Codes Linéaires

Malika More
(malika.more@iut.u-clermont1.fr)
Alex Esbelin
(Alex.Esbelin@math.u-bpclermont.fr)

IREM de Clermont-Ferrand

Formation ISN

30 Juin 2011

Plan du cours

Fabrication d'un code linéaire

- Pour fabriquer un code quelconque
  - Mots d'information de m bits
    $\rightsquigarrow 2^m$ mots de code à définir
  - Exemple : $m = 4$
    $\rightsquigarrow 2^m = 2^4 = 16$
- Pour fabriquer un code *linéaire*
  - Mots d'information de m bits
    $\rightsquigarrow$ Seulement m mots de code à définir
  - On définit seulement les mots de codes correspondant aux mots d'information *de poids* 1
  - On a une méthode pour *calculer* les autres mots de code à partir de ceux-là
- Les mots d'information de poids 1 constituent la *base*

Exemple : Fabrication d'un code linéaire de type $\mathcal{C}_{7,4}$

(Longueur des mots d'info $m = 4$ bits - Longueur des mots de code $n = 7$ bits)

- Mots de codes correspondant à la base (mots d'info de poids 1)

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111
0010	$\longrightarrow$	0010100
0001	$\longrightarrow$	0001011

Exemple : Fabrication d'un code linéaire de type $\mathcal{C}_{7,4}$

(Longueur des mots d'info $m = 4$ bits - Longueur des mots de code $n = 7$ bits)

- Mots de codes correspondant à la base (mots d'info de poids 1)

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111
0010	$\longrightarrow$	0010100
0001	$\longrightarrow$	0001011

- Mot d'information 1101 $\longrightarrow$ Quel mot de code ?

$$\begin{array}{cc} & 1000 \\ \oplus & 0100 \\ \oplus & 0001 \\ \hline & 1101 \end{array} \longrightarrow \begin{array}{cc} & 1000101 \\ \oplus & 0100111 \\ \oplus & 0001011 \\ \hline & 1101001 \end{array}$$

Le mot d'information 1101 est codé par le mot de code 1101001

Exemple : Fabrication d'un code linéaire de type $\mathcal{C}_{7,4}$

(Longueur des mots d'info $m = 4$ bits - Longueur des mots de code $n = 7$ bits)

- Mots de codes correspondant à la base (mots d'info de poids 1)

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111
0010	$\longrightarrow$	0010100
0001	$\longrightarrow$	0001011

- Mot d'information 0110 $\longrightarrow$ Quel mot de code ?

Exemple : Fabrication d'un code linéaire de type $\mathcal{C}_{7,4}$

(Longueur des mots d'info $m = 4$ bits - Longueur des mots de code $n = 7$ bits)

- Mots de codes correspondant à la base (mots d'info de poids 1)

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111
0010	$\longrightarrow$	0010100
0001	$\longrightarrow$	0001011

- Mot d'information 0110 $\longrightarrow$ Quel mot de code ?

$$\begin{array}{cc} & 0100 \\ \oplus & 0010 \\ \hline & 0110 \end{array} \longrightarrow \begin{array}{cc} & 0100111 \\ \oplus & 0010100 \\ \hline & 0110011 \end{array}$$

Le mot d'information 0110 est codé par le mot de code 0110011

Propriétés importantes

- Le mot $\underbrace{0\dots0}_{m\text{ fois}}$ est *toujours* codé par le mot $\underbrace{0\dots0}_{n\text{ fois}}$

- La somme $\oplus$ de deux mots de code est *toujours* un mot de code

- (Ces deux propriétés permettent de reconnaître les codes linéaires parmi tous les codes possibles.)

Propriétés importantes

- Le mot $\underbrace{0\ldots0}_{m \text{ fois}}$ est *toujours* codé par le mot $\underbrace{0\ldots0}_{n \text{ fois}}$

$$\begin{array}{cr} & 0100 \\ \oplus & 0100 \\ \hline & 0000 \end{array} \longrightarrow \begin{array}{cr} & 0100111 \\ \oplus & 0100111 \\ \hline & 0000000 \end{array}$$

- La somme $\oplus$ de deux mots de code est *toujours* un mot de code

$$\begin{array}{cr} & 1101001 \\ \oplus & 0110011 \\ \hline & 1011010 \\ & \text{mot de code ?} \end{array} \longrightarrow \begin{array}{cr} & 1000101 \\ \oplus & 0010100 \\ \oplus & 0001011 \\ \hline & 1011010 \\ & \text{oui !} \end{array}$$

- (Ces deux propriétés permettent de reconnaître les codes linéaires parmi tous les codes possibles.)

