

**UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA – PATOS DE MINAS
ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES**

GUILHERME ALVES DE AMORIM

**CODIFICAÇÃO DE DADOS POR SOBREPOSIÇÃO DE
ESTADOS**

GUILHERME ALVES DE AMORIM

**CODIFICAÇÃO DE DADOS POR SOBREPOSIÇÃO DE
ESTADOS**

Projeto de pesquisa apresentado à banca examinadora como requisito parcial de avaliação da disciplina de TCC2 da graduação em Engenharia Eletrônica e de Telecomunicações, da Faculdade de Engenharia Elétrica, da Universidade Federal de Uberlândia, Campus Patos de Minas.

Orientador: Prof. Dr. Laurence Rodrigues do Amaral

GUILHERME ALVES DE AMORIM

**CODIFICAÇÃO DE DADOS POR SOBREPOSIÇÃO DE
ESTADOS**

Projeto de pesquisa apresentado à banca examinadora como requisito parcial de avaliação da disciplina de TCC2 da graduação em Engenharia Eletrônica e de Telecomunicações, da Faculdade de Engenharia Elétrica, da Universidade Federal de Uberlândia, Campus Patos de Minas.

Orientador: Prof. Dr. Laurence do Amaral

Patos de Minas, 30 de setembro de 2024

Banca Examinadora:

Prof. Dr. Laurence Rodrigues do Amaral – FACOM/UFU (Orientador)

Prof. Dr. Pedro Luiz Lima Bertarini – FEELT/UFU (Membro 1)

Prof. Dr. Matheus de Souza Gomes – IBTEC/UFU (Membro 2)

AGRADECIMENTOS

Agradeço a todas as pessoas que me auxiliaram na execução do presente trabalho, principalmente ao meu orientador, Prof. Dr. Laurence Rodrigues do Amaral, o qual tive o prazer de desenvolver algumas atividades em conjunto na minha graduação que foram bastante engrandecedoras; e em especial ao Prof. Dr. André dos Anjos, que mesmo sem um vínculo formal ao trabalho dispôs de seu tempo para me esclarecer algumas dúvidas e propor ideias além de um forte incentivo durante a graduação no momento de pandemia. Outro agradecimento especial vai para o Prof. Dr. Ricardo Ávila que também sem um vínculo contribuiu enormemente com materiais didaticamente mais acessíveis para fundamentar a minha pesquisa, sem os quais o projeto não seria o mesmo. Agradeço também a todos os docentes que tive durante minha formação, que de uma forma ou de outra me contribuíram no meu conhecimento.

Agradeço eternamente à minha família que com todas as dificuldades nunca mediram esforços para que nunca me faltasse condições e apoio em todos os meus momentos de empasse. Em especial a minha mãe, por tanta ternura e carinho e por ser uma verdadeira guerreira em prol do meu bem. E também ao meu pai, por ser meu porto seguro e estar comigo sempre que necessário.

Agradeço ainda aos vários amigos adquiridos neste percurso, pelos momentos passados, pelo companheirismo e pelo apoio, principalmente a meus dois colegas Caio Séjour e Raphael Santos que se tornaram companheiros inseparáveis que levarei para o resto da vida.

Por fim agradeço minha companheira Carol, que foi fonte de encorajamento, força e inspiração fundamental para a realização deste trabalho com sua presença constante, amor e apoio em todos os momentos. Obrigado por estar ao meu lado em cada passo desta jornada. Sua contribuição para este trabalho, e para minha vida, é inestimável.

RESUMO

Recentemente, tem se falado muito em uma nova área da computação chamada computação quântica. Muita dessa repercussão vem pelo termo quântica que é visto como sinônimo de ciência de ponta e, conseqüentemente, tecnologia de ponta, de forma a se fazer imaginar que a computação quântica é uma evolução direta e a substituta da computação clássica, o que não é verdade.

O presente trabalho faz um estudo básico sobre o funcionamento de dispositivos cujo hardware opera valendo-se fenômenos que acontecem com grandezas na escala quântica, elencando quais os benefícios e dificuldades de implementação de tal tecnologia, com o foco principal na exploração da possibilidade de usá-la para transmissão de dados.

Palavras-chave: Computação quântica. Informação quântica. *Qubit*. Codificação de dados. Transmissão de dados.

ABSTRACT

There has been a lot of talk recently in a new area of computing called quantum computing. Much of this repercussion comes from the term quantum, which always is associated with cutting-edge science and technology, what makes us imagine that quantum computing is a direct evolution and replacement of classical computing, which is not true.

The present work makes a basic study on the functioning of devices whose hardware operates using phenomena that happen with quantities on the quantum scale, listing the benefits and difficulties of implementing such technology, with the main focus on exploring the possibility of using it for data transmission.

Keywords: Quantum computing. Quantum information. Qubit. Data encoding. Data transmission.

LISTA DE QUADROS E TABELAS

Figura 2.1 – Esfera de Bloch.....	19
Figura 2.2 – Especificações do computador utilizado.....	26
Figura 4.1 – Sistema de um estado misto com quatro bases de medição.....	37
Figura 4.2 – FFT do sinal original.....	42

LISTA DE ABREVIATURAS E SIGLAS

BER	Taxa de Erro de Bit
QKD	Quantum Key Distribution
Qubit	Bit quântico
Qiskit	Quantum Information Software Development Kit

Lista de Símbolos

$ \dots\rangle$	BRA (Vetor coluna)
$\langle\dots $	KET (Vetor linha)
$ \dots $	Norma
$\mathbb{C}^2$	Conjunto dos números complexos de duas dimensões
$\langle\dots \dots\rangle$	Produto interno
$\otimes$	Produto tensorial
$ \dots\rangle\langle\dots $	Produto vetorial

SUMÁRIO

1. INTRODUÇÃO	12
1.1 TEMA DO PROJETO	13
1.2 PROBLEMATIZAÇÃO	13
1.3 HIPÓTESES	16
1.4 OBJETIVOS	16
1.4.1 Objetivos Gerais	16
1.4.2 Objetivos Específicos	16
1.5 JUSTIFICATIVAS	17
1.6 CONSIDERAÇÕES FINAIS	17
2. DESENVOLVIMENTO TEORICO.....	18
2.1 BITS E QUBITS	18
2.2 ESPAÇO VETORIAL COMPLEXO	19
2.3 ESTADOS DE UM QUBIT	20
2.3.1 Sobreposição de estados	20
2.3.2 Emaranhamento	21
2.4 ESFERA DE BLOCH.....	22
2.5 <i>QUANTUM GATES</i>	24
2.6 INFORMAÇÃO QUÂNTICA.....	25
2.6.1 Teoremas da Informação Quântica	26
2.6.2 Transmissão de Informação quântica	27
2.7 CONSIDERAÇÕES FINAIS	28
3. MATERIAIS E MÉTODOS	29
3.1. O HARDWARE	29
3.2. MATLAB.....	30
3.3. QISKIT	31
3.4. JUPYTER NOTEBOOK	31

3.5.	CONSIDERAÇÕES FINAIS	31
4.	RESULTADOS	32
4.1.	OPERADOR DENSIDADE	32
4.2.	CODIFICAÇÃO	34
4.3.	PREPARAÇÃO DO SINAL	36
4.4.	CODIFICAÇÃO COM QUBITS.....	38
5.	CONCLUSÃO E TRABALHOS FUTUROS	39
5.1.	CONCLUSÃO	39
5.2.	TRABALHOS FUTUROS	40
	REFERÊNCIAS.....	41
	APÊNDICES.....	42
	APÊNDICE 1: Código do Matlab.....	43
	APÊNDICE 2: Código do Qiskit	44

1. INTRODUÇÃO

A computação quântica, uma fronteira emergente na ciência da computação, está se tornando cada vez menos misteriosa e mais acessível. Embora não seja projetada para substituir completamente a computação clássica, acredita-se que ela possa servir como um acréscimo valioso, ampliando as capacidades da computação como a conhecemos.

A distinção da computação quântica reside em seu elemento fundamental, o bit quântico, ou qubit. Este se diferencia do bit convencional da computação clássica por sua habilidade de não ser limitado apenas aos dois estados de 0 e 1. Em contrapartida, um qubit pode assumir valores probabilísticos de uma superposição desses estados. Esta característica probabilística permite que os problemas computacionais sejam abordados sob uma perspectiva diferente da lógica binária, o que pode ser vantajoso para a solução de determinados problemas.

Adicionalmente, a partir desta nova concepção de um bit e todos os seus estados, surge também a possibilidade de usar esses estados de maneira mais eficiente quando se trata de armazenamento de informação. Considerando que existem não apenas dois, mas vários valores que o qubit pode assumir, ele pode, conseqüentemente, representar mais informação.

No entanto, manter o qubit neste estado de superposição é uma tarefa complexa, pois exige condições laboratoriais extremamente precisas. Isso é necessário para garantir que o sistema físico que representa o qubit não interaja com seus arredores a ponto de que a função de onda colapse para um dos dois estados convencionais, o que o transformaria novamente em um bit clássico com dois valores possíveis.

A transmissão do qubit em um estado sobreposto é ainda mais delicada, pois exige muita integridade do canal de comunicação. No entanto, estudos recentes estão demonstrando avanços na capacidade de transmitir qubits, o que abre espaço para uma nova área da teoria da comunicação, que alguns estão chamando de internet quântica. Esta é uma área promissora que pode revolucionar a forma como a informação é transmitida e processada, abrindo novas possibilidades para a computação e a comunicação no futuro.

