Contemporânea
Contemporary Journal
Vol. 4 N°. 7: p. 01-18, 2024
ISSN: 2447-0961

Artigo

ALGORITMO DE SHOR

SHOR'S ALGORITHM

ALGORITMO DE SHOR

DOI: 10.56083/RCV4N7-034
Receipt of originals: 06/04/2024
Acceptance for publication: 06/24/2024

Marcelo Gabriel Batista
Graduando em Engenharia Mecânica
Instituição: Universidade Tecnológica Federal do Paraná
Endereço: Guarapuava, Paraná, Brasil
E-mail: marcelobatista@alunos.utfpr.edu.br

Antonio Carlos Amaro de Faria Junior
Doutor em Física
Instituição: Universidade Tecnológica Federal do Paraná
Endereço: Guarapuava, Paraná, Brasil
E-mail: antonioc@utfpr.edu.br

RESUMO: Este artigo explora a intersecção fascinante entre a mecânica quântica e a computação, dois campos aparentemente distintos que se entrelaçam em uma simbiose surpreendente. Ao destacar os princípios fundamentais da mecânica quântica, como superposição e emaranhamento, este estudo lança luz sobre sua aplicação inovadora na computação quântica. Em particular, focamos no algoritmo Shor, uma conquista marcante neste campo emergente. O algoritmo Shor demonstra a capacidade única da computação quântica de resolver rapidamente problemas que seriam intratáveis para computadores clássicos. Exploramos como o algoritmo utiliza os princípios quânticos de superposição e emaranhamento para fatorar números inteiros em seus primos constituintes com eficiência exponencialmente superior aos métodos clássicos. Além disso, discutimos as implicações profundas desse avanço, desde a criptografia até a modelagem de sistemas complexos. Ao destacar o potencial revolucionário da computação quântica, este artigo lança luz sobre o futuro promissor de uma nova era de computação, onde os limites tradicionais são desafiados e novas fronteiras são abertas.

PALAVRAS-CHAVE: mecânica quântica, computação quântica, superposição, emaranhamento, Algoritmo de Shor.

ABSTRACT: This article explores the fascinating intersection between quantum mechanics and computing, two seemingly distinct fields that intertwine in a surprising symbiosis. By highlighting the fundamental principles of quantum mechanics such as superposition and entanglement, this study sheds light on their innovative application in quantum computing. In particular, we focus on Shor's algorithm, a landmark achievement in this emerging field. Shor's algorithm demonstrates the unique capability of quantum computing to solve problems that would be intractable for classical computers efficiently. We explore how the algorithm leverages quantum principles of superposition and entanglement to factor integers into their prime constituents exponentially faster than classical methods. Furthermore, we discuss the profound implications of this breakthrough, from cryptography to modeling complex systems. By highlighting the revolutionary potential of quantum computing, this article illuminates the promising future of a new era of computation where traditional boundaries are challenged and new frontiers are opened.

KEYWORDS: quantum mechanics, quantum computing, superposition, Shor´s Algorithm.

RESUMEN: Este artículo explora la fascinante intersección entre la mecánica cuántica y la computación, dos campos aparentemente distintos que se entrelazan en una simbiosis sorprendente. Al resaltar los principios fundamentales de la mecánica cuántica, como la superposición y el entrelazamiento, este estudio arroja luz sobre su aplicación innovadora en la computación cuántica. En particular, nos centramos en el algoritmo de Shor, un hito en este campo emergente. El algoritmo de Shor demuestra la capacidad única de la computación cuántica para resolver eficientemente problemas que serían intratables para las computadoras clásicas. Exploramos cómo el algoritmo aprovecha los principios cuánticos de superposición y entrelazamiento para factorizar números enteros en sus constituyentes primos de manera exponencialmente más rápida que los métodos clásicos. Además, discutimos las profundas implicaciones de este avance, desde la criptografía hasta la modelización de sistemas complejos. Al resaltar el potencial revolucionario de la computación cuántica, este artículo ilumina el prometedor futuro de una nueva era de computación donde se desafían los límites tradicionales y se abren nuevas fronteras.

PALABRAS CLAVE: mecánica cuántica, computación cuántica, superposición, enredo, algoritm o de shor.

