Universidade de São Paulo
Instituto de Matemática e Estatística
Bacharelado em Ciência da Computação

Estudo histórico e discussão sobre o futuro da computação quântica

João Vitor Magalhães Leite

Monografia Final

mac 499 — Trabalho de Formatura Supervisionado

Supervisor: Alfredo Goldman

São Paulo
2024

Ficha catalográfica elaborada com dados inseridos pelo(a) autor(a)
Biblioteca Carlos Benjamin de Lyra
Instituto de Matemática e Estatística
Universidade de São Paulo

Leite, João Vitor, Magalhães
Estudo histórico e discussão sobre o futuro da computação quântica / João Vitor, Magalhães Leite; orientador, Alfredo Goldman. - São Paulo, 2024.
39 p.: il.

Trabalho de Conclusão de Curso (Graduação) - Ciência da Computação / Instituto de Matemática e Estatística / Universidade de São Paulo.
Bibliografia

1. Computação quântica. I. Goldman, Alfredo. II. Título.

Bibliotecárias do Serviço de Informação e Biblioteca
Carlos Benjamin de Lyra do IME-USP, responsáveis pela
estrutura de catalogação da publicação de acordo com a AACR2:
Maria Lúcia Ribeiro CRB-8/2766; Stela do Nascimento Madruga CRB 8/7534.

Dedico esse trabalho àqueles que tão pacientemente esperaram meu regresso ao lar. Esse foi um período de lutas, alegrias e, principalmente, saudades, mas que agora concluo com a cabeça erguida e o olhar no futuro.

Sumário

Resumo

João Vitor Magalhães Leite. **Estudo histórico e discussão sobre o futuro da computação quântica**. Monografia (Bacharelado). Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2024.

Esse trabalho investiga o evolução histórica e perspectivas futuras da computação quântica, um campo promissor da tecnologia que utiliza os princípios da mecânica quântica para revolucionar a computação clássica. Os objetivos desse trabalho incluem uma análise do desenvolvimento da área, uma revisão dos conceitos teóricos principais, como *qubits*, sobreposição, emaranhamento e portas quânticas, uma discussão do estado atual, com destaque a agentes importantes envolvidos no progresso da computação quântica e suas contribuições. Também está inclusa uma discussão sobre os desafios técnicos como correção de erros, incoerência quântica e os desafios éticos a serem enfrentados. Os métodos principais são uma revisão da literatura para fundamentação teórica e construção de histórico, bem como de documentos e notícias atuais para construção de uma perspectiva futura. O trabalho conclui que apesar de computadores quânticos escaláveis e confiáveis ainda estarem no futuro, avanços nas áreas de fidelidade de *qubits*, correção de erros e portas quânticas mais precisas tem um potencial alto de tranformar significativamente indústrias financeiras, farmacêuticas, de segurança, entre outras.

Palavras-chave: Computação quântica. *qubits*. sobreposição. correção de erro. portas quânticas.

Abstract

João Vitor Magalhães Leite. **Historic study and discussion about the future of quantum computation**. Capstone Project Report (Bachelor). Institute of Mathematics and Statistics, University of São Paulo, São Paulo, 2024.

This thesis investigates the historical evolution and future prospects of quantum computing, a promising field of technology that uses the principles of quantum mechanics to revolutionize classic computing. The objectives of this work include an analysis of the field's development, a review of the key theoretical concepts, such as *qubits*, superposition, entanglement and quantum gates, a discussion of the current state of the field, highlighting key players involved in the progress of quantum computing and their contributions. It also includes a discussion of the technical challenges such as error correction, quantum decoherence and the ethical challenges that have to be addressed. The main methods are a literature review for theoretical foundation and historical construction, as well as the analysis of current documents and news for building a future outlook. The study concludes that, although scalable and reliable quantum computers are still in the future, advancements in areas such as *qubit* fidelity, error correction and precise quantum gates have a high potential of significantly transforming industries such as finance, pharmaceuticals, security, and others.

Keywords: Quantum computing. qubtis. superposition. error correction. quantum gates.

Introdução

A computação é uma área do conhecimento que se mostrou indispensável para o estado atual da sociedade, com contribuições que vão desde atividades cotidianas, como comunicação instantânea, com e-mails, mensageiros instantâneos e redes sociais, passando por entretenimento digital, com serviços de streaming e efeitos visuais, comércio eletrônico, gestão de grandes volumes de dados para fins educativos ou comerciais, e chegando a exemplos complexos, como pesquisa científica, simulações, desenvolvimento de remédios, automações industriais e exploração espacial.

Ao longo da corrida pelo avanço da computação, a tendência observada foi a diminuição dos componentes e popularização dos computadores pessoais. No entanto, essa redução constante do tamanho das partes das máquinas acabou esbarrando em problemas de natureza quântica. Transistores tão pequenos passam a serem regidos pelas propriedades da física quântica e sofrem com fenômenos particulares a ela, como quantum tunneling, ou tunelamento quântico, que permitiria a elétrons atravessar barreiras antes intransponíveis e assim inutilizar todo o princípio por trás de um transistor convencional.

Assim, o estudo da computação quântica se tornou necessário e os primeiros computadores quânticos surgiram. Esses computadores funcionam de maneira completamente diferente dos computadores clássicos. Enquanto os computadores tradicionais utilizam bits (0 ou 1) para processar informações, os computadores quânticos utilizam *qubits*, que podem existir em múltiplos estados ao mesmo tempo, devido ao fenômeno da sobreposição. Outro fenômeno, chamado entanglement ou emaranhamento quântico, permite que *qubits* separados por grandes distâncias possam estar interconectados de tal maneira que a alteração do estado de um *qubit* instantaneamente altera o estado do outro.

Ainda nos anos 80, Richard Feynman propôs que computadores quânticos seriam uma ferramenta importante para resolver problemas complexos de física e química, pois poderiam simular de forma eficiente os fenômenos que, para a computação clássica, se tornariam exponencialmente custosos.

Diante disso, a computação quântica pode ser vista como um próximo passo para a área como um todo, levando a capacidade computacional atual para níveis ainda não alcançados anteriormente. Experimentos foram realizados para tentar demonstrar a supremacia quântica, ou seja, a existência de problemas que são fáceis para computadores quânticos e difíceis para computadores convencionais, sendo um exemplo famoso o publicado em 2019 na revista Nature por Arute, F., Arya, K., Babbush, R. et al. Nesse experimento, processadores quânticos baseados em *qubits* supercondutores criados especificamente para essa tarefa, chamados “Sycamore”, foram capazes de realizar computações em um espaço de

Hilbert de dimensão 2^{53}, superando os computadores clássicos mais rápidos da atualidade e demonstrando um problema resolvido exclusivamente por computadores quânticos.

De uma forma mais geral, a computação quântica já possui usos importantes nos dias atuais, como em criptografia, por meio do método de comunicação de distribuição de chave quântica (QKD); e simulações quânticas, como em problemas da química que também são regidos pela física quântica, podendo usufruir de propriedades como a sobreposição de estados. A sobreposição também é esperada como ferramenta importante de paralelismo de operações, permitindo operações de forma mais acelerada quando comparada com computadores clássicos.

Esse trabalho tem como objetivo fazer um levantamento histórico da computação quântica, passando por seu surgimento, dificuldades iniciais e primeiras aplicações. Também irá investigar o estado atual da computação quântica, discutindo as principais plataformas, algoritmos e desafios, bem como fará uma análise do futuro do tema, questionando possíveis soluções e limitações.

Para isso, o trabalho contará com uma introdução, seguida de fundamentação teórica, incluindo história, conceitos fundamentais, comparações com a computação clássica e algoritmos básicos. Adiante, uma seção de estado atual, com desenvolvimentos recentes, plataformas disponíveis, desafios tecnológicos e áreas de aplicação atuais. Dando continuidade, será discutida a perspectiva futura da área, com possíveis evoluções tecnológicas, indústrias que podem ser impactadas e políticas e regulamentações sobre a computação quântica. Por fim, uma conclusão, resumindo os principais pontos discutidos e refletindo sobre o futuro dessa tecnologia.

Capítulo 1

Fundamentação Teórica

1.1 Contexto histórico

Conforme mencionado anteriormente, a motivação para a computação quântica surgiu para suprir as limitações causadas pela computação clássica, sejam estas físicas ou relacionadas à eficiência. Apesar de computadores clássicos serem excelentes em diversas tarefas, sendo utilizados majoritariamente até hoje, estes ainda sofrem com problemas envolvendo paralelismo massivo, como por exemplo, fatoração de números grandes, otimização de sistemas complexos e simulação de sistemas quânticos (ref). Esse último tipo de problema é relevante pois é através dele que podemos estudar a forma que a natureza opera, uma vez que ela é regida pelos princípios quânticos. Sendo assim, a criação desse novo paradigma computacional seria uma forma de aproximar a área do mundo natural.

