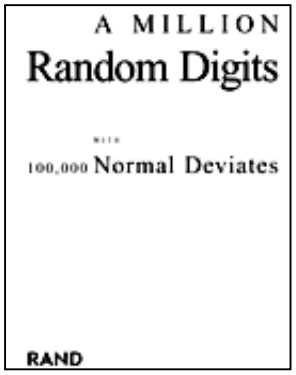
Geração de números pseudo-randômicos

Algoritmo que gere uma seqüência de números → DETERMINÍSTICA

Na natureza: jogo de dados, roleta, movimento browniano...

Abordagem atual

- construção de funções
- número gerado depende do número anterior na seqüência
- seqüências pseudo-randômicas



RAND Corp. (1955): seqüência (tabela) de 1 milhão de n^{os} randômicos, a partir de ruído eletrônico em um tubo de vácuo;

- projeto Rand (Força Aérea americana; **R**esearch **A**nd **N**o **D**evelopment :-)
- complexidade algorítmica = conteúdo de informação algorítmica (**CIA**) = randomicidade algorítmica;
- CIA introduzido independentemente por Kolmogorov / Chaitin / Solomonoff;

- string de 0s e 1s; quais os algoritmos que farão o comput. gerar esta seqüência
  - O tamanho do algoritmo + curto é o CIA desta string;
  - ex.: string = **110 110 110 110** → 4x print (110) ⇨ baixo CIA
  - esta cadeia tem ALTA compressabilidade;
- uma cadeia randômica não é comprimível (ou tem baixa compressabilidade) e tem CIA máximo !
- randomicidade ≠ complexidade: alta entropia (elementos simples) = CIA alto mas sem complexidade

random.org

Fill out this form to generate genuine random numbers.

Generate 100 random integers (maximum 10,000).

Smallest value 1 (limit -1000,000,000).

Largest value 100 (limit 1000,000,000).

Format in 5 columns.

Get Numbers | Reset Form

Request HotBits

Generate 128 random bytes (maximum 2048).

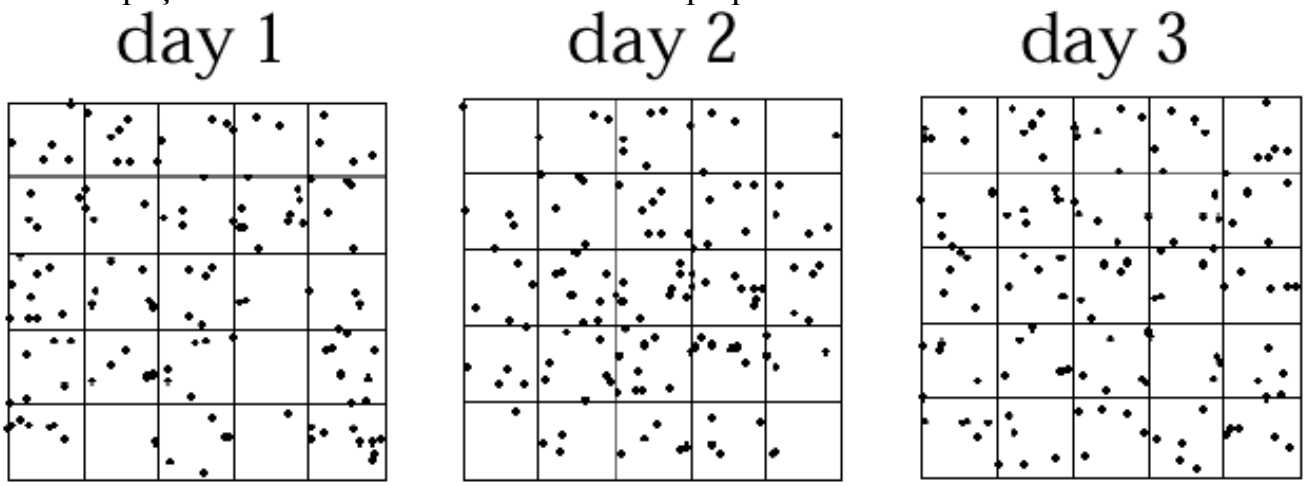
Format:

- (•) Hexadecimal (sample)
- ( ) Binary download to a file
- ( ) C language constant declaration (sample)

Get HotBits | Reset defaults

Propriedades desejáveis de geradores pseudo-randômicos

1. os n^{os} devem ser uniformemente distribuídos;
2. os n^{os} devem ser independentes, i.e., sem correlação dentro da seqüência;
3. ciclo deve ser grande;
4. a seqüência deve ser reprodutível; deve ser possível utilizar diferentes sementes (*seeds*), o que gera seqüências diferentes;
5. gerador deve ser rápido;
6. espaço de memória necessário deve ser pequeno.



Qual é o dia onde a distrib. das gotas de chuva foi ao acaso?

Métodos clássicos para geração de seqüências pseudo-randômicas

Random number generators should not be chosen at random.
– Donald Knuth (1986)

❶ método do quadrado médio (John von Neumann+Metropolis em 1940)

Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. – John von Neumann (1951)

Exemplo:
semente = 6735
a)
$X_1 = 6735^2 = 45360225 \rightarrow 3602$
$X_2 = 3602^2 = 12974409 \rightarrow 9744$
$X_3 = 9744^2 = 94945536 \rightarrow 9455$
$X_4 = 9455^2 = 89397025 \rightarrow 3970$
: : : :

Problema: tendência de degenerar rapidamente para zero.

b) conversão para base unitária (Xi entre 0 e 1)

$X_1 = 3602/9999 = 0{,}36023$
$X_2 = 9744/9999 = 0{,}97449$
$X_3 = 9455/9999 = 0{,}94559$
: : :

c) convertendo para um intervalo (de A→B) $FN_i = A+(B-A)* X_i$

se A=5 e B=15 então:
$FN_1 = 5+(10) * 0{,}36023 = 8{,}602$
$FN_2 = 5+(10) * 0{,}97449 = 14{,}7449$
$FN_3 = 5+(10) * 0{,}94559 = 14{,}4559$

❷ gerador congruente linear (LCG)

LCG **aditivo**:

$X_i = (a*X_{i-1} + c) \bmod m$

Xi : um número da seqüência
a : constante multiplicativa
c : constante aditiva
X_0 : semente

Exemplo:
$X_0=4$ a=3 c=1 m=5
$X_i = (3 * X_{i-1} + 1) \bmod 5$

Obs.:
O modulo m determina o intervalo dos valores obtidos [0 a m-1]

$X_1 = 13 \bmod 5 = 3$
$X_2 = 10 \bmod 5 = 0$
$X_3 = 1 \bmod 5 = 1$
$X_4 = 4 \bmod 5 = 4$
$X_5 = 13 \bmod 5 = 3$

→ Ciclo = 4 iterações

LCG **multiplicativo**: c=0

Exemplo:
$X_0=4$ a=3 m=5
$X_i = (3 * X_{i-1}) \bmod 5$

$X_1 = 12 \bmod 5 = 2$
$X_2 = 6 \bmod 5 = 1$
$X_3 = 3 \bmod 5 = 3$
$X_4 = 9 \bmod 5 = 4$

Obs.:
Os maiores ciclos seriam obtidos quando:
m → primo
a → raíz primitiva de m :

$a^p = 1 + mK$
Onde
p = m-1
K é inteiro