Test et optimisation d'un générateur pseudo-aléatoire

I / Le test de la période

II/ Le test d'uniformité

III/ Le test d'indépendance

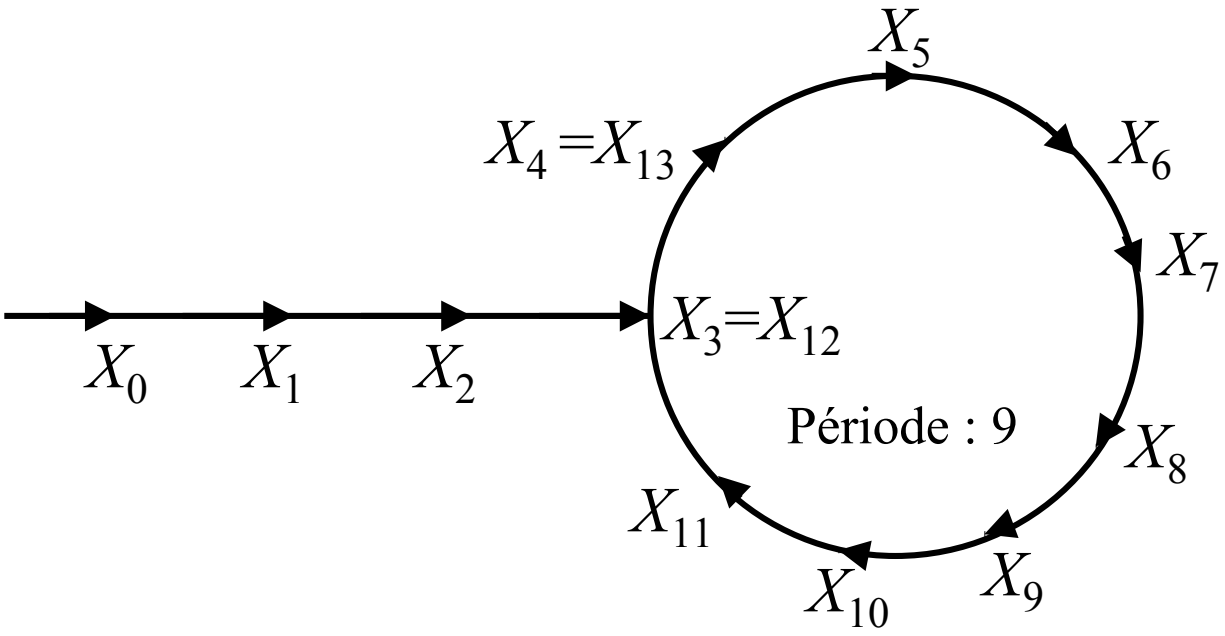
I / Le test de la période

Le Générateur Congruentiel Linéaire

Définition :

GCL(a,c,m,X_0) :

X_0 ; $X_{n+1} = (a\, X_n + c) \bmod m$



Formule générale :

$$X_{n+k} = \left[a^k X_n + (a^k - 1) \frac{c}{a-1} \right] \bmod m$$

Suite aléatoire normalisée :

$U_n = X_n / m$

I / Le test de la période

Le théorème de la période ($m=2^n$) :

$$\begin{array}{c} c \text{ impair} \\ a = 1 \mod 4 \end{array} \quad \Leftrightarrow \quad \lambda = 2^n$$

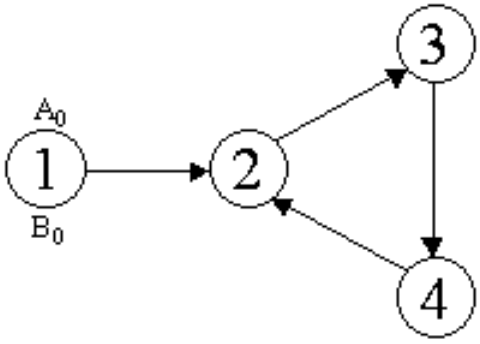
La détermination de la période :

