Cours de Méthodes Numériques

Licence M.I.A.S.H.S. Deuxième Année

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

Année 2019-2020

Créer du hasard ?

Ordinateur = fonctionnement totalement **déterministe** !

Propriété

Un ordinateur ne pourra générer qu'un **pseudo-hasard** *et en particulier des* **nombres pseudo-aléatoires**.

Comment "mimer" le hasard ?

$\Longrightarrow$ Choisir uniformément un réel dans $[0, 1]$

$\Longrightarrow$ Choisir uniformément un décimal de $[0, 1]$ à 2.10^{-16} près

Créer du hasard ?

Ordinateur = fonctionnement totalement **déterministe** !

Propriété

Un ordinateur ne pourra générer qu'un **pseudo-hasard** *et en particulier des* **nombres pseudo-aléatoires**.

Comment "mimer" le hasard ?

$\Longrightarrow$ Choisir uniformément un réel dans $[0, 1]$

$\Longrightarrow$ Choisir uniformément un décimal de $[0, 1]$ à 2.10^{-16} près

Créer du hasard ?

Ordinateur = fonctionnement totalement **déterministe** !

Propriété

Un ordinateur ne pourra générer qu'un **pseudo-hasard** *et en particulier des* **nombres pseudo-aléatoires**.

Comment "mimer" le hasard ?

$\Longrightarrow$ Choisir uniformément un réel dans $[0, 1]$

$\Longrightarrow$ Choisir uniformément un décimal de $[0, 1]$ à 2.10^{-16} près

Créer du hasard ?

Ordinateur = fonctionnement totalement **déterministe** !

Propriété

Un ordinateur ne pourra générer qu'un **pseudo-hasard** *et en particulier des* **nombres pseudo-aléatoires**.

Comment "mimer" le hasard ?

$\Longrightarrow$ Choisir uniformément un réel dans $[0, 1]$

$\Longrightarrow$ Choisir uniformément un décimal de $[0, 1]$ à 2.10^{-16} près

Créer du hasard ?

Ordinateur = fonctionnement totalement **déterministe** !

Propriété

Un ordinateur ne pourra générer qu'un **pseudo-hasard** *et en particulier des* **nombres pseudo-aléatoires**.

Comment "mimer" le hasard ?

$\Longrightarrow$ Choisir uniformément un réel dans $[0, 1]$

$\Longrightarrow$ Choisir uniformément un décimal de $[0, 1]$ à 2.10^{-16} près

Créer du hasard ?

Ordinateur = fonctionnement totalement **déterministe** !

Propriété

Un ordinateur ne pourra générer qu'un **pseudo-hasard** *et en particulier des* **nombres pseudo-aléatoires**.

Comment "mimer" le hasard ?

$\Longrightarrow$ Choisir uniformément un réel dans $[0,1]$

$\Longrightarrow$ Choisir uniformément un décimal de $[0,1]$ à 2.10^{-16} près

Nombre pseudo-aléatoire sur $[0, 1]$

Définition

Soit $m \in \mathbb{N}^* \setminus \{1\}$. *Pour* $k \in \mathbb{N}$, *il existe un unique* $k' \in \{0, 1, \ldots, m-1\}$ *tel que* $k = k'$ $[m]$ (**modulo** m) $\iff k - k'$ *est divisible par* m

Exemples : $18 = 3$ $[5]$, $18 = 0$ $[9]$, $18 = 18$ $[25]$, $324903 = 462$ $[531]$.

Idée : Prendre k et m grand et revenir dans $[0, 1]$ en divisant par m

Exemples :

$$324903 = 462\ [531] \implies u = 462/531 \simeq 0.870$$
$$324903 * 462 = 513\ [531] \implies u = 513/531 \simeq 0.966$$
$$324903 * 513 = 180\ [531] \implies u = 180/531 \simeq 0.339$$

Nombre pseudo-aléatoire sur $[0,1]$

Définition

*Soit $m \in \mathbb{N}^* \setminus \{1\}$. Pour $k \in \mathbb{N}$, il existe un unique $k' \in \{0, 1, \ldots, m-1\}$ tel que $k = k'$ $[m]$ (**modulo** m) $\iff k - k'$ est divisible par m*

Exemples : $18 = 3$ $[5]$, $18 = 0$ $[9]$, $18 = 18$ $[25]$, $324903 = 462$ $[531]$.

Idée : Prendre k et m grand et revenir dans $[0,1]$ en divisant par m

Exemples :

$$324903 = 462 \ [531] \implies u = 462/531 \simeq 0.870$$
$$324903 * 462 = 513 \ [531] \implies u = 513/531 \simeq 0.966$$
$$324903 * 513 = 180 \ [531] \implies u = 180/531 \simeq 0.339$$

Nombre pseudo-aléatoire sur $[0, 1]$

Définition

Soit $m \in \mathbb{N}^* \setminus \{1\}$. Pour $k \in \mathbb{N}$, il existe un unique $k' \in \{0, 1, \ldots, m-1\}$ tel que $k = k'$ $[m]$ (**modulo** *m*) $\Longleftrightarrow$ *$k - k'$ est divisible par m*

Exemples : $18 = 3$ $[5]$, $18 = 0$ $[9]$, $18 = 18$ $[25]$, $324903 = 462$ $[531]$.

