TESTE DE ALEATORIEDADE

TARTAGLIA, Gustavo; MARQUES, Maxsuel; BAIA, Joas Weslei

CENTRO UNIVERSITÁRIO GOVERNADOR OZANAM COELHO

Ciência da Computação

UNIFAGOC
CENTRO UNIVERSITÁRIO GOVERNADOR OZANAM COELHO

INTRODUÇÃO

No mundo de hoje a criptografia está presente em todos os lugares; desde a comunicação militar até conversas em aplicativos de mensagens, todos precisam de saber que suas informações não podem ser acessadas com facilidade. Um dos elementos mais importantes da criptografia são as chaves utilizadas, que podem ser formadas a partir de dados aleatórios para evitar que sejam descobertas. Porém, os computadores geram números pseudoaleatórios.

A universidade nacional da Australia em Canberra encontrou como solução a utilização da física quântica para resolver esse problema. A teoria diz que as flutuações quânticas no vácuo tem valores aleatórios, logo, ao medir esses valores em tempo real é possível obter valores que, teoricamente, seriam verdadeiramente randomizados.

OBJETIVO

Neste projeto foram aplicados testes de aleatoriedade com o objetivo de verificar o processo de geração de números aleatórios, ou seja, testar se os resultados fornecidos pelo servidor australiano realmente atingem níveis de aleatoriedade satisfatórios.

Para obter esses resultados criou-se um programa que fosse capaz de realizar testes e apresentar ao usuário os resultados. Para isso, utilizou-se os testes de Chi-Quadrado e Kolmogorov-Smirnov.

MATERIAIS E MÉTODOS

TESTE QUI-QUADRADO

O teste do Qui-Quadrado (também chamado de teste Chi-Quadrado) é um teste estatístico com o objetivo de avaliar qualquer discrepância que ocorra aos dados apresentados. Após o cálculo apresentado na expressão, o resultado é comparado ao da tabela de distribuição esperada para descobrir a probabilidade da amostra não ter sido gerada aleatoriamente. Para o cálculo, foi utilizada a seguinte função:

$$\sum_{k=1}^{n} \frac{(o_i - e_i)^2}{e_i} < \chi^2_{[1-\alpha;k-1]}$$

onde $\mathbf{e}_i$ é a frequência esperada e $\mathbf{O}_i$ é a frequência observada.

TESTE KOLMOGOROV-SMIRNOV

O teste Kolmogorov-Smirnov (conhecido como teste KS ou teste K-S) é aplicado com a mesma intenção do Chi-Quadrado, mas o mesmo é baseado na comparação das probabilidades acumuladas das duas distribuições, isto é, observada e teórica.

Para o cálculo do valor crítico, é utilizado a seguinte equação:

$$VC = \frac{1,36}{\sqrt{n}}$$

Onde **n** é a quantidade de números aleatórios testados. Se o valor encontrado pela equação for maior que o valor da maior diferença, então a distribuição é uniforme. Indicando que todos os valores gerados tem a mesma chance de serem gerados pelo servidor de números aleatórios.

RESULTADOS

O teste de Chi-Quadrado revelou que a média dos resultados obtidos foram de 260,559 que, ao ser verificada na tabela gerada pelo site AtoZMath, mostrou que as chances de que a amostra não seja aleatória são de apenas 0,3752, demonstrando resultado satisfatório.

Chi square Distribution

Degree of freedom =	254
p-value = 0.3752 Or χ^2 value =	260.559

p-value type : right tail

Find

Answer :

If p-value = 0.3752 then χ^2-value=260.5602

Logo após a avaliação do teste de Kolmogorov-Smirnov, chegamos a conclusão que o algoritmo está próximo da uniformidade, visto que o valor critico mínimo calculado foi de 0,12 e, o valor máximo calculado do valor critico é de 0,14.

CONCLUSÃO

Após a execução do projeto, fomos capazes de perceber que os números fornecidos conseguiram demonstrar valores satisfatórios em ambos os testes utilizados. Apesar da necessidade de se aplicar mais testes para confirmar a aleatoriedade do gerador, esse projeto possibilitou nosso aprendizado nos testes estatísticos e dos modelos matemáticos gerados.

REFERÊNCIAS

QRNG. Disponível em <https://qrng.anu.edu.au>. Acesso em 03 de mar de 2021.

Teste Qui-Quadrado. Disponível em <shorturl.at/vCU23>. Acesso em 10 de mar. de 2021.

Teste Qui-Quadrado. Disponível em <shorturl.at/dsLTY>. Acesso em 17 de mar. de 2021.

AtoZMath. Disponível em <shorturl.at/gAQ35>. Acesso em 24 de mar. de 2021.