Aplicação de protocolos de testes para geradores de números aleatórios

Rodrigo Silva de Almeida , Lucca Rodrigues Cunha, Bernardo Maia Coelho, Pedro Calligaris Delbem, César Magno Leite de Oliveira Junior, Filippo Ghiglieno, Alexandre Delbem

***Resumo*— A importância das sequências aleatórias e pseudo-aleatórias tem crescido exponencialmente devido a suas aplicações, principalmente com o advento dos Quantum Random Number Generators (QRNGs). Para garantir a validade dessas sequências, foram criados testes estatísticos que se propõem a definir o quão aleatória uma sequência é, e consequentemente o quão viável ela é para uma aplicação. A fim de criar uma bateria de testes eficaz, o National Institute of Standards and Technology (NIST) desenvolveu os 15 testes que serão implementados neste projeto. Neste trabalho, o intuito é implementar tais verificações e sugerir novos métodos para determinar a aleatoriedade.**

***Palavras-Chave*— Geradores de números aleatórios, NIST, QRNG, Protocolos de Verificação de Aleatoriedade.**

***Abstract*— The importance of random and pseudo-random sequences has grown exponentially due to their applications, particularly with the advent of Quantum Random Number Generators (QRNGs). To ensure the validity of these sequences, statistical tests have been created to determine how random a sequence is and, consequently, how viable it is for an application. To create an effective test suite, the National Institute of Standards and Technology (NIST) developed the 15 tests that will be implemented in this project. This work aims to implement these checks and suggest new methods for determining randomness.**

***Keywords*— Random Number Generators, NIST, QRNG, Randomness Verification Protocols.**

I. Introdução

As sequências aleatórias e pseudo-aleatórias têm-se mostrado cada vez mais importantes hoje em dia, principalmente quando se trata de assuntos como criptografia [4]. Por conta dessa importância, tem sido buscado cada vez mais métodos para obter esses números [4], podendo separá-los em três grupos: os Pseudo Random Number Generators (PRNGs), os True Random Number Generators (TRNGs) e os Quantum Random Number Generators (QRNGs), todos eles contendo suas próprias variações.

De maneira breve, os PRNGs utilizam algoritmos determinísticos, ou seja, algoritmos cuja entrada altera de maneira significativa a saída do sistema, não importando o quão ínfima seja a mudança na entrada. Pode-se tomar como exemplo desses geradores os Geradores congruentes lineares[4]. Os TRNGs, assim como o grupo anterior, se beneficiam de sistemas determinísticos, porém utilizam sistemas físicos como meio de gerar os números aleatórios, como os números que podem ser encontrados no site random.org, o qual extrai dados atmosféricos para gerar seus números. Por fim, temos os QRNGs que usam os fenômenos quânticos na geração de números aleatórios, como o dispositivo da ID Quantique [5], que faz uso de tecnologia fotônica.

Os 15 testes do National Institute of Standards and Technology (NIST) [1] (Seção II) são considerados o estado da arte. Neste projeto buscou-se implementar todos os testes do NIST, gerando códigos otimizados, confiáveis e de acesso aberto. Além disso, foi implementado um teste adicional denominado desentropia (Seção III).

Rodrigo Silva de Almeida, Instituto de Ciências Matemáticas e de Computação (ICMC), Universidade de São Paulo (USP), São Carlos(SC)-SP, e-mail: rodrigo_almeida_04@usp.br; Lucca Rodrigues Cunha, Instituto de Física, Universidade de Brasília, Brasília-DF, e-mail: lucca.cunha@aluno.unb.br; Bernardo Maia Coelho, ICMC, USP, SC-SP, e-mail: bernardomc@usp.br; Pedro Calligaris Delbem, Instituto de Física de São Carlos, USP, SC-SP, e-mail: pedrodelbem@usp.br; César Magno Leite de Oliveira Junior, Escola Politécnica de São Paulo, USP, São Paulo-SP, e-mail: cesar.magno@usp.br; Filippo Ghiglieno, Departamento de Física, Laboratório de Óptica, LASer e Fotônica, Universidade Federal de São Carlos, SC-SP, e-mail: filippo.ghiglieno@df.ufscar.br; Alexandre Delbem, ICMC, USP, SC-SP, e-mail: acbd@icmc.usp.br.

II. Sobre os testes do NIST

São os 15 testes desenvolvidos pelo NIST citados acima:

1) Teste de frequência (monobit): Analisa a proporção entre 0's e 1's e compara com o esperado em um número aleatório.
2) Teste de frequência em bloco: Semelhante ao anterior, porém realizado em "blocos" do número, verificando assim a distribuição da sequência binária.
3) Teste de subsequências constantes: Verifica o número total de subsequências constantes dentro da sequência.
4) Teste para maior sequência de um em um bloco: Verifica a maior frequência do número 1 em um bloco de tamanho determinado dentro do número fornecido.
5) Teste de classificação de matrizes disjuntas: Verifica a dependência linear entre subsequências da original.
6) Teste de transformação discreta (espectral) de fourier: Verifica se há periodicidade dentro da sequência binária que constitui o número fornecido.
7) Teste de correspondência de modelos não sobrepostos: Verifica as ocorrências de uma dada sequência não periódica. Se a sequência não é encontrada a subsequência move um bit para o lado
8) Teste de correspondência de modelos sobrepostos: Verifica se tem muitas ocorrências de uma dada sequência não periódica. Se a sequência é encontrada, a subsequência move para um bit anterior.
9) Teste de "estatística universal" de Maurer: Verifica o número de bits entre sequência de números que combinam.

