Universidade Federal de Goiás
Instituto de Física

Milena Maria Fernandes

Informação e computação quântica e suas aplicações na física médica

Goiânia
2024

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE FÍSICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome completo da autora: Milena Maria Fernandes

Título do trabalho: Informação e computação quântica e suas aplicações na física médica

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Norton Gomes De Almeida**, **Professor do Magistério Superior**, em 15/07/2024, às 09:03, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Milena Maria Fernandes**, **Discente**, em 15/07/2024, às 13:25, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Milena Maria Fernandes

Informação e computação quântica e suas aplicações na física médica

Trabalho de Conclusão de Curso apresentado à banca examinadora do Instituto de Física da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Bacharel em Física Médica.

Área: Computação Quântica

Orientador: Prof. Dr. Norton Gomes de Almeida

Goiânia
2024

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Fernandes, Milena Maria
Informação e computação quântica e suas aplicações na física médica [manuscrito] / Milena Maria Fernandes. - 2024.
63 f.

Orientador: Prof. Dr. Norton Gomes de Almeida .
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Instituto de Física (IF), Física Médica, Goiânia, 2024.
Bibliografia.
Inclui tabelas, lista de figuras, lista de tabelas.

1. Computação quântica. 2. Física médica . I. Almeida , Norton Gomes de, orient. II. Título.

CDU 53

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE FÍSICA

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos doze dias do mês de julho do ano de 2024 iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado "Informação e computação quântica e suas aplicações na física médica", de autoria de Milena Maria Fernandes, do curso de Bacharelado em Física Médica, do Instituto de Física da UFG. Os trabalhos foram instalados pelo Prof. Dr. Norton Gomes de Almeida (IF/UFG) com a participação dos demais membros da Banca Examinadora: Prof. Dr. Jonas Oliveira da Silva (IF/UFG) e Prof. Dr. Emerson Nobuyuki Itikawa (IF/UFG). Após a apresentação, a banca examinadora realizou a arguição da estudante. Posteriormente, de forma reservada, a Banca Examinadora atribuiu a nota final de 10,0 (dez vírgula zero), tendo sido o TCC considerado aprovado.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Emerson Nobuyuki Itikawa**, **Professor do Magistério Superior**, em 12/07/2024, às 11:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Norton Gomes De Almeida**, **Professor do Magistério Superior**, em 12/07/2024, às 11:01, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Jonas Oliveira Da Silva**, **Professor do Magistério Superior**, em 12/07/2024, às 11:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4601245** e o código CRC **49F05EFD**.

Referência: Processo nº 23070.015577/2024-73 SEI nº 4601245

Dedico este trabalho aos meus pais.

Agradecimentos

Agradeço a Deus por todas as graças concedidas e o consolo necessário para enfrentar essa caminhada.

Agradeço ao meu pai e minha mãe por todos os esforços e investimentos na minha formação profissional e pessoal. Agradeço à minha família pela torcida e felicidade com minhas conquistas.

Agradeço aos colegas de curso que durante muitos anos dividiram comigo os momentos bons e ruins da graduação.

Agradeço ao meu orientador professor Dr. Norton Gomes de Almeida pela paciência e dedicação de me auxiliar em longos anos de pesquisa e na realização deste trabalho.

Agradeço aos professores Drs. Jonas Oliveira e Emerson Nobuyuki por aceitarem participar da banca de avaliação.

Agradeço a todos os professores, amigos, familiares que de alguma forma contribuíram e participaram desta importante fase da minha vida.

Por fim, agradeço a Universidade Federal de Goiás e ao CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) por tornarem esse trabalho possível e pelo auxílio financeiro concedido.

"Nada começa e nada acaba sem seu preço de sofrimento."

– Francisco Thompson

Resumo

A Computação Quântica é uma área de pesquisa emergente e relativamente recente que promete mudar o processamento da informação. Este trabalho tem como objetivo principal estudar os fundamentos da computação e da informação quântica, destacando por fim suas potenciais aplicações e benefícios na física médica. Inicialmente são expostos os fundamentos da computação quântica, incluindo as portas lógicas e os princípios das teorias de informação clássica e quântica. Em seguida o foco se dá no processamento da informação quântica, demonstrando os principais algoritmos e suas finalidades. Além disso, apresenta-se alguns tipos de simuladores quânticos e são realizadas simulações de circuitos em uma plataforma a fim de demonstrar seu funcionamento. Por fim, o trabalho oferece uma visão geral das potenciais contribuições da computação quântica para a física médica, destacando os principais benefícios e dificuldades envolvidas.

Palavras - chave: Computação Quântica, Qbits, Informação, Simulação Computacional, Física Médica.

Abstract

Quantum Computing is an emerging and relatively recent research area that promises to change information processing. The main objective of this work is to study the fundamentals of quantum computing and information, ultimately highlighting their potential applications and benefits in medical physics. Initially, the fundamentals of quantum computing are presented, including logic gates and the principles of classical and quantum information theories. Next, the focus is on quantum information processing, demonstrating the main algorithms and their purposes. Additionally, some types of quantum simulators are presented, and circuit simulations are performed on a platform to demonstrate their functioning. Finally, the work provides an overview of the potential contributions of quantum computing to medical physics, highlighting the main benefits and challenges involved.

Key - words: Quantum Computing, Qbits, Information, Computational Simulation, Medical Physics.

Lista de Figuras

Lista de Tabelas

Sumário

CAPÍTULO 1

Introdução

A ideia de se usar uma máquina para realizar cálculos existe desde o século XVII. O matemático francês Blaise Pascal criou um contador mecânico, que a partir de engrenagens, realizava operações de somas e multiplicações. Apenas em 1890, o norte americano Hermann Hollerith desenvolve o primeiro computador mecânico. A partir disso, os desenvolvimentos concentraram-se em substituir as partes mecânicas por elétricas.

Em 1938 o alemão Konrad Zuse fez o primeiro computador elétrico usando a teoria binária, com os bits 0 e 1, estabelecida por George Boole. A partir de 1936 Alan Mathison Turing cria a teoria da "Máquina de Turing", que através de um número finito de operações, resolvia problemas computacionais. Com o decorrer dos anos e com os diversos avanços na ciência, os computadores passaram de enormes máquinas para objetos cada vez mais compactos e poderosos [2].

Com a evolução da eletrônica, a computação clássica se desenvolveu rapidamente. Em paralelo, com o surgimento da teoria da mecânica quântica no século XX percebeu-se a necessidade de explicar e simular certos fenômenos da natureza. A ideia de um computador quântico veio da dificuldade de simular esses sistemas quânticos em um computador clássico.

1.1 Início da computação quântica

Em 1981, durante uma conferência, o físico Richard Philips Feynman afirma que é impossível representar os resultados da mecânica quântica com um dispositivo universal clássico. Enfatizando que a natureza não é clássica, Feynman sugere a criação de um dispositivo que usasse as leis da mecânica quântica para simular eficientemente os fenômenos quânticos [3].

Em 1985, David Deutsch mostra que o computador quântico universal pode simular perfeitamente qualquer máquina de Turing apresentando os requisitos para simular vários sistemas físicos, reais e teóricos, que estão além do âmbito da máquina

de Turing. Deutsch cria ainda o primeiro algoritmo quântico que utiliza da propriedade do paralelismo para demonstrar a eficiência de um computador quântico [4].

Em 1994, Peter Shor cria um algoritmo para fatorar números inteiros que é executado exponencialmente mais rápido do que o algoritmo clássico. Esse fato despertou grande interesse pois a fatoração possibilita a quebra de criptografia de chave pública relacionadas à segurança do comércio eletrônico. Em 1996, Grover propõe um algoritmo de busca que demonstra que na computação quântica, o tempo para se encontrar um elemento é consideravelmente menor em relação à clássica [5].

Com essas descobertas, o interesse pela computação quântica cresceu no meio científico e ao longo dos anos levou ao desenvolvimento de algoritmos para muitas outras tarefas. Atualmente, a promessa de solucionar problemas com mais facilidade e rapidez e por vezes intratáveis na computação clássica, torna a computação quântica atrativa para vários pesquisadores. O potencial de revolucionar e beneficiar muitas áreas da ciência é a principal motivação para o investimento financeiro e intelectual aplicados à tecnologia quântica.

1.2 Corrida para a vantagem quântica

Os principais avanços na computação quântica foram feitos no início do ano 2000. Neste ano, o primeiro computador de 5 qubits foi testado pela Universidade Técnica de Munique. Em 2007, a empresa D-wave Systems afirmou ter desenvolvido um computador quântico de 28 qbits. Desde então diversas empresas começaram a construção de seus hardwares quânticos, iniciando uma "corrida pela vantagem quântica" [6]. A Figura 1.1 mostra um breve histórico da evolução da computação quântica ao longo dos anos.

Em 2019, a empresa Google afirmou ter alcançado a vantagem com a criação do processador quântico Sycamore, de 53 qbits [7]. Outras empresas como Amazon e a Microsoft também investiram na criação de processadores cada vez mais poderosos. A IBM (International Business Machines Corporation) é considerada líder em desenvolvimento da tecnologia quântica. Em 2016 ela foi a primeira a disponibilizar computação quântica em nuvem, permitindo que pesquisadores de diversos lugares do mundo fizessem experimentos num computador quântico real de maneira remota e gratuita. Os investimentos aplicados fazem com que a empresa se desenvolva rapidamente, tendo atualmente o maior chip quântico do mundo com 1.121 bits quânticos, chamado IBM Condor [8].

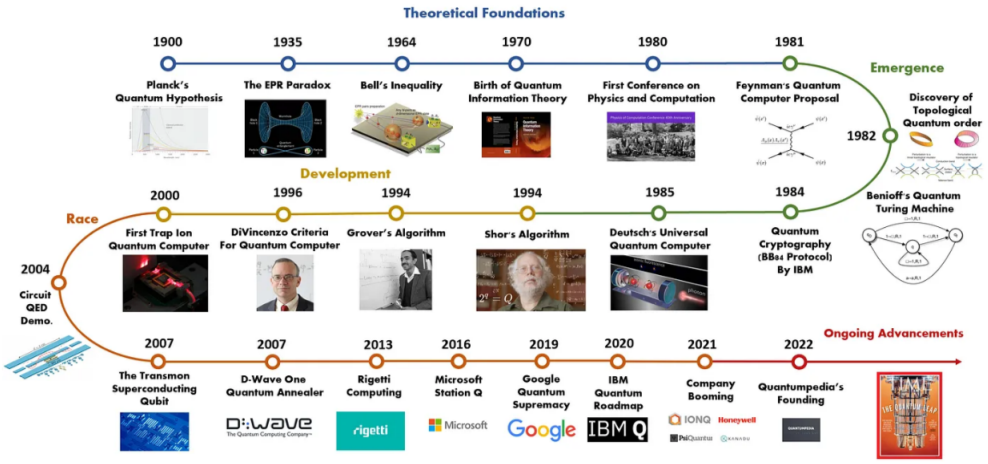

Figura 1.1: Breve história da computação quântica. Retirada de [9].

Em 2023, a IBM implantou oficialmente um computador quântico fora de suas dependências. O IBM Quantum System One instalado na Cleveland Clinic será o primeiro computador quântico do mundo dedicado exclusivamente à pesquisa em saúde, com projetos nas áreas de genômica, saúde populacional, aplicações clínicas e descoberta de medicamentos. Apesar de nenhuma empresa propor formalmente a entrada de seus processadores quânticos no mercado, essa parceria é um marco fundamental para explorar e facilitar o poder computacional quântico em diversas áreas, inclusive à saúde [10].

A computação quântica fornece muitas possibilidades e abordagens para o processamento de informação. Porém ainda não é uma tecnologia amplamente dominada e possui muitos desafios atrelados. Uma das principais dificuldades trata-se dos erros gerados pelas máquias quânticas, relacionados principalmente a interação do sistema quântico com o ambiente. Atualmente, os cientistas investem na correção de tais erros, com a criação de algoritmos de correção de falhas e alterando até mesmo a estrutura física do dispositivo, aperfeiçoando assim a capacidade de processamento.

Espera-se que ao longo dos anos, com a disputa de várias empresas pelo domínio da tecnologia, os computadores quânticos possam ser aproveitados em cada vez mais ramos da ciência. Com sua real eficácia comprovada e futuras investigações, a expectativa é que a tecnologia quântica resulte em dispositivos de processamento de informação muito superiores aos atuais, gerando grandes benefícios para a sociedade.

1.3 Objetivos

Este trabalho tem como objetivo principal estudar os fundamentos da computação e da informação quântica e apresentar as aplicações na física médica. De forma específica:

- Estudar as principais portas lógicas quânticas.
- Estudar os rudimentos de teorias de informação clássica e quântica.

- Estudar os algoritmos quânticos.
- Simular alguns algoritmos e portas lógicas quânticas.
- Compreender e apresentar o potencial da computação quântica na área de física médica.

CAPÍTULO 2

Computação e Informação Quântica

Um computador clássico manipula bits a partir de circuitos elétricos e portas lógicas. Analogamente, um computador quântico opera manipulando a sua unidade fundamental, o qbit, que é preparado, manipulado e medido através de circuitos quânticos baseados em portas lógicas quânticas.

2.1 Bit quântico (qbit)

Na computação clássica, a unidade de informação é conhecida como bit, contração de Binary Digit e representa um estado lógico com dois valores 0 ou 1. Fisicamente esses bits podem ser representados pela presença ou não de tensão elétrica nos componentes eletrônicos, onde a presença de tensão corresponde ao bit 1 (ligado) e ao bit 0 (desligado).

