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

TRANSMISSÃO DE INFORMAÇÃO QUÂNTICA: SIMULAÇÃO DE RUÍDOS NO FENÔMENO DE TELETRANSPORTE QUÂNTICO

Sorocaba

Abril, 2023

Bianca Miyabe Santos Freitas

TRANSMISSÃO DE INFORMAÇÃO QUÂNTICA: SIMULAÇÃO DE RUÍDOS NO FENÔMENO DE TELETRANSPORTE QUÂNTICO

Trabalho de Conclusão de curso apresentado ao curso de Licenciatura Plena em Física, como requisito para a obtenção do título de Licenciado em Física.

Orientador: Prof. Dr. Renato Fernandes Cantão

Sorocaba

Abril, 2023

Modelo de ficha catalográfica (VERSO DA FOLHA DE ROSTO).

Incluir um PDF de acordo com as regras de seu curso!

https://www.bso.ufscar.br/servicos-e-informacoes/ficha-catalografica

Errata

SOBRENOME, Nome. Título: subtítulo. 20XX. Trabalho de Conclusão de Curso (Licenciatura Plena em [Matemática/Física]) – Universidade Federal de São Carlos, Sorocaba, 20XX.

Folha	**Linha**	**Onde se lê**	**Leia-se**
12	13	Bilologia	Biologia

Folha de aprovação.

Incluir um PDF de acordo com as regras de seu curso!

DEVE ESTAR ASSINADA!

Dedico este trabalho à minha versão de 2016, nós conseguimos.

Agradecimentos

Gostaria de iniciar os agradecimentos ressaltando que este trabalho é o fruto das inúmeras interações que me trouxeram até aqui. Iniciando por minha família. Aos meus pais, por muitas vezes ao longo desses anos, terem abdicado de sonhos e desejos para que eu pudesse estar aqui, finalmente, fazendo o que eu amo. Ao meu irmão, por entender minhas necessidades de estudo e remanejar seus momentos de lazer, as vezes. Aos meus avós Júlia *in memoriam* e Jaime *in memoriam*, que apesar de não terem visto esse caminho se iniciar, me motivam diariamente pelas memórias e pelo incentivo, nas palavras de meu avô: ”um dia você vai ser doutora”, talvez seja esse o início de sua profetização. À minha avó de consideração Hermelina *in memoriam*, pela constante preocupação e por, literalmente, proporcionar meu material de estudo. Agradeço também aos meus amigos Matheus Pecci, Jéssica Leonel, Juliana Mendes e Ricardo Almagro por compartilhar momentos de desespero e de sabedoria ao longo desses anos, pelo incentivo e exemplo, vocês também fazem parte disso aqui! Ao meu companheiro de aventuras Felipe Aranha, por não me deixar desistir, por me ouvir falar sobre esse trabalho, por ler e reler trechos, por ter paciência, muita paciência comigo. Obrigado não é suficiente, mas o faço de todo o meu coração! Aos professores do curso de Licenciatura em Física da UFSCar - Sorocaba, pelos ensinamentos compartilhados em aula e fora dela, obrigada por me mostrarem o caminho! Em especial ao meu orientador Renato Cantão que eu sinceramente não sei como não desistiu de mim, mas obrigada por não o fazer! Agradeço a compreensão pelos momentos difíceis, a motivação e por tornar todo esse processo menos pesado!

Os Computadores do futuro não devem pesar mais do que 1,5 toneladas.
(Mecânicos Populares, prevendo a marcha implacável da ciência, 1949)
Acho que existe um mercado mundial para talvez cinco computadores.
(Thomas Watson, Presidente da IBM, 1943)

Resumo

SOBRENOME, Nome. Título: subtítulo. 20XX. Trabalho de Conclusão de Curso (Licenciatura Plena em [Matemática/Física]) – Universidade Federal de São Carlos, Sorocaba, 20XX.

[A referência acima é opcional quando o resumo estiver contido no próprio documento e deve ficar logo após o título da seção (Resumo).]

Item obrigatório. Resumo é a apresentação concisa dos pontos relevantes de um documento. O resumo deve ressaltar sucintamente o conteúdo de um texto. A ordem e a extensão dos elementos dependem do tipo de resumo (informativo ou indicativo) e do tratamento que cada item recebe no documento original. O resumo deve ser composto por uma sequência de frases concisas em parágrafo único, sem enumeração de tópicos. Em documento técnico ou científico, recomenda-se o resumo informativo. Convém usar o verbo na terceira pessoa. Convém que, nos trabalhos acadêmicos, os resumos tenham de 150 a 500 palavras. Segundo a Associação Brasileira de Normas Técnicas (ABNT) 6028:2021, as palavras-chave devem figurar logo abaixo do resumo, antecedidas da expressão Palavras-chave, seguida de dois-pontos, separadas entre si por ponto e vírgula e finalizadas por ponto. Devem ser grafadas com as iniciais em letra minúscula, com exceção dos substantivos próprios e nomes científicos.