1. Introdução

Em 1900, a física experimentou uma revolução transformadora, com a mecânica quântica emergindo, possibilitou-se a explicação de diversos fenômenos e redefiniu-se toda a nossa compreensão do universo em escala microscópica. Esta nova vertente da física não apenas desvendou enigmas existentes, mas também abriu portas para inúmeras aplicações tecnológicas, sendo a mais proeminente até o momento a computação quântica.

A computação quântica se distancia significativamente do modelo convencional, incorporando princípios únicos da mecânica quântica, tais como superposição, emaranhamento e uma natureza probabilística intrínseca.

Esta nova era da computação não apenas representa uma mudança paradigmática, mas também promete redefinir os limites da capacidade computacional, desbravando fronteiras anteriormente inexploradas e desafiando as concepções convencionais de processamento de informações. Neste artigo, mergulharemos a fundo na cativante interseção entre a mecânica quântica e a computação, revelando as implicações e promessas que essa fusão oferece ao avanço tecnológico. Além disso, exploraremos de forma prática os princípios da computação quântica, destacando a sua aplicação notável por meio do algoritmo de Shor. Este algoritmo, conhecido por sua capacidade de fatorar números inteiros de forma eficiente em um contexto quântico, servirá como uma ilustração concreta das potencialidades revolucionárias que a computação quântica proporciona à solução de problemas complexos.

2. Superposição e Qubits

Uma maneira acessível de compreender a superposição quântica é por meio do exercício mental proposto por Erwin Schrödinger em 1935. Imagine um gato trancado em uma caixa com um frasco de veneno que pode ou não se romper. Enquanto não observamos o gato, ele está em um estado de superposição entre estar vivo e morto:

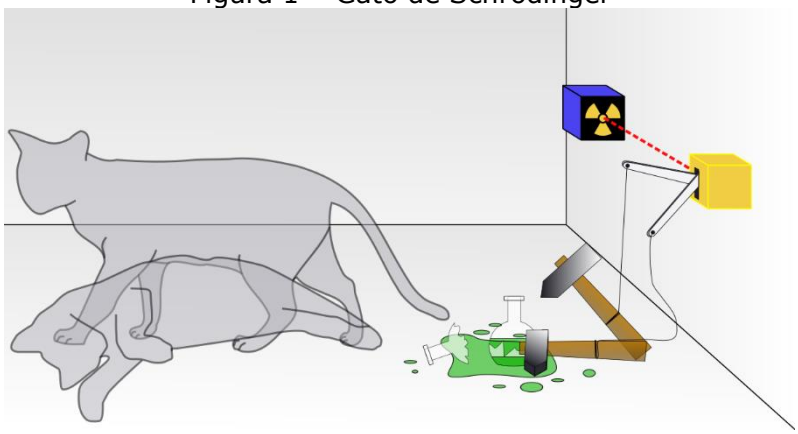
$$|\Psi\rangle = \alpha|Vivo\rangle + \beta|Morto\rangle \quad (1)$$

Ao abrirmos a caixa, realizamos a medição, e a expressão que estava em superposição colapsa então para um resultado mensurável, ou o gato está vivo, ou está morto.

Neste caso alpha e beta são números complexos que dizem a probabilidade do estado que está relacionado, deve-se obedecer a seguinte relação:

$$|a|^2 + |b|^2 = 1 \quad (2)$$

Figura 1 – Gato de Schrödinger



Fonte: O Gato de Schrödinger. Ilustração. 2015. Disponível em:https://roberto-furnari.blogspot.com/2015/02/para-fundir-cuca-gato-de-schrodinger.html. Acesso em: 05/04/2024.

A partir desse conceito de superposição, surge o conceito de qubit. Analogamente aos bits na computação clássica, que possuem estados bem definidos (zero ou um), os qubits são uma superposição de zeros e uns:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (3)$$

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (4)$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (5)$$

Apenas depois da medição saberemos seu estado (zero ou um).

3. Paradoxo EPR, Desigualdade de Bell e Emaranhamento

Refiro-me ao emaranhamento como uma propriedade intrínseca do domínio quântico, caracterizada pela interdependência direta entre o estado de duas partículas. Por exemplo, se dois fótons estiverem emaranhados e modificarmos o spin de um deles, o estado do outro será alterado, mesmo que estejam separados por grandes distâncias.