Dentre os pioneiros da computação quântica, pode-se destacar o físico Richard Feynman, que na década de 80 foi um dos primeiros a propor que sistemas quânticos são melhor simulados utilizando computadores quânticos do que clássicos, o que incentivou o desenvolvimento da área. O físico tem inclusive uma frase famosa, onde ele afirma que "a natureza não é clássica, droga, e, se você quiser fazer uma simulação da natureza, é melhor torná-la mecânica quântica. E, caramba, esse é um problema maravilhoso, porque não parece tão fácil.".

Outra figura importante para a área foi David Deutsch, que formalizou o conceito de “computador quântico universal” em 1985. Em um dos artigos mais famosos da área, “Quantum theory, the Church–Turing principle and the universal quantum computer”, Deutsch aborda o que seria o modelo desse computador quântico universal, funcionando como uma generalização de uma máquina de Turing, capaz de transpor o salto entre a natureza contínua da física clássica e a natureza discreta das máquinas de Turing. Dessa maneira, a computação quântica seria responsável por simulações mais fidedignas dos sistemas físicos reais.

Diante de figuras importantes do cenário chegando a conclusões bem similares sobre o potencial da computação quântica e as limitações da computação clássica, o crescimento da área já era uma realidade na década de 80. No entanto, o momento histórico que impulsionou de vez o assunto foi um dos primeiros algoritmos quânticos desenvolvidos,

que superou exponencialmente os algoritmos clássicos mais estabelecidos para fatoração de inteiros grandes. Esse algoritmo foi criado pelo matemático Peter Shor em 1994, recebeu seu nome e levantou interesse na área pelo potencial em campos como a criptografia.

Avanços teóricos foram de suma importância para solidificar a área e demonstrar sua relevância, mas experimentos em hardware precisavam garantir que a utilização de princípios quânticos para a computação era algo possível. Em 1995, David Wineland, do National Institute of Standards and Technology (NIST), juntamente com seu time, conseguiu utilizar íons aprisionados em campos eletromagnéticos para criar portas quânticas. Juntamente com outros experimentos, como os relacionados à ressonância magnética nuclear, provaram que era possível manipular e medir os bits quânticos, chamados de *qubits*, abrindo as portas para operações e algoritmos mais complexos.

Os dois algoritmos mais importantes a serem desenvolvidos na infância da computação quântica são os algoritmos de Shor, comentado anteriormente, e o de Grover. Enquanto o algoritmo de Shor apresentava uma ameaça de quebrar sistemas de criptografia baseados na dificuldade, até então, de fatorar números muito grandes, o algoritmo de Grover oferecia um avanço quadrático na velocidade para busca em bases de dados não ordenadas, facilitando problemas de otimização e busca de diversas naturezas.

Quanto ao hardware, o desenvolvimento seguiu alguns anos após os resultados teóricos iniciais, com os primeiros protótipos surgindo no início dos anos 2000. Para implementar esses computadores era necessário estabelecer formas de representar os *qubits*, que foram surgindo à medida que a área se aprofundava. Formas como íons presos em campos elétricos, circuitos supercondutores e sinais de microondas para alteração do spin de átomos de nitrogênio foram algumas das soluções encontradas para esse objetivo, mas o número de *qubits* e as taxas de erros ainda eram aquém do desejado.

As principais empresas envolvidas no desenvolvimento dessa tecnologia na época foram IBM e Google. A primeira desenvolveu programas como o IBM Q Experience, que com certas modificações existe até hoje, proporcionando acesso público através da nuvem a máquinas quânticas e facilitando o acesso da população em geral a esse tipo de máquina. A segunda buscou, inclusive através de parcerias com empresas como a NASA, atingir o conceito de supremacia quântica e estabelecer esse paradigma com o caminho do futuro, feito que a empresa afirma ter alcançado no experimento já mencionado, através do processador Sycamore, em 2019.

Desde então, essas empresas, juntamente com outras da área como Microsoft e D-Wave têm continuado a progredir cada vez mais na área, tentando resolver problemas recorrentes como correção de erros mais eficiente, crescimento do tempo de coerência dos *qubits* e aumento na quantidade de *qubits* para processamento. Tudo isso em busca de computadores quânticos totalmente funcionais e escaláveis, que potencialmente possam substituir os computadores clássicos de forma realista em cada vez mais cenários.

1.2 Conceitos fundamentais

A base da computação quântica vem dos princípios da mecânica quântica, um ramo da física que estuda e descreve os comportamentos da matéria e energia na menor escala

possível, a nível molecular, onde os conceitos da mecânica clássica não são mais aplicáveis. Dessa maneira, algumas propriedades únicas vão surgir, gerando tanto problemas quanto possibilidades diferentes daquelas relacionadas a computadores clássicos. Para um melhor entendimento dessas questões, é preciso compreender alguns dos conceitos básicos de computação quântica, que serão explicados nesta seção.

1.2.1 Qubits, sobreposição e emaranhamento

O primeiro conceito fundamental é o de quantum bit, ou *qubit*, que representa a unidade de informação básica e está para a computação quântica como o bit está para a computação clássica. No entanto, enquanto o bit existe apenas em um de dois possíveis estados, 0 ou 1, *qubits* podem existir em uma sobreposição desses dois estados simultaneamente. Por tanto, para representar um *qubit* normalmente se utiliza um vetor em um espaço bidimensional, construindo seu estado como uma combinação de 0 e 1.

Para essa representação, normalmente os vetores base utilizados são

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ e } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

escritos na notação "bra-ket" e pronunciados "ket 0" ($|0\rangle$) e "ket 1" ($|1\rangle$). Uma vez que o estado de um *qubit* é a sobreposição desses estados bases, um *qubit* (ψ) pode ser descrito pela combinação linear dos dois, da seguinte forma

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

onde alfa e beta são amplitudes de probabilidades e números complexos que, pela lei de Born devem obedecer a equação

$$\alpha^2 + \beta^2 = 1$$

O fenômeno de sobreposição em si é outro dos conceitos fundamentais da área. Graças a ele, um *qubit* pode representar 0 e 1 simultaneamente com as probabilidades alfa e beta mencionadas. Essa possibilidade é a causa da capacidade de computadores quânticos funcionarem tão bem com paralelismo, sendo capazes de processar múltiplos caminhos computacionais simultaneamente, tornando certos algoritmos quânticos muito mais velozes que suas versões clássicas.

Outra particularidade da computação quântica é a forma que *qubits* interagem entre si e influenciam uns aos outros, algo que não existe de forma equivalente na computação clássica. Duas formas se destacam, sendo elas emaranhamento e interferência quântica.

A primeira forma descreve um fenômeno no qual *qubits* se "conectam" e o estado de um *qubit* passa a se relacionar diretamente com o estado de outro, independente da distância entre eles. Dessa maneira, processos como a medida de um deles afeta instantaneamente o estado do outro. Vários algoritmos quânticos se utilizam dessa propriedade para gerar correlações que não podem ser replicadas em computadores clássicos.

A segunda forma se refere à combinação de diferentes estados quânticos, amplificando ou cancelando uns aos outros. Através dessa propriedade, alguns algoritmos quânticos são capazes de manipular as probabilidades dos estados dos *qubits*, tornando as soluções desejadas mais prováveis e reduzindo erros. A utilização de portas quânticas pode se apropriar desse fenômeno para conduzir o sistema para as respostas corretas.

1.2.2 Portas lógicas quânticas

Essas portas quânticas são as versões pertinentes das portas lógicas da computação clássica. Enquanto nessa comumente se utilizam portas como AND, OR, e NOT, por exemplo, em computadores quânticos se usam portas quânticas, com nomes e propriedades específicas. Essas portas são representadas por matrizes e incluem um número infinito de variações. No entanto, alguns que se demonstraram úteis ou particularmente interessantes receberam nomes por diversos autores da área, exemplos como a porta de Hadamard, as de Pauli, CNOT, phase, entre outros podem ser destacados.

Algumas das portas quânticas têm paralelos bem fortes com seus pares clássicos, como é o caso do Pauli-X, que assim como o NOT padrão, simplesmente inverte o *qubit* sobre o qual é aplicado, e é representado pela matriz

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Esse não é a única das portas de Pauli, que também estabeleceu as portas Pauli-Y e Pauli-Z. A porta Pauli-Y também inverte o bit sobre o qual é aplicado, mas introduz também um deslocamento de fase de i, através da matriz

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

e a porta Pauli-Z afeta apenas o estado $|1\rangle$, causando uma inversão de fase neste, enquanto deixa o estado $|0\rangle$ sem qualquer alteração. Sua forma matricial é

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Outra forma de inverter bits é com a porta CNOT, ou controlled not, que age em dois *qubits*, de modo que um deles funciona como controlador e aplica a operação NOT apenas se esse controlador for $|1\rangle$, e é representado pela matriz Hermitiana unitária

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Uma porta que é intrínseca à computação quântica é a de Hadamard, que atua sobre

um único *qubit* e gera uma sobreposição dos dois estados, com probabilidade igual de cada um deles, sendo representado pela matriz

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

ao ser aplicado no estado $|0\rangle$, o transforma em $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e ao ser aplicado ao estado $|1\rangle$, o transforma em $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. A capacidade dessa porta de gerar a sobreposição dos estados faz com que seja presente em algoritmos como os de Grover e de Shor.