A computação quântica, embora ainda esteja em seus estágios iniciais de desenvolvimento, já está mostrando seu potencial para transformar a maneira como processamos e armazenamos informações. A capacidade de um qubit de existir em

vários estados ao mesmo tempo, conhecida como superposição, abre novas possibilidades para o processamento de informações. Isso poderia levar a avanços significativos em áreas como criptografia, otimização de problemas e simulação de sistemas quânticos.

No entanto, a computação quântica também apresenta desafios significativos. A natureza delicada dos qubits e a necessidade de manter condições laboratoriais extremamente precisas para preservar seu estado de superposição são obstáculos significativos. Além disso, a transmissão de qubits requer canais de comunicação de alta integridade para evitar a perda de informações.

Apesar desses desafios, os avanços recentes na capacidade de transmitir qubits estão abrindo novas possibilidades para a comunicação quântica. Isso poderia levar ao desenvolvimento de uma “internet quântica”, onde as informações podem ser transmitidas e processadas de maneiras que não são possíveis com a tecnologia atual.

Em conclusão, a computação quântica é uma área de pesquisa empolgante e promissora que tem o potencial de transformar a maneira como processamos e armazenamos informações. Embora ainda esteja em seus estágios iniciais, os avanços recentes sugerem um futuro brilhante para esta tecnologia emergente.

1.1 TEMA DO PROJETO

Este projeto de pesquisa se concentra em um estudo aprofundado do armazenamento de informação em qubits. Adicionalmente, aborda a viabilidade de um sistema de comunicação que utiliza a sobreposição de estados. Uma comparação é feita entre esses sistemas de comunicação quântica e os sistemas de telecomunicação convencionais atualmente em uso. O tema se situa no campo da ciência da computação, especificamente na interseção da computação quântica e telecomunicações.

1.2 PROBLEMATIZAÇÃO

A computação quântica, sem dúvida, é um dos temas mais discutidos e relevantes na atualidade. Este campo emergente da ciência da computação já conquistou

seu lugar no mercado global de tecnologia, com gigantes da indústria como Google e IBM liderando a corrida. Ambas as empresas estão em uma competição acirrada para lançar o primeiro computador quântico de uso comercial, o que poderia revolucionar a maneira como processamos informações.

Essas empresas não estão apenas desenvolvendo tecnologia quântica, mas também estão tornando-a acessível para a comunidade científica e acadêmica. Elas disponibilizaram plataformas com hardwares quânticos gratuitamente para o público. Essas plataformas permitem que pesquisadores e estudantes testem e desenvolvam algoritmos quânticos, proporcionando uma oportunidade única para aprender e contribuir para este campo em rápido crescimento.

Além disso, Google e IBM estão investindo em educação e formação, fornecendo uma variedade de materiais de estudo para ajudar a próxima geração de cientistas da computação quântica. Isso indica claramente a direção em que essas empresas líderes em tecnologia estão direcionando seus investimentos. Também destaca uma preocupação crescente com a possível falta futura de profissionais qualificados em computação quântica.

A competição no campo da computação quântica não se limita apenas ao setor comercial. Ela também tem implicações geopolíticas significativas, envolvendo duas das maiores potências mundiais: os Estados Unidos da América (EUA) e a China. Ambos os países estão profundamente envolvidos no que alguns especialistas estão chamando de “corrida quântica”.

Esta corrida é uma competição global para dominar a tecnologia quântica, que tem o potencial de redefinir a paisagem tecnológica e geopolítica. Os EUA e a China, em particular, estão investindo pesadamente em pesquisa e desenvolvimento nesta área.

A China, por exemplo, investiu uma quantia impressionante de 10 bilhões de dólares em pesquisas relacionadas à computação quântica entre os anos de 2017 e 2020 (1). Este investimento maciço demonstra o compromisso da China em se tornar uma líder global em tecnologia quântica.

A computação quântica não é apenas uma questão de avanço tecnológico, mas também uma questão de poder e influência geopolítica. A corrida quântica entre os EUA e a China é um reflexo disso, com ambos os países investindo bilhões para garantir uma posição de liderança neste campo.

Além da corrida para o desenvolvimento de computadores quânticos, a literatura científica também apresenta propostas de protocolos para redes quânticas. Estes protocolos têm o potencial de revolucionar a forma como as informações são transmitidas e processadas.

No campo comercial, já existem aplicações práticas da computação quântica, especialmente na área de criptografia de dados. Um exemplo notável é o *Quantum Key Distribution* (QKD), um método de criptografia que utiliza princípios quânticos para garantir a segurança das informações. O QKD já está em uso em algumas áreas, demonstrando a viabilidade e o potencial da computação quântica.

Empresas de tecnologia reconhecidas, como a Ericsson, já reconhecem o impacto significativo que a computação quântica pode ter na segurança das redes móveis (2, 3, 4, 5). A capacidade de processar e transmitir informações de maneira segura é fundamental para a infraestrutura de redes móveis, e a computação quântica oferece novas e poderosas ferramentas para melhorar essa segurança.

Portanto, a computação quântica não é apenas uma área de pesquisa acadêmica, mas também uma tecnologia emergente com aplicações práticas e comerciais. Seu impacto já pode ser visto em áreas como criptografia de dados e segurança de redes móveis, e é provável que seu alcance continue a se expandir à medida que a tecnologia continua a se desenvolver.

A evolução das aplicações de telecomunicações com o uso de conceitos de computação quântica é uma realidade em progresso. A transmissão de dados utilizando qubits, que é uma abordagem mais complexa em comparação com os métodos tradicionais, é um avanço que já está sendo explorado e estudado intensivamente.

Este avanço traz consigo um desafio significativo: como armazenar dados em um qubit? Portanto, a questão de como codificar dados usando qubits é de grande importância. A codificação de dados em qubits deve levar em consideração as propriedades quânticas únicas para maximizar a eficiência e a segurança da transmissão de dados. Este é um campo de pesquisa ativo e os avanços nesta área têm o potencial de revolucionar a forma como transmitimos e armazenamos informações.

1.3 HIPÓTESES

Sabe-se que, um qubit, diferentemente de um bit clássico, possui infinitos estados de sobreposição entre os estados tradicionais de 1 e 0. Esses estados extras podem também ser utilizados como uma forma de se representar informação, como um bit clássico.

Existem características únicas na computação quântica, como a decoerência e os teoremas da informação quântica, que são considerações importantes no desenvolvimento de sistemas de armazenamento e processamento de informações baseados em qubits (2).

Portanto, pode-se pressupor que os qubits oferecem um novo universo de possibilidades para o armazenamento e processamento de informações.

1.4 OBJETIVOS

1.4.1 Objetivos Gerais

Este trabalho tem como objetivo geral fazer um estudo aprofundado de tecnologias de computação quântica aplicadas na codificação de dados utilizando qubits.

1.4.2 Objetivos Específicos

- Estudar formas de se representar informação em qubits;
- Propor um modelo de representação e simulá-lo, na plataforma *Quantum Information Software Development Kit* (Qiskit) da empresa IBM;
- Fazer simulações no *software* Matlab para representar efeitos de decoerência, e aspectos relacionados à qualidade da comunicação tais como a taxa de erro de bits (BER);
- Comparar o modelo proposto com modelos de computação clássica levando em consideração os parâmetros da simulação;

- Além de analisar a viabilidade técnica da utilização de tecnologias quânticas em sistemas de telecomunicações, suas vantagens e desvantagens.

1.5 JUSTIFICATIVAS

Com o avanço das pesquisas em transmissão de qubits e simulação de canais quânticos, o estudo atual se torna relevante no campo das telecomunicações. A exploração de métodos para armazenar informações em qubits é crucial e será implementada à medida que as tecnologias de transmissão evoluem.

Além disso, este estudo acompanha o desenvolvimento de novas pesquisas em telecomunicações, como a teoria da informação quântica e conceitos inovadores, como as *quantum networks* (6,7). Esses avanços representam um marco importante na evolução das telecomunicações e têm o potencial de transformar a maneira como as informações são transmitidas e processadas. Portanto, a importância deste estudo é inegável, pois contribui para o progresso contínuo neste campo em rápida evolução.

1.6 CONSIDERAÇÕES FINAIS

Neste capítulo foi feita uma breve introdução ao tema e o cada vez mais crescente uso da computação quântica para que fosse possível discorrer sobre qual a ideia o propósito principal deste trabalho, dada a problematização apresentada. Também foi proposto neste capítulo algumas hipóteses sobre o que se espera obter ao final da pesquisa.

No próximo capítulos, alguns conceitos iniciais sobre a computação quântica serão abordados, no intuito de fundamentar uma base de conceitos científicos que se fazem necessários para o bom entendimento do presente trabalho.

2. DESENVOLVIMENTO TEORICO

2.1 BITS E QUBITS

Na teoria da informação clássica, o bit, que é uma abreviação para BInary digiT, serve como a unidade básica e fundamental de informação em dispositivos computacionais. Este conceito é a pedra angular da teoria da computação clássica, que moldou o desenvolvimento da tecnologia da informação como a conhecemos hoje.