Essa peculiaridade desafia nossa intuição e, à primeira vista, suscita dúvidas sobre sua real possibilidade. No entanto, não estamos sozinhos em questionar essa propriedade. Em 1935, Albert Einstein, Boris Podolsky e Nathan Rosen publicaram um artigo que deu origem ao termo paradoxo EPR.

Considerando o exemplo do emaranhamento entre dois fótons, imaginemos que um deles está na Terra e o outro em outra galáxia. Ao alterarmos o spin de um fóton, o outro é modificado instantaneamente, sugerindo uma transmissão de informação mais rápida que a velocidade da luz. Diante disso, EPR postulou duas hipóteses: ou a mecânica quântica é não local, ou é uma teoria incompleta, com variáveis ocultas.

Somente em 1964, John Bell desenvolveu a expressão conhecida como desigualdade de Bell, proporcionando uma resposta sobre a verdadeira natureza da mecânica quântica. Se essa desigualdade for violada, é uma confirmação de que não existem variáveis ocultas, demonstrando que a mecânica quântica é verdadeiramente não local. Em 1980, Alain Aspect realizou experimentos que confirmaram a possibilidade do emaranhamento, validando as implicações teóricas de Bell.

Essa propriedade intrigante, que desempenha um papel significativo no universo microscópico, suscita considerável interesse desde sua descoberta. Pesquisadores têm buscado aplicações práticas para impulsionar avanços tecnológicos, sendo a computação quântica uma área destacada que se beneficia diretamente do emaranhamento entre qubits.

Para provar a existência do emaranhamento entre qubits, começamos escrevendo um sistema com dois qubits:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \quad (6)$$

Mantendo a condição de normalização:

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \quad (7)$$

Para analisar um possível emaranhamento entre os qubits, utilizamos o produto tensorial:

$$|\psi\rangle = |\psi 1\rangle \otimes |\psi 2\rangle \quad (8)$$

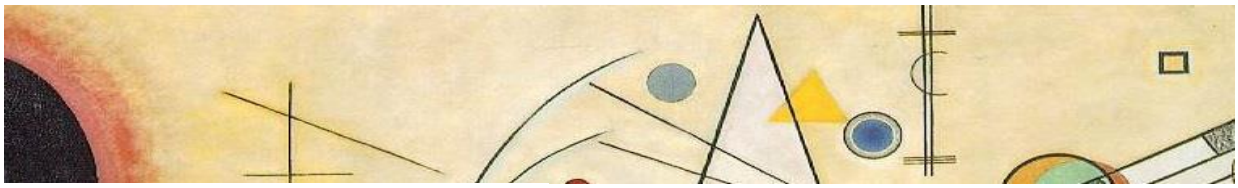
Vamos considerar um caso para entender matematicamenteo emaranhamento, chamaremos $|\psi\rangle$ de:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (9)$$

Nos parece aleatório escolher este $|\psi\rangle$, mas é uma espressão conhecida de emaranhamento. Podemos escrevê-lo como:

$$(\alpha|0\rangle + \beta|1\rangle)\otimes(\gamma|0\rangle + \delta|1\rangle) \quad (10)$$

Resultando em:



$$\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \quad (11)$$

Portanto:

$$\begin{cases} \alpha\gamma = 0 \\ \beta\delta = 0 \\ \alpha\delta = \frac{1}{\sqrt{2}} \\ \beta\gamma = \frac{-1}{\sqrt{2}} \end{cases} \quad (12)$$

O que não é possível pois para αγ = 0, α ou γ devem ser iguais a zero, o que de cara impossibilita a terceira ou quarta equação do sistema.

Quando isso ocorre, dizemos que os dois vetores do sistema não são decomponíveis, ou seja, estão emaranhados. O emaranhamento entre os qubits traz aplicações que melhoram a eficiência de algoritmos que utilizam qubits em relação à computação convencional, aplicaremos neste artigo com o algoritmo de Shor, que tem por finalidade a decodificação de chaves baseadas em fatoração de grandes números inteiros.

