

Licence 3
Informatique
Codage de l'information
175UD04

Florent Carlier

Le Mans Université

prenom.nom@univ-lemans.fr

Le Mans Université



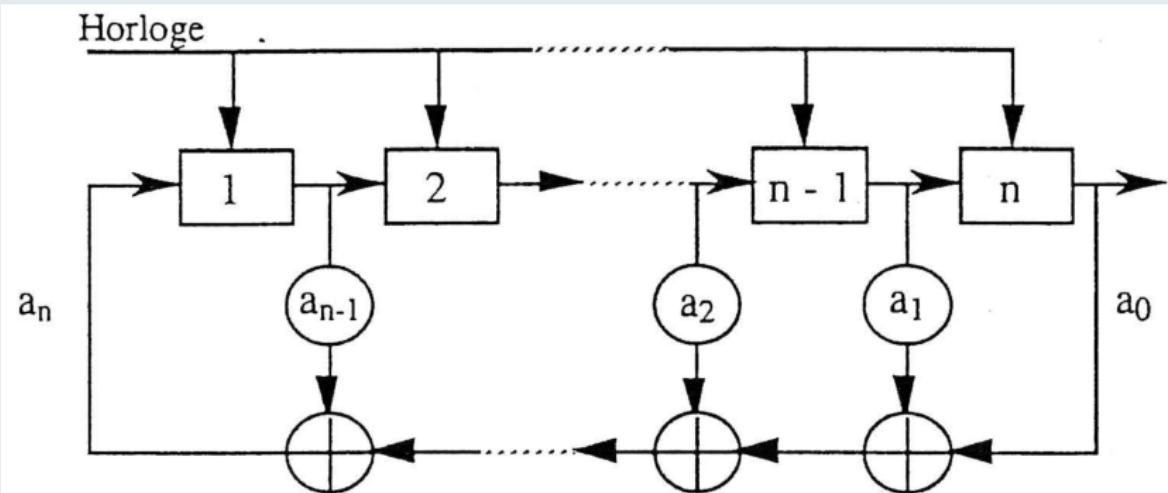
Générateurs de codes pseudo-aléatoires.

Conditions :

- Générées facilement,
- suffisamment longues,
- difficilement reconstituables à partir d'un segment,
- distribution des éléments binaires apparaît aléatoire.

Code à Longueur Maximale.

Registres à décalage en réaction linéaire comportant n étages.



Code à Longueur Maximale.

Définition.

- La contre réaction est obtenue par une addition modulo-2 de deux ou plusieurs étages de registres.
- La longueur maximale : $L = (2^n - 1)$.

Code à Longueur Maximale.

Définition.

- La contre réaction est obtenue par une addition modulo-2 de deux ou plusieurs étages de registres.
- La longueur maximale : $L = (2^n - 1)$.

Forme polynomiale.

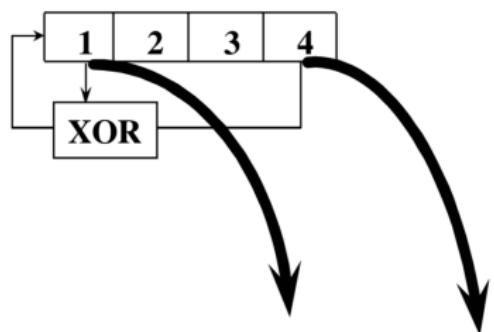
$$f(x) = \sum_{i=0}^n a_i \cdot x^i$$

Code à Longueur Maximale.

