Générateurs de nombres aléatoires
Cours 1 - Générateurs à congruences linéaires

L. Naert
Merci à A. Ridard pour son cours

Vannes
iut :
Université Bretagne Sud

A propos de ce document

- Pour naviguer dans le document, vous pouvez utiliser :
  - le menu (en haut à gauche)
  - l'icône en dessous du logo IUT
  - les différents liens
- Pour signaler une erreur, vous pouvez envoyer un message à l'adresse suivante : lucie.naert@univ-ubs.fr

Plan du cours

Vannes iut : Université Bretagne Sud

Organisation

- Espace Moodle : Générateurs de nombres aléatoires
- Cours les mercredis matins pendant 3 semaines jusqu'aux vacances de Pâques
- 1 CM suivi de 2 séances de travaux pratiques sur machine
- 1 Jupyter Notebook à rendre chaque semaine sur Moodle
- Contrôle terminal le lundi 6 mai (durée : 1h30)

Évaluation

- Contrôle terminal (coeff. 3)
- 1 TP noté sur les 3 (coeff. 1)

Définitions

Définition (aléatoire)

De "aléa" en latin qui signifie "dé" ou "jeu de dés". Un processus aléatoire est un processus soumis au hasard.

Définition (Générateur de nombres aléatoires - première définition)

Programme dont le but est de produire une suite de nombres tirés "au hasard".

Mais qu'est-ce que le hasard ?

Voici quelques exemples de suites d'entiers compris entre 1 et 6. Sont-elles aléatoires ?

1. $6,6,6,6,6,6,6,6,6,6,6,6,6,6$
2. $1,2,3,4,5,6,1,2,3,4,5,6,1,2,3,4,5,6$
3. $1,3,2,4,1,2,1,5,4,1,1,6,4,3,6,1,2,4,$

Il est difficile de dire ce qui est aléatoire et ce qui ne l'est pas.
Mais on peut avoir une bonne intuition en utilisant, par exemple :

- la fréquence : chaque nombre doit avoir la même chance d'apparaitre (équiprobable)
- la prédictibilité : il ne doit pas être possible de prédire le terme suivant de la suite. En effet, la suite ne doit pas présenter de structure ou de corrélation identifiable

Vannes iut : Université Bretagne Sud

Nous avons besoin d'aléatoire

- dans les jeux vidéos : initialisation différente d'un monde à chaque partie, nature des loots...
- pour des simulations de jeux de hasard : lancé de dès, de pièces, roulette et autres jeux de Casino
- pour simuler des processus biologiques ou physiques : désintégration des atomes radioactifs par exemple
- dans la vie d'un prof : tirage d'un(e) étudiant(e) pour aller au tableau, placement des étudiant(e)s dans la salle d'examen
- dans la vie d'un étudiant : ?
- à un niveau national : tirage aléatoire des jurés pour participer à certains procès, aux conventions citoyennes (sur le climat, sur la fin de vie...), tirage au sort par des entreprises de sondage, pour le recensement...
- en cryptographie : génération d'une clef jetable pour le chiffrement d'un message
- ...

Procédés physiques

Il est possible de générer de l'aléatoire en utilisant des sources physiques :

- lancers de dès, de pièces, de roulettes
- détection de vibrations sismiques,
- température (à très haute précision)
- microsecondes de l'horloge de l'ordinateur

Mais, ce sont des procédés :

- **non reproductibles** (problématique en cryptographie pour l'opération de déchiffrement, ou pour rejouer une simulation précise) → finalement, on a besoin d'un aléatoire contrôlé !
- peu analysables (et donc peu fiables, peut-être)
- lourds à mettre en œuvre et à associer avec une procédure numérique.

Ces procédés, et notamment les micro-secondes de l'ordinateur, restent cependant utilisés pour **initialiser** les générateurs aléatoires.

Générateurs pseudo-aléatoires

Les générateurs de nombres aléatoires sont des programmes permettant de produire une suite de nombre aléatoire.

