Générations et tests de suites pseudoaléatoires

Thème: Sports et Jeux

Perig MONTFORT

N° SCEI : 11965

Création d'un jeu de poker

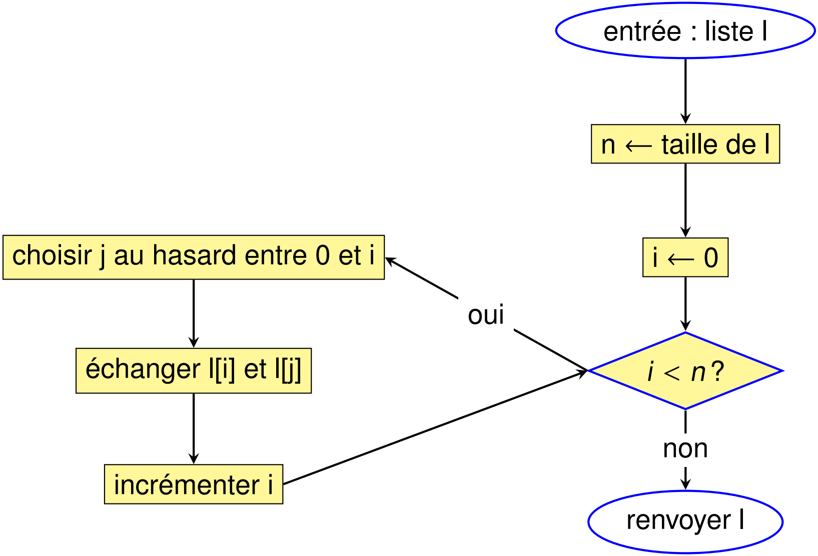
TIPE 2024

Table des matières

TIPE 2024

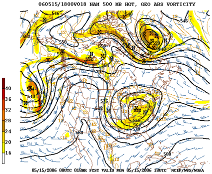
Introduction

Mélange de Knuth



Différentes utilisations de l’aléatoire sur ordinateur

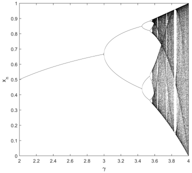
(a) Cryptage d’informations



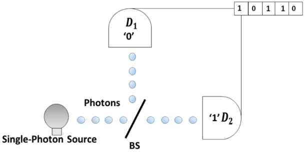
(b) Simulations météorologiques

(c) Jeux en ligne

Différentes méthodes de génération



(a) Procédés algorithmiques



(b) Procédés quantiques

(c) Lavarand, un procédé matériel

Comment faire pour simuler l'aléatoire qui est non déterministe à l'aide d'outils déterministes ?

Von Neumann

Premier générateur - méthode de Von Neumann

Principe

Soit un nombre u_n, la méthode de Von Neumann permetant de générer le nombre u_{n+1} consiste à élever le nombre u_n au carré puis de prendre les chiffres du milieu comme sortie.

Exemple

La suite u_n de graîne 1725 sera créée de cette manière :

$$u_1 = 1725$$

$$u_1^2 = 02\underline{9756}25$$

$$u_2 = 9756$$

$$u_3 = 1795,\ u_4 = 2220,\ u_5 = 9284,\ u_6 = 1926$$

$$u_7 = 7094,\ u_8 = 3248,\ u_9 = 5495,\ u_{10} = 1950...$$

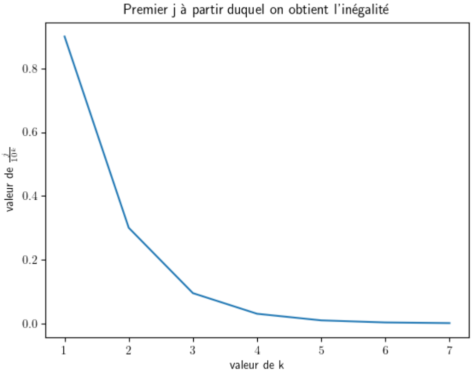
TIPE 2024

Faible périodicité

Probabilité d'obtenir un cycle

La probabilité de ne pas obtenir de cycle après j tirages est :

