MERSENNE TWISTER

Elizandro Benedet

Gabriel Vinicius T. Kanczewski

Sandro Miguel Weizenmann

INTRODUÇÃO

- O Mersenne Twister é um gerador de números pseudo - aleatórios (pseudorandom number generator - PRNG).
- É de longe o PRNG de uso geral mais utilizado, também usado no Linux.
- Seu nome deriva do fato de que a duração do período é escolhida para ser um número primo de Mersenne .

INTRODUÇÃO

- O Mersenne Twister foi desenvolvido em 1997 por Makoto Matsumoto e Takuji .
- Foi projetado especificamente para corrigir a maioria das falhas encontradas nos PRNGs mais antigos

VANTAGENS

- Permissivamente licenciado e livre de patentes para todas as variantes, exceto o CryptMT.
- Passa em vários testes de aleatoriedade estatística, incluindo os testes Diehard e a maioria, mas não todos os testes TestU01.
- Um período muito longo de 2 ^(19937) -1 . Observe que, embora um longo período não seja uma garantia de qualidade em um gerador de números aleatórios, períodos curtos, como o 2^(32) comum em muitos pacotes de software mais antigos, podem ser problemáticos.
- k distribuído com precisão de 32 bits para cada $1 \leq k \leq 623$
- As implementações geralmente criam números aleatórios mais rapidamente do que outros métodos. Um estudo descobriu que o Mersenne Twister cria números aleatórios de ponto flutuante de 64 bits aproximadamente vinte vezes mais rápido que o conjunto de instruções RDRAND , implementado em hardware e com processador

DESVANTAGENS

- Um buffer de estado relativamente grande, de 2,5 KiB , a menos que a variante TinyMT seja usada.
- Taxa de transferência medíocre pelos padrões modernos, a menos que a variante SFMT seja usada.
- Exibe duas falhas claras (complexidade linear) no Crush e BigCrush no conjunto TestU01.
- Múltiplas instâncias que diferem apenas no valor da semente (mas não em outros parâmetros) geralmente não são apropriadas para simulações de Monte Carlo que requerem geradores de números aleatórios independentes, embora exista um método para escolher vários conjuntos de valores de parâmetros.

DESVANTAGENS

- Pode levar muito tempo para começar a gerar resultados que passam nos testes de aleatoriedade , se o estado inicial for altamente não aleatório - principalmente se o estado inicial tiver muitos zeros. Uma conseqüência disso é que duas instâncias do gerador, iniciadas com estados iniciais quase iguais, geralmente produzem quase a mesma sequência para muitas iterações, antes de eventualmente divergir. A atualização de 2002 para o algoritmo MT melhorou a inicialização, de modo que é muito improvável começar com esse estado.
- Não é criptograficamente seguro , a menos que a variante CryptMT seja usada. O motivo é que a observação de um número suficiente de iterações (624 no caso de MT19937, já que esse é o tamanho do vetor de estado do qual as iterações futuras são produzidas) permite prever todas as iterações futuras.

CÓDIGO

- https://repl.it/@ElizandroBenede/MersenneTwister