Ces générateurs doivent respecter les propriétés suivantes :

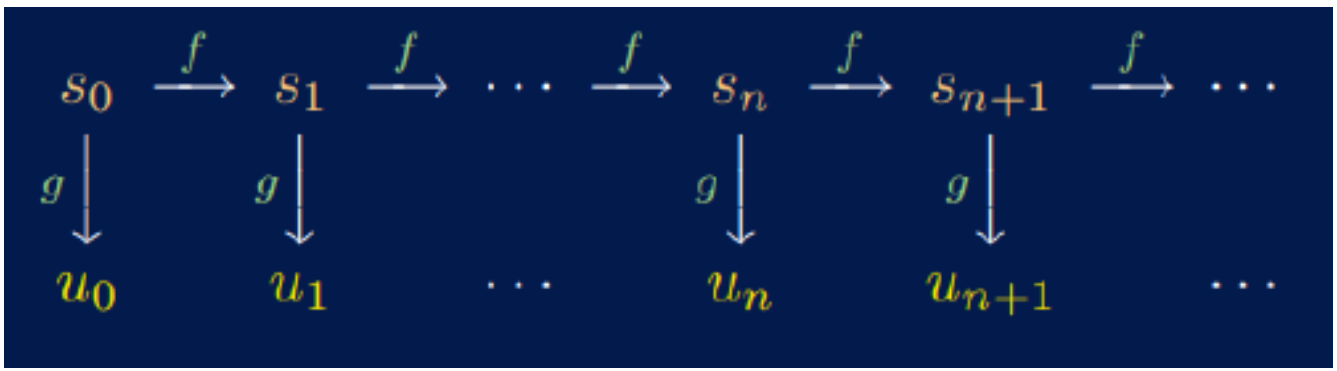
- déterminisme : un même départ à paramètres internes identiques doit produire la même suite.
- reproductibilité : il doit être possible de retrouver la suite.
- fiabilité/équiprobabilité : la fréquence d'apparition de chaque nombre est identique quand le nombre de tirage tend vers l'infini.
- facile à mettre en œuvre algorithmiquement.
- rapides en temps de calcul.

Les suites sont déterministes et reproductibles. Il s'agit donc d'un aléatoire apparent : les générateurs sont donc **pseudo-aléatoires** (GPA).

Définition formelle

Un GPA est caractérisé par un quadruplet (S, f, U, g) :

- S est l'ensemble (très grand mais fini) des états contenant la graine s_0
- $f : S \to S$ est la fonction de transition permettant de calculer $s_n = f(s_{n-1})$
- U est l'ensemble des valeurs de sortie (souvent $U = [0; 1[$)
- $g : S \to U$ est la fonction de sortie permettant d'obtenir $u_n = g(s_n)$



Une fois la graine s_0 choisie (au hasard : par exemple en utilisant les millisecondes de l'horloge), toutes les sorties sont entièrement déterminées !

Générateurs congruentiels linéaires (GCL)

Un GCL est défini par :

- $S = \{0, 1, ..., m-1\}$
- $f(s) = as + b \ [m]$
- $U = [0; 1[$
- $g(s) = \frac{s}{m}$

Quels sont les éléments dont nous avons besoin pour déterminer une suite aléatoire produite par un GCL ?

1. Calculer les 10 premiers nombres de la suite produite par le GCL de paramètres : $a = 3, b = 5, m = 10, s_0 = 2$.
2. Calculer les 10 premiers nombres de la suite produite par le GCL de paramètres : $a = 3, b = 5, m = 10, s_0 = 0$.
3. Calculer les 10 premiers nombres de la suite produite par le GCL de paramètres : $a = 4, b = 4, m = 10, s_0 = 1$.
4. Que remarquez-vous ?

Périodicité des GCL

Le nombre d'états S étant fini, il y aura forcément répétition d'un état à un moment donné. Or, l'état suivant dépend de l'état courant. La suite est donc **ultimement périodique**, c'est à dire périodique à partir d'un certain rang :

$$\exists T \in \mathbb{N}^*, \exists n_0 \in \mathbb{N}, \forall n \geq n_0, s_{n+T} = s_n$$

Le plus petit entier T vérifiant cette condition est appelé période de la suite.
Si la suite est ultimement périodique à partir du rang 0, on dit qu'elle est également périodique.

Les GCL produisent toujours des suites ultimement périodiques. Les concepteurs de GCL cherche donc à proposer des GCL avec une période maximale quelle que soit la graine s_0. Quelle est la valeur de cette période maximale ?

Période maximale

Pour $b \neq 0$ [1], un GCL de paramètres a, b, m est de période maximale (égale à m) quelle que soit la graine si et seulement si :

1. b et m sont premiers entre eux
2. Tout nombre premier p qui divise m doit également diviser $a-1$
3. Si m est un multiple de 4 alors $a-1$ doit également être un multiple de 4.

Ces conditions sont appelées "Critères de Knuth".

Pour $m = 16$, proposer des valeurs de a et b telles que la suite produite est de période maximale.