$$P_j = \prod_{i=0}^{j-1}\left(1 - \frac{i}{10^k}\right)$$



Générateur à congruence linéaire

Second générateur - générateur à congruence linéaire

Principe

Soient $m \in \mathbb{N}$, $(a, c, X_0) \in [[0; m-1]]^3$, on génère la suite X_n par :

$$X_{n+1} = aX_n + c \; mod \; m$$

Exemple

La suite u_n de graîne $X_0 = 17$, de multiplicateur $a = 13$, d'incrément $c = 25$ et de modulo $m = 64$ sera créée de cette manière :

$$X_0 = 17$$

$$X_1 = (17 * 13 + 25) mod \; 64 = 246 \; mod \; 64 = 54$$

$$X_2 = 21, \; X_3 = 4, \; X_4 = 13$$

$$X_5 = 2, \; X_6 = 48, \; X_7 = 9...$$

TIPE 2024

Etude du générateur congruentiel linéaire

Objectif : Ne pas commencer chaque partie à X_0

Solution :

Proposition (Formule explicite)

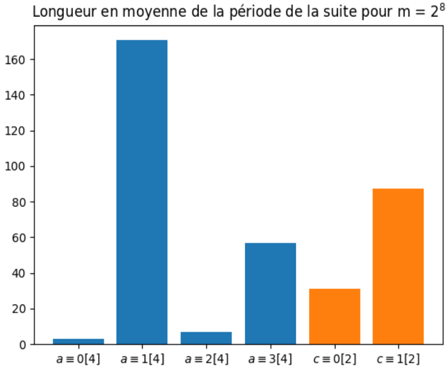
Soient $n \in \mathbb{N}, k \in \mathbb{N}^*$: $X_{n+k} = (a^k X_n + c\frac{(a^k - 1)}{a-1})$ *mod* m

Pour trouver k on peut utiliser différentes solutions :

- Utilisation d'une autre suite pseudo-aléatoire
- Générateurs matériels comme lavarand
- Utilisation de données physiques connues comme le temps, la température du processeur...

TIPE 2024

Périodicité du générateur



Proposition (Choix de a et c pour $m = 2^n$)

Soit λ la périodicité : $a \equiv 1[4] \land c \equiv 1[2] \Leftrightarrow \lambda = 2^n$

TIPE 2024

Cas général pour un m quelconque

Soit λ la périodicité, $m = m_1^{\alpha_1}...m_d^{\alpha_d}$ la décomposition en produit de facteurs premiers de m, alors $\lambda = m$ si et seulement si :

- $c \wedge m = 1$
- $a - 1$ est multiple de m_i, $\forall i \in [\![1\ ;\ d]\!]$
- si m est multiple de 4, $a - 1$ est multiple de 4

On priorisera $m = 2^n$ sauf en cas de rejet de ces suites puisque la congruence modulo 2^n est facile.

Blum Blum Shub

Dernier générateur - Blum Blum Shub

Principe

Soit $M = pq$ avec p et q deux grands nombres premiers congrus à 3 modulo 4, soit (x_n) la suite définie par : $x_0 \wedge M = 1$ et pour tout n, $x_{n+1} = x_n^2 \bmod M$. On pose la suite (u_n) de Blum Blum Shub tel que pour tout n, u_n soit le bit le moins significatif de x_n

Exemple

On prend $p = 11, q = 23, x_0 = 7$

$$x_1 = x_0^2 \ mod \ pq = 49 \ mod \ 253 = 49$$

$$49 = \overline{110001}^2 \implies u_1 = 1$$

$$x_2 = 49^2 \ mod \ 253 = 2401 \ mod \ 253 = 124$$

$$124 = \overline{1111100}^2 \implies u_2 = 0$$

TIPE 2024

Etude de Blum Blum Shub

Formule explicite

Soient $n \in \mathbb{N}$, $(p, q) \in \mathbb{N}^2$, $N = pq$ et $x_0 \wedge N = 1$:

$$x_n = x_0^{2^n \ mod \ \phi(N)} \ mod \ N$$

où $\phi(N) = (p-1)(q-1)$ avec ϕ la fonction d'Euler.