Forme polynomiale.

$$f(x) = \sum_{k=0}^R a_k \cdot x^k$$

Modulo 2

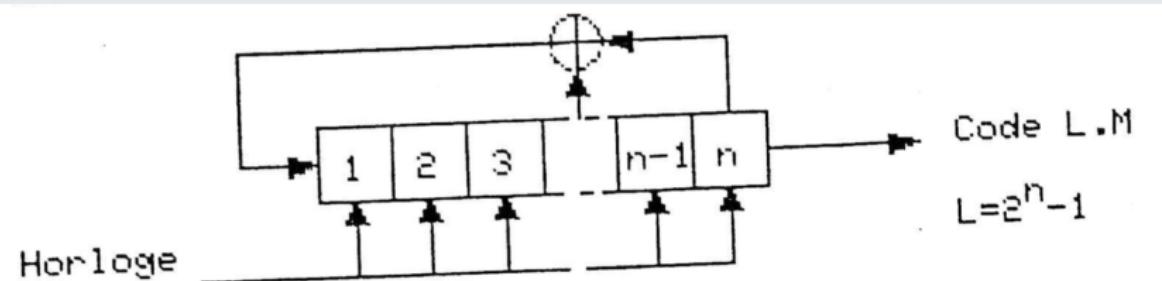


$$f(x) = \sum_{k=0}^R a_k \cdot x^k = 1 + x + x^4$$

Modulo 2

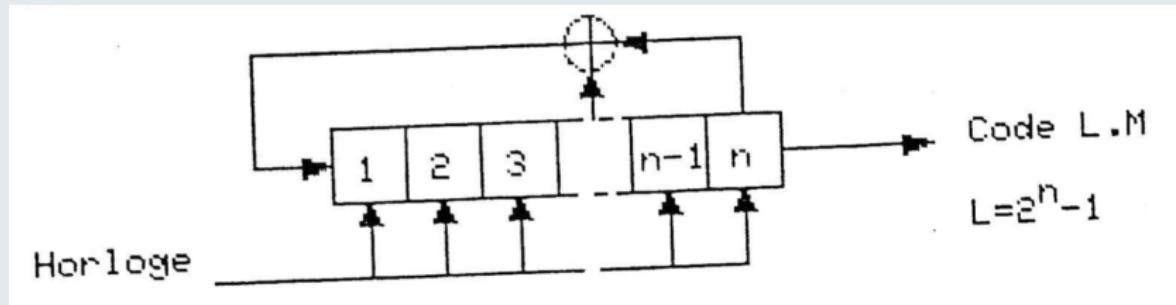
Code à Longueur Maximale.

Schéma simplifié.



Code à Longueur Maximale.

Schéma simplifié.



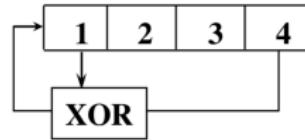
Propriété.

- Sur une longueur L , $(L+1)/2$ Bits "1" et $(L-1)/2$ Bits à "0"

Longueur n=4

Combinaisons du
registre
1 1 1 1

Exemple: Registre à décalage de longueur 4 Prises sur cases 1 et 4



Longueur n=4

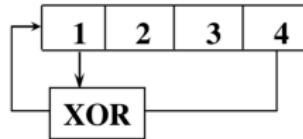
Combinaisons du
registre
1 1 1 1

Exemple: Registre à décalage de longueur 4 Prises sur cases 1 et 4

L=15

Nombre de "1"=8

Nombre de "0"=7



Code à Longueur Maximale : Exemple et Propriété.

Longueur n=4

Combinaisons du registre

1 1 1 1

0 1 1 1

1 0 1 1

0 1 0 1

1 0 1 0

1 1 0 1

0 1 1 0

0 0 1 1

1 0 0 1

0 1 0 0

0 0 1 0

0 0 0 1

1 0 0 0

1 1 0 0

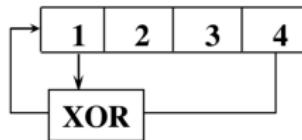
1 1 1 0

**Exemple: Registre à décalage de longueur 4
Prises sur cases 1 et 4**

L=15

Nombre de "1"=8

Nombre de "0"=7



Code à Longueur Maximale : Exemple et Propriété.

