TD3 - Primitives symétriques

Exercice 1. *Registres à décalage à rétroaction linéaire*

Un registre à décalage à rétroaction linéaire (LFSR) d'ordre n est défini par n *coefficients de rétroaction* $(c_0, \dots, c_{n-1})$. La mise à jour de l'état courant $(s_i, \dots, s_{i+n-1})$ est l'état $(s_{i+1}, \dots, s_{i+n-1}, \bigoplus_{j\geq 0} c_j s_{i+j})$. On note naturellement $s_{i+n} = \bigoplus_{j\geq 0} c_j s_{i+j}$.

Au lieu de voir les c_i et s_i comme des variables booléennes et d'utiliser les connecteurs logiques, il est plus pratique de les décrire comme des éléments du *corps fini à deux éléments*. On note $\mathbb{F}_2$ l'ensemble $\{0, 1\}$ muni des opérations $+$ et $\times$ *modulo* 2. Cela revient simplement à remplacer les ET par des $\times$ et les OU-EXCLUSIF par des $+$. Par exemple, $s_{i+n} = \sum_j c_j s_{i+j}$. *On admet que les opérations dans $\mathbb{F}_2$ se « comportent comme d'habitude », c'est-à-dire par exemple que $a \times (b + c) = a \times b + a \times c$, etc.*

Un LFSR $(c_0, \dots, c_{n-1})$ et un état initial $(s_0, \dots, s_{n-1})$ définissent une suite [1] $(s_m)_{m\geq 0}$ par $s_m = \sum_{j=0}^{n-1} c_j s_{m-n+j}$ pour $m \geq n$. On considère aussi la *suite des états* du LFSR $(\mathsf{st}_m)_{m\geq 0}$ où $\mathsf{st}_m = (s_m, \dots, s_{m+n-1})$.

Puisque les éléments manipulés sont des booléens, on représente les n-uplets (états ou coefficients du LFSR) par des mots binaires.

1. On considère le LFSR défini par les coefficients 1100.
   - **i.** Étant donné l'état initial $\mathsf{st}_0 = 1011$, calculer les états st_1 et st_2.
   - **ii.** Soit $c = 000001111001000$. On suppose que $c = m \oplus s_{[0,|m|[}$ où $(s_m)_m$ est la suite définie par le LFSR. Retrouver m.
2. Soit $(s_m)_m$ une suite définie par un LFSR d'ordre n. Montrer que s_m est ultimement périodique de période $T < 2^n$, c'est-à-dire qu'il existe $T < 2^n$ et $M \geq 0$ tels que pour tout $m \geq M$, $s_m = s_{m+T}$.

Soit (s_m) une suite définie par un LFSR de période maximale, $2^n - 1$. On considère $2^n - 1$ éléments consécutifs de cette suite. On veut montrer que statistiquement, ces $2^n - 1$ éléments se comportent presque comme s'ils avaient été tirés aléatoirement.

3. - **i.** Montrer que toute suite de $2^n - 1$ états successifs est constituée des $2^n - 1$ états non nuls.
   - **ii.** En déduire que dans n'importe quelle suite de $2^n - 1 + (k - 1)$ bits consécutifs, chaque suite de k bits apparaît 2^{n-k} fois si elle est non nulle, et $2^{n-k} - 1$ si elle est nulle.

Exercice 2. *LFSR inconnu*

On s'intéresse au problème suivant : étant donné la suite $(s_m)_m$ produite par un LFSR à n coefficients *inconnus*, on cherche à calculer les coefficients $(c_0, \dots, c_{n-1})$ du LFSR. On note $\vec{c}$ le vecteur (colonne) des c_i.

1. - **i.** On suppose $n = 3$. Construire une matrice S telle que $\mathsf{st}_{m+3} = S\vec{c}$.
   - **ii.** Généraliser à n quelconque : construire une matrice S telle que $\mathsf{st}_{m+n} = S\vec{c}$; exprimer S en fonction des st_i.
2. - **i.** Supposons que la matrice S n'est pas inversible. Montrer qu'il existe $k < n$ et $\lambda_0, \dots, \lambda_{k-1}$ tels que $\mathsf{st}_{m+k} = \sum_{j=0}^{k-1} \lambda_j \mathsf{st}_{m+j}$. *Rappel : une matrice est inversible si et seulement s'il n'existe pas de combinaison linéaire de ses colonnes qui s'annule.*
   - **ii.** En déduire que la suite $(s_n)_n$ est de période $< 2^n - 1$.
3. - **i.** En supposant que (s_m) est de période $2^n - 1$, donner un algorithme pour calculer les coefficients du LFSR à partir de $2n$ éléments consécutifs de $(s_m)_m$ et estimer sa complexité.
   - **ii.** Généraliser l'algorithme précédent sans hypothèse sur $(s_m)_m$, et estimer sa complexité.

1. Une telle suite est appelée une *suite récurrente linéaire d'ordre n*.