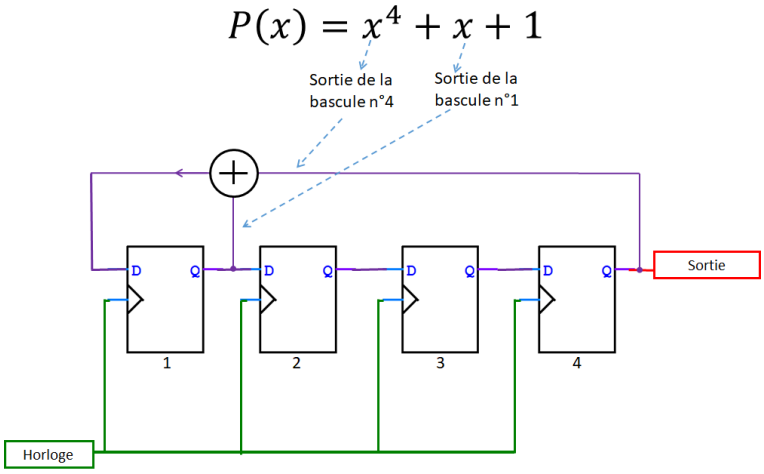
TP6 : Le générateur binaire pseudo-aléatoire par LFSR

Dans un LFSR (Linear Feedback Shift Register), la position des entrées du XOR peut être représentée par un polynôme. Exemple :



Le terme 1 est toujours présent ; le terme x^k est présent si la sortie de la bascule k est connectée à l'entrée d'un XOR.

La suite de bits générée est périodique. La valeur initiale des sorties des bascules peut être quelconque, en dehors de $00\ldots0$ (car $0 \oplus 0 = 0$ donc le contenu du registre ne change jamais). Voyons ce qui se passe avec la valeur initiale 0001.

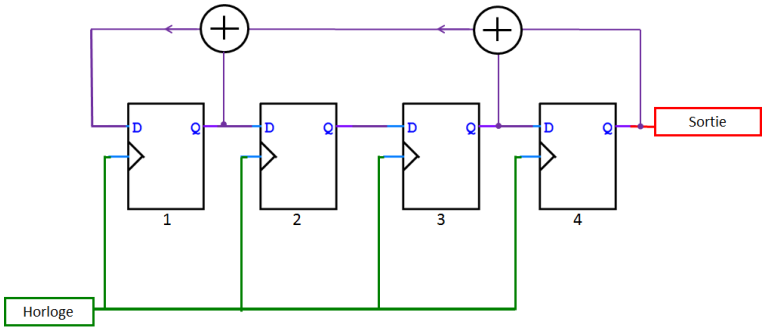
La sortie du XOR est $1 \oplus 0 = 1$ donc au front montant d'horloge, on trouve 1 en sortie de la bascule 1. Les nouvelles sorties des bascules 2, 3, 4, sont celles des bascules 1, 2, 3 avant le front d'horloge (décalage). Ainsi, on obtient après le front d'horloge 1000.

En refaisant le même travail, on obtient la séquence des états du circuit, représentés ci-dessous (d'abord sur la première ligne, de gauche à droite, puis sur la seconde ligne). Pour chaque état, le bit qui est émis est le plus à droite :

0001	1000	1100	1110	1111	0111	1011	0101
1010	1101	0110	0011	1001	0100	0010	0001

Dans la dernière case, on retrouve l'état initial. La suite de bits émise est donc *périodique*, et dans ce cas, la période vaut $15 = 2^n - 1$ où n est le nombre de bascules. La période est ici maximale.

Autre exemple :



Comme on calcule le XOR des sorties des bascules 1, 3 et 4, on a le polynôme :

$$P(x) = x^4 + x^3 + x + 1$$

De nouveau, voyons ce qui se passe avec la valeur initiale 0001 :

0001	1000	1100	1110	0111	0011	0001

Cette fois, la période vaut seulement 6. Ainsi, le le polynôme va déterminer la période.

Il est intéressant d'obtenir une période la plus grande possible ; on montre que la période maximale est $2^n - 1$, où n est le nombre de bascules. Il a été montré qu'on l'obtient pour les polynômes suivants [1] :

Nombre de bascules (n)	Polynôme
2, 3, 4, 6, 7, 22	$x^n + x + 1$
5, 11, 21, 29	$x^n + x^2 + 1$
8, 19	$x^n + x^6 + x^5 + x + 1$
9	$x^n + x^4 + 1$
10, 17, 20, 25, 28	$x^n + x^3 + 1$
12	$x^n + x^7 + x^4 + x^3 + 1$
13, 24	$x^n + x^4 + x^3 + x + 1$
14	$x^n + x^{12} + x^{11} + x + 1$
16	$x^n + x^5 + x^3 + x^2 + 1$
18	$x^n + x^7 + 1$
23	$x^n + x^5 + 1$
26, 27	$x^n + x^8 + x^7 + x + 1$
30	$x^n + x^{16} + x^{15} + x + 1$

1. Il en existe d'autres, mais ceux-là ont le nombre minimal de termes pour un degré donné.