A computação quântica possui estrutura análoga, o bit quântico, usualmente chamado de qbit (ou qubit). A principal diferença é que o bit clássico pode estar somente com um valor armazenado num determinado instante (0 ou 1), já o qbit está numa sobreposição de 0's e 1's num determinado instante, ou seja, 0 e 1 estão armazenados ao mesmo tempo. Assim, um bit quântico é um estado representado por uma combinação linear:

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

onde, α e β são números complexos, que representam amplitudes de probabilidade tais que $|\alpha|^2 + |\beta|^2 = 1$. Os estados $|0\rangle$ e $|1\rangle$ são conhecidos como base computacional e formam uma base ortonormal para este espaço vetorial complexo de duas dimensões [11]. Essa base também pode ser representada na notação matricial:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \mathbf{e} \, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.2}$$

O qbit é representado por dois estados, sendo por isso chamado de sistema de dois níveis. Sendo $\alpha = |\alpha|e^{i\phi}$ e $\beta = |\beta|e^{i\gamma}$, pode-se escrever $|\psi\rangle$ na base computacional, na sua forma mais geral, como:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \tag{2.3}$$

em que a fase global é ignorada. Para que um sistema de dois níveis possa ser utilizado como qbit, ele deve satisfazer as seguintes condições:

- O estado inicial deve poder ser preparado com precisão.
- Deve ser possível transformar um estado em outro através de uma operação unitária.
- Deve ser possível realizar medições na base computacional $|0\rangle, |1\rangle$.

Os infinitos estados possíveis do qbit podem ser associados a pontos localizados na superfície de uma esfera de raio unitário, a esfera de Bloch [12].

2.1.1 Qbit na esfera de Bloch

A Esfera de Bloch é uma representação possível para um qbit em três dimensões. Supondo que o estado de um qbit seja dado por $|\psi\rangle$ (eq. 2.3), uma medição nesse sistema o levará para $|0\rangle$ ou $|1\rangle$ com probabilidades, respectivamente:

$$P_0 = |\langle 0|\psi\rangle|^2 = \left|\cos\frac{\theta}{2}\langle 0|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\langle 0|1\rangle\right|^2 = \cos^2\frac{\theta}{2} \tag{2.4}$$

$$P_1 = |\langle 1|\psi\rangle|^2 = \left|\cos\frac{\theta}{2}\langle 1|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\langle 1|1\rangle\right|^2 = \sin^2\frac{\theta}{2} \tag{2.5}$$

Nota-se que a soma das probabilidades resulta em 1. As coordenadas (x, y, z) da esfera de Bloch podem ser obtidas através de medições. Usando os operadores de Pauli, escritos na base computacional como:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2.6}$$

então, para o estado $|\psi\rangle$ tem-se que:

$$\sigma_x|\psi\rangle = e^{i\phi}\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle \tag{2.7}$$

$$\sigma_y |\psi\rangle = -ie^{i\phi} \sin\frac{\theta}{2} |0\rangle + i \cos\frac{\theta}{2} |1\rangle \tag{2.8}$$

$$\sigma_z |\psi\rangle = \cos\frac{\theta}{2} |0\rangle - e^{i\phi} \cos\frac{\theta}{2} |1\rangle \tag{2.9}$$

Portanto, os seguintes valores esperados para o estado são obtidos:

$$\langle\psi|\sigma_x|\psi\rangle = \langle\psi| \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |\psi\rangle = \sin\theta\cos\phi = x \tag{2.10}$$

$$\langle\psi|\sigma_y|\psi\rangle = \langle\psi| \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} |\psi\rangle = \sin\theta\sin\phi = y \tag{2.11}$$

$$\langle\psi|\sigma_z|\psi\rangle = \langle\psi| \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} |\psi\rangle = \cos\theta = z \tag{2.12}$$

As coordenadas (x, y, z) podem ser obtidas com precisão arbitrária por meio de medições projetivas na base computacional. [13]. As equações (2.10)-(2.12) estão escritas em coordenadas esféricas, então definindo $\vec{R} = x\hat{i} + y\hat{j} + z\hat{k} \equiv (x, y, z)$, tal que

$$R^2 = x^2 + y^2 + z^2 = 1 \tag{2.13}$$

então cada ângulo θ e ϕ estarão associados ao ponto $(1, \theta, \phi)$ de uma esfera de raio $R = 1$.

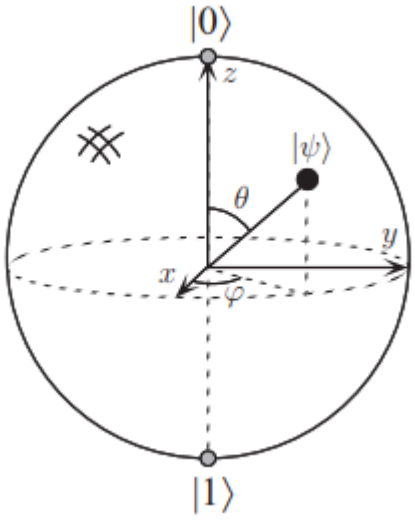

Figura 2.1: Representação de um qbit na Esfera de Bloch. Retirada de [11].

Exemplo: Dado o estado $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ pode-se obter a localização dos estados na esfera de Bloch:

θ	ϕ	ψ	Localização
0	0	$\|0\rangle$	Polo superior
π	0	$\|1\rangle$	Polo inferior
$\frac{\pi}{2}$	0	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	Eixo x positivo
$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\|0\rangle+i\|1\rangle}{\sqrt{2}}$	Eixo y positivo

Tabela 2.1: Direção e sentido do vetor representativo do qbit para alguns estados [1].

2.2 Portas lógicas quânticas

Um computador clássico é construído a partir de um circuito elétrico contendo fios e portas lógicas, analogamente, um computador quântico é construído a partir de um circuito quântico contendo fios e portas quânticas elementares para transportar e manipular a informação quântica.

2.2.1 Portas quânticas de 1 qbit

Uma porta de 1 qbit na sua forma mais geral é dada por uma matriz unitária 2×2:

$$U = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \tag{2.14}$$

O conjunto de portas quânticas (matrizes), que realizam operações unitárias sobre um qbit é infinito. As matrizes unitárias garantem que a computação possa ser reversível [11, 12].

As portas quânticas de 1 qbit mais úteis são:

Porta identidade

Também é conhecida como porta Pauli-I, sua operação não altera o estado do qbit de entrada. É representada pela matriz:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.15}$$

A aplicação dela sobre um estado retorna o mesmo estado $I\,|\psi\rangle = |\psi\rangle$.

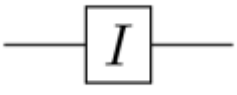

Figura 2.2: Representação circuital da porta identidade. Retirada de [11].

Porta X

A porta X é o análogo da porta NOT, usada na computação clássica. É representada pela matriz:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.16}$$

A aplicação da porta X corresponde a um inversor lógico, uma vez que ela nega o valor do bit de entrada.

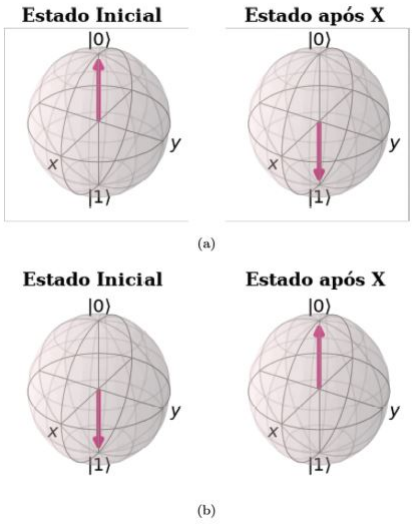

Figura 2.3: Representação na esfera de Bloch da atuação da porta X sobre os estados da Base Computacional (a) $|0\rangle$ e (b) $|1\rangle$. Retirada de [14].

Figura 2.4: Representação circuital da porta X. Retirada de [11].

Porta Y

A porta Y gira o qbit ao redor do eixo y. É representada pela matriz:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{2.17}$$

A atuação sobre um estado $|\psi\rangle = |0\rangle + |1\rangle$ será:

$$Y|\psi\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\alpha \\ i\beta \end{bmatrix} = i(|0\rangle - |1\rangle) \tag{2.18}$$

Figura 2.5: Representação circuital da porta Y. Retirada de [11].

Porta Z

A porta Z produz uma fase relativa em um estado de superposição dos qbits. É representada pela matriz:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.19}$$

Esta porta não altera o qbit, mas desloca a fase em π radianos. Quando aplicada sobre um estado $|\psi\rangle = |0\rangle + |1\rangle$ resulta em $|\psi\rangle = |0\rangle - |1\rangle$.

Figura 2.6: Representação circuital da porta Z. Retirada de [11].

Porta Hadamard ou H

A porta Hadamard não possui análogo clássico, pois em geral "força"um qbit a se sobrepor. É representada pela matriz:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.20}$$

Atua em $|0\rangle$ e $|1\rangle$ deixando o estado do qbit de saída numa superposição de estados na base computacional:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \equiv |+\rangle \tag{2.21}$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \equiv |-\rangle \tag{2.22}$$

A porta Hadamard é uma das portas quânticas mais úteis. Vizualizando na esfera de Bloch a operação Hadamard é apenas uma rotação da esfera em torno do eixo y por 90°, seguida por uma rotação de 180° em torno do eixo x.

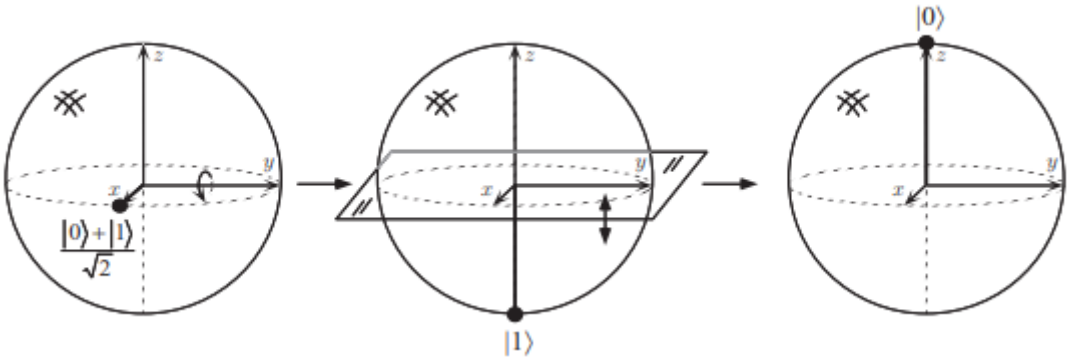

Figura 2.7: Visualização da porta Hadamard na esfera de Bloch. Retirada de [11].

Figura 2.8: Representação circuital da porta H. Retirada de [11].

A porta Hadamard pode ainda ser combinada com a porta Z para formar a porta X, e combinada com a porta X para formar a porta Z, através das seguintes sequências:

$$X = HZH \tag{2.23}$$

$$Z = HXH \tag{2.24}$$

Essas combinações se mostram bastante úteis quando é necessário o uso de portas que não estão presentes na biblioteca. [14]

Porta de Fase ou S

A porta de fase é representada matricialmente como:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{2.25}$$

Assim como Z, a porta S produz uma fase relativa em um estado de superposição dos qbits. Quando aplicada sobre um estado genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ resulta em $|\psi\rangle = \alpha|0\rangle + i\beta|1\rangle$.

Figura 2.9: Representação circuital da porta S. Retirada de [11].

2.2.2 Portas quânticas de múltiplos qbits

A grande vantagem da computação quântica aparece quando trabalha-se com sistemas de múltiplos qbits. Trabalhar com vários qbits permite realizar operações em subconjuntos de qbits e ainda assim fazer uso das propriedades quânticas de como a superposição, por exemplo [14].

Porta CNOT quântica

A porta CNOT (CONTROLLED-NOT, CTRLNOT, ou C-NOT) atua em estados de 2 qbits de entrada, o controle e o alvo. O primeiro qbit é o qbit de controle, que nunca se altera, já o segundo é o alvo, que sofre uma operação NOT. Se o qbit de controle estiver definido como 0, então o qbit alvo é deixado como está. Se o qbit de controle estiver definido como 1, então o qbit alvo é invertido. A porta CNOT é análoga da porta XOR clássica cuja atuação é $CNOT\,|x,y\rangle \rightarrow |x, x \oplus y\rangle$.

$$CNOT\,|00\rangle = |00\rangle \tag{2.26}$$

$$CNOT\,|01\rangle = |01\rangle \tag{2.27}$$

$$CNOT\,|10\rangle = |11\rangle \tag{2.28}$$

$$CNOT\,|11\rangle = |10\rangle \tag{2.29}$$

A representação matricial da porta quântica CNOT é a dada por:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.30}$$

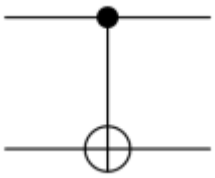

Figura 2.10: Representação circuital da porta CNOT. O círculo menor preenchido representa o qbit de controle e a linha inferior o qbit alvo. Retirada de [11].

Porta SWAP quântica

A porta SWAP inverte os qbits de entrada. É análoga a porta SWAP clássica. A ação pode ser representada como:

$$\text{SWAP}\,|x, y\rangle \rightarrow |y, x\rangle \tag{2.31}$$

Esta porta é formada por três portas CNOT.

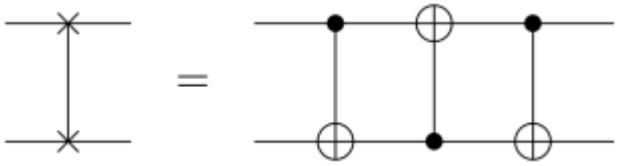

Figura 2.11: Representação circuital da Porta Swap Quântica. Retirada de [11].

Porta Toffoli quântica

É uma porta de 3-qbits. Também chamada de CCNOT, a porta Toffoli é uma porta CNOT com dois qbits de controle. A atuação da porta pode ser representada por:

$$\text{Toffoli}\,|x, y, z\rangle \rightarrow |y, x, z \oplus xy\rangle \tag{2.32}$$

O qbit alvo pode mudar de posição. Na representação Toffoli tanto o qbit $|x\rangle$, $|y\rangle$ ou $|z\rangle$ podem ser alvos, e os qbits restantes serão os controles.