Idée : Prendre k et m grand et revenir dans $[0, 1]$ en divisant par m

Exemples :
$324903 = 462 \ [531] \implies u = 462/531 \simeq 0.870$
$324903 * 462 = 513 \ [531] \implies u = 513/531 \simeq 0.966$
$324903 * 513 = 180 \ [531] \implies u = 180/531 \simeq 0.339$

Nombre pseudo-aléatoire sur $[0, 1]$

Définition

*Soit $m \in \mathbb{N}^* \setminus \{1\}$. Pour $k \in \mathbb{N}$, il existe un unique $k' \in \{0, 1, \ldots, m-1\}$ tel que $k = k'$ $[m]$ (**modulo** m) $\iff$ $k - k'$ est divisible par m*

Exemples : $18 = 3\ [5]$, $18 = 0\ [9]$, $18 = 18\ [25]$, $324903 = 462\ [531]$.

Idée : Prendre k et m grand et revenir dans $[0, 1]$ en divisant par m

Exemples : $324903 = 462\ [531] \implies u = 462/531 \simeq 0.870$

$324903 * 462 = 513\ [531] \implies u = 513/531 \simeq 0.966$

$324903 * 513 = 180\ [531] \implies u = 180/531 \simeq 0.339$

Nombre pseudo-aléatoire sur $[0,1]$

Définition

*Soit $m \in \mathbb{N}^* \setminus \{1\}$. Pour $k \in \mathbb{N}$, il existe un unique $k' \in \{0,1,\ldots,m-1\}$ tel que $k = k'$ $[m]$ (**modulo** m) $\Longleftrightarrow$ $k - k'$ est divisible par m*

Exemples : $18 = 3$ $[5]$, $18 = 0$ $[9]$, $18 = 18$ $[25]$, $324903 = 462$ $[531]$.

Idée : Prendre k et m grand et revenir dans $[0,1]$ en divisant par m

Exemples :

$$324903 = 462\ [531] \implies u = 462/531 \simeq 0.870$$
$$324903 * 462 = 513\ [531] \implies u = 513/531 \simeq 0.966$$
$$324903 * 513 = 180\ [531] \implies u = 180/531 \simeq 0.339$$

Nombre pseudo-aléatoire sur $[0, 1]$

Définition

*Soit $m \in \mathbb{N}^* \setminus \{1\}$. Pour $k \in \mathbb{N}$, il existe un unique $k' \in \{0, 1, \ldots, m-1\}$ tel que $k = k'$ $[m]$ (**modulo** m) $\iff$ $k - k'$ est divisible par m*

Exemples : $18 = 3$ $[5]$, $18 = 0$ $[9]$, $18 = 18$ $[25]$, $324903 = 462$ $[531]$.

Idée : Prendre k et m grand et revenir dans $[0, 1]$ en divisant par m

Exemples :

$$324903 = 462 \ [531] \implies u = 462/531 \simeq 0.870$$
$$324903 * 462 = 513 \ [531] \implies u = 513/531 \simeq 0.966$$
$$324903 * 513 = 180 \ [531] \implies u = 180/531 \simeq 0.339$$

Nombre pseudo-aléatoire sur $[0, 1]$

Définition

Soit $m \in \mathbb{N}^* \setminus \{1\}$. Pour $k \in \mathbb{N}$, il existe un unique $k' \in \{0, 1, \ldots, m-1\}$ tel que $k = k'$ $[m]$ (**modulo** *m*) $\Longleftrightarrow$ *$k - k'$ est divisible par m*

Exemples : $18 = 3$ $[5]$, $18 = 0$ $[9]$, $18 = 18$ $[25]$, $324903 = 462$ $[531]$.

Idée : Prendre k et m grand et revenir dans $[0, 1]$ en divisant par m

Exemples :

$$\begin{aligned} 324903 = 462\ [531] &\implies u = 462/531 \simeq 0.870 \\ 324903 * 462 = 513\ [531] &\implies u = 513/531 \simeq 0.966 \\ 324903 * 513 = 180\ [531] &\implies u = 180/531 \simeq 0.339 \end{aligned}$$

Nombres pseudo-aléatoires sur $[0, 1]$ (suite)

Une procédure pour simuler plusieurs nombres pseudo-aléatoires sur $[0, 1]$:

Procédure

Soit $m \in \mathbb{N}^* \setminus \{1\}$, $a \in \mathbb{N}^* \setminus \{1\}$ et $b \in \{0, 1, \ldots, m-1\}$ fixés.

