

Trabalho 1 - Modelação Estocástica



Trabalho realizado por:
Ana Almeida nº111658 | Rita Guerreiro nº 112018

Em 1942, Lehmer sugeriu que o período da sequência cíclica de números pseudo-aleatórios (NPA's) deveria ser o mais longo possível, e quase todos os geradores de NPA's atuais baseiam-se nesta ideia.

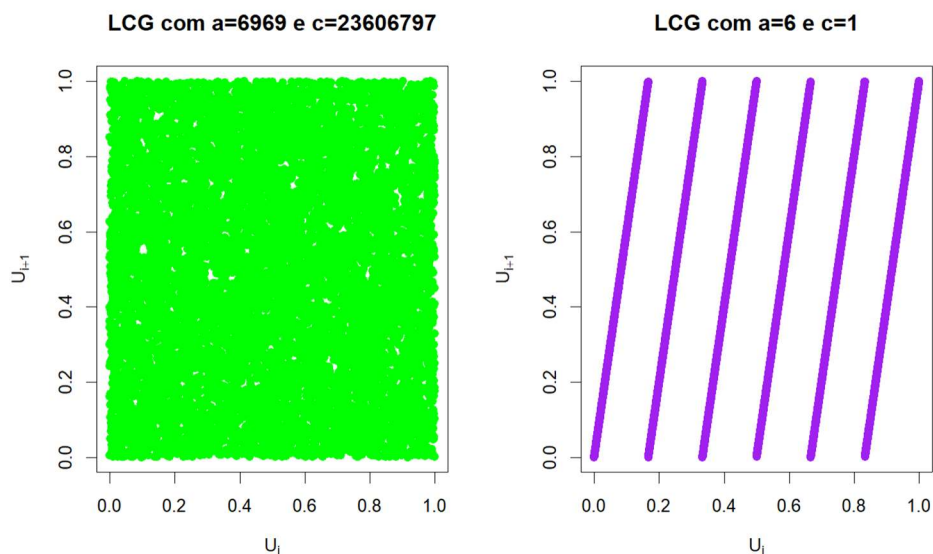
O Gerador Congruencial Linear (GCL), ou algoritmo de Lehmer, gera NPA's inteiros através da seguinte função:

$$X_{n+1} = (a * X_n + c) \bmod m$$

A eficácia do GCL depende criticamente da escolha dos parâmetros a , c e m . O período máximo teórico é m , mas o real pode ser menor ($n \leq m$), causando repetições indesejadas ($x_n = x_0$) (*Linear Congruential Generators*). Para atingir o período máximo, os parâmetros devem ser cuidadosamente selecionados (L'Ecuyer, 1999).

Nos seguintes gráficos, alteramos apenas o parâmetro a e c :

$$m = 2^{32}; x_0 = 0; n \text{ (número de valores a gerar)} = 12 \times 10^4$$



Os gráficos demonstram como a escolha dos parâmetros (a , c) afeta significativamente a qualidade da sequência gerada. No gráfico da esquerda os

parâmetros apresentam claramente melhores resultados em termos de aleatoriedade e período do que no gráfico da direita.

O Gerador Mersenne Twister (GMT), usado no R, oferece um período substancialmente maior ($2^{19937} - 1$) e melhor qualidade de aleatoriedade. Utiliza operações bit a bit numa matriz de 624 números de 32 bits cada. O algoritmo modifica esses bits para gerar novos números (*What Is Mersenne Twister?*).

O GMT assenta na seguinte função:

$$X_{k+n} = X_{k+m} \oplus (X_k^u \mid X_{k+1}^l)A$$

(*The Mersenne Twister*)

No R, o GMT é o gerador de NPA's padrão, sendo utilizado em diversas funções como *rnorm()*.

Os dois geradores (GCL e GMT) partilham algumas características:

- Ambos são geradores de NPA's que usam funções recursivas para criar sequências determinísticas;
- Dependem de uma semente para inicializar;
- Projetados para criar sequências aleatórias e com boas propriedades estatísticas;
- Amplamente utilizados em aplicações como simulações e jogos pela sua eficiência e fácil implementação.

As principais diferenças entre os algoritmos assentam na complexidade e qualidade dos números gerados. O GCL usa uma função linear simples com período limitado pelo módulo m , enquanto o GMT é mais sofisticado, com operações bit a bit e período longo (Matsumoto & Nishimura, 1998). O GMT tem melhor distribuição dos números, passando em testes mais rigorosos de aleatoriedade e sendo preferido para aplicações que requerem NPA's de alta qualidade. O GCL, embora mais simples, ainda é útil em muitas aplicações e pode ser mais fácil de implementar e analisar matematicamente.

Para concluir, apesar do GCL ser útil para muitas aplicações devido à sua simplicidade, o GMT é preferido quando se requer NPA's de alta qualidade e longos períodos, como em simulações complexas ou criptografia.

Referências:

L'Ecuyer, P. (1999). Good Parameters and Implementations for Combined Multiple Recursive Random Number Generators. *Operations Research*, 47(1), 159–164.

<https://doi.org/10.1287/opre.47.1.159>

Linear Congruential Generators. Obtido 13 de outubro de 2024, de

<https://homes.luddy.indiana.edu/kapadia/project2/node7.html>

Matsumoto, M., & Nishimura, T. (1998). Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model.*

Comput. Simul., 8(1), 3–30. <https://doi.org/10.1145/272991.272995>

What is Mersenne Twister? Educative. Obtido 13 de outubro de 2024, de

<https://www.educative.io/answers/what-is-mersenne-twister>

Fitzmaurice, F. (2017, Maio 23). *The Mersenne Twister*. Maths.tcd.ie.

<https://www.maths.tcd.ie/~fionn/misc/mt/>