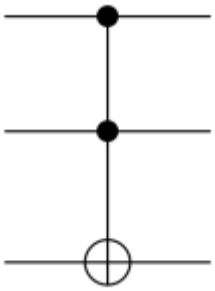

Figura 2.12: Representação circuital da Porta Toffoli Quântica. Retirada de [11].

Porta Fredkin quântica

A porta Fredkin ou CSWAPP possui um qbit de controle e dois alvos. Se o qbit de controle é $|0\rangle$, os outros dois qbits, não mudam. Se o qbit de controle é $|1\rangle$, os outros qbits trocam de valor. [12]

$$\text{Fredkin}\,|0yz\rangle \rightarrow |0yz\rangle \tag{2.33}$$

$$\text{Fredkin}\,|1yz\rangle \rightarrow |1zy\rangle \tag{2.34}$$

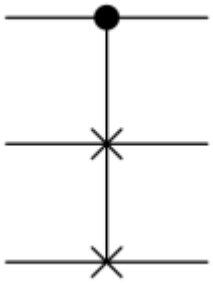

Figura 2.13: Representação circuital da Porta Fredkin Quântica. A primeira linha representa o qbit de controle, as linhas inferiores representam os qbits alvo. Retirada de [11].

Porta U_f quântica

A porta U_f ou oráculo, é uma porta genérica onde se pode implementar qualquer operação, desde que esta obedeça às regras dos operadores unitários. Oráculos são amplamente utilizados em algoritmos quânticos voltados para problemas de busca ou extração de informações de funções desconhecidas [15].

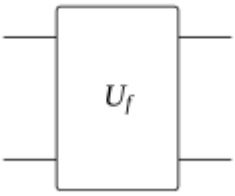

Figura 2.14: Representação circuital de uma Porta Oráculo. Retirada de [15].

2.3 Informação e Entropia de Shannon

O conceito da entropia estatística surge fornecendo uma medida do grau de incerteza de um dado sistema. A construção do conceito de entropia de Shannon se dá inicialmente dentro da estrutura da teoria matemática da comunicação ou teoria da informação. No âmbito da informação Shannon apresenta a teoria que permite quantificar a quantidade de informação recebida ou enviada [16].

2.3.1 A entropia de Shannon

Shannon propôs alguns requisitos que qualquer medida de informação deve possuir. Destacam-se:

- A quantidade de informação I em um evento x deve depender apenas de sua probabilidade p.

- I é uma função contínua da probabilidade.
- I é aditiva.

Esses requisitos levam a uma medida única de informação [17]. Na teoria da informação de Shannon uma mensagem é uma sequência de letras, escolhidas de um alfabeto com N letras, gerados por uma fonte com probabilidades independentes. A quantidade de informação contida em uma variável obedece a uma função logarítmica. Para uma variável aleatória com valores em um conjunto finito, a entropia de Shannon é definida por:

$$H(p) = -\sum_{i=1}^{n} p_i \log_2 p_i \geq 0 \tag{2.35}$$

Desta forma, pode-se obter a quantidade de informação média contida em uma mensagem, onde p(x) é a probabilidade de ocorrência de cada evento [18]. Nota-se que $H(x) = 0$ é a menor informação possível. Para qualquer mensagem, a quantidade de informação é definida em termos de probabilidades, portanto terá entropia descrita pela equação 2.35.

A entropia de Shannon permite quantificar a incerteza e generalizar para casos complexos, permitindo fazer a composição de eventos e obter a incerteza conjunta.

2.3.2 A entropia binária

A entropia de uma variável aleatória de dois resultados recebe o nome de entropia binária. É definida por:

$$\text{H(p)} = \text{-p log p - (1-p) log (1-p)} \tag{2.36}$$

Nota-se que $H(0) = H(1) = 0$. O máximo de entropia se dá quando $dH/dp = 0$, isso ocorre para $p = 1/2$, nesse caso o recebimento de um "bit" representa um ganho máximo de informação [12]. O comportamento da função é côncavo:

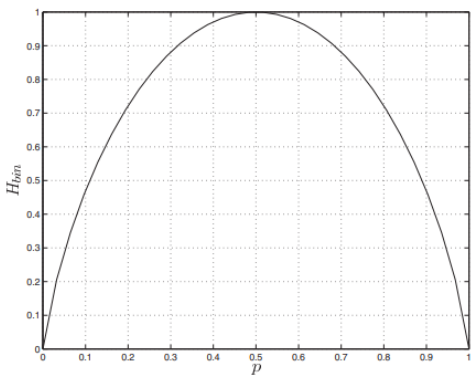

Figura 2.15: Função entropia binária. Retirada de [11].

2.3.3 A Teoria fundamental para um canal sem ruído

Uma das aplicações mais importantes da entropia de Shannon está no fato da possibilidade de comprimir mensagens, sem perda de informação. Isso prova que H determina a capacidade do canal requerida com a codificação mais eficiente.

Teorema: Suponha que uma fonte tenha entropia H (bits por símbolo) e um canal tenha capacidade C (bits por segundo). Então é possível codificar a saída da fonte de tal forma que seja transmitida à taxa média C/H. Não é possível transmitir a uma taxa média maior que C/H [19].

Isso significa que a máxima taxa de compressão da mensagem que pode ser atingida para que ela possa posteriormente ser recuperada sem erros, é dada pela entropia de Shannon.

2.4 Informação Quântica e Entropia de von Neumman

O análogo quântico da entropia de Shannon é a entropia de von Neumann. Ela é usada para medir incerteza sobre o estado de um sistema quântico. É definida por:

$$S(\rho) = -Tr\rho \log_2 \rho \tag{2.37}$$

O sistema é descrito pela matriz densidade ρ e Tr é a função traço. Os autovalores de ρ formam uma distribuição de probabilidades, logo os operadores densidade podem ser vistos como uma generalização para distribuições de probabilidades. Portanto, a entropia de von Neumann, pode ser escrita como:

$$S(\rho) = -Tr\rho \log_2 \rho = -\sum_{i=1}^{n} \lambda_i \log_2 \lambda_i \tag{2.38}$$

Os λ_i são os autovalores de ρ. Assim nota-se que a entropia de von Neumann $S(\rho)$ se assemelha a entropia de Shannon da distribuição de probabilidades obtida usando os autovalores de ρ [20].

Embora a entropia de Shannon e de von Neumman exibam semelhanças, elas têm muitas propriedades diferentes. Considerando também subsistemas, as propriedades da entropia de von Neumman são:

- Não negatividade da entropia $S(A)$.
- $S(\rho) = 0$ se e somente se ρ é puro.
- Não negatividade da quantidade $S(A|B) + S(A) = S(AB) - S(B) + S(A)$
- $S(\rho)$ é invariante sob transformação unitária

- Não negatividade de $S(C|A) + S(C|B) = S(CA) + S(CB) - S(A) - S(B)$
- Se $\rho_{AB} = \rho_A \otimes \rho_B$, $S(\rho)$ é aditiva para sistemas independentes.
- Se $\rho_{AB} \neq \rho_A \otimes \rho_B$, $S(\rho)$ é subaditiva.
- Não negatividade da informação mútua quântica e mútua condicional.

Nota-se então a diferença fundamental entre a entropia de Shannon e a de von Neumman: enquanto a entropia de um sistema composto clássico nunca pode ser menor do que a entropia de qualquer uma de suas partes, na entropia de von Neumman para sistemas quânticos esse não é o caso [12, 21].

CAPÍTULO 3

Processamento da informação quântica

Um computador processa informações e realiza tarefas através de uma série de comandos agrupados em um algoritmo. Os computadores quânticos realizam tarefas executando algoritmos quânticos que processam a informação muito mais rapidamente que algoritmos clássicos, em razão da propriedade de paralelismo quântico. Os algoritmos são aplicações de circuitos quânticos.

3.1 Paralelismo quântico

O paralelismo é uma propriedade dos computadores quânticos que permite a realização de várias tarefas simultaneamente. Por exemplo, é a capacidade que tais computadores têm de calcular um função $f(x)$ para muitos diferentes valores de x ao mesmo tempo. No paralelismo clássico seriam necessários circuitos múltiplos para computar simultaneamente uma função, já no paralelismo quântico um único circuito é empregado no cálculo de $f(x)$ para diferentes valores de x simultaneamente. Essa é uma consequência direta do fato de que um qbit pode estar num estado de superposição [22].

3.2 Circuitos quânticos

A maioria dos protocolos e algoritmos de informação quântica podem ser explicados como uma sequência de transformações aplicadas a um estado inicial conhecido e uma etapa de medição final. A representação em circuitos é muito útil e amplamente usada para analisar essas transformações. Os circuitos quânticos são compostos por fios, geralmente representados como linhas, que transportam os qbits para diferentes pontos do circuito. As operações básicas são representadas como portas lógicas.A Figura 3.1 mostra

um exemplo da representação de circuitos, segue-se a convenção usual de um estado indo da esquerda para a direita [23].

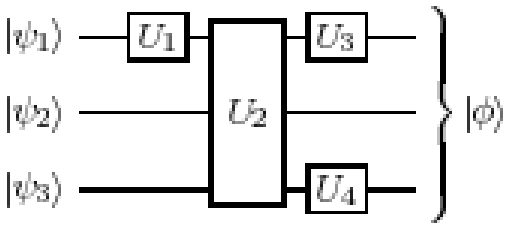

Figura 3.1: Representação de um Circuito. Retirada de [23].

É comum notar no final da linha de um circuito um símbolo de medição, cujo resultado de sua aplicação é interpretado como a probabilidade de encontrar o sistema em certo estado, como ilustrado na Figura 3.2.

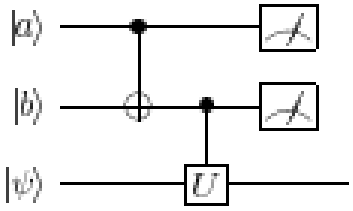

Figura 3.2: Representação circuital de uma medição quântica. Retirada de [23].

3.3 Algoritmo de Deutsch

O algoritmo de Deutsch utiliza da propriedade quântica da superposição coerente de estados para então determinar, a partir de uma única medida, se uma dada função $f(x)$ é constante ou balanceada. Em um computador clássico, seria necessária a avaliação da função para todos os dois valores x de entrada, assim determina-se com certeza se a função é constante ou balanceada. Já num computador quântico, devido às propriedades de superposição, é possível que a função seja avaliada simultaneamente para os dois valores, e ainda é possível que seja determinado, com certeza, por meio de uma única medida, se é constante ou balanceada [24].

O circuito esquematizado na Figura 3.3 implementa a variante do algoritmo de Deutsch.

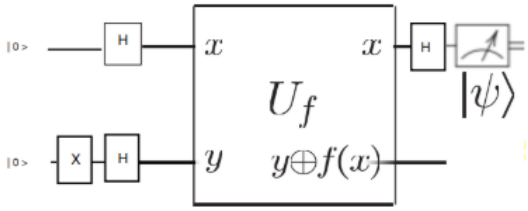

Figura 3.3: Circuito que implementa o algoritmo de Deutsch. Retirada de [12].

O circuito pode ser escrito como $H_1 U_f H_1 H_2 X_2 |0\rangle |0\rangle = U_f H_1 H_2 |0\rangle |1\rangle$, Depois da aplicação das duas portas H, o estado do sistema será:

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{3.1}$$

Usando a operação $U : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ obtêm-se que:

$$U_f |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & f(x) = 0 \\ |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} = - |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & f(x) = 1 \end{cases} \tag{3.2}$$

que pode ser escrito como:

$$U_f |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.3}$$

Nota-se que se $f(0) = f(1)$ então $(-1)^{f(x)}$ será uma fase global, podendo ser ignorada:

$$|\psi_2\rangle = \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{3.4}$$

Por outro lado, se $f(0) \neq f(1)$, haverá uma fase relativa:

$$|\psi_2\rangle = \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{3.5}$$

Por fim, uma porta Hadamard é aplicada ao primeiro qbit, resultando em:

$$|\psi_3\rangle = \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) |-\rangle \rightarrow \pm \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) |-\rangle = \pm |0\rangle |-\rangle \textbf{ Constante} \tag{3.6}$$

$$|\psi_3\rangle = \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) |-\rangle \rightarrow \pm \frac{1}{2}(|0\rangle + |1\rangle - |0\rangle + |1\rangle) |-\rangle = \pm |1\rangle |-\rangle \textbf{ Balanceada} \tag{3.7}$$

Pode-se reescrever as equações 3.6 e 3.7 na forma:

$$|\psi_3\rangle = \pm\,|f(0)\oplus f(1)\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{3.8}$$

Assim, o estado do primeiro qbit contém a informação desejada sobre a função. Fazendo uma medição no primeiro qbit sabe-se se a função é constante ou balanceada [25].

A generalização para o caso de n bits é dada pelo algoritmo de Deutsch-Jozsa ilustrado na Figura 3.4. É o resultado de uma junção dos trabalhos de David Deutsch e Richard Josza, em que, agora, a função $f(x)$ a ser avaliada permite N entradas em seu domínio usando o método da computação por paralelismo quântico [24].

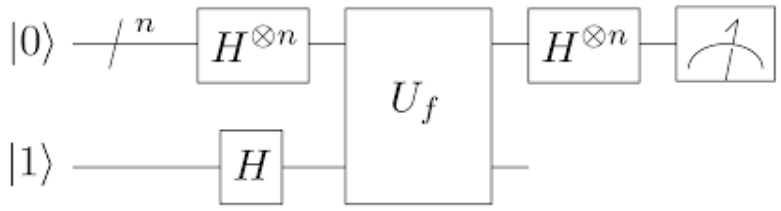

Figura 3.4: Circuito que implementa o algoritmo de Deutsch-Jozsa para n qbits. Retirada de [11].