Um tipo de porta que não altera a probalidade do estado do *qubit* é a de deslocamento de fase. Como o próprio nome diz, essas portas unitárias modificam a fase do estado quântico e são representadas pela matriz

$$P(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

onde φ é o deslocamento de fase com período 2π. Alguns dos valores de φ geram portas nomeadas, como $\varphi = \frac{\pi}{4}$, conhecido como porta T, $\varphi = \frac{\pi}{2}$, conhecida como porta S e $\varphi = \pi$, que gera a própria porta Pauli-Z mencionada anteriormente.

1.2.3 Bits ancilla

O conceito de bits ancilla é crucial para o funcionamento de técnicas quânticas, como a correção de erros, que será abordada em um próximo capítulo. Esses *qubits*, que podem ser construídos com seus estados iniciais definidos a priori, são bits extras utilizados para a extração de síndromes, permitindo que os erros sejam detectados sem o colapso da sobreposição quântica que decorreria da medição do estado do *qubit* de interesse. Além disso, algumas das portas lógicas mencionadas utilizam *qubits* ancilla para realizar operações mais sofisticadas, servindo de armazenamento intermediário de informações e permitindo a conversão de portas mais complicadas para portas mais simples, como de uma porta Toffoli para uma CNOT. Dessa maneira, esses bits tem um papel muito importante na área e permitem o estado atual da computação quântica.

Capítulo 2

Estado atual da computação quântica

2.1 Principais atores no cenário

Os avanços da computação quântica foram se acumulando com cada vez mais rapidez ao longo dos anos, com vários experimentos passando do campo teórico para o prático. Atualmente tanto empresas privadas quanto instituições de pesquisa investem nessa tecnologia em busca de extrair máximo proveito e mitigar os principais problemas relacionados a ela.

Um desses participantes é a IBM, uma gigante do setor, que já chegou a dominar a produção de 70% dos computadores do mundo inteiro. No campo da computação quântica ela foi uma das pioneiras, tendo lançado em 2016 o IBQ Quantum Experience, que proporciona acesso público a computadores quânticos através da nuvem. Seus processadores quânticos mais recentes são o Eagle, com 127 *qubits*, lançado em 2021, o Osprey, com 433 *qubits*, lançado em 2022 e o par Condor, com 1121 *qubits* e Heron, com 133 *qubits*, mas com uma tecnologia específica que o torna mais rápido que os outros membros da linha, ambos em 2023.

A Google é outra empresa que participa da área, com avanços como a declaração de supremacia quântica atingida pelo processador Sycamore, conforme comentado anteriormente, com seus 53 *qubits*. Nesse experimento, a Google afirma que o computador quântico foi capaz de realizar em 200 segundos operações que levariam 10 mil anos em um supercomputador clássico. A empresa também tem parcerias com entidades como a NASA, com quem desenvolve o projeto Quantum Artificial Intelligence Labs.

Também se destacam no meio empresas como a D-Wave Systems e Rigetti Cois. A primeira foca especificamente em computadores quânticos que implementam recozimento quântico (quantum annealing), um processo para encontrar o mínimo global de uma função objetiva utilizando um grupo de soluções candidatas. Esse processo, que foi proposto pela primeira vez em 1988 por B. Apolloni, N. Cesa Bianchi e D. De Falco, é especialmente relevante para um conjunto de problemas que tem soluçoes discretas, como aqueles de otimização combinatorial. A segunda oferece uma abordagem híbrida, integrando computadores quânticos e clássicos para resolver problemas específicos de otimização e química quântica.

2.2 Plataformas quânticas de acesso público

2.2.1 Simuladores quânticos

Com a popularização da tecnologia, a computação quântica vem se tornando mais acessível para grupos como pesquisadores, desenvolvedores e estudantes, graças a esforços de algumas das empresas citadas anteriormente em prover soluções. Existem simuladores que utilizam computadores clássicos para emular os comportamentos esperados em máquinas quânticas, o que é importante para a democratização do assunto, já que ao contrário dos computadores clássicos, computadores quânticos não estão presentes na maioria dos locais de estudo do mundo. No entanto, ressalta-se que essa simulação é custosa e o número de *qubits* simulados por bit clássico é bastante reduzido, uma vez que há a necessidade de simular os possíveis estados quânticos, que crescem de forma exponencial.

Na tentativa de mitigar esses problemas, alguns métodos de simulação foram desenvolvidos, como baseados em Schrodinger, sendo esses a maioria, integrais de Feynman, baseados em Heisenberg e métodos híbridos. Um dos métodos é a simulação por meio de redes de tensores, que reduz a complexidade da simulação e funciona para simulação de sistemas com pouco emaranhamento. Outro método é o baseado no teorema de Gottesman-Knill, que demonstra que as portas Clifford (Hadamard, porta S e CNOT) podem ser simuladas de forma eficiente por computadores clássicos, permitindo que circuitos baseados majoritamente nesse tipo de portas sejam simulados sem grandes limitações.

Grandes empresas fornecem plataformas de simulação, com o IBM Qiskit Aer, um simulador de alta performance da IBM, que inclui modelos de ruído reallistas e pode ser rodado em GPUs. A Google participa desse mercado com o Cirq, um framework capaz de modelar e simular circuitos quânticos, anunciado em 2018. Ambos são iniciativas open-source, com código hospedado no GitHub.

2.2.2 Computadores quânticos cloud-based

Enquanto simuladores são úteis para estudos e práticas específicas, para aplicações grandes o uso de simulações se torna inviável. Além disso, certas particularidades só são completamente respeitadas em máquinas quânticas propriamente ditas. Para que a comunidade tenha acesso a esses computadores, muitas dessas mesmas empresas oferecem serviços baseados na nuvem, com custos associados, que permitem aos usuários rodar código em máquinas quânticas a distância. A plataforma mais utilizada é a IBQ Q Experience, que através do framework Qiskit permite o uso dos seus computadores com planos gratuitos, pagamentos sob demanda e planos premium, além de fornecer cursos e tutoriais sobre o tema. Outras plataformas são a Rigetti Quantum Cloud Services (QCS), que conta com a Forest SDK para oferecer acesso aos computadores quânticos e a Azure Quantum da Microsoft que gerencia o acesso ao hardware de empresas como IonQ e Honeywell.

2.3 Desafios da computação quântica

Apesar dos avanços consideráveis na área de computação quântica, ainda existem muitos desafios no caminho entre a teoria e sistemas quânticos de larga escala confiáveis.

Esses obstáculos surgem da natureza específica da mecânica quântica, que causa estados quânticos fŕageis e a torna suscetível a erros. Há um esforço grande de pesquisadores e empresas para tentar mitigar esse problemas e tornar a computação quântica uma realidade prática, capaz de ser utilizada com confiança em apllicaçôes reais. Os principais temas que devem ser resolvidos são coerência e incoerência, ruído quântico e correção de erros.

2.3.1 Coerência e incoerência quântica

A coerência quântica é a capacidade dos *qubits* de manterem seus estados de sobreposição e emaranhamento ao logo do tempo. Em um sistema quântico ideal, os *qubits* existem e se mantém em um estado delicado, sendo capazes de processar informações de forma eficiente e superar os bits clássicos. No entanto, a incorência é um dos problemas críticos da área, que causa a perda das propriedades dos *qubits* por conta de interações com o ambiente externo.

Isso acontece porque estados quânticos são muito sensíveis ao ambiente em que se localizam, podendo sofrer influência de alterações de temperatura, radiação eletromagnética, entre outros. Esses fatores externos podem fazer o *qubit* perder a coerência e colapsar sua sobreposição quântica, se tornando essencialmente um bit clássico e acarretando na incorretude dos cálculos realizados. Na prática, isso reduz significativamente o tempo que as operações podem ocorrer de forma confiável, para evitar a chance da perda de coerência.

Algumas das soluções estudadas envolvem técnicas de isolamento, sistemas criogênicos capazes de reduzir o ruído térmico e materiais mais resistentes a distúrbios externos. Uma das formas mais eficientes de isolamento com sistemas criogênicos, especialmente para *qubits* supercondutores, é a utilização de refrigeradores de diluição, método proposto por Heinz London na década de 50 e que é capaz de chegar a temperaturas na ordem de milikelvin através da mistura dos isótopos hélio-3 e hélio-4. Apesar de ser eficaz em proteger os *qubits* do ruído térmico, aumentando o tempo de coerência, esse método requer infraestrutura específica e tem alta demanda de energia, diminuindo a sua escalabilidade. Para isolamento com materiais, as estratégias mais comuns para qubtis de íons aprisionados envolvem câmaras de vácuo, dentro das quais esses são manipulados com laser. Outra abordagem é a de desenvolver outras formas de representar *qubits* mais estáveis, como os pontos quânticos e centros de vacância de nitrogênio em diamantes.

2.3.2 Ruído quântico

O ruído quântico é um fenômeno próximo a incoerência e que também ocasiona erros nas operações. Sua origem é mais abrangente, podendo ser ocasionado por imperfeições nas portas quânticas, processos de medição, interações externas, entre outros, levando a inconsistências nos resultados. Devido a essa naturez, decorre que circuitos mais profundos com mais portas e *qubits* são mais suscetíveis a esse problema, que normalmente se apresenta na ordem de 1% por operação.