1. *Avec $x_0 \in \mathbb{N}$, $x_{n+1} = a \times x_n + b\ [m]$ pour $n \geq 0$*
2. *Avec $u_n = x_n/m$, $(u_1, \ldots, u_n)$ n nombres pseudo-aléatoires de $[0, 1]$*

Exemples : Avec $m = 531$, $a = 324903$, $b = 0$ et $x_0 = 1$

$(x_1, \ldots, x_{10})$=(462 513 180 324 477 9 441 369 27 261..)
$(u_1, \ldots, u_{10}) \simeq$(0.870 0.966 0.339 0.610 0.898 0.017 0.831 0.695 0.051..)

Nombres pseudo-aléatoires sur $[0, 1]$ (suite)

Une procédure pour simuler plusieurs nombres pseudo-aléatoires sur $[0, 1]$:

Procédure

Soit $m \in \mathbb{N}^* \setminus \{1\}$, $a \in \mathbb{N}^* \setminus \{1\}$ *et* $b \in \{0, 1, \dots, m-1\}$ *fixés.*

1. *Avec* $x_0 \in \mathbb{N}$, $x_{n+1} = a \times x_n + b \ [m]$ *pour* $n \geq 0$
2. *Avec* $u_n = x_n/m$, $(u_1, \dots, u_n)$ *n nombres pseudo-aléatoires de* $[0, 1]$

Exemples : Avec $m = 531$, $a = 324903$, $b = 0$ et $x_0 = 1$

$(x_1, \dots, x_{10})$=(462 513 180 324 477 9 441 369 27 261..)
$(u_1, \dots, u_{10}) \simeq$(0.870 0.966 0.339 0.610 0.898 0.017 0.831 0.695 0.051..)

Nombres pseudo-aléatoires sur $[0,1]$ (suite)

Une procédure pour simuler plusieurs nombres pseudo-aléatoires sur $[0,1]$:

Procédure

Soit $m \in \mathbb{N}^* \setminus \{1\}$, $a \in \mathbb{N}^* \setminus \{1\}$ *et* $b \in \{0,1,\dots,m-1\}$ *fixés.*

1. *Avec* $x_0 \in \mathbb{N}$, $x_{n+1} = a \times x_n + b\ [m]$ *pour* $n \geq 0$
2. *Avec* $u_n = x_n/m$, $(u_1,\dots,u_n)$ *n nombres pseudo-aléatoires de* $[0,1]$

Exemples : Avec $m = 531$, $a = 324903$, $b = 0$ et $x_0 = 1$

$(x_1,\dots,x_{10})$=(462 513 180 324 477 9 441 369 27 261..)
$(u_1,\dots,u_{10}) \simeq$(0.870 0.966 0.339 0.610 0.898 0.017 0.831 0.695 0.051..)

Nombres pseudo-aléatoires sur $[0,1]$ (suite)

Une procédure pour simuler plusieurs nombres pseudo-aléatoires sur $[0,1]$:

Procédure

Soit $m \in \mathbb{N}^* \setminus \{1\}$, $a \in \mathbb{N}^* \setminus \{1\}$ *et* $b \in \{0, 1, \ldots, m-1\}$ *fixés.*

1. *Avec* $x_0 \in \mathbb{N}$, $x_{n+1} = a \times x_n + b \; [m]$ *pour* $n \geq 0$
2. *Avec* $u_n = x_n/m$, $(u_1, \ldots, u_n)$ *n nombres pseudo-aléatoires de* $[0,1]$

Exemples : Avec $m = 531$, $a = 324903$, $b = 0$ et $x_0 = 1$

$(x_1, \ldots, x_{10})$=(462 513 180 324 477 9 441 369 27 261..)
$(u_1, \ldots, u_{10}) \simeq$(0.870 0.966 0.339 0.610 0.898 0.017 0.831 0.695 0.051..)

Nombres pseudo-aléatoires sur $[0, 1]$ (suite)

Une procédure pour simuler plusieurs nombres pseudo-aléatoires sur $[0, 1]$:

Procédure

Soit $m \in \mathbb{N}^* \setminus \{1\}$, $a \in \mathbb{N}^* \setminus \{1\}$ *et* $b \in \{0, 1, \ldots, m-1\}$ *fixés.*

1. *Avec* $x_0 \in \mathbb{N}$, $x_{n+1} = a \times x_n + b\ [m]$ *pour* $n \geq 0$
2. *Avec* $u_n = x_n / m$, $(u_1, \ldots, u_n)$ *n nombres pseudo-aléatoires de* $[0, 1]$

Exemples : Avec $m = 531$, $a = 324903$, $b = 0$ et $x_0 = 1$

$(x_1, \ldots, x_{10})$=(462 513 180 324 477 9 441 369 27 261..)
$(u_1, \ldots, u_{10})$ $\simeq$(0.870 0.966 0.339 0.610 0.898 0.017 0.831 0.695 0.051..)