São necessários n qbits para representar as $N = 2^n$ possíveis entradas. A operação U_f se dá da mesma maneira $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$. O sistema é iniciado com todos os qbits do primeiro registro no estado $|0\rangle$ e o qbit do segundo registro no estado $|1\rangle$ [24].

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle = x \otimes f(x) \tag{3.9}$$

Aplica-se então portas Hadamard em todos os qbits de ambos os registros:

$$|\psi_1\rangle = (H^{\otimes n} \otimes H)\,|0\rangle^{\otimes n}\,|1\rangle = (H\,|0\rangle)^{\otimes n} \otimes (H\,|1\rangle) = |+\rangle^{\otimes n}\,|-\rangle \tag{3.10}$$

Como o primeiro registro está em um estado de superposição a equação 3.10 fica:

$$|\psi_1\rangle = \sum_{x=0}^{2^n-1} \frac{|x\rangle}{\sqrt{2^n}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.11}$$

Aplicando a operação U_f para N entradas:

$$|\psi_1\rangle = \sum_{x=0}^{2^n-1} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}\right) \tag{3.12}$$

Considerando que, se $f(x) = 0$ a operação retorna $|0\rangle - |1\rangle$, se $f(x) = 1$ a operação retorna $(-1)(|0\rangle - |1\rangle)$, portanto:

$$|\psi_2\rangle = \sum_{x=0}^{2^n-1} (-1)^{f(x)} \frac{|x\rangle}{\sqrt{2^n}} \otimes |-\rangle \tag{3.13}$$

Por fim, aplica-se a Hadamard no primeiro registro, resultando em:

$$|\psi_3\rangle = \left(\sum_{x=0}^{2^n-1} \frac{H^{\otimes n} |x\rangle}{\sqrt{2^n}} \right) \otimes |-\rangle \tag{3.14}$$

De forma específica, o estado final será do tipo:

$$|\psi_3\rangle = (-1)^{\alpha_y} |y\rangle \otimes |-\rangle \tag{3.15}$$

O termo α_y é uma constante que pode assumir os valores 0 ou 1. Assim, uma medição no primeiro registro teria como resultado $|y\rangle = |00, ...0\rangle$ (todos os qbits no estado 0) caso $f(x)$ for constante; ou medindo $|y\rangle \neq |00, ..., 0\rangle$ (pelo menos um qbit no estado 1), caso $f(x)$ for balanceada, e isso para uma única execução do circuito [24].

3.4 Transformada de Fourier quântica

A Transformada de Fourier é uma das ferramentas mais úteis da matemática, que mapeia uma função em um novo espaço de funções, denominado espaço recíproco, com diversos campos de aplicação. A Transformada de Fourier Discreta (DFT) é uma transformada que atua sobre conjuntos de dados discretos e possui grande importância em algoritmos clássicos, incluindo processamento de sinais e análise de frequência. Já a Transforada de Fourier Quântica é essencial para muitos algoritmos quânticos, pois atua de forma eficiente em problemas de fatoração, busca e estimativa de fase. A DFT, aplicada a um vetor unitário de números complexos $(x_0, x_1, ..., x_{N-1})$, onde o comprimento N do vetor é um parâmetro fixo, produz um outro vetor também complexo $(y_0, y_1, ..., y_{N-1})$ onde: [26]

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i jk/N} x_j \tag{3.16}$$

A Transformada de Fourier Quântica (QFT) atua da mesma maneira, porém mudando a notação [27]. Em uma base ortonormal ela é definida como um operador linear com a seguinte ação nos estados de base:

$$|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle \tag{3.17}$$

A QFT realiza a transformada discreta de Fourier nas amplitudes:

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle \tag{3.18}$$

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i jk/N} x_j \right) |k\rangle \tag{3.19}$$

Cada amplitude y_k é a transformada de Fourier discreta das amplitudes x_j. Definindo $N = 2^n$, onde n é um número inteiro, que representa a quantidade de qbits, a QFT permite que os coeficientes transformados de Fourier sejam codificados na base computacional $(|0\rangle, |1\rangle, ..., |N-1\rangle)$. Assim, é possível escrever j utilizando a representação binária $j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0 = j_1 j_2 ... j_n$. Então, a transformada de Fourier quântica do estado $|j\rangle$ tem a seguinte representação de produto: [28]

$$|j_1 ... j_n\rangle = \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}|1\rangle)}{2^{\frac{n}{2}}} \tag{3.20}$$

Nota-se com a representação de produto que, com o paralelismo quântico, a transformada de Fourier quântica pode ser realizada como um circuito quântico com menos operações que classicamente seria necessário. A transformada de Fourier quântica, permite rapidez exponencial em comparação com a transformada de Fourier clássica, e desempenha um papel importante na computação quântica como parte essencial de muitos algoritmos quânticos (principalmente, o algoritmo de fatoração de Shor) [28, 29]. A aplicação da QFT em algoritmos possibilita, por exemplo, melhorias nos sistemas de segurança digital, criptografia bancaria, proteção de informações e recentemente está sendo aplicada a áreas da física médica. A Figura 3.5 ilustra a implementação da QFT com as portas lógicas necessárias e a transformação do estado.

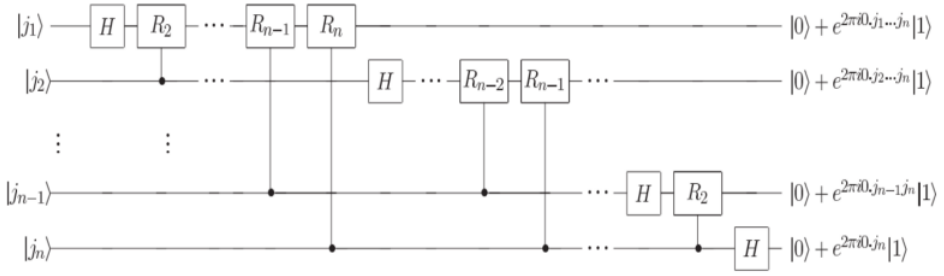

Figura 3.5: Representação do circuito de Transformada de Fourier Quântica. Retirada de [11].

A operação R_k denota uma transformação unitária e é dada por [30]:

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \tag{3.21}$$

O número de portas lógicas utilizadas para n qbits é então, para o primeiro qbit uma Hadamard e $(n-1)R_k$, observa-se no circuito que o número total de portas lógicas Hadamard e R_k é dada pela progressão aritmética:

$$n + (n-1) + (n-2) + ... + 2 + 1 = \frac{n(n+1)}{2} \tag{3.22}$$

O número de portas lógicas utilizadas é da ordem de $O(n^2)$, em contra partida à implementação clássica da transformada de Fourier, que requer exponencialmente mais portas lógicas [30].

3.5 Codificação super densa

Codificação super densa é o exemplo mais simples da aplicação de comunicação de emaranhamento quântico. Este protocolo consiste em enviar do ponto A para um ponto B distante, dois bits de informação clássica através de um canal de apenas um qbit. Para este protocolo, é necessário previamente preparar um estado entrelaçado, e enviar o primeiro qbit para o ponto A e o segundo para o ponto B. Dependendo da informação que se pretende enviar para o ponto B, aplica-se uma de quatro sequências de portas ao qbit em posse e, em seguida envia-se o qbit para o ponto B através do canal [31]. A Figura 3.6 ilustra como o protocolo pode ser implementado, em que U representa uma das quatro possíveis portas a serem aplicadas.

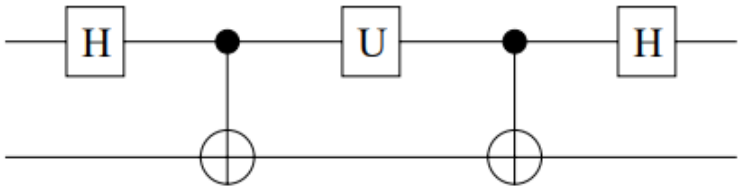

Figura 3.6: Implementação do circuito quântico para o protocolo de dense coding. Retirada de [13].

Suponha que Alice queira enviar dois bits clássicos de informação (00, 01, 10 ou 11) para Bob usando qbits (em vez de bits clássicos). O protocolo pode ser dividido em etapas de preparação, compartilhamento, codificação, envio e decodificação [13].

Preparação e compartilhamento: Uma fonte S prepara um estado emaranhado, que posteriormente é compartilhado entre Alice e Bob. O estado foi obtido após a aplicação de uma porta Hadamard e CNOT.

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \tag{3.23}$$

Após a preparação do estado, o qbit denotado pelo subscrito A é enviado para Alice e o qbit denotado pelo subscrito B é enviado para Bob, que podem estar em locais diferentes, a uma distância ilimitada um do outro.

Codificação: Existem quatro casos, que correspondem às quatro possíveis strings de dois bits que Alice pode querer enviar: $00, 01, 10, 11$. Essa escolha determina qual U será usado no circuito, cujas possibilidades são as portas $U = I, X, Y, Z$. As matrizes X, Y, Z são conhecidas como matrizes de Pauli $(\sigma_x, \sigma_y, \sigma_z)$.

Se Alice deseja enviar 00 para Bob, então ela aplica a porta quântica de identidade I para seu qbit, para que permaneça inalterado:

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) = |\phi^+\rangle \tag{3.24}$$

Se Alice deseja enviar 01 para Bob, então ela aplica a porta quântica NOT X para seu qbit, de modo que o estado quântico emaranhado resultante se torne:

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|1_A 0_B\rangle + |0_A 1_B\rangle) = |\psi^+\rangle \tag{3.25}$$

Se Alice deseja enviar 10 para Bob, então ela aplica a porta quântica de inversão de fase Z para seu qbit, de modo que o estado quântico emaranhado resultante se torne:

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle) = |\phi^-\rangle \tag{3.26}$$

Se Alice deseja enviar 11 para Bob, então ela aplica a porta quântica $Z * I = iY$ para seu qbit, de modo que o estado quântico emaranhado resultante se torne:

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle) = |\psi^-\rangle \tag{3.27}$$

Envio: Após ter realizado uma das operações descritas acima, Alice envia seu qbit emaranhado para Bob.

Decodificação: Por fim, para que Bob descubra quais bits clássicos Alice enviou, ele realizará a operação CNOT , com A como qbit de controle e B como qbit de destino. Então ele irá atuar $H \otimes I$ operação unitária no qbit emaranhado A (Hadamard é aplicada apenas a A). Para cada um dos quatro casos obtêm-se os seguintes resultados: [32]

$$H_1(CNOT\,|\phi^+\rangle) = H_1\left(CNOT * \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)\right) = H_1\frac{|00\rangle + |10\rangle}{\sqrt{2}} = |00\rangle \tag{3.28}$$

$$H_1(CNOT\,|\psi^+\rangle) = H_1\left(CNOT * \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_B\rangle)\right) = H_1\frac{|01\rangle + |11\rangle}{\sqrt{2}} = |01\rangle \tag{3.29}$$

$$H_1(CNOT\,|\phi^-\rangle) = H_1\left(CNOT * \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle)\right) = H_1\frac{|00\rangle - |10\rangle}{\sqrt{2}} = |10\rangle \tag{3.30}$$

$$H_1(CNOT\,|\psi^-\rangle) = H_1\left(CNOT * \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle)\right) = H_1\frac{|01\rangle - |11\rangle}{\sqrt{2}} = |11\rangle \tag{3.31}$$

As operações realizadas por Bob podem ser vistas como uma medida que projeta o estado emaranhado em um dos quatro vetores de base de dois qbits. Nota-se que o estado inicial e as portas quânticas usadas poderiam ter sido outras, desde que destas resultassem quatro estados distintos ortonormais [32].

3.6 Outros algoritmos quânticos

As aplicações potenciais da computação quântica vão desde quebrar sistemas criptográficos até o projeto de novos medicamentos. Essas aplicações são baseadas em algoritmos quânticos, que utilizando propriedades como a sobreposição e o entrelaçamento, realizam tarefas mais eficientemente do que algoritmos clássicos [33]. Alguns dos mais importantes algoritmos quânticos são:

- **Shor:** Em 1994, Peter Shor desenvolveu um algoritmo quântico que calcula os fatores primos de um número grande de forma muito mais eficiente do que um computador clássico. Este algoritmo pode ser usado para quebrar códigos de criptografia, como o protocolo RSA cuja aplicação principal se dá no comércio eletrônico, desde bancos na internet até pagamentos online seguros. Este algoritmo pode ser executado classicamente, no entanto usando a transformada de Fourier quântica é possível executá-lo em tempo polinomial. [34].

- **Simon:** proposto em 1994 por Daniel Simon, é um dos primeiros algoritmos quânticos importantes. Fornece uma maneira eficiente de encontrar uma estrutura oculta em uma função booleana, exibe uma aceleração exponencial na complexidade de consulta em comparação com qualquer algoritmo clássico [35].

- **Grover:** O algoritmo Grover foi proposto em 1996 e é habitualmente referenciado como sendo um algoritmo de procura de base de dados ou listas. A busca de Grover oferece um aumento de eficiência quadrático $O(\sqrt{N})$ na velocidade em relação a uma busca linear clássica, que tem complexidade $O(N)$. Por se tratar de um algoritmo probabilístico, usando sucessivas iterações, determina-se o resultado correto com alta probabilidade de sucesso [32].

- **Harrow:** O algoritmo quântico desenvolvido por Harrow, Hassidim e Lloyd (2009), chamado de Algoritmo HHL, é um exemplo de algoritmo promissor na área, demonstra aceleração exponencial na resolução de sistemas lineares ($ax = b$) se comparado com os métodos clássicos. O HHL pode executar essa tarefa com

complexidade polinomial em comparação com a complexidade clássica. O algoritmo HHL é usado em diversas aplicações de pesquisa, como máquinas vetoriais de suporte quântico, regressão linear quântica, sistemas de recomendação quântica, limitação de valor singular quântico, entre outras [36].

CAPÍTULO 4

Simulações e Aplicações

Como citado na introdução, em 1982, o físico Richard Feynman afirmou que é impossível representar os resultados da mecânica quântica com um dispositivo universal clássico. Feynman sugeriu que computadores operando com base nas leis da Mecânica Quântica poderiam ser usados para simular sistemas quânticos, retornando assim probabilidades quânticas corretas [3].