Uma vez que os estados quânticos são delicados, uma variação diminuta no início de um circuito pode gerar um efeito crescente a medida que a computação avança atravessando outras portas lógicas e interagindo com mais *qubits*, acarretando em erros grandes na

avaliação geral da computação. Um exemplo de algoritmo que é vulnerável a erros por conta do grande número de operações é o de Shor.

Os tipos de ruído quântico mais comuns são o bit-flip e o phase-flip. Por um lado, no bit-flip, um *qubit* tem seu estado alterado de forma indesejada de $|0\rangle$ para $|1\rangle$ ou vice versa. Existe um erro similar nos computadores clássicos, mas ele é especialmente problemático em algoritmos quânticos pois estes corriqueiramente se baseiam em manipulações e sobreposições de estados precisas para realizar as operações, aumentando o impacto que um único bit-flip pode causar na operação. Uma forma de mitigar esse problema especificamente é a utilização de múltiplos *qubits* físicos para representar um único *qubit* lógico, mas isso torna o uso de recursos ainda maior com o aumento da quantidade de *qubits*. Por outro lado, no phase-flip não há alteração no estado base do *qubit* e sim na fase relativa da sobreposição dos estados, alterando por exemplo o estado de sobreposição $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ para $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, o que não muda a probabilidade do *qubit* ser medido como $|0\rangle$ ou $|1\rangle$, mas causa alterações nos padrões de interferência nas operações seguintes. Para diminuir esse problema, causado pela incoerência, as técnicas de isolamento e formas de redundância são utilizadas, como mencionadas anteriormente.

2.3.3 Correção de erros quânticos

Devido a fragilidade do estado dos *qubits* diante dos ruídos quânticos mencionados anteriormente, o campo de correção de erros quânticos surgiu e se solidificou como uma parte fundamental do desenvolvimento e evolução da área. Uma das maiores limitações para correção de erros é ilustrada pelo teorema da não-clonagem, que afirma que é impossível criar uma cópia independente e idêntica de um estado quântico arbitrário desconhecido, o que impede adoção de técnicas clássicas como a clonagem de bits. Para atingir um resultado similar, a técnica utilizada é espalhar a informação de um *qubit* lógico em um estado de vários *qubits* físicos altamente emaranhados, tendo sido descoberta por Peter Shor, que foi capaz de armazenar a informação de 1 *qubit* em 9 *qubits* emaranhados.

Outra limitação da correção de erros na computação quântica é o fato de que a simples medição do estado do *qubit* para a detecção de erros causa um colapso da sobreposição, o que pode ser indesejado para operações realizadas no momento. A solução mencionada anteriormente de utilizar múltiplos *qubits* físicos em um estado de emaranhamento para representar um único *qubit* lógico permite a verificação de erros sem a perda das características desejadas, através de uma medição dos *qubits* sem perturbar a informação armazenada e sendo capaz de determinar a ocorrência, localização e tipo de erro.

Historicamente, as estimativas sugeriam por volta de 1000 *qubits* físicos para um *qubit* lógico para alcançar tolerância a erros, no entanto, pesquisas do ano de 2024 da Microsoft sugerem um número bem menor, próximo de uma dúzia. A empresa afirma ter conseguido, com o uso de um sistema de virtualilzação de *qubits*, gerar 4 *qubits* lógicos utilizando apenas 30 *qubits* físicos. Além disso, também desenvolveram uma forma de diagnosticar e corrigir os erros sem colapsar os estados dos *qubits*, através de uma técnica chamada por eles de "extração de síndrome ativa". Esses resultados ajudam a imaginar um futuro mais promissor para a correção de erros e para a escalabilidade da computação quântica como um todo.

Um método específico de correção que funciona como ilustração dessa técnica é o

three-qubit bit flip code, proposto por Asher Peres em 1985 que garante a correção se até um único bit flip ocorreu. Ele funciona através do emaranhamento dos *qubits* para alcançar uma forma de repetição.

Assumindo então que deve-se transmitir o estado de um *qubit* $|\psi_0\rangle$ por um meio $\mathcal{E}$ propenso a ruído, pode-se considerar que este causa um bit flip com probabilidade p, que em situações regulares é um valor esperado baixo. Por conta do valor de p, na maioria dos casos a inversão afeta nenhum ou apenas um *qubit*, com a chance de afetar dois *qubits* (p^2) sendo desconsiderada.

O estado inicial é arbitrário e representado por $\alpha|0\rangle + \beta|1\rangle$. Para atingir o estado de emaranhamento, utiliza-se dois *qubits* $|0\rangle$ com duas portas CNOT, gerando a isometria

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

Após passar por ε, o novo estado $|\psi_1\rangle$ pode ter tido nenhum bit invertido, o primeiro bit invertido, o segundo bit invertido ou o terceiro bit invertido, o que pode-se representar na forma

$$|000\rangle + |111\rangle$$
$$|100\rangle + |011\rangle$$
$$|010\rangle + |101\rangle$$
$$|001\rangle + |110\rangle$$

Em seguida, é necessário descobrir em qual deles ocorreu a inversão, sem medir o estado dos *qubits*. Para isso, dois *qubits* auxiliares $|0\rangle$ são submetidos cada um a duas portas CNOT. Um deles usando os *qubit* 1 e 2 como cada um dos controladores e o outro usando os *qubits* 2 e 3 como cada um dos controladores. Os resultados dessas operações, sejam S_1 e S_2, são utilizados para identificar o *qubit* que sofreu inversão.

Caso S_1 seja medido 0, isso significa que os dois primeiros bits são idênticos (o bit auxiliar não foi invertido ou foi invertido duas vezes). De forma similar, o mesmo vale para S_2, mas em relação aos dois últimos bits. Com a combinação dos resultados, é possível identificar exatamente qual dos bits foi invertido (ou se não houve inversão) e aplicar a correção necessária.

S_1	S_2	Correção
0	0	$I \otimes I \otimes I$
1	0	$X \otimes I \otimes I$
1	1	$I \otimes X \otimes I$
0	1	$I \otimes I \otimes X$

Tabela 2.1: *Correção condicional de erro de inversão de bit*

Onde X é a porta lógica Pauli-X. Chega-se assim no estado corrigido $|\psi_2\rangle$ Figura 2.1.

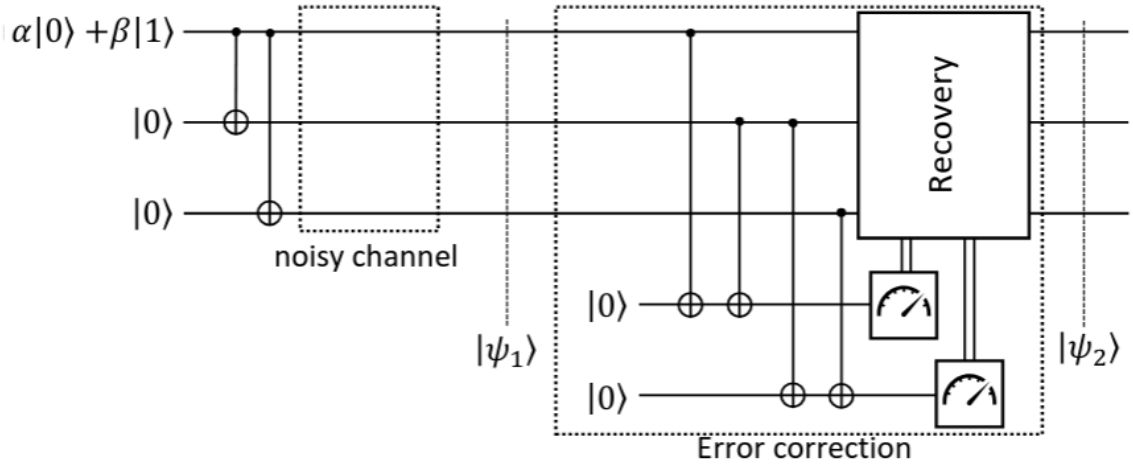

Figura 2.1: *Esquema de detecção e correção de erro de inversão de bit*

Considerando a outra forma de erro quântico, a inversão de fase, a correção de erro pode ser realizada de forma bem semelhante com a da inversão do estado do bit quando consideramos a seguinte propriedade. Um bit flip, representado por Pauli-X, é equivalente a sequência de uma porta de Hadamard, um phase flip (Pauli-Z) e outra porta de Hadamard; e um phase flip é equivalente à sequência de uma porta de Hadamard, um bit flip (Pauli-X) e outra porta de Hadamard, como ilustrado pelas equações abaixo

$$\underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}}_{Hadamard} \cdot \underbrace{\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}}_{Pauli-X} \cdot \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}}_{Hadamard} = \underbrace{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}}_{Pauli-Z}$$

$$\underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}}_{Hadamard} \cdot \underbrace{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}}_{Pauli-Z} \cdot \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}}_{Hadamard} = \underbrace{\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}}_{Pauli-X}$$

