# Generación de números aleatorios $\hat{U}(0,1)$

Funciones $rand()$ , $rand\_f()$.

rand() números aleatorios independientes y uniformemente distribuidos en el intervalo $(0,1)$

Para el ordenador es suficiente considerar $m/M$, con $m$ un número entero distribuido uniformemente en el intervalo $(0, M-1)$.

$(m+0.5)/M$.

Mtodo de la mano inocente

Método de Von Neumann. $M = 10000$.

Semilla $m_0 \in (0, M-1)$

$$m_0 = 5232 \rightarrow m_0^2 = 27373824 \rightarrow m_1 = 3738$$

$$m_1 = 3738 \rightarrow m_1^2 = 13972644 \rightarrow m_2 = 9726$$

$$m_2 = 9726 \rightarrow m_2^2 = 94595076 \rightarrow m_3 = 5950$$

$x_0 = 0.5232, x_1 = 0.3738, x_2 = 0.9726, x_3 = 0.5950, ....$ Parece aleatoria?

Nmeros pseudoaleatorios

Tests estadisticos:

–Momentos. $< x_i^n >= (n+1)^{-1}$

–Correlaciones.

$$\langle x_i x_j \rangle = \begin{cases} 1/4 & \text{if } i \neq j \\ 1/3 & \text{if } i = j \end{cases}$$

El generador de von Neumann no es un buen generador.

– Buenas propiedades estadísticas.

– Eficiencia en la generación.

– Periodo largo.

– Reproducibilidad.

## Generadores Congruenciales

Relación recurrente del tipo:

$$m_{i+1} = F(m_0, m_1, ....m_i) \mod (\mathrm{M})$$

Obviamente $m \in (0, M-1)$.

Von Neumann $m_{i+1} = [m_i^2/100] \; mod \; 10000$

Buenos resultados con funciones lineales

$$m_{i+1} = (am_i + c) \mod (\mathrm{M})$$

$m_0$ "semilla"

$m_{i+1} = F(m_i)$ mod (M)

necesariamente se repite al cabo de $M$ iteraciones

Probabilidad de que $m_{i+1} = m_i$ es $0 \neq 1/M$

Ecuacin determinista

$c = 0$ generadores congruenciales multiplicativos

$c \neq 0$ generadores congruenciales mixtos

## Generadores Congruenciales Mixtos

Secuencia $m_i$ definida con periodo máximo $(M)$. Condiciones necesarias y suficientes:

–(i) c es primo con M

–(ii) a=1 mod g, para cada divisor primo g de M

–(iii) a=1 mod 4 si M es múltiplo de 4

Es útil si $M = 2^b$

876487 mod $2^6 = 7$

1101010111111000111 mod $2^6 = 000111 = 7$

SI $M = 2^b$, para un periodo mximo

–(i) $c$ ha de ser impar

–(ii) $a = 1$ mod (4)

Algunos valores:

$$M = 2^{35} = 34359738368; \quad a = 2^7 + 1 = 129; \quad c = 1$$

$$M = 2^{32} = 4294967296; \quad a = 69069; \quad c = 1$$

Generador utilizado en el VAX y otros ordenadores

$$M = 2^{32}; \quad a = 1812433253; \quad c = 1$$

## Generadores Congruenciales Multiplicativos

$c = 0$ , $m_{i+1} = am_i$ mod M. Ms sencillos.

No pueden alcanzar el ciclo máximo $M$.

Pueden alcanzar un ciclo quasi–mximo de $M - 1$ si:

–(i) M es primo

–(ii) a es una raíz primitiva de M. Es decir:

$a^M = 1$ mod M, pero $a^n \neq 1$ mod M, $\forall$n $<$ M.

Algunos valores:

$M = 2^{31} - 1$ (número primo de Mersenne)

$a = 7^5 = 16807$

$a = 742938285$

$a = 69069$

$M = 2147483563$, $a = 40014$

$M = 2147483399$, $a = 40692$

Si $M = 2^b$, el periodo máximo es $M/4$ y se alcanza cuando $a = 8r \pm 3$, r es un número positivo, y $m_0$ es un número impar

$M = 2^{35},\ a = 2^{17} + 3$

$M = 2^{32},\ a = 69069$

$M = 2^{32},\ a = 1664525$

$M = 2^{47},\ a = 5^{15}$

$M = 2^{29},\ a = 65539$ generador RANDU, particularmente malo.

**El Teorema de Marsaglia**

Todos los generadores congruenciales tienen correlaciones cuando se consideran en un espacio d-dimensional con d suficientemente alto

Los puntos $(x_1, x_2, ..., x_d)$ caen en hiperplanos de dimensión $d-1$.

**Generadores FSR**

Los generadores FSR ("Feedback Shift Register") generan números pseudoaletorios $z_i$ binarios, 0,1

$$z_i = c_1 z_{i-1} + c_2 z_{i-2} + ... + c_n z_{i-n} \bmod 2$$

$c_i = 0, 1$ son $n$ constantes binarias.

Periodo mximo $2^n$. Se alcanza si y slo si:

$$f(z) = 1 + c_1 z + c_2 z^2 + ... + c_n z^n$$

no se pueda escribir como $f(z) = f_1(z) f_2(z)$ (todas las operaciones módulo 2)

Las relaciones más sencillas se basan en polinomios:

$$f(z) = 1 + z^q + z^p$$

Que reducen la relación de recurrencia a la forma:

$$z_i = z_{i-p} + z_{i-q} \ \ mod(2)$$

Si consideramos que $z_i$ son variables lógicas:

$$z_i = z_{i-p} \otimes z_{i-q}$$

$p = 250, q = 103$ generador R250.

Periodo $= 2^{250} \approx 1.8 \times 10^{75}$

$p = 1279$, $q = 418$ se muestra superior al R250

Teorema de Marsaglia también es válido.