Uma vez que a computação quântica oferece vantagens quanto a execução de algoritmos, a construção de protótipos de computadores quânticos tornou-se uma realidade nos últimos anos. Grandes empresas como Google, IBM (International Business Machines Corporation), Intel e Amazon apresentam avanços significativos na implementação de um hardware quântico [29].

A empresa Google criou um processador quântico chamado Sycamore, que com o uso de qbits supercondutores cria estados quânticos em 53 qbits, correspondendo a um espaço de estados computacional de dimensão cerca de 10^{16}. A Google afirma que esse processador levou cerca de 200 segundos para encontrar um padrão em uma série aleatória de números, um supercomputador clássico de última geração levaria aproximadamente 10.000 anos para executar essa mesma tarefa. O Sycamore também foi usado para simulações em Química Quântica, o que abre possibilidades na busca por novos fármacos e novos materiais [7].

Atualmente, a IBM possui um novo processador de 1.121 bits quânticos, chamado IBM Condor. Esse processador tem o potencial de executar cálculos muito além da capacidade computacional de qualquer computador clássico. O objetivo da empresa é que até 2025 um novo processador de mais de 4.000 qbits esteja finalizado. [8].

4.1 Simuladores de circuitos quânticos

Uma das alternativas mais viáveis para o estudo e o desenvolvimento da computação quântica é uso de simulações computacionais. Um simulador de circuitos permite

descrever um algoritmo usando portas lógicas e testá-lo para um estado quântico específico através da simulação do hardware. A seguir será apresentado alguns simuladores quânticos que permitem implementar algoritmos utilizando a ideia de circuitos.

Quantum - Davy Wybiral

É um simulador online desenvolvido por Davy Wybiral de Austin Texas. Possui interface simples, mostrada na Figura 4.1, com um menu superior com algumas opções e uma área com as portas quânticas que podem ser adicionadas nos circuitos.

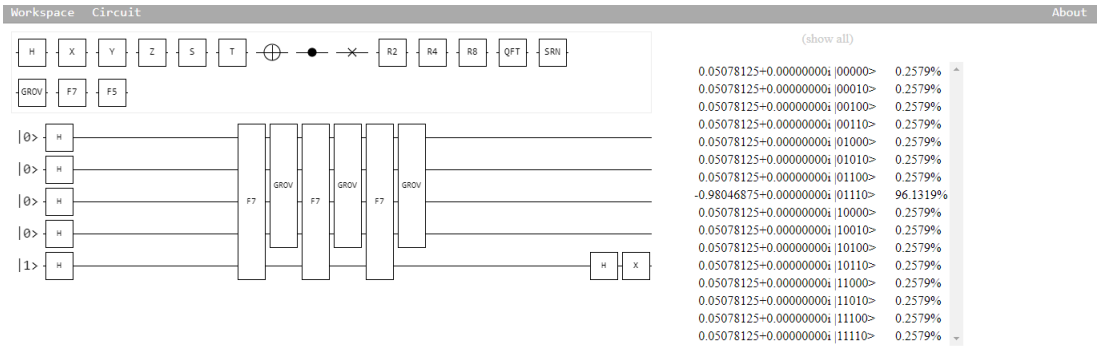

Figura 4.1: Algoritmo de Grover no simulador quântico de Davy Wybiral.

Para efetuar o cálculo do circuito basta pressionar a tecla Enter ou selecionar no menu a opção Evaluate. O resultado é mostrado ao lado direito com todas as possibilidades possíveis e suas respectivas probabilidades. O projeto e o simulador estão disponíveis através do GitHub [37].

Simulador Quirk

Desenvolvido por Craig Gidney, o *Quirk* é um simulador online com diversos exemplos e recursos para construir circuitos quânticos, disponível gratuitamente. Possui a função de edição de circuito com arrastar e soltar; reage, simula e anima em tempo real; tem a capacidade de até 16 qbits. O simulador permite também que o usuário crie portas e possa salvá-las para usar posteriormente [38]. A Figura 4.2 mostra a interface do simulador com todas os recursos disponíveis.

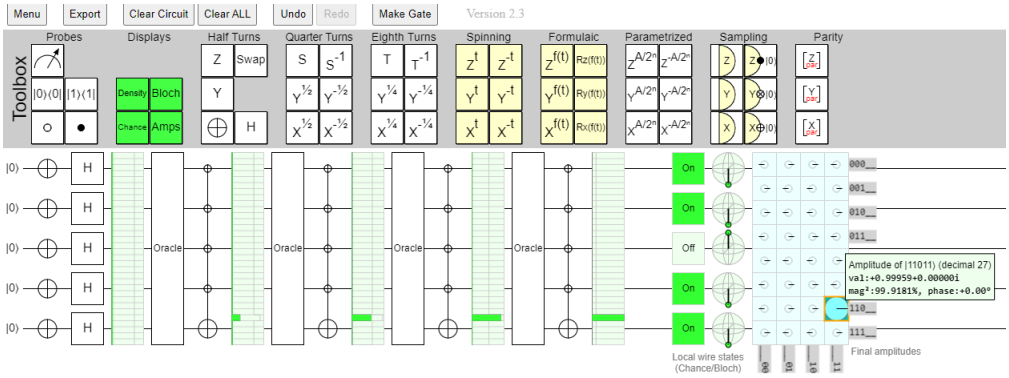

Figura 4.2: Algoritmo de Grover no simulador quântico de Quirk.

IBM Quantum experience

O IBM Quantum experience (IBM Q experience) é um simulador online e gratuito que oferece uma interface gráfica, ilustrada na Figura 4.3, para circuitos quânticos. A plataforma permite simular um circuito nos servidores clássicos ou executar no dispositivo real - processador quântico que opera nos laboratórios da *IBM Quantum Computing*.

A plataforma conta com diversos tutoriais e guias para a execução de experimentos simples ou complexos. A criação de circuitos se dá pelo *Quantum Composer*, interface gráfica que contém diversas portas que podem ser arrastadas para montar o circuito, porém também há a possibilidade de montar o circuito utilizando linha de comando com a linguagem QASM (Quantum Assembly Language). A plataforma permite que o usuário acesse o *IBM Quantum Lab* onde é possível criar, manipular e executar algoritmos quânticos através do QisKit (Quantum information software Kit) [39].

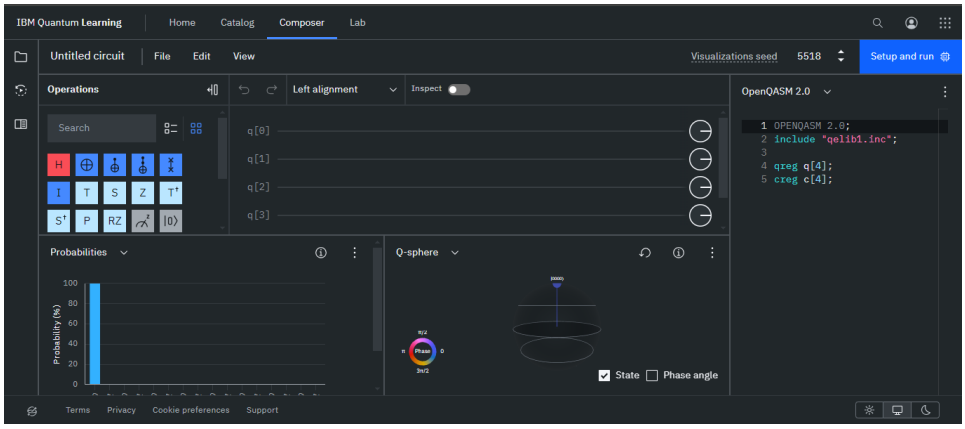

Figura 4.3: Imagem da interface do IBM-Q.

Após a montagem do circuito pode-se realizar testes no hardware quântico real ou em um ambiente de simulação. Na janela "Setup and Run" há a opção de executar o circuito num hardware real selecionando um "System" ou em simulador escolhendo uma opção de "Simulators". Nessa mesma etapa é possível verificar a quantidade de qbits disponíveis no hardware ou no simulador e também escolher a quantidade de medições

realizadas alterando o campo "shots". A seguir será apresentado os resultados obtidos simulando alguns circuitos, os testes serão feitos no *Quantum Composer* utilizando as opções “System” e “Simulators” para fins comparativos.

4.2 Simulações na IBM-Q Experience

Inicialmente é válido ressaltar que durante a execução deste trabalho a plataforma IBM-Q passou por uma série de mudanças com o intuito de beneficiar o hardware quântico. Desde o dia 15 de maio de 2024 foram desativados os serviços de simuladores de nuvem e o IBM Quantum Lab, migrando tais serviços para o Qiskit. Apesar disso, alguns resultados foram obtidos anteriormente as mudanças e estão presentes neste tópico.

Foram utilizados para executar todos os circuitos, o simulador clássico *simulator statevector* e o dispositivo quântico *ibm brisbane*.

4.2.1 Geração de dois qbits emaranhados

Para analisar as características da computação quântica foi construído um sistema físico simples que gera dois qbits emaranhados. A Figura 4.4 ilustra a montagem do circuito.

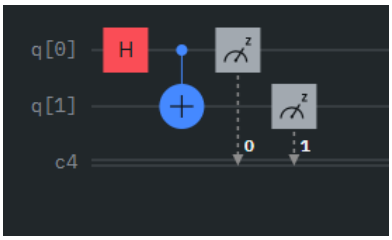

Figura 4.4: Representação do circuito quântico de um sistema de 2 qbits emaranhados. Fonte: IBM Q e editada pelo autor.

O estado inicial do sistema na plataforma é padronizado em $|0\rangle$. A atuação das portas Hadamard e CNOT irá resultar em:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{4.1}$$

Assim, é intuitivo dizer que os dois únicos possíveis resultados são 00 e 11, ambos com 50% de probabilidade. O código foi processado tanto no simulador clássico quanto num computador quântico, inicialmente com 1016 medidas e obteve-se os seguintes resultados:

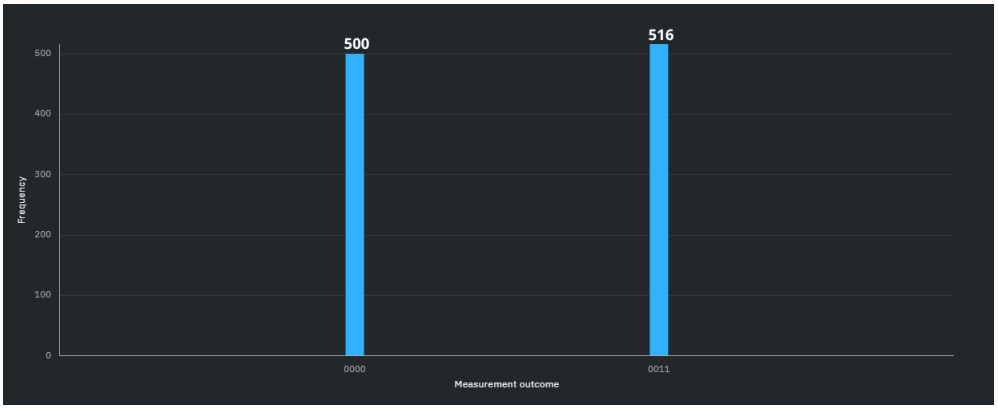

Figura 4.5: Resultados obtidos no simulador clássico. Fonte: IBM Q e editada pelo autor.

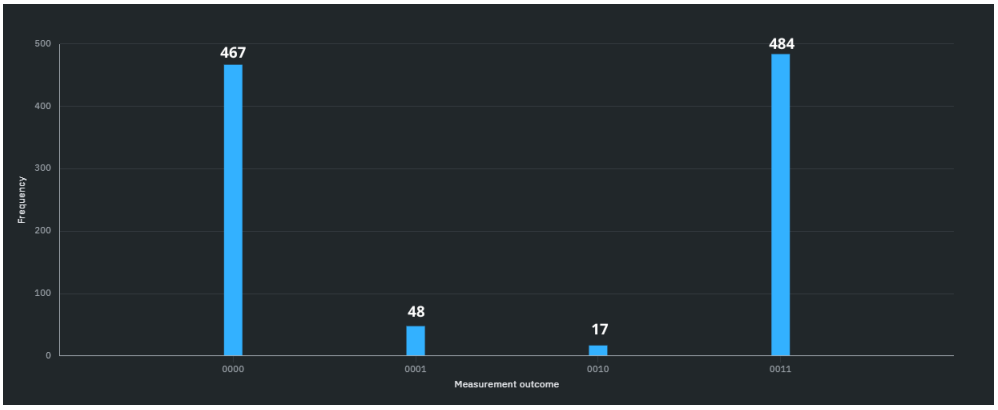

Figura 4.6: Resultados obtidos no computador quântico. Fonte: IBM Q e editada pelo autor.

Nota-se que na Figura 4.5, que os resultados obtidos se aproximam da previsão teórica, pois um simulador implementa o computador quântico ideal, e é possível notar o caráter probabilístico da mecânica quântica. Já na Figura 4.6, é interessante notar as probabilidades não nulas para os resultados 01 e 10. Num sistema físico ideal seria impossível obter-se resultados de medições diferentes de 00 e 11, portanto as probabilidades não nulas encontradas resultam de erros relacionados as interferências que o computador quântico pode sofrer com a vizinhança. Diferentemente do simulador, um computador quântico real sempre apresentará erros, pois é ainda impossível construir um sistema quântico perfeitamente isolado. Porém, os erros não impossibilitam a análise estatística do problema.

Por fim, executou-se o circuito novamente com 1 e 8000 medições apenas no processador quântico real. Obteve-se os resultados mostrados na Figura 4.7 e 4.8.