Nombres pseudo-aléatoires sur $[0, 1]$ (fin)

Comment choisir m, a et b ?

Remarque : Au plus la suite x_i peut être périodique de **période** m

Pour simplifier, on prend $b = 0$. Pour avoir une période $(m-1)$:

1. On choisit m nombre premier
2. On prend a tel que $a^{m-1} - 1$ multiple de m et $a^j - 1$ non divisible par m, pour $j = 1, \ldots, m-2$.

$\Longrightarrow$ Par exemple, $m = 2^{31} - 1$ et $a = 16807$

$\Longrightarrow$ Choix de x_0 : horloge interne de l'ordinateur !

Nombres pseudo-aléatoires sur $[0, 1]$ (fin)

Comment choisir m, a et b ?

Remarque : Au plus la suite x_i peut être périodique de **période** m

Pour simplifier, on prend $b = 0$. Pour avoir une période $(m - 1)$:

1. On choisit m nombre premier
2. On prend a tel que $a^{m-1} - 1$ multiple de m et $a^j - 1$ non divisible par m, pour $j = 1, \ldots, m - 2$.

$\Longrightarrow$ Par exemple, $m = 2^{31} - 1$ et $a = 16807$

$\Longrightarrow$ Choix de x_0 : horloge interne de l'ordinateur !

Nombres pseudo-aléatoires sur $[0, 1]$ (fin)

Comment choisir m, a et b ?

Remarque : Au plus la suite x_i peut être périodique de **période** m

Pour simplifier, on prend $b = 0$. Pour avoir une période $(m-1)$:

1. On choisit m nombre premier
2. On prend a tel que $a^{m-1} - 1$ multiple de m et $a^j - 1$ non divisible par m, pour $j = 1, \ldots, m-2$.

$\Longrightarrow$ Par exemple, $m = 2^{31} - 1$ et $a = 16807$

$\Longrightarrow$ Choix de x_0 : horloge interne de l'ordinateur !

Nombres pseudo-aléatoires sur $[0,1]$ (fin)

Comment choisir m, a et b ?

Remarque : Au plus la suite x_i peut être périodique de **période** m

Pour simplifier, on prend $b = 0$. Pour avoir une période $(m-1)$:

1. On choisit m nombre premier
2. On prend a tel que $a^{m-1} - 1$ multiple de m et $a^j - 1$ non divisible par m, pour $j = 1, \ldots, m-2$.

$\Longrightarrow$ Par exemple, $m = 2^{31} - 1$ et $a = 16807$

$\Longrightarrow$ Choix de x_0 : horloge interne de l'ordinateur !

Nombres pseudo-aléatoires sur $[0, 1]$ (fin)

Comment choisir m, a et b ?

Remarque : Au plus la suite x_i peut être périodique de **période** m

Pour simplifier, on prend $b = 0$. Pour avoir une période $(m - 1)$:

1. On choisit m nombre premier
2. On prend a tel que $a^{m-1} - 1$ multiple de m et $a^j - 1$ non divisible par m, pour $j = 1, \ldots, m - 2$.

$\Longrightarrow$ Par exemple, $m = 2^{31} - 1$ et $a = 16807$

$\Longrightarrow$ Choix de x_0 : horloge interne de l'ordinateur !

Nombres pseudo-aléatoires sur $[0, 1]$ (fin)

Comment choisir m, a et b ?

Remarque : Au plus la suite x_i peut être périodique de **période** m

Pour simplifier, on prend $b = 0$. Pour avoir une période $(m - 1)$:

1. On choisit m nombre premier
2. On prend a tel que $a^{m-1} - 1$ multiple de m et $a^j - 1$ non divisible par m, pour $j = 1, \ldots, m - 2$.

   $\Longrightarrow$ Par exemple, $m = 2^{31} - 1$ et $a = 16807$

   $\Longrightarrow$ Choix de x_0 : horloge interne de l'ordinateur !

Nombres pseudo-aléatoires sur $[0, 1]$ (fin)

Comment choisir m, a et b ?

Remarque : Au plus la suite x_i peut être périodique de **période** m

Pour simplifier, on prend $b = 0$. Pour avoir une période $(m-1)$:

1. On choisit m nombre premier
2. On prend a tel que $a^{m-1} - 1$ multiple de m et $a^j - 1$ non divisible par m, pour $j = 1, \dots, m-2$.

$\Longrightarrow$ Par exemple, $m = 2^{31} - 1$ et $a = 16807$

$\Longrightarrow$ Choix de x_0 : horloge interne de l'ordinateur !

Générer des nombres pseudo-aléatoires de toute loi

On sait générer n réalisations de v.a. indépendantes de loi $\simeq \mathcal{U}([0,1])$:
commande `R` : `runif(n,0,1)`

Comment générer n réalisations de v.a. indépendantes de loi quelconque ?