4. Codificação e Decodificação

Ao lidar com a transmissão de mensagens privadas, surge a preocupação com interceptações por parte de espiões. Uma estratégia inteligente para preservar a confidencialidade consiste em codificar a mensagem usando uma chave compartilhada entre remetente e destinatário. Dessa forma, mesmo que um espião obtenha a mensagem codificada, a informação confidencial permanece segura. A figura abaixo ilustra o processo de decodificação, onde o destinatário, ao possuir a chave, pode decifrar e compreender a mensagem.

Atualmente, a segurança na codificação baseada na fatoração de grandes números inteiros é amplamente adotada. Esse método é altamente seguro, pois a fatoração de grandes números é uma tarefa árdua e demorada, mesmo com o auxílio de ferramentas computacionais. No entanto, a computação quântica oferece uma abordagem que melhora exponencialmente o tempo de decodificação. Em vez de testar números individualmente, a computação quântica utiliza o algoritmo de Shor, explorando a superposição para identificar eficientemente os fatores do grande número inteiro.

5. O Algoritmo de Shor

O algoritmo de Shor opera da seguinte maneira: para encontrar os dois números (p e q) cuja multiplicação resulta no grande número inteiro (N), aplicamos a expressão:

$$N = p.q \quad (13)$$

$$N = MDC(p, N) \,.\, MDC(q, N) \quad (14)$$

$$N = MDC(a^{r/2} - 1, N) \,.\, MDC(a^{r/2} + 1, N) \quad (15)$$

$$p = a^{r/2} - 1 \quad (16)$$

$$q = a^{r/2} + 1 \quad (17)$$

$$a^r \equiv 1 \; mod \; N \qquad (18)$$

Onde MDC é o máximo divisor comum, a é um número aleatório escolhido, e r é o período da função modular relacionada à periodicidade em relação ao nosso número que desejamos fatorar.

$$f(x) = a^x \; mod \; N \qquad (19)$$

O algoritmo parece simples, e realmente se tivermos os dados corretos as operações não passam de matemática básica, porém o grande desafio é obter o período r da função modular. Manualmente por métodos computacionais clássicos é uma tarefa árdua e demorada, por isso é uma ótima escolha utilizar um algoritmo quântico para encontrar o período da função modular.

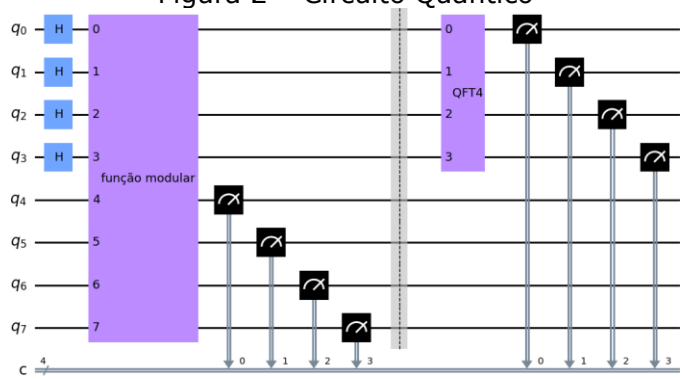
6. O Algoritmo Quântico de Shor

Para implementar a parte quântica do algoritmo de Shor a quantidade de qubits necessários para o circuito quântico é determinada pela relação:

$$N = 2^n \qquad (20)$$

Onde N é o número que desejamos fatorar e n é a quantidade de qubits. O circuito quântico do algoritmo de Shor com quatro qubits é representado da seguinte forma:

Figura 2 – Circuito Quântico



Fonte: Autoria Própria.

No início, colocamos n qubits em superposição e outros n qubits auxiliares. Essa superposição é crucial, pois permite realizar simultaneamente o processo em todos os qubits, melhorando a eficiência em comparação com métodos convencionais.

Em seguida, aplicamos a função modular a todos os qubits, armazenando nos qubits em superposição os valores relevantes, enquanto os qubits auxiliares registram valores intermediários de f(x).

