

UNIVERSIDADE FEDERAL DE SÃO CARLOS — *CAMPUS* SOROCABA
CENTRO DE CIÊNCIAS E TECNOLOGIAS PARA A SUSTENTABILIDADE
DEPARTAMENTO DE FÍSICA, QUÍMICA E MATEMÁTICA

Bianca Miyabe Santos Freitas

Simulação de Circuitos Quânticos para o estudo de ruídos no fenômeno de teletransporte quântico

Sorocaba
Abril, 2022

Resumo

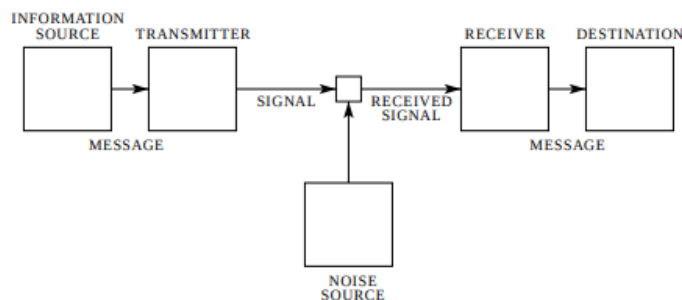
Abstract

1 Introdução

Segundo Capurro e Hjørland (2007), o conceito de informação cotidianamente possui seu significado atribuído como *conhecimento comunicado*. Nesse sentido, a informação já existia nas pinturas rupestres, ou seja, cerca de 45,5 mil anos atrás, nas quais estão registradas uma série de imagens no intuito de comunicar, seja um evento ou ainda uma quantidade. Apesar do conceito de informação aparecer desde os primórdios do estabelecimento da humanidade, é apenas na década de 1940 que a mesma passa a ser objeto de estudo com os trabalhos de Claude Elwood Shannon (1916-2001), onde o mesmo desenvolve uma teoria matemática para a informação (JUNIOR; GRECA; EL-HANI, 2014).

O objetivo principal da Teoria da Comunicação de Shannon ou Teoria Matemática da Comunicação (TMC), consistiu em sistematizar o conhecimento, até então, acerca da compreensão da eficiência em sistemas de comunicação. Tal teoria, descreve o funcionamento lógico-matemático de um destes sistemas composto por um gerador de informação, um meio de transmissão e um receptor, conforme Figura 1 (SHANNON, 1948).

Figura 1 – Esquema geral de um sistema de comunicação com a Fonte de Informação (*Information Source*) criando uma Mensagem (*Message*) a ser transmitida pelo Transmissor (*Transmitter*) transformando a mesma em um Sinal (*Signal*). Na transmissão pode haver uma fonte de ruído (*Noise Source*). O sinal é recebido (*Received Signal*) pelo Receptor (*Receiver*) e finalmente a mensagem chega ao seu destino (*Destination*).



Fonte: Shannon (1948, p. 380).

De acordo com a TMC, um Gerador de informação é um objeto capaz de produzir um conjunto X de n eventos com probabilidade de ocorrência $P(X)$ e um Receptor possui portanto um conjunto Y de mesmo valor n de eventos, com probabilidades associadas de $P(Y)$. Durante a transmissão, é possível que parte da informação seja perdida, devido a ocorrência de ruídos na transmissão e isso resulta diretamente, na modificação dos valores de probabilidade dos elementos recebidos do conjunto Y . Reconhecendo portanto os elementos de X e suas probabilidades associadas, espera-se que uma mensagem bem transmitida, ou seja, sem interferência de ruídos, seja aquela cujo as probabilidades dos elementos do conjunto Y sejam as mesmas dos conjunto de elementos de X portanto, se essas probabilidades forem distintas, podemos concluir que houve perda de informação na transmissão (KHINCHIN, 1957).

De maneira geral, a informação é quantificada de acordo com os recursos físicos necessários para que a mesma seja representada, ou seja, na capacidade de armazenamento, comunicação e representação de um conjunto X de possíveis informações. Em um computador, por exemplo, armazenamos nossa informação

através das unidades binárias chamadas *bits* ¹ Os *bits* são portanto a menor unidade de armazenamento de informação em um computador de arquitetura clássica, podendo representar o estado 1 ou o estado 0 (SHANNON, 1948).

