

---

# Sécurité des Réseaux

**Jean-Yves Antoine**

LI - Université François Rabelais de Tours

Jean-Yves.Antoine AT univ-tours.fr



---

# Sécurité des réseaux

Codage : codes polynomiaux et cycliques  
*application aux réseaux informatiques*

# Codes polynomiaux: motivations

- Sous-classe des codes linéaires systématiques
- Codes polynomiaux standards — capacité à détecter des « paquets d'erreurs » : détection et retransmission
- Codes cycliques — sous-classe des codes polynomiaux aux capacités de correction intéressantes
- Implémentation aisée et efficace des opérations de codage / décodage (registres linéaires)

## Représentation polynomiale d'un nombre binaire

Soit un mot binaire  $(b_{n-1} b_{n-2} \dots b_1 b_0)$  de longueur  $n$ .

On peut représenter ce nombre par un polynôme  $P(X)$  de variable  $X$  et de degré  $(n-1)$  donc les coefficients binaires sont tq :

$$P(x) = b_0 + b_1 X + b_2 X^2 + \dots + b_{n-1} X^{n-1}$$

On note  $P_B$  l'ensemble des polynômes à coefficients binaires.

## Calculs sur les polynômes à coefficients binaires

- addition, soustraction, multiplication et division euclidienne comme sur les polynômes à coefficients réels
- spécificités dues à la nature binaire des coefficients

### Exemples

- $(1 + X + X^2) + (1 + X^2 + X^3) =$
- $(1 + X + X^2) - (1 + X^2 + X^3) =$
- $(1 + X).(X + X^2) =$

## Division euclidienne

Soient A et B deux polynômes à coefficients binaires. Diviser A par B revient à chercher les polynômes Q (quotient) et R (reste) de  $P_B$  tq :

$$A = B.Q + R \text{ avec } \text{degré}(R) < \text{degré}(B)$$

### Exemple

- $(X^3 + X) / (1 + X)$                       Q =                      R =
- $(X^5 + X^3 + X^2) / (X^2 + X + 1)$                       Q =                      R =

## Théorème de la division euclidienne

Soient A et B deux polynômes de  $P_B$ . Alors il existe toujours deux polynômes de  $P_B$  Q et R (de degré inférieur à Q) qui sont le quotient de la division euclidienne de A par B et ils sont **uniques**

**Diviseur** — Soient A et B deux polynômes de  $P_B$ . On dit que B est un diviseur de A ssi le reste de la division euclidienne de A par B est nul.

# Codage polynomial

---

## Principe

Un code polynomial de  $B^m \rightarrow B^n$  est défini par un polynôme générateur  $G(X)$  de degré  $r = n-m$ . Le codage s'effectue comme suit :

- On représente le mot  $M$  à coder sous la forme d'un polynôme  $M(X)$  de degré  $m-1$
- On multiplie  $M(X)$  par le polynôme  $X^r$  (**décalage** de  $r$  bits du mot  $M$ )
- On effectue la division euclidienne de  $X^r.M(X)$  par  $G(X)$  : on obtient  $X^r.M(X) = G(X).Q(X) + R(X)$  avec degré  $R(X) \leq r-1$
- Mot transmis  $T$  de représentation polynomiale  $T(X) = G(X).Q(X)$