Por fim, aplicamos a Transformada Quântica de Fourier (QFT) nos quatro primeiros qubits, refletindo os possíveis períodos da função. A forma genérica da QFT é:

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=1}^{N-1} e^{2\pi i \frac{XY}{N}} |y\rangle \qquad (21)$$

Fazendo algumas manipulações podemos chegar em:

$$|x\rangle = (|0\rangle + e^{2\pi i \frac{X}{2}}|1\rangle) \otimes (|0\rangle + e^{2\pi i \frac{X}{2^2}}|1\rangle) \otimes \ldots \otimes (|0\rangle + e^{2\pi i \frac{X}{2^N}}|1\rangle) \qquad (22)$$

Com essa notação já podemos pensar em como fazer uma porta QFT. Precisamos de uma função que:

$$U(\alpha)|0\rangle \rightarrow |0\rangle \quad (23)$$

$$U(\alpha)|1\rangle \rightarrow e^{ia}|1\rangle \quad (24)$$

Há uma relação que diz que:

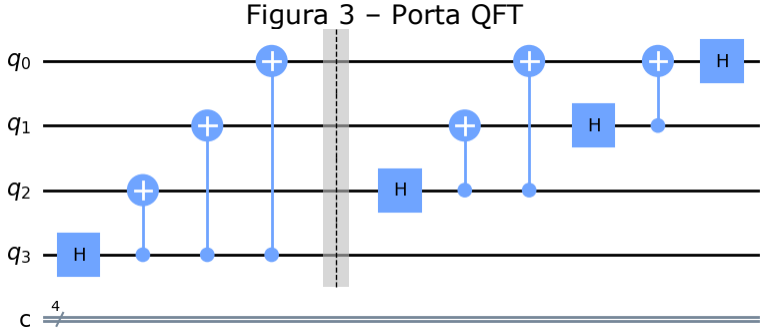
$$H|X_K\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i X_K}|1\rangle) \quad (25)$$

Se aplicarmos H em X_3 no último termo da equação obteremos uma porta H em X^3. Podemos escrever X no último termo como:

$$e^{2\pi i \frac{X_2}{4}} = e^{\frac{\pi}{2} X_2 i} \quad (26)$$

Aplicando em todos os termos adquirimos a porta QFT como:

Figura 3 – Porta QFT



Fonte: Autoria Própria.

Assim podemos realizar as medições, aplicando o MDC aos resultados obtidos encontramos o período r.

7. Aplicação em Qiskit

Para entendermos melhor o conceito, vamos criar um código em qiskit para fatorar o número 15 utilizando o algoritmo de Shor. Começando o código em qiskit, primeiramente importamos todas as bibliotecas necessárias:

```
from qiskit import *
from qiskit.visualization import plot_histogram
from math import pi
```

Agora precisamos criar as portas da função modular e a transformada quântica de Fourier (QFT):

```
def f():

circuit = QuantumCircuit(8)
circuit.x(4)
circuit.cx(0,5)
circuit.cx(0,6)
circuit.cx(1,4)
circuit.cx(1,6)
for i in range(4,8):
circuit.ccx(0,1,i)
porta = circuit.to_gate()
porta.name = "função modular"
return porta

def QFT(n):
qft_circuit = QuantumCircuit(n)
```

```
for i in range(n-1, -1, -1):
qft_circuit.h(i)
for j in range(i - 1, -1, -1):
qft_circuit.cp(pi/(2 ** (i - j)), j, i)

for i in range(n // 2):
qft_circuit.swap(i, n - i - 1)
porta = qft_circuit.to_gate()
porta.name = "QFT" + str(n)
return porta
```

Com as portas criadas montamos o circuito (imagem 7), seguindo o passo a passo instruído na seção anterior.

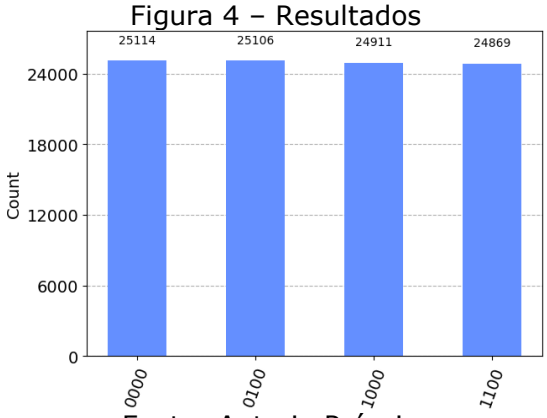
-Deixamos q0 a q4 em superposição
-Aplicamos a função modular em todos os qubits
-Aplicamos a QFT de q0 a q4
-Realizamos a medição

```
circuit = QuantumCircuit(8,4)
circuit.h(range(4))
circuit.append(f(), range(8))
circuit.measure(range(4,8),range(4))
circuit.barrier(range(8))
circuit.append(QFT(4), range(4))
circuit.measure(range(4), range(4))
circuit.draw(output = 'mpl')
```

Para verificar os resultados:

```
backend = Aer.get_backend("qasm_simulator")
job = execute(circuit, backend, shots = 100000)
result = job.result()
counts = result.get_counts()
plot_histogram(counts)
```

Figura 4 – Resultados



Fonte: Autoria Própria.

