Probabilités et Simulation

Générateurs de loi uniforme et de lois discrètes

Jean-Marc Vincent [1]

[1] Laboratoire d'Informatique de Grenoble
Polytech Grenoble

Septembre 2014

Outline

1. Introduction
2. Lois uniformes

Histoires de dés

Pièces, dés, roues,...

Mécanisme physique :

Suite d'observations : $x_1, x_2, x_3, \cdots, x_n, \cdots$ à valeur dans $\{1, 2, \cdots, K\}$

Modèle probabiliste :

La séquence d'observations est modélisée par une suite de

- variables aléatoires,
- indépendantes,
- identiquement distribuées,
- de loi uniforme sur l'ensemble $\{1, 2, \cdots, K\}$ notée $\{X_n\}_{n\in\mathbb{N}}$

Notations et propriétés

Pour tout n et pour toute séquence $\{x_1, \cdots, x_n\}$ de $\{1, 2, \cdots, K\}^n$

$$\begin{aligned}
\mathbb{P}(X_1 = x_1, \cdots, X_n = x_n) &= \mathbb{P}(X_1 = x_1). \cdots .\mathbb{P}(X_n = x_n) \text{ indépendance;} \\
&= \mathbb{P}(X = x_1). \cdots .\mathbb{P}(X = x_n) \text{ même loi;} \\
&= \frac{1}{K} \cdots \frac{1}{K} = \frac{1}{K^n} \text{ loi uniforme.}
\end{aligned}$$

Outline

1 Introduction

2 Lois uniformes

Histoires de dés (suite)

Pièce $\mapsto$ Dé-8

À partir d'une pièce de monnaie écrire un générateur aléatoire d'un dé à 8 faces:

Dé-8()

Données: Une fonction "Pièce()" générateur aléatoire de $\{0, 1\}$
Résultat: Une séquence i.i.d. de loi uniforme sur $\{1, \cdots, 8\}$

A_0 =Pièce()
A_1 =Pièce()
A_2 =Pièce()
$S = A_0 + 2 * A_1 + 4 * A_2 + 1$
return S

UNIVERSITE JOSEPH FOURIER

Histoires de dés (suite)

Pièce $\mapsto$ Dé-8

À partir d'une pièce de monnaie écrire un générateur aléatoire d'un dé à 8 faces:

Dé-8()

Données: Une fonction "Pièce()" générateur aléatoire de $\{0, 1\}$
Résultat: Une séquence i.i.d. de loi uniforme sur $\{1, \cdots, 8\}$

$A_0 =$Pièce()
$A_1 =$Pièce()
$A_2 =$Pièce()
$S = A_0 + 2 * A_1 + 4 * A_2 + 1$
return S

Histoires de dés (Preuve de l'algorithme)

Spécification : une séquence d'appels à la fonction **Dé-8()** est modélisée par une séquence de variables aléatoires i.i.d. de loi uniforme sur $\{1, \cdots, 8\}$.
Hypothèse : $P_0, P_1, \cdots, P_n, \cdots$ séquence des appels à **Pièce()** iid de loi uniforme sur $\{0, 1\}$
Preuve : Soit $S_0, S_1, \cdots, S_n, \cdots$ la séquence des résultats obtenus par appels successifs de **Dé-8()**

$$\begin{aligned}
\mathbb{P}(S_0 = x_0, \cdots, S_n = x_n) &= \mathbb{P}(S_0 = x_0) \cdots \mathbb{P}(S_n = x_n) \\
&\quad \text{car } S_k \text{ ne dépend que de } P_{3k}, P_{3k+1}, P_{3k+2} \text{ et que les } P_i \text{ sont indépendants;} \\
&= \mathbb{P}(S_0 = x_0) \cdots \mathbb{P}(S_0 = x_n) \text{ car } (P_{3k}, P_{3k+1}, P_{3k+2}) \text{ ont même loi.}
\end{aligned}$$