Na computação clássica, o bit é uma variável que pode assumir apenas dois estados lógicos possíveis, que são 0 e 1. Esta dualidade é o que permite a representação de informações em sistemas digitais. Cada bit representa um estado distinto, e a combinação de vários bits permite a representação de uma ampla gama de informações.

Além disso, os bits têm várias outras interpretações que se estendem além dos valores numéricos de 0 e 1. Por exemplo, em linguagens de programação, os bits são frequentemente usados para representar variáveis booleanas, que podem assumir os valores de verdadeiro ou falso. Esta interpretação é fundamental para a lógica de programação e para a tomada de decisões em algoritmos.

Em outro contexto, na eletrônica transistorizada, os bits são usados para indicar se uma corrente está ou não circulando em um circuito. Neste caso, os estados de 0 e 1 são interpretados como ‘desligado’ e ‘ligado’, respectivamente. Esta interpretação é crucial para o funcionamento de dispositivos eletrônicos, desde computadores até smartphones e outros dispositivos inteligentes.

Portanto, embora o bit possa parecer um conceito simples à primeira vista, ele desempenha um papel fundamental na computação clássica. A versatilidade do bit e sua capacidade de representar uma variedade de estados e informações é o que torna a computação digital possível (8).

Na computação quântica, o qubit é o análogo do bit clássico e também serve como a unidade fundamental e básica. O qubit é um sistema quântico de dois níveis, o que significa que ele pode existir em qualquer estado entre os dois níveis, ao contrário de um bit clássico que pode existir apenas em um dos dois estados.

Este sistema é estudado a partir da perspectiva da mecânica quântica, que permite a ocorrência de fenômenos como a superposição. A superposição permite que um qubit exista em um estado que é uma combinação dos estados 0 e 1. Isso significa

que um qubit, considerando que um nível equivalha a 1 e o outro a 0, pode assumir infinitos estados de sobreposição entre 0 e 1.

Essa capacidade de existir em múltiplos estados simultaneamente é o que dá aos qubits seu poder e o que permite que a computação quântica tenha o potencial de resolver certos problemas muito mais rapidamente do que a computação clássica.

2.2 ESPAÇO VETORIAL COMPLEXO

Um qubit pode ser matematicamente representado como um vetor de estado situado em um espaço bidimensional de Hilbert, que é uma subestrutura de um espaço vetorial complexo. O espaço de Hilbert é um espaço vetorial que é equipado com um produto interno que permite definir ângulos e comprimentos. Além disso, é completo, o que significa que uma sequência de vetores que se aproxima de um limite resultará nesse limite estando também no espaço. A norma, que é uma medida do tamanho ou do comprimento de um vetor, é derivada desse produto interno (8, 9).

A notação de Dirac, também conhecida como notação bra-ket, é uma linguagem matemática usada na mecânica quântica. Ela é útil para representar vetores de estado e operadores de maneira concisa e clara.

Com essa notação, os vetores de estado que correspondem aos estados 0 e 1 na computação clássica são expressos da seguinte maneira:

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

e

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2)$$

Esses vetores constituem a base para a representação dos estados em um sistema quântico. Diz-se que um par de estados $|\gamma\rangle$ e $|\phi\rangle$, pertencentes a $\mathbb{C}^2$ constitui uma base ortogonal se e somente se o produto interno entre eles for nulo, em termos matemáticos, se $\langle\gamma|\phi\rangle = 0$. Caso a base, além de ortogonal seja formada por vetores de norma unitária, esta base é dita como ortonormal.

Logo, podemos afirmar que os estados $|0\rangle$ e $|1\rangle$ formam uma base ortonormal pois é fácil ver que $\langle 0|1\rangle = 0$ e $\langle 0|0\rangle = \langle 1|1\rangle = 1$. Pode-se a princípio definir infinitas bases ortonormais, porém a base $|0\rangle$ e $|1\rangle$ é comumente a mais utilizada na computação

quântica, e recebe o nome de base canônica. Uma propriedade muito importante de uma base ortonormal é que com ela é possível escrever qualquer outro vetor estado que também pertença ao espaço vetorial complexo bidimensional (8).

2.3 ESTADOS DE UM QUBIT

Uma partícula descrita pela mecânica quântica possui certas grandezas que são descritas por uma função de onda que diz qual a probabilidade de se medir aquela grandeza em algum ou alguns valores.

De maneira análoga acontece com o qubit, onde a propriedade a ser medida é o estado do mesmo, e os valores em que se pode encontrar são os estados que compõem a base ortonormal escolhida.

Uma característica importante sobre o qubit é que os todos os estados que ele pode assumir é convencionalmente normalizado, ou seja, seja um estado $|\psi\rangle$ de um qubit qualquer, tem-se a propriedade (8):

$$\langle\psi|\psi\rangle = 1 \quad (3)$$

2.3.1 Sobreposição de estados

Quando se mede o valor de um qubit em uma base ortonormal, o valor obtido irá invariavelmente ser um dos estados da base. Na mecânica quântica esse fenômeno é chamado de colapso da função de onda, em que ela não mais representa a probabilidade de se medir um dos estados, mas passa a assumir um único valor (o medido) com probabilidade de 100% (8).

É importante salientar que antes que se faça a medição, o qubit está sob um regime probabilístico entre os estados da base com uma probabilidade associada a cada um deles. Quando isto ocorre, diz-se que o qubit está em uma sobreposição de estados, ou em um estado sobreposto (8).

Levando em consideração a base canônica para representar um estado sobreposto $|\psi\rangle$ em notação de Dirac, temos que o mesmo pode ser expresso como:

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (4)$$

Onde a e b são números complexos em que $|a|^2$ representa a probabilidade de se medir o qubit no estado $|0\rangle$ e $|b|^2$ a probabilidade de se medir o qubit no estado $|1\rangle$ (8).

Como em uma medida o qubit tem apenas dois estados possíveis para assumir, os estados da base, as probabilidades do colapso em cada um destes são complementares, logo:

$$|a|^2 + |b|^2 = 1 \quad (5)$$

2.3.2 Emaranhamento

Quanto se tem um sistema com mais de um qubit, outro fenômeno que passível de ocorrência é o entrelaçamento quântico entre eles, que ocorre em certos estados de múltiplos qubits onde os qubits possuem estados que após medida estão sempre correlacionados (10).

Suponha um sistema formado por dois qubits. Tomando a notação de produtos tensoriais como $|\gamma\rangle \otimes |\phi\rangle = |\gamma\phi\rangle$, pode-se escrever um estado geral de um estado $|\psi\rangle$ destes dois qubits na base canônica como:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad (6)$$

Onde a , b , c e d assim como no estado de um qubit são números complexos, o quadrado de suas normas também representa a probabilidade de se medir o sistema em cada um dos respectivos estados respeitando a relação:

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1 \quad (7)$$

Partindo deste caso geral para alguns mais específicos, para fins de exemplo, observa-se o seguinte estado:

$$|\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \quad (8)$$

Pode-se notar, que através da propriedade de fatoração do produto tensorial, é possível separar e escrever este estado também da seguinte forma:

$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \quad (9)$$

O que faz deste estado um chamado estado separável. Existem alguns estados em que não existe essa possibilidade de fatoração, não sendo separáveis. É o caso do seguinte estado:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \quad (10)$$

Neste caso, a separabilidade com um único produto tensorial é impossível, sendo possível escrevê-lo com dois, como no terceiro membro da igualdade. Em estados de múltiplos qubits com essa característica, quando o primeiro ou o segundo qubit colapsa, só existe uma única possibilidade de estado para o outro qubit, pois o estado não é separável por não ter a coincidência de valores para o primeiro e o segundo qubit (11).

Em outras palavras, o estado de um dos qubits após uma medida está intrinsecamente relacionado com o outro, e quando a medida é realizada, o outro qubit é colapsado no único estado possível para tal, tornando possível o conhecimento instantâneo do par com uma medida apenas. Este fenômeno é conhecido como emaranhamento quântico e a estes estados dá-se o nome de estados emaranhados (11).

2.4 ESFERA DE BLOCH

Existe também uma forma de representar o estado de um qubit que permite uma visualização geométrica e traz consequentemente algumas vantagens no entendimento deste estado e também como algumas operações o modificam. Esta forma consiste em um mapeamento esférico chamado Esfera de Bloch.