Propriété

Si X v.a. continue avec $f_X > 0$ de $I \subset \mathbb{R}$. Alors F_X sur I admet une fonction réciproque F_X^{-1} et pour $U \overset{\mathcal{L}}{\sim} \mathcal{U}([0,1])$ alors $F_X^{-1}(U)$ a la même loi que X.

Démonstration.

F_X strictement croissante sur I : F_X est bien bijective, et admet une fonction réciproque F_X^{-1} sur $]0,1[$ continue : $F_X^{-1}(U)$ est une v.a. Pour tout $x \in \mathbb{R}$, avec $F_X(F_X^{-1}(U)) = U$ et

$$\mathbb{P}(F_X^{-1}(U) \leq x) = \mathbb{P}(U \leq F_X(x)) = F_U(F_X(x)) = F_X(x) \qquad \text{car } F_U(u) = u \text{ pour tout } u \in [0,1].$$

La v.a. $F_X^{-1}(U)$ a donc même fonction de répartition que X, ces deux v.a. ont donc même loi. $\square$

Générer des nombres pseudo-aléatoires de toute loi

On sait générer n réalisations de v.a. indépendantes de loi $\simeq \mathcal{U}([0,1])$: commande `R` : `runif(n,0,1)`

Comment générer n réalisations de v.a. indépendantes de loi quelconque ?

Propriété

Si X v.a. continue avec $f_X > 0$ de $I \subset \mathbb{R}$. Alors F_X sur I admet une fonction réciproque F_X^{-1} et pour $U \overset{\mathcal{L}}{\sim} \mathcal{U}([0,1])$ alors $F_X^{-1}(U)$ a la même loi que X.

Démonstration.

F_X strictement croissante sur I : F_X est bien bijective, et admet une fonction réciproque F_X^{-1} sur $]0,1[$ continue : $F_X^{-1}(U)$ est une v.a. Pour tout $x \in \mathbb{R}$, avec $F_X(F_X^{-1}(U)) = U$ et

$$\mathbb{P}(F_X^{-1}(U) \leq x) = \mathbb{P}(U \leq F_X(x)) = F_U(F_X(x)) = F_X(x) \qquad \text{car } F_U(u) = u \text{ pour tout } u \in [0,1].$$

La v.a. $F_X^{-1}(U)$ a donc même fonction de répartition que X, ces deux v.a. ont donc même loi. $\square$

Générer des nombres pseudo-aléatoires de toute loi

On sait générer n réalisations de v.a. indépendantes de loi $\simeq \mathcal{U}([0,1])$: commande R : `runif(n,0,1)`

Comment générer n réalisations de v.a. indépendantes de loi quelconque ?

Propriété

Si X v.a. continue avec $f_X > 0$ de $I \subset \mathbb{R}$. Alors F_X sur I admet une fonction réciproque F_X^{-1} et pour $U \overset{\mathcal{L}}{\sim} \mathcal{U}([0,1])$ alors $F_X^{-1}(U)$ a la même loi que X.

Démonstration.

F_X strictement croissante sur I : F_X est bien bijective, et admet une fonction réciproque F_X^{-1} sur $]0,1[$ continue : $F_X^{-1}(U)$ est une v.a. Pour tout $x \in \mathbb{R}$, avec $F_X(F_X^{-1}(U)) = U$ et

$$\mathbb{P}(F_X^{-1}(U) \leq x) = \mathbb{P}(U \leq F_X(x)) = F_U(F_X(x)) = F_X(x) \qquad \text{car } F_U(u) = u \text{ pour tout } u \in [0,1].$$

La v.a. $F_X^{-1}(U)$ a donc même fonction de répartition que X, ces deux v.a. ont donc même loi. $\square$

Générer des nombres pseudo-aléatoires de toute loi (suite)

Exemple : Si X suit la loi $\mathcal{E}(\lambda)$, alors $F_X(x) = \begin{cases} 0 & \text{si } x \leq 0 \\ 1 - e^{-\lambda x} & \text{si } x > 0 \end{cases}$.

$\Longrightarrow F_X$ bijective de $]0, \infty[\to [0,1[$ et $F_X^{-1}(y) = -\frac{\ln(1-y)}{\lambda}$ sur $[0,1[$.

Donc si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$
$\Longrightarrow (X_1, \ldots, X_n)$ réalisations indépendantes $\simeq \mathcal{E}(\lambda)$, $X_i = -\frac{\ln(1-U_i)}{\lambda}$

Exemple moins facile :

Si on veut générer $(X_1, \ldots, X_n)$ indépendantes avec $X_i \overset{\mathcal{L}}{\sim} \simeq \mathcal{N}(0,1)$:

$F_X(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$ $\Longrightarrow$ pas d'expression pour F_X^{-1} ! !
$\Longrightarrow$ Autre méthode...

Générer des nombres pseudo-aléatoires de toute loi (suite)

Exemple : Si X suit la loi $\mathcal{E}(\lambda)$, alors $F_X(x) = \left\{ \begin{array}{ll} 0 & \text{si } x \leq 0 \\ 1 - e^{-\lambda x} & \text{si } x > 0 \end{array} \right.$.