1. Nous ne verrons pas les critères dans le cas où $b = 0$.

Exemples de GCL ($b \neq 0$)

- la fonction `rand()` du langage C ANSI est définie par :

$$m = 2^{31},\ a = 1103515245 \text{ et } b = 12345$$

- la fonction `drand48()` du langage C ANSI est définie par :

$$m = 2^{48},\ a = 25214903917 \text{ et } b = 11$$

Exemples de GCL ($b = 0$)

- le générateur `RANDU` implanté sur les IBM des années 60 est défini par :

$$m = 2^{31} \text{ et } a = 65539$$

- le générateur du logiciel de calcul formel `MAPLE` est défini par :

$$m = 10^{12} - 11 \text{ et } a = 427419669081$$

C'est le cas $b = 0$ que nous allons maintenant généraliser.

Générateurs multi-récursifs (GMR)

Un GMR d'ordre k est défini par :

- $S = \{0, 1, ..., m-1\}^k$
- La fonction de transition est, cette fois, appliquée à un vecteur[2] $\boldsymbol{s}$:

$$f(\boldsymbol{s}) = f(s^{(1)}, s^{(2)}, ..., s^{(k)})$$
$$= (s^{(2)}, ..., s^{(k)}, a_1 s^{(1)} + a_2 s^{(2)} + ... + a_k s^{(k)} [m])$$

- $U = [0; 1[$
- $g(\boldsymbol{s}) = \frac{s^{(k)}}{m}$

- Un GMR avec $k = 1$ est un GCL où $b = 0$.
- Un GMR avec $m = 2$ est un LFSR[a]

a. cf. cours suivant

2. Les vecteurs sont notés en gras

1. Donner un exemple de graine possible pour $k = 2$ et $m = 3$.
2. Calculer les 5 premiers termes de la suite générée par un GMR de paramètres $k = 3$, $a_1 = 2$, $a_2 = 0$, $a_3 = 5$ et $m = 10$, et de graine $s_0 = (1, 0, 3)$.

GMRs combinés

Un GMR combiné est un générateur composé de plusieurs GMR d'ordre k.

Un tel générateur sera défini de la façon suivante (exemple d'un générateur composé de deux GMR d'ordre 3) :

- $S = S_1 x S_2$ avec $S_i = \{0, 1, ..., m_i - 1\}^3$
- $f(\boldsymbol{s}) = f(\boldsymbol{s}_1, \boldsymbol{s}_2) = (f_1(\boldsymbol{s}_1), f_2(\boldsymbol{s}_2))$ avec :

$$f_i(\boldsymbol{s_i}) = (s_i^{(2)}, s_i^{(3)}, a_{i1} s_i^{(1)} + a_{i2} s_i^{(2)} + a_{i3} s_i^{(3)} [m_i])$$

- $U = [0; 1[$
- $g(\boldsymbol{s}) = \frac{s_1^{(3)} - s_2^{(3)} [m_1]}{m_1}$

MRG32k3 (L'Ecuyer 1999)

Le MRG32k3 est un GMR combiné d'ordre 3 tel que :

- $a_{11} = 0$,
  $a_{12} = 1403580$,
  $a_{13} = -810728$,
  $m_1 = 2^{32} - 209$

- $a_{21} = 527612$,
  $a_{22} = 0$,
  $a_{23} = -1370589$,
  $m_2 = 2^{32} - 22853$

Générateurs digitaux

Un générateur digital d'ordre k est défini par :

- $S = \{0,1\}^k$
- $f(\boldsymbol{s}) = A(s)$ où A est une matrice $k \times k$
- $U = [0;1[$
- $g(\boldsymbol{s}) = ((B\boldsymbol{s})_i[2])2^{-i}$ où B est une matrice $w \times k$

Un LFSR (d'ordre k) est un tel générateur avec :

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ a_1 & a_2 & a_3 & \dots & a_k \end{pmatrix}$$

et $B = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & & & \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \end{pmatrix}$

Précision et période

Une suite (s_n) de nombres produits par un GPA :

- mime des variables aléatoires uniformes sur $\{\frac{0}{K}, \frac{1}{K}, \ldots, \frac{K}{K}\}$ et non sur $[0,1]$ à cause de la précision nécessairement finie des nombres réels dans un ordinateur.
- est ultimement périodique du fait de l'ensemble fini S d'états internes du GPA.

La période :

- est sensible à la nature et aux paramètres du GPA
- doit être la plus grande possible.