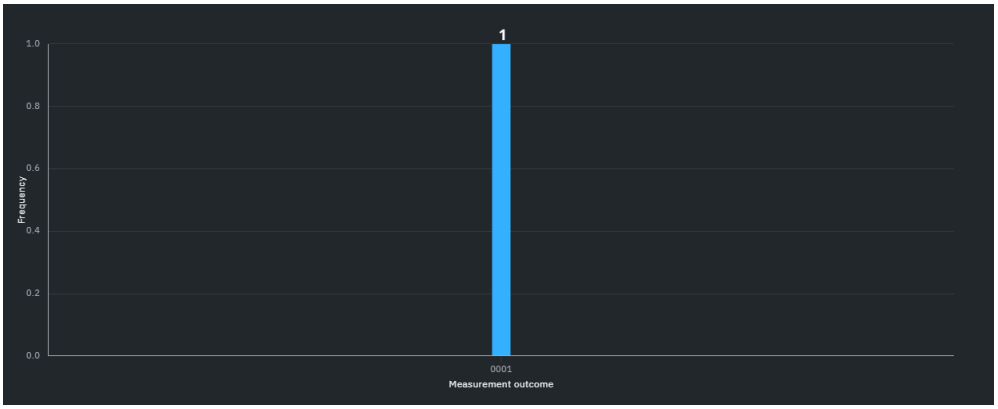

Figura 4.7: Resultados obtidos no computador quântico para 1 medição. Fonte: IBM Q e editada pelo autor.

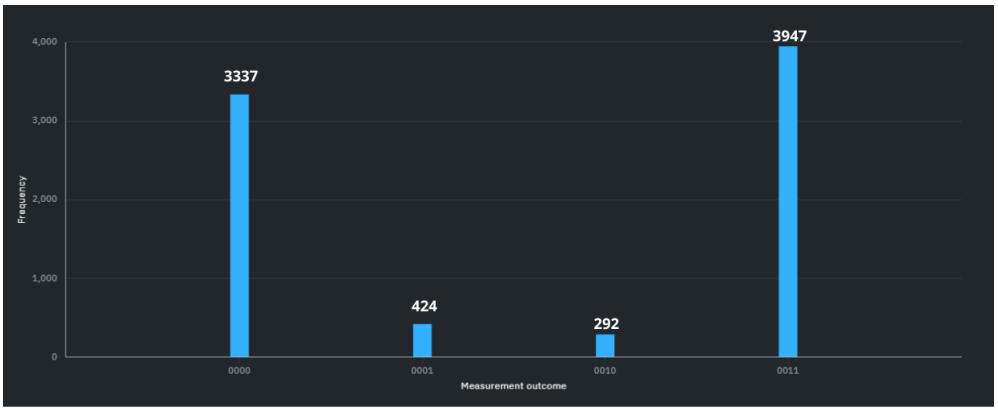

Figura 4.8: Resultados obtidos no computador quântico para 8000 medições. Fonte: IBM Q e editada pelo autor.

É notório que para 1 medição o sistema sofreu alguma interferência e retornou um valor incorreto. Já para 8000 medições pode-se observar uma maior semelhança com os valores esperados.

4.2.2 Codificação super densa

Seguindo os mesmos passos do exemplo anterior, foi testado também um circuito que implementa a codificação super densa.

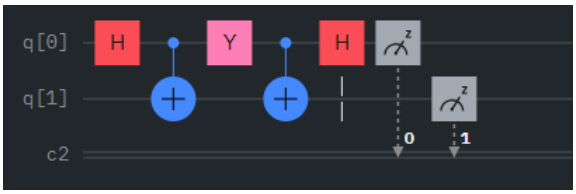

Figura 4.9: Implementação do circuito quântico para o protocolo de dense coding Fonte: IBM Q e editada pelo autor.

Neste exemplo foi escolhido o caso em que o remetente deseja enviar as strings 11 para o receptor, portanto é aplicada a porta quântica $Z * I = iY$. Após a decodificação

e medição o resultado esperado para este circuito é $|11\rangle$, conforme mostrado no Capítulo 3. O código foi processado tanto no simulador clássico quanto num computador quântico, inicialmente com 1016 medidas e obteve-se os seguintes resultados:

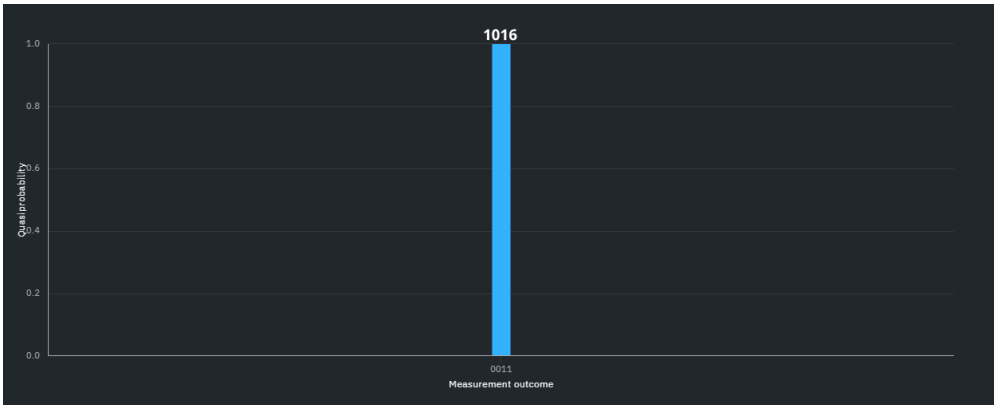

Figura 4.10: Resultados obtidos no simulador clássico. Fonte: IBM Q e editada pelo autor.

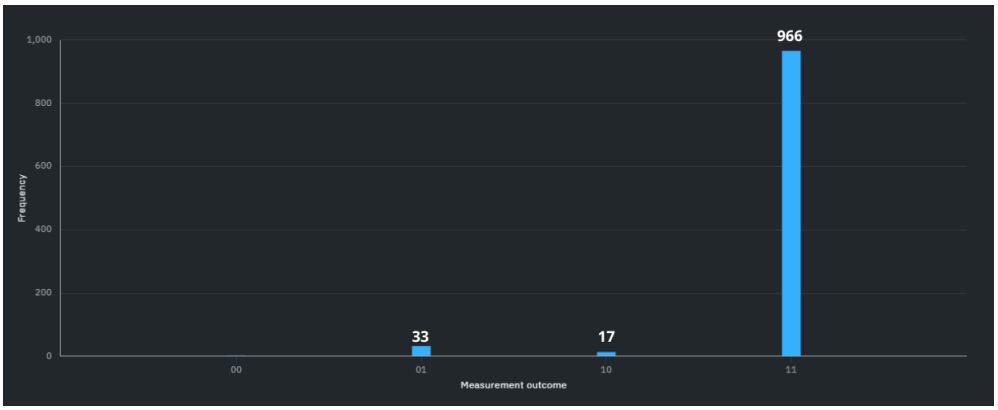

Figura 4.11: Resultados obtidos no computador quântico. Fonte: IBM Q e editada pelo autor.

Novamente, percebe-se na Figura 4.11 os erros associados as medições realizadas num computador quântico real. Ainda assim, a estatística do problema se aproxima resultado esperado. Por fim, executou-se o circuito novamente com 1 e 8000 medições apenas no processador quântico real. Obteve-se os seguintes resultados:

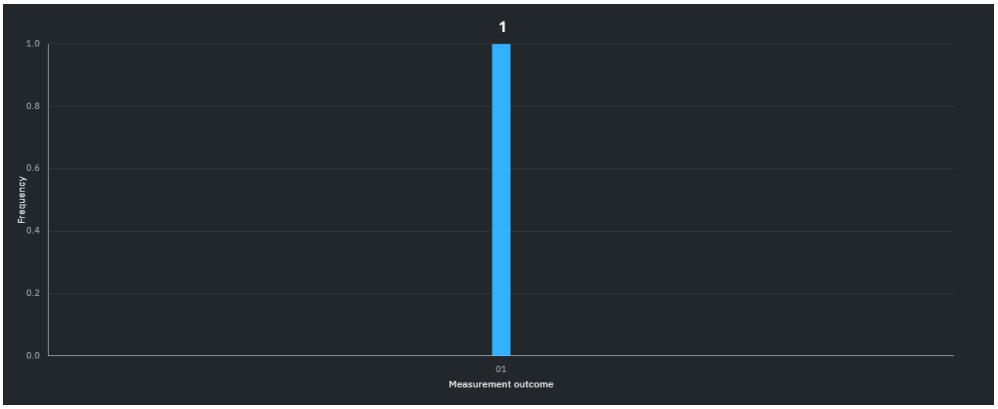

Figura 4.12: Resultados obtidos no computador quântico para 1 medição. Fonte: IBM Q e editada pelo autor.

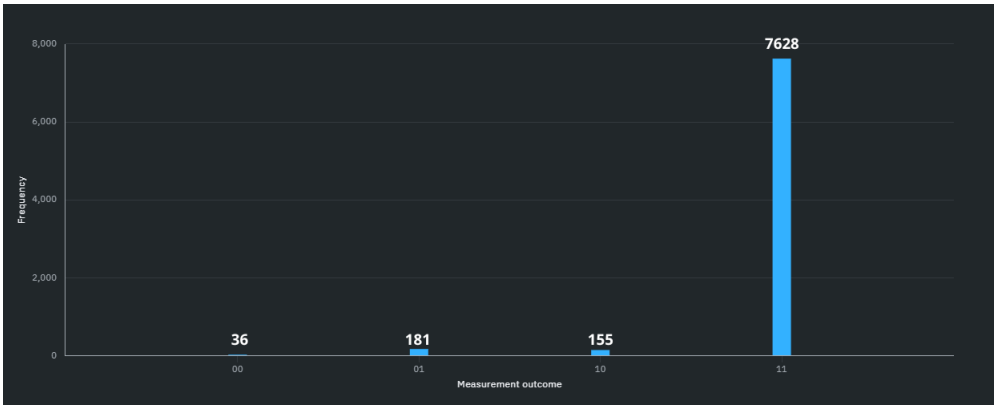

Figura 4.13: Resultados obtidos no computador quântico para 8000 medições. Fonte: IBM Q e editada pelo autor.

Analisando a Figura 4.12 é evidente que com 1 medição o sistema sofreu alguma interferência e retornou um valor incorreto. Já para 8000 medições mostrado na Figura 4.13 pode-se observar uma maior semelhança com o valor esperado.

4.2.3 Algoritmo de Deutsch-Jozsa

Por fim, foi testado também um circuito que implementa o algoritmo de Deutsch-Jozsa. Neste exemplo utilizou-se como base o artigo [24]. O objetivo foi utilizar o circuito para testar a eficiência do computador quântico num caso onde a função já é conhecida. Foram necessários 3 qbits para codificar as variáveis de entrada e 1 qbit auxiliar para armazenar $f(x)$, cuja característica corresponde a uma função balanceada. A representação circuital do problema é ilustrada na Figura 4.14.

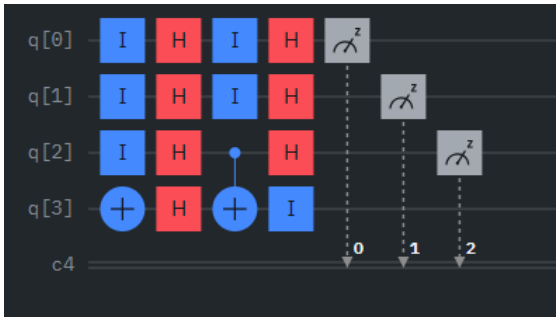

Figura 4.14: Circuito que implementa o algoritmo de Deutsch-Jozsa. Fonte: IBM Q e editada pelo autor.

O código foi processado para 10.000 medidas e obteve-se os seguintes resultados:

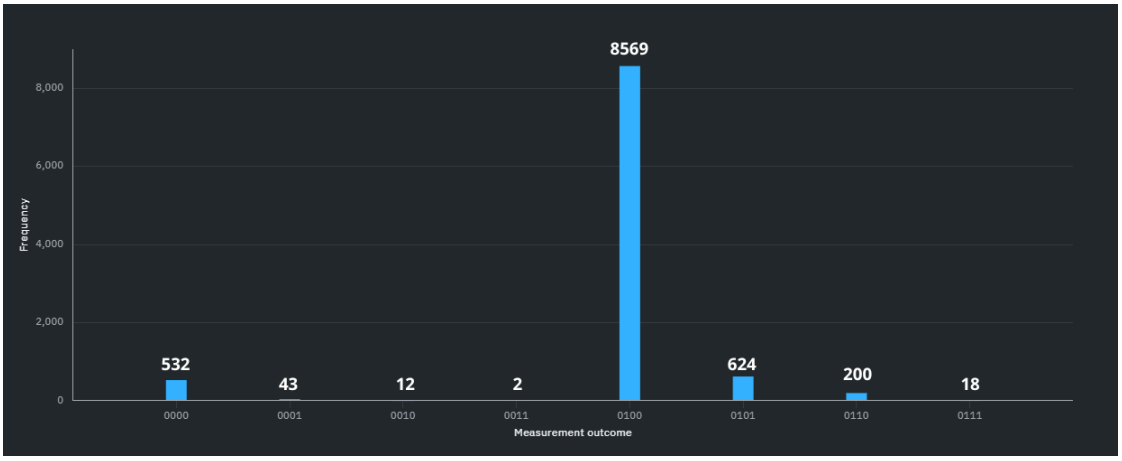

Figura 4.15: Resultados obtidos no computador quântico para 10.000 medições. Fonte: IBM Q e editada pelo autor.

Por se tratar de uma função balanceada e conhecida era esperado que houvesse ocorrência apenas do estado final $|100\rangle$, porém devido a erros intrínsecos ao computador quântico, nota-se as probabilidades não nulas dos outros resultados, ilustrado na Figura 4.15. Apesar disso, os resultados mais expressivos correspondem ao esperado para a determinação de uma função balanceada, atestando assim a eficiência do algoritmo de Deutsch.