$\Longrightarrow F_X$ bijective de $]0, \infty[\to [0,1[$ et $F_X^{-1}(y) = -\frac{\ln(1-y)}{\lambda}$ sur $[0,1[$.

Donc si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$\Longrightarrow (X_1, \ldots, X_n)$ réalisations indépendantes $\simeq \mathcal{E}(\lambda)$, $X_i = -\frac{\ln(1-U_i)}{\lambda}$

Exemple moins facile :

Si on veut générer $(X_1, \ldots, X_n)$ indépendantes avec $X_i \overset{\mathcal{L}}{\sim} \simeq \mathcal{N}(0,1)$:

$F_X(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$ $\Longrightarrow$ pas d'expression pour F_X^{-1} ! !

$\Longrightarrow$ Autre méthode...

Générer des nombres pseudo-aléatoires de toute loi (suite)

Exemple : Si X suit la loi $\mathcal{E}(\lambda)$, alors $F_X(x) = \left\{ \begin{array}{ll} 0 & \text{si } x \leq 0 \\ 1 - e^{-\lambda x} & \text{si } x > 0 \end{array} \right.$.

$\Longrightarrow F_X$ bijective de $]0, \infty[\to [0, 1[$ et $F_X^{-1}(y) = -\frac{\ln(1-y)}{\lambda}$ sur $[0, 1[$.

Donc si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0, 1])$
$\Longrightarrow (X_1, \ldots, X_n)$ réalisations indépendantes $\simeq \mathcal{E}(\lambda)$, $X_i = -\frac{\ln(1-U_i)}{\lambda}$

Exemple moins facile :

Si on veut générer $(X_1, \ldots, X_n)$ indépendantes avec $X_i \overset{\mathcal{L}}{\sim} \simeq \mathcal{N}(0, 1)$:

$F_X(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$ $\Longrightarrow$ pas d'expression pour F_X^{-1} ! !
$\Longrightarrow$ Autre méthode...

Générer des nombres pseudo-aléatoires de toute loi (suite)

Exemple : Si X suit la loi $\mathcal{E}(\lambda)$, alors $F_X(x) = \begin{cases} 0 & \text{si } x \leq 0 \\ 1 - e^{-\lambda x} & \text{si } x > 0 \end{cases}$.

$\Longrightarrow F_X$ bijective de $]0, \infty[\to [0, 1[$ et $F_X^{-1}(y) = -\frac{\ln(1-y)}{\lambda}$ sur $[0, 1[$.

Donc si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0, 1])$
$\Longrightarrow (X_1, \ldots, X_n)$ réalisations indépendantes $\simeq \mathcal{E}(\lambda)$, $X_i = -\frac{\ln(1-U_i)}{\lambda}$

Exemple moins facile :

Si on veut générer $(X_1, \ldots, X_n)$ indépendantes avec $X_i \overset{\mathcal{L}}{\sim} \simeq \mathcal{N}(0, 1)$:

$F_X(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$ $\Longrightarrow$ pas d'expression pour F_X^{-1} ! !
$\Longrightarrow$ Autre méthode...

Générer des nombres pseudo-aléatoires de toute loi (suite)

Et pour les variables aléatoires discrètes ?

Propriété

Soit X v.a. prenant pour valeurs $(x_j)_{j\geq 1}$ et $x_j < x_{j+1}$ de loi $\mathbb{P}(X = x_j) = p_j$. Soit $H : [0,1] \to (x_j)_{j\in J}$ telle que $H(x) = x_j$ pour $F_X(x_{j-1}) \leq x < F_X(x_j)$ avec $F_X(x_0) = 0$, alors si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$$\Longrightarrow (V_1, \ldots, V_n) \text{ réalisations indépendantes de loi } (p_j),\ V_i = H(U_i).$$

Autrement : Pour $U \overset{\mathcal{L}}{\sim} \simeq \mathcal{U}([0,1])$

- si $0 \leq U < p_1$, $V = H(U) = x_1$
- si $p_1 \leq U < p_1 + p_2$, $V = H(U) = x_2$
- si $p_1 + p_2 \leq U < p_1 + p_2 + p_3$, $V = H(U) = x_3$
- ....

Générer des nombres pseudo-aléatoires de toute loi (suite)

Et pour les variables aléatoires discrètes ?