A combinação desses *bits*, faz com que uma mensagem possa ser armazenada, processada ou transmitida em um computador clássico. Nesse sentido, quão maior, ou ainda, quão mais complexa for a mensagem a se operar, mais *bits* serão necessários e consequentemente mais recursos físicos para a representação destes. Com a evolução dos computadores e consequentemente a necessidade de um maior número de *bits* a se operar, ocorreu um processo de miniaturização do hardware, nesse caso, do dispositivo transistor. Com transistores cada vez menores, menos espaço físico era necessário para operar a informação e cada vez mais informação foi capaz de ser operada simultaneamente. Basta recordar que o tamanho de um smartphone é razoavelmente menor do que a primeira unidade de computador eletrônico criado, o ENIAC que ocupava o espaço de 180 metros quadrados (JULIA GADELHA, 2015).

Porém, um limite de processamento devido ao número de transistores necessários limitados em um pequeno espaço versus a dissipação de calor dos mesmos, o que corrompe a informação, foi estabelecido em 1965 por Gordon E. Moore, a chamada "Lei de Moore". Nela, Moore (1965) determina que o número de transistores de um computador dobraria a cada dois anos sem que seu valor fosse alterado. Esse limite foi brevemente superado por novas tecnologias de materiais ² porém, deixou evidente a necessidade de expandir a capacidade de processamento dos sistemas atuais, visto que, a tendência de crescimento na quantidade de informação processada é cada vez mais urgente.

Em 1981, o físico Richard Feynman, em um de seus seminários, sugere que os conceitos de Mecânica Quântica fossem aplicados à computação para que a informação pudesse ser operada de maneira mais rápida e em maior quantidade (PIQUEIRA, 2011).

A Mecânica Quântica é o ramo da física que surge na virada do século XX a partir de uma série de experimentos que não puderam ser explicados classicamente. As hipóteses produzidas por nomes como Planck, Einstein, Bohr e De Broglie e posteriormente aperfeiçoadas por Schrödinger, Heisenberg e Dirac, descrevem uma nova área na física. Para o desenvolvimento de um computador de arquitetura quântica, destacamos a importância do Princípio da Superposição de Estados.

O Princípio da Superposição de Estados determina que um estado de um sistema físico é composto por todas as informações possíveis de serem extraídas do mesmo em uma medição. Disso ocorre que um estado possui definição probabilística a partir de todas as possibilidades de ocupação do mesmo. Tais estados são representados por um vetor do espaço complexo de Hilbert H , chamados também, pela notação de Dirac, de *kets* e representados por $|\psi\rangle$.

Nesse sentido, unindo a teoria quântica às necessidades de aumento no processamento de informação, surge uma nova área de estudo, a Computação Quântica. Segundo Oliveira e Sarthour (2004) e COMPUTADOR... (2007), a devida construção de um Computador de arquitetura quântica foi precedida pelos eventos descritos a seguir:

- David Deutsch em 1985, propõe matematicamente o primeiro computador quântico universal;
- Peter Shor em 1994, criou o primeiro programa essencialmente quântico, ou seja, ele não poderia ser executado em um computador clássico. Este programa, conhecido como Algoritmo de Shor reduzi-

¹ Nome proposto, segundo o artigo original de Shannon por J.W. Turkey (SHANNON, 1948).

² A empresa IBM, produziu em 2014 um nanochip de silício de 7 nm e em 2015 anunciou a produção de chips de processamento com nanotubos de carbono de tamanho 1,8nm (IBM..., 2015).

ria o tempo de fatoração de números grandes de possíveis meses para apenas segundos caso fosse utilizado em um computador de arquitetura quântica;

- Em 1999 o MIT apresenta o primeiro protótipo de um computador quântico real;
- A empresa D-Wave apresenta, em 2007, o primeiro computador essencialmente quântico;

A descrição da arquitetura de um computador quântico, esbarra no mesmo princípio de um computador clássico, ou seja, em sua unidade fundamental de armazenamento de informação. De maneira análoga ao computador clássico que utiliza como unidade de informação o *bit*, o computador quântico utilizará o *qubit* (ou q-bit, ou ainda, quantum bit).

Um bit quântico, que nesse trabalho chamaremos de *qubit* pode ser produzido de maneiras distintas³, porém nosso foco de estudo está nas suas propriedades. Um *qubit* é uma unidade com propriedades quânticas que atua sob o regime de superposição de estados. Isso significa que este consegue armazenar simultaneamente mais de um estado de informação, diferente do bit clássico que armazena apenas um dos estados por vez. Decorre desta propriedade a maior capacidade de operar a informação em comparação aos mecanismos clássicos segundo apresentado na tabela 1.

Tabela 1 – Comparação entre a quantidade de bits clássicos e quânticos para se operar a informação

Quantidade de informação	Quantidade de bits clássicos	Quantidade de qubits
1 byte	8 bits	3 qubits
1 Megabyte	$8,3 \times 10^6$ bits	23 qubits
1 Terabyte	$8,8 \times 10^{12}$ bits	43 qubits

Fonte: Elaborada pelo autor.

