O Aleatório em Computação

Por Diogo Anderson (diogo@dsc.ufcg.edu.br)

Integrante do Grupo PET Computação

Agenda

- Introdução
  - Definição
  - Aplicações
- Números aleatórios
  - Números aleatórios vs pseudo-aleatórios
  - Geração de números aleatórios
  - Geração de números pseudo-aleatórios

Objetivos

- Mostrar conceitos de números aleatórios;
- Explicar a importância de números aleatórios em computação;
- Apresentar modos de geração de aleatoriedade em sistemas computacionais.

Definição

- Do Aurélio, aleatório é aquilo que é “dependente de fatores incertos, sujeitos ao acaso”;
- Em computação, todo dado é numérico, assim a aleatoriedade se dá com os números aleatórios;
- Número aleatório é, em Estatística, um número que pertence a uma série numérica e não pode ser previsto a partir dos membros anteriores da série.

Aplicações

a) Simulação: quando um computador é utilizado para reproduzir fenômenos naturais;
b) Amostragem: é geralmente impraticável examinar todos os casos possíveis;
c) Análise numérica: técnicas mais simples para resolver problemas numéricos complicados foram desenvolvidas usando aleatoriedade;

Aplicações

d) Programação: números aleatórios servem de dados para testar algoritmos. Além disso, são cruciais na execução de algoritmos aleatórios;

e) Outras aplicações: criptografia, tomada de decisão, arte, recreação (jogos, loterias, etc).

Dificuldades

- O computador é um dispositivo determinístico, logo, a geração de números aleatórios necessita de dispositivos especiais;
- Ironicamente, a aleatoriedade é um problema para algumas aplicações que podem requerer a repetição de uma dada execução: simuladores, testadores, etc.

Números Pseudo-aleatórios

- São números gerados por meio de manipulação aritmética;
- Não são aleatórios, afinal, os números da sequência gerada dependem dos valores anteriores.