10) Teste de complexidade linear: Verifica se a sequência é ou não complexa o suficiente para ser considerada aleatória.
11) Teste serial: verifica todas as possibilidades de sobreposição de tamanho pré-determinado dentro da sequência.
12) Teste de entropia aproximada: verifica a frequência de sobreposição de um bloco com os dois blocos consecutivos, comparando com o esperado em um número aleatório.
13) Teste de somas cumulativas: verifica se as somas cumulativas das sequências parciais nas sequências testadas são muito grandes ou muito pequenas quando comparadas com o que é esperado de uma sequência aleatória.
14) Teste de excursão aleatória: Verifica o número de ciclos com exatamente k visitas em uma caminhada de somas cumulativas.
15) Teste de variantes de excursões aleatórias: Verifica o número total de vezes que um determinado estado é visitado em uma caminhada de somas cumulativas aleatória.

III. Teste de desentropia de autocorrelação

O estado da arte dos geradores de números aleatórios avançou significativamente. Sob esse viés, surge a necessidade de se incrementar o número de verificações na bateria. Nesse sentido, o que se propõe no projeto é o uso da desentropia de autocorrelação conforme descrito em [2].

A desentropia de autocorrelação para valores discretos é definida em [2] como sendo:

$$D_2 = \sum_{k=1}^{N} \frac{r_k^3}{r_k + 1} \tag{1}$$

onde r_k é o k-ésimo valor para a função de autocorrelação normalizada. A autocorrelação possui sua forma para uma sequência binária $B = (b_0, ..., b_{n-1})$, onde cada elemento b_i da sequência pode assumir os valores 1 ou -1, definida em [3], que na sua forma normalizada, resulta em:

$$r_k = \frac{1}{n-k} \cdot \sum_{i=0}^{n-k-1} b_i \cdot b_{i+k} \tag{2}$$

O uso da autocorrelação apresentada na equação (2) torna o teste sensível a ciclos dentro da sequência que está sendo analisada, sendo então útil para detectar números gerados de maneira "ruim", seja pelo próprio método utilizado ou, no caso dos PRNGs, por condições iniciais mal escolhidas. Como foi ilustrado em [2] onde a desentropia de autocorrelação se mostrou capaz de distinguir geradores considerados bons de geradores considerados ruins com boa taxa de sucesso. Desse modo, a desentropia de autocorrelação se mostra ser uma ótima candidata para um "décimo sexto teste".

IV. Resultados

Com o objetivo de validar implementação elaborada, foram utilizadas três sequências, uma gerada pela função rand() da biblioteca nist.h da linguagem C, uma gerada pela função os.urandom() da biloteca os da linguagem Python e uma terceira que foi gerada usando um QRNG da ID Quantique [5], cada uma dessas sequências foi submetida aos testes 1, 5, 7 e 15 do NIST e ao teste de Desentropia.

TABELA I
Resultados dos testes selecionados de aleatoriedade para cada método de gerar a sequência.

Teste	ID Quantique	os.urand()	rand()
Test 1	true	true	true
Test 5	true	ture	true
Test 7	true	true	false
Test 15	true	true	true
Desentropia	false	false	false

Note "true" significa que a sequência passou o teste e "false" significa que não passou. Documento com resultado de todos os testes disponível em: https://drive.google.com/file/d/1HC05NxhSyBvkf7owZxOqn8AtRm-DTHpc/view?usp=drive_link

Os resultados expostos na tabela I apontam o teste de desentropia como possível adição positiva à bateria do NIST, sendo um teste mais criterioso e que pode conferir confiabilidade extra aos resultados dos outros 15 testes.

V. Conclusões

O projeto aponta o uso da desentropia de autocorrelação como fonte para uma nova medida de aleatoriedade que pode ser integrada com outros testes existentes, como os do próprio NIST, com o objetivo de conferir uma maior eficácia ao processo de validação de geradores de números aleatórios.

Agradecimentos

Os autores deste trabalho agradecem ao Centro de Inteligência Artificial (C4AI-USP), ao apoio da Fundação de Amparo à Pesquisa do Estado de São Paulo (processo FAPESP nº 2019/07665-4), à IBM Corporation, ao Centro de Ciências Matemáticas Aplicadas à Indústria (CeMEAI, processo FAPESP nº 2013/07375-0) e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Referências

[1] A. Rukhin, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, Booz-Allen and Hamilton Inc., Mclean, VA, 2001.

[2] P. Jimenez, R. Cardoso, M. G. de Queiroz, M. Abdalla, C. Marchand, X. Letartre, and F. Pavanello, *Complexity Assessment of Analog Security Primitives Using the Disentropy of Autocorrelation*, arXiv preprint arXiv:2402.17488, 2024.

[3] I. Mercer, *Autocorrelations of Random Binary Sequences*, Combinatorics, Probability & Computing, vol. 15, pp. 663–671, Sep. 2006. doi: 10.1017/S0963548306007589

[4] F. Ghiglieno, L. Roncaratti, L. R. Cunha, P. C. Delbem, R. S. de Almeida, A. M. Saraiva, e A. Delbem, "Geradores de números aleatórios: da pseudoaleatoriedade à verdadeira aleatoriedade na era da segunda revolução quântica," *Revista Brasileira de Ensino de Física*, v. 47, e20240469, 2025. DOI: 10.1590/1806-9126-RBEF-2024-0469. Disponível em: https://doi.org/10.1590/1806-9126-RBEF-2024-0469. Acesso em: 20 ago. 2025.

[5] ID QUANTIQUE. *Quantis Quantum Random Number Generator (QRNG) Overview*. Disponível em: https://www.idquantique.com/random-number-generation/overview/. Acesso em: 20 ago. 2025.