De modo a generalizar a comparação entre bits clássicos e quânticos, podemos estabelecer a relação:

$$n \text{ qubits} = 2^n \text{ bits} \quad (1)$$

Portanto, podemos concluir que menos *qubits* são necessários para operar a informação, em comparação ao bit clássico, o que está diretamente relacionado a velocidade e capacidade de realização da mesma.

A descrição de um *qubit* consiste em uma combinação linear de dois possíveis estados quânticos $|0\rangle$ e $|1\rangle$ de modo que:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \text{com } \alpha^2 + \beta^2 = 1, \quad (2)$$

sendo α e β as amplitudes probabilísticas dos estados quânticos $|0\rangle$ e $|1\rangle$.

É interessante observar que, apesar de *qubits* conseguirem armazenar mais informação devido à superposição de estados, a obtenção direta da mesma é impossível visto que, diferente da mecânica clássica onde podemos observar se um bit se encontra em um estado 0 ou um estado 1, em situações quânticas, a

³ Podemos criar fisicamente *qubits* utilizando por exemplo, spins de átomos presos em uma armadilha. Tal armadilha pode ser do tipo óptica ou até mesmo magnética. É possível também polarizar fótons para a obtenção destes. A determinação do método é definida principalmente pelo mecanismo que melhor conseguir isolar o *qubit*, já que este é facilmente influenciado pelo ambiente externo (JORIO, 2019).

observação faz com que o sistema colapse. Portanto, o foco de aproveitamento de um *qubit* está em conseguir transferir a informação que o mesmo armazena, sem que uma medida seja realizada diretamente nesta unidade quântica (NIELSEN; CHUANG, 2010).

Apesar dessa aparente dificuldade em se obter a informação quântica, existem alguns mecanismos que facilitam e possibilitam a obtenção desta. Segundo Jorio (2019), para a compreensão destes serão necessários estabelecer alguns teoremas que regem a informação quântica, são eles:

- É impossível clonar um estado quântico, ou seja, qualquer dispositivo que receba um estado quântico como entrada, será incapaz de reproduzir como saída exatamente o mesmo estado quântico. Este teorema é conhecido como Teorema da não-clonagem.
- Não é possível obter um estado quântico desconhecido de um sistema único e individual realizando uma medição sobre este, independente do tipo e/ou sequência de medições que se realize.

Nos teoremas descritos, parece ser improvável a proposta de que a informação quântica se sobressaia em relação a clássica, mas são exatamente devido a eles e a mecanismos provenientes destes que a informação quântica se torna tão promissora. Os mecanismos que estudaremos nesse trabalho são o Emaranhamento (ou Entrelaçamento) Quântico e o Teletransporte Quântico.

O Emaranhamento quântico é uma consequência quântica proveniente da superposição de estados de elementos dessa natureza. Vale ressaltar que objetos e fenômenos quânticos, nem sempre possuem o análogo clássico, como o caso de spins. Nesse fenômeno duas partículas interagem de modo que, o estado quântico de uma destas não pode ser mais descrito sem o da outra. Isso faz com que, mesmo que as partículas estejam distantes uma da outra, elas continuam a compartilhar os estados quânticos. Isso faz com que seja possível, conhecendo algumas propriedades de uma das partículas, a exemplo a posição, é possível determinar esta mesma característica da outra partícula. A determinação das propriedades de uma das partículas culmina na instantânea definição na segunda, pois elas compartilham o mesmo estado quântico, o que nos leva a utilização do Emaranhamento para a realização do Teletransporte Quântico (JORIO, 2019; FONZAR, 2017; PIQUEIRA, 2011).

O Teletransporte Quântico consiste em uma série de operações realizadas por intermédio de um circuito de natureza quântica que pretende enviar uma mensagem de um ponto A até um ponto B. Para a realização desse procedimento, dependemos essencialmente de, ao menos, três *qubits*. Para introduzir ao leitor o conceito, iremos nos apropriar de uma história hipotética a título de esclarecer a ideia principal do fenômeno. Imagine por um instante que você deseja mandar uma fotografia para alguém que não vê há muito tempo. Existem essencialmente duas maneiras de realizar o envio, você pode enviar a foto pelo correio e aguardar que essa pessoa receba. Esse processo poderia ser chamado de Transporte de informação, ou ainda, você poderia criar um arquivo digital com informações sobre a fotografia, de maneira que a pessoa que recebe o arquivo, possa de alguma maneira recriar a foto, nesse segundo caso, a foto seria teletransportada (JORIO, 2019).