4.3 Aplicações da computação quântica

Diante do exposto, é notável que a computação quântica tem mostrado o potencial de resolver tarefas complexas de forma rápida. O hardware e o software de computação quântica avançaram significadamente nos últimos anos, criando inúmeras possibilidades de gerar e processar informações. À medida que a tecnologia quântica avança surgem novas oportunidades de vantagem em diversos setores como: bancos e mercados financeiros, indústria química, eletrônicos, medicina, seguros, logística, entre outros [40].

4.3.1 Computação quântica na física médica

A Física Médica é o ramo da Física que consiste na aplicação dos conceitos, leis, modelos e métodos da Física para a prevenção, diagnóstico e tratamento de doenças, desempenhando uma importante função na assistência médica, na pesquisa e na otimização da proteção radiológica. [41]

Nesse contexto, os avanços tecnológicos impactam diretamente a área da saúde. Recentemente, as vantagens da computação quântica têm despertado interesse para soluções quânticas clínicas e médicas. Nota-se um crescimento de estudos que exploram o uso da computação quântica na medicina e ciências da vida. A aplicação consiste em usar as características de cada algoritmo quântico e direcioná-las a um problema específico. Em geral, as categorias de aplicação incluem simulações de fenômenos da natureza, processamento de dados com estrutura complexa, busca e otimização [42].

Simulações moleculares

O variational quantum eigensolver (VQE) é um algoritmo híbrido relevante no contexto da química quântica e de materiais, usado para calcular a energia de sistemas moleculares e outras propriedades físicas. Já o Quantum Phase Estimation (QPE) é um algoritmo empregado para calcular as fases associadas aos autovalores de operadores unitários. Um estudo de 2022 mostra a aplicação do VQE e QPE na investigação do espaço ativo de moléculas [43].

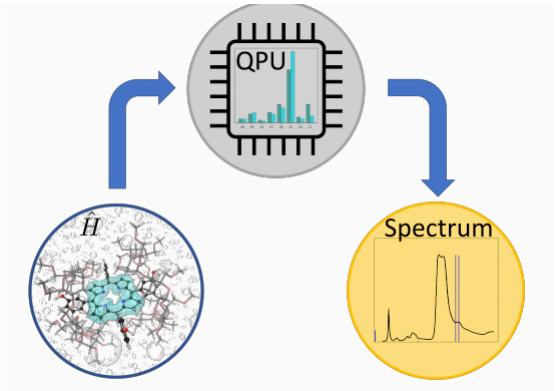

Figura 4.16: Esquema de seleção do espaço ativo. Retirada de [43]

O estudo consiste em criar um protocolo que possibilite a análise química de sistemas com relevância farmacêutica. O computador quântico se destaca no tratamento de um número moderado de orbitais dentro de um espaço ativo (fragmento quimicamente relevante da molécula) de maneira totalmente quântica. Foi criado um esquema para selecionar automaticamente o espaço ativo, conforme representado na Figura 4.16, os resultados foram obtidos por meio de cálculos teóricos usando tanto os algoritmos de estimativa de fase quântica (QPE) quanto o variational quantum eigensolver (VQE).

Esses resultados passam por um esquema básico de mitigação de erros e possibilitam a análise da estrutura eletrônica das moléculas.

Foi constatado que a abordagem de incorporação de algoritmos quânticos melhora as fraquezas do sistema tradicional corrigindo contribuições dentro do espaço ativo, e também permite um tratamento de dados de alto nível. Em alguns casos as propriedades específicas da reação envolvida tornam o uso dos algoritmos quânticos irrelevantes, mas espera-se que no geral o computador quântico melhore significativamente a descrição dos sistemas. Por fim, os resultados obtidos pelo estudo demonstram que embora os tamanhos dos espaços ativos atualmente adequados para um tratamento computacional quântico não sejam suficientes para demonstrar uma vantagem quântica, o protocolo criado é aplicável a qualquer tamanho de espaço ativo, incluindo aqueles que estão fora do alcance da computação clássica. À medida que os espaços ativos aumentam, e os computadores quânticos se tornem mais poderosos, isso permitirá a demonstração de vantagens quânticas práticas em aplicações farmacêuticas, como na criação de novos fármacos [43].

Reconstrução de imagens

O ramo da física de imagens médicas tem como tarefa principal a reconstrução de uma imagem a partir de dados coletados por dispositivos médicos, tal como a ressonância magnética (RM), a tomografia computadorizada (CT), a tomografia por emissão de pósitrons (PET), entre outros. Os algoritmos clássicos de reconstrução frequentemente usam as relações entre uma imagem e sua representação no domínio da frequência (Fourier). A implementação de algoritmos quânticos na reconstrução de imagens oferecem vantagens únicas em relação ao ambiente clássico. Dentre elas, está a possibilidade de coletar dados de entrada de maneira quântica usando potencialmente menos tempo ou doses menores de radiação [44]. Recentemente diversos estudos sobre a aplicação de algoritmos quânticos para reconstrução de imagens ganharam notoriedade.

Para exemplificar a vantagem quântica há um estudo publicado na Nature-Scientifc Reports, em que relata-se o uso de um algoritmo de otimização quântica altamente preciso para reconstrução de imagem de tomografia computadorizada [45].

A tomografia computadorizada é um procedimento não invasivo de diagnóstico que direciona um feixe de raios X colimado ao paciente e através da radiação atenuada, um sinal é transmitido para um computador que realiza cálculos matemáticos para reconstruir a imagem anatômica. No estudo citado, foi criado um algoritmo de otimização quântica que obtém com precisão a estrutura interna real de uma amostra.

Um sinograma é uma imagem criada pelo acúmulo de imagens projetadas de um objeto, curvas que correspondem aos pixels na imagem. O algoritmo representa os pixels de uma imagem CT em qbits. São usados um sinograma indeterminado e um experimentalmente de um sistema CT. Depois disso, o algoritmo obtém uma otimização binária quadrática irrestrita (QUBO) ou modelo de Ising através de cálculos otimizados

do sinograma indeterminado e do sinograma obtido experimentalmente. Este modelo determina o valor de todos os qbits. Por fim, a combinação determinada de qbits relacionada à energia pode representar a estrutura interna de uma amostra. A Figula 4.17 ilustra os resultados obtidos utilizando o algoritmo quântico para a reconstrução da imagem.

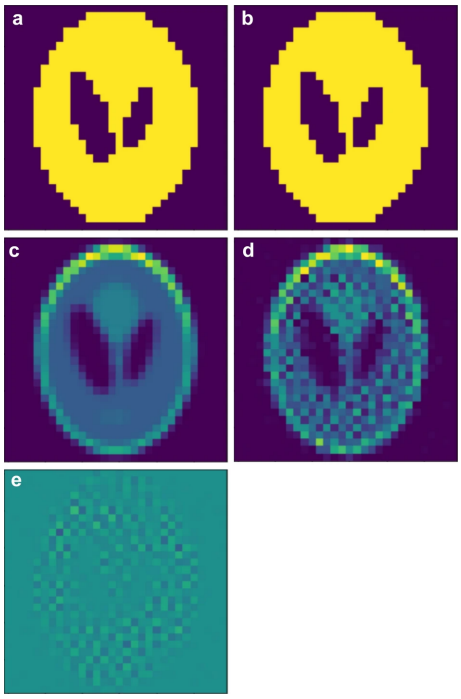

Figura 4.17: Imagens de tomografia computadorizada reconstruídas aplicando o algoritmo de otimização quântica. **(a)** Esta imagem é a amostra usada para teste. **(b)** Imagem de CT reconstruída usando um solucionador híbrido no sistema D-Wave para **(a)**. **(c)** Amostra usada no teste, e cada pixel é arredondado para ter valores inteiros de 0 a 1023. **(d)** Imagem CT para a amostra em **(c)** é reconstruída usando um solucionador híbrido. **(e)** Esta imagem mostra a diferença entre a imagem original em **(c)** e a imagem CT em **(d)**. Retirada de [45]

O algoritmo de otimização quântica para reconstrução de imagens apresentou as seguintes vantagens: pode reconstruir imagens de CT altamente precisas, assumindo que haja um número suficiente de qbits; o algoritmo é altamente resistente a artefatos nas imagens projetadas pois realiza aproximações precisas mesmo que apareça um erro em partes específicas; produz bons resultados mesmo que o número de imagens de raios X não seja suficiente, esse algoritmo pode reconstruir uma imagem precisa usando um pequeno número de projeções, logo a radiação recebida pelo paciente durante a tomografia computadorizada é reduzida.

Radioterapia adaptativa

Personalizar o tratamento de radioterapia de acordo com as características de cada paciente é crucial para otimizar os resultados do tratamento e aumentar a taxa de sobrevivência ao câncer. A necessidade de um plano de tratamento mais personalizado foi

motivo do desenvolvimento de uma nova estrutura baseada em algoritmos quânticos para suporte à decisão clínica que pode estimar a resposta à dose de um paciente individual no meio do tratamento e recomendar ajuste de dose [46].

A estrutura de aprendizagem de reforço profundo quântico (qDRL) considera as características biológicas, físicas, genéticas, clínicas e dosimétricas de cada paciente. Empregam-se algoritmos quânticos para representar e otimizar a tomada de decisão humana em um cenário da vida real. A estrutura foi aplicada em um conjunto de dados institucionais de 67 pacientes com câncer de pulmão (mas é aplicável a todos os tipos de câncer) e treinada em um computador quântico da IBM. Os resultados mostraram que a estrutura qDRL pode potencialmente melhorar a tomada de decisão clínica de radioterapia em pelo menos cerca de 10% em comparação com a prática clínica sem ajuda [46].

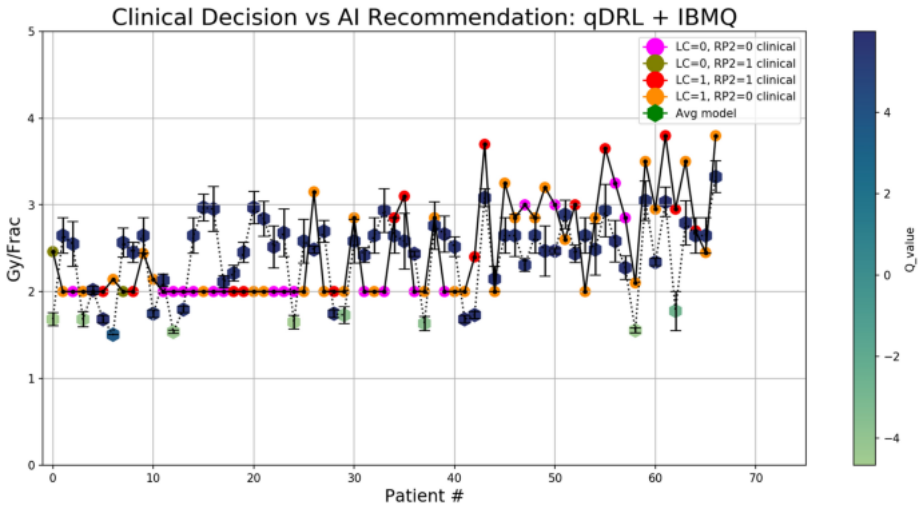

Figura 4.18: Comparação entre a decisão clínica e a recomendação da qDRL. Retirada de [46]

A Figura 4.18 ilustra de forma comparativa a decisão clínica sem ajuda e a recomendação da estrutura qDRL para ajuste de dose. O único resultado clínico desejável corresponde a controle tumoral local bem-sucedido (LC = 1) e sem ocorrência de pneumonite induzida por radiação (RP2 = 0), representado pelo círculo laranja. Já para a qDRL o parâmetro aceitável são os valores positivos representados pela faixa a direita do gráfico. Nota-se que na maioria dos pacientes a estrutura recomenda de forma eficaz o ajuste de dose, fato que acontece com menor frequência para a decisão clínica sem suporte. Esses resultados mostram o potencial benéfico da computação quântica no suporte a decisão clínica.

Diagnósticos

O diagnóstico precoce de doenças, além de proporcionar maiores chances de cura, reduz os custos de tratamento. Os algoritmos quânticos no auxílio de diagnóstico não se restringem a apenas análise de dados das informações de prontuários médicos eletrônicos. As aplicações quânticas começam desde o aprimoramento no processamento de imagens,

detecção de bordas e classificação até o uso de circuitos quânticos de amostragem para reunir informações diagnósticas e procedimentais para pacientes [42].

Além das imagens, a classificação e a previsão de doenças foram apontadas como áreas com potencial de utilizar a eficiência dos computadores quânticos, permitindo assim um diagnóstico mais preciso para cada indivíduo. Estudos iniciais com os chamados circuitos quânticos variacionais (VQCs) foram utilizados para diagnosticar doenças com base em características como temperatura, fadiga, dor muscular e tosse; prever diabetes e até mesmo prever respostas com base em sinais de eletroencefalograma [42].

Panorama geral

Além dos casos apresentados, existem dezenas de estudos que focam em aplicar tecnologia quântica para solucionar problemas relacionados a área da saúde. A Tabela 4.1 cita alguns outros exemplos do uso de algoritmos quânticos nesse contexto [42].

Princípio Quântico	**Aplicação**
Grover's	Alinhamento da sequência de DNA
Transformada de Fourier quântica	Reconstrução de imagens
Rede neural	Previsão de COVID-19
Otimização	Classificação de doenças cardiovasculares
Solucionador quântico variacional	Simulação de interações proteína-ligante
Técnicas de machine learning	Previsão de diabetes

Tabela 4.1: Exemplos de aplicações clínicas e médicas da computação quântica.

