REVISTA DA sbfoton
Vol. 2 - Mar/2023

Aleatoriedade quântica e sua aplicação em geração de números verdadeiramente aleatórios

Muriel A. de Souza e Luiz Vicente Gomes Tarelho
Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)

RESUMO: *A geração de números verdadeiramente aleatórios é algo que tem se tornado cada dia mais importante. Experimentos que utilizam física quântica têm sido largamente utilizados para essa finalidade, devido à sua aleatoriedade intrínseca. O presente artigo faz uma comparação entre a física clássica e a física quântica quanto às suas imprevisibilidades, fornece uma explicação sobre superposição de estados quânticos e comenta a utilização desse "colapso" na função de onda para a geração de números aleatórios, uma das formas utilizadas para a geração de números aleatórios quânticos.*

ABSTRACT: *The true generation of random numbers is something that has become increasingly most important day. Experiments that use quantum physics have been widely used for this purpose, due to its intrinsic randomness. THE This article makes a comparison between classical physics and quantum physics in terms of its unpredictability, providing a explanation about superposition of states quantum and comments on the use of this in the wave function "collapse" for generation of random numbers, one of the ways used to generate quantum random numbers.*

http://doi.org/10.5281/zenodo.14890174

INTRODUÇÃO

Em nosso cotidiano, muitas coisas são atribuídas ao acaso e, por isso, são chamadas de aleatórias. A aleatoriedade tem diversas aplicações que vão desde jogos como loteria, cartas de baralho, cassinos, até simulações de Monte Carlo, modelagem de sistemas complexos, como na meteorologia, e chaves criptográficas. Números aleatórios são usados diariamente em inúmeras atividades, como em *CAPTCHAs* antes de *login*, ou quando são geradas senhas únicas para liberar o uso de determinado aparelho, por exemplo. Um número é considerado aleatório quando, se extraído de um conjunto de números possíveis, todos os números deste conjunto têm a mesma probabilidade de serem selecionados [1]. Ou seja, os números devem obedecer ao princípio da uniformidade e independência, o que significa que todos os valores devem ser equiprováveis e não correlacionados [2]. Todos os mecanismos de segurança em informática, desde a criptografia, senhas de acesso, segurança de transações bancárias pela internet, etc., dependem da geração de números aleatórios. O grande problema está em como gerar números que sejam realmente aleatórios. Na prática, é usual a utilização de números chamados “pseudoaleatórios”, que se aproximam de um número realmente aleatório, mas possuem vulnerabilidades no processo de produção. Ou seja, se um hacker obtiver informação suficiente e repetir o mesmo processo, poderá encontrar esse número “aleatório” [3], quebrando a segurança do processo. Em um computador, por exemplo, é impossível gerar algo que seja completamente imprevisível, por ser um dispositivo determinístico. Por isso, recorre-se ao mundo físico para realizar medições que se comportam aleatoriamente e, com isso, possam gerar números aleatórios. Mas, quais são os processos físicos verdadeiramente aleatórios? E é esse assunto que o presente artigo mostra: como utilizar a física para a geração de números verdadeiramente aleatórios.

FÍSICA CLÁSSICA X FÍSICA QUÂNTICA

Quando se trabalha com medições no contexto da física clássica, entende-se que certa propriedade da natureza possui um valor numérico. Por esse motivo ela é considerada realista e determinística: porque acredita que as partículas por si só possuem características bem definidas e seus processos podem ser calculados e

previstos através de suas condições iniciais. A imprevisibilidade encontrada em sistemas clássicos complexos de muitos corpos interagindo, por exemplo, implica em indeterminismo, mas não implica em aleatoriedade, porque as quantidades mensuráveis podem ser determinadas classicamente a cada momento utilizando medições apropriadas, maiores resoluções, ajuda de computadores etc. O surgimento da mecânica quântica revolucionou a física no início do século passado e foi desenvolvida para calcular e demonstrar fenômenos que não tinham explicação na visão da física clássica. O seu desenvolvimento provocou uma quebra de paradigma ao não contemplar o realismo e o determinismo, pois na mecânica quântica não se pode afirmar o estado de um sistema sem antes realizar uma medição sobre ele. Quando se realiza uma medição o resultado é totalmente imprevisível, porque as propriedades dos objetos são incertas e só podem ser descritas probabilisticamente por uma função de onda. Para entender melhor esses argumentos, é necessário entender sobre superposição de estados.