## Calcul pratique du mot transmis

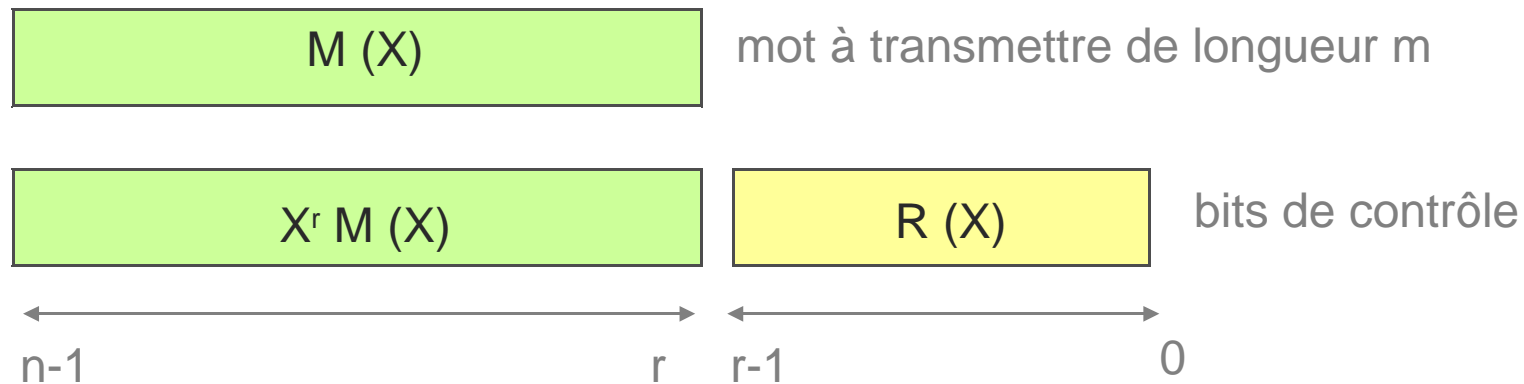
- $T$  est obtenu directement à partir de  $T(X) = G(X).Q(X) = X^r.M(X) + R(X)$
- $T(X)$  est de degré  $n-1$ : mot transmis  $T$  de longueur  $n$

**Exemple**  $G(X) = X^5 + X^2 + 1$  et  $M = (0010\ 1110)$  alors  $T =$

# Codage polynomial

## Codes polynomiaux et codes linéaires

Tout code polynomial est un code **linéaire** et **systematique**



## Mots de code

Soit un code polynomial de  $B^m \rightarrow B^n$  de polynôme générateur  $G(X)$ .  
Alors les mots de codes sont les polynômes de degré inférieur ou égal à  $n$  qui sont multiples du polynôme générateur.

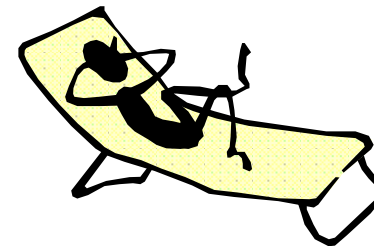
## Principe

On fait la division euclidienne de la représentation polynomiale  $M(X)$  du mot reçu par le polynôme générateur  $G(X)$

- **Reste nul:**  $M(X)$  est un mot de code
- **Reste non nul:** décodage par calcul direct du syndrome

## Syndrome d'un code polynomial

Le syndrome du mot  $M(X)$  est égal au reste de la division euclidienne de  $M(X)$  par le polynôme générateur





## Théorème

Soit un code polynomial de  $B^m \rightarrow B^n$  de polynôme générateur  $G(X)$ . Le reste de la division de tout mot reçu par  $G(X)$  est égal au reste de la division du polynôme représentant le vecteur d'erreur de transmission.

## Capacités de détection des codes polynomiaux

Soit un code de polynôme générateur  $G(X)$  de degré  $r$  qui est de la forme  $1 + \dots + X^r$  (i.e. coefficient  $g_0$  non nul). Alors :

- Ce code détecte toute erreur simple
- Les erreurs doubles sont toutes détectées si le polynôme générateur  $G(X)$  ne divise pas  $X^u+1$  pour tout  $u \in [1, n-1]$

Soit un code de polynôme générateur  $G(X)$ . Tout message comportant un nombre impair d'erreur est détecté si  $G(X)$  comporte  $X+1$  en facteur

# Détection: paquets d'erreurs

---

## Paquet d'erreurs de longueur n

Tout suite de n bits ( $n > 1$ ) dans lequel se trouvent plusieurs erreurs (en nombre compris entre 1 et n).

## Capacités de détection de salves d'erreurs

Soit un code polynomial de polynôme générateur  $G(X)$  de degré r de la forme  $1 + \dots + X^r$ . Alors le code détecte :

- toutes les salves d'erreurs de longueur inférieure ou égale à r,
- les salves d'erreur de longueur supérieure à r sont détectée avec une probabilité très élevée.

