# CODES CORRECTEUR D'ERREUR

## Encoder :

Message (un pixel) qui est encodé sur k bits, m

$m \in \Omega^k$ , $\Omega = \{0, 1\}$

$\Omega^k = \{ \bar{x} = \{x_0\ x_1\ \dots\ x_{k-1}\},\ x_i \in \Omega \}$

$\oplus$ est xor

$0 \oplus 0 = 0$

$0 + 1 = 1$

$1 + 0 = 1$

$1 + 1 = 0$

$\alpha \cdot \bar{x} = \{\alpha \cdot x_i\}_{i=0}^{k-1}$

$\{\bar{e}_i\}_{i=0}^{k-1}$ est une base :

$\bar{e}_0 = \{1\ 0\ \dots\ 0\}$

$\bar{e}_1 = \{0\ 1\ 0\ \dots\ 0\}$

$\vdots$

$\bar{e}_{k-1} = \{0\ \dots\ 0\ 1\}$

$\bar{x} = \sum_{i=0}^{k-1} x_i \bar{e}_i$

$$\mathrm{dec}: \Omega^k \to [0, 2^k-1] \in \mathbb{N}$$

$$x = \sum_{i=0}^{k-1} x_i 2^i$$

$$\mathrm{bin}: [0, 2^k-1] \to \Omega^k$$

<u>But</u>: Créer un code $\Omega^k \to \Omega^n$, $n > k$

$$\bar{y} = C(\bar{x})$$

mot encodé    mot d'origine

J'aimerais que les $\bar{y}$ soient "éloignés" les uns des autres pour d $\bar{x}$ "proches".

Proches ou éloignés au sens de Hamming:

$$\bar{u} = (u_0 \dots u_{k-1}), \quad \bar{v} = (v_0 \dots v_{k-1})$$

$$d_H(\bar{u}, \bar{v}) = \# i \mid v_i \neq u_i$$
$$= d_H(\bar{u} + \bar{v}, 0)$$
$$= \sum_{i=0}^{k-1} \bar{u}_i + \bar{v}_i$$

<u>Ex</u>:

$$\begin{array}{l} \bar{u} = 0\,1\,0\,0\,1\,1 \\ \bar{v} = 0\,1\,1\,0\,1\,0 \end{array} \qquad d_H(\bar{u}, \bar{v}) = 2$$

---

Pour un code $C$:

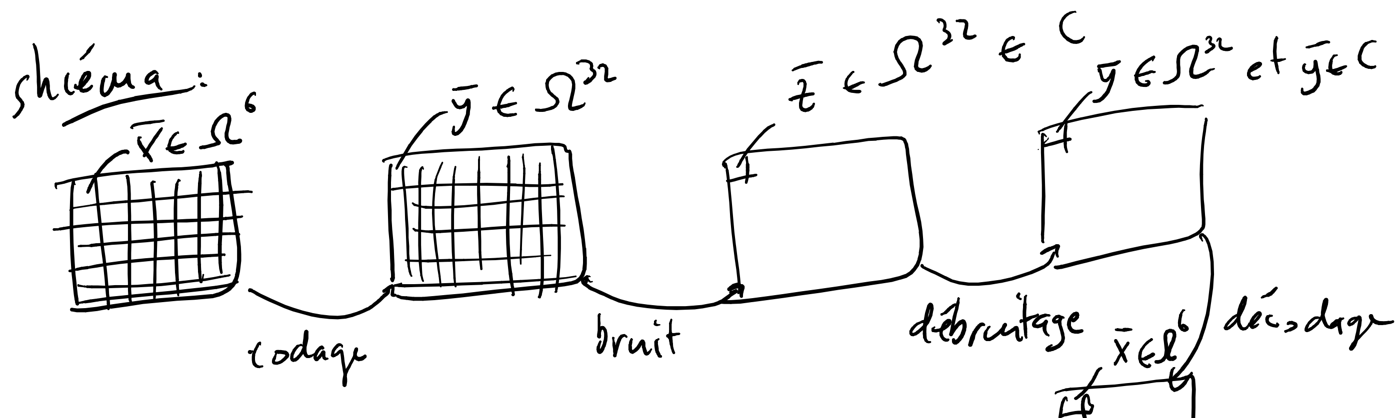
$$d_H(C) = \min \{ d_H(\bar{u}, 0) \mid \bar{u} \in C \text{ et } \bar{u} \neq 0 \}$$

## III.2 DEBRUITAGE

transmet $\bar{y}$ et on reçoit $\bar{z}$.