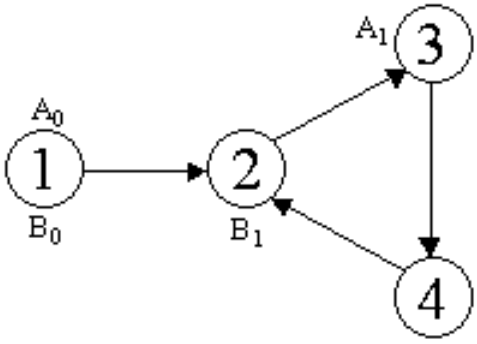
L'algorithme trivial : on compare tous les X_k avec les précédents.
Mémoire : O(n)
Temps : O(n^2)

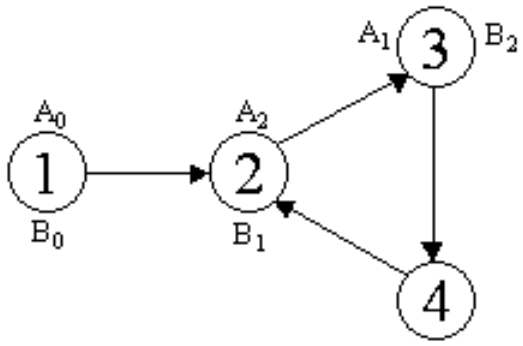
L'algorithme de Pollard : on compare X_k et X_{2k}.
Mémoire : O(1)
Temps : O(n)
Entre deux fois consécutives où $X_k=X_{2k}$, on a parcouru une période.

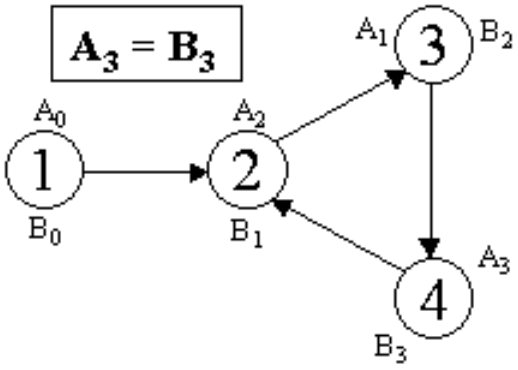
I / Le test de la période

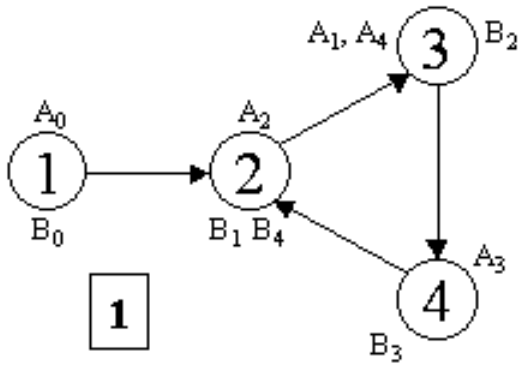
L'algorithme de Pollard :