Como o estado genérico de um qubit, uma vez escolhida a uma base pode ser descrito apenas por dois números, que são suas amplitudes complexas, como visto na equação (4), é possível escrevê-los em sua forma polar, com um módulo e um ângulo (ou fase), o que resulta na equação:

$$|\psi\rangle = r_0 e^{i\phi_0} |0\rangle + r_1 e^{i\phi_1} |1\rangle \quad (11)$$

Pode-se fazer a seguinte operação para eliminar a fase associada ao estado:

$$e^{-i\phi_0} |\psi\rangle = e^{-i\phi_0} [r_0 e^{i\phi_0} |0\rangle + r_1 e^{i\phi_1} |1\rangle] = r_0 |0\rangle + r_1 e^{i(\phi_1 - \phi_0)} |1\rangle \quad (12)$$

$$|\psi\rangle = e^{i\phi_0} [r_0 |0\rangle + r_1 e^{i(\phi_1 - \phi_0)} |1\rangle] \quad (13)$$

Como $e^{i\phi_0}$ é uma fase que multiplica todo o estado, ela é chamada de fase global e analisando do ponto de vista probabilístico, esta fase não altera as características de um vetor estado, o que nos leva a seguinte equação (9):

$$|\psi\rangle = r_0 |0\rangle + r_1 e^{i\phi} |1\rangle \quad (14)$$

Fazendo $\phi_1 - \phi_0 = \phi$, levando-se em consideração a condição vista na equação (5) vê-se que:

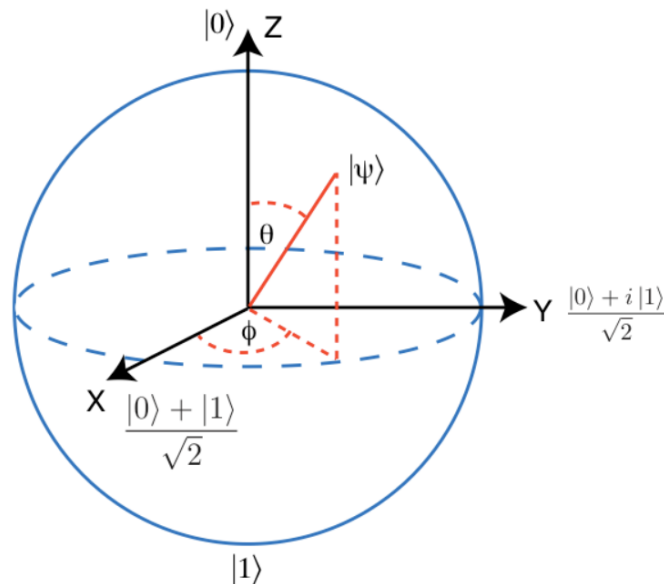
$$r_0^2 + r_1^2 = 1 \quad (15)$$

Valendo-se da primeira relação fundamental da trigonometria é possível chamar r_0 de $\cos \theta$, r_1 de $\sin \theta$ ainda respeitando a equação (15). Com isso pode-se escrever a equação (14) da seguinte forma:

$$|\psi\rangle = \cos \theta |0\rangle + e^{i\phi} \sin \theta |1\rangle \quad (16)$$

Com esta parametrização, é possível representar o estado do qubit na esfera de Bloch. É importante notar que, assim como antes, para descrever completamente o vetor estado (que nesta representação também pode ser chamado de vetor de Bloch) são necessárias apenas duas variáveis, θ e ϕ .

Figura 2.1: Esfera de Bloch



Fonte: (12)

Na Figura 2.1 vemos a representação das duas variáveis que parametrizam o qubit na representação da esfera de Bloch, em que θ é o ângulo do vetor estado em relação ao eixo Z, compreendido entre 0 e π ; e ϕ em relação ao eixo X, compreendido entre 0 e 2π (8).

Nota-se que θ e ϕ têm o mesmo papel de latitude e longitude respectivamente quando se trata da posição no globo terrestre e, assim como na esfera de Bloch, são necessários apenas estes dois parâmetros pra localizar qualquer ponto no globo. Os estados $|0\rangle$ e $|1\rangle$ da base canônica são os polos norte e sul da esfera, respectivamente (8).

2.5 QUANTUM GATES

Os *quantum gates* ou portas lógicas quânticas são o análogo às portas lógicas da computação clássica em que se faz operações de lógica booleana com um bit ou entre bits manipulando a informação binária neles contidos como as operações NOT, AND ou OR (11).

Todas as operações passíveis de serem feitas em bits clássicos podem também ser definidas para a um qubit, uma vez que o espaço de Hilbert compreende os estados colapsados de $|0\rangle$ e $|1\rangle$ que podem ser interpretados como o 0 e 1 da lógica binária. Porém o bit quântico não possui somente estes estados, mas sim uma gama de infinitas sobreposições entre eles, o que torna possível uma série de operações que levam o qubit de um estado a outro (8,11).

Tomando como representação a esfera de Bloch, uma porta lógica quântica que age em apenas um qubit pode ser qualquer operação que faça uma rotação nessa esfera, ou no vetor de Bloch em si, o que altera o estado do qubit em relação à base canônica. Existem também portas que atuam em sistemas de múltiplos qubits, onde nestes a representação geométrica na esfera de Bloch se torna pouco ou nada útil.

Matematicamente, uma porta lógica quântica é uma matriz U dita como operador unitário, ou seja, com a característica de o resultado da operação $U^\dagger U$ ser uma matriz identidade e, para aplicá-la em um qubit basta multiplicá-la pelo vetor estado. Pelas condições de multiplicação de matrizes e vetores, chega-se à conclusão de que a matriz U deve ter tamanho $2^n \times 2^n$, onde n é o número de qubits que formam o estado a ser operado (10).

Dentre algumas portas importantes temos a porta Hadamard, que quando aplicada nos estados dos polos, leva para estados maximamente sobrepostos, com 50% de chance de se medir $|0\rangle$ e 50% de chance de se medir $|1\rangle$ (estados posicionados no “equador” da esfera de Bloch). A matriz unitária que representa a porta de Hadamard é (12):

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (17)$$

Outra porta que desempenha uma função muito importante é a porta CNOT ou *Controlled-NOT*, que atua em sistemas de dois qubits e tem o poder de tornar estados

não-emaranhados em estados emaranhados e vice-versa. A sua matriz unitária é dada por (11):

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (18)$$

Existem diversas outras portas lógicas quântica, porém estas serão definidas à medida que o presente trabalho demandar.

2.6 INFORMAÇÃO QUÂNTICA

Existe uma área da ciência chamada teoria da informação que tem como objeto de estudo de como se dá o armazenamento, transmissão e processamento de informação. Para bits clássicos, esta teoria já se encontra bem desenvolvida e é muito utilizada nos mais diversos tipos de produtos e serviços tanto no setor de telecomunicações quanto em diversos outros que necessitam trabalhar com dados sob quaisquer circunstâncias (11).

Análoga a essa teoria “clássica” da informação, pode-se desenvolver a partir da mesma uma teoria da informação que consegue lidar com os bits quânticos, contemplando todos os seus estados intermediários de sobreposição, os considerando como potenciais portadores de informação, e valendo de suas peculiaridades como possíveis ferramentas para certos tipos processamento e transmissão de dados (11).

O que Claude Shannon propôs na sua teoria da informação em 1948, foi como mensurar a quantidade de informação em um sistema através de um conceito que determinou de entropia. A entropia mede basicamente qual é o grau de previsibilidade no valor de uma unidade de informação, isto é, quanto mais alta a entropia, maior é a certeza da informação contida e quanto menor, mais aleatória é esta informação (13).

Sabendo que o conteúdo desta informação é agora tratado de uma maneira probabilística, e que os próprios estados sobrepostos dos bits quânticos também são estados probabilísticos, é natural se assumir que os mesmos podem servir como armazenadores de informação. Juntando esta premissa com a já conhecida teoria da informação, cunha-se o termo “Teoria de Informação Quântica” (11).

O passo inicial para se colocar em prática esta teoria é, no entanto, bem desafiador: realizar um qubit tão funcional quanto os bits clássicos. Dentre as várias maneiras possíveis de se fazer isso, a forma que será abordada neste trabalho levará em consideração um fóton e sua polarização como um sistema que representa um qubit. Desta forma, assim como na representação matemática, onde são necessárias apenas duas variáveis para se caracterizar qualquer estado possível do qubit, sejam elas as amplitudes a e b como mostrado na equação (8) ou os ângulos θ e ϕ como na equação (16); a polarização deste fóton também contempla estes dois parâmetros, onde a polarização horizontal ou vertical representa uma variável e a polarização circular para a esquerda ou para a direita representa a outra. É importante salientar a existência da natureza quântica deste sistema, pois não se sabe qual a polarização de um fóton antes de medi-la através de um filtro polarizador e, diferentemente de um feixe de luz que cuja passagem ou não pelo filtro é parcial e regida pela lei de Malus, o fóton é uma partícula fundamental, não divisível e seu comportamento não está sujeito a uma passagem parcial pelo filtro. O que acontece em uma medição é o fóton assumir a polarização contrária do filtro e ser barrado ou passar e adquirir a polarização do mesmo (11).

O complicado em termos de praticidade em tal sistema é o fóton em sobreposição não interagir com o canal de transmissão, pois isso pode alterar o estado sobreposto e consequentemente a informação que será carregada na sobreposição em um fenômeno conhecido como decoerência (8).

2.6.1 Teoremas da Informação Quântica

A área da informação quântica está contida dentro da mecânica quântica e, devido a isso existem alguns teoremas decorrentes de conceitos fundamentais da mesma que, uma vez estabelecidos proíbem a ocorrência de alguns fenômenos e a existência de alguns processos que na computação quântica se resumem a algoritmos e certos dispositivos. A seguir serão descritos de forma breve, três teoremas primordiais quando se trata de informação quântica (11).

O primeiro deles é o “Teorema na não-clonagem” que diz que é impossível que algum dispositivo receba um estado sobreposto desconhecido e aleatório e após isso

copiar o estado de forma idêntica fornecendo-o depois de tal processo. Em outras palavras, o que o teorema diz é que é impossível gerar uma cópia exata de um estado quântico (11).

O segundo (que não possui um nome em específico) diz que é impossível determinar com total exatidão o estado quântico desconhecido de um qubit, independentemente da quantidade de medidas que sejam feitas. O que se pode ter, é uma aproximação com um grau de probabilidade que pode ser aumentado tanto quanto se queira, porém sem nunca a 100% de certeza, pois para isso, o número de medidas a serem feitas tende ao infinito (11).