Palavras-chave: resumo; Associação Brasileira de Normas Técnicas; trabalho acadêmico.

Abstract

Item obrigatório. É a versão do Resumo em língua vernácula para um idioma de divulgação internacional.

Keywords: word 1; word 2; word 3.

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

Nas últimas décadas a humanidade passou por um intenso e revolucionário processo de inovações e renovações tecnológicas envolvendo o dispositivo que conhecemos por computador. Basta recordar que o tamanho de um smartphone moderno é muito menor do que a primeira unidade de computador eletrônico criado, o ENIAC, que ocupava um espaço de 180 m^2 (GADELHA, 2015).

Nesse processo evolutivo do computador podemos destacar que a miniaturização dos processadores resultou no aumento da sua capacidade de processamento de informação e estes foram essenciais para a popularização dos dispositivos e ainda, para o aumento da sua velocidade operacional. Diante dessa constante mudança, em 1965 foi estabelecido por Gordon E. Moore um limite de processamento devido ao número de transistores[1] necessários comprimidos em um pequeno espaço versus sua dissipação de calor, o que corrompe a informação. Esse limite recebeu o nome de "Lei de Moore". Nela, Moore (1965) estimou 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], deixando evidente, entretanto, 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 maior.

Diante do limite físico para o tamanho dos processadores e do crescimento do volume de informação a ser processado, uma possível solução foi proposta pelo físico Richard Feynman em 1981. Feynman, na tentativa de compreender a simulação de sistemas físicos para seus estudos, propõe que se sistemas físicos são regidos pela física quântica, sua simulação deve ser feita por um dispositivo que corresponda a mesma natureza (CALDEIRA, 2018).

Nesse período temos portanto a junção de três importantes áreas de estudo: a computação, a informação e a física quântica. Esta união visava superar os limites da computação até então, em relação à velocidade de processamento e volume de armazenamento de informação, dando início aos estudos da chamada *Computação Quântica*. A computação quântica é um campo emergente cujo objetivo é desenvolver computação com base nos princípios da mecânica quântica que, conforme veremos na Seção 2.2, é a teoria da Física que descreve o comportamento dos átomos, íons e partículas subatômicas. As partículas quânticas podem existir em múltiplos estados ao mesmo tempo e essa característica única permite que os computadores quânticos manipulem simultaneamente muitos estados de dados, o que não é possível com computadores convencionais, permitindo aos computadores quânticos processar muito mais informação, de forma mais rápida

[1] O transistor é um componente eletrônico desenvolvido por John Bardeen, William Shockley e Walter Brattain em meados de 1947. O dispositivo passou por diversos aperfeiçoamentos desde então e sua principal função consiste em amplificar ou interromper sinais elétricos. Nos computadores, são os responsáveis por indicar a presença ou ausência do sinal elétrico, sendo possível a interpretação da informação nos dispositivos de processamento (SEDRA; SMITH, 2007).

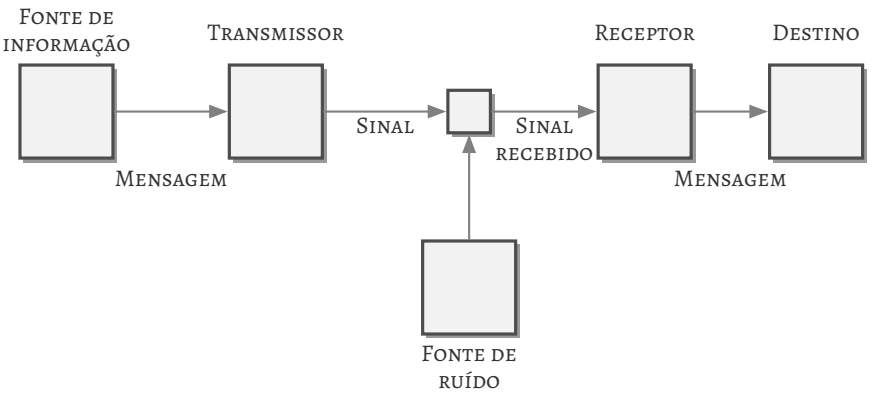
[2] A empresa IBM, produziu em 2014 um nanochip de silício de 7 nm e em 2015 anunciou a produção de chips de processamento com nanotubos de carbono de tamanho 1,8 nm (IBM, 2015).

e eficiente do que os computadores convencionais, que utilizam a arquitetura de dados clássica, ou seja, informação clássica (OLIVEIRA; SARTHOUR, 2004).

