H$

message $\longmapsto$ code

② Montrer que $\underbrace{\forall x \in \mathbb{F}_2^7 \setminus H}_{\text{pour tout code erroné}}$, $\exists ! \, j \in [\![1;7]\!]$ tq $\underbrace{x - \underset{\text{bit erroné à inverser}}{e_j}}_{\text{en inversant le bon bit, on retrouve}} \in H$:

$x \notin H \Rightarrow u(x) \neq \begin{pmatrix}0\\0\\0\end{pmatrix} \Rightarrow u(x) \in \{q_1, \dots, q_7\}$

$\Rightarrow \exists!\, j \in [\![1;7]\!]$ tq $u(x) = q_j = u(e_j)$

et alors $u(x - e_j) = 0$ et donc $x - e_j \in H$.

j est le nombre dont l'écriture en base 2 est $q_j = u(e_j) = u(m)$.

④ Montrer que l'application p induit un isomorphisme de H sur $\mathbb{F}_2^4$.

$$p : (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \longmapsto \underbrace{(x_3, x_5, x_6, x_7)}_{\text{extraction du message}}$$

- $\mathrm{Ker}(p) = \{ x \in \mathbb{F}_2^7 \mid (x_3, x_5, x_6, x_7) = (0,0,0,0) \}$
  $= \{ (x_1, x_2, 0, x_4, 0, 0, 0) \mid x_1, x_2, x_4 \in \mathbb{F}_2 \}$
  $= \mathrm{Vect}(e_1, e_2, e_4)$.

- $u(e_1) = q_1$, $u(e_2) = q_2$, $u(e_4) = q_4$ or (q_1, q_2, q_4) est la base canonique de $\mathbb{F}_2^3$.

Rappel : $f : E \longrightarrow F$ linéaire, $\mathcal{B}$ une base de E.
f bijective $\Leftrightarrow$ $f(\mathcal{B})$ est une base de F

Donc $u_{|\mathrm{Ker}(p)} : \mathrm{Vect}(e_4, e_2, e_1) \longrightarrow \mathbb{F}_2^3$ est bijective.

Donc $\mathrm{Ker}(u) \cap \mathrm{Ker}(p) = \{0\}$

- Soit $p' : H \longrightarrow \mathbb{F}_2^4$ induite par p. Montrons qu'elle est bijective :

  * $\forall m \in \mathrm{Ker}(p')$: $m \in H$ et $p'(m) = 0$
    $\rightarrow p'(m) = 0$ donc $p(m) = 0$ donc $m \in \mathrm{Ker}(p)$

    Donc $m \in \mathrm{Ker}(p) \cap \mathrm{Ker}(u) = \{0\}$, donc $m = 0$.

    Donc p' est injective.

  * Par le théorème du rang :

$$\underbrace{\dim(H)}_{=4 \text{ (voir ①)}} = \underbrace{\dim(\mathrm{Ker}(p'))}_{=0 \text{ car } \mathrm{Ker}(p') = \{0\}} + \dim(\mathrm{Im}(p'))$$

$\Rightarrow \dim(\mathrm{Im}(p')) = 4 = \dim(\mathbb{F}_2^4)$ donc $\mathrm{Im}(p') = \mathbb{F}_2^4$

$\Rightarrow p'$ est surjective.

5 Construire l'isomorphisme réciproque $\gamma : \mathbb{F}_2^4 \longrightarrow H$:

↳ permet d'encoder les messages.

On veut que : $\begin{cases} p \circ \gamma = id & (1) \\ u \circ \gamma = 0 & (2) \end{cases}$

(1) → iso. réc.

(2) → décoder un message correct doit donner une erreur nulle.

On note G la matrice de γ, appelée <u>matrice génératrice</u> :

(1) => les lignes 3, 5, 6 et 7 de G forment I_4 :

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

(2) La première colonne est donnée par $\varphi\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}x_1\\ | \\ x_7\end{pmatrix}$.

$p \circ \varphi = id \Rightarrow \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}x_3\\x_5\\x_6\\x_7\end{pmatrix} \Rightarrow \varphi\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}x_1\\x_2\\1\\x_4\\0\\0\\0\end{pmatrix}$

$u \circ \varphi = 0 \Rightarrow u\begin{pmatrix}x_1\\x_2\\1\\x_4\\0\\0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix} \Rightarrow \begin{pmatrix}x_4\\x_2+1\\x_1+1\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix} \Rightarrow \begin{cases} x_4 = 0 \\ x_2 = 1 \\ x_1 = 1 \end{cases}$

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

De même : $2^{\text{ème}}$ colonne : $\varphi\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$ ... $\Rightarrow G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

6) Exemple d'utilisation :

- message : $m = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$

- Encodage : $x = G \cdot m = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$

- Décodage sans erreur :

  → contrôle de l'erreur : $C \cdot x = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}}_{\text{pas d'erreur}}$

  → extraction du message : $P \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = m$

- Décodage avec erreur sur le bit 6 : $x' = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

  → contrôle de l'erreur : $C \cdot x' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 6$

  erreur sur le bit 6.