O terceiro e último (também sem um nome) diz que é impossível diferenciar estados quânticos que não sejam ortogonais de forma inequívoca (11).

Estes são os três teoremas fundamentais e básicos da teoria da informação quântica e, apesar desta área ser calcada em três teoremas restritivos, isto é, limitantes e impeditivos em relação à realização de processos, se verá nos próximos capítulos deste trabalho que existe na área um grande teor de aplicabilidade (11).

2.6.2 Transmissão de Informação quântica

Quando um processo que envia a informação que intermedia a transmissão de alguma mensagem entre um transmissor (remetente) e um receptor (destinatário) recebe o nome de canal. Canais quânticos de informação podem ser definidos como conceitos de preparação de estados no transmissor e medidas no receptor (11).

De acordo com os teoremas vistos anteriormente, percebe-se que um entendimento importante quando se trata da determinação de um estado está em compreender as probabilidades que estão associadas às tais medidas. A partir de um aspecto básico da mecânica quântica que recebe o nome de “causalidade estatística”, que é um tipo mais fraco de causalidade que o determinismo, pode-se chegar na conclusão de que um qubit tem a probabilidade de ser mensurado em um estado quântico específico sempre menor que 1. Por sua vez, em um sistema binário clássico, após uma medida, um bit está exclusivamente em um de dois únicos estados estabelecidos e possíveis com 100% de certeza (11).

Por isso, a forma como se é preparado um qubit em sobreposição para que o mesmo porte informação tem influência causal nas medições que serão feitas no receptor, determinando apenas a probabilidade da ocorrência de algum estado quântico específico quando este chega no destinatário dado o estado preparado na parte remetente (11).

Da mesma maneira, dado um estado medido qualquer no receptor, para que se possa medir qual estado que foi preparado no transmissor e o seu origem, está associada a tal medida, uma probabilidade que pode ser calculada, fazendo com que a medida tenha na verdade um caráter de inferência com um grau de certeza, não sendo, portanto, uma determinação exata (11).

2.7 CONSIDERAÇÕES FINAIS

Neste capítulo foi construída uma fundamentação teórica básica de conceitos essenciais para que se possa compreender a pesquisa proposta. É necessário salientar que, a computação quântica é uma área cujo pleno entendimento provém de uma base de conhecimentos extremamente mais densa e cientificamente ampla.

Nos próximos capítulos, será explicado o método em que a pesquisa será embasada, os recursos utilizados e o cronograma a ser seguido.

3. MATERIAIS E MÉTODOS

O presente trabalho terá como metodologia de desenvolvimento uma pesquisa científica prévia dos conhecimentos necessários dentro da área de teoria da informação de Shannon, de teoria da informação quântica e computação quântica para se determinar formas de se utilizar de estados sobrepostos como carregadores de informação, baseando-se em artigos científicos, livros base do assunto, referenciais de empresas que possuem computadores quânticos funcionais à disposição de pesquisadores, e materiais de estudo de universidades renomadas que estudam o tema.

Uma vez consolidada essa base, será feito um *script* no software Matlab preparando um pequeno áudio para servir de mensagem que será transmitida utilizando qubits em um canal quântico. Tal preparo consiste em utilizar uma codificação de linha para transformar o sinal em um sinal binário e gerar um arquivo contendo apenas zeros e uns.

Diante de tal arquivo, será utilizadas ferramentas gratuitamente disponíveis para que possa ser feita uma implementação de codificação de informação em qubits rodando em computadores quânticos reais, preparando tal informação para ser trafegada em um canal quântico funcional que possa manter a coerência dos qubits.

Para que se faça a realização do trabalho, alguns recursos básicos serão necessários, detalhados a seguir.

3.1. O HARDWARE

Para a simulação será utilizado um computador pessoal *laptop* com 500 GB de SSD; um processador Intel® Core™ i7-11800H com clock máximo de 2.30 GHz, memória RAM instalada de 16 GB composta por dois pentes DDR5 de 8 GB cada um. O sistema operacional instalado e utilizado no hardware estabelecido é o Microsoft Windows 11 Home Single Language 23H2 de 64 bits.

Figura 2.2: Especificações do computador utilizado

 Especificações do dispositivo	
Nome do dispositivo	Nitro5
Processador	11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz 2.30 GHz
RAM instalada	16,0 GB (utilizável: 15,8 GB)
ID do dispositivo	DA616C75-81FA-40E1-9F54-EA8FFA916789
ID do Produto	00342-43317-49881-AAOEM
Tipo de sistema	Sistema operacional de 64 bits, processador baseado em x64
Caneta e toque	Nenhuma entrada à caneta ou por toque disponível para este vídeo
Links relacionados Domínio ou grupo de trabalho Proteção do sistema Configurações avançadas	
 Especificações do Windows	
Edição	Windows 11 Home Single Language
Versão	23H2
Instalado em	13/10/2023
Compilação do SO	22631.3447
Experiência	Windows Feature Experience Pack 1000.22688.1000.0
Contrato de Serviços Microsoft Termos de Licença de Software da Microsoft	

Fonte: Próprio autor

3.2. MATLAB

O Matlab é uma plataforma desenvolvida pela MathWorks® para a criação de algoritmos e cálculos numéricos, amplamente utilizada na engenharia e em muitas outras áreas da ciência exata.

Para o presente projeto, será utilizada a versão 2024a para que sejam feitas simulações de cálculos e métricas de maneira paralela ao Qiskit.

3.3. QISKIT

O Qiskit é um SDK de código aberto para se trabalhar com um *Hardware* quântico no nível de circuitos, pulsos e algoritmos utilizando a linguagem de programação python.

Ele tem por objetivo principal construir uma pilha de softwares de forma a facilitar o uso de computadores quânticos, sem a necessidade de ter um alto nível de habilidade ou conhecimento na área. O mesmo permite o projeto e a execução de experimentos e aplicações em máquinas clássicas rodando simuladores de hardwares quânticos ou mesmo enviá-los para rodar em um computador quântico real e já está sendo utilizado em todo o mundo, na área educacional, comercial ou entre entusiastas (14).

Será utilizado neste trabalho, a versão 0.26.1 de tal SDK.

3.4. JUPYTER NOTEBOOK

O Jupyter Notebook é uma aplicação da web de código aberto e uso gratuito da Google que permite a criação, execução e compartilhamento de algoritmos. Com ele é possível compilar códigos em diversas linguagens, porém será utilizado única e exclusivamente para a compilação de códigos Python.

3.5. CONSIDERAÇÕES FINAIS

Foram utilizados para a realização deste trabalho, poucos recursos de *hardware* e os recursos de *software*, em sua maioria são todos gratuitos, com exceção do Matlab, gratuito apenas por um mês em sua versão *trial*.

A configuração do sistema se deu de maneira bem simplificada, com toda a documentação e procedimentos necessários descritos em suas respectivas páginas de referência, com destaque ao qiskit, que tem dispõe de vídeos tutoriais detalhando passo a passo a sua configuração inicial e a de todas as ferramentas adjacentes necessárias.

4. RESULTADOS

4.1. OPERADOR DENSIDADE

Dada uma fonte emissora de qubits, e sabendo do segundo teorema visto na Seção 2.6.1 que diz que é impossível reproduzir o mesmo estado quântico com exatidão absoluta, o ato de representar o qubit apenas como o estado de uma função de onda tal qual na equação (4) pela notação de Dirac ou na equação (16) representado como um vetor de Bloch, pode se mostrar limitante quando se trata de um sistemas quânticos de transmissão de informação, pois uma vez que tanto no transmissor quanto no receptor os respectivos estados preparados e inferidos possuem uma probabilidade intrínseca, a fonte poderá emitir qubits que sejam tão semelhantes quanto se queira, porém nunca iguais.

Posto isso, torna-se necessário uma representação mais eficaz, geral e completa de um estado necessita de mais de um qubit, de forma a representá-lo de uma forma mais geral e com suas probabilidades associadas. Para que esta representação seja entendida, é necessário entender o conceito de operador densidade de um estado $|\psi\rangle$ genérico.

Denota-se o operador densidade como ρ e é obtido através da seguinte operação a ser feita com um estado $|\psi\rangle$ do produto vetorial do estado com ele mesmo:

$$\rho = |\psi\rangle\langle\psi| \quad (19)$$

Com a Equação (19), a definição de $|\psi\rangle$ dada na Equação (4), a sua consequência, $\langle\psi| = a^*\langle 0| + b^*\langle 1|$ e as definições de $|0\rangle$ e $|1\rangle$ nas equações (1) e (2), tem-se que:

$$\rho = \left\{ a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \{ a^* [1 \ 0] + b^* [0 \ 1] \}$$

$$\rho = \left\{ \begin{bmatrix} a \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ b \end{bmatrix} \right\} \{ [a^* \ 0] + [0 \ b^*] \}$$

$$\rho = \begin{bmatrix} a \\ b \end{bmatrix} [a^* \ b^*]$$

$$\rho = \begin{bmatrix} aa^* & ab^* \\ ba^* & bb^* \end{bmatrix}$$

$$\rho = \begin{bmatrix} |a|^2 & ab^* \\ ba^* & |b|^2 \end{bmatrix} \quad (20)$$

Nota-se que os elementos da diagonal principal da matriz, ρ_{11} e ρ_{22} são justamente a probabilidade de se medir o estado $|\psi\rangle$ em $|0\rangle$ ou $|1\rangle$ respectivamente e a eles se dão o nome de população. Já os termos da diagonal secundária da matriz, ρ_{12} e ρ_{21} são justamente a coerência do sistema quântico, o que significa que quando nulas significa que a função de onda do estado já está colapsada e o qubit voltou a ser um sistema binário clássico sem sobreposição, ou seja, um bit convencional. Este é o fenômeno da decoerência citado de maneira breve nos capítulos 1 e 2 deste trabalho.