Desafios e perspectivas

Os recursos da computação quântica apresentados, mostram que esse poder computacional pode ser aproveitado de maneira eficiente para avanços significativos na área da saúde. Para que a computação quântica possa ser amplamente explorada e incorporada em pesquisas clínicas e rotinas hospitalares, uma série de desafios técnicos e éticos devem ser superados [6, 42]:

- Desenvolvimento do hardware e o software quânticos. Isso inclui o aumento do número de qbits e algoritmos mais eficientes
- Acessibilidade e segurança de dados. Garantir acesso fácil aos dados clínicos mundiais para a criação de uma base de dados eficiente. Empregar criptografia quântica para proteger a longo prazo as informações médicas de cada paciente.
- Correção de erros. Deve-se reduzir os erros nos qbits e no mecanismo de medição, implementando códigos de correção de erros cada vez mais eficientes.

- Disponibilidade. Em geral os computadores quânticos estão localizados longe dos usuários. Para acesso virtual em clínicas, hospitais e centros de pesquisa os requisitos de disponibilidade dos computadores quânticos devem ser analisados e facilitados.
- Replicabilidade. É um fator necessário para aprovações clínicas e aceitação individual dos profissionais. Portanto, a natureza probabilística da computação quântica e pela presença de ruído torna a replicabilidade ainda mais complexa.

Apesar dos desafios existentes, baseados nos estudos já realizados e apresentados, é fato de que a computação quântica tem potencial para proporcionar inúmeros avanços que serão benéficos na área da saúde. Espera-se que com os desafios superados, em poucos anos os computadores quânticos estejam em uso no contexto citado.

4.3.2 Outras aplicações

Apesar do foco deste trabalho ser apresentar as aplicações na saúde, cabe citar que a tecnologia quântica pode ser empregada em diversas áreas para solucionar vários tipos de problemas. Estudos recentes, relatam as vantagens da computação quântica quando aplicadas nas áreas de engenharia química (descoberta de novos medicamentos e propriedades de moléculas), sistemas de proteção de computadores e rede de dados (evitando ataques de invasores e vírus) , proteção de senhas bancárias, problemas da física da matéria condensada, modelagem de dinâmica de fluidos, logística, entre outros [47,48].

CAPÍTULO 5

Conclusão

A computação quântica promete revolucionar os sistemas computacionais tradicionais. As propriedades da mecânica quântica, na qual os dispositivos são pautados, permitem simular com fidelidade muitos fenômenos e realizar o processamento da informação de maneira muito mais rápida que um computador clássico. Apesar de ser potencialmente poderosa, a computação quântica ainda deve superar uma série de dificuldades. Um dos maiores desafios consiste na correção de erros, pois os computadores quânticos são muito suscetíveis a erros causados por interferências externas, como a temperatura do ambiente. A correção de tais erros vêm sendo uma área de pesquisa intensa, a criação de algoritmos de mitigação dessas falhas é fundamental para melhorar a estatística dos resultados.

Os circuitos quânticos são a forma mais simples e útil para representar as transformações aplicadas a um estado inicial referentes aos comandos agrupados em um algoritmo quântico. A alternativa mais viável para testar tais comandos se dá com o uso de simuladores computacionais, que permitem extrair informações importantes dos algoritmos simulados. Logo, é notável que um bom simulador, que oferece muitos recursos, como diferentes portas lógicas disponíveis, é uma ferramenta indispensável para a pesquisa em informação quântica.

Com o desenvolvimento do hardware e software de computação quântica, os algoritmos criados tem mostrado o potencial de resolver tarefas complexas de forma rápida. Desse modo, a vantagem de se usar essa tecnologia alcança notoriedade em muitos setores. Recentemente, as aplicações na área da saúde ganharam grande destaque. Conforme apresentado ao longo deste trabalho, as pesquisas realizadas demonstram que o uso de algoritmos quânticos específicos têm potencial de beneficiar desde o tratamento de dados da saúde, desenvolvimento de novos medicamentos até a redução do uso de radiação em exames e tratamentos. Porém, para que esse potencial seja explorado e inserido nas clínicas e centros de pesquisas, uma série de desafios técnicos e éticos devem ser superados.

A perspectiva é que inicialmente os computadores quânticos entrem no mercado como um complemento aos tradicionais, formando um sistema híbrido poderoso. Um dos principais focos de desenvolvimento deve ser na correção de erros e aumento do número

de qbits. Cabe salientar que devido a estrutura e condições físicas de operação, ainda é inviável a instalação de computadores quânticos em diversos centros de pesquisa do mundo, portanto é fundamental que o acesso virtual à essas máquinas seja cada vez mais facilitado aos pesquisadores e entusiastas da área.

Por fim, cabe ressaltar que existem inúmeras pesquisas e melhorias a serem feitas acerca de computadores quânticos. Esta é uma área com muitos desafios para a comunidade científica. Com novas descobertas os processadores, algoritmos e componentes físicos vão sendo aperfeiçoados, o que tornará o processamento da informação cada vez mais ágil e eficaz, gerando muitos benefícios para a sociedade.

Referências Bibliográficas

[1] OLIVEIRA, I. S.; SARTHOUR, R. S. Computação quântica e informação quântica. **V Escola do CBPF**, 2004. Citado 2 vezes nas páginas 13 e 23.

[2] GADELHA, J. A evolução dos computadores. **Universidade Federal Fluminense**, 2001. Citado na página 16.

[3] FEYNMAN, R. P. Simulating physics with computers. **International Journal of Theoretical Physics, VoL 21, Nos. 6/7**, 1982. Citado 2 vezes nas páginas 16 e 43.

[4] DEUTSCH, D. Quantum theory, the church-turing principle and the universal quantum computer. **Proceedings of the Royal Society of London A 400, pp. 97-117**, 1985. Citado na página 17.

[5] SINGH, J.; SINGH, M. Evolution in quantum computing. **International Conference on System Modeling and Advancement in Research Trends**, 2016. Citado na página 17.

[6] RASOOL, R. U. et al. Quantum computing for healthcare: A review. **Future Internet 15, no. 3: 94**, 2023. Citado na página 17.

[7] ARUTE, F. et al. Quantum supremacy using a programmable superconducting processor. **Nature;574(7779):505-510.**, 2019. Citado 2 vezes nas páginas 17 e 43.

[8] GAMBETTA, J. The hardware and software for the era of quantum utility is here. Quantum Research Blog. Citado 2 vezes nas páginas 17 e 43.

[9] CHEN, L. **A Brief History of Quantum Computing**. [S.l.], 2023. Citado na página 18.

[10] NEWSROOM, I. **Cleveland Clinic and IBM Unveil First Quantum Computer Dedicated to Healthcare Research**. Disponível em: <https://newsroom.ibm.com/2023-03-20-Cleveland-Clinic-and-IBM-Unveil-First-Quantum-Computer-Dedicated-to-Healthcare-Research>. Citado na página 18.

[11] NIELSEN, M. A.; CHUANG, I. L. **Quantum Computing and Quantum Information.** [S.l.]: Cambridge University Press, 1^o edição, 2000. Citado 17 vezes nas páginas 20, 22, 23, 24, 25, 26, 27, 28, 29, 30, 36 e 38.

[12] ALMEIDA, N. G. de. **Introdução à computação e informação quântica**. [S.l.]: Editora Livraria da Física, 2023. Citado 6 vezes nas páginas 21, 23, 28, 30, 32 e 35.

[13] BENENTI, G.; CASATI, G.; STRINI, G. **Principles of Quantum Computation and Information - Volume I: Basic Concepts**. [S.l.]: World Scientific Publishing Company, 2004. Citado 3 vezes nas páginas 22 e 39.

[14] JESUS, G. F. de. Computação quântica: uma abordagem para a graduação usando o qiskit. **Revista Brasileira de Ensino de Física 43**, 2021. Citado 3 vezes nas páginas 24, 26 e 27.

[15] SILVA, W. J. N. da. Uma introdução à computação quântica. **USP**, 2018. Citado na página 29.

[16] NASCIMENTO, W. S.; PRUDENTE, F. V. Sobre um estudo da entropia de shannon no contexto da mecanica quantica: Uma aplicacao ao oscilador harmonico livre e confinado. **Química Nova, 39(6), 757–764.**, 2016. Citado na página 29.

[17] VEDRAL, V. **Introduction to Quantum Information Science.** [S.l.]: Cambridge University Press, 2006. Citado na página 30.

[18] LESNE, A. Shannon entropy: a rigorous notion at the crossroads between probability, information theory, dynamical systems and statistical physics. **Mathematical Structures in Computer Science. 24(3):e240311.**, 2014. Citado na página 30.

[19] SHANNON, C. E. A mathematical theory of communication. **The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656**, 1948. Citado na página 31.

[20] MAZIERO, J. Entendendo a entropia de von neumann. **Revista Brasileira de Ensino de Física, v. 37, n. 1, 1314**, 2015. Citado na página 31.

[21] LINDEN, N.; WINTER, A. A new inequality for the von neumann entropy. **Commun. Math. Phys. 259, 129–138**, 2005. Citado na página 32.

[22] SILVA, F. L. S. da. Computação quântica: O algoritmo de deutsch e o paralelismo quântico. **Revista Physicae 3**, 2002. Citado na página 33.

[23] ESCARTIN, J. C. G.; POSADA, P. C. Equivalent quantum circuits. **arXiv:1110.2998**, 2011. Citado na página 34.

[24] OLIVEIRA, A. N. et al. Algoritmos quânticos com ibmq experience: Algoritmo de deutsch-jozsa. **Revista Brasileira De Ensino De Física, 44, e20210333**, 2022. Citado 5 vezes nas páginas 34, 36, 37 e 50.

[25] CABRAL, G. E. M.; LIMA, A. F. de; JR, B. L. Interpretando o algoritmo de deutsch no interferômetro de mach-zehnder. **Revista Brasileira De Ensino De Física, 26(2), 109–116**, 2004. Citado na página 36.

[26] ZHOU, S. S. et al. Quantum fourier transform in computational basis. **Quantum Information Processing, 16(3)**, 2017. Citado na página 37.

[27] GRIFFITHS, R. B.; NIU, C.-S. Semiclassical fourier transform for quantum computation. **arXiv:quant-ph/9511007**, 1995. Citado na página 37.

[28] WANG, Y. Quantum computation and quantum information. **Statistical Science 2012, Vol. 27, No. 3, 373–394**, 2012. Citado na página 38.

[29] ALVES, W. M. S.; FELIPE, J. C. C. Algoritmos quânticos usando o qiskit: Uma abordagem para o ensino de informação e computação quântica. **Revista Brasileira De Ensino De Física, 44, e20210290.**, 2022. Citado 2 vezes nas páginas 38 e 43.

[30] OLIVEIRA, E. V. B. de. **Computação Quântica com o IBM Q Experience**. 2019. Citado 2 vezes nas páginas 38 e 39.

[31] BENNETT, C. H.; WIESNER, S. J. Communication via one- and two-particle operators on einstein-podolsky-rosen states. **Physical Review Letters, 69(20), 2881–2884.**, 1992. Citado na página 39.

[32] FIGUEIREDO, F. D. R. L. S. **Simulador de Circuitos Quânticos**. 2013. Citado 3 vezes nas páginas 40 e 41.

[33] MONTANARO, A. Quantum algorithms: an overview. **npj Quantum Inf 2, 15023**, 2016. Citado na página 41.

[34] FOWLER, A. G.; DEVITT, S. J.; HOLLENBERG, L. C. L. Implementation of shor's algorithm on a linear nearest neighbour qubit array. **Quant. Info. Comput. 4, 237-251**, 2004. Citado na página 41.

[35] SANTOLI, T.; SCHAFFNER, C. Using simon's algorithm to attack symmetric-key cryptographic primitives. **Quantum Information and Computation, volume 17 no.1e2, pages 65-78**, 2017. Citado na página 41.

[36] HARROW, A. W.; HASSIDIM, A.; LLOYD, S. Quantum algorithm for solving linear systems of equations. **Physical Review Letters. 103 (15): 150502**, 2008. Citado na página 42.

[37] WYBIRAL, D. **Git project quantum circuit simulator**. 2017. Disponível em: <https://github.com/qcsimulator/qcsimulator.github.io>. Citado na página 44.

[38] GIDNEY, C. **My quantum circuit simulator: Quirk.** 2016. Disponível em: <https://algassert.com/2016/05/22/quirk.html>. Citado na página 44.

[39] IBM, Q. **IBM Quantum Platform**. Disponível em: <https://quantum.ibm.com/>. Citado na página 45.

[40] SIEGER, L. et al. **The Quantum Decade**. [S.l.]: IBM Institute for Business Value, 2023. Citado na página 51.

[41] MéDICA, A. B. de F. **CONHEÇA A FÍSICA MÉDICA**. 2021. Disponível em: <https://www.abfm.org.br/paginas/conheca-a-fisica-medica.php>. Citado na página 52.

[42] FLöTHER, F. F. The state of quantum computing applications in health and medicine. **Research Directions: Quantum Technologies. 1, e10, 1–10.**, 2023. Citado 5 vezes nas páginas 52 e 56.

[43] IZSAK, R. et al. Quantum computing in pharma: A multilayer embedding approach for near future applications. **Journal of Computational Chemistry**, 2022. Citado 3 vezes nas páginas 52 e 53.

[44] KIANI, B. T.; VILLANYI, A.; LLOYD, S. Quantum medical imaging algorithms. **arXiv:2004.02036v3 [quant-ph]**, 2020. Citado na página 53.

[45] JUN, K. A highly accurate quantum optimization algorithm for ct image reconstruction based on sinogram patterns. **Scientifc Reports 13, 14407**, 2023. Citado 2 vezes nas páginas 53 e 54.

[46] NIRAULA, D. et al. Quantum deep reinforcement learning for clinical decision support in oncology: application to adaptive radiotherapy. **Scientifc Reports 11, 23545**, 2021. Citado na página 55.

[47] BOVA, F.; GOLDFARB, A.; MELKO, R. G. Commercial applications of quantum computing. **EPJ Quantum Technology**, 2021. Citado na página 57.

[48] PAUDEL, H. P. et al. Quantum computing and simulations for energy applications: Review and perspective. **ACS Eng. Au, 2, 3, 151–196**, 2022. Citado na página 57.