Segundo Capurro e Hjorland (2007), o conceito de informação possui seu significado cotidianamente atribuído como *conhecimento comunicado*. Nesse sentido, a informação já existia nas pinturas rupestres há 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 esta passa a ser objeto de estudo com os trabalhos de Claude Elwood Shannon (1916–2001), que 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), era sistematizar o conhecimento acumulado até então acerca da eficiência em sistemas de comunicação, ou seja, de como a informação é transmitida. A teoria descreve o funcionamento lógico-matemático de um destes sistemas, composto por um gerador de informação, um meio de transmissão e um receptor, conforme ilustra a Figura 1 (SHANNON, 1948).

Figura 1 – Esquema geral de um sistema de comunicação com a Fonte de Informação criando uma Mensagem a ser transmitida pelo Transmissor que a transforma em um Sinal. Na transmissão pode haver uma Fonte de Ruído. O sinal é recebido pelo Receptor e finalmente a mensagem chega ao seu Destino.



Fonte: Adaptado de 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 $P(X)$, enquanto um *receptor* possui um conjunto Y, também com n eventos, com probabilidades associadas $P(Y)$. Durante a transmissão é possível que parte da informação seja perdida devido a ocorrência de ruídos, o que 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 cujas probabilidades dos elementos do conjunto Y sejam as mesmas dos elementos do conjunto X. Assim, 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 ela seja representada, ou seja, na capacidade de armazenamento, comunicação e representação de um conjunto X de possíveis informações. Em um computador clássico, por exemplo, armazenamos informações através das unidades binárias chamadas *bits*[3]. Dessa forma, os bits são 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.

A descrição da arquitetura de um computador quântico esbarra no mesmo princípio daquela 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 qubit, ou bit quântico, pode ser produzido de maneiras distintas[4], 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 ele 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 necessários para se operar uma informação.

Quantidade de bytes (informação)	Quantidade de bits clássicos	Quantidade de qubits
1	8	3
10^6	$8{,}3 \times 10^6$	23
10^{12}	$8{,}8 \times 10^{12}$	43

Fonte: Elaborada pelo autor.

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

$$n \text{ qubits} = 2^n \text{ bits}. \tag{1.1}$$

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

[4] Qubits podem ser fisicamente criados utilizando, por exemplo, spins de átomos presos em uma armadilha. Essa armadilha pode ser do tipo óptica ou até mesmo magnética. É possível também polarizar fótons para sua obtenção. 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).

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

Segundo Oliveira e Sarthour (2004) e FAPESP (2007), a devida construção de um computador de arquitetura quântica foi precedida pelos eventos descritos a seguir:

1985 David Deustch propõe matematicamente o primeiro computador quântico universal;

1994 Peter Shor cria o primeiro programa essencialmente quântico, ou seja, ele não poderia ser executado em um computador clássico. Este programa, conhecido como Algoritmo de Shor, reduziria o tempo de fatoração de números grandes de possíveis meses para apenas segundos caso fosse utilizado em um computador real de arquitetura quântica;

1999 O MIT apresenta o primeiro protótipo de um computador quântico real;

2007 A empresa D-Wave apresenta o primeiro computador essencialmente quântico.

Apesar de na atualidade processadores quânticos existirem e operarem[5], ainda estamos distantes da efetiva implementação comercial de um computador quântico. Podemos utilizar de exemplo, o fato de que apesar de possuirmos um análogo para a TMC de Shannon em um computador quântico[6], ainda não temos um análogo quântico para um sistema submetido a ruídos na transmissão[7] (NIELSEN; CHUANG, 2010).

Portanto, o estudo de simulações de sistemas de informação quânticos se faz necessário para aperfeiçoamento desses mecanismos e ainda para o desenvolvimento da própria Física, visto que o avanço da compreensão da utilização da mecânica quântica atrelado ao conceito de informação, possibilita a compreensão da natureza de maneira cada vez mais complexa, sem a necessidade de aproximações e simplificações (NIELSEN; CHUANG, 2010).

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 de operações com a informação quântica, a título do estudo, por exemplo, dos efeitos de ruídos na transmissão da informação quântica conforme propomos nesse trabalho. Nesse sentido, os próximos capítulos irão introduzir conceitos sobre informação quântica e mecânica quântica para a compreensão do desenvolvimento do trabalho.

[5] FALAR SOBRE O AZURE QUANTUM E IBM QUANTUM

[6] Em 1995, Benjamin Schumacher propõe com êxito um análogo quântico para o TMC (SCHUMACHER, 1995).

[7] Contudo, foi desenvolvida a teoria de correção de erros quânticos que permite que computadores quânticos possam operar na presença de ruídos e que a informação quântica seja transmitida de maneira confiável (NIELSEN; CHUANG, 2010)

2 Fundamentação Teórica

Conforme descrito no Capítulo de Introdução, para o estudo da Computação Quântica e da Informação Quântica, são necessários alguns recursos provenientes da Mecânica Quântica bem como a construção de análogos quânticos para o processamento dessa informação. As seções a seguir apresentarão a fundamentação teórica e os recursos matemáticos necessários para o desenvolvimento da simulação proposta na Metodologia.