Affinement de la formule

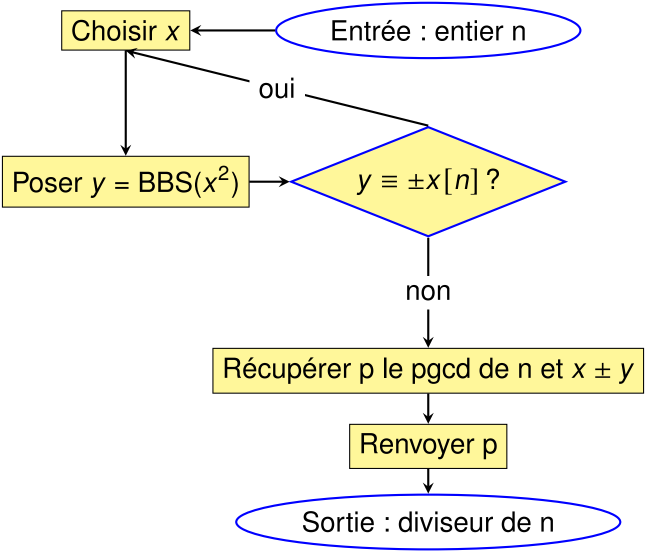
Soient $n \in \mathbb{N}$, $(p, q) \in \mathbb{N}^2$, $N = pq$ et $x_0 \wedge N = 1$:

$$x_n = x_0^{2^n \ mod \ \lambda(N)} \ mod \ N$$

où $\lambda(N) = \dfrac{(p-1)(q-1)}{(p-1) \wedge (q-1)}$ avec λ la fonction de Carmichael.

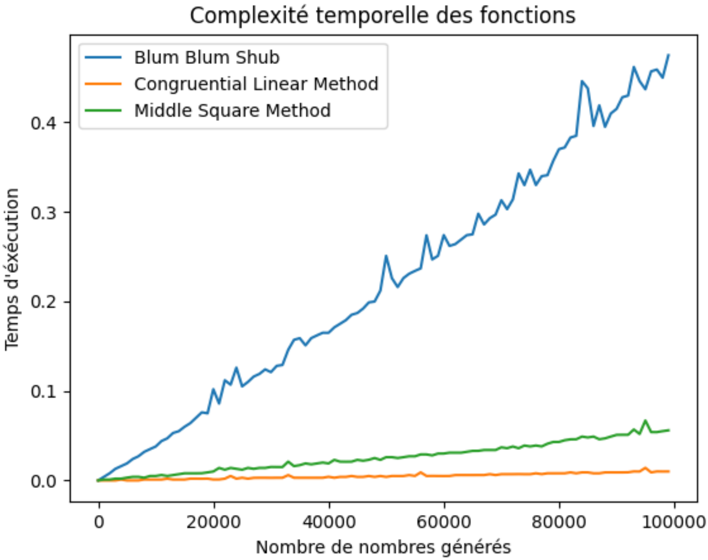
TIPE 2024

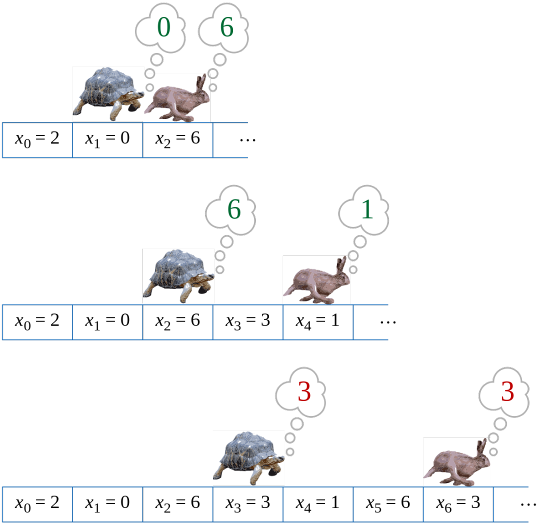
Difficulté d’extraire la racine sans connaître N