$z \notin C$

schéma :




## III.3 CODES DE REED-MULLER 1er odre et de longueur r

$RM(k, l) \longrightarrow RM(1, r)$

ordre ↑ longueur

1) $d_H(RM(1,r)) = 2^{r-1}$

2) On peut corrige $2^{r-2} - 1$ erreurs.

3) La longueur du message "utile" $r+1$.

$RM(1,5)$ : $2^3 - 1 \rightarrow 7$ erreurs

$RM(1,5)$ : $2^3 - 1 \to 7$ erreurs

Longueur du message : 6 bits

<u>CODE</u> : base $\{b_i\}_{i=0}^{r}$

$b_i = rm(e_i)$

$b_0 = rm(\underbrace{10 \ldots 0}_{r+1}) = (\underbrace{01\ 01 \ldots 01}_{2^r})$

$b_1 = rm(010 \ldots 0) = (00\ 11\ 00 \ldots 11)$

$b_2 = rm(0010 \ldots 0) = (0000\,1111 \ldots)$

$\vdots$

$b_{r-1} = rm(0 \ldots 010) = (000000 \ldots 01 \ldots 1)$

$b_r = rm(0 \ldots 1) = (1 \ldots 1)$

$\bar{x} = (x_0 \ldots x_r) \in \Omega^{r+1} \to \bar{y} = rm(\bar{x}) = \sum_{i=0}^{r} x_i \bar{b}_i$

$$\bar{y} = x_0 \cdot \bar{b}_0 + x_1 \cdot \bar{b}_1 + \ldots + x_r \cdot \bar{b}_r$$

On peut aussi formaliser le code via

On peut aussi formaliser le code via $G$ : la matrice génératrice :

$$G : (r+1) \times 2^r$$

$$\bar{y} = \bar{x} \cdot G$$

<u>Ex</u> : $r = 3$

$$\bar{x} = (x_0\ x_1\ x_2\ x_3) \qquad \begin{array}{c} b_0 \\ \vdots \\ \\ b_3 \end{array} \overbrace{\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}}^{2^3} = G$$

$$\bar{y} = x_0 \bar{b}_0 + x_1 \bar{b}_1 + x_2 \bar{b}_2 + x_3 \bar{b}_3$$
$$= \bar{x}\, G$$

<u>Ex</u> : $\bar{x} = (\underset{x_0}{\underset{\uparrow}{0}}\ \underset{x_1}{\underset{\uparrow}{1}}\ \underset{x_2}{\underset{\uparrow}{1}}\ \underset{x_3}{\underset{\uparrow}{0}})$

$$\bar{y} = 0 \cdot \bar{b}_0 + 1 \cdot (00\ 11\ 00\ 11) +$$
$$1\,(0000\ 1111) + 0 \cdot \bar{b}_3$$
$$= (0\ 0\ 1\ 1\ 1\ 1\ 0\ 0)$$

<u>Décodage</u>

$$\bar{x} = rm^{-1}(\bar{y})$$

$$\begin{array}{c} b_0 \\ \vdots \\ \\ b_3 \end{array} \overbrace{\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}}^{2^3}$$

$$\bar{y} = (y_0 \; \cdots \; y_{2^r-1}) = x_0 b_0 + x_1 b_1 + \cdots + x_r \bar{b}_r$$