2.1 Conceitos básicos de Álgebra Linear

2.2 Mecânica Quântica

Esta teoria foi criada no início do século XX para explicar o comportamento dos átomos e estudar os efeitos relativos ao tamanho microscópico das partículas. A mecânica quântica explica como as partículas subatômicas se comportam, como interagem com a luz e como são afetadas por forças externas. Ela é essencial para a compreensão de muitos fenômenos físicos, como a estrutura de átomos e moléculas e as propriedades de materiais, da radiação eletromagnética e da matéria escura.

Podemos definir seus postulados como:

1. Princípio da incerteza de Heisenberg: é impossível, ao mesmo tempo, medir com precisão a localização e a velocidade de uma partícula subatômica.
2. Princípio da dualidade onda-partícula: uma partícula subatômica pode se comportar tanto como onda quanto como partícula.
3. Princípio da superposição: qualquer sistema quântico pode encontrar-se simultaneamente em vários estados.
4. Princípio da exclusão de Pauli: dois fótons ou partículas idênticas não podem ocupar o mesmo estado quântico.
5. Princípio da ação à distância: o efeito de uma interação quântica entre partículas pode se propagar instantaneamente, independentemente da distância.

Para os estudos que seguem nesse trabalho, iremos enfatizar os postulados 3 e 5.

2.3 Qubits

As definições de qubits descritas nesse tópico baseiam-se principalmente nas ideias apresentadas por Nielsen e Chuang (2010) e Oliveira e Sarthour (2004).

Qubits são elementos fundamentais da computação quântica. Eles são usados para representar informações binárias (zeros e uns) e são capazes de armazenar e processar muito mais informações que os bits convencionais usados na computação clássica. Isso é possível graças ao fato de que, enquanto os bits tradicionais podem estar em dois estados (ligado ou desligado), os qubits podem estar em um estado de superposição, o que permite que eles representem simultaneamente vários estados ou informações diferentes. Isso significa que os qubits podem armazenar muito mais informação em um espaço muito menor, tornando a computação quântica muito mais poderosa e eficiente.

Comentar sobre os termos "poderosa" e "eficiente" num sentido computacional.

Podemos começar a descrição de um qubit como uma superposição dos estados quânticos $|0\rangle$ e $|1\rangle$, de modo a representá-los pela combinação linear dada por

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

com α e β parametrizados por $\alpha^2 + \beta^2 = 1$.

Os números α e β são complexos e determinam as amplitudes probabilísticas da obtenção dos estados quânticos. O estado descrito por $|\psi\rangle$ é uma superposição dos estados quânticos $|0\rangle$ e $|1\rangle$, ou seja, seguindo os postulados da mecânica quântica, o qubit pode existir num estado contínuo entre $|0\rangle$ e $|1\rangle$ porém, ao ser medido, colapsando o sistema, retornará apenas os valores de $|0\rangle$ e $|1\rangle$ com as probabilidades α e β associadas.

"$|0\rangle$ **e** $|1\rangle$" ou "$|0\rangle$ **ou** $|1\rangle$"

Um recurso para visualizar o comportamento de qubits é sua representação geométrica chamada de Esfera de Boch. Como entidades quânticas não são observáveis diretamente e frequentemente são expressas por recursos matemáticos, a visualização da superposição dos estados de um qubit utilizando a Esfera de Boch facilita, ainda que ligeiramente, sua compreensão.

Em primeiro lugar, vale lembrar que o qubit, descrito por $|\psi\rangle$, está parametrizado e podemos reescrever (2.1) em coordenadas polares

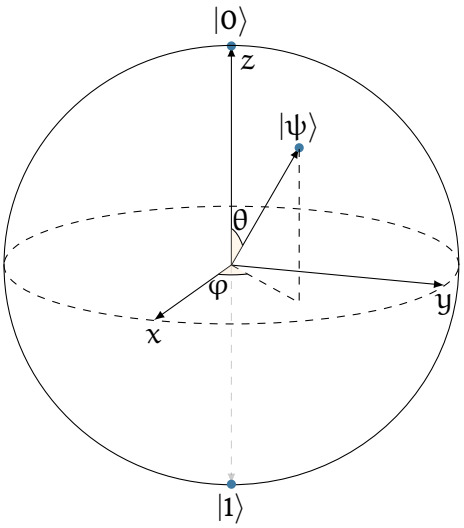
$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\,\operatorname{sen}\frac{\theta}{2}\,|1\rangle\right). \tag{2.2}$$

O termo $e^{i\gamma}$ não possui efeitos observáveis na representação geométrica e portanto, podemos simplificar a equação acima, obtendo

$$|\psi\rangle = \left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\,\operatorname{sen}\frac{\theta}{2}\,|1\rangle\right), \tag{2.3}$$

com θ e φ sendo números reais correspondentes aos ângulos entre os eixos z, y e y, x respectivamente, conforme a Figura 2.