Uma vez que o qubit se trata de um sistema quântico probabilístico e o operador densidade ter um formalismo capaz de fornecer as informações de probabilidade de mensuração através da população e da condição da sobreposição através da coerência, ele se torna um parâmetro com métricas bastante convencionais para ser analisar a qualidade de uma comunicação e resultados obtidos.

Porém como a fonte de qubits é incapaz de replicar o mesmo estado duas ou mais vezes e a redundância se faz necessária para uma inferência mais acurada no receptor, uma sequência de qubits que deveriam representar a mesma sobreposição (formando o que se chama de estado puro), na verdade são sobreposições ligeiramente diferentes o que é denominado de “estado misto” de dois ou mais qubits que compõe a sequência.

Com isso, o operador densidade que antes era determinado por apenas um qubit agora leva em consideração todos os qubits, conforme mostra a seguinte equação:

$$\rho = \sum_{i=0}^n (p_i |\psi_i\rangle \langle \psi_i|) \quad (21)$$

Onde n é a quantidade de qubits enviados em uma sequência, i é o índice de cada qubit e p é a probabilidade de ocorrência do estado $|\psi_i\rangle$.

É importante retificar que existem também parâmetros para se medir o grau de pureza de um estado, ou seja, saber o quão puro ou misto ele é e pode servir também como um indicador de resultado.

4.2. CODIFICAÇÃO

Apesar dos teoremas vistos na Seção 2.6.1, a informação quântica tem muitas aplicações em uso e já é possível se transmitir qubits utilizando luz, mesmo que de uma maneira na qual ainda não seja tão eficiente (6). Esta possibilidade, atrelada às aplicações possíveis apenas através da computação quântica fundamenta esse trabalho e uma codificação viável é esperada como um resultado plausível.

Espera-se que, com um canal de comunicação que não cause uma decorrência significativa o estado sobreposto e a informação nele contida cheguem no receptor de tal maneira que uma inferência precisa seja feita e que a comunicação tenha um grau de assertividade suficiente para que seja eficaz.

Como visto em (6), tal sistema de transmissão pode ser dado como um fóton viajando em uma fibra ótica, em que o sistema quântico é estabelecido utilizando a polarização do mesmo e as medidas são feitas com filtros polarizadores. Desta forma, um fóton representa um qubit e uma sequência de qubits que compõem um estado misto é representada por um conjunto de fótons.

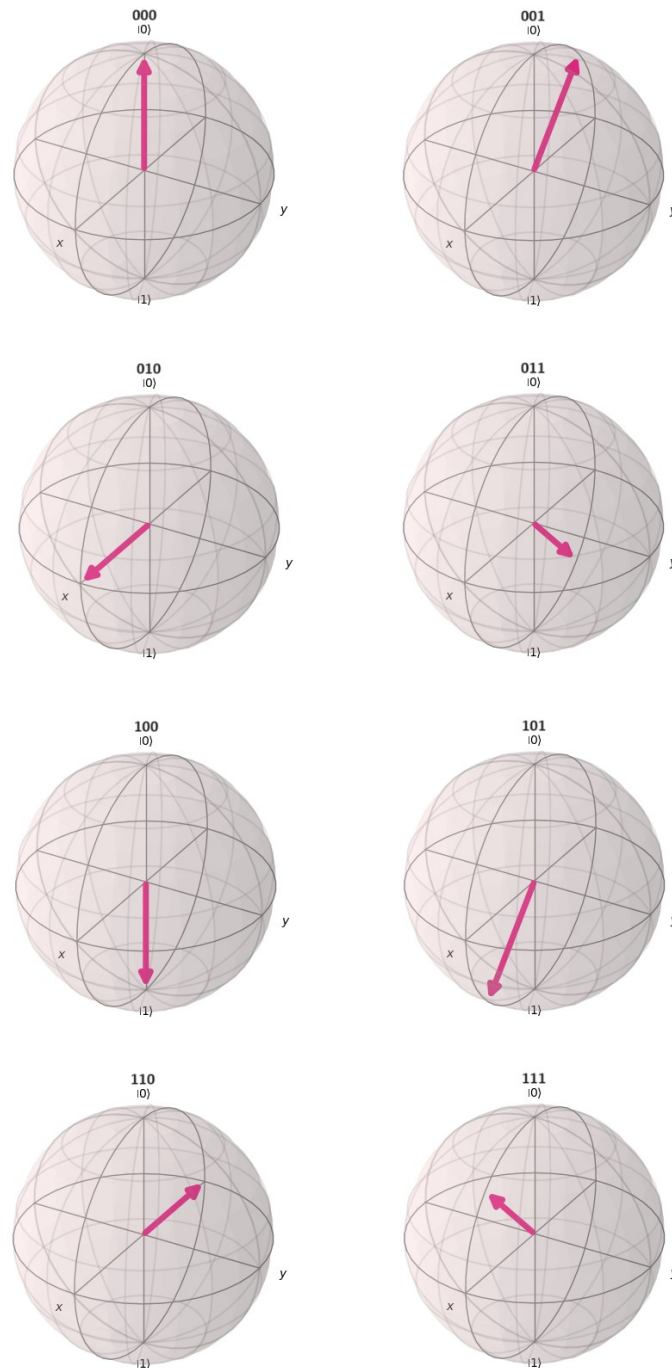
Estes fótons viajam pela fibra óptica mantendo o seu estado sobreposto e, ao chegar no receptor, suas polarizações são medidas em diversas bases ortogonais colapsando a função de onda do qubit para um dos estados binários das diversas bases. O estado que apresentar, após as medidas uma maior incidência de colapso tem maior chance de ser o estado preparado e enviado pelo transmissor.

A quantidade de informação contida no qubit pode ser estabelecida de acordo com a quantidade de bases ortogonais definidas a priori, ou seja, quanto mais bases forem utilizadas no sistema, mais estados são possíveis de serem preparados no transmissor e passíveis de inferência no receptor; porém espera-se que haja um limitante: quanto mais bases se utiliza, mais estados possíveis existem e os mesmos ficam mais semelhantes entre si, e dependendo da decoerência que os qubits sofrem devido ao sistema, definir muitas bases e muitos estados pode levar a uma inferência inacurada. Este fenômeno pode ser facilmente entendido quando utilizado a esfera de Bloch como representação de um qubit.

Tomando-se como exemplo uma definição de uma codificação de informação utilizando quatro bases ortogonais para se medir um estado misto, existem oito estados

possíveis de inferência após as medidas, pois como o sistema é binário, cada base é composta por dois estados distintos e opostos.

Figura 4.1: Estados possíveis do sistema de um estado misto com quatro bases de medição



Fonte: Próprio autor

Na figura 4.1, gerada por códigos de programação em linguagem Python no ambiente de desenvolvimento qiskit é mostrada, utilizando a esfera de Bloch para um entendimento de caráter mais visual, os oito estados possíveis estados que um estado misto no sistema anteriormente proposto. Estes oito estados podem, caso definido previamente, representar respectivamente a informação contida em um sistema de três bits clássicos, que são: 000, 001, 010, 011, 100, 101, 110 e 111. Nota-se que com esta quantidade de bases de medição estabelecidas seria possível representar com um único estado misto de qubit uma quantidade de informação que utilizando a computação clássica seriam necessários três bits. Além do mais, é possível aumentar estas 4 bases para quantas mais o sistema físico permitir de forma que os erros fiquem dentro de níveis aceitáveis.

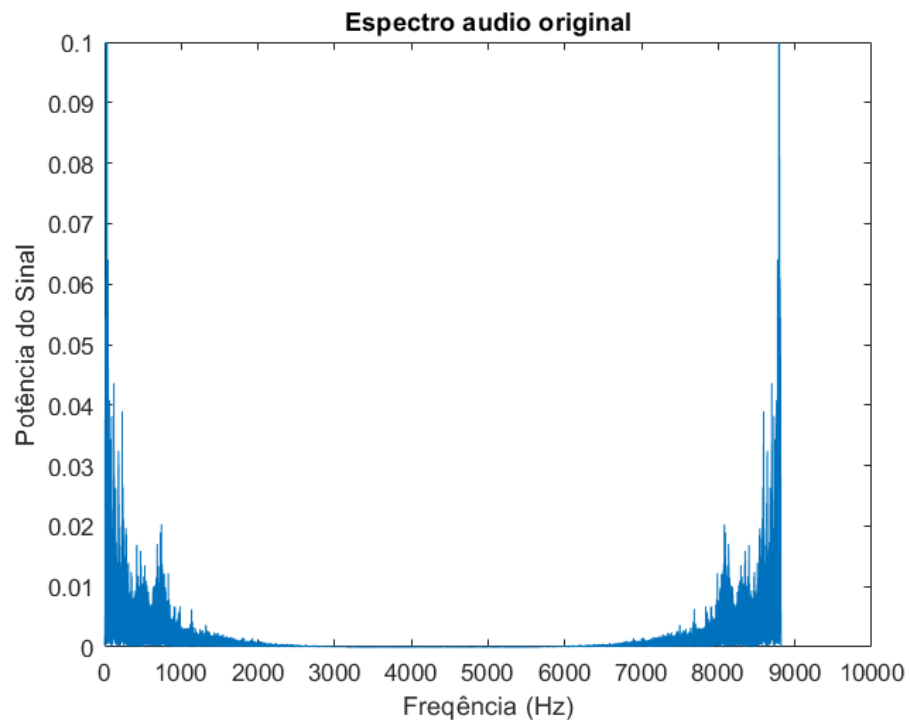
Uma vez definidas as bases e seus valores correspondentes (neste caso, trios de bits convencionais), será feito uma simulação de como é possível a transmissão de qubits. Para tal, foi escolhida como mensagem a ser transmitida, um trecho da música *Bohemian Rhapsody*, escrita pela banda *Queen* em 1975. Note que esta simulação parte da premissa de que haja um canal quântico funcional, não considerando os erros que podem ocorrer em tal parte do sistema de comunicação.

