**Théorie de l'information et codage** **2010/2011**

# Cours 9 — 26 avril 2011

*Enseignant: Marc Lelarge* *Scribe: Quentin de Mourgues*

Pour information

- Page web du cours
  `http://www.di.ens.fr/~lelarge/info11.html`

## 9.1 Codes cycliques

### 9.1.1 Propriétés générales des codes cycliques

**Définition 9.1.1** *Un code $(n,k)$ linéaire sur $F_q$ est cyclique si pour tout mot code $\underline{C} = (C_0, \dots, C_{n-1})$ le shift droit de $\underline{C}$ : $\underline{C}^R = (C_{n-1}, C_0, \dots, C_{n-2})$ est aussi un mot code.*

Exemple 9.1.1:

Les codes à répétition.

Exemple 9.1.2:

Le $(7,3)$-code sur $F_2$ de matrice :

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

en effet :

$$L_1 \xrightarrow{C^R} L_2 \xrightarrow{C^R} L_3 \xrightarrow{C^R} L_1 + L_2 \xrightarrow{C^R} L_1 + L_2 + L_3 \xrightarrow{C^R} L_1 + L_3 \xrightarrow{C^R} L_2 + L_3 \xrightarrow{C^R} L_1$$

Exemple 9.1.3:

Le $(4,2)$-code sur $F_3$ de matrice :

$$G = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 1 & 1 & 2 & 2 \end{pmatrix}$$

en effet :

$$L_1 \xrightarrow{C^R} 2L_1 + L_2 \xrightarrow{C^R} 2L_1 \xrightarrow{C^R} L_1 + 2L_2 \xrightarrow{C^R} L_1$$

et

$$L_2 \xrightarrow{C^R} L_1 + L_2 \xrightarrow{C^R} 2L_2 \xrightarrow{C^R} 2L_1 + 2L_2 \xrightarrow{C^R} L_2$$

---

**Définition 9.1.2** *La fonction génératrice d'un mot code* $\underline{C} = (C_0, \ldots, C_{n-1})$ *est le polynôme* $C(X) = C_0 + \ldots + C_{n-1}X^{n-1}$

**Théorème 9.1.1** *Si* $\underline{C} = (C_0, \ldots, C_{n-1})$ *est un mot code de fonction génératrice* $C(X)$ *alors la fonction génératrice de* $\underline{C}^R$ *est* $C^R(X) = XC(X) \mod (X^n - 1)$

**Démonstration.** On a par définition :

$$\begin{aligned} C(X) &= C_0 + \ldots C_{n-1}X^{n-1} \\ XC(X) &= XC_0 + \ldots C_{n-1}X^n \\ C^R(X) &= C_{n-1} + C_0X + \cdots + C_{n-2}X^{n-1}. \end{aligned}$$

Donc $XC(X) - C^R(X) = C_{n-1}(X^n - 1)$ et,

$$XC(X) \mod (X^n - 1) = \left[C^R(X) \mod (X^n - 1)\right] + \left[XC(X) - C^R(X) \mod (X^n - 1)\right] = C^R(X).$$

□

**Notation :** $[P(X)]_n = P(X) \mod (X^n - 1)$.
On a en particulier, $\forall i\ X^i \mod (X^n - 1) = [X^i]_n = X^{i \mod n}$

**Théorème 9.1.2** *Si C est un code* $(n,k)$ *cyclique et si* $C(X)$ *est un mot code (on identifie mot code et fonction génératrice d'un mot code) alors* $\forall P(X)\ [P(X)C(X)]_n$ *est aussi un mot code.*

**Démonstration.** Découle du théorème précédent et de la linéarité du code. □

**Définition 9.1.3** *Une fonction génératrice de degré minimal dans C est appelée generatrice du code C.*

Exemple 9.1.4:

Reprenons l'exemple 9.1.2
$C_1(X) = 1 + X^2 + X^3 + X^4$ est un polynôme générateur de $C$.

Exemple 9.1.5:

Reprenons l'exemple 9.1.3
$C_1(X) = 1 + 2X^2$ est un polynôme générateur de $C$.
Remarquons que les polynômes générateurs ne sont pas uniques $2C_1(X) = 2 + X^2$ est aussi polynôme générateur. Le lemme suivant montre qu'il existe un unique polynôme générateur unitaire.