Dessa maneira, o processo de detecção e correção de um phase flip é similar ao de bit flip com a adição de uma porta de Hadamard antes do ruído e outra porta de Hadamard depois do ruído, que essencialmente transformam o possível phase flip em um bit flip. Assim, basta realizar a mesma correção anterior, com o a seguinte alteração da correção baseado no S_1 e S_2

S_1	S_2	Correção
0	0	$I \otimes I \otimes I$
1	0	$Z \otimes I \otimes I$
1	1	$I \otimes Z \otimes I$
0	1	$I \otimes I \otimes Z$

Tabela 2.2: *Correção condicional de erro de inversão de fase*

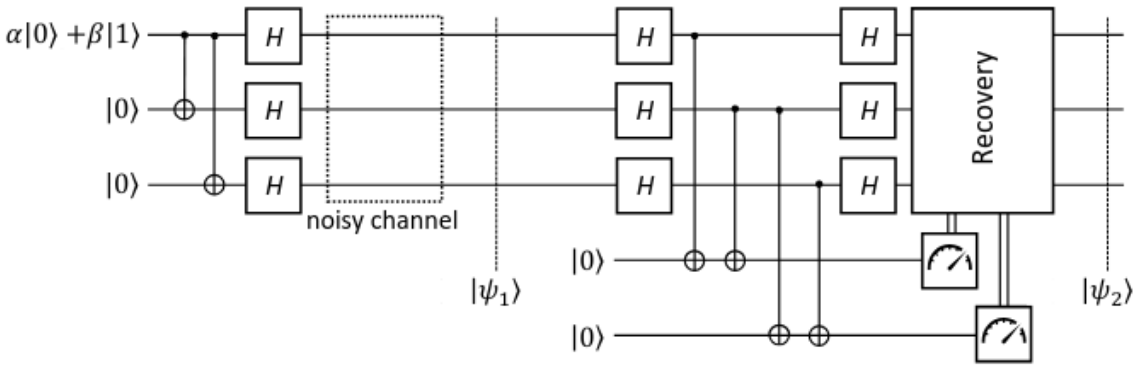

Figura 2.2: *Esquema de detecção e correção de erro de inversão de fase*

2.4 Obtenção de resultados de algoritmos quânticos

Conforme mencionado múltiplas vezes ao longo desse trabalho, uma das principais vantagens da computação quântica e a razão pela qual se espera que esta supere a com-

putação clássica é a capacidade de paralelizar operações de forma eficiente pelo uso de *qubits* em sobreposição.

Na sua forma mais simples, existem duas maneiras de obter e visualizar os resultados dos algoritmos quânticos. Isso fica ilustrado de forma clara nas primitivas disponíveis no Qiskit, o framework de computação quântica de código aberto desenvolvida pela IBM Quantum. Nele, temos a *sampler primitive*, ou primitiva de amostra e a *estimator primitive*, ou primitiva de estimativa. Na primeira, a computação é realizada um número de vezes, os chamados *shots*, e cada resultado é medido e apresentado como uma contagem de frequência; na segunda, uma precisão é definida e o resultado apresentado é o valor médio esperado estimado para os parâmetros analisados e o desvio em relação a essa média.

```
bits = data_bell_meas.meas
print("shape:", bits.shape)
print("num_bits:", bits.num_bits)
print("num_shots:", bits.num_shots)
print("array:\n", bits.array)
```

```
shape: ()
num_bits: 2
num_shots: 10
array:
 [[0]
 [0]
 [0]
 [3]
 [0]
 [0]
 [3]
 [3]
 [3]
 [0]]
```

Figura 2.3: *Exemplo em Qiskit do resultado de uma sampler primitive*

Run an Estimator pub

```
# Construct Estimator
estimator = EstimatorV2(backend)

# Construct pub and run
pub = (isa_bell, isa_obs)
est_job_bell = estimator.run([pub])
est_result_bell = est_job_bell.result()
```

View result data

```
data = est_result_bell[0].data
evs = data.evs
stds = data.stds
print(f"<ZZ> = {evs:.3f} ± {stds:.3f}")
```

```
<ZZ> = 1.002 ± 0.008
```

Figura 2.4: *Exemplo em Qiskit do resultado de uma estimator primitive*

Formas mais sofisticadas de obtenção de resultados são necessárias para aplicações mais complexas. Um exemplo comum é o algoritmo de Shor, uma forma eficiente de fatorar inteiros pseudoprimos em seus fatores primos, efetivamente quebrando a cripografia RSA atual. Sem aprofundar na lógica completa, esse algoritmo possui uma parte puramente matemática, que pode inclusive ser implementada em uma máquina clássica, e uma parte quântica, que garante a velocidade no encontro do resultado desejado.

Esse processo em questão é achar um número p, tal que o chute inicial g elevado a p seja 1 a mais que um múltiplo do pseudoprimo de interesse N. Em uma fórmula, busca-se p tal que

$$g^p = m \cdot N + 1$$

para algum valor de m. A computação envolve então elevar g a vários valores x e calcular quão maior que um múltiplo de N o resultado é.

Em vez de calcular cada um dos resultados para os diferentes valores x como um computador clássico faria, é possível realizar essa operação para inúmeros valores simultaneamente, usando uma sobreposição dos estados dos *qubits* e obtendo para cada valor um certo r, que representa quanto esse número é maior que um múltiplo de N. No entanto, a dificuldade se encontra no fato de que ao medir o resultado dessa operação, apenas um único elemento é retornado, de acordo com as probabilidades dos estados e com grandes chances de ser um valor indesejado qualquer, ou seja, com $r \neq 1$.

Realizar o processo e a medição diversas vezes, na expectativa de se deparar com o resultado esperado, tornaria a computação tão ineficiente quanto em um computador clássico. Cabe então ao pesquisador utilizar ferramentas tanto matemáticas quanto computacionais para tornar o resultado desejado significativamente mais provável ou único. No caso do algoritmo de Shor, os artifícios utilizados são: a propriedade matemática que garante a existência de um p que representa o período com o qual o resto das divisões de g^x por N se repete e a propriedade quântica que garante que ao medir uma parte do resultado que aparece em múltiplos termos da sobreposição, chega-se a uma sobreposição apenas desses estados específicos.

Na prática, é possível medir apenas o resto da divisão, obtendo um valor de resto qualquer, e colapsar parcialmente a sobreposição para uma onde todos os resultados do resto são o mesmo, seja ele qual for, associados a expoentes se repetindo em um período específico. Em seguida, uma transformada de Fourier quântica pode ser utilizada para gerar uma interferência destrutiva entre todas as frequências ausentes na sobreposição, resultando apenas na frequência de interesse, $\frac{1}{p}$.

De uma forma geral, para obter resultados concretos de operações quânticas, é preciso manipular as sobreposições e as amplitudes de probabilidade através de interferências construtivas e destrutivas, resultando em um reforço na primeira e um cancelamento na segunda.

Em relação às formas que essas manipulações podem ser alcançadas podemos destacar algumas, como a já mencionada transformada de Fourier quântica; as portas de fase, similares a porta de Hadamard e capazes de ajustar as fases das amplitudes e o operador de difusão. No algoritmo de Grover, por exemlo, o operador de difusão é utilizado juntamente

ao óraculo de Grover para aumentar a probabilidade da solução desejada. O operador de difusão consegue esse efeito calculando a média das amplitudes das sobreposições e as refletindo em relação a média, amplificando os estados desejados e diminuindo os indesejados.

A obtenção de resultados concretos a partir de algoritmos quânticos é uma área de grande importância no avanço da computação quântica, permitindo que todos os outros avanços possam ser efetivamente utilizados para um fim objetivo. Técnicas, como a transformada de Fourier quântica, podem ser usadas em diversas situações semelhantes, mas uma parte integral de algoritmos quânticos úteis ainda é uma implementação criativa, desenhada de forma a usufruir das vantagens das máquinas quânticas e capaz de superar suas fraquezas.

Capítulo 3

Perspectiva futura da computação quântica

3.1 Avanços tecnológicos

Gigantes da tecnologia, como IBM, Google e Microsoft, bem como governos e outros agentes globais já investiram mais de 55 bilhões de dólares na área da computação quântica, segundo matéria de 2024 da Forbes [14]. Parte desse dinheiro é destinada para alcançar máquinas mais robustas, melhorando tanto a qualidade dos *qubits*, com maior fidelidade nas operações e estados quânticos, quanto a quantidade desses, visando uma escala cada vez maior na casa de dezenas de milhares até milhões por máquina.

O roadmap da IBM [15] inclui planos de desenvolvimentos até pós 2033, com marcos relacionados a quantidade de portas por circuito em 2024, 2026, 2027, 2029 e 2033+, prometendo circuitos com até 5000 portas, 7500 portas, 10000 portas, 100 milhões de portas e 1 bilhão de portas respectivamente. Além disso, a demonstração do primeiro supercomputador *quantum-centric*, integrando processadores modulares, middleware e comunicação quântica está prevista para 2025, bem como desenvolvimentos em eletrônicos, *qubits* e softwares para reduzir os seus impactos, custos e demanda energética.