Trazendo a situação descrita para o universo quântico, o teletransporte de estados quânticos consiste em uma série de operações que possibilitam descrever no ponto B um estado existente no ponto A. A princípio, devido ao teorema da não-clonagem ⁴, seria impossível 'clonar' um *qubit*, ou seja, teletransportar a

⁴ A informação clássica pode ser facilmente reproduzida, basta recordar que um livro pode ser impresso com a tiragem de exemplares que desejar. Já a informação quântica não é plausível de reprodução direta. Algumas provas matemáticas desta impossibilidade estão apresentadas em Piqueira (2011).

informação de modo semelhante ao que ocorre com um canal clássico. Porém, segundo Bennet et al. (1993), é possível contornar o problema utilizando um canal de informação clássico, semelhante ao apresentado por Shannon na TMC, porém utilizando como emissor-receptor um par de partículas emaranhadas quanticamente.

Na literatura, encontram-se as mais diversas explicações sobre como funciona o teletransporte quântico (BENNET et al., 1993; BOUWMEESTER et al., 1997; ZEILINGER, 2000; BRASSARD, 1996; JORIO, 2019) e na maioria dos casos, os leitores são introduzidos a dois personagens Alice e Bob. Na história, os cientistas Alice e Bob estão localizados em dois laboratórios distintos, cada um deles possui um *qubit*, q_A e q_B e estes estão emaranhados, produzindo um estado quântico emaranhado denominado de $|\psi_{AB}\rangle$. A Alice, precisa enviar uma mensagem urgente ao Bob utilizando um outro *qubit*, q_C . Portanto no início do processo de teletransporte, a Alice possui dois *qubits*, o que ela deseja enviar e o que possui o estado quântico emaranhado com o *qubit* do Bob. Alice então, realiza uma série de operações entre seus *qubits* e, como um deles está emaranhado com o *qubit* de Bob, este saberá que algo está mudando. Para continuar o processo de teletransporte, Alice faz uma medição em seus *qubits*, colapsando-os e envia, via canal clássico, a informação dos *qubits* colapsados para Bob. Este por sua vez, por saber qual era o estado inicial de q_A , devido ao emaranhamento, consegue reconstruir a mensagem presente originalmente no *qubit* q_C enviado por Alice. Portanto, a mensagem é reconstruída e não clonada, não violando os princípios da não-clonagem, citado anteriormente. A não clonagem fica explicitada no momento em que a medida é realizada em q_A e q_C , colapsando-os, de modo que existe apenas uma cópia do estado de q_C dado por $|\psi_C\rangle$.

O teletransporte quântico possui algumas questões a se salientar. A primeira delas é que, de fato, este é um método de transmissão de informação extremamente seguro, visto que, se o receptor não tiver o *qubit* emaranhado com o do emissor, a mensagem não poderá ser recuperada, além do fato de que a informação original é destruída na transmissão da mensagem. Disso decorre imediatamente a segunda questão, a informação pode, eventualmente, sofrer interferência de ruídos externos durante o envio da mensagem e por não possuir mais a mensagem original, esta pode ser perdida.

Portanto, o estudo dos possíveis ruídos que possam interferir no teletransporte, assim como na transmissão clássica, faz com que, mesmo que estes ocorram, seja possível recuperar a informação ao final do processo, corrigindo tais erros. Existem os mais diversos tipos de ruídos aos quais a mensagem pode ser exposta, o que torna praticamente impossível prever quais deles efetivamente ocorreram ao recuperar uma mensagem, porém, o estudo de ruídos familiares torna possível o reconhecimento destes tornando mais provável a recuperação da informação enviada (FONZAR, 2017).

A construção do sistema de teletransporte quântico demanda de um circuito onde operam as chamadas portas lógicas quânticas e portanto, a realização experimental de um teletransporte quântico demanda efetivamente de um computador de arquitetura quântica para que as operações ocorram sob os *qubits*. Apesar de já existirem computadores quânticos, ainda é necessário estudos acerca do mesmo para que cada vez mais, a qualidade dos *qubits* seja melhorada. Porém, devido aos recursos de simulação, podemos utilizar um computador de arquitetura clássica para simular tanto um *qubit* quanto os circuitos lógicos necessários para a realização do teletransporte quântico, a título do estudo, por exemplo, dos efeitos de ruídos na transmissão da informação quântica conforme propomos nesse trabalho.

