Master CSI 2 2013-2014

Cryptanalyse — M1MA9W06
Responsable : G. Castagnos

TP 3 — LFSR, Berlekamp-Massey

1 Le polynôme $f(X) = X^5+X^4+1$ sur $\mathbf{F}_2$ est le polynôme de rétroaction d'un LFSR de longueur 5.

1. Écrire une fonction qui simule une étape de ce LFSR : elle doit prendre en entrée l'état au temps t et ressortir l'état au temps $t+1$ et le bit de sortie. En déduire une fonction donnant les N premiers bits de ce LFSR, et prenant en paramètre son état initial.
2. Donner les 50 premiers bits de la suite d'état initial 00101. Déterminer sa période.
3. Généraliser vos fonctions pour prendre également le polynôme de rétroaction en paramètre (on supposera que le degré du polynôme est égal à la longueur de l'état initial). Tester en comparant vos résultats avec la fonction `lfsr_sequence` de Sage (attention au sens des coefficients du polynôme).

2 On s'intéresse maintenant aux cycles des registres d'un LFSR.

1. Écrire une fonction prenant en paramètre l'état initial du LFSR et le polynôme de rétroaction (de même degré que la longueur des registres) et retournant le cycle des registres obtenus, c'est à dire les différents registres obtenus dans une période.
2. Tester avec $f(X) = X^5 + X^4 + 1$ et les états initiaux 00101, 01000 et 10100. Que remarquez vous ?
3. Écrire une fonction prenant en paramètre le polynôme de rétroaction et retournant tous les cycles de registres possibles (en faisant varier l'état initial).
4. Combien de cycles produit le LFSR de longueur 5 de polynôme de rétroaction f ? Même question avec les LFSR de longueur 4 de polynômes de rétroaction $1+X^2+X^4$, $1+X+X^2+X^3+X^4$ et $1+X+X^4$. Quelles sont les propriétés de ces divers polynômes ?
5. Écrire une fonction qui prend en paramètre f et un état initial et qui renvoie le polynôme g telle que $Z(X) = g(X)/f(X)$ soit la série formelle du LFSR engendré par f et initialisé par l'état initial. Tester dans les différents cas de la question précédente si f est le polynôme minimal.

3 Profil de complexité

1. Implanter l'algorithme de Berlekamp-Massey pour retourner le profil de complexité d'une suite finie, c'est à dire la suite des $(\ell_k, P_k(X))$ associés aux suites tronquées $z^{(k)}$.
   On pourra comparer avec la fonction `lfsr_connection_polynomial` de Sage.

2. Tester sur quelques exemples de LFSR avec les polynômes de rétroaction de l'exercice précédent et les états initiaux de différents cycles.
3. Tester sur une suite finie aléatoire. Observer la fonction qui à k associe ℓ_k.

4 On note $(z_i)_{i\geq 0}$ la suite produite par un LFSR de polynôme de rétroaction X^7+X^6+1. On suppose que cette suite vérifie $z_{2i}=z_i$ pour tout $i\geq 0$. Quel est l'état initial $(z_0,z_1,\ldots,z_6)$ du LFSR ?

5 On a partiellement intercepté une suite binaire dont on sait qu'elle est produite par un LFSR de longueur 5 :

$$1,0,*,0,0,1,1,0,1,0,1,0,0,*,0,0,*,1,0,*,1$$

Peut on retrouver les bits manquants et le polynôme de rétroaction ?

6 Trace et LFSR

1. soit $\mathbf{F}=\mathbf{F}_{2^\ell}$. On note $\sigma(x)=x^2$ le Frobenius. On pose, pour tout $\alpha\in\mathbf{F}$,

$$\mathrm{trace}(\alpha)=\alpha+\alpha^2+\alpha^4+\cdots+\alpha^{2^{L-1}}=\alpha+\sigma(\alpha)+\cdots+\sigma^{\ell-1}(\alpha).$$

   (a) Montrez que $\mathrm{trace}(\alpha)\in\mathbf{F}_2$.
   (b) Montrez que $\mathrm{trace}(\alpha)+\mathrm{trace}(\beta)=\mathrm{trace}(\alpha+\beta)$ pour tout $\alpha,\beta\in\mathbf{F}$.
   (c) Soit $\alpha\in\mathbf{F}$. Montrez que, si $\mathrm{trace}(\alpha u)=0$ pour tout $u\in\mathbf{F}$, alors $\alpha=0$.

2. Soit $f(X)=1+c_1X+c_2X^2+\cdots+c_\ell X^\ell$ un polynôme de $\mathbf{F}_2[X]$ de degré ℓ que l'on suppose irréductible. On fixe une racine α de f dans F et on pose $\mathbf{F}=\mathbf{F}_2[\alpha]$.

   (a) On note $\gamma=\alpha^{-1}$. Montrez que, pour tout $\beta\in\mathbf{F}$, la suite définie par $z_j=\mathrm{trace}(\beta\gamma^j)$ pour $j\geq 0$ est engendrée par un LFSR de polynôme de rétroaction f.
   (b) Rappeler combien de suites distinctes sont engendrées par P, et en déduire que toute suite engendrée par P est de la forme précédente.
   (c) Pour tout entier t, on note $z^{(t)}$ la suite définie par

$$\left(z^{(t)}\right)_j=z_{tj},\forall j\geq 0$$

      i. Exemple : $f(X)=1+X^3+X^4$. On sait que f est irréductible sur $\mathbf{F}_2$ et que ses racines engendrent $\mathbf{F}_{16}^*$. Soit

$$z=1,0,0,0,1,0,0,1,1,0,1,0,1,1,1,\ldots$$

      Quels sont les bits suivants de z ? Calculez le début de $z^{(2)}$, $z^{(3)}$, $z^{(5)}$, et le plus petit polynôme qui les engendre.
      ii. Retour au cas général : montrez que la suite $z^{(t)}$ est engendrée par le polynôme minimal de α^t sur $\mathbf{F}_2$.

3. Déduire de tout cela un algorithme utilisant Berlekamp-Massey pour lister les polynômes irréductibles sur $\mathbf{F}_2$ de degré divisant ℓ.