A Google apresenta no seu roadmap [16], metas como a construção de um *qubit* lógico de vida longa, definido por eles como um *qubit* capaz de performar um milhão de passos computacionais com menos de um erro. Para isso eles precisam continuar com os esforços em correção de erros, reduzindo os erros mesmo com o aumento no número de *qubits*. Como a última meta estabelecida, a empresa busca construir, conectar e controlar um milhão de *qubits*, levando a computação quântica para um novo patamar capaz de revolucionar indústrias como a medicinal e de sustentabilidade e atingir mais de dez aplicações quânticas com correção de erros.

Os esforços recentes da Microsoft incluem o desenvolvimento de dispositivos capaz de induzir e controlar a fase topológica da matéria baseados nos *Majorana Zero Modes*, tornando possível a criação de um novo tipo de qubit; um *qubit* protegido por hardware, que tem proteção contra erros imbutida, de forma isolada e em grupos onde trabalham

juntos como uma Quantum Processing Unit (QPU). A meta é alcançar um supercomputador quântico capaz de resolver problemas mais rapidamente que computadores clássicos, com funcionamento superior a um milhão de operações quânticas por segundo e taxas de erro inferiores a uma em um trilhão.[18]

3.2 Impacto na economia e sociedade

O impacto atual de computadores quânticos é bastante questionado por uma parte da comunidade científica. Mesmo entre pesquisadores da área, há vozes como Brierley, fundador da empresa de computação quântica Riverlane em Cambridge, que afirmam que a empolgação para o curto prazo está alta demais, mas a empolgação para longo prazo não está nada próxima do que deveria.[?] Winfried Hensinger, um físico da Universidade de Sussex em Brighton falou sobre computadores quânticos: "Eles são todos terríveis. Eles não fazem nada de útil."No entanto, sua startup Universal Quantum está trabalhando em conjunto com a Rolls-Royce para construir a sua demonstação de um computador quântico modular e de larga escala, publicada em 2023. [2]

Esse sentimento de que o potencial da computação quântica é enorme, mas ainda não está em um futuro próximo é bem presente nas discussões e declarações de envolvidos na área. Todavia, hoje já são utilizadas máquinas com resultados reais. Pesquisadores da parceria entre IBM e JP Morgan, um empresa de soluções financeiras, publicaram um estudo sobre a avaliação de preços de opções (uma forma de investimento) que segue padrões estocásticos, utilizando computadores quânticos. Na conclusão do estudo, foi afirmado que o algoritmo quântico apresentou um aumento de velocidade quadrático em relação às simulações de Monte Carlo, comumente utilizadas, mas foi apontado a provável necessidade da construção de um computador tolerante a erros.[19]

Uma combinação que vem se mostrando cada vez mais forte é a de computação quântica e machile learning/inteligência artificial. Pesquisadores da empresa Rigetti conseguiram usar um híbrido entre clássico e quântico em uma máquina de 19 quits para acelerar um algoritmo de classificação de machine learning não supervisionado. Mais uma vez, na conclusão do artigo, o texto sugere que problemas combinatórios mais difíceis e complexos exigiriam mais iterações e consequentemente portas com maior fidelidade e um número maior de *qubits*, mas que mesmo sob essas considerações, melhorias modernas nesses pontos poderiam levar a algoritmos híbridos com performance superior aos seus pares clássicos.[20]

3.3 Regulamentações e ética

Uma preocupação constante com o desenvolvimento de novas tecnologias, que surgem cada vez mais rapidamente e globalmente, é o estabelecimento de legislação e boas práticas éticas que ajudem a garantir um ambiente justo para todos os envolvidos. A área de computação quântica apresenta alguns pontos com impactos diretos na forma como sistemas funcionam atualmente, como é o caso de criptografias que se baseiam na dificuldade de processos facilmente realizados por computadores quânticos competentes, como o caso da criptografia RSA. A expectativa de especialistas, como John Preskill, professor da Caltech,

é que haja uma transposição de criptografia de chaves públicas para sistemas baseados em problemas que não sejam resolvidos por computadores quânticos de forma eficiente. Uma forma em estudo é o *Quantum key distribution* (QKD), que usa uma série de fótons para transmitir a sequência utililzada como chave e se utiliza da impossibilidade de observar a chave sem perturbar o seu estado.[21]

Outra questão ética é uma repetição da mesma feita a avanços de inteligência artificial, uma vez que os campos estão intimamente relacionados. O desenvolvimento desse tipo de tecnologia tem uma possibilidade alta de modificar indústrias ao nível de eliminar empregos em certas áreas. Uma maior porcentagem de tomada de decisão nas mãos de IAs pode gerar decisões enviesadas, exacerbando os preconceitos dos dados usados nos seus treinamentos. Para pesquisadores como Joseph Fuller, professor da escola de negócios de Harvard, uma solução seria o crescimento de empregos híbridos, nos quais ao delegar processos mais técnicos para a IA, os humanos conseguiriam fazer mais coisas de forma melhor e com menos erros, além de disseminar a sua expertise em outras áreas da empresa.[22]

No que tange legislação, pouca coisa já foi desenvolvida, mas certos avanços acontecem aos poucos. No final de 2022, o presidente americano Joe Biden assinou o *Quantum Computing Cybersecurity Preparedness Act*, que trata da provável vulnerabilidade futura de sistemas criptografados que o governo utiliza atualmente diante do avanço da computação quântica. Esse ato prevê a realização de um inventário desses sistemas e planos de migração.[23] Na Europa, 26 países membros da união européia assinaram uma declaração sobre tecnologias quânticas, na qual reconhecem a importância da tecnologia para o avanço e competitividade da união européia no cenário global e demonstram um desejo de tornar a europa um centro mundial de inovação e excelência na área.[24] Essas movimentações de grandes potências globais ilustram o interesse internacional em desenvolver e aperfeiçoar a computação quântica.

3.4 O debate entre defensores e céticos

A trajetória da computação quântica e seus desafios têm fomentado debates constantes dentro da comunidade científica e tecnológica global. De um lado, defensores da área enxergam uma mudança de paradigma sem precedentes na capacidade computacional atual, celebrando conquistas já alcançadas como parte da argumentação. Do outro lado, céticos questionam se os avanços prometidos conseguirão de fato ser atingidos, e se a computação quântica realmente apresenta vantagens sobre a clássica em aplicações mais variadas.

Os defensores da tecnologia argumentam que as propriedades quânticas e sua aplicação, comentadas nesse texto, podem alterar fundamentalmente a forma que a computação é aplicada em diferentes áreas, tanto na forma como ela se encontra atualmente, quanto com melhorias futuras para seus principais problemas do presente.

Um dos argumentos a favor da tecnologia é o aumento teórico exponencial na velocidade dos algoritmos, quando comparados com alternativas clássicas. Em dezembro de 2024, o computador quântico da Google, chamado Willow, foi capaz de realizar um cálculo em cinco minutos que, segundo a própria empresa, levaria 10 septilhões de anos nos supercomputadores mais rápidos da atualidade. Essa medição de performance ocorreu em um benchmark de amostragem de circuito aleatório (random circuit sampling, ou RCS),

que é notoriamente difícil para computadores clássicos, devido a falta de padrões que possam ser explorados para aumentar sua eficiência.[32]

Outro exemplo ocorreu em janeiro de 2025, quando pesquisadores da Pharmaceuticals e da Universidade de Sorbonne desenvolveram algoritmos quânticos que aceleram de forma exponencial a análise de cadeias de Markov não reversíveis, que têm aplicações em desenvolvimento de remédios e modelagens financeiras. Enquanto modelos clássicos usam passeios aleatórios, transicionando entre estados passo a passo através de probabilidades, os modelos quânticos usam passeios quânticos (quantum walks), usufruindo da sobreposição quântica para explorar múltiplos caminhos simultaneamente.[33]

Essa abordagem permite manipular a velocidade com a qual os sistemas atingem seus estados estacionários, resultando na solução de problemas que levariam anos, em minutos. Segundo os pesquisadores, para cadeias de Markov reversíveis, esses algoritmos podem atingir uma melhoria quadrática da velocidade; e para algumas cadeias não reversíveis, essa melhoria pode ser até exponencial. Esses avanços ajudariam áreas como desenvolvimento de novos materiais, novos remédios e até na modelagem de sistemas financeiros.

Outro argumento para a aplicabilidade da computação quântica são os avanços na correção e prevenção de erros. Taxas de erros e suscetibilidade a ruído sempre foram problemas muito significantes para área, mas que cada vez mais estão sendo mitigados.

Ainda no mesmo computador quântico, Willow, a Google afirma que utilizando grades de quibits cada vez maiores, de 3x3, para 5x5 e para 7x7, a taxa de erro caiu pela metade em cada passo, o que representaria uma redução exponencial, chamada de "abaixo do limiar"(below threshold), um marco desde a introdução do conceito de correção de erro quântica, por Peter Shor em 1995.[32]

A empresa afirma ser um dos primeiros exemplos de correção de erros em tempo real em um sistema supercondutor, onde a vida útil do conjunto de *qubits* é maior que dos *qubits* individuais, o que demonstraria um avanço do sistema como um todo. Com isso, a Google visualiza um futuro em que computadores quânticos escaláveis e úteis podem ser construídos, alcançando usos práticos e comerciais que não podem ser replicados em computadores clássicos.