Figura 2 – Representação gráfica de um qubit como um ponto sob a superfície da Esfera de Bloch.



Fonte: Adaptado de Nielsen e Chuang (2010).

2.4 Portas Lógicas Quânticas

2.5 Emaranhamento Quântico

2.6 Teletransporte Quântico

2.7 Protocolo de Teletransporte Quântico

A realização de um Protocolo de Teletransporte Quântico consiste, essencialmente, em uma série de operações que possuem por objetivo principal fazer com que uma mensagem, ou na linguagem quântica, um estado quântico, se teletransporte entre dois pontos distintos fisicamente. Como em qualquer outra operação computacional é necessária a existencia de um circuito lógico, nesse caso, quântico que media as operações. Esse circuito consistirá nas combinações das portas lógicas CNOT, Haddamard, portas de medição e as portas X e Z conforme a Figura 3

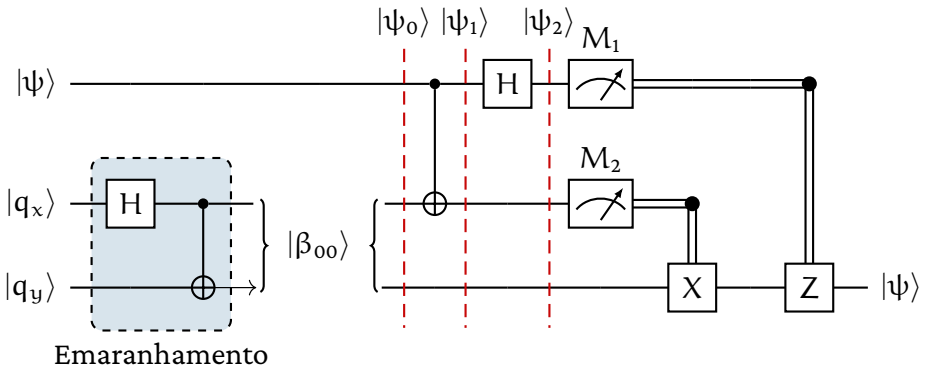
Dúvida: devemos usar maiúsculas em “Protocolo”, “Mecânica Quântica”, “Local”, etc? Se sim, precisamos padronizar.

No inicio do Protocolo é necessário que tenhamos um par de qubits emaranhados nas bases de Bell, no estado $|\beta_{00}\rangle$, que podemos representar pela expressão

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.4}$$

Um dos qubits do par emaranhado em (2.4) é mantido em A e o outro necessariamente precisa estar em B para que exista um canal de comunicação entre essas partes. Além do par emaranhado, em A teremos o estado quântico a ser enviado, ou seja sua mensagem dada por $|\psi\rangle$, segundo a Equação (2.1). De posse do par emaranhado e da mensagem, o protocolo é iniciado com a aplicação

Figura 3 – Protocolo de Teletransporte Quântico mediado pelo circuito com as portas CNOT, Hadamard, Medição aplicadas no Local A e as portas X e Z aplicadas no Local B.



Fonte: Adaptado de

da porta CNOT entre $|\psi\rangle\,|\beta_{00}\rangle$, que chamaremos de $|\psi_0\rangle$. A porta CNOT possui como tabela verdade a seguinte proposição:

Da forma como estão escritas, as portas não se configuram como teoremas...Precisamos discutir.

Teorema 2.1: Operação CNOT

A operação CNOT deve:

i. Inverter o segundo qubit, caso o primeiro esteja no estado $|1\rangle$;

ii. Não realizar nenhuma operação no segundo qubit, caso o primeiro esteja no estado $|0\rangle$.

Dessa maneira, aplicando o Teorema 2.1 no estado dado por $|\psi_0\rangle$

$$\begin{aligned}\text{CNOT}\,|\psi_0\rangle &= \text{CNOT}\,|\psi\rangle\,|\beta_{00}\rangle \\ &= \text{CNOT}\,\frac{1}{\sqrt{2}}\Big[\alpha\,|0\rangle\,\big(|00\rangle+|11\rangle\big)+\beta\,|1\rangle\,\big(|00\rangle+|11\rangle\big)\Big] \\ &= \frac{1}{\sqrt{2}}\Big[\alpha\,|0\rangle\,\big(|00\rangle+|11\rangle\big)+\beta\,|1\rangle\,\big(|10\rangle+|01\rangle\big)\Big]. \qquad (2.5)\end{aligned}$$

A operação descrita pela Equação (2.5) resulta no estado que chamaremos de $|\psi_1\rangle$ e neste, segundo o circuito da Figura 3, deve-se aplicar a porta Hadamard:

Teorema 2.2: Operação Hadamard

A operação Hadamard deve:

i. Aplicar no estado 0 a operação $\frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)$;

ii. Aplicar no estado 1 a operação $\frac{1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)$.