## Conclusion

Facilité de concevoir des codes de bonne capacité de détection pour un bon choix de polynômes générateurs

# Polynômes normalisés

---

## ➤ Réseaux informatiques : **CRC** — *Cyclic Redundancy Check*

**CRC-8**

$$G(X) = X^8 + X^2 + X + 1$$

**CRC-10**

$$G(X) = X^{10} + X^9 + X^5 + X^4 + X + 1$$

**CRC-12**

$$G(X) = X^{12} + X^{11} + X^3 + X^2 + X + 1$$

**CRC-16**

$$G(X) = X^{16} + X^{15} + X^2 + 1$$

**CRC-CCITT V41**

$$G(X) = X^{16} + X^{12} + X^5 + 1$$

**CRC-32**

$$G(X) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + \\ X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

**Efficacité** — CRC-16 et CRC-CCITT détectent :

- 100% des paquets d'erreurs inférieurs ou égaux à 16
- 99,997% des erreurs de longueur égale ou supérieure à 17

## ➤ Codes polynomiaux cycliques

# Codes cycliques



## Définition

Soit un code **polynomial** de  $B^m \rightarrow B^n$  de polynôme générateur  $G(X)$ . Le code est dit cyclique si  **$G(X)$  divise  $X^n+1$** . (ou  $X^n-1$ )

## Mots de code

Toute **permutation circulaire** d'un mot d'un **code cyclique** (polynomial ou non) est encore un mot de code

**Exemples** code polynomial avec  $G(X) = X^4 + X + 1$

Longueur du code	Mots de code	Code cyclique ?
N = 6	Pas de permutation	
N = 15	Permutation circulaire	

## Codes cycliques à polynômes irréductibles primitifs

- On appelle **période** ou **ordre d'un polynôme**  $G(X)$  le plus petit entier  $u$  tel que  $G(X)$  divise  $X^u+1$ .

**Exemple** : un code polynomial cyclique a une période au moins égale à la longueur du code

- Un polynôme  $G(X)$  est dit **irréductible** s'il ne possède aucun diviseur (autre que lui-même) de degré supérieur à zéro
- Si un polynôme de degré  $r$  est irréductible, sa période divise  $2^r-1$ . Lorsque sa période est égale à  $2^r-1$ , on parle de **polynôme primitif**

## Capacités de correction

Un code cyclique dont le polynôme générateur est primitif est capable de **corriger** toutes les erreurs simples.

## Conception d'un code cyclique

On prend tous les diviseurs de  $X^n+1$  et on cherche un polynôme qui a des propriétés intéressantes

**Exemple** : polynômes irréductibles primitifs

- $N= 2$      $P(X) = X^2 + X + 1$
- $N= 3$      $P(X) = X^3 + X + 1$
- $N= 4$      $P(X) = X^4 + X + 1$
- $N= 5$      $P(X) = X^5 + X^2 + 1$
- $N= 6$      $P(X) = X^6 + X + 1$
- $N= 7$      $P(X) = X^7 + X + 1$
- $N= 8$      $P(X) = X^8 + X^6 + X^5 + X^4 + 1$
- $N= 9$      $P(X) = X^9 + X^4 + 1$
- $N= 10$     $P(X) = X^{10} + X^3 + 1$
- $N= 11$     $P(X) = X^{11} + X^2 + 1$
- $N= 12$     $P(X) = X^{12} + X^7 + X^4 + X^3 + 1$

# Codes cycliques: exemples

---

## Code de Golay

- $G_{12}(X) = 1 + X^2 + X^4 + X^5 + X^6 + X^{10} + X^{11}$
- Distance 8 : corrige tous les erreurs indépendantes simples, doubles ou triples

## Codes BCH (Bose, Chaudhuri, Hocquenghem)

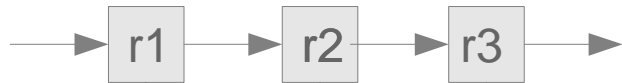
- Généralisation des codes de Hamming
- Permet de définir un code en définissant a priori sa longueur et sa distance