Longueur n=4

Combinaisons du registre

1 1 1 1

0 1 1 1

1 0 1 1

0 1 0 1

1 0 1 0

1 1 0 1

0 1 1 0

0 0 1 1

1 0 0 1

0 1 0 0

0 0 1 0

0 0 0 1

1 0 0 0

1 1 0 0

1 1 1 0

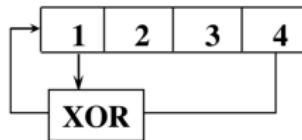
**Exemple: Registre à décalage de longueur 4
Prises sur cases 1 et 4**

1 1 1 1 0 1 0 1 1 0 0 1 0 0 0

L=15

Nombre de "1"=8

Nombre de "0"=7



Code à Longueur Maximale : Exemple et Propriété.

Longueur n=4

Combinaisons du registre

1 1 1 1

0 1 1 1

1 0 1 1

0 1 0 1

1 0 1 0

1 1 0 1

0 1 1 0

0 0 1 1

1 0 0 1

0 1 0 0

0 0 1 0

0 0 0 1

1 0 0 0

1 1 0 0

1 1 1 0

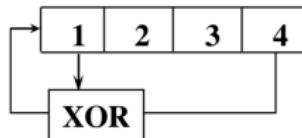
**Exemple: Registre à décalage de longueur 4
Prises sur cases 1 et 4**

1 1 1 1 0 1 0 1 1 0 0 1 0 0 0

L=15

Nombre de "1"=8

Nombre de "0"=7



C(n):

1 1 1 1 0 1 0 1 1 0 0 1 0 0 0

C(n+6):

0 1 1 0 0 1 0 0 0 1 1 1 1 0 1

C(n) XOR C(n+6):

1 0 0 1 0 0 0 1 1 1 1 0 1 0 1

Code à Longueur Maximale : Propriété.

Longueur n=4

Sur une période de ML séquence il y a:

Aucune série de "0" de longueur R, Une série de "1" de longueur R

Une série de "0" de longueur R-1, Aucune série de "1" de longueur R-1

2^{R-P-2} séries de "0" de longueur P, 2^{R-P-2} séries de "1" de longueur P

Code à Longueur Maximale : Exemple et Propriété.

Longueur n=4

Sur une période de ML séquence il y a:

Aucune série de "0" de longueur R, Une série de "1" de longueur R

Une série de "0" de longueur R-1, Aucune série de "1" de longueur R-1

2^{R-P-2} séries de "0" de longueur P, 2^{R-P-2} séries de "1" de longueur P

Registre à décalage de longueur 4 (Prises sur cases 1 et 4)

1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	1 série de R=4 "1"
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	1 série de R-1=3 "0"
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	1 série de 2 "1"
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	1 série de 2 "0"
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	2 séries de 1 "1"
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	2 séries de 1 "0"
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0	

Code à Longueur Maximale : Tableau.

Longueur n=4

Longueur Registre	Prises
2	[1,2]
3	[1,3]
4	[1,4]
5	[2,5][2,3,4,5][1,2,4,5]
6	[1,6][1,2,5,6][2,3,5,6]
7	[3,7][1,2,3,7][1,2,4,5,6,7][2,3,4,7][1,2,3,4,5,7][2,4,6,7][1,7][1,3,6,7][2,5,6,7]
8	[2,3,4,8][3,5,6,8][1,2,5,6,7,8][1,3,5,8][2,5,6,8][1,5,6,8][1,2,3,4,6,8]
9	[4,9][3,4,6,9][4,5,8,9][1,4,8,9][2,3,5,9][1,2,4,5,6,9][5,6,8,9][1,3,4,6,7,9][2,7,8,9]
10	[3,10][2,3,8,10][3,4,5,6,7,8,9,10][1,2,3,5,6,10][2,3,6,8,9,10][1,3,4,5,6,7,8,10]
11	[2,11][2,5,8,11][2,3,7,11][2,3,5,11][2,3,10,11][2,3,7,11]
12	[1,4,6,12][1,2,5,7,8,9,11,12][1,3,4,6,8,10,11,12][1,2,5,10,11,12][2,3,9,12][1,2,4,6,11,12]
13	[1,3,4,13][4,5,7,9,10,13][1,4,7,8,11,13][1,2,3,6,8,9,10,13][5,6,7,8,12,13][1,5,7,8,9,13]

Code à Longueur Maximale : Tableau.