Aplicando portanto o Teorema 2.2 em $|\psi_1\rangle$, teremos

$$\mathrm{H}\,|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^2 \Big[\alpha\big(|0\rangle + |1\rangle\big)\big(|00\rangle + |11\rangle\big) + \beta\big(|0\rangle - |1\rangle\big)\big(|10\rangle + |01\rangle\big)\Big]. \tag{2.6}$$

O estado obtido em (2.6) pode ser identificado como $|\psi_2\rangle$ e evidenciando os estados emaranhados deste ao organizá-lo da seguinte maneira

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\Big]. \tag{2.7}$$

O próximo passo do protocolo consiste em realizar medidas em ambos os qubits presentes em A. Essas medidas farão com que os estados quânticos sejam colapsados e deixem de coexistir, passando a ser considerados clássicos. As medidas possíveis de serem obtidas em A são apresentadas na Tabela 2.

Tabela 2 – Possíveis resultados das medidas realizadas nos qubits presentes em A no estado quântico $|\psi_2\rangle$.

Medida realizada	Estado quântico associado
$\|00\rangle$	$\big(\alpha\,\|0\rangle + \beta\,\|1\rangle\big)$
$\|01\rangle$	$\big(\alpha\,\|1\rangle + \beta\,\|0\rangle\big)$
$\|10\rangle$	$\big(\alpha\,\|0\rangle - \beta\,\|1\rangle\big)$
$\|11\rangle$	$\big(\alpha\,\|1\rangle - \beta\,\|0\rangle\big)$

Fonte: Elaborada pelo autor.

Os valores dos estados medidos em A, são enviados via canal clássico até B que, devido ao emaranhamento com o qubit operado em A, terá seu colapso consequentemente em seu estado quântico associado, segundo a Tabela 2.

A última etapa do protocolo, ocorre em B, na tentativa de reconstruir a mensagem original, nesse momento já inexistente, que estava em A. Nessa última etapa, serão utilizadas (ou não) as portas lógicas X e Z, cujas operações estão definidas a seguir.

Teorema 2.3: Operação X

A porta lógica quântica X deve trocar os estados quânticos, ou seja, torná-lo 1 quando este for 0 e torná-lo 0, quando este for 1.

Teorema 2.4: Operação Z

A porta lógica quântica Z deve inverter a fase do estado quântico, ou seja, torná-la negativa quando esta for positiva e torná-la positiva quando esta for negativa.

A aplicação das portas dependerá do resultado da medida enviado por A, seguindo o estipulado na Tabela 3. Com isso, o protocolo se encerra e a mensagem é teletransportada do ponto A para o ponto B, sem que nenhum teorema da física quântica seja violado.

Tabela 3 – Aplicação das portas lógicas quânticas, de acordo com a medida da informação enviada por A.

Resultado medido	**Ação**
$\|00\rangle$	Nenhuma porta deve ser aplicada e o estado colapsado em B é exatamente o mesmo da mensagem enviada em $\|\psi\rangle$
$\|10\rangle$	Apenas a porta Z deve ser aplicada
$\|01\rangle$	Apenas a porta X deve ser aplicada
$\|11\rangle$	Tanto a porta X quanto a porta Z devem ser aplicadas

2.8 Algoritmo do protocolo de Teletransporte

Descrição das etapas para o protocolo de teletransporte

1. Determinar as funções que descrevem os qbits a serem emaranhados
   - qbit x
   - qbit y
2. Determinas as matrizes que descrevem as portas utilizadas no emaranhamento
   - Porta Hadamard
   - Porta CNOT
   - Matriz Identidade
3. Determinar as operações entre os qbits e as portas e a ordem de realização para o emaranhamento
   - Produto tensorial entre qbit x e qbit y $\rightarrow$ qbit xy
   - Produto tensonial entre Porta Haddamard e Matriz Identidade $\rightarrow$ H $\otimes$ I
   - Multiplicação entre qbit xy e H $\otimes$ I $\rightarrow$ Hxy
   - Multiplicação entre Hxy e a Porta CNOT $\rightarrow \beta_0 0$
4. Determinar o qbit a ser enviado
   - Definir a entrada de dados feita pelo usuário
   - Verificar a possibilidade de acordo com a normalização $\alpha + \beta = 1$
5. Aplicar a porta CNOT
   - Verificar a condição lógica de aplicação da porta CNOT
   - Aplicar CNOT em $\beta_0 0 \rightarrow |\psi_1\rangle$
6. Aplicar a porta Hadamard em $|\psi_1\rangle \rightarrow |\psi_2\rangle$