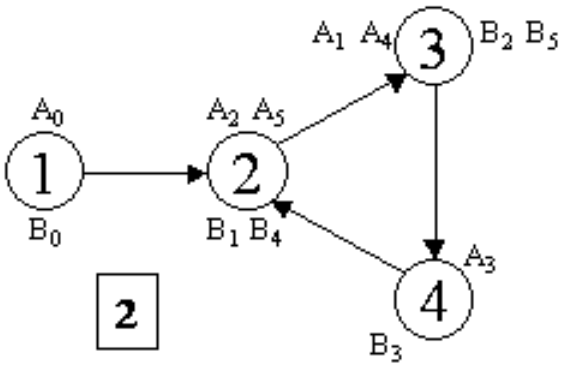


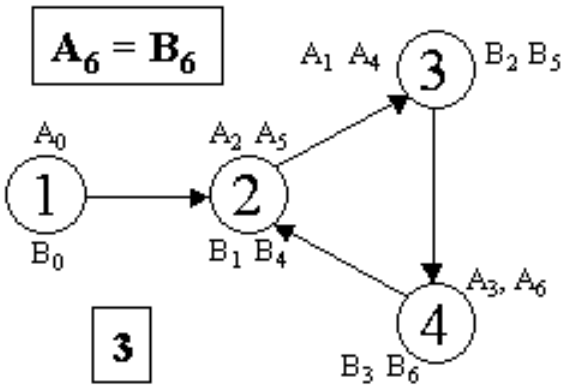












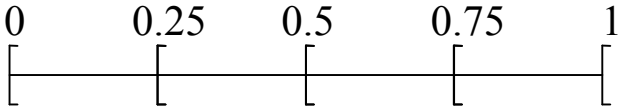
La période est donc 3

II / Le test d'uniformité

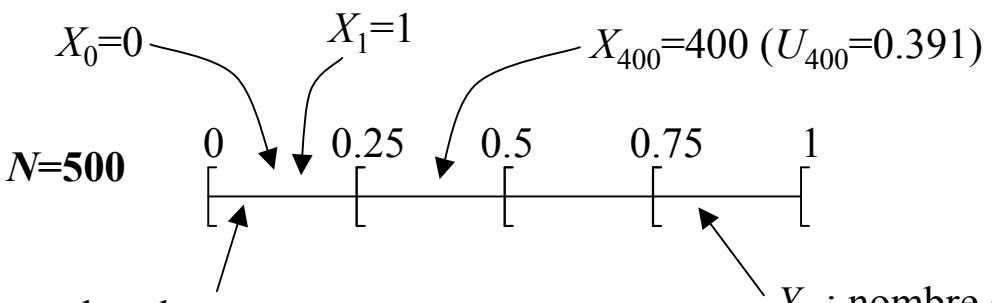
Déroulement du test :

- Choix de m catégories

Exemple : GCL(1,1,1024,0), m=4



- Affectation de chacun des X_k à l'une des catégories, pour $k<N$ (avec N grand, $N>5m^2$)



Y_1 : nombre de termes dans ce premier segment

Y_4 : nombre de termes dans ce quatrième segment

Répartition : Y_1=256 ; Y_2=245 ; Y_3=0 ; Y_4=0

Probabilité de tomber dans la s-ième catégorie : P_s=0.25

- Calcul de la variance $V = \sum_{s=1}^{m} \frac{(Y_s - N P_s)}{N P_s}$ V=501.5

- Utilisation du tableau de variances de référence :

m	1%	5%	25%	50%	75%	95%	99%
2	0.00016	0.00393	0.1015	0.5449	1.323	3.841	6.635
3	0.0201	0.1026	0.5754	1.386	2.773	5.991	9.21
4	0.1148	0.3518	1.213	2.366	4.108	7.815	11.34
5	0.2971	0.7107	1.923	3.357	5.385	9.488	13.28

générateur rejeté (variance trop grande)

Annexe

Tableau :

m	1%	5%	25%	50%	75%	95%	99%
2	0.00016	0.00393	0.1015	0.5449	1.323	3.841	6.635
3	0.0201	0.1026	0.5754	1.386	2.773	5.991	9.21
4	0.1148	0.3518	1.213	2.366	4.108	7.815	11.34
5	0.2971	0.7107	1.923	3.357	5.385	9.488	13.28
6	0.5543	1.1455	2.675	4.351	6.626	11.07	15.09
7	0.8721	1.635	3.455	5.348	7.841	12.590	16.81
8	1.239	2.167	4.255	6.346	9.037	14.07	18.48
9	1.646	2.733	5.071	7.344	10.220	15.510	20.09
10	2.088	3.325	5.899	8.343	11.39	16.92	21.67
11	2.558	3.940	6.737	9.342	12.550	18.310	23.210
12	3.053	4.575	7.584	10.34	13.7	19.68	24.72
13	3.571	5.226	8.348	11.340	14.850	21.030	26.22
>13	$m+\sqrt{2\,m}\,x_p+\frac{2}{3}x_p^2-\frac{2}{3}+O\left(\frac{1}{\sqrt{(m)}}\right)$						
x	-2.33	-1.64	-0.674	0	0.674	1.64	2.33