Matrice génératrice du code ou matrice de codage

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111
0010	$\longrightarrow$	0010110
0001	$\longrightarrow$	0001011

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

("Matrice" = tableau de nombres à deux dimensions)

Matrice génératrice du code ou matrice de codage

mot de la base		mot de code
1000	$\longrightarrow$	1000101

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

("Matrice" = tableau de nombres à deux dimensions)

Matrice génératrice du code ou matrice de codage

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111

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

("Matrice" = tableau de nombres à deux dimensions)

Matrice génératrice du code ou matrice de codage

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111
0010	$\longrightarrow$	0010100
0001	$\longrightarrow$	0001011

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

("Matrice" = tableau de nombres à deux dimensions)

Utilisation de la matrice génératrice $GI = M$

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

matrice génératrice | mot d'info | mot de code

$$G \quad I \quad = \quad M$$

("Produit matriciel" = voir cours d'Algèbre Linéaire en seconde année)

Détails du calcul des mots de code

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

- On calcule le mot de code M en faisant la somme $\oplus$ des *colonnes* de la matrice génératrice G qui correspondent aux *lignes* des 1 du mot d'information I.

Exemples

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

- On calcule le mot de code M en faisant la somme $\oplus$ des *colonnes* de la matrice génératrice G qui correspondent aux *lignes* des 1 du mot d'information I.

Exemples

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

- On calcule le mot de code M en faisant la somme $\oplus$ des *colonnes* de la matrice génératrice G qui correspondent aux *lignes* des 1 du mot d'information I.

Exemples

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

Exemples

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

- Le mot de code M associé à un mot d'info I avec un seul 1 est la colonne correspondante de la matrice génératrice G.

Exemples

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

Exemples

$$\left(\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \right) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

- Le mot de code M associé au mot d'info I qui ne contient que des 0 ne contient que des 0.

Structure de la matrice génératrice G

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

- Code de type $\mathcal{C}_{7,4}$
  - Longueur des mots de code $n = 7$ bits
  - Longueur des mots d'info $m = 4$ bits
- Matrice génératrice G
  - Nombre de lignes $n = 7$
  - Nombre de colonnes $m = 4$

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- Matrice identité I_m
  - Nombre de lignes $m = 4$
  - Nombre de colonnes $m = 4$

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

- Matrice de surcodage Q
  - Nombre de lignes $r = n - m = 3$
  - Nombre de colonnes $m = 4$

Rôle des matrices I_m et Q

- La matrice identité I_m sert à recopier les bits d'information

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

- La matrice de surcodage Q sert à calculer les bits de contrôle

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

1. Qu'est-ce-qu'un code linéaire ?
2. Matrice génératrice
3. Matrice de contrôle

Rappel de l'exemple

mot de la base		mot de code
1000	$\longrightarrow$	1000101
0100	$\longrightarrow$	0100111
0010	$\longrightarrow$	0010110
0001	$\longrightarrow$	0001011

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

Le mot d'information 1101 est codé par le mot de code 1101001

Matrice de contrôle H

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

Matrice de contrôle H

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

$$Q = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \qquad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Matrice de contrôle H

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

$$Q = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \qquad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

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

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

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

Utilisation de la matrice de contrôle

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

matrice de contrôle — message reçu — *syndrome*

$$H \quad M = S$$

Utilisation de la matrice de contrôle

$$\begin{pmatrix} \color{blue}{1} & \color{blue}{1} & \color{blue}{0} & \color{red}{0} \\ \color{blue}{0} & \color{blue}{1} & \color{blue}{1} & \color{red}{0} \\ \color{blue}{1} & \color{blue}{1} & \color{blue}{1} & \color{red}{1} \end{pmatrix} \begin{pmatrix} \color{red}{1} \\ \color{red}{1} \\ \color{red}{0} \\ \color{red}{1} \\ \color{blue}{0} \\ \color{blue}{0} \\ \color{blue}{1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

matrice de contrôle — message reçu — *syndrome*

$$H \quad M = S$$

Syndrome d'un message $HM = S$

- Le message reçu est un mot de code : syndrome nul

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

- Le message reçu n'est pas un mot de code : syndrome non nul

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

Structure de la matrice de contrôle H

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

- Code de type $\mathcal{C}_{7,4}$
  - Longueur des mots de code $n = 7$ bits
  - Longueur des mots d'info $m = 4$ bits
- Matrice de contrôle H
  - Nombre de lignes $r = n - m = 3$
  - Nombre de colonnes $n = 7$

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

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- Matrice de surcodage Q
  - Nombre de lignes $r = 3$
  - Nombre de colonnes $m = 4$
- Matrice identité I_r
  - Nombre de lignes $r = 3$
  - Nombre de colonnes $r = 3$

Décomposition du produit $HM = S$

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

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

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

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

Rôle des matrices Q et I_r

- La matrice de surcodage Q agit sur les bits d'info reçus et sert à recalculer les bits de contrôle

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

- La matrice identité I_r agit sur les bits de contrôle reçus et sert à les recopier

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

- La somme $\oplus$ permet de tester si les deux colonnes obtenues sont identiques

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

Rôle des matrices Q et I_r

- La matrice de surcodage Q agit sur les bits d'info reçus et sert à recalculer les bits de contrôle

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

- La matrice identité I_r agit sur les bits de contrôle reçus et sert à les recopier

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

- La somme $\oplus$ permet de tester si les deux colonnes obtenues sont identiques

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

Détection des erreurs

Propriété

M est un mot de code ssi son syndrome $S = HM = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

Message reçu	Syndrome	Contrôle
M	$HM = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$	OK
M'	$HM' \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$	Anomalie

Passage d'une matrice à l'autre

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

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

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

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

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

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

FIN