## Codes de Reed-Salomon

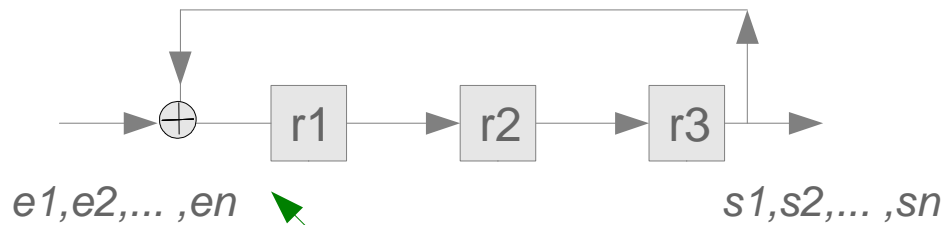
- Code de base des codes de correction de paquets d'erreurs
- CD-audio

# Implémentation des codes

## Registres linéaires



entrée	r1	r2	r3	sortie
0001 <b>1</b>	0	0	0	0
000 <b>1</b>	1	0	0	00
000 <b>0</b>	1	1	0	000
00 <b>0</b>	0	1	1	1000
<b>0</b>	0	0	1	11000



addition  
binaire  
(ou exclusif)

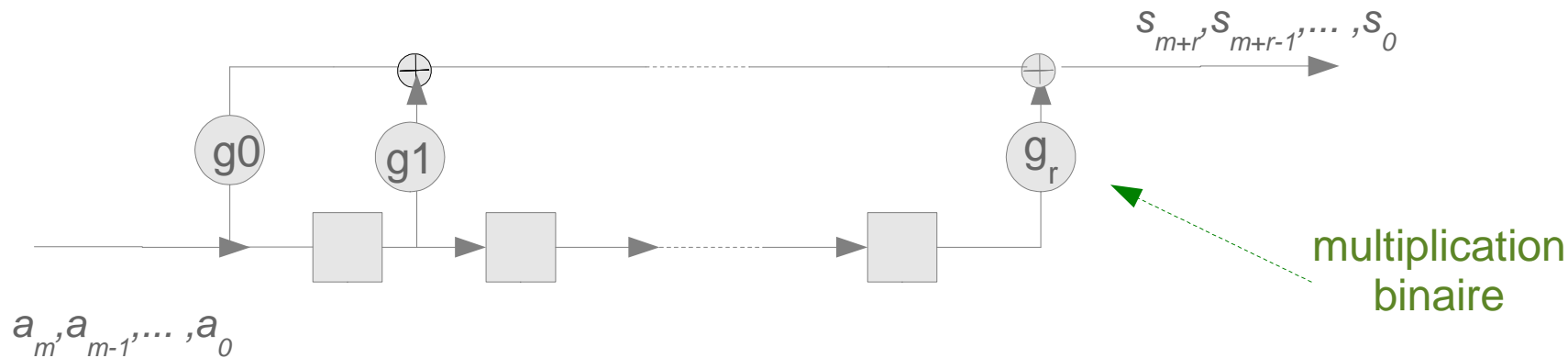
entrée	r1	r2	r3	sortie
0000011	0	0	0	0
000001	1	0	0	00
00000	1	1	0	000
0000	0	1	1	0000
000	0	0	1	10000
00	<b>1</b>	<b>0</b>	<b>0</b>	110000
0	1	1	0	0110000
	0	1	1	00110000



# Implémentation des codes

## Multiplication polynômiale

Multiplication de polynômes de la forme  $A(X) = a_0 + a_1 X + \dots + a_m X^m$  par un polynôme constant  $G(X) = g_0 + g_1 X + \dots + g_r X^r$



