Théorie de l'information

M1 Informatique 2013-2014

Fiche de TD 3

Codes correcteurs

Exercice 1. (Opérations sur les polynômes)

Soient $\mathbb{F}_2 := \mathbb{Z}/_{2\mathbb{Z}}$ le corps à deux éléments et $\mathbb{F}_2[x]$ l'anneau des polynômes à coefficients dans $\mathbb{F}_2$ sur une indéterminée x .

1. Rappeler la table d'addition et de multiplication de $\mathbb{F}_2$.
2. Simplifier dans $\mathbb{F}_2[x]$ les sommes suivantes :

   (a) $(x^2 + 1) + (x^3 + x)$;

   (b) $(x^3 + x + 1) + (x^4 + x)$;

   (c) $(x^2 + 1) + (x^2 + 1)$;

   (d) $(x^4 + x^3 + x) + (x^3 + x^2 + x + 1)$.

3. Simplifier dans $\mathbb{F}_2[x]$ les produits suivants :

   (a) $(x^3 + x^2 + 1)(x^2 + 1)$;

   (b) $(x^2 + x)(x^2 + x + 1)$;

   (c) $(x^2 + 1)^3$;

   (d) $(x^2 + 1)^4$.

4. Calculer le quotient et le reste de la division du polynôme $f(x)$ par le polynôme $g(x)$ pour chacun de cas suivants :

   (a) $f(x) := x^3 + x^2 + x$ et $g(x) := x^2 + 1$;

   (b) $f(x) := x^4 + x$ et $g(x) := x^2 + 1$;

   (c) $f(x) := x^5 + 1$ et $g(x) := x^3 + x + 1$;

   (d) $f(x) := x^6 + x^5 + x^3 + x^2$ et $g(x) := x^3 + x + 1$.

5. Soit $g(x) := x^4 + x^3 + 1$. Pour chacun des polynômes f suivants, calculer $f \mod g$.

   (a) $x^4 + x$;

   (b) $x^4 + x^3$;

   (c) $x^5 + x^2 + x + 1$;

   (d) $x^6 + x^4 + x^3 + 1$.

6. Pour chacun des polynômes suivants, démontrer ou infirmer le fait qu'ils soient ou non irréductibles.

   (a) $x^3 + 1$;

   (b) $x^2 + x + 1$;

   (c) $x^4 + x^2 + 1$;

   (d) $x^5 + x^2 + 1$.

Exercice 2. (Codage de Hamming)

On considère le codage de Hamming $[7, 4, 3]$ avec le polynôme irréductible

$$g(x) := x^3 + x^2 + 1.$$

Ce codage consiste à associer à tout bloc $m := m_0m_1m_2m_3$ de longueur 4 un bloc $c := c_0c_1c_2c_3c_4c_5c_6$ de longueur 7 défini par

$$c(x) := x^3m(x) + (x^3m(x) \mod g(x)),$$

où l'on note $m(x) := m_3x^3 + m_2x^2 + m_1x + m_0$ et $c(x) := c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$,

1. Encoder, par le codage de Hamming, le message

   `0000100100101011`.

2. Démontrer que pour tout bloc m,

   $$c(x) \mod g(x) = 0.$$

3. Démontrer que si c un bloc de message codé tel que l'on ait $c(x) \mod g(x) = x^i \mod g(x)$ avec $0 \leq i \leq 6$, alors le bit c_i est altéré.

4. Décoder, par le codage de Hamming, le message

   `010000011110111000101`.

Exercice 3. (Codage de convolution)

On considère un codage de convolution défini de la façon suivante. Chaque bit m_n d'une source $m := m_1m_2m_3\dots$ est codé par un bloc de deux bits c_nd_n, calculés modulo 2 par

$$c_n := m_{n-2} + m_n \quad \text{et} \quad d_n := m_{n-2} + m_{n-1} + m_n.$$

1. Construire le transducteur de codage correspondant.

2. En utilisant le transducteur précédent, encoder le message

   `000111`.

3. Utiliser l'algorithme de décodage de Viterbi pour décoder le message

   `001011`.

On considère à présent le codage défini par

$$c_n := m_{n-2} + m_{n-1} + m_n \quad \text{et} \quad d_n := m_{n-3} + m_{n-2} + m_{n-1} + m_n.$$

4. Construire le transducteur de codage correspondant.

5. En utilisant le transducteur précédent, encoder le message

   `0100110110`.

6. Utiliser l'algorithme de décodage de Viterbi pour décoder le message

   `0001110101001111`.