Generadores de números pseudo-aleatorios

Eliana Scheihing[1]

[1]Instituto de Informática
Facultad de Ciencias de la Ingeniería
Universidad Austral de Chile

octubre 2022

Contenido

Contenido

Generadores de números pseudo-aleatorios

La mayor parte de los lenguajes de programación poseen un generador de números al azar o pseudo-aleatorios. Que se entiende por *números al azar* depende de la naturaleza de los mismos: booleanos, enteros, reales. En esta presentación vamos a analizar el caso de las funciones que retornan un real al azar en el intervalo $[0, 1]$. Esta concepción de azar considera los siguientes postulados:

Postulados:

1. Para todo a, b, $0 \leq a < b \leq 1$, $P[\text{ Random } \in]a, b]\,] = b - a$.
2. Los sucesivos llamados a la función Random genera experiencias aleatorias **independientes**

Interpretación

En el lenguaje habitual *al azar* no significa solamente aleatorio, sino que también uniformemente distribuido. Escoger al azar es dar la misma probabilidad a todos los resultados posibles (equiprobabilidad). Por otra parte, si consideramos que dos extraciones sucesivas de la función Random representan *puntos al azar* en el plano $[0,1]^2$, entonces el postulado de independencia se puede escribir como:

$$\forall a, b \ , \ 0 \leq a < b \leq 1 \ , \ \forall c, d \ , \ 0 \leq c < d \leq 1$$

$$P[(\mathrm{Random}_1, \mathrm{Random}_2) \in]a, b] \times]c, d]\,] = (b-a)(d-c)$$

Esta formulación puede extenderse a n dimensiones.

Proposición:

Para todo $k \in \mathbb{N}^*$, sean $(R_1, \ldots, R_k)$ k llamados sucesivos de la función Random . Los postulados (1) y (2) implican que para todo rectángulo:

$$D =]a_1, b_1] \times \cdots \times]a_k, b_k],\ 0 \leq a_i < b_i \leq 1\ ,\ i = 1, \ldots, k\ :$$

$$P[\,(R_1, \ldots, R_k) \in D\,] = (b_1 - a_1) \cdots (b_k - a_k)$$

Además, la probabilidad de que Random tome un valor particular es nula:

$$\forall a \in [0, 1]\ P[\ \text{Random} = a\,] = 0$$

En efecto,

$$\forall \varepsilon > 0\ ,\ P[\ \text{Random} = a\,] \leq P[\ \text{Random} \in]a - \varepsilon,\ a]\,] = \varepsilon$$

Y entonces se cumple que

$$\begin{aligned} P[\text{Random}\ \in]a, b]\,] &= P[\text{Random}\ \in\ [a, b]\,] \\ &= P[\text{Random}\ \in\ [a, b[\,] = P[\,\texttt{Random} \in]a, b[\,] \end{aligned}$$

Ejemplos

1. Sea $Int()$ la función parte entera, entonces se define la v.a.

$$X \longleftarrow (Int(\underbrace{\texttt{Random}}_{R_1} * 3)) * (\text{Int}(\underbrace{\texttt{Random}}_{R_2} * 2))$$

X toma valores $0, 1, 2$ y se cumple:

$$\begin{aligned} P[X = 2] &= P[Int(\,R_1 * 3\,) = 2 \text{ y } Int(\,R_2 * 2\,) = 1\,] \\ &= P[\,R_1 \in [2/3,\, 1[\text{ y } R_2 \in [1/2,\, 1[\,] \\ &= \left(1 - \tfrac{2}{3}\right)\left(1 - \tfrac{1}{2}\right) = \tfrac{1}{6} \end{aligned}$$

Asi mismo se puede mostrar que

$$P[X = 1] = 1/6 \text{ y } P[X = 0] = 4/6$$

2. Lanzar un dado.
Definamos,

$$D \longleftarrow Int(\text{Random} * 6) + 1$$

Entonces,

$$\begin{aligned} P[D = k] &= P[Int(\text{Random} * 6) = k - 1] \\ &= P[\text{Random} * 6 \in [k-1, k[] \\ &= P[\text{Random} \in [(k-1)/6,\ k/6[] = \frac{k}{6} - \frac{k-1}{6} = \frac{1}{6} \end{aligned}$$

$$\forall k \in \{1, \ldots, 6\}$$

Contenido

Secuencias Uniformes

Un generador pseudo-aleatorio retorna secuencias de números, cuyas frecuencias experimentales buscamos que cumplan en el límite con las características de la distribución uniforme.