**Exemple**  $A(X) = 1 + X + X^2$  et  $G(X) = X + X^2$

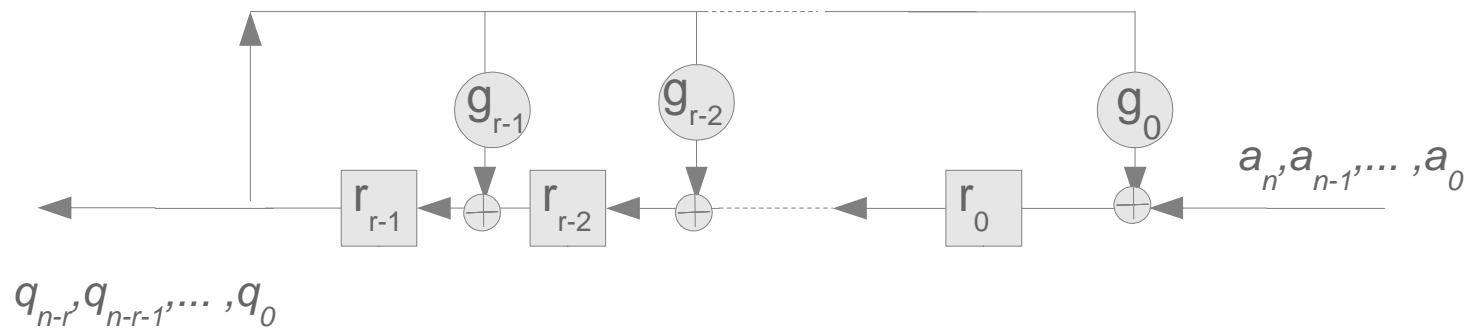
## Codage

Les mots de codes d'un code polynomial sont les multiples du polynôme générateur  $G(X)$  de degré inférieur à la longueur du code : multiples par un polynôme  $A(X)$  de degré strictement inférieur à  $m$

# Implémentation des codes

## Division polynôme

Multiplication de polynômes de la forme  $A(X) = a_0 + a_1 X + \dots + a_n X^n$  par un polynôme constant  $G(X) = g_0 + g_1 X + \dots + g_r X^r$  avec  $g_r = 1$



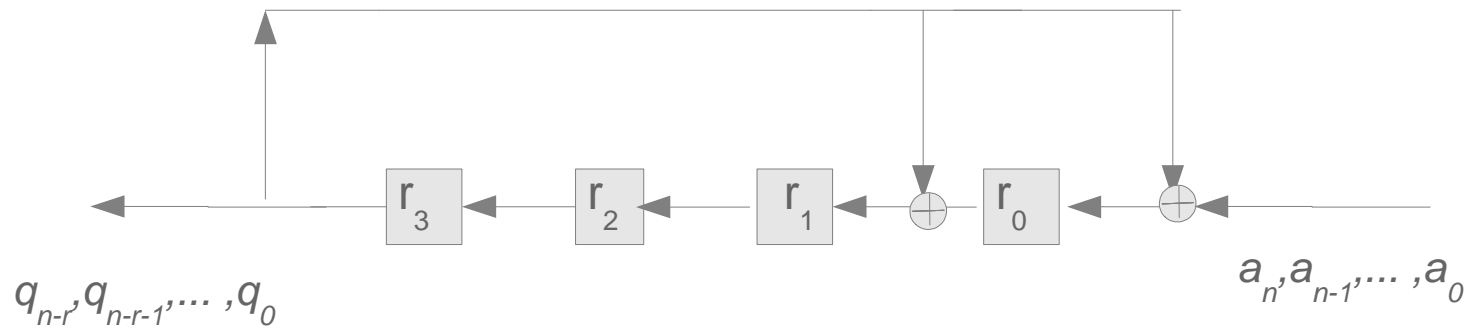
Une fois que l'entrée a complètement été transmise au registre :

- Reste  $R(X) = r_0 + \dots + r_{r-1} X^{r-1}$  (contenu des registres)
- Quotient  $Q(X) = q_0 + \dots + q_{n-r} X^{n-r}$  (sortie)

# Implémentation des codes

## Division polynômeiale : exemple

$$A(X) = X^8 + X^5 \quad \text{divisé par } G(X) = X^4 + X + 1$$



<u>sortie</u>	<u>r3</u>	<u>r2</u>	<u>r1</u>	<u>r0</u>	<u>entrée</u>
	0	0	0	0	100100000
0	0	0	0	1	00100000
00	0	0	1	0	0100000
-----					
000010001	0	0	1	1	
$Q(X) = X^4 + 1$	$R(X) = X + 1$				