Computação Quântica: desafios e oportunidades

Franklin de Lima Marquezino

Resumo

A computação quântica é a proposta de controlar sistemas físicos quânticos, como átomos ou fótons, para resolver alguns problemas que são muito difíceis nos computadores clássicos. Embora ainda esteja em estágio experimental, seu potencial revolucionário promete transformar áreas estratégicas da economia global. Este artigo explora o impacto potencial da computação quântica em diversos setores, destacando suas aplicações mais promissoras, como a simulação de sistemas quânticos e a otimização combinatória. O artigo discute os principais desafios tecnológicos e econômicos, incluindo a correção de erros e a escalabilidade dos sistemas quânticos, e também aborda o impacto social e a necessidade de educar a sociedade sobre essa tecnologia emergente.

Abstract

Quantum computing is the proposal to control quantum physical systems, such as atoms or photons, to solve problems that are extremely difficult for classical computers. Although still in an experimental stage, its revolutionary potential promises to transform strategic areas of the global economy. This article explores the potential impact of quantum computing across various sectors, highlighting its most promising applications, such as quantum system simulation and combinatorial op-

timization. It also discusses key technological and economic challenges, including error correction and system scalability, as well as the social impact and need for public education on this emerging technology.

Introdução

A mecânica quântica é uma área da física moderna que surgiu no início do século XX para estudar sistemas em escalas extremamente pequenas, como partículas subatômicas e moléculas, já que a mecânica clássica não funcionava corretamente nessas situações. Sistemas quânticos se comportam de forma muito diferente dos objetos com os quais interagimos cotidianamente, de modo que algumas previsões da mecânica quântica podem causar grande perplexidade. Se lançarmos um dado comum dentro de uma caixa podemos afirmar com convicção, mesmo antes de olhar o resultado, que a face voltada para cima tem um número de um a seis. Se esse dado fosse do tamanho de um átomo, a mecânica quântica prevê que situações mais estranhas poderiam acontecer. Antes de olhar dentro da caixa, o „dado quântico“ poderia existir em um estado como se de alguma forma tivesse várias faces voltadas para cima ao mesmo tempo. Mas ao olharmos dentro da caixa, veríamos somente um dado comum, com um único número voltado para cima. Claro, trata-se apenas de uma metáfora, com suas limitações. No entanto, por mais estranho que um cenário desses possa parecer, o arcabouço matemático da mecânica quântica tem sido extremamente bem sucedido em prever resultados de experimentos com altíssima precisão. Pensando ainda na metáfora anterior, o leitor certamente deve ter diversos questionamentos sobre o que realmente há dentro da caixa e o que ocorre objetivamente ao observarmos seu interior. De fato, discussões acaloradas sobre as interpretações da mecânica quântica vem acontecendo até os dias de hoje, sendo esta uma importante área de estudo da filosofia da ciência.

Muito além de ser um campo fascinante do ponto de vista teórico, a mecânica quântica já vem sendo usada há muitas décadas para aplica-

ções tecnológicas. Por exemplo, os transistores e o *laser* são tecnologias quânticas de primeira geração, que portanto somente foram viáveis a partir da compreensão de fenômenos quânticos. A computação quântica, um dos assuntos tecnológicos mais discutidos nos últimos anos e tema principal deste artigo, é um exemplo típico de tecnologia quântica de segunda geração, por utilizar fenômenos quânticos mais diretamente e de forma mais controlada. Trata-se de um modelo computacional que emprega sistemas físicos quânticos como componentes fundamentais dos computadores, permitindo realizar certos tipos de cálculos de forma muito mais eficiente do que com computadores clássicos. Alguns desses cálculos teriam impactos profundos na sociedade ao serem resolvidos de forma eficiente – eis o motivo pelo qual a computação quântica tem atraído tanta atenção. Por exemplo, cálculos precisos e eficientes em química quântica têm impactos profundos tanto na indústria farmacêutica como na produção de fertilizantes para o agronegócio. A fatoração de inteiros grandes representa uma ameaça concreta para a segurança da informação e obriga a adoção de métodos criptográficos mais seguros que os atuais.

Dado que a computação quântica tem potencial para impactar profundamente tantos setores estratégicos, alguns fatos básicos sobre essa tecnologia precisam ser conhecidos por todos os cidadãos, independentemente de sua área de atuação na sociedade. No entanto, muitas pessoas que desejam aprender sobre computação quântica sentem-se intimidadas pela expectativa de lidar com conceitos muito avançados de física moderna. Em nossa sociedade, a mecânica quântica é reconhecida como um dos tópicos mais