1) $y_0 = x_r$

2) $\bar{w} = \bar{y} + x_r b_r$

3) $x_i = w_{2^i}$

<u>Ex</u>: $r = 3$ $\qquad \bar{y} = (\overset{y_0}{\downarrow}\!\!\!0 \; 0 \; 1 \; 1 \; 1 \; 1 \; 0 \; 0)$

$$y_0 = x_3 = 0$$

$$\bar{w} = x_3 \cdot b_3 + \bar{y}$$

$$= \overbrace{(0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0)}^{= x_3 \bar{b}_3}$$

$$+ \underbrace{(0 \; 0 \; 1 \; 1 \; 1 \; 1 \; 0 \; 0)}$$

$$1\,(\underbrace{0\,0\quad 1\,1\quad 1\,1\quad 0\,0}_{\bar{y}})$$

$$= (\underset{\substack{\uparrow\\ w_0}}{0}\ \underset{\substack{\uparrow\\ w_1}}{0}\quad \underset{\substack{\uparrow\\ w_2}}{1}\,1\quad \underset{\substack{\uparrow\\ w_4}}{1}\,1\quad 0\,0)$$

$x_0 = w_{20} = w_1 = 0$

$x_1 = w_2 = 1$ $\qquad\qquad \bar{x} = (0\ 1\ 1\ 0)$

$x_2 = w_4 = 1$

$$\bar{x} = rm^{-1}(\underbrace{rm(\bar{x})}_{\bar{y}})$$

$$= rm^{-1}(\bar{y})$$

## DEBRUITAGE :

$\bar{z} \notin RM$ , $\bar{y}$ ?

$$\bar{y} = \min \{ d_H(\bar{z}, \bar{u}),\ \bar{u} \in RM \}$$

## ALGORITHMES :

1) RECHERCHE EXHAUSTIVE $\rightarrow$ inefficace

2) Vote :

$$\bar{y} = \sum_{i=0}^{r} x_i \bar{b}_i$$

$r = 3$ :

$$\bar{u} = x_0 \bar{b} + x_1 \bar{b}_1 + x_2 \bar{b}_2 + x_3 \bar{b}_3$$

$$\bar{y} = x_0\bar{b} + x_1\bar{b}_1 + x_2\bar{b}_2 + x_3\bar{b}_3$$

$$= x_0(01\ 01\ 01\ 01) +$$

$$x_1(00\ 11\ 00\ 11) +$$

$$x_2(0000\ 1111) +$$

$$x_3(1111\ 1111)$$

$$= (\underset{y_0}{x_3}, \underset{y_1}{x_0+x_3}, \underset{y_2}{x_1+x_3}, \underset{y_3}{x_0+x_1+x_3}, \underset{y_4}{x_2+x_3},$$

$$\underset{y_5}{x_0+x_2+x_3}, \underset{y_6}{x_1+x_2+x_3}, \underset{y_7}{x_0+x_1+x_2+x_3})$$

$$\left.\begin{array}{l} x_0 = y_0+y_1 = y_2+y_3 = y_4+y_5 = y_6+y_7 \\ x_1 = \ldots \\ x_2 = \ldots \\ \cancel{x_3} = \ldots \end{array}\right\}$$ 4 possibilités pour calculer $x_0, x_1, \ldots, x_3$.

1 erreur corrigeable: $e = 2^{r-2} - 1 = 1$

$$\bar{y} + x_0\bar{b}_0 + x_1\bar{b}_1 + x_2\bar{b}_2 = \bar{y} + x_0(01\ 01\ 01\ 01) +$$

$$x_1(00\ 11\ 00\ 11)$$

$$x_2(0000\ 1111)$$

$$= (y_0, y_1+x_0, y_2+x_1, y_3+x_0+x_1, y_4+x_2$$

$$= (y_0, y_1 + x_0, y_2 + x_1, y_3 + x_0 + x_1, y_4 + x_2, y_5 + x_0 + x_2, y_6 + x_1 + x_2, y_7 + x_0 + x_1 + x_2)$$

$$= (x_3, \overbrace{x_0 + x_3 + x_0}^{x_3}, x_3, x_3, x_3, x_3, x_3, x_3)$$

$x_3$ est le vote majoritaire de 0 ou de 1 dans $\bar{y} + x_0 \bar{b}_0 + x_1 \bar{b}_1 + x_2 \bar{b}_2$.