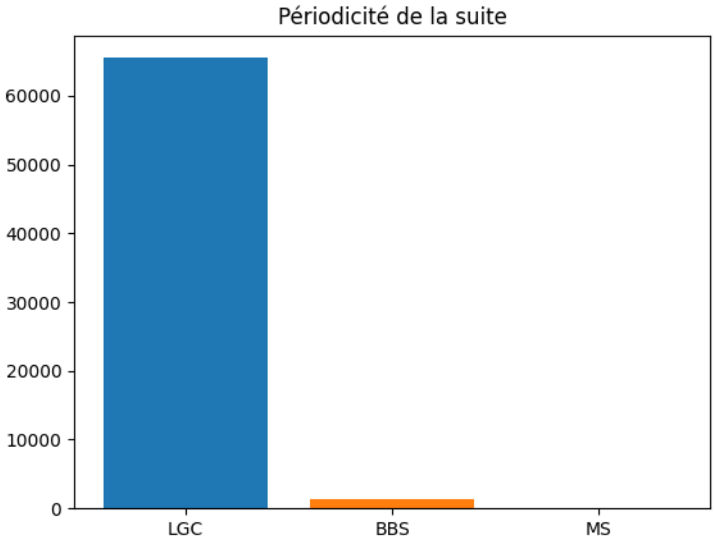
Tests des générateurs

Temps d'éxécution




0
6
$x_0 = 2$ | $x_1 = 0$ | $x_2 = 6$ | …
6
1
$x_0 = 2$ | $x_1 = 0$ | $x_2 = 6$ | $x_3 = 3$ | $x_4 = 1$ | …
3
3
$x_0 = 2$ | $x_1 = 0$ | $x_2 = 6$ | $x_3 = 3$ | $x_4 = 1$ | $x_5 = 6$ | $x_6 = 3$ | …

Périodicité



Premier test : Le test du Chi-Carré

Formule

Soit n $\in \mathbb{N}$, soit $p = (p_i)_{i \in [\![1\ ;\ n]\!]}$ et $q = (q_i)_{i \in [\![1;n]\!]}$ deux vecteurs.
On définit l'adéquation de p par rapport à q χ^2 par :

$$\chi^2(p, q) = \sum_{i=1}^{n} \frac{(p_i - q_i)^2}{q_i}$$

Sens des notations

p désignera les valeurs empiriques et q les valeurs théoriques obtenues par une loi X
On note D le degré de liberté de χ^2 et on pose une risque α d'erreur.
On peut comparer nos valeurs obtenues par rapport au tableau du chi carré.

TIPE 2024

Tableau du Chi-Carré (observations)

Degrés de liberté	valeurs limites pour $\alpha = 0.05$
1	3.841
2	5.991
3	7.815
4	9.488
5	11.070
6	12.592
7	14.067
8	15.507
9	16.919
10	18.307
100	113.145
N-1>100	$N + 1.64\sqrt{2N} + \frac{2}{3}(1.64^2 - 1) + O(\frac{1}{\sqrt{N}})$

Exemple

On prend les 1000 premiers nombres du générateur congruentiel linéaire $x_0 = 1, a = 67, c = 1, m = 2^{12}$ et on pose $h = \dfrac{m}{8}$

Intervalle	Valeurs dedans	Nombre attendu	Ecart
$[0; h-1]$	104	125	3.528
$[h; 2h-1]$	134	125	0.648
$[2h; 3h-1]$	116	125	0.648
$[3h; 4h-1]$	131	125	0.288
$[4h; 5h-1]$	143	125	2.592
$[5h; 6h-1]$	120	125	0.200
$[6h; 7h-1]$	134	125	0.648
$[7h; m-1]$	118	125	0.392
Total :	1000	1000	8.944

Ici $8.944 \leq 14.067$ donc le test est validé.