SUPERPOSIÇÃO DE ESTADOS

Superposição, matematicamente falando, refere-se a uma combinação linear de inúmeros estados simultâneos. Para explicar essa superposição, seu caráter quântico e aleatoriedade, imagine um sistema composto por setas. Você preparou esse sistema com todas as setas apontando para a direita. Se você perguntar para o sistema se as setas estão para a direita ou para a esquerda, sua resposta será 100% para a direita. Porém, se você perguntar para cada seta se ela é para cima ou para baixo, sua resposta será 50% para cima e 50% para baixo (figura 1). Isso porque setas apontadas para a direita podem ser descritas como uma superposição de ‘para cima’ e ‘para baixo’ [4]. 14 Agora você prepara outro estado com as respostas obtidas anteriormente, em que metade das setas apontam para cima e metade das setas apontam para baixo. Se você refizer a pergunta, você terá o mesmo resultado do sistema anterior: 50% ‘para cima’ e 50% ‘para baixo’ (figura 2). Ou seja, para dois sistemas diferentes, tem-se o mesmo resultado [4].

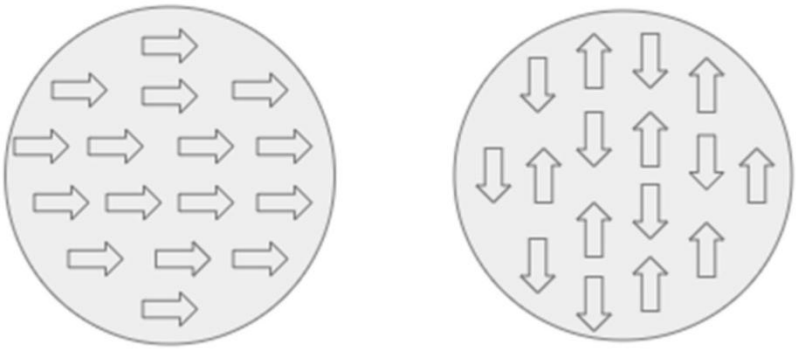

Figura 1 – Esquerda: sistema inicial, 100% das setas para a direita; direita: sistema após ser interrogado, com 50% das setas ‘para cima’ e 50% das setas ‘para baixo’.

Porém, o que difere esses sistemas? O segundo caso pode ser pensado de acordo com o realismo da física clássica: o sistema desde o início possui determinada característica que independe do observador. Uma medição apenas revela informações desse objeto, mas não altera o sistema. O mesmo não acontece no primeiro caso, em que as setas não estão ‘para cima’ ou ‘para baixo’, mas em uma superposição desses dois estados. E, ao realizar a medição, houve alteração no sistema. Isso é o que acontece na mecânica quântica. Quando você tem uma superposição de estados, você não consegue ter um resultado determinístico, o que você tem são funções de probabilidade que descrevem o estado. Houve o acréscimo de um sujeito, o observador, que, ao realizar a medição, provoca uma perturbação no sistema, o chamado “colapso da função de onda”. No caso do exemplo acima, a medição seria a resposta à pergunta. No sistema de setas para a direita, ao perguntar se elas estavam ‘para cima’ ou ‘para baixo’, a resposta foi uma ou outra. Essa superposição deixou de existir. Fisicamente falando, na quântica não se tem um único estado, mas sim uma função de onda de muitos autoestados e, ao realizar a medição, ela provoca um “colapso” nessa função de onda, pois os muitos autoestados se desdobram em um único autoestado específico relacionado a essa medição. Ou seja, tem-se uma perturbação provocada pelo observador no sistema que está sendo observado.