4.3. PREPARAÇÃO DO SINAL

Antes de representar o sinal com qubits foi feita uma preparação com o mesmo. Utilizando o Matlab, foi utilizada uma codificação de linha do sinal.

Inicia-se com a leitura do arquivo de áudio. Os canais esquerdo e direito do sinal de áudio estéreo são extraídos e a média deles é calculada para obter um sinal de áudio mono. Posteriormente, é feito o cálculo da Transformada Rápida de Fourier (FFT) do sinal de áudio original e o resultado é mostrado na figura 4.2. Isso permite a visualização do espectro de frequências do sinal de áudio.

Figura 4.2: FFT do Sinal Original



Fonte: Próprio autor

Após a análise do espectro, aplica-se um filtro Chebyshev tipo I ao sinal de áudio. Este filtro tem como objetivo remover frequências acima de 4000 Hz. O sinal de áudio filtrado é então normalizado para garantir que sua amplitude máxima seja 1 e, em seguida, calcula-se e plota-se a FFT do sinal de áudio filtrado, permitindo a visualização do espectro de frequências do sinal após a filtragem. O sinal de áudio filtrado e normalizado é salvo em um novo arquivo de áudio.

O passo seguinte é a subamostragem do sinal de áudio filtrado. Isso é realizado reduzindo a taxa de amostragem do sinal por um fator especificado. O sinal de áudio subamostrado é salvo em um novo arquivo de áudio.

Realiza-se então uma operação de quantização no sinal de áudio subamostrado. Isso envolve a normalização do sinal, a quantização dele em um número especificado de níveis e, em seguida, a desnormalização do resultado.

Finalmente, converte-se o sinal quantizado em uma sequência de bits que é salva em um arquivo de nome "Binario.txt". Tal vetor é o que será utilizado no código que implementará a parte que utiliza bits quânticos para representar esta mensagem.

É possível ver todo o código do Matlab no Apêndice 1.

4.4. CODIFICAÇÃO COM QUBITS

Inicialmente, são criados oito circuitos quânticos, cada um com um qubit. Em seguida, são aplicadas rotações a cada um desses qubits, colocando-os em estados distribuídos uniformemente na esfera de Bloch. As rotações são realizadas em torno dos eixos y e z , com ângulos θ e ϕ , os mesmos ângulos da presentes na equação (16), que são calculados de forma com que tais estados fiquem os mais separados possíveis um do outro. Os estados dos qubits são os que estão na figura 4.1, mostrada anteriormente.

Após a aplicação das rotações, é aberto o arquivo de texto chamado “Binario.txt” que foi gerado no Matlab e convertido em um vetor de dígitos binários, ou seja, bits convencionais. Como o intuito deste trabalho é mostrar a capacidade de armazenamento de um qubit em comparado com um bit convencional, esses bits são agrupados em grupos de três para serem transportados utilizando apenas um qubit convencional.

Em seguida, é realizada uma varredura no vetor, analisando o conteúdo de cada elemento, tomando ciência de qual das oito combinações de um conjunto de três bits se trata. Associa-se então ao estado quântico correspondente, da maneira com que a figura 4.1 arbitra.

Por fim é montado um novo vetor onde cada elemento, ao invés de ser composto por três bits, convencionais, é composto pelas características do estado de um único bit quântico contendo portanto, de acordo com a codificação proposta da mensagem, a mesma informação contida nos três bits.

É possível ver toda a codificação em Python feita no qiskit no Apêndice 2.

5. CONCLUSÃO E TRABALHOS FUTUROS

5.1. CONCLUSÃO

A proposta de modelo de comunicação apresentada, que combina a computação clássica e a computação quântica, é um exemplo viável de como essas duas tecnologias podem trabalhar juntas para resolver problemas complexos. A escolha de representar três bits convencionais com um qubit é feita por conveniência neste modelo, mas um qubit tem o potencial de representar muito mais informações devido à sua capacidade de existir em uma superposição de estados, o que na esfera de bloch seriam infinitas possibilidades de vetores. Isso é uma das características fundamentais da computação quântica que a torna tão poderosa e promissora.

O código Matlab desempenha um papel crucial na preparação da mensagem de áudio para transmissão neste experimento. Ele realiza várias operações de processamento de sinal, para converter a mensagem de áudio em uma sequência de bits que pode ser facilmente manipulada pelo código Python.

O Qiskit desempenhou um papel fundamental na ponte entre a computação clássica e a computação quântica neste modelo de comunicação proposto. No contexto deste experimento, permitiu a manipulação e a preparação dos estados quânticos em hardwares quânticos reais. Isso possibilitou a representação da mensagem de áudio como uma sequência de estados quânticos, prontos para serem transmitidos em um sistema quântico.

Nota-se que este modelo de comunicação está alinhado com a visão atual de muitos cientistas de que a computação quântica não substituirá a computação clássica (visto que ela é mais eficiente para alguns tipos de problemas, não todos), mas sim complementar e melhorará suas capacidades. Assim como os dois códigos trabalham juntos neste modelo, a computação clássica e a computação quântica podem trabalhar juntas para realizar tarefas que seriam impossíveis ou impraticáveis para cada uma delas sozinha.

É importante frisar no entanto, a implementação prática deste modelo de comunicação enfrenta vários desafios. O canal de transmissão quântica deve ser capaz de preservar a coerência quântica dos estados quânticos durante a transmissão, o que pode ser difícil devido à decoerência e ao ruído do canal que não foram levadas em

consideração neste trabalho. Além disso, a preparação, preservação e a medição precisas dos estados quânticos são tarefas não triviais que requerem tecnologia avançada e controle preciso.

Em resumo, este modelo de comunicação proposto é um exemplo interessante de como a computação clássica e a computação quântica podem ser combinadas para criar novas possibilidades para a transmissão de informações. Embora ainda haja muitos desafios a serem superados, este modelo oferece uma visão do futuro potencial da comunicação quântica.

5.2. TRABALHOS FUTUROS

Para a trabalhos futuros, podem simulados canais de comunicação quântica levando em consideração a decoerência que os mesmos implicam aos qubits e analisar de maneira mais quantitativa os resultados, utilizando as métricas e parâmetros de medidas vistos na Seção 4.1.

Outra área que poderia ser explorada é a implementação de técnicas de correção de erros quânticos no código. Isso poderia ajudar a mitigar os efeitos da decoerência e outros erros que podem ocorrer durante a transmissão. Além disso, a eficácia de diferentes protocolos de codificação quântica poderia ser investigada para otimizar a eficiência da transmissão.

Também podem ser explorados os erros e efeitos decorridos da inserção de cada vez mais bases e estados possíveis, a fim de encontrar um ponto ótimo de acordo com as características de cada canal.

REFERÊNCIAS

- 1 G. PASCUAL, Manuel. IBM apresenta processador quântico com potência que não pode mais ser simulada por computadores convencionais. **El País**. Disponível em: <https://brasil.elpais.com/tecnologia/2021-11-16/ibm-apresenta-processador-quantico-com-potencia-que-nao-pode-mais-ser-simulada-por-computador-convencionais.html>. Acesso em: 16 jan. 2022.

- 2 KOZLOWSKI, W.; DAHLBERG, A.; WEHNER, S. **Designing a quantum network protocol**. Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies, 23 nov. 2020. Disponível em: <https://doi.org/10.1145/3386367.3431293>

- 3 KOZLOWSKI, W.; WEHNER, S. **Towards Large-Scale Quantum Networks**. Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, 25 set. 2019. Disponível <https://doi.org/10.1145/3345312.3345497>.

- 4 ROBERTS, G. L. et al. **Modulator-Free Coherent-One-Way Quantum Key Distribution**. Laser & Photonics Reviews, v. 11, n. 4, p. 1700067, 23 jun. 2017 Disponível em: <https://doi.org/10.1002/lpor.201700067>.

- 5 P. MATTSSON, John; SMEETS, Ben; THORMARKER, Erik. Quantum technology and its impact on security in mobile networks. **Ericsson**. Disponível em: <https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/ensuring-security-in-mobile-networks-post-quantum>. Acesso em: 16 jan. 2022.