Propriété

Soit X v.a. prenant pour valeurs $(x_j)_{j\geq 1}$ et $x_j < x_{j+1}$ de loi $\mathbb{P}(X = x_j) = p_j$. Soit $H : [0,1] \to (x_j)_{j\in J}$ telle que $H(x) = x_j$ pour $F_X(x_{j-1}) \leq x < F_X(x_j)$ avec $F_X(x_0) = 0$, alors si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$$\Longrightarrow (V_1, \ldots, V_n) \text{ réalisations indépendantes de loi } (p_j),\ V_i = H(U_i).$$

Autrement : Pour $U \overset{\mathcal{L}}{\sim} \simeq \mathcal{U}([0,1])$

- si $0 \leq U < p_1$, $V = H(U) = x_1$
- si $p_1 \leq U < p_1 + p_2$, $V = H(U) = x_2$
- si $p_1 + p_2 \leq U < p_1 + p_2 + p_3$, $V = H(U) = x_3$
- ....

Générer des nombres pseudo-aléatoires de toute loi (suite)

Et pour les variables aléatoires discrètes ?

Propriété

Soit X v.a. prenant pour valeurs $(x_j)_{j\geq 1}$ et $x_j < x_{j+1}$ de loi $\mathbb{P}(X = x_j) = p_j$. Soit $H : [0,1] \to (x_j)_{j\in J}$ telle que $H(x) = x_j$ pour $F_X(x_{j-1}) \leq x < F_X(x_j)$ avec $F_X(x_0) = 0$, alors si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$$\Longrightarrow (V_1, \ldots, V_n) \text{ réalisations indépendantes de loi } (p_j),\ V_i = H(U_i).$$

Autrement : Pour $U \overset{\mathcal{L}}{\sim} \simeq \mathcal{U}([0,1])$

- si $0 \leq U < p_1$, $V = H(U) = x_1$
- si $p_1 \leq U < p_1 + p_2$, $V = H(U) = x_2$
- si $p_1 + p_2 \leq U < p_1 + p_2 + p_3$, $V = H(U) = x_3$
- ....

Générer des nombres pseudo-aléatoires de toute loi (suite)

Et pour les variables aléatoires discrètes ?

Propriété

Soit X v.a. prenant pour valeurs $(x_j)_{j\geq 1}$ et $x_j < x_{j+1}$ de loi $\mathbb{P}(X = x_j) = p_j$. Soit $H : [0,1] \to (x_j)_{j\in J}$ telle que $H(x) = x_j$ pour $F_X(x_{j-1}) \leq x < F_X(x_j)$ avec $F_X(x_0) = 0$, alors si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$$\Longrightarrow (V_1, \ldots, V_n) \text{ réalisations indépendantes de loi } (p_j),\ V_i = H(U_i).$$

Autrement : Pour $U \overset{\mathcal{L}}{\sim} \simeq \mathcal{U}([0,1])$

- si $0 \leq U < p_1$, $V = H(U) = x_1$
- si $p_1 \leq U < p_1 + p_2$, $V = H(U) = x_2$
- si $p_1 + p_2 \leq U < p_1 + p_2 + p_3$, $V = H(U) = x_3$
- ....

Générer des nombres pseudo-aléatoires de toute loi (suite)

Et pour les variables aléatoires discrètes ?

Propriété

Soit X v.a. prenant pour valeurs $(x_j)_{j\geq 1}$ et $x_j < x_{j+1}$ de loi $\mathbb{P}(X = x_j) = p_j$. Soit $H : [0,1] \to (x_j)_{j\in J}$ telle que $H(x) = x_j$ pour $F_X(x_{j-1}) \leq x < F_X(x_j)$ avec $F_X(x_0) = 0$, alors si $(U_1, \dots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$$\Longrightarrow (V_1, \dots, V_n) \text{ réalisations indépendantes de loi } (p_j),\ V_i = H(U_i).$$

Autrement : Pour $U \overset{\mathcal{L}}{\sim} \simeq \mathcal{U}([0,1])$

- si $0 \leq U < p_1,\ V = H(U) = x_1$
- si $p_1 \leq U < p_1 + p_2,\ V = H(U) = x_2$
- si $p_1 + p_2 \leq U < p_1 + p_2 + p_3,\ V = H(U) = x_3$
- ....

Générer des nombres pseudo-aléatoires de toute loi (suite)

Et pour les variables aléatoires discrètes ?

Propriété

Soit X v.a. prenant pour valeurs $(x_j)_{j\geq 1}$ et $x_j < x_{j+1}$ de loi $\mathbb{P}(X = x_j) = p_j$. Soit $H : [0,1] \to (x_j)_{j\in J}$ telle que $H(x) = x_j$ pour $F_X(x_{j-1}) \leq x < F_X(x_j)$ avec $F_X(x_0) = 0$, alors si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$$\Longrightarrow (V_1, \ldots, V_n) \text{ réalisations indépendantes de loi } (p_j),\ V_i = H(U_i).$$

Autrement : Pour $U \overset{\mathcal{L}}{\sim} \simeq \mathcal{U}([0,1])$

- si $0 \leq U < p_1$, $V = H(U) = x_1$
- si $p_1 \leq U < p_1 + p_2$, $V = H(U) = x_2$
- si $p_1 + p_2 \leq U < p_1 + p_2 + p_3$, $V = H(U) = x_3$
- ....