7. Reorganizar e apresentar os estados antes da medição
8. Realizar a medição
    - Determinar de modo aleatório qual dos estados serão medidos
9. Apresentar a medição - Transmissão clássica da informação
10. Determinar as operações a serem realizadas de acordo com a medição realizada
11. Apresentar a mensagem original recuperada

2.9 Ruídos

3 Metodologia

A Representação Matricial dos protocolos de Emaranhamento e Teletransporte

As representações matriciais dos protocolos de Emaranhamento e Teletransporte nos permitem observar com maior clareza a natureza binária dos qubits numa representação de como seria seu comportamento em uma situação real. Para todos os efeitos não é considerada a origem do qubit mas sim sua natureza, ou seja, uma entidade quântica. A notação de *bracket* permite que as operações sejam realizadas considerando os estados quânticos possíveis armazenados dentro do qubit como versores num espaço complexo.

Para iniciar o protocolo, consideraremos as seguintes representações binárias dos estados quânticos

$$|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{e} \quad |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{A.1}$$

Consideraremos também que estados quânticos que dependem de mais de um qubit (emaranhados ou não), são representados pelo produto tensorial dos seus estados internos, como segue o exemplo:

$$|00\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{A.2}$$

A representação gráfica do circuito quântico que realiza o protocolo de emaranhamento possibilita o entendimento dos procedimentos contidos no mesmo, conforme a região destacada da Figura 3

Para que o emaranhamento seja possível, ambos os qubits representados por $|q_x\rangle$ e $|q_y\rangle$ devem existir no mesmo espaço de Hilbert e portanto a operação de produto tensorial entre eles deve ser possível de modo que, considerando o estado quântico $|0\rangle$:

$$|q_x\rangle \otimes |q_y\rangle = |0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{A.3}$$

Seguindo a Figura 3, aplicamos a porta Hadamard, H, multiplicando-a pela matriz identidade I, obtendo:

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \tag{A.4}$$

e, aplicando o resultado acima em (A.2):

$$\mathrm{H}\,|00\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}. \tag{A.5}$$

Em seguida, aplicamos a porta CNOT:

$$\mathrm{CNOT}\big(\mathrm{H}\,|00\rangle\big) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{A.6}$$

A equação também é conhecida como uma das Bases de Bell. A comparação da Base de Bell no estado $|00\rangle$ em notação de Dirac e em notação matricial é feita considerando as (A.2) e (A.1) de modo que, seja $|\beta_{00}\rangle$ a Base de Bell em notação de Dirac dada por $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$, reescrevendo teremos:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{A.7}$$

O resultado obtido em (A.7) é exatamente o mesmo obtido na (2.4). A próxima etapa do protocolo de teletransporte, consiste na aplicação da porta lógica quântica CNOT. Portanto, seja o estado $|\psi_0\rangle$ descrito por:

$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \left[\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right] \tag{A.8}$$

Conforme Figura 3, a porta CNOT possui como controle o qubit descrito pelo estado $|\psi\rangle$ e como alvo o par emaranhado presente no Local A $|\beta_{00}\rangle$. Sua atuação apenas ocorrerá quando o qubit de controle estiver no estado $|1\rangle$. Desse modo, reescrevendo (A.8):

$$|\psi_0\rangle = \frac{1}{\sqrt{2}} \left\{ \left[\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right] + \left[\beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right] \right\} \tag{A.9}$$

A porta CNOT será aplicada apenas no qubit alvo que acompanha o qubit de controle $\beta \begin{pmatrix} 1 \\ 0 \end{pmatrix}$:

$$\begin{aligned}\text{CNOT}\,|\psi_0\rangle &= \frac{1}{\sqrt{2}}\left\{\left[\alpha\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}\right]+\left[\beta\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&1&1&0\end{pmatrix}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}\right]\right\}\\ &= \frac{1}{\sqrt{2}}\left\{\left[\alpha\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}\right]+\left[\beta\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right]\right\}\end{aligned} \tag{A.10}$$

Está portanto definido o estado $|\psi_1\rangle$. A próxima etapa, consiste na aplicação da porta H no qubit $|\psi\rangle$, de modo que:

$$\begin{aligned}\text{H}\,|\psi_1\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\left(\alpha\begin{pmatrix}1\\0\end{pmatrix}+\beta\begin{pmatrix}0\\1\end{pmatrix}\right)\\ \text{H}\,\alpha\begin{pmatrix}1\\0\end{pmatrix} &= \frac{1}{2}\alpha\begin{pmatrix}1\\1\end{pmatrix}\\ \text{H}\,\beta\begin{pmatrix}0\\1\end{pmatrix} &= \frac{1}{2}\beta\begin{pmatrix}1\\-1\end{pmatrix}\end{aligned} \tag{A.11}$$