A Microsoft é outra empresa na vanguarda do desenvolvimento e um dos principais destaques do seu chip anunciado em 2025, Majorana 1, é sua menor suscetibilidade a erros. Segundo a empresa, o chip que está sob desenvolvimento há quase 20 anos utiliza uma partícula subatômica chamada *Majorana fermion*, com propriedades que a tornam mais resistente a erros.[28]

Mais um sinal da relevância da computação quântica apontada pelos seus defensores é o investimento massivo de múltiplos agentes. Empresas gigantescas do setor como IBM, Google e Microsoft investem orçamentos substanciais nos seus avanços tecnológicos, discutidos em diversos momentos desse texto. No entanto, não apenas iniciativas privadas demonstram confiança na área. Cada vez mais, governos estão apostando nas pesquisas e aplicações quânticas também.

No início de 2025, o governador Wes Moore de Maryland, nos EUA, anunciou uma iniciativa público-privada de 1 bilhão de dólares em conjunto com a Universidade de

Maryland e IonQ, na tentativa de recrutar os melhores cientistas e engenheiros do mundo, expandir laboratórios e fomentar de forma geral a computação quântica na região.[30]

Outros investimentos de natureza similar acontecem pelo mundo, como em programas nos últimos dois anos de mais de 70 milhões de dólares no Canadá e em Singapura, de 100 milhões de libras no Reino Unido, e de mais de um bilhão de dólares na Austrália, superando lá inclusive os investimentos de iniciativas privadas.[31][35][34]

Todavia, apesar desses argumentos positivos, muitos especialistas continuam encarando a computação quântica com ceticismo, apontando suas falhas intrínsecas que podem impedir seu uso de forma prática se esses desafios não forem superados.

Talvez a maior crítica seja a dificuldade de escalabilidade das máquinas. Planejamentos como *roadmap* da IBM preveem sistemas com milhares de *qubits* físicos até 2033, mas especialistas estimam que uma ordem de milhões de *qubits* físicos seja necessária para atingir uma real tolerância a falhas.

A IonQ é outra empresa que enfrenta dificuldades para escalar sua tecnologia, preocupando seus investidores sobre os retornos prometidos. Segundo um artigo da SeekingAlpha, a IonQ não se apresenta como um investimento promissor, pois seus computadores, que operam no regime NISQ (Noisy Intermediate-Scale Quantum), têm um número limitado de qubits e altas taxas de erro.[36]

Sua tecnologia de íons aprisionados enfrenta desafios estruturais para escalabilidade, uma vez que seus qubits estão dispostos em uma geometria unidemensional, e expandir para sistemas maiores exigiria redes mais complexas, ainda não comprovadas experimentalmente em grande escala. Além disso, a fabricação de armadilhas de íons é altamente complexa e cara, restringindo o crescimento a um ritmo linear em vez do esperado crescimento exponencial.

Assim como outros empresas dedicadas exclusivamente à computação quântica, a IonQ tem alto investimento em pesquisa e desenvolvimento, mas sua baixa receita, pela falta de aplicabilidade quântica atual, causa dependência de um fluxo constante de parcerias e contratos, com entrada de dinheiro por investidores na expectativa de grandes avanços na área.

Muitos dos críticos também apontam para a limitação dos casos em que a computação quântica demonstrou uma superioridade substancial sobre a clássica. Apesar de alguns resultados apontarem que certos algoritmos quânticos perfomaram de forma muito mais eficiente que certos algoritmos clássicos, especialistas questionam se esses exemplos podem ser traduzidos para vantagens aplicáveis em problemas reais.

Um exemplo é a afirmação do Google em 2009, quando seus pesquisadores sugeriram ter alcançado supremacia quântica, demonstrando como o Sycamore levou apenas 200 segundos para um cálculo que demoraria dez mil anos em um supercomputador clássico. No entanto, a própria IBM questionou a conquista, publicando um artigo que sugeria uma técnica aprimorada que permitira ao supercomputador clássico concluir a operação em dois dias e meio, tempo bem menor que o sugerido inicalmente pela Google.[27]

Da mesma forma, com o Willow, a Google novamente faz afirmações sobre a superioridade na execução do RCS, mas esse é um teste que naturalmente favorece o desempenho

do sistema quântico, uma vez que consiste na execução de circuitos quânticos aleatórios e na medição dos resultados, uma tarefa que é computacionalmente difícil para supercomputadores clássicos.[29]

Além disso, o RCS não tem relevância prática, sendo apenas um experimento que demonstra velocidade do processamento sem resolver problemas reais, o que pode estar sendo utilizado para gerar uma expectativa além da realidade sobre o estado atual da computação quântica. Conseguir traduzir os problemas reais em algoritmos quânticos para extrair os resultados desejados, como no algoritmo de Shor, é um desafio por si só, que exige um esforço intelectual de pesquisadores e desenvolvedores.

Outro dos desafios da área é o custo associado a construção e manutenção de hardware quântico, tanto monetário quanto energético. *Qbits* supercondutores, por exemplo, exigem temperaturas de resfriamento da ordem de milikelvin, próximas do zero absoluto. É importante ressaltar que supercomputadores clássicos atuais também usam energia em enorme escala, como o Frontier, que consome 21.1 megawatts para operar, o equivalente a uma conta de mais de 23 milhões de dólares por ano em energia.[38]

Um caminho que já é percorrido hoje e pode se desenvolver ainda mais é o de utilização híbrida de computadores clássicos e quânticos, que utilizam dos princípios quânticos sem depender de processadores quânticos complexos. Esse é o exemplo da parceria da Volskwagen com a D-Wave em 2019, que utilizou essa técnica para tentar evitar congestinoamentos no trânsito antes mesmo que ocorressem.[37]

A realidade é que o futuro da computação quântica ainda é incerto, com avanços significativos constantes, mas com desafios ainda não resolvidos. O uso da computação quântica em larga escala e livre de erros depende da melhoria dos algoritmos, soluções de escalabilidade e definição de problemas adequados para essa tecnologia, possibilitando uma transformação do paradigma atual.

Capítulo 4

Conclusão

Esse trabalho buscou demonstrar a natureza da computação quântica, seus avanços significativos e as promessas ainda não realizadas, enquanto aponta os desafios que se colocam no caminho desse desenvolvimento. Ao longo do texto, foi explorado o desenvolvimento histórico da computação quântica, desde fundamentos teóricos até experimentos práticos. A natureza dos*qubits*, as propriedades quânticas relevantes, a forma das portas quânticas e o funcionamnto de algoritmos como o de Shor foram explorados para ajudar a esclarecer o potencial quântico de resolver problemas não facilmente solucionáveis pela computação clássica.

Diante de tantas expectativas, o presente trabalho buscou também apontar os principais desafios da área, como a dificuldade da correção de erros e coerência dos*qubits*. Os esforços de gigantes como IBM, Google e Microsoft foram comentados, incluindo seus esforços para o desenvolvimento, acessibilidade e criação de soluções na computação quântica, buscando atingir o estado de escalabilidade e viabilidade econômica. O interesse dessas empresas em um futuro com funcionalidade quântica total permitiria o domínio destas em áreas como cripografia, otimização, simulações, entre outras.

Por fim, mesmo sem atingir ainda todo o seu potencial, os fundamentos teóricos relacionados à computação quântica, o estado dos avanços até hoje e os investimentos que estão sendo feitos apontam para um futuro promissor, ainda que não imediato. O progresso deve vir, no entanto, atrelado a desenvolvimentos no campo legislativo e ético, assim como com qualquer nova tecnologia com potencial tão disruptivo.

Em uma análise pessoal, esse texto foi de grande importância para apresentar áreas e conceitos da computação que me eram desconhecidos até então. Por se tratar de um assunto atual, em uma fase inicial em seu desenvolvimento, foi muito interessante estar presente e informado em um momento tão oportuno do ciclo dessa tecnologia. No entanto, esses mesmos pontos positivos geraram dificuldades constantes, uma vez que a maioria das informações presentes nesse texto não fazem parte da grade padrão do curso, tornando o aprendizado de assuntos novos uma exigência a cada tópico. Termino esse trabalho com uma base sólida mais extensa, somando-se àquela fornecida pelo resto das matérias e pronto para me aprofundar cada vez mais nos temas aprendidos.

Referências Bibliográficas

[1] ARUTE, F.; ARYA, K.; BABBUSH, R. et al. Quantum supremacy using a programmable superconducting processor. Nature, v. 574, p. 505–510, 2019. Disponível em: https://doi.org/10.1038/s41586-019-1666-5. Acesso em: 15 nov. 2024.

[2] BROOKS, Michael. "Quantum computers: what are they good for?"Nature, vol. 617, maio 2023, pp. S1-S3. Disponível em: https://www.nature.com/articles/d41586-023-01692-9. Acesso em: 30 nov. 2024.

[3] FEYNMAN, Richard P. Simulating physics with computers. International Journal of Theoretical Physics, v. 21, n. 6/7, p. 486, 1982.

