Master CSI 2 — 2010-2011

Cryptanalyse — MHT912

Responsable : G. Castagnos

Devoir surveillé — 2 novembre 2010

Durée 1h30
accés aux fonctions programmées en TP autorisé, autres documents non autorisés,
toute réponse doit être **justifiée** *par un raisonnement et/ou par un code Magma.*
Barème indicatif : Exercice 1 : 8, Exercice 2 : 12

Exercice 1. Dans tout l'exercice on note $s = (s_n)_{n\geqslant 0}$ une suite binaire et $S(X)$ sa série génératrice définie par $S(X) = \sum_{n\geqslant 0} s_n X^n$.

(a) Soit $f(X) \in \mathbb{F}_2[X]$ un polynôme de degré L avec $f(X) = 1 + c_1X + c_2X^2 + \cdots + c_LX_L$. Rappeler sans démonstration la formule reliant $S(X)$ et $f(X)$ pour que s soit produite par un LFSR de polynôme de rétroaction $f(X)$.

(b) On suppose maintenant que s est une suite binaire périodique quelconque de période T. Montrer que $X^T S(X) = S(X) + \sum_{i=0}^{T-1} s_i X^i$. En déduire le polynôme de rétroaction d'un LFSR permettant d'engendrer S ainsi qu'une méthode pour déterminer le polynôme de rétroaction minimal d'une suite binaire périodique.

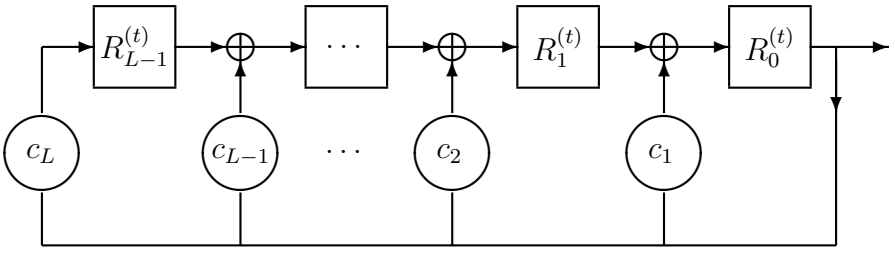
(c) On suppose que s est une *m-sequence* de complexité linéaire L. Comparer l'efficacité de la méthode de la question précédente avec la méthode vue en cours pour trouver le polynôme de rétroaction minimal de s (on rappelle que le calcul du pgcd de deux polynômes de $\mathbb{F}_2$ de degrés inférieurs à e peut être effectué en $\mathcal{O}(e \log^2 e \log\log e)$ opérations dans $\mathbb{F}_2$).

(d) **Application avec Magma.** Soit une suite binaire périodique de période 7, répétant le motif 1000101. Calculer le polynôme de rétroaction minimal avec la méthode de la question (b). Retrouver ce résultat avec une méthode plus efficace. Indiquer et justifier les commandes Magma utilisées.

Exercice 2. Soit $f(X) \in \mathbb{F}_2[X]$ un polynôme de degré L avec $f(X) = 1 + c_1X + \cdots + c_LX_L$. On considère un automate constitué d'un registre à décalage de L bits. On note $R^{(t)} = (R_0^{(t)}, R_1^{(t)}, \ldots, R_{L-1}^{(t)})$ l'état du registre à l'instant $t \geqslant 0$. À l'instant t, on sort le bit de poids faible du registre, $R_0^{(t)}$, et on met à jour l'état du registre de la façon suivante (calculs dans $\mathbb{F}_2$) :

$$R_i^{(t+1)} = R_{i+1}^{(t)} + c_{i+1}R_0^{(t)}, \text{ pour } 0 \leqslant i \leqslant L-2 \text{ et } R_{L-1}^{(t+1)} = c_L R_0^{(t)}$$

Un tel automate est appelé **LFSR en représentation Galois**. Le polynôme $f(X)$ est son polynôme de rétroaction. On le représente par le schéma suivant :



(a) Avec Magma. Donner le code d'une fonction prenant en entrée $f(X)$ de degré L, R de L bits et N et retournant les N premiers bits générés par un LFSR en représentation Galois de polynôme de rétroaction $f(X)$, dont le registre est initialisé par R (c'est à dire tel que $R^{(0)} = R$). Donner les 5 premiers bits produits par le LFSR Galois de polynôme de rétroaction $1 + X + X^3$ et initialisé par $[1, 1, 0]$.

(b) Pour tout entier t, on désigne par $R^{(t)}(X)$ le polynôme de $\mathbb{F}_2[X]$ de degré $L-1$ correspondant au registre au temps t : c'est à dire $R^{(t)}(X) = R_0^{(t)} + R_1^{(t)}X + \cdots + R_{L-1}^{(t)}X^{L-1}$. On note s_t le bit sorti au temps t (c'est à dire $R_0^{(t)}$).
Montrer que pour tout entier $t \geqslant 0$, $X \times R^{(t+1)}(X) = R^{(t)}(X) + s_t \times f(X)$.

(c) On note $S^{(0)}(X) = 0$ et pour tout $t \geqslant 1$, $S^{(t)}(X) := s_0 + s_1X + \cdots + s_{t-1}X^{t-1}$. Montrer par récurrence sur t que pour tout $t \geqslant 0$, $R^{(0)}(X) = f(X) \times S^{(t)}(X) + X^t \times R^{(t)}(X)$.

(d) On note $S(X)$ la série génératrice de la suite produite par le LFSR en représentation Galois, c'est à dire que $S(X) = \sum_{t \geqslant 0} s_t X^t$. Déduire de la question précédente que $S(X) = R^{(0)}(X)/f(X)$. Montrer que toute suite récurrente linéaire produite par un LFSR classique peut l'être par un LFSR en représentation Galois et réciproquement.

(e) Application avec Magma. Donner les commandes pour construire les 100 premiers bits de la suite produite par le LFSR en mode Galois de polynôme de rétroaction $1 + X^2 + X^4$ et initialisé par $[0, 1, 0, 1]$. Donner les commandes pour construire ces 100 bits par un LFSR en mode classique en précisant le polynôme de rétroaction et l'initialisation utilisés.

(f) Autre application avec Magma. Réciproquement, donner les commandes pour construire les 100 premiers bits de la suite produite par le LFSR classique de polynôme de rétroaction $1 + X^3 + X^5$ et initialisé par $[1, 0, 1, 0, 0]$. Donner les commandes pour construire ces 100 bits par un LFSR en mode Galois en précisant le polynôme de rétroaction et l'initialisation.

(g) Pour des implantations matérielles on préfère parfois représenter les LFSR en mode Galois plutôt qu'en mode classique (on dit Fibonacci). Pourquoi ?