Longueur n=4

Longueur Registre	Prises
14	[1,6,10,14][1,3,4,6,7,9,10,14][4,5,6,7,8,9,12,14][1,6,8,14][5,6,9,10,11,12,13,14]
15	[1,15][1,5,10,15][1,3,12,15][1,2,4,5,10,15][1,2,6,7,11,15][1,2,3,6,7,15]
16	[1,3,12,16][1,3,6,7,11,12,13,16][2,3,4,6,7,8,9,16][7,10,12,13,14,16][1,2,4,6,8,9,16]
17	[3,17][1,2,3,17][3,4,8,17]
18	[7,18][5,7,10,18][7,8,9,10,15,16,17,18]
19	[1,2,5,19][3,4,5,8,13,19][3,7,9,10,12,19]
20	[3,20][3,5,9,20][2,3,6,8,11,20]
21	[2,21][2,7,,14,21][2,5,13,21]
22	[1,22][1,5,9,22][1,4,7,10,13,16,19,22]
23	[5,23][5,11,17,23]
24	[1,2,7,24][4,5,7,8,9,11,14,16,18,20,22,24][1,4,5,9,10,13,14,15,16,17,18,19,21,24]
25	[3,25] [1,2,3,25][3,4,12,25]
26	[1,2,6,26][1,3,4,5,8,10,11,12,16,21,22,26][2,3,5,6,7,8,9,11,13,14,15,16,19,26]

Code à Longueur Maximale : Tableau.

Longueur n=4

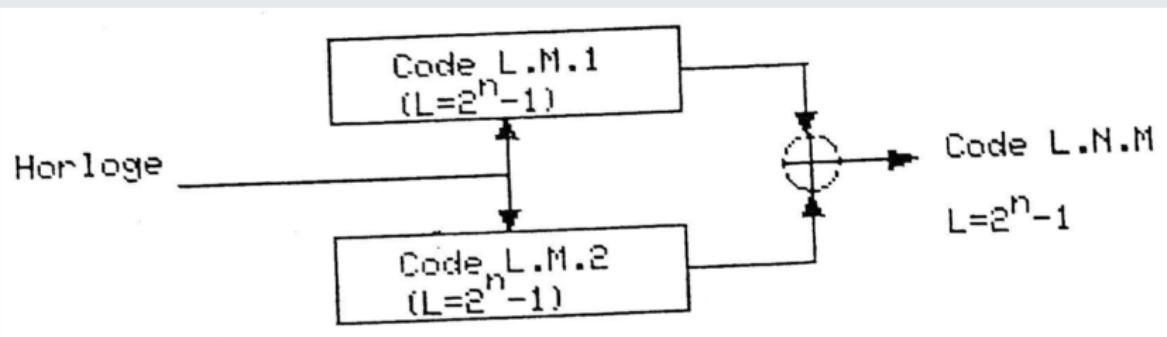
Longueur Registre	Prises
27	[1,2,5,27][3,4,5,9,10,11,18,27][3,4,5,6,11,13,22,27]
28	[3,28][3,4,8,12,16,20,24,28][3,5,9,11,13,28]
29	[2,29][2,11,20,29][2,5,21,29]
30	[1,2,23,30][1,3,4,6,7,9,12,13,15,18,20,21,24,30)
31	[3,31][1,2,3,31][3,8,13,31]
32	[1,2,22,32][1,5,6,9,10,11,14,16,18,19,28,32]
33	[13,33][11,13,22,33][13,17,29,33]
34	[1,2,27,34][1,2,6,11,13,19,21,22,23,26,27,34][1,2,4,6,8,9,10,11,27,28,29,30,31,32,33,34]
61	[1,2,5,61]
89	[3,5,6,89]

Code de Gold.

f(x) et g(x) étant des polynômes générant des paires préférées
On peut générer des codes de Gold en utilisant un registre à décalage utilisant le polynôme $z(x)=f(x).g(x)$ ou bien utiliser deux registres à décalage utilisant respectivement les polynômes f(x) et g(x) et dont on fait la somme modulo 2.