Or pour i dans $\{1, \cdots, 8\}$, $i - 1$ s'écrit de manière unique en binaire $i - 1 =_2 a_2 a_1 a_0$.

$$\begin{aligned}
\mathbb{P}(S_0 = i) &= \mathbb{P}(P_0 = a_0, P_1 = a_1, P_2 = a_2) \\
&= Prob(P_0 = a_0)\mathbb{P}(P_1 = a_1)\mathbb{P}(P_2 = a_2) \text{ les appels à Piece() sont indépendants;} \\
&= \frac{1}{2}\frac{1}{2}\frac{1}{2} = \frac{1}{8} \text{ car même loi uniforme.}
\end{aligned}$$

d'où

$$\mathbb{P}(S_0 = x_0, \cdots, S_n = x_n) = \frac{1}{8^{n+1}} \qquad \text{cqfd.}$$

Histoires de dés (suite)

Pièce $\mapsto$ Dé-2^k

À partir d'une pièce de monnaie écrire un générateur aléatoire d'un dé à 2^k faces:

Dé(k)

Données: Une fonction "Pièce()" générateur aléatoire de $\{0, 1\}$
Résultat: Une séquence i.i.d. de loi uniforme sur $\{1, \cdots, 2^k\}$

S=0
for $i = 1$ **to** k
  S=Pièce() +2.S `// cf Schéma de Hörner`
$S = S + 1$
return S

Preuve: Identique au **Dé-8**, unicité de la décomposition binaire d'un entier de $\{0, \cdots, 2^k - 1\}$ par un vecteur de k bits.

Histoires de dés (suite)

Pièce $\mapsto$ Dé-2^k

À partir d'une pièce de monnaie écrire un générateur aléatoire d'un dé à 2^k faces:

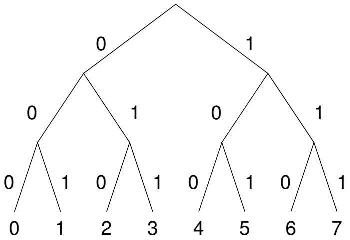
Dé(k)

Données: Une fonction "Pièce()" générateur aléatoire de $\{0, 1\}$
Résultat: Une séquence i.i.d. de loi uniforme sur $\{1, \cdots, 2^k\}$

S=0
for $i = 1$ **to** k
  S=Pièce() +2.S `// cf Schéma de Hörner`
$S = S + 1$
return S

Preuve: Identique au **Dé-8**, unicité de la décomposition binaire d'un entier de $\{0, \cdots, 2^k - 1\}$ par un vecteur de k bits.

Représentation binaire :



$$5 =_2 101,\ 2 =_2 010,\ 42 =_2 101010 \cdots$$

Histoires de dés (suite)

Pièce $\mapsto$ Dé-6

À partir d'une pièce de monnaie écrire un générateur aléatoire d'un dé à 6 faces:

Dé-6()

Données: Une fonction **Dé-8()** générateur aléatoire de $\{1, \cdots, 8\}$
Résultat: Une séquence i.i.d. de loi uniforme sur $\{1, \cdots, 6\}$

repeat
  $X =$**Dé-8()**
until $X \leqslant 6$
return X

Preuve: voir plus tard

Histoires de dés (suite)

Pièce $\mapsto$ Dé-6

À partir d'une pièce de monnaie écrire un générateur aléatoire d'un dé à 6 faces:

Dé-6()

Données: Une fonction **Dé-8()** générateur aléatoire de $\{1, \cdots, 8\}$
Résultat: Une séquence i.i.d. de loi uniforme sur $\{1, \cdots, 6\}$

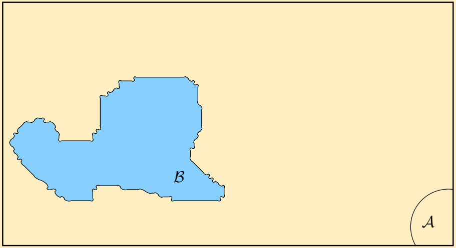
repeat
| X =**Dé-8()**
until $X \leqslant 6$
return X

Preuve: voir plus tard

Méthode basée sur le rejet

Principe

Générer uniformément sur $\mathcal{A}$ accepter si le point est dans $\mathcal{B}$.