TIPE 2024

Deuxième test : Test Spectral

Principe

Le test Spectral sur une suite $(u_n)_{n\in\mathbb{N}}$ en dimension k consiste à étudier la répartition du nuage de points $(u_n, u_{n+1}, ..., u_{n+k-1})$ pour tout n

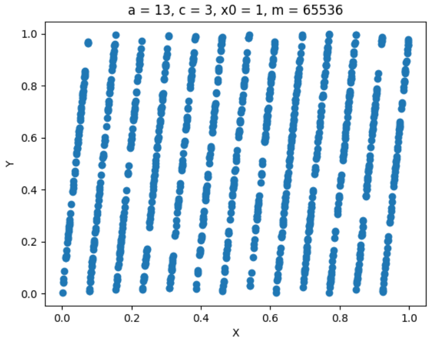


Figure – Exemple d'un test Spectral en dimension 2

Intérêt de passer à la dimension supérieure

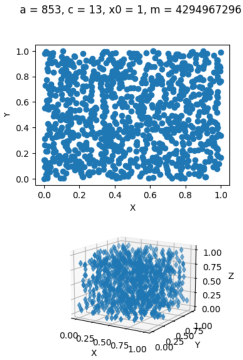


Figure – Test Spectral valide en dimensions 2 et 3

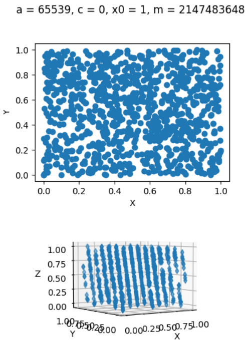


Figure – Test Spectral valide en dimension 2 mais invalide en dimension 3

TIPE 2024

Troisième test : test sur un jeu de poker

Pour un jeu de 52 cartes dont on tire 5 cartes on aura ce tableau :

Main	Jeux	Probabilité (%)	Jeux / 2M coups
Quinte flush royale	4	0.000154	3.08
Quinte flush	36	0.00139	27.7
Carré	624	0.024	480
Full	3 744	0.144	2 881
Couleur	5 108	0.197	3 930
Quinte	10 200	0.392	7 849
Brelan	54 912	2.133	42 256
Deux paires	123 552	4.754	95 078
Paire	1 098 240	42.257	845 138
Carte haute	1 302 540	50.118	1 002 354
Total	2 598 960	100	2 000 000

TIPE
2024

Un test sur une suite LGC

On va tester la suite $a = 121$, $c = 1$, $m = 2^{32}$

Main	Empiriques	Théoriques	Ecart
Quinte flush royale	2	3.08	0.378
Quinte flush	70	27.7	64.058
Carré	556	480	12.033
Full	2 755	2 881	98.958
Couleur	8 353	3 930	$\boxed{4942.784}$
Quinte	7 059	7 849	77.801
Brelan	42 368	42 256	1.998
Deux paires	95 078	95 080	3.477
Paire	843 018	845 138	5.332
Carte haute	1 000 164	1 002 354	4.811
Total	2 000 000	2 000 000	5211.629

Le test n'est pas validé. On remarque une grosse disparité pour Couleur

TIPE 2024

On va tester la suite $p = 1028207$, $q = 996803$, $x_0 = 425431$

Main	Empiriques	Théoriques	Ecart
Quinte flush royale	2	3.08	0.38
Quinte flush	22	27.7	1.17
Carré	484	480	0.03
Full	2 903	2 881	0.17
Couleur	4 010	3 930	1.63
Quinte	7 622	7 849	6.57
Brelan	42 318	42 256	0.09
Deux paires	95 735	95 080	4.51
Paire	844 478	845 138	0.52
Carte haute	1 003 425	1 002 354	1.14
Total	2 000 000	2 000 000	16.21

Le test est validé tout justement.

Conclusion

Conclusion

	Middle Square	GCL $m = 2^n$	GCL $m = 2^n \pm 1$	BBS
Sûreté	$\approx$	$\approx$	$\approx$	✓
Rapidité	$\approx$	✓	$\approx$	✗
Périodicité	✗	✓	✓	$\approx$
Uniformité	✗	✓	✓	✓
k-uniformité	✗	$\approx$	$\approx$	✓
Jeu de poker	✗	✗	✓	✓

Pour jeu en ligne avec plusieurs parties simultanées : GCL avec $m = 2^n \pm 1$
Pour tournois avec enjeu important et peu de parties : Blum Blum Shub

TIPE 2024

Merci !