Générer des nombres pseudo-aléatoires de toute loi (suite)

Et pour les variables aléatoires discrètes ?

Propriété

Soit X v.a. prenant pour valeurs $(x_j)_{j\geq 1}$ et $x_j < x_{j+1}$ de loi $\mathbb{P}(X = x_j) = p_j$. Soit $H : [0,1] \to (x_j)_{j\in J}$ telle que $H(x) = x_j$ pour $F_X(x_{j-1}) \leq x < F_X(x_j)$ avec $F_X(x_0) = 0$, alors si $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$$\Longrightarrow (V_1, \ldots, V_n) \text{ réalisations indépendantes de loi } (p_j),\ V_i = H(U_i).$$

Autrement : Pour $U \overset{\mathcal{L}}{\sim} \simeq \mathcal{U}([0,1])$

- si $0 \leq U < p_1$, $V = H(U) = x_1$
- si $p_1 \leq U < p_1 + p_2$, $V = H(U) = x_2$
- si $p_1 + p_2 \leq U < p_1 + p_2 + p_3$, $V = H(U) = x_3$
- ....

Générer des nombres pseudo-aléatoires de toute loi (fin)

Remarque : $\mathbb{P}\big(\alpha \leq U < \beta\big) = \beta - \alpha$ pour $0 \leq \alpha \leq \beta \leq 1$

$\Longrightarrow \mathbb{P}(V = H(U) = x_j) = \mathbb{P}\big(p_1 + \cdots + p_{j-1} \leq U < p_1 + \cdots + p_j\big) = p_j$

Exemple : Pour générer $(X_1, \ldots, X_n)$ réalisations indépendantes de loi $\mathcal{B}(p)$

$\Longrightarrow$ On génère $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$
$\Longrightarrow$ Si $0 \leq U_i < 1 - p$, $X_i = 0$, si $1 - p \leq U_i < 1$, $X_i = 1$

Commandes `R` : `rbinom(n,1,p)`, `rbinom(n,m,p)`, `rexp(n,1)`,...

Générer des nombres pseudo-aléatoires de toute loi (fin)

Remarque : $\mathbb{P}\big(\alpha \leq U < \beta\big) = \beta - \alpha$ pour $0 \leq \alpha \leq \beta \leq 1$

$$\Longrightarrow \mathbb{P}(V = H(U) = x_j) = \mathbb{P}\big(p_1 + \cdots + p_{j-1} \leq U < p_1 + \cdots + p_j\big) = p_j$$

Exemple : Pour générer $(X_1, \ldots, X_n)$ réalisations indépendantes de loi $\mathcal{B}(p)$

$\Longrightarrow$ On génère $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$
$\Longrightarrow$ Si $0 \leq U_i < 1 - p$, $X_i = 0$, si $1 - p \leq U_i < 1$, $X_i = 1$

Commandes R : `rbinom(n,1,p)`, `rbinom(n,m,p)`, `rexp(n,1)`,...

Générer des nombres pseudo-aléatoires de toute loi (fin)

Remarque : $\mathbb{P}\big(\alpha \leq U < \beta\big) = \beta - \alpha$ pour $0 \leq \alpha \leq \beta \leq 1$

$$\Longrightarrow \mathbb{P}(V = H(U) = x_j) = \mathbb{P}\big(p_1 + \cdots + p_{j-1} \leq U < p_1 + \cdots + p_j\big) = p_j$$

Exemple : Pour générer $(X_1, \ldots, X_n)$ réalisations indépendantes de loi $\mathcal{B}(p)$

$\Longrightarrow$ On génère $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$

$\Longrightarrow$ Si $0 \leq U_i < 1 - p$, $X_i = 0$, si $1 - p \leq U_i < 1$, $X_i = 1$

Commandes R : `rbinom(n,1,p)`, `rbinom(n,m,p)`, `rexp(n,1)`,...

Générer des nombres pseudo-aléatoires de toute loi (fin)

Remarque : $\mathbb{P}\big(\alpha \leq U < \beta\big) = \beta - \alpha$ pour $0 \leq \alpha \leq \beta \leq 1$

$$\Longrightarrow \mathbb{P}(V = H(U) = x_j) = \mathbb{P}\big(p_1 + \cdots + p_{j-1} \leq U < p_1 + \cdots + p_j\big) = p_j$$

Exemple : Pour générer $(X_1, \ldots, X_n)$ réalisations indépendantes de loi $\mathcal{B}(p)$

$\Longrightarrow$ On génère $(U_1, \ldots, U_n)$ réalisations indépendantes $\simeq \mathcal{U}([0,1])$
$\Longrightarrow$ Si $0 \leq U_i < 1 - p$, $X_i = 0$, si $1 - p \leq U_i < 1$, $X_i = 1$

Commandes `R` : `rbinom(n,1,p)`, `rbinom(n,m,p)`, `rexp(n,l)`,...