Code de Gold. Code à Longueur NON Maximale

Schéma simplifié

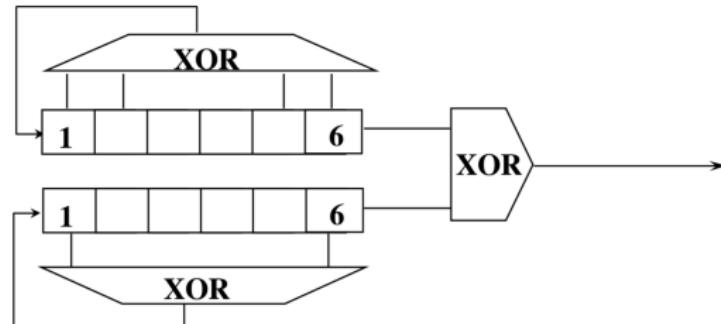
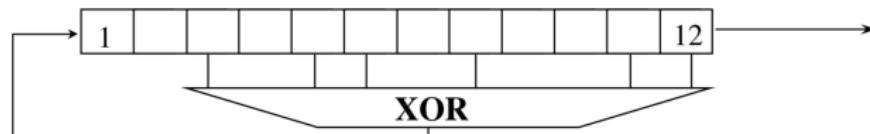


Code de Gold.

Accès Multiple par Répartition de Code (CDMA).

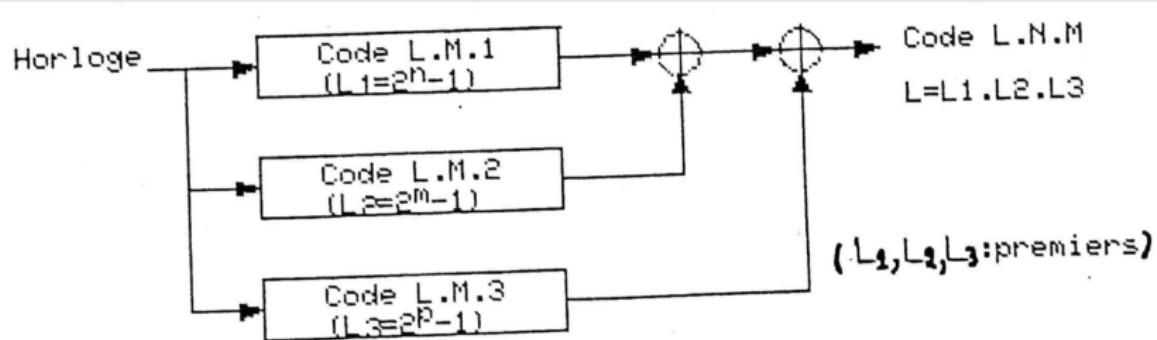
Exemple

Exemple: $R=6$, $f(x)=x^6+x+1$ et $g(x)=x^6+x^5+x^2+x+1$,
 $z(x)=x^{12}+x^{11}+x^8+x^6+x^5+x^3+1$



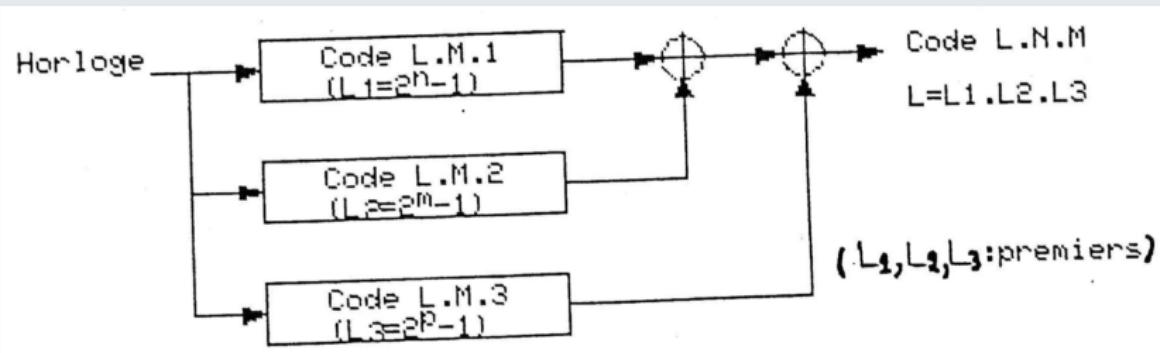
Code JPL. (Jet Propulsion Laboratory).