**Lemme 9.1.1** *Soit C un code cyclique de générateur $g(X)$*

1. *Si $\tilde{g}(X)$ est un autre polynôme générateur alors $\tilde{g}(X) = \lambda g(X)$ avec $\lambda \in F_q$*
2. *Si $P(X)$ est un polynôme tel que $[P(X)]_n$ est un mot code alors $g \mid P$*

**Démonstration.**
2. : On a $P(x) = Q(x)g(x) + R(x)$ or $[P(X)]_n$ et $[Q(X)g(X)]_n$ sont des mots codes donc $R(X)$ est un mot code de degré strictement inférieur à $g$ c'est donc 0.
1. : découle directement de 2. □

**Théorème 9.1.3** 1. *Si C est un code $(n, k)$ cyclique sur $F_q$ alors son générateur g est un diviseur de $X^n - 1$ de plus $\underline{C} = (C_0, \ldots, C_{n-1})$ est un mot code ssi il est divisible par g.*
2. *Inversement si g est un diviseur de $X^n - 1$ alors il existe un $(n, k)$ code cyclique de générateur g avec $k = n - \deg g$. C'est exactement l'ensemble des vecteurs $(C_0, \ldots, C_{n-1})$ de fonction génératrice divisible par g.*

**Démonstration.**
1. : Soit $P(X) = X^n - 1$ alors $[P(X)]_n = 0$ donc est un mot code par conséquent le lemme nous donne que $g \mid P$.

$\Longleftarrow$ immédiat d'après le théorème précédent car $g$ est un mot code.
$\Longrightarrow$ Immédiat d'après le lemme précédent car si $\underline{C}$ mot code alors $C(X) = [C(X)]_n$ donc $C(X) = I(X)g(X)$ avec $\deg I \leq n - 1 - \deg g$.

2. : Soit $g(x) \mid X^n - 1$. $C(X)$ est un multiple de $g$ ssi $C(X) = I(X)g(X)$ et il est facile de voire que le code est un code $(n, k)$-linéaire.
Pour montrer que le code est cyclique on montre que $[XI(X)g(X)]_n$ est un mot code. Or

$$\begin{aligned} [xI(x)g(x)]_n \mod g(x) &= xI(x)g(x) \mod (x^n - 1) \mod g(x) \\ &= xI(x)g(x) \mod g(x) \text{ car } g(X) \mid X^n - 1 \\ &= 0 \end{aligned}$$

□

**Définition 9.1.4** *On appelle polynôme de parité d'un code $C$ le polynôme $h(X) = \frac{X^n-1}{g(X)}$ avec $g$ générateur de $C$.*

**Corollaire 9.1.1** *Soit $C$ un code $(n, k)$ cyclique de générateur $g$ et de polynôme de parité $h$. On définit :*

$$G_1 = \begin{pmatrix} g_0 & \dots & g_r & 0 & \dots & 0 \\ 0 & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & g_0 & \dots & g_r \end{pmatrix} = \begin{pmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{pmatrix}$$

*et*

$$H_1 = \begin{pmatrix} h_k & \dots & h_0 & 0 & \dots & 0 \\ 0 & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & h_k & \dots & h_0 \end{pmatrix}$$

*. La matrice $G_1$ génère le code $C$ et sa matrice de parité est donnée par $H_1$. De plus le vecteur $\underline{I} = (I_0, \dots, I_{k-1})$ est encodé par $\underline{C} = \underline{I}G_1$ i.e. $C(X) = I(X)g(X)$.*

## 9.1.2 Classification des codes cycliques de longueur 7

On a :

$$\begin{aligned} X^7 - 1 &= (1 + X^2 + X^3 + X^4)(1 + X^2 + X^3) \\ &= (1 + X)(1 + X + X^3)(1 + X^2 + X^3) \end{aligned}$$

d'où :

| $(n,k)$ | $g(X)$ | |
|---|---|---|
| $(7,7)$ | $1$ | |
| $(7,6)$ | $X+1$ | |
| $(7,4)$ | $X^3+X+1$ | code de Hamming |
| $(7,4)$ | $X^3+X^2+1$ | code de Hamming |
| $(7,3)$ | $(X+1)(X^3+X+1)$ | Exemple 9.1.2 |
| $(7,3)$ | $(X+1)(X^3+X^2+1)$ | Exemple 9.1.2 à l'envers |
| $(7,1)$ | $(X^3+X^2+1)(X^3+X+1)$ | code à répétition |
| $(7,0)$ | $X^7-1$ | |

Remarque : Le polynôme $g(x) = x^3 + x + 1$ divise $x^n - 1$ pour tout $n$ multiple de 7. Il est donc possible de construire des codes $(7,4), (14,11), (21,18), \ldots$ cependant tous ces codes sauf le premier contiennent un vecteur de fonction génératrice $x^7 - 1$ donc ont une distance minimum de égale à 2.