Os resultados de (**??**) e (**??**) podem ser reescritos como:

$$\begin{aligned}\frac{1}{2}\alpha\begin{pmatrix}1\\1\end{pmatrix} &= \frac{1}{2}\alpha\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}\\ \frac{1}{2}\beta\begin{pmatrix}1\\-1\end{pmatrix} &= \frac{1}{2}\beta\begin{pmatrix}1\\0\end{pmatrix}-\begin{pmatrix}0\\1\end{pmatrix}\end{aligned} \tag{A.12}$$

Portanto, o estado $|\psi_2\rangle$ é descrito por:

$$|\psi_2\rangle = \frac{1}{2}\left\{\left[\alpha\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}\right]+\left[\beta\begin{pmatrix}1\\-1\end{pmatrix}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right]\right\} \tag{A.13}$$

Reescrevendo (A.13):

$$|\psi_2\rangle = \frac{1}{2}\left\{\left[\alpha\begin{pmatrix}1\\1\end{pmatrix}\left[\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right]\right]+\left[\beta\begin{pmatrix}1\\-1\end{pmatrix}\left[\begin{pmatrix}0\\1\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\right]\right]\right\} \tag{A.14}$$

No resultado (A.14), podemos evidenciar as seguintes relações:

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}$$
$$\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}$$
$$\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}$$
$$\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \tag{A.15}$$

Substituindo as relações de (A.15) e (A.12) em (A.14):

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}\left\{\left[\alpha\begin{pmatrix}1\\0\end{pmatrix} + \alpha\begin{pmatrix}0\\1\end{pmatrix}\right]\left[\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right) + \left(\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right)\right]\right\}\\ \frac{1}{2}\left\{\left[\beta\begin{pmatrix}1\\0\end{pmatrix} - \beta\begin{pmatrix}0\\1\end{pmatrix}\right]\left[\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right) + \left(\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)\right]\right\}\end{aligned} \tag{A.16}$$

Podemos reorganizar (A.16) evidenciando os termos correspondentes às possíveis medidas realizadas no Local A e no resultado correspondente do par emaranhado no Local B:

$$\begin{aligned}|\psi_2\rangle = &\frac{1}{2}\left\{\left[\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right]\left[\alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}\right]\right\}\\ &+\frac{1}{2}\left\{\left[\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right]\left[\alpha\begin{pmatrix}0\\1\end{pmatrix} - \beta\begin{pmatrix}1\\0\end{pmatrix}\right]\right\}\\ &+\frac{1}{2}\left\{\left[\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right]\left[\alpha\begin{pmatrix}0\\1\end{pmatrix} + \beta\begin{pmatrix}1\\0\end{pmatrix}\right]\right\}\\ &+\frac{1}{2}\left\{\left[\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right]\left[\alpha\begin{pmatrix}1\\0\end{pmatrix} - \beta\begin{pmatrix}0\\1\end{pmatrix}\right]\right\}\end{aligned} \tag{A.17}$$

O resultado acima é exatamente mesmo obtido na Tabela 2.

Referências

CALDEIRA, Amir. Feynman, dissipação e computação quântica. **Revista Brasileira de Ensino de Física [online]**, v. 40, 2018. ISSN 1806-1117. Disponível em: <https://doi.org/10.1590/1806-9126-RBEF-2017-0381>. Citado na p. 13.

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#>. Citado na p. 14.

FAPESP, Revista. **Computador quântico em ação**. 2007. Disponível em: <https://revistapesquisa.fapesp.br/computador-quantico-em-acao/>. Acesso em: 7 abr. 2022. Citado na p. 16.

GADELHA, Julia. **A Evolução dos computadores**. 2015. Disponível em: <http://www.ic.uff.br/~aconci/evolucao.html>. Acesso em: 7 abr. 2022. Citado na p. 13.

IBM. **IBM Newsroom**. 2015. Disponível em: <https://newsroom.ibm.com/>. Acesso em: 7 abr. 2022. Citado na p. 13.

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>. Citado na p. 15.

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>. Citado na p. 14.

KHINCHIN, Aleksandr Yakovlevich. **Mathematical foundations of information theory**. Dover Publications, New York, 1957. Citado na p. 15.

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>. Citado na p. 13.

NIELSEN, Michael A.; CHUANG, Isaac L. **Quantum Computation and Quantum Information**. Cambridge University Press, New York, 2010. Citado nas pp. 16, 17, 19.

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>. Citado nas pp. 14, 16, 17.

SCHUMACHER, Benjamin. Quantum Coding. **Physics Review**, v. 51, 1995. Disponível em: <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.51.2738>. Citado na p. 16.

SEDRA, Adel S.; SMITH, Kenneth C. **Microeletrônica**. Pearson Universidades, 2007. Citado na p. 13.

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>. Citado nas pp. 14, 15.