1. Codes linéaires
2. Matrice de code linéaire
    1. Forme reduite:
        1. Regles :
        2. Codage systematique
        3. Exemple
        4. Exemple
3. Code cyclique
    1. Définition
    2. Remarque
        1. Exemple:
    3. Remarque
    4. Ideal
    5. Théoreme 1
    6. Théoreme 2

Codes linéaires

- C s.e.v $(\mathbb{Z}/2\mathbb{Z})^n$
- Dualité $\mathrm{C}^{\perp} = \{u \in (\mathbb{Z}/2\mathbb{Z})^n | \forall v \in \mathrm{C} u.v = \vec{0}\}$
- $\dim(\mathrm{C}) + \dim(\mathrm{C})^{\perp} = n$

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

Matrice de code linéaire

On peut représenter code V ***(s.e.v)*** comme une matrice : matrice de la base du code C
si $\dim\,\mathrm{C} = k$

$$\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$$

vecteur d'une base de C

$$\begin{array}{cc} & \longleftarrow \quad n \quad \longrightarrow \\ \begin{array}{c}\uparrow \\ k \\ \downarrow\end{array} & \begin{pmatrix} & & & & & \\ & & & & & \\ & & & & & \end{pmatrix} \end{array}$$

$u \in \mathrm{C} \iff \exists l_1, \cdots, l_k | u = l_1 b1, \cdots, l_k b_k$

- Message m
- erreur e
- reçu r

1. Forme reduite:

$(\mathrm{I}_k | \mathrm{A}) = \mathbb{M}_R$

1.1. Regles :

- permuter des lignes
- remplacer des ligne par des combinaisons linéaire
- multiplier par une constante
- permuter des colonne

$\Longrightarrow$ **matrice equivalente**

1.2. Codage systematique

$(x_1, \cdots, c_k) \sim (x_1, \cdots, c_k).\mathbb{M}_R = (x_1, \cdots, c_k).(\mathrm{I}_k|\mathrm{A}) = (x_1, \cdots, c_k, (x_1, \cdots, c_k).\mathrm{A})$

$(x_1, \cdots, c_k).\mathrm{C}_\mathrm{R} = (x_1, x_2, x_3, x_1 + x_2 + x_3, x_1 + x_3, x_2 + x_3)$
$< u, p(u) >$ u mot a coder $p(u)$ bits de contrôle

$$\mathrm{C}_\mathrm{R} = \begin{array}{l} c_1 + c_2 \\ c_1 \\ c_4 \end{array} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

1.3. Exemple

C' engendré par:

$$\begin{array}{l} a \\ b \\ c \\ d \end{array} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{array}{l} a \\ a + b \\ d + a \\ a + b + c \end{array} \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

reduite $\Longrightarrow \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array} \right)$

$\mathrm{G} =$ (C engendré par G) = $(Id_k|\mathrm{A})$
Alors $\mathrm{H} = (\mathrm{A}^t.\mathrm{Id}_{n-k})$ alors H^t engendre $\mathrm{C}^\perp$

$\mathrm{H}.\mathrm{G} = (\mathrm{A}^t.\mathrm{Id}_{n-k})(Id_k\mathrm{A}^t) = (\mathrm{A}^t + \mathrm{A}^t) = (0)$

$\mathrm{G} = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array} \right)$ $\mathrm{H} = \left(\begin{array}{ccc|cc} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{array} \right)$ Tout vecteur de
$\mathrm{H} estorthogonaltoutvecteurde \mathrm{G}.\mathrm{H}^t$ est une matrice de $\mathrm{C}^\perp$

H^t est une base de l'othogonal de C
$c \in \mathrm{C} \Longleftrightarrow (c)\mathrm{H}.\vec{0}$

1.4. Exemple

$u = 10111$ $u \in \mathrm{C}$?

$$(10111).\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (0,1)$$

donc $u \notin \mathrm{C}$

$v = 11101$ $v \in \mathrm{C}$?

$$(11101).\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (0,0)$$

donc $v \in \mathrm{C}$

H^t est une base de l'orthogonal de C

```
On a donc :
```

$c \in \mathrm{C} \Longleftrightarrow c.\mathrm{H}^t = \vec{0}$

Code cyclique

$\mathrm{F} = \mathbb{Z}/2\mathbb{Z}$ $\mathrm{F}^n = (\mathbb{Z}/2\mathbb{Z})^n$

$\mathrm{F}^n \longrightarrow \mathrm{F}^n$

Décalage $\mathrm{S} : (x_0, \cdots, x_{n-1}) \longrightarrow (x_{n-1}, x_0, x_1, \cdots, x_{n-2})$

1. Définition

C est un code cyclique $\Longleftrightarrow$ C est un code linéaire invariant par décalage $(\mathrm{C} = s(\mathrm{C}))$

exemple: $\mathrm{C} = (000), (110), (011), (101)$ C est un cycle

$\prod : (a_0, \cdots, a_{n-1}) \sim a_0 + a_1\mathrm{X} + \cdots + a_{n-1}\mathrm{X}^{n-1}$

$\prod : (a_0, \cdots, a_{n-1})$ le polynome de $\mathrm{F}[\mathrm{X}/(\mathrm{X}^n - 1)]$

2. Remarque

dans $\mathrm{F}[\mathrm{X}/(\mathrm{X}^n-1)]$ le décalage correspond au produit par X.

$\mathrm{P}(\mathrm{X}) = a_0+, \cdots + a_{n-1}.\mathrm{X}^{n-1}$

$$\begin{cases} \mathrm{X.P(X)} = a_0.\mathrm{X}+, \cdots + a_{n-1}.\mathrm{X}^n \\ \mathrm{X.P(X)} = a_{n-1} + a_0.\mathrm{X}+, \cdots + a_{n-2}.\mathrm{X}^{n-1} (\mathrm{mod}[\mathrm{X}^n-1]) \\ \mathrm{X.P(X)} = \mathrm{S(p(X))} & (\mathrm{mod}[\mathrm{X}^n-1]) \\ \mathrm{X.P(X)} = \prod(\mathrm{S}(\prod^{-1}(\mathrm{p}))) & (\mathrm{mod}[\mathrm{X}^n-1]) \end{cases}$$

2.1. Exemple:

$\prod(\mathrm{C}) = (0, 1+x, x+x^2, 1+x^2)$

$$\prod(\mathrm{C}) = \begin{matrix} (0, 110, 011, 101) \\ (0, 1+x, x+x^2, 1+x^2) \end{matrix} .$$

3. Remarque

$\mathrm{F}[\mathrm{X}/(\mathrm{X}^n-1)]$ est un anneau sur A

4. Ideal

I est un **Idéal** $\Longleftrightarrow$

- $0 \in \mathrm{I}$
- $\forall a, b \in \mathrm{I} \Longrightarrow a \pm b \in \mathrm{I}$
- $\forall r \in \mathrm{A}$ et $\forall a \in \mathrm{I} \Longrightarrow a.r \in \mathrm{I}$

$\mathbb{Z}$ les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$
$n\mathbb{Z} = \{p.n | p \in \mathbb{Z}\}$

Idéal est ***principal*** $\Longleftrightarrow \exists g \in \mathrm{I}$ tq $\mathrm{I} =< g >= \{g.x | x \in \mathrm{A}\}$

5. Théoreme 1

Dans $\mathrm{F}[\mathrm{X}/(\mathrm{X}^n-1)]$ tout idéal est principal

6. Théoreme 2

C est un code cyclique $\Longleftrightarrow \prod(\mathrm{C})$ est principal