Algorithme

Génère-unif($\mathcal{B}$)

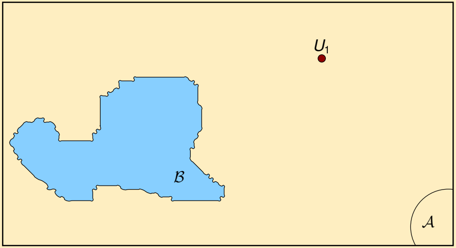
Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

repeat
X =**Génère-unif**($\mathcal{A}$)
until $X \in \mathcal{B}$
return X

Méthode basée sur le rejet

Principe

Générer uniformément sur $\mathcal{A}$ accepter si le point est dans $\mathcal{B}$.



Algorithme

Génère-unif($\mathcal{B}$)

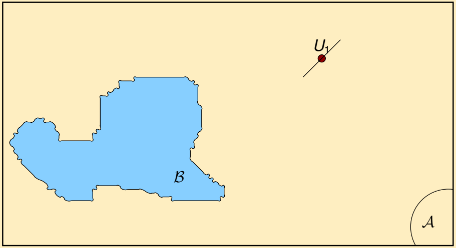
Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

repeat
  $X =$ **Génère-unif**($\mathcal{A}$)
until $X \in \mathcal{B}$
return X

Méthode basée sur le rejet

Principe

Générer uniformément sur $\mathcal{A}$ accepter si le point est dans $\mathcal{B}$.



Algorithme

Génère-unif($\mathcal{B}$)

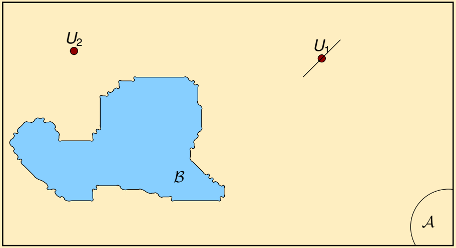
Données: Générateur uniforme sur $\mathcal{A}$
Résultat: Générateur uniforme sur $\mathcal{B}$

repeat
  X =**Génère-unif**($\mathcal{A}$)
until $X \in \mathcal{B}$
return X

Méthode basée sur le rejet

Principe

Générer uniformément sur $\mathcal{A}$ accepter si le point est dans $\mathcal{B}$.



Algorithme

Génère-unif($\mathcal{B}$)

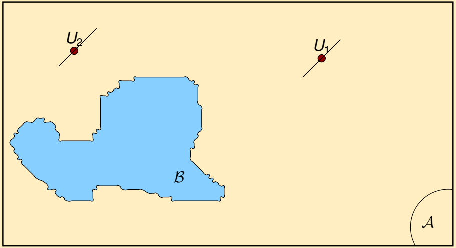
Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

repeat
X =**Génère-unif($\mathcal{A}$)**
until $X \in \mathcal{B}$
return X

Méthode basée sur le rejet

Principe

Générer uniformément sur $\mathcal{A}$ accepter si le point est dans $\mathcal{B}$.



Algorithme

Génère-unif($\mathcal{B}$)

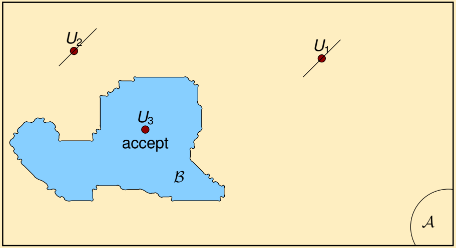
Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

repeat
  $X =$**Génère-unif($\mathcal{A}$)**
until $X \in \mathcal{B}$
return X

Méthode basée sur le rejet

Principe

Générer uniformément sur $\mathcal{A}$ accepter si le point est dans $\mathcal{B}$.