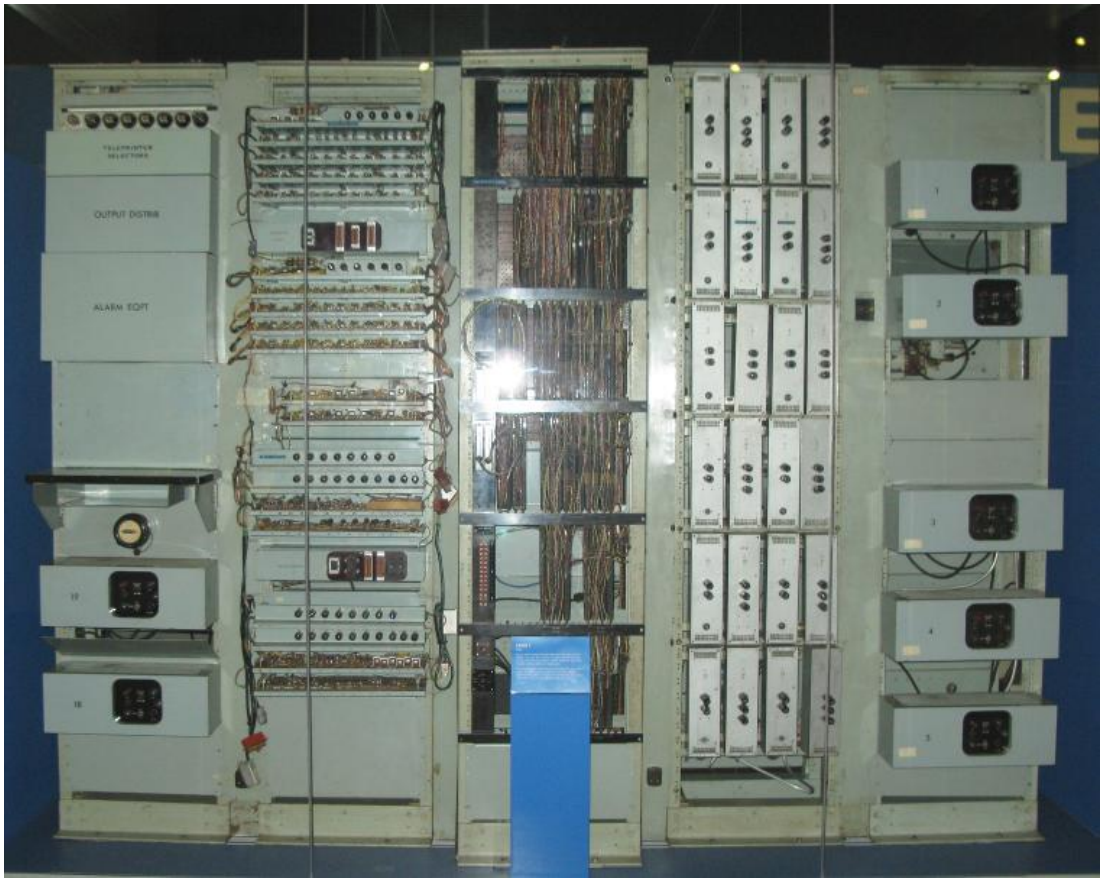
APLICABILIDADE

Aplicação	Tipo de Gerador
Loteria e Sorteios	Aleatório Real
Jogos	Aleatório Real
Amostragem	Aleatório Real
Simulação e Modelagem	Pseudo Aleatório
Segurança (Geração de Chaves)	Aleatório Real
Arte	Varia

Gerando números aleatórios

- A geração de números aleatórios demanda fenômenos físicos (hardware);
- Exemplos de fenômenos que podem ser utilizados:
  - Decaimento de núcleos radiativos (HotBits);
  - Ruído atmosférico (RANDOM.org).

ERNIE (1957)



Determinismo na Natureza

- Para o conhecimento atual de Física Quântica, muitos fenômenos subatômicos são não determinísticos;
- Métodos que não utilizam propriedades quânticas são determinísticos, porém, caóticos.
  - Para fins de sequências numéricas, são geralmente aleatórios (a dependência não se dá entre os números);

Gerando números pseudo-aleatórios

- Algumas manipulações clássicas para dar à sequência de números uma "aparência" de aleatoriedade:
  - John Von Neumann – elevação ao quadrado e seleção de dígitos centrais;
  - Métodos de Congruência – utilização de operações de módulo.

Método de Von Neumann

- Suponha que queremos gerar números de 10 dígitos, e o número atual é 5772156649;
- Ao quadrado: 33317792380594909201;
- Próximo número: 7923805949.

Método de congruência

- Utilizado para gerar números com “distribuição uniforme”:

$$X_{n+1} = (aX_n + c) \bmod m$$

$$X_k = (a^k X_o + (a^k - 1)c/(a-1)) \bmod m$$

- Sequência periódica de comprimento menor ou igual a m, determinada pela escolha dos parâmetros.

Gerando outras Distribuições

- Dada uma sequência de números U_1, U_2, ..., U_n de números com distribuição uniforme.
- Se $F(x)$ é a função de distribuição acumulada de uma dada distribuição, podemos gerar uma sequência de números $\{X_n\}$ nesta distribuição fazendo:

$$X_n = F^{-1}(U_n)$$

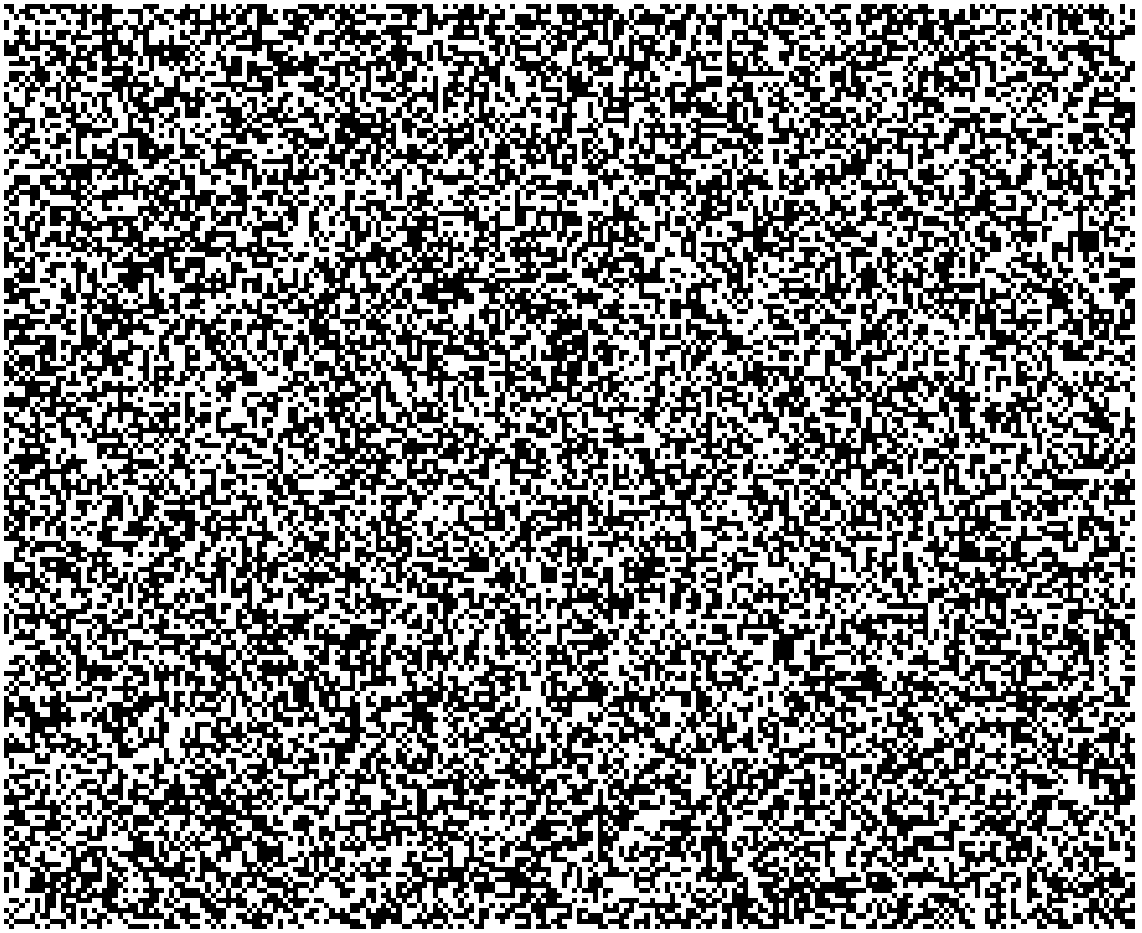
Comparação De Geradores

Característica	Pseudo Aleatórios	Aleatório Real
Eficiência	Alta	Baixa
Determinismo	Determinístico	Não Determinístico
Periodicidade	Periódico	Aperiódico