Exemple



Code JPL. (Jet Propulsion Laboratory).

Exemple



Radiolocation (GPS)

L'intérêt est d'avoir des séquences très longues tout en gardant des temps de synchronisation relativement courts

Code Cyclique.

Les codes en blocs linéaires ont une représentation matricielles. Les codes cycliques sont un cas particulier avec une représentation dans l'ensemble des polynômes modulo $(x^n - 1)$.

Code Cyclique.

Définition :

Un code en bloc linéaire est cyclique si en permuttant circulairement les éb d'un mot code, on obtient un autre mot code. Autrement dit le vecteur

$$C^{(1)} = (C_{n-1}, C_0, C_1, C_2, \dots, C_{n-2})$$

obtenu en permuttant une fois les éb de C est aussi un mot code. De proche en proche en permuttant i fois, on obtient un autre mot code noté:

$$C^{(i)} = (C_{n-i}, C_{n-i+1}, \dots, C_0, C_1, \dots, C_{n-i-1})$$

On peut toujours associer au mot code C de n éb un polynome de degré (n-1) de la façon suivante:

C ==>

$$C(x) = C_0 + C_1x + C_2x^2 + \dots + C_{n-1}x^{n-1}$$

Code Cyclique.

Exemple :

Si on multiplie $C(x)$ par x on obtient:

$$xC(x) = xC_0 + C_1x^2 + C_2x^3 + \dots + C_{n-1}x^n$$

En ajoutant C_{n-1} puis en retranchant C_{n-1} dans l'expression ci-dessus, on obtient:

$$xC(x) = C_{n-1} + xC_0 + C_1x^2 + C_2x^3 + \dots + C_{n-1}(x^n - 1)$$

<----->

reste de la division de $xC(x)$ par $(x^n - 1)$

Comme on travaille dans l'ensemble des polynômes¹ modulo $(x^n - 1)$, $x \cdot C(x)$ s'écrit:

$$xC(x) = C_{n-1} + xC_0 + C_1x^2 + C_2x^3 + \dots + C_{n-2}x^{n-1}$$

Code Cyclique.

Propriété :

Le vecteur code associé à ce polynôme est $C(1) = (C_{n-1}, C_0, C_1, C_2, \dots, C_{n-2})$

Conclusion: Multiplier par x le polynôme $C(x)$ revient à faire une permutation circulaire sur les éb du mot code associé à $C(x)$. On déduit que multiplier $C(x)$ par x^i revient à faire i permutations circulaires.

Code Cyclique.

Exemple de code cyclique : Code à 7 éléments binaires.

On a montré précédemment que les codes cycliques à 7 éb sont représentés par un polynôme multiple modulo $x^7 - 1$, de l'un des diviseurs de $x^7 - 1$. Or la décomposition de $x^7 - 1$ s'écrit:

$$x^7 - 1 = (1 + x^2 + x^3) (1 + x + x^3) (1 + x)$$

<----->
polynômes primitifs

Code Cyclique.

Codage par multiplication des polynômes.

Donc, trois codes possibles:

- $(1 + x^2 + x^3)$ multiplié par des polynômes de degré < 4
- $(1 + x + x^3)$ multiplié par des polynômes de degré < 4
- $(1 + x)$ multiplié par des polynômes de degré < 6

Prenons, par exemple, $g(x) = 1 + x + x^3$.