2 Objetivo(s) da Proposta

O objetivo principal deste trabalho consiste em realizar um estudo acerca dos efeitos de possíveis ruídos no fenômeno de teletransporte quântico, utilizando uma simulação de circuitos quânticos em um computador de arquitetura clássica. Para atingir tal proposta, pretende-se:

1. Definir o conceito de Teletransporte Quântico;
2. Delinear as situações onde o fenômeno é utilizado;
3. Elencar os tipos de ruídos que podem interferir na transmissão de informação durante o fenômeno;
4. Construir a simulação de comportamento de um *qubit*;
5. Estruturar as portas lógicas quânticas a serem simuladas para o presente estudo;
6. Estabelecer uma sequência de testes com os algoritmos de ruído;
7. Comparar os resultados obtidos na simulação desenvolvida com os resultados provenientes de simuladores em computadores de arquitetura quântica como o IBM Quantum e o Azure Quantum.

3 Metodologia

4 Cronograma de Atividades

Referências

- BENNET, Charles H. et al. Teleporting a Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. **Physical Review Letters**, v. 70, n. 13, p. 1895–1899, mar. 1993. ISSN 1981-5344. Disponível em: <<https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.70.1895>>.
- BOUWMEESTER, Dik et al. Experimental quantum teleportation. **Nature**, v. 390, p. 575–579, dez. 1997. Disponível em: <<https://www.nature.com/articles/37539>>.
- BRASSARD, Gilles. Teleportation as a quantum computation. **Physics Computation**, 1996.
- CAPURRO, Rafael; HJORLAND, Birger. O conceito de Informação. **Perspectivas em Ciência da Informação [online]**, v. 12, p. 148–207, abr. 2007. ISSN 1981-5344. Disponível em: <<https://www.scielo.br/j/pci/a/j7936SHkZJkpHGH5ZNYQXnC/?lang=pt#>>.
- COMPUTADOR quântico em ação. 2007.
<https://revistapesquisa.fapesp.br/computador-quantico-em-acao/>. Accessed: 2022-04-07.
- FONZAR, Icaro Souza. **Transmissão de informação através do teletransporte quântico**. 2017. Monografia – Universidade Estadual Paulista “Júlio de Mesquita Filho”.
- IBM. 2015. <https://newsroom.ibm.com/>. Accessed: 2022-04-07.
- JORIO, Ado. Informação Quântica. In: MECÂNICA Quântica. Universidade Federal de Minas Gerais, 2019. P. 241–272. Disponível em:
<http://lilith.fisica.ufmg.br/~adojorio/disciplinas/mecanica_quantica.html>.
- JULIA GADELHA. **A Evolução dos computadores**. 2015. <http://www.ic.uff.br/~aconci/evolucao.html>. Accessed: 2022-04-07.
- JUNIOR, Olival Freire; GRECA, Ileana Maria; EL-HANI, Charbel Niño. Ciências na transição dos séculos: conceitos, práticas e historicidade. In: CIÊNCIAS na transição dos séculos: conceitos, práticas e historicidade. EDUFBA, 2014. P. 07–28. ISBN 9788523212438. Disponível em:
<<https://repositorio.ufba.br/bitstream/ri/22111/1/Ciencia%20na%20transicao%20dos%20seculos-RI.pdf>>.
- KHINCHIN, Aleksandr Yakovlevich. **Mathematical foundations of information theory**. Dover Publications, New York, 1957.
- MOORE, Gordon E. Cramming more components onto integrated circuits. **Electronics Magazine**, v. 38, n. 8, abr. 1965. Disponível em: <<https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf>>.
- NIELSEN, Michael A.; CHUANG, Isaac L. **Quantum Computation and Quantum Information**. Cambridge University Press, New York, 2010.
- OLIVEIRA, Ivan S.; SARTHOUR, Roberto S. Computação Quântica e Informação Quântica. **V Escola do CBPF**, 2004. Disponível em: <<http://www.cbpf.br/~qbitrmn/didaticos/cqiq.pdf>>.
- PIQUEIRA, José Roberto Castilho. Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte. **Revista Brasileira de Ensino de Física [online]**, v. 33, dez. 2011. ISSN 1806-9126. Disponível em:
<<https://www.scielo.br/j/rbef/a/XZ8FbFnDYZ33r4xHtJFSDQL/abstract/?lang=pt#>>.

SHANNON, Claude Elwood. A Mathematical Theory of Communication. **The Bell System Technical Journal**, v. 27, p. 379–423, jul. 1948. Disponível em:

<<https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf>>.

ZEILINGER, Anton. Quantum Teleportation. **Scientific American**, v. 282, n. 2, p. 50–59, abr. 2000.

Disponível em: <<https://www.jstor.org/stable/26058672>>.