[4] NASA. Google and NASA achieve quantum supremacy. 23 out. 2019. Disponível em: https://www.nasa.gov/technology/computing/google-and-nasa-achieve-quantum-supremacy/. Acesso em: 18 out. 2024.

[5] INTERNATIONAL BUSINESS MACHINES CORPORATION. Encyclopædia Britannica. Disponível em: https://www.britannica.com/topic/International-Business-Machines-Corporation/. Acesso em: 27 nov. 2024.

[6] PTI. Quantum leap in computing as Google claims supremacy. Business Standard, 23 out. 2019. Disponível em: https://www.business-standard.com/article/pti-stories/quantum-leap-in-computing-as-google-claims-supremacy-119102301575_1.html. Acesso em: 10 dez. 2024.

[7] CHEN, Y.; ZHANG, Z.; LI, Y. et al. Quantum computing research progress. arXiv preprint arXiv:2311.16505, 2023. Disponível em: https://arxiv.org/abs/2311.16505. Acesso em: 05 nov. 2024.

[8] QISKIT DEVELOPMENT TEAM. Qiskit Aer Documentation. Disponível em: https://qiskit.github.io/qiskit-aer/. Acesso em: 22 out. 2024.

[9] CHICAGO QUANTUM. It's colossal: creating world's largest dilution refrigerator. Disponível em: https://chicagoquantum.org/news/its-colossal-creating-worlds-largest-dilution-refrigerator. Acesso em: 30 out. 2024.

[10] NO-CLONING THEOREM. Wikipedia: The Free Encyclopedia. Disponível em: https://en.wikipedia.org/wiki/No-cloning_theorem. Acesso em: 05 dez. 2024.

[11] CLARKE, P. Microsoft's quantum computer: Quantinuum. IEEE Spectrum, 2023. Disponível em: https://spectrum.ieee.org/microsoft-quantum-computer-quantinuum. Acesso em: 04 dez. 2024.

[12] HARROW, A. W.; HASIDIM, A.; LLOYD, S. Quantum algorithm for linear systems of equations. Physical Review Letters, v. 103, n. 15, p. 150502, 2009. Disponível em: https://arxiv.org/abs/1208.0928. Acesso em: 20 out. 2024.

[13] FITZSIMONS, J. Quantum Computing Lecture 13. University of Cambridge, 2020. Disponível em: https://www.cl.cam.ac.uk/teaching/1920/QuantComp/Quantum_Computing_Lecture_13.pdf. Acesso em: 07 dez. 2024.

[14] DURANTON, S. Quantum now. Forbes, 26 jun. 2024. Disponível em: https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/. Acesso em: 21 nov. 2024.

[15] IBM. "Expanding the IBM Quantum Roadmap to Anticipate the Future of Quantum-Centric Supercomputing."IBM Quantum Blog, 10 maio 2022. Disponível em: https://www.ibm.com/quantum/blog/ibm-quantum-roadmap-2025. Acesso em: 22 nov. 2024.

[16] GOOGLE. Quantum AI Roadmap. Disponível em: https://quantumai.google/roadmap. Acesso em: 08 nov. 2024.

[17] O'BRIEN, J. L.; FURUSAWA, A.; VUCKOVIC, J. Photonic quantum technologies. Nature Photonics, v. 3, p. 687–695, 2009. Disponível em: https://www.nature.com/articles/npjqi20151. Acesso em: 09 dez. 2024.

[18] MICROSOFT. Microsoft achieves first milestone towards a quantum supercomputer. 21 jun. 2023. Disponível em: https://azure.microsoft.com/en-us/blog/quantum/2023/06/21/microsoft-achieves-first-milestone-towards-a-quantum-supercomputer/. Acesso em: 14 dez. 2024.

[19] STAMATOPOULOS, Nikitas; EGGER, Daniel J.; SUN, Yue; ZOUFAL, Christa; ITEN, Raban; SHEN, Ning; WOERNER, Stefan. "Option Pricing using Quantum Computers."arXiv preprint, arXiv:1905.02666, 2019. Disponível em: https://arxiv.org/pdf/1905.02666. Acesso em: 29. nov 2024.

[20] OTTERBACH, Johannes S.; MANENTI, Riccardo; ALIDOUST, N.; et al. "Unsupervised Machine Learning on a Hybrid Quantum Computer."arXiv preprint, arXiv:1712.05771, 2017. Disponível em: https://arxiv.org/pdf/1712.05771. Acesso em: 11 dez. 2024.

[21] CALTECH. How Will Quantum Technologies Change Cryptography?. Disponível em: https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography. Acesso em: 19 nov. 2024.

[22] HARVARD GAZETTE. Ethical concerns mount as AI takes bigger decision-making role in more industries. 2020. Disponível em: https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/. Acesso em: 17 out. 2024.

[23] UNITED STATES. H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act. Disponível em: https://www.congress.gov/bill/117th-congress/house-bill/7535. Acesso em: 25 nov. 2024.

[24] EUROPEAN COMMISSION. European Declaration on Quantum Technologies. 06 dez. 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies. Acesso em: 03 nov. 2024.

[25] MDPI. "Quantum Computing: Advances and Challenges."MDPI, vol. 6, no. 4, 2023, p. 39. Disponível em: https://www.mdpi.com/2624-960X/6/4/39. Acesso em: 25 fev. 2025.

[26] LIU, Junyu; JIANG, Hansheng; SHEN, Zuo-Jun Max. Potential Energy Advantage of Quantum Economy. arXiv preprint, arXiv:2308.08025, 2023. Disponível em: https://arxiv.org/abs/2308.08025. Acesso em: 26 fev. 2025.

[27] CONOVER, Emily. "Google's Quantum Supremacy Claim and Its Controversy."Science News, 23 dez. 2019. Disponível em: https://www.sciencenews.org/article/google-quantum-supremacy-claim-controversy-top-science-stories-2019-yir. Acesso em: 24 fev. 2025.

[28] REUTERS. "Microsoft Creates Chip It Says Shows Quantum Computers Are Years, Not Decades Away."Reuters, 19 fev. 2025. Disponível em: https://www.reuters.com/technology/microsoft-creates-chip-it-says-shows-quantum-computers-are-years-not-decades-2025-02-19/. Acesso em: 27 fev. 2025.

[29] QRYPTONIC. "Revisiting Google's Willow Quantum Chip."Qryptonic Substack, 2025. Disponível em: https://qryptonic.substack.com/p/revisiting-googles-willow-quantum?utm_campaign=post&utm_medium=web. Acesso em: 23 fev. 2025.

[30] UNIVERSITY OF MARYLAND. "Moore Announces $1B Capital of Quantum Initiative Centered at UMD."Today UMD, 2025. Disponível em: https://today.umd.edu/moore-announces-1b-capital-of-quantum-initiative-centered-at-umd. Acesso em: 24 fev. 2025.

[31] DATA CENTER DYNAMICS. "Canadian Government Pledges CA$74M to Fund Quantum Technology Projects."Data Center Dynamics, 2025. Disponível em: https://www.datacenterdynamics.com/en/news/canadian-government-pledges-ca74m-to-fund-quantum-technology-projects/. Acesso em: 26 fev. 2025.

[32] GOOGLE. "Google Willow Quantum Chip."Google Research Blog, 2025. Disponível em: https://blog.google/technology/research/google-willow-quantum-chip/. Acesso em: 25 fev. 2025.

[33] CLAUDON, Baptiste; PIQUEMAL, Jean-Philip; MONMARCHÉ, Pierre. Quantum Speedup for Nonreversible Markov Chains. arXiv preprint, arXiv:2501.05868, 2025. Disponível em: https://arxiv.org/pdf/2501.05868. Acesso em: 27 fev. 2025.

[34] ABC NEWS. "Quantum Public Investment Larger Than Private."ABC News, 13 nov. 2024. Disponível em: https://www.abc.net.au/news/2024-11-13/quantum-public-investment-larger-than-private-psiquantum-/104591346. Acesso em: 25 fev. 2025.

[35] USA-ASEAN BUSINESS COUNCIL. "Government of Singapore Increases Investment in Quantum Computing and AI."USA-ASEAN Business Council, 2025. Disponível em: https://www.usasean.org/article/government-singapore-increases-investment-quantum-computing-and-ai. Acesso em: 26 fev. 2025.

[36] SEEKING ALPHA. "IonQ: No Scaling Out of a Unprofitability Problem."Seeking Alpha, 2024. Disponível em: https://seekingalpha.com/article/4641287-ionq-no-scaling-out-of-a-unprofitability-problem. Acesso em: 23 fev. 2025.

[37] D-WAVE SYSTEMS INC. "How Volkswagen is Using Practical Quantum Computing to Explore Traffic Optimization and More."Disponível em: https://www.dwavequantum.com/media/bbximewp/dwave_vw_case_study_v8.pdf. Acesso em: 22 fev. 2025.

[38] BOGER, Yuval. "The dual-pronged energy-saving potential of quantum computers."Data Center Dynamics, 26 jun. 2023. Disponível em: https://www.datacenterdynamics.com/en/opinions/the-dual-pronged-energy-saving-potential-of-quantum-computers/. Acesso em: 23 fev. 2025.