Code Cyclique.

Message	Polynômes cycliques	Mots-code
0000	$0 \cdot (1+x+x^3) = 0$	0000000
1000	$1 \cdot (1+x+x^3) = (1+x+x^3)$	1101000
0100	$x \cdot (1+x+x^3) = x+x^2+x^4$	0110100
1100	$(1+x) \cdot (1+x+x^3) = 1+x^2+x^3+x^4$	1011100
0010	$x^2 \cdot (1+x+x^3) = x^2+x^3+x^5$	0011010
1010	$(1+x^2) \cdot (1+x+x^3) = 1+x+x^2+x^5$	1110010
0110	$(x+x^2) \cdot (1+x+x^3) = x+x^3+x^4+x^5$	0101110
1110	$(1+x+x^2) \cdot (1+x+x^3) = 1+x^4+x^5$	1000110
0001	$x^3 \cdot (1+x+x^3) = x^3+x^4+x^6$	0001101
1001	$(1+x^3) \cdot (1+x+x^3) = 1+x+x^4+x^6$	1100101
0101	$(x+x^3) \cdot (1+x+x^3) = x+x^2+x^3+x^6$	0111001
1101	$(1+x+x^3) \cdot (1+x+x^3) = 1+x^2+x^6$	1010001
0011	$(x^2+x^3) \cdot (1+x+x^3) = x^2+x^4+x^5+x^6$	0010111
1011	$(1+x^2+x^3) \cdot (1+x+x^3) = 1+x+x^2+x^3+x^4+x^5+x^6$	1111111
0111	$(x+x^2+x^3) \cdot (1+x+x^3) = x+x^5+x^6$	0100011
1111	$(1+x+x^2+x^3) \cdot (1+x+x^3) = 1+x^3+x^5+x^6$	1001011

Code Cyclique.

Codage par division des polynômes

Soit $D = (d_0, d_1, d_2, \dots, d_m)$ un bloc de message de m bits et $g(x)$, de degré k , le polynôme générateur.

Associons à D un polynôme $D(x) = d_0 + d_1x + d_2x^2 + \dots + d_{m-1}x^{m-1}$
 Multiplions $D(x)$ par x^k , puis divisons $x^kD(x)$ par $g(x)$, nous avons:

$$r(x) + x^k D(x) = q(x) g(x) \quad (I)$$

degré de $r(x) < k$ (degré de $g(x)$)

D'après les propriétés démontrées plus haut pour les codes cycliques:

$$r(x) + x^k D(x) = C(x) \quad (\text{voir relation I})$$

Nous obtenons un mot-code associé de la forme:

$$[\underbrace{r_0 r_1 r_2 \dots r_{k-1}}_{k \text{ eb fournis par } r(x)} : \underbrace{d_0 d_1 d_2 \dots d_{m-1}}_D]$$

Code Cyclique.

Exemple: Code (7,4) avec $g(x) = 1 + x + x^3$ $k = 3$

$$D = 1110 \implies D(x) = 1 \cdot x^0 + 1 \cdot x + 1 \cdot x^2 + 0 \cdot x^3$$

$$x^k D(x) = x^3 D(x) = x^3 + x^4 + x^5$$

Rappel: l'addition est la même chose que la soustraction en arithmétique modulo 2.

$$\begin{array}{r} x^5 + x^4 + x^3 \\ + x^5 + x^3 + x^2 \\ \hline + x^4 + x^2 \\ + x^4 + x^2 + x \\ \hline x \end{array} \quad \left| \begin{array}{r} x^3 + x + 1 \\ \hline x^2 + x \end{array} \right.$$

On en déduit $r(x) = x$

On écrit: $r(x) = 0 \cdot x^0 + 1 \cdot x + 0 \cdot x^2$ d'où: $r_0 = 0$; $r_1 = 1$; $r_2 = 0$

Le mot code C est égal à: $C = [0 \ 1 \ 0 : \ 1 \ 1 \ 1 \ 0]$
contrôle message

Merci...