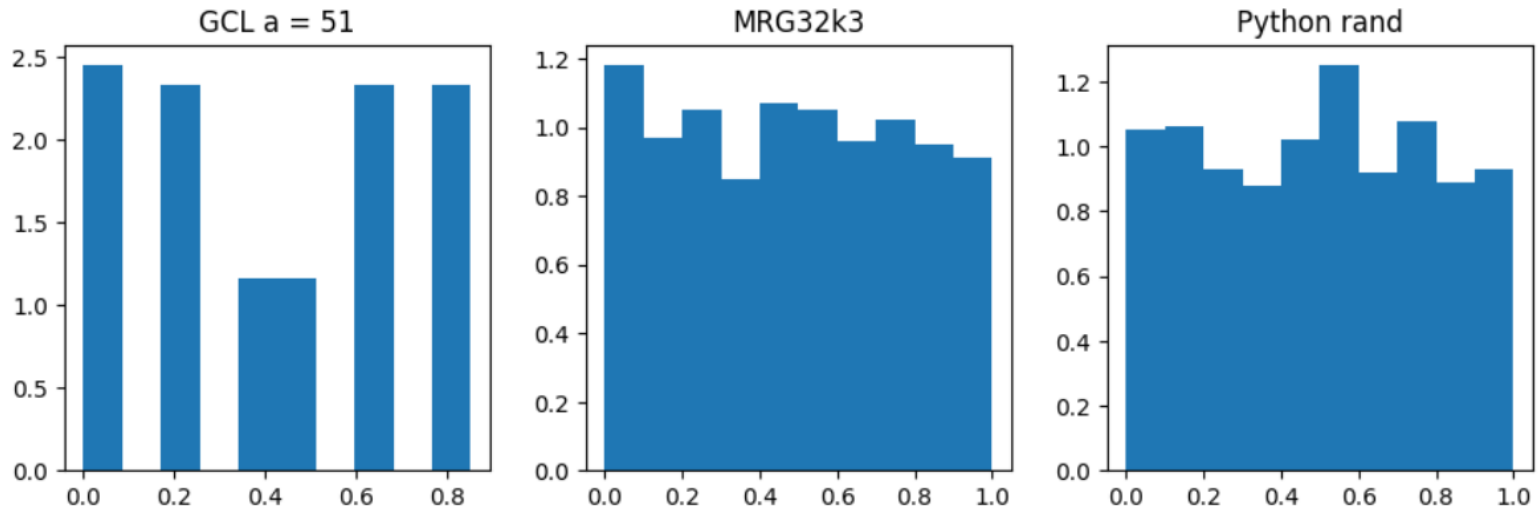
La conception d'un bon GPA nécessite une analyse théorique. Tout GPA doit être testé avant usage.

Tests statistiques

- Pour écarter des générateurs ne présentant pas les qualités requises, de nombreux tests statistiques ont été élaborés pour détecter un éventuel biais du générateur.
- On peut citer la batterie de tests Diehard comprenant par exemple le "test d'espacement des anniversaires" ou le "test des places de parking".
- Pour citer l'adéquation entre la loi empirique et la loi théorique, on peut faire un test d'ajustement (test du chi2 ou de Kolmogorov-Smirnov).
- **Test spectral** : L'idée de ce test est de représenter visuellement la suite des nombres pseudo-aléatoires générés en 1, 2 ou 3 dimensions.

Test spectral à une dimension

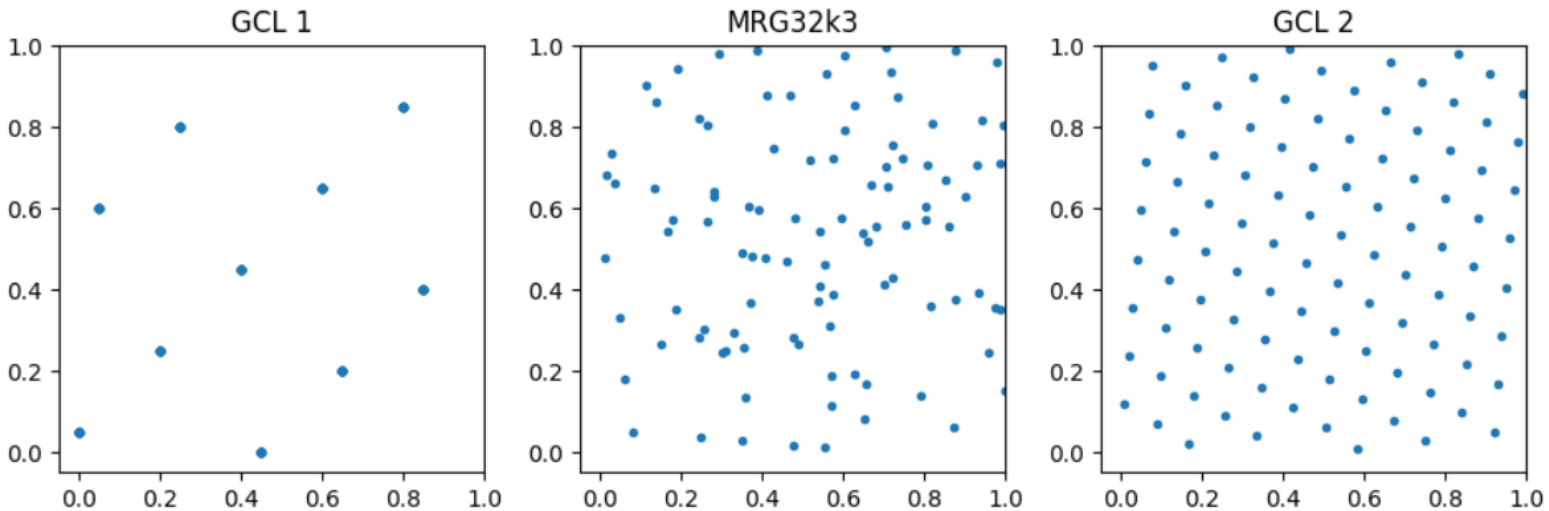
Le test spectral prend la forme d'un histogramme présentant la fréquence de chaque valeur :