Definición: Una secuencia (x_n), $n \in \mathbb{N}$, de valores en $[0,1]$ se dice k-uniforme si para todo rectángulo:

$$D =]a_1, b_1] \times \cdots \times]a_k, b_k],\ 0 \leq a_i < b_i \leq 1\ ,\ i = 1, \ldots, k$$

cumple

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \mathbb{1}_D((x_{ki}, x_{ki+1}, \ldots, x_{k(i+1)-1})) = (b_1 - a_1) \cdots (b_k - a_k)$$

Donde $\mathbb{1}_D$ es la notación de la función indicatriz del conjunto D:

$$\mathbb{1}_D(y) = \begin{cases} 1 & \text{si } y \in D, \\ 0 & \text{si no.} \end{cases}$$

El vector $(x_{ki}, x_{ki+1}, \ldots, x_{k(i+1)-1})$ es la i-ésima k-tupla de elementos consecutivos de la secuencia y la suma $\sum_{i=0}^{n-1} \mathbb{1}_D((x_{ki}, x_{ki+1}, \ldots, x_{k(i+1)-1}))$ es el número de k-tuplas de elementos consecutivos de la secuencia que pertenecen a D entre los n primeros elementos.

Definición:

Una N-*tupla* de números en $[0, 1]$ se dice pseudo-aleatoria si cumple con éxito una serie de test estadísticos destinados a verificar su k-uniformidad. Los generadores disponibles en los compiladores habituales son el resultados de una amplia experimentación estadística.

Generadores congruenciales lineales

Los generadores mas simples se denominan generadores congruenciales lineales y son de la forma:

$$u_{n+1} = g(u_n) = (Au_n + C) \text{ modulo } M$$

Diversos resultados matemáticos permiten justificar una buena elección de A, C y M, como por ejemplo:

$$g(u) = (\,16807\, u\,) \text{modulo}\, 2147483647$$

Todo generador necesita una inicialización o semilla u_0. Si se utiliza una misma semilla, se puede reproducir la misma secuencia de valores. Si se desean obtener distintas secuencias de una ejecución a otra es necesario cambiar el valor de la semilla en cada nueva ejecución.

Generador Mersenne Twister

Este generador debido a M. Matsumoto y T. Nishimura (1997) es ampliamente utilizado y su principal característica es que tiene un largo periodo de $M = 2^{19937} - 1$ (primo Mersenne) y que cumple con la k-uniformidad antes descrita.
Las series x se definen como series de cantidades de w bits con la siguiente relación de recurrencia:

$$x_{k+n} = x_{k+m} \oplus \left(({x_k}^u \mid\mid {x_{k+1}}^l)A \right) \qquad\qquad k = 0, 1, \ldots$$

donde n es el grado de recurrencia, m el desplazamiento , $||$ denota la concatenación de vectores de bits y $\oplus$ la operación o-exclusivo (XOR) w^u son los $w - r$ bits superiores de w y w^l los r bits inferiores de w. A es la transformación (twist) definida por:

$$A = \begin{pmatrix} 0 & I_{w-1} \\ a_{w-1} & (a_{w-2}, \ldots, a_0) \end{pmatrix}$$

con I_{w-1} la matriz identidad de dimensión $(w-1)x(w-1)$.

La mayor parte de los generadores de números pseudo-aleatorios generan números enteros y se transforman a la escala [0,1] al dividir por M cada elemento de la secuencia generada. Las propiedades se verifican sobre las secuencias generadas.

Contenido

Proposición:
Sea U v.a. $\sim \mathbb{U}[0,1]$ y F una función de distribución de probabilidad acumulada de una v.a. continua, entonces se cumple que:

$$X = F^{-1}(U) \sim F$$

Demostración:
En efecto

$$P(X \leq x) = P(F^{-1}(U) \leq x) = P(U \leq F(x)) = F(x)$$

De manera que para generar una secuencia pseudo-aleatoria de valores de X, basta generar una secuencia

$$u_1, \cdots, u_n$$

de valores pseudo-aleatorios en $[0,1]$ y calcular

$$x_i = F^{-1}(u_i), \qquad i = 1, \cdots, n$$

En el caso de v.a. discretas se tiene lo siguiente: Sea X v.a. discreta que cumple

$$P(X = x_j) = p_j \qquad j = 1, 2, \cdots \qquad \text{tal que} \sum_{j=1}^{\infty} p_j = 1$$

y U v.a. $\sim \mathbb{U}[0, 1]$ entonces podemos definir:

$$X = \begin{cases} x_0 & \text{si } U < p_0 \\ x_1 & \text{si } p_0 \leq U < p_0 + p_1 \\ & \vdots \\ x_j & \text{si } \sum_{i=0}^{j-1} p_i \leq U < \sum_{i=0}^{j} p_i \\ & \vdots \end{cases}$$

Y entonces se cumple que X tiene la distribución deseada:

$$P(X = x_j) = P\left(\sum_{i=0}^{j-1} p_i \leq U < \sum_{i=0}^{j} p_i\right) = p_j$$

De manera que para generar una secuencia pseudo-aleatoria de valores de X, basta generar una secuencia

$$u_1, \cdots, u_n$$

de valores pseudo-aleatorios en $[0,1]$ y calcular

$$y_k = \begin{cases} x_0 & \text{si } u_k < p_0 \\ x_1 & \text{si } p_0 \leq u_k < p_0 + p_1 \\ & \vdots \\ x_j & \text{si } \displaystyle\sum_{i=0}^{j-1} p_i \leq u_k < \sum_{i=0}^{j} p_i \\ & \vdots \end{cases} \qquad k = 1, \cdots, n$$