Percebemos que as probabilidades são: 0100, 1000 e 1100, que em binário representam os números: 4, 8 e 12. Fazendo o MDC obtemos r = 4. Sabendo disso:

```
import math
p = math.gcd(4-1, 15)
q = math.gcd(4+1, 15) print("p =", p)
print("q =", q)
```

Dessa forma obtemos os resultados: p=3 e q=5.

Certamente, a abordagem para fatorar o número 15 pode parecer trivial à primeira vista, no entanto, ela serve como uma introdução simples à implementação da parte quântica do algoritmo de Shor. Através desse exemplo, torna-se evidente que é viável fatorar números inteiros por meio

da programação quântica. Além disso, ao seguir a mesma lógica, podemos estender essa capacidade para fatorar números muito maiores, requerendo apenas um aumento no número de qubit. A promessa de maior eficiência em comparação com computadores convencionais é inegável.

Esse exemplo é apenas uma entre as diversas aplicações da computação quântica. O potencial se estende tanto para aplicações em desenvolvimento quanto para aquelas que ainda estão por surgir, todas fundamentadas em métodos quânticos.

A exploração contínua dessas possibilidades certamente abrirá portas para avanços significativos em diversas áreas, alimentando o progresso da computação quântica.

8. Conclusão

Diante da intrincada interseção entre a mecânica quântica e a computação, a codificação e decodificação de informações por meio da fatoração de grandes números inteiros assume papel crucial. Esse método, embora seguro, enfrenta limitações temporais significativas quando aplicado à computação convencional. A introdução da computação quântica, evidenciada pelo algoritmo de Shor, oferece uma perspectiva revolucionária ao apresentar uma abordagem eficiente para a fatoração de números inteiros em um contexto quântico.

No cenário prático, a implementação do algoritmo de Shor com o Qiskit destaca a promissora capacidade da computação quântica em resolver desafios computacionais complexos de forma expedita. Conforme exploramos os limites da capacidade computacional, a computação quântica surge como uma ferramenta poderosa, promovendo avanços tecnológicos que transcendem as fronteiras convencionais da computação clássica.

Em síntese, a convergência entre mecânica quântica e computação abre novos horizontes e desafia concepções tradicionais, sinalizando uma era empolgante de inovação tecnológica e descobertas científicas.

Referências

AMARAL, Bárbara. Informação Quântica. YouTube. Disponível em: https://www.youtube.com/watch?v=_G4hBwbtTDA&list=PLbgl7cwByXU57o-eDjpa55G8q7dQqDazP. Acesso em: 12/01/2024.

GRIFFITHS, David J. Introdução à mecânica quântica. 2. ed. New Jersey: Prentice Hall, 2011.

KET.G. Algoritmo de Shor. YouTube. Disponível em: https://www.youtube.com/playlist?list=PLXba1eqsWDsTbUvXfsKx4CpOqKbBPa5Xp. Acesso em: 04/02/2024.

MARTINS, R. C. O algoritmo de Fatoração de Shor. Dissertação (Mestrado) - PUC Rio de Janeiro, 2018.

MORKROSS, B. J. Não Localidade na Mecânica Quântica. Revista Brasileira de Ensino de Física, Rio de Janeiro, v. 19, n. 1, p. 16, 1997.

NUSSENZVEIG, Moyses. Curso de Física Básica. 8. ed. São Paulo: Blucher, 1998. v. 4.

RIGOLIN, G. Emaranhamento Quântico. Revista Physicæ, São Paulo, v. 1, p. 1-7, 2008.

SILVA, W. Uma Introdução à Computação Quântica. Trabalho de Conclusão de Curso, Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2018.