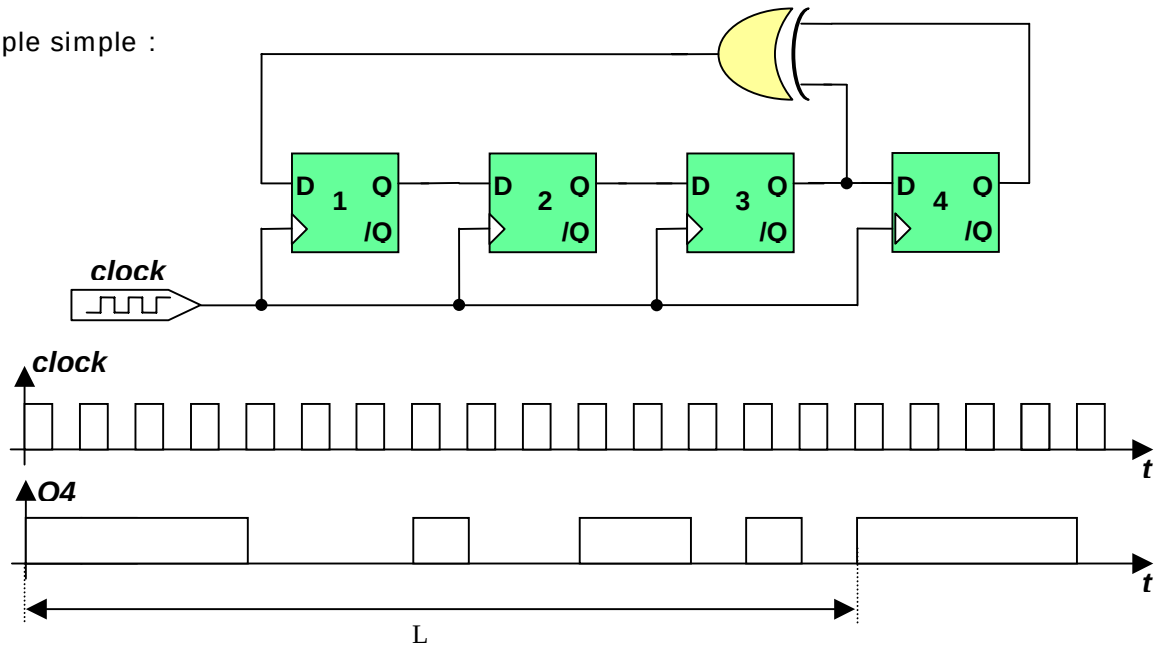
Pseudo Random Binary Generator

Introduction

La génération de séquence binaire pseudo aléatoire peut se réaliser avec des registres à décalage à rétroaction linéaire ou *Linear Feedback Shift Registers* (LFSRs). La théorie qui se cache derrière ces dispositifs fait appel au calcul algébrique dans le corps de Galois GF(2).

Exemple simple :



La séquence binaire obtenue dure L = $(2^N-1).T_{CLK}$ ou N est le nombre de bascules et T_{CLK} la période d'horloge. Si N devient grand alors l'observation d'une des sorties des N bascules laisse apparaître une série apparemment aléatoire de 1 et de 0. La période L de répétions très grande justifie le nom de séquence pseudo aléatoire.

Pour obtenir une séquence maximale il est nécessaire d'effectuer un rebouclage avec les valeurs données dans le tableau ci dessous.

Table

Nombre de bascules	Rebouclage D1= Qi ⊕ Qj ⊕ ..	Période	Nombre de bascules	Rebouclage D1= Qi ⊕ Qj ⊕ ..	Période
3	3,2	7	18	18,11	262 143
4	4,3	15	19	19,6,2,1	524 287
5	5,3	31	20	20,17	1 048 575
6	6,5	63	21	21,19	2 097 151
7	7,6	127	22	22,21	4 194 303
8	8,6,5,4	255	23	23,18	8 388 607
9	9,5	511	24	24,23,22,17	16 777 215
10	10,7	1023	25	25,22	33 554 431
11	11,9	2047	26	26,6,2,1	67 108 863
12	12,6,4,1	4095	27	27,5,2,1	134 217 727
13	13,4,3,1	8191	28	28,25	268 435 455
14	14,5,3,1	16383	29	29,27	536 870 911
15	15,14	32767	30	30,6,4,1	1 073 741 823
16	16,15,13,4	65535	31	31,28	2 147 483 647
17	17,14	131071	32	32,22,2,1	4 294 967 295