Simuladores

Simulação

Modelo matemático

Experimento real

Ingredientes básicos para simulação
* modelo
* se estocástico : RNG (bom)

Gerador de Numeros aleatorios

* Efeitos físicos (térmico, diodo Zener, átomo)
* computador é determinístico → PRNG

PRNG → Eficiente
PRNG → Determinístico
PRNG → Periódico

Linear Congruential Generator (LCG)

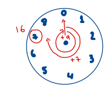
$$\boxed{z_i = (a z_{i-1} + c) \bmod m}$$

Lets starts with $a=2, c=0, \underbrace{z_0 = 1}_{\text{seed}}, m=9$

Period

$z_i = (2 z_{i-1}) \bmod 9$
$z_1 = 2 \bmod 9 = 2$
$z_2 = (2\times2) \bmod 9 = 4$
$z_3 = (2\times4) \bmod 9 = 8$
$z_4 = (2\times8) \bmod 9 = 7$
$z_5 = (2\times7) \bmod 9 = 5$
$z_6 = (2\times5) \bmod 9 = 1$
$z_7 = (2\times1) \bmod 9 = 2$
$z_8 = (2\times2) \bmod 9 = 4$

Ex. 16 mod 9



$u_1 = 2/9 = 0{,}22$
$u_2 = 4/9 = 0{,}44$
$u_3 = 8/9 = 0{,}88$
$u_4 = 7/9 = 0{,}77$
$u_5 = 5/9 = 0{,}55$
$u_6 = 1/9 = 0{,}11$
$u_7 = 2/9 = 0{,}22$

Linear Recursive Generator

* Adiciona mais os anteriores no LCG:

$$\boxed{z_i = (a_1 z_{i-1} + a_2 z_{i-2} + \dots) \bmod m}$$

hoje → Mersenne Twister é o mais utilizado (Python)
hoje → criptografia

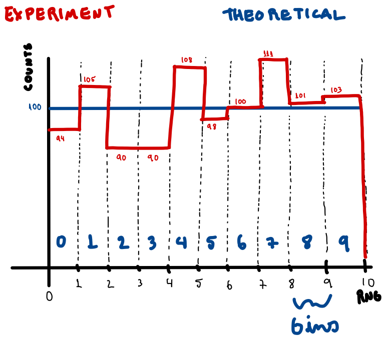
Entropy Source

Soft test, Reseed, good Alg.

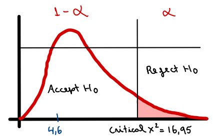
{ SP 800, FIPS 140, NIST }

Chi-square goodness of fit

histograma (Experimental) × Uniforme (teoria)



$$\boxed{X^2 = \sum_{i=1}^{10} \frac{(O_i - E_i)^2}{E_i} = 4.6}$$

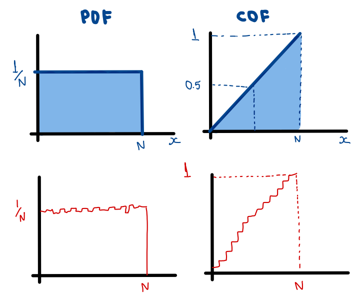


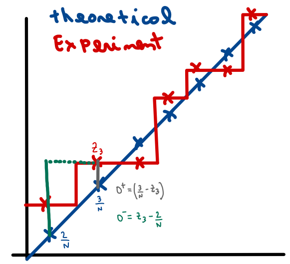
Accept H0!

$\alpha = 0{,}05$ and $\underbrace{DF = 9}_{\text{grau de liberdade}}$

$$\begin{cases} H_0 : \text{Is uniform where } X^2 \leq 16{,}95 \\ H_1 : \text{non-uniform where } X^2 > 16{,}95 \end{cases}$$

Kolmogorov-Smirnov test





$D^- = \max_{1 \leq i \leq N} \left(z_i - \frac{i-1}{N} \right)$

$D^+ = \max_{1 \leq i \leq N} \left(\frac{i}{N} - z_i \right)$

$D = \max(D^-, D^+)$

If $D \leq D_\alpha$ accept the hypothesis.

Outros testes : Runs

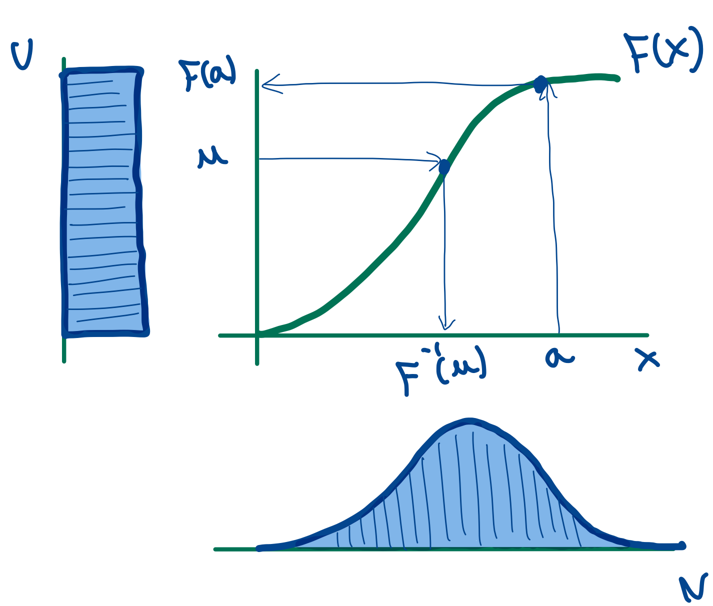
Statistical test Suite do NIST

STS : 16 testes

DIEHARD : 12 testes

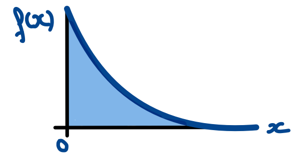
* α entre [0.01, 0.001] para equipamentos críticos como HSM, cartões, tokens. (security module)

Transformada Inversa



Exponencial

$$f(x) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 ; \lambda > 0 \\ 0 & \text{otherwise} \end{cases}$$



$$F(x) = \int_0^x \lambda e^{-\lambda t} dt = -\cancel{\frac{\lambda}{\lambda}} e^{-\lambda t} \Big]_0^x = -e^{-\lambda x} - (-1) \Rightarrow \boxed{F(x) = 1 - e^{-\lambda x}}$$

Now put the x in function of y:

$$y = 1 - e^{-\lambda x}$$

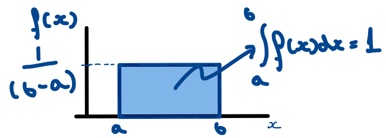
$$e^{-\lambda x} = 1 - y$$

$$-\lambda x = \ln(1-y)$$

$$\boxed{x = -\frac{1}{\lambda} \ln(1-y)}$$

Uniforme deslocada

$$f(x) = \begin{cases} 1/(b-a), & x \in [a, b] \\ 0, & \text{otherwise} \end{cases}$$



$$F(x) = \int_a^x \frac{1}{(b-a)} dt = \frac{1}{(b-a)} t \Big]_a^x = \frac{x-a}{(b-a)}$$

Setting $y = \frac{x-a}{(b-a)}$, we obtain the inverse by writing x in terms of y.

$$\boxed{x = a + (b-a)y}$$