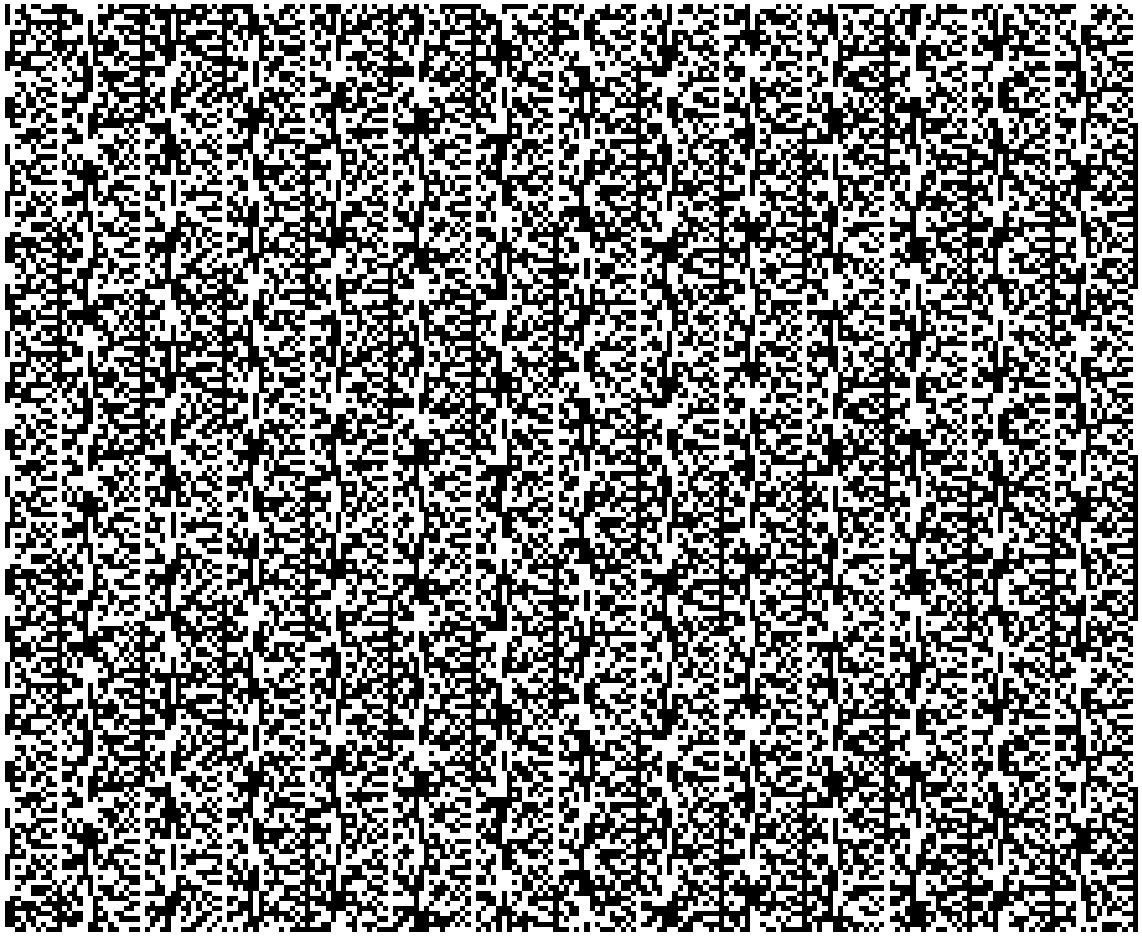
Utilizando Geradores

- Formas mais comuns de utilizar geradores de números (pseudo) aleatórios:
  - Linguagens e bibliotecas: rand() em C e PHP, classe Random, em Java;
  - Serviços web de números aleatórios reais, como RANDOM.org e HotBits.

Comparação Visual: RANDOM.org



Comparação Visual:PHP rand()



Testando a aleatoriedade do gerador

- Há mecanismos para se checar a qualidade de um gerador de números aleatórios:
  - Testes Empíricos;
  - Testes Teóricos;
  - Testes Espectrais;
- Exemplos: Correlação Serial, Teste Chi-Quadrado.

Considerações Finais

- Números aleatórios desempenham um papel importante na Computação;
- Há diferença entre número aleatório e número pseudo aleatório, com aplicabilidade diferente para cada classe;
- Há muitos métodos para a geração de números pseudo aleatórios, e bastante teoria para fazê-la de forma adequada.

Referências

- Comparação Visual:
  - http://www.boallen.com/random-numbers.html
- RANDOM.org
  - http://www.random.org
- HotBits Service:
  - http://www.fourmilab.ch/hotbits/
- Knuth, D. E., Art of Computer Programming, Volume 2 – Seminumerical Algorithms

Dúvidas