Ce test est bien évidemment insuffisant. Des suites non aléatoires présentent des fréquences égales d'apparition de chaque nombre.

Test spectral à deux dimensions

En 2D, le test prend la forme suivante : deux valeurs consécutives seront les coordonnées d'un point du plan. Un "mauvais" GPA ne couvre qu'une petite partie du plan.



Remarquons que les GCL présentent une structure bien visible : cela est dû à la définition même des GCL. Les droites (ou plans dans des dimensions plus élevées) sont appelées **hyperplan**. Plus la distance entre deux hyperplans est faible, meilleur est le générateur.

Test spectral à trois dimensions

En 3D, le test prend la forme suivante :trois valeurs consécutives seront les coordonnées d'un point de l'espace. Un "mauvais" GPA ne couvre qu'une petite partie du cube

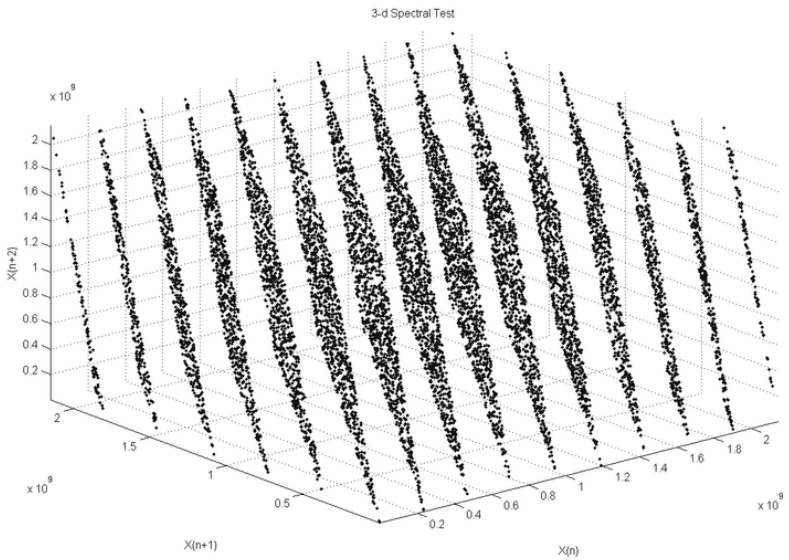


Figure – Test spectral 3D de RANDU d'IBM : les points de l'espace sont tous contenus dans 15 plans parallèles (source : researchGate)

Test spectral à plus de trois dimensions

Le test spectral peut-être généralisé à plus de trois dimensions mais les résultats perdent leur aspect visuel. Dans ce cas, on ajoute donc des métriques de distances pour les interpréter.

Rapport entre la distance minimale réelle entre les hyperplans et la distance minimale théorique (en dimension 2 à 8). Plus on est proche de 1, meilleur est le générateur :

rand	0,84	0,52	0,63	0,49	0,68	0,43	0,54
drand48	0,51	0,80	0,45	0,58	0,66	0,80	0,60
RANDU	0,93	0,012	0,059	0,16	0,29	0,45	0,62
MAPLE	0,75	0,74	0,65	0,73	0,63	0,56	0,56

Ressources

Ce cours s'appuie principalement sur le cours d'A.Ridard et sur cet article.