- 6 CHEN, X. **The capacity of transmitting atomic qubit with light**. Quantum Information Processing, v. 9, n. 4, p. 451–462, 4 nov. 2009 Disponível em: <https://doi.org/10.48550/arXiv.0802.2327>.

- 7 FANG, K. et al. **Quantum Channel Simulation and the Channel's Smooth Max-Information**. 2018 IEEE International Symposium on Information Theory (ISIT), jun. 2018 Disponível em: <https://doi.org/10.1109/ISIT.2018.8437484>.

- 8 YANOFISKY, Noson S.; MANNUCCI, Mirco A.. **Quantum Computing for Computer Scientists**. Cambridge University Press, v. 3, 2008. Disponível em: <https://doi.org/10.1017/CBO9780511813887>.

- 9 AMARAL, Bárbara; T. BARAVIERA, Alexandre; O. T. CUNHA, Marcelo. **Mecânica Quântica para Matemáticos em Formação**. IMPA, 2011.

- 10 JESUS, G. F. DE et al. Computação quântica: uma abordagem para a graduação usando o Qiskit. **Revista Brasileira de Ensino de Física**, v. 43, 2021 Disponível em: <https://doi.org/10.1590/1806-9126-rbef-2021-0033>.

- 11 JORIO, Ado; FROSSARD, João Vitor. **Material de Estudos para Mecânica Quântica**. 2019.

- 12 LEARNING Quantum Computation. Qiskit. Disponível em: <https://qiskit.org/learn>. Acesso em: 17 jan. 2022.

- 13 SHANNON, C. E. **A Mathematical Theory of Communication**. The Bell System Technical Journal, 1948. Disponível em: <https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf>. Acesso em: 16 jan. 2022.

- 14 Documentação do Qiskit 0.26.1. Disponível em: https://qiskit.org/documentation/stable/0.26/locale/pt_BR/index.html. Acesso em: 18/07/2022.

APÊNDICES

APÊNDICE 1: Código do Matlab

```

tic
%% Limpeza
clear all; close all; clc;
%% Leitura do audio
[y,F] = audioread('mammamia.mp3');
yl = y(:,1);
yr = y(:,2);
y = (yl+yr)/2;
am = 5; % Número de vezes que a quantidade de amostras do vetor originaln será
dividida por

T = 1/F;
Fs = F/am;
Ts = 1/Fs;

y_am = zeros(1,round(length(y)/am));
v_t = 0:T:length(y)*T; % Vetor tempo original
v_t_am = 0:Ts:length(y_am)*Ts; % Vetor tempo amostrado

%% FFT sinal original
eixo_f = Fs*(1:(length(y)))/length(y);
plot(eixo_f,10*abs(fft(y)/length(y)));
axis([0 10000 0 0.1]);
title('Espectro audio original');
xlabel('Frequência (Hz)');
ylabel('Potência do Sinal');

%% Filtragem
Rp = 0.1;
n = 8;
fc = 7400;
Wp = fc/Fs;
[b,a] = cheby1(n,Rp,Wp); % ordem ripple e frequencia
y_f = filter(b,a,y);
y_f_norm = (1/max(y_f))*y_f;

%% FFT sinal filtrado
figure
plot(eixo_f,10*abs(fft(y_f)/length(y)));
axis([0 10000 0 0.1])
title('Espectro audio filtrado')
xlabel('Frequência (Hz)')
ylabel('Potência do Sinal')
audiowrite('sinalfiltrado.wav',y_f_norm,F);

%% Subamostrando
y_am = y_f_norm(1:am:end);
audiowrite('mammamia_subamostrado.wav',y_am,Fs);

%% Quantização
y_norm = (y_am + 1)/2; % normalização

n=8; % Número de Bits
L=(2^n)-1; % numero de níveis

```

```

y_norm = y_norm*L;

y_arr = round(y_norm); % Arredondando para um múltiplo de L

y_quant = 2*((y_arr)/L)-1; % Desnormalizando

figure;
audiowrite('mammamia_quantizado.wav',y_quant,Fs);
stem(y_quant);
grid;
xlabel('Tempo (s)'); % eixo horizontal
ylabel('Amplitude (W)'); % eixo vertical
legend('Sinal Amostrado');

%% Codificação

h=[]; % Criação de um vetor de zeros e uns a partir dos níveis de quantização
for i=1:length(y_arr)
    d=dec2bin(y_arr(i),n);
    h=[h double(d)-48];
end

%% NRZ

h_nrz = h;
stairs([h_nrz h_nrz(length(h_nrz))], 'linewidth',2);
axis([1 length(h_nrz)+1 -0.5 1.5]);
grid;
xlabel('Bits'); % eixo horizontal
ylabel('Amplitude (W)'); % eixo vertical
legend('Sinal NRZ Bipolar');

binario = h_nrz;

%gravando .txt
fileID = fopen('Binario.txt','w');
fprintf(fileID,'%2u',binario);
fprintf(fileID,'%d',binario);
fclose(fileID);
%fim da gravação
toc

```

APÊNDICE 2: Código do Qiskit

```

from qiskit import QuantumCircuit, transpile, IBMQ
from qiskit.tools.visualization import plot_histogram, plot_state_city
from qiskit.tools.monitor import job_monitor
from qiskit_ibm_runtime import QiskitRuntimeService
from qiskit.quantum_info import Statevector
from qiskit.visualization import plot_bloch_multivector
import matplotlib.pyplot as plt
import numpy as np
import os
%matplotlib inline

# Criando 1 circuito quântico com oito qubits
qc000 = QuantumCircuit(1)
qc001 = QuantumCircuit(1)
qc010 = QuantumCircuit(1)
qc011 = QuantumCircuit(1)
qc100 = QuantumCircuit(1)
qc101 = QuantumCircuit(1)
qc110 = QuantumCircuit(1)
qc111 = QuantumCircuit(1)

# Aplicando rotações para distribuir os qubits uniformemente na esfera de Bloch
theta = np.pi * (0 / 4) # Rotação em torno do eixo y
phi = np.pi * (0 % 2) # Rotação em torno do eixo z
qc000.ry(theta, 0)
qc000.rz(phi, 0)

theta = np.pi * (1 / 4) # Rotação em torno do eixo y
phi = np.pi * (1 % 2) # Rotação em torno do eixo z
qc001.ry(theta, 0)
qc001.rz(phi, 0)

theta = np.pi * (2 / 4) # Rotação em torno do eixo y
phi = np.pi * (2 % 2) # Rotação em torno do eixo z
qc010.ry(theta, 0)
qc010.rz(phi, 0)

theta = np.pi * (3 / 4) # Rotação em torno do eixo y
phi = np.pi * (3 % 2) # Rotação em torno do eixo z
qc011.ry(theta, 0)
qc011.rz(phi, 0)

theta = np.pi * (4 / 4) # Rotação em torno do eixo y
phi = np.pi * (4 % 2) # Rotação em torno do eixo z
qc100.ry(theta, 0)
qc100.rz(phi, 0)

theta = np.pi * (5 / 4) # Rotação em torno do eixo y
phi = np.pi * (5 % 2) # Rotação em torno do eixo z
qc101.ry(theta, 0)
qc101.rz(phi, 0)

theta = np.pi * (6 / 4) # Rotação em torno do eixo y
phi = np.pi * (6 % 2) # Rotação em torno do eixo z
qc110.ry(theta, 0)
qc110.rz(phi, 0)

theta = np.pi * (7 / 4) # Rotação em torno do eixo y

```

```

phi = np.pi * (7 % 2) # Rotação em torno do eixo z
qc111.ry(theta, 0)
qc111.rz(phi, 0)

# Criando vetor de estado a partir do circuito e plotando na esfera de Bloch
#qc = transpile(qc111)
#state = Statevector.from_instruction(qc)
#plot_bloch_multivector(state)

path = 'Documents\MATLAB\Binario.txt'
with open(path, 'r') as arquivo:
    texto = arquivo.read()
binario = [int(digito) for digito in texto if digito in ('0', '1')]
binario_agrupado = [binario[n:n+3] for n in range(0, len(binario), 3)] #agrupa de
3 em 3
states = [0] * len(binario_agrupado) #Cria um vetor do tamanho de
binario_agrupado
for i in range(len(binario_agrupado)):
    # Use um dicionário para mapear cada caso possível para uma ação
    switch = {
        (0, 0, 0): [Statevector.from_instruction(transpile(qc000))],
        (0, 0, 1): [Statevector.from_instruction(transpile(qc001))],
        (0, 1, 0): [Statevector.from_instruction(transpile(qc010))],
        (0, 1, 1): [Statevector.from_instruction(transpile(qc011))],
        (1, 0, 0): [Statevector.from_instruction(transpile(qc100))],
        (1, 0, 1): [Statevector.from_instruction(transpile(qc101))],
        (1, 1, 0): [Statevector.from_instruction(transpile(qc110))],
        (1, 1, 1): [Statevector.from_instruction(transpile(qc111))],
    }
    states[i] = switch.get(tuple(binario_agrupado[i]), "Caso não encontrado")

#print("Tamanho do binario:", len(binario))
#print("Tamanho do binario agrupado:", len(binario_agrupado))

# Converta o vetor states para string
states_str = '\\n'.join([str(state) for state in states])

# Escreva o vetor states em um arquivo txt
with open('states.txt', 'w') as f:
    f.write(states_str)

# Imprima uma mensagem de sucesso
print("O vetor states foi gravado com sucesso em states.txt")

```