REFORMULATION:

$$\Omega^{r+1} = \Omega^r \times \{0\} \cup \Omega^r \times \{1\}$$

$$= \{0, 1, \ldots, 2^{r-1}\} \cup \{2^r, \ldots, 2^{r+1} - 1\}$$

$$RM = RM_0 \cup RM_1$$

$$= \{v_0 \bar{b}_0 + \ldots + v_{r-1} \bar{b}_{r-1}\} \cup \{v_0 b_0 + \ldots + v_{r-1} \bar{b}_{r-1} + \bar{b}_r\}$$

$$RM_1 = RM_0 + b_r.$$

On change le problème:

$\bar{z} \notin RM$

$$f : RM \to \mathbb{Z}$$

$$\bar{y} \to \sum_{i=0}^{2^r-1} (-1)^{y_i} (-1)^{z_i} = \sum_{i=0}^{2^r-1} (-1)^{y_i + z_i}$$

$$= |\# i \mid y_i = z_i| - |\# i \mid y_i \neq z_i|$$

$$\overbrace{d_H(\bar{y}+\bar{b}_r, \bar{z})} \qquad \overbrace{d_H(\bar{y}, \bar{z})}$$

$$\hat{F}(\bar{y}) = \underbrace{d_H(\bar{y}+\bar{b}_r, \bar{z})}_{2^r - d_H(\bar{y},\bar{z})} - d_H(\bar{y},\bar{z})$$

$$= 2^r - 2 d_H(\bar{y},\bar{z})$$

$$d_H(\bar{y},\bar{z}) = \frac{1}{2}\left(2^r - \hat{F}(y)\right), \quad \text{si } \hat{F}(y) < 0 \text{ et } |\hat{F}(y)| \text{ maximal}$$

$$d_H(\bar{y}+b_r,\bar{z}) = \frac{1}{2}\left(2^r + \hat{F}(y)\right), \quad \text{si } \hat{F}(y) \geq 0 \ |\hat{F}(y)| \text{ maximal}$$

Si $\bar{v}$ et t.q. $|\hat{F}(v)|$ est maximal, alors

on a minimisé $\underline{d_H(\bar{y},\bar{z})}$ ou $d_H(\bar{y}+\bar{b}_r,\bar{z})$.

Transformée d'Hadamard:

$$\hat{F} : \{0, \ldots, 2^r - 1\} \to \mathbb{Z}$$

$$u \to \sum_{i=0}^{2^r-1} (-1)^{y_i} F(i)$$

$\in \mathbb{N}$, $(-1)^{z_i}$

$$\begin{pmatrix} \hat{F}(0) \\ \hat{F}(1) \\ \hat{F}(2) \\ \vdots \\ \hat{F}(2^r-1) \end{pmatrix} = \begin{pmatrix} F(0) & F(1) & \ldots & F(2^r-1) \end{pmatrix} H_r$$

$[2^r \times 2^r]$

Ex avec $r=1$ :

$u=0$ $\quad b_0 \quad b_1$

Ex avec $r=1$ :

$$u = \{0,1\} \to \bar{y}(0) = rm(\underset{u}{\underset{\downarrow}{0}}\ \underset{b_0}{0}) = 0\cdot(0\,1) + 0\cdot(1\,1)$$

$$= \boxed{0\ \ 0 = \bar{y}}$$

$y_0 = 0$
$y_1 = 0$

$$\hat{F}(0) = \sum_{i=0}^{1} (-1)^{y_i} \cdot F(i)$$

$$= (-1)^{y_0} F(0) + (-1)^{y_1} F(1)$$

$$= F(0) + F(1)$$

$\bar{y}(1) = rm(1\ 0)$
$= 1\,(0\,1)$
$+ 0\,(1\,1)$
$= \underset{y_0}{0}\ \underset{y_1}{1}$

$$\hat{F}(1) = \sum_{i=0}^{1} (-1)^{y_i} F(i)$$

$$= F(0) - F(1)$$

$$\begin{pmatrix} \hat{F}(0) \\ \hat{F}(1) \end{pmatrix} = \begin{pmatrix} F(0) & F(1) \end{pmatrix} H_1 \quad , \quad H_1 = ?$$

