R&T1 R1 TD4

Mise en oeuvre des codes polynomiaux

1. Présentation (boite à outils)

1.1 Représentation polynomiale des mots binaires

10111 -> x^4+x^2+x+1

un mot de **n bits** s'écrit avec un polynôme de degré **n-1**

1.2 Arithmétique polynomiale modulo 2

Addition :

0+0=0
0+1=1
1+0=1
1+1=0 ~~(retenue 1)~~

Soustraction :

0-0=0
1-0=1
0-1=1 ~~(report 1)~~
1-1=0

Les opérations d'addition et de soustraction dans ce cadre sont équivalentes (à cause du modulo 2) et sont réalisables à l'aide de l'opérateur OU exclusif (⊕):

OU exclusif :

0⊕0=0
0⊕1=1
1⊕0=1
1⊕1=0

1.3 Multiplication d'un polynôme par x^k

Cela revient à ajouter k bits à droite de la suite binaire associée au polynôme :

10111 * x^2 = 10111**00**

1.4 Utilisation de polynômes dans le CRC

Soit N(x) le polynôme qui représente les informations à envoyer

Soit G(x) le polynôme générateur de degré k

G(x) est connu de l'émetteur et du récepteur

A l'émission :

- N(x) * x^k
- puis N(x) * x^k qui va donner : Q(x)*G(x) + R(x)
  avec Q(x) : le quotient et R(x) : le reste
  R(x) est appelé CRC, c'est un polynôme de degré **k-1**

- L'information envoyée est : $T(x) = N(x) * x^k + CRC$
  i.e. transmission des bits de N(x) suivis par ceux du CRC

A la réception, récupération de T'(x) qui devrait être identique à T(x) :

- $T'(x) / G(x) = Q'(x)*G(x) + R'(x)$
- Si R'(x) = 0 : pas d'erreur de transmission détectée

2. Exemple 1 :

Soit 1100101 à transmettre avec $G(x) = x^3+x+1$
$N(x) = x^6+x^5+x^2+1$

- $N(x) * x^k => N(x) * x^3$
- R(x) de degré 2 : $r_2x^2+r_1x^1+r_0x^0$
- Par division polynomiale :

principe : l'opération consiste à faire des soustractions succéssives tant que le polynôme correspondant au reste de la division possède un degré supérieur à celui du diviseur. Les opérations de soustraction donneront toujours un résultat positif (car soustraction et addition s'obtiennent de la même manière dans ce système arithmétique)

$N(x) * x^3 = x^3*(x^6+x^5+x^2+1) = x^9+x^8+x^5+x^3$

$x^9+x^8+.\cdot+.\cdot+x^5+.\cdot+x^3$	x^3+x+1
$x^9+.\cdot+x^7+x^6$	$x^6+x^5+x^4+x^2+x$
$x^8+x^7+x^6+x^5$	
$x^8+.\cdot+x^6+x^5$	
$x^7+.\cdot+.\cdot+.\cdot$	
$x^7+.\cdot+x^5+x^4$	
$x^5+x^4+x^3$	
$x^5+.\cdot+x^3+x^2$	
$x^4+.\cdot+x^2$	
$x^4+.\cdot+x^2+x$	
x	

=> $Q(x) = x^6+x^5+x^4+x^2+x$
et R(x) = x, avec R(x) de degré 2, soit :
R(x) -> **010**

- Par division binaire :

principe : l'opération consiste à faire des soustractions succéssives en binaire modulo 2 : on abaisse 1 bit du dividande que l'on met à droite du reste intermédiaire, on fait un ou exclusif avec la valeur du diviseur. Si le bit le plus

significatif du reste intermédiaire vaut 0, on abaisse 2 bits du dividande.

```
1100101000 | 1011
1011       | 1110110
01111      |
 1011      |
 01000     |
  1011     |
  001110   |
    1011   |
    01010  |
     1011  |
     00010 |
```

=> Q(x) -> **1110110**
et reste = 10, avec R(x) de degré 2, soit :
R(x) -> **010**

- Information transmise :
C'est : T(x) = N(x) * x^3 + R(x) -> **1100101 010**

A la réception :

T'(x) divisé par G(x), soit : $x^9+x^8+x^5+x^3+$ x divisé par x^3+x+1 donne un reste nul => pas d'erreur détectée.
Si T'(x) différent T(x), par exemple $x^9+x^8+x^5+x^3+x^2+x$, cette division donne un reste différent de 0 => erreur !

3. Exercices

3.1 Calcul de CRC4

Calculez le CRC4 pour les données **1010010111**, le polynôme générateur étant **x^4+x^2+x+1**.

3.2 Transmission

Supposons que l'on transmette des données codées par la méthode du CRC, dont le polynôme générateur est : **G(x) = x^5+x+1**

3.2.1 Si l'on désire envoyer les données sur 9 bits, dont la représentation octale est la suivante : **456_8**, quel sera le message envoyé ?

3.2.2 Si l'on reçoit le message suivant de 15 bits dont la forme octale est : **76543_8**, que peut-on dire du message initial ?

3.3 Réception

Le CRC est calculé avec le polynôme générateur suivant :

$G(x) = x^2+x+1$.

Le message reçu (données + CRC) est :

$T(x) = x^{10}+x^7+x^6+x^4+ x^3+x$

3.3.1 Dites si des erreurs de transmission se sont produites.

3.3.2 Donnez, sous forme de polynôme M(x), les données initiales transmises.

4. Autres exercices

4.1 G(x) = x^2+x+1

On désire protéger le message **110111** par une clé calculée à l'aide du polynôme générateur : **x^2+x+1**

4.1.1 Représentez le message binaire transmis par l'émetteur.

4.1.2 Le message reçu par le récepteur est **11010111**. Déterminez si ce message comporte des erreurs.

4.2 G(x) = x^4+x^2+x+1

Le message reçu par un récepteur est **10100101110100**. Déterminez si ce message comporte des erreurs.

4.3 Code correcteur

Voir exemple du code de Huffman dans le cours.