Rappel

1. Code correcteur d'erreur

$u =< u_1, \cdots, u_m >$ vecteur sur $\mathbb{Z}/2\mathbb{Z}$

$v =< v_1, \cdots, v_m >$ $u_i \in \{0,1\} v_i \in \{0,1\}$

$d_{\mathrm{H}}(u,v)$ distance de Hamming $\sum_{i=1}^{n} d(u_i, v_i)$ où $d(0,0) = d(1,1) = 0$ et $d(0,1) = d(1,0) = 0$

$\text{code} \leq (\mathbb{Z}/2\mathbb{Z})^4$

Ensemble de vecteur

$u = 011011$ $v = 011000$ $d(u,v) = 2$

c mot émis $c \in \mathrm{C}$ x reçu $x + e$ où e est l'erreur si e inverse le 2e bit $e = 010000$ u émis reçu $u + e = 001011$

C un code

- détection d'une erreur (ou plusieurs)

$< 0,0,0,0,0 >$
$< 1,0,0,0,0 >$
$< 0,1,0,0,0 >$
$< 0,0,1,0,0 >$
$< 0,0,0,1,0 >$
$< 0,0,0,0,1 >$ Vecteurs correspondant a une erreur

c émis x reçu $x + e$ pouvoir distinguer entre x et u pour $u \in textcode$

Condition pour détecter une erreur

(sur les mots de c) $\forall u, v \in \mathrm{C} u \neq v, d(u,v) > 1$

$u < 0111 > \in \mathrm{C}$
$v < 1111 > \in \mathrm{C}$
si on a reçu $< 1111 >$
u avec une erreur ou v?

1. Poids

$p(u) = d(u, \vec{0})$
$d(\mathrm{C}) = \min(u,v) u, v \in \mathrm{C} u \neq v$

$x = c + e$ où $e \in \mathrm{E}$
$d(x,c) = d(e, \vec{0}) = p(e)$

$d(\mathrm{C}) = 1$ alors il existe $u, v \in \mathrm{C}$
$u + e = v$ avec $p(e) = 1$
$u + e$ et v indistingables

Réciproquement si $d(\mathrm{C}) \geq 2$
$c, c' \in \mathrm{C}$ $c \neq c'$ $d(c, c') \geq 2$

x reçu tel que $x = u + e$ avec $p(e) = 1$ et $u \in \mathrm{C}$
il n'existe aucun $v \in \mathrm{C}$ tel que $x \in \mathrm{C}$ **on peut donc détecter l'erreur** e

1.1. Théoreme:

C un code,
si $d(\mathrm{C}) = d$ alors on peut corriger des erreurs de poids $p \leq \frac{d-1}{2}$

$d(\mathrm{C}) \geq 2.v + 1$ alors on peut corriger des erreurs de poids $\leq v$

2. Corriger des erreur de poids p

Ayant reçu $x = c + e$ avec $p(e) \leq p$ et $c \in \mathrm{C}$
On peut retrouver c à partir de x

si $d(\mathrm{C}) \geq 2.v + 1$ on peut corriger des erreurs de poids au plus v

Soit $c \in \mathrm{C}$ émis et x reçu
$x = c + e$ avec $p(e) \leq v$
on a $d(x, c) \leq v$
Soit c' un element quelconque def de c avec $c' \in \mathrm{C}$
(on a $d(c, c') \geq 2.v + 1$)
$d(c, c') \leq d(c, x) + d(x, c')$
$d(x, c') \geq d(c, c') - d(c, x)$
$2.v + 1 - v \geq v + 1 > d(x, c)$

Reciproquement: Sinon $(\neg(d(\mathrm{C}) \geq d.v + 1))$
$d(\mathrm{C}) \leq 2.v$
il existe c, c' tel que $d(c, c') \leq 2.v$
il existe e_1, e_2 tel que $p(e_1) \leq v$ et $p(e_2) \leq v$

$u_1 = 000$ $u_2 = 101$
$u_3 = 011$ $u_4 = 110$
$()\mathbb{Z}/2\mathbb{Z})^3 < u_1, u_2, u_3 >$

$d(\mathrm{C}) = 2$ il faudrait $d(\mathrm{C}) = 3$ pour pouvoir corriger des erreurs

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

$n = 6$
$|\mathrm{C}| = 8$
$d(\mathrm{C}) = 3$

Taux d'un code : $\frac{\log(|c|)}{n} = 1/2$

On peut corriger une erreur

Codes linéaires

1. def

C est un code linéaire si C est un sous-espace vectoriel de $\mathbb{Z}/2\mathbb{Z}$

s.e.v:

$u, u' \in \mathrm{C} u + u' \in \mathrm{C}$
$\lambda \in \mathbb{Z}/2\mathbb{Z}$, $u \in \mathrm{C}\ \lambda.u \in \mathrm{C}$
$\vec{0} \in \mathrm{C}$

1.1. Remarque

C s.e.v
$c, c' \in \mathrm{C} d(c, c') = d(c + c', \vec{0}) = p(c + c')$
On en deduit : $d(\mathrm{C}) = \min p(c)$ avec $c \in \mathrm{C}$ et $c \neq \vec{0}$

$$\begin{array}{c} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{array}
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1
\end{pmatrix}$$

$$\begin{array}{llcl}
c_1 & c_2 & = & c_3 \\
c_1 & c_3 & = & c_2 \\
c_2 & c_3 & = & c_1 \\
c_1 & c_4 & = & c_5 \\
c_1 & c_6 & = & c_7 \\
c_2 & c_4 & = & c_6 \\
\ldots & \ldots & \ldots & \ldots
\end{array}$$

C est un code linéaire

Base de C

- 8 éléments
- $|\mathrm{C}| = 8$
- $dim(\mathrm{C}) = 3$
- $\mathbb{Z}/2\mathbb{Z}^n = 2^n$ elt
- (c_1, c_2, c_4)

1.2. Rappels

$(w_1, \cdots, w_k)$ base de F ssi: $(w_1, \cdots, w_k)$ *engendre* $(w_1, \cdots, w_k)$ libre *(Aucun ne peux s'écrire comme **CL** des autres)*

$dim(\mathrm{F})$: le nombre d'élément de la base (si $dim(\mathrm{F}) = k$ alors F contient 2^k elts)

1.3. Dualité

$v =< v_1, \cdots, v_n >$
$w =< w_1, \cdots, w_n >$
$v.w = \sum v_i.w_i$ $v.w = 0 \iff v.w$ orthogonaux.

Soit S on notera $< \mathrm{S} >$ (si S est un s.e.v)

$\mathrm{S}^\perp = \{u \in \mathbb{Z}/2 * \mathbb{Z} | \forall v \in \mathbb{S}\mathrm{u.v} = 0\}$

1.4. Resultat

$dim(< \mathrm{S} >) + dim(< \mathrm{S}^\perp >) = n$

$\mathrm{C} = \{0000, 1010, 0101, 1111\}$ C un s.e.v
$\mathrm{C}^\perp = \{0000, 1010, 0101, 1111\}$

ATTENTION on a pas $\mathrm{C} \cap \mathrm{C}^\perp = \{\vec{0}\}$

1.5. Propriété:

Si C est un code linéaire et $dim(\mathrm{C}) = k$ alors $|\mathrm{C}| = 2^k$
Si C est un code linéaire alors $dim(\mathrm{C}) = log(|\mathrm{C}|)$

C un code linéaire
$u \in \mathrm{C}^\perp \iff \forall v \in \mathrm{C}\ u.v = 0$

Mais aussi : $u \in \mathrm{C}^\perp \iff \forall v$ *elément d'une base de* C $u.v = 0$ $u \in \mathrm{C} \iff \forall v \in \mathrm{C}^\perp$ $u.v = 0$

$dim(\mathrm{C}) = n$ et $dim(\mathrm{C}^\perp) = n - m$

1.6. Matrice d'un code

$g_1, cdots, g_k$ Base

$$\begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$$

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

$$u \in C \Longleftrightarrow \exists \lambda_1, \cdots, \lambda_k \; u = \lambda_1 . g_1 + \cdots + \lambda_k . g_k$$

$$\left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & B \\ 0 & & 1 & \end{array} \right)$$

$$\mathcal{M}_{C_1} = \begin{array}{cccc|ccc} c_1 + c_2 & 1 & 0 & 0 & 1 & 1 & 0 \\ c_1 & 0 & 1 & 0 & 1 & 0 & 1 \\ c_3 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}$$

$$(x_1, x_2, x_3)(x_1, x_2, x_3, x_1 + x_2 + x_3, x_1 + x_3, x_2 + x_3)$$

$$(x_1, x_2, x_3)(\mathrm{Id}, \mathrm{A}) = (x_1, x_2, x_3, (x_1, x_2, x_3)\mathrm{A})$$

(x_1, x_2, x_3) à coder

$(\mathbb{Z}/2\mathbb{Z})^3 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^6 \; (x_1, x_2, x_3) \longrightarrow (x_1, x_2, x_3).\mathcal{M}$
$101 \longrightarrow (101.001)$