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$r = 2$ :

$u = \{0, 1, 2, 3\}$

$(0\,0\,0\,0)$ $1\,0\,0\,0$ $(0\,1\,0\,0)$ $(1\,1\,0\,0)$

$\boxed{(0\,0\,0\,0)}$ $\boxed{(0\,1\,0\,1)}$ $\boxed{(0\,0\,1\,1)}$

$(0\,1\,0\,1)$
$(0\,0\,1\,1)$
$\boxed{(0\,1\,1\,0)}$

$$\hat{F}(0) = (-1)^{y_0} F(0) + (-1)^{y_1} F(1) + (-1)^{y_2} F(2) + (-1)^{y_3} F(3)$$

$$\hat{F}(0) = (-1)^{y_0} F(0) + (-1)^{y_1} F(1) + (-1)^{y_2} F(2) + (-1)^{y_3} F(3)$$
$$= F(0) + F(1) + F(2) + F(3)$$
$$\hat{F}(1) = F(0) - F(1) + F(2) - F(3)$$
$$\hat{F}(2) = F(0) + F(1) - F(2) - F(3)$$
$$\hat{F}(3) = F(0) - F(1) - F(2) + F(3)$$

$$\begin{pmatrix} \hat{F}(0) \\ \hat{F}(1) \\ \hat{F}(2) \\ \hat{F}(3) \end{pmatrix} = \begin{pmatrix} F(0) & F(1) & F(2) & F(3) \end{pmatrix} \begin{pmatrix} \overbrace{\boxed{\begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix}}}^{H_1} & \overbrace{\boxed{\begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix}}}^{H_1} \\ \underbrace{\boxed{\begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix}}}_{H_1} & \underbrace{\boxed{\begin{matrix} -1 & -1 \\ -1 & 1 \end{matrix}}}_{-H_1} \end{pmatrix}$$

Cas général:

$$H_r = \begin{pmatrix} H_{r-1} & H_{r-1} \\ H_{r-1} & -H_{r-1} \end{pmatrix}$$

Une fois qu'on a tous $\hat{F}$, on cherche

$$\max |\hat{F}(\bar{v})|$$

Si $\hat{F}(v) \geq 0$ $\quad \bar{y} = v_0 \bar{b}_0 + \ldots + v_{r-1} \bar{b}_{r-1}$

$\hat{F}(v) < 0$ $\quad \bar{y} = v_0 b_0 + \ldots + v_{r-1} b_{r-1} + b_r$

Ex: $\bar{z} = (0\ 1\ \ 0\ 0\ 0\ 0\ 1\ 1)$

$$\downarrow \hat{z}$$

$(1\ -1\ \ 1\ 1\ \ 1\ 1\ -1\ -1)$

$\hat{F} = F\ H_3 = (2\ \ 2\ 2\ 2\ \ 2\ 2\ -6\ \ 2)$

$\hat{f}(6) = -6$

$|\hat{f}(6)| = 6 > \hat{f}(u \neq 6)$

$6 \to 0110$

$\bar{y} = \overset{b_3}{1} + 1\bar{b}_2 + 1b_1 + 0 \cdot b_0$

$= (1\ 1\ \ 1\ 1\ \ 1\ 1\ \ 1\ 1)$

$+ (0\ 0\ \ 0\ 0\ \ 1\ 1\ \ 1\ 1)$

$+ (0\ 0\ \ 1\ 1\ \ 0\ 0\ \ 1\ 1)$

$= (1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ 1\ 1)$