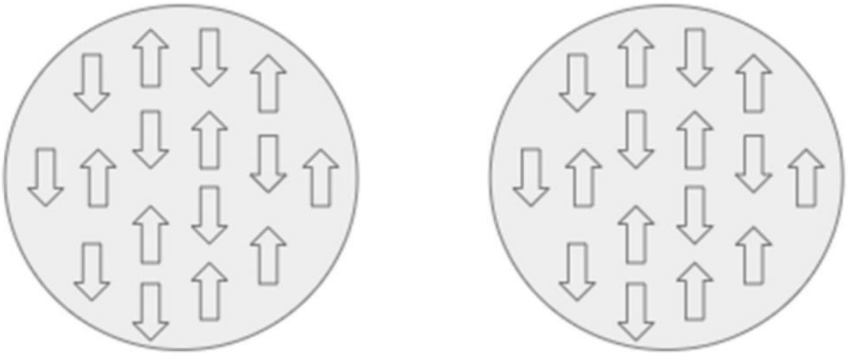

Figura 2 – Esquerda: sistema inicial, com 50% das setas ‘para cima’ e 50% das setas ‘para baixo’; direita: sistema após ser interrogado, igual ao sistema inicial.

UTILIZANDO A SUPERPOSIÇÃO QUÂNTICA PARA A GERAÇÃO DE NÚMEROS ALEATÓRIOS QUÂNTICOS

Uma vez que a mecânica quântica é intrinsecamente aleatória, ela tem sido amplamente estudada para a geração de números verdadeiramente aleatórios. Já existem diversos geradores de números aleatórios quânticos (QRNG) implementados, e os sistemas que utilizam fótons têm vantagem na geração de bits aleatórios devido à existência de inúmeros componentes ópticos de alta qualidade e fácil manuseio [5]. Basicamente um QRNG inclui uma fonte de entropia para gerar estados quânticos bem definidos e um sistema de medição correspondente [6]. Uma forma bastante utilizada para produzir QRNG ópticos é utilizando um sistema quântico em superposição dos estados básicos, em que, após a medição, o sistema colapsaria para um dos estados básicos [6]. Isso pode ser feito através da medição de um fóton que pode estar em superposição de estados de polarização ou de caminho. Em computação, esse fóton em estado de superposição é chamado de *qubit*, que corresponde a uma superposição das bases computacionais { $|0\rangle$, $|1\rangle$}. Um *qubit* é a base da computação quântica: enquanto um bit na computação clássica corresponde a 0 ou 1, um *qubit* é uma superposição desses valores. A medição de um *qubit* produzirá um dos dois estados possíveis, ou seja, cada medição irá gerar um bit aleatório.

CONCLUSÃO

Uma vez que a mecânica quântica é intrinsecamente aleatória, ela pode ser utilizada para geração de números aleatórios, conhecidos como números verdadeiramente aleatórios, que têm se tornado cruciais com o advento da computação quântica, pois a criptografia, toda a segurança de transações bancárias pela internet etc., dependem da geração desses números. Diversos experimentos têm sido desenvolvidos utilizando a mecânica quântica para tal e nesse artigo é destacado o uso da superposição. Estados em superposição quântica são representados por uma função de onda de autoestados e que, ao realizar uma medição, se desdobra em um único autoestado específico e aleatório. Esse é um dos princípios que pode ser utilizado para gerar números aleatórios, em que os estados superpostos são *qubits*, que são superposições das bases computacionais {$|0\rangle$, $|1\rangle$}, e que, ao serem medidos, irão colapsar em $|0\rangle$ ou $|1\rangle$, gerando assim, sequências de bits aleatórios.

REFERÊNCIAS

[1] [1] GUIDE, S., HAAHR, M., & CHAITIN, G. J. (s.d.). RANDOM.ORG - Introduction to Randomness and Random Numbers. https://www.random.org/randomness/

[2] *MANNALATH, V., MISHRA, S., & PATHAK, A. (outubro de 2022). A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness. https://doi.org/10.48550/arXiv.2203.00261*

[3] *PIRONIO, S., ACÍN, A., & MASSAR, S. (2010). Random numbers certified by Bell's theorem. Nature, 464, 1021–1024. https://doi.org/10.1038/nature09008*

[4] *GERSHIN, T. Quantum Computing: you know it's cool, now find out how it works IBM ResearchBlog https://www.ibm.com/blogs/research/2017/09/qc-how-it-works/?mhsrc=ibmsearch_a&mhq=superposition*

[5] *MA, X., YUAN, X., CAO, Z. et al. Quantum random number generation. npj Quantum Inf 2, 16021 (2016). https://doi.org/10.1038/npjqi.2016.21*

[6] *MANNALATH, V., MISHRA, S., & PATHAK, A. A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness. https://doi.org/10.48550/arXiv.2203.00261*