Algorithme

Génère-unif($\mathcal{B}$)

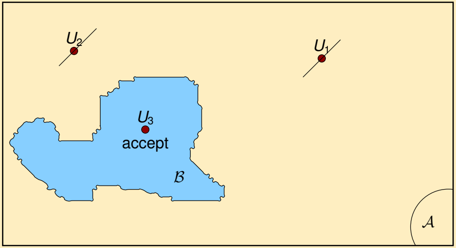
Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

repeat
X =**Génère-unif($\mathcal{A}$)**
until $X \in \mathcal{B}$
return X

Méthode basée sur le rejet

Principe

Générer uniformément sur $\mathcal{A}$ accepter si le point est dans $\mathcal{B}$.



Algorithme

Génère-unif($\mathcal{B}$)

Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

repeat
  X =**Génère-unif($\mathcal{A}$)**
until $X \in \mathcal{B}$
return X

Méthode basée sur le rejet : preuve

Génère-unif($\mathcal{B}$)

Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

$N = 0$
repeat
  $X =$**Génère-unif($\mathcal{A}$)**
  $N = N + 1$
until $X \in \mathcal{B}$
return X, N

Preuve

Tirages **Génère-unif($\mathcal{A}$)**: $X_1, X_2, \cdots, X_n, \cdots$

$$\begin{aligned}
& \mathbb{P}(X \in \mathcal{C}, N = k) \\
= & \mathbb{P}(X_1 \notin \mathcal{B}, \cdots, X_{k-1} \notin \mathcal{B}, X_k \in \mathcal{C}) \\
= & \mathbb{P}(X_1 \notin \mathcal{B}) \cdots \mathbb{P}(X_{k-1} \notin \mathcal{B})\mathbb{P}(X_k \in \mathcal{C}) \\
= & \left(1 - \frac{|\mathcal{B}|}{|\mathcal{A}|}\right)^{k-1} \frac{|\mathcal{C}|}{|\mathcal{A}|}
\end{aligned}$$

$$\begin{aligned}
\mathbb{P}(X \in \mathcal{C}) & = \sum_{k=1}^{+\infty} \mathbb{P}(X \in \mathcal{C}, N = k) \\
& = \sum_{k=1}^{+\infty} \left(1 - \frac{|\mathcal{B}|}{|\mathcal{A}|}\right)^{k-1} \frac{|\mathcal{C}|}{|\mathcal{A}|} = \frac{|\mathcal{C}|}{|\mathcal{B}|}
\end{aligned}$$

Donc la loi est **uniforme** sur $\mathcal{B}$

Méthode basée sur le rejet : complexité

Génère-unif($\mathcal{B}$)

Données:
Générateur uniforme sur $\mathcal{A}$
Résultat:
Générateur uniforme sur $\mathcal{B}$

```
N = 0
repeat
    X = Génère-unif(A)
    N = N + 1
until X ∈ B
return X, N
```

Complexité

N Nombre d'itérations

$$\begin{aligned}\mathbb{P}(N=k) &= \mathbb{P}(X \in \mathcal{B}, N=k) \\ &= \left(1-\frac{|\mathcal{B}|}{|\mathcal{A}|}\right)^{k-1}\frac{|\mathcal{B}|}{|\mathcal{A}|}\end{aligned}$$

Loi géométrique de paramètre $p_a = \frac{|\mathcal{B}|}{|\mathcal{A}|}$.
Nombre moyen d'itérations

$$\begin{aligned}\mathbb{E}\,N &= \sum_{k=1}^{+\infty} k(1-p_a)^{k-1}p_a \\ &= \frac{1}{(1-(1-p_a))^2}p_a = \frac{1}{p_a}.\end{aligned}$$

$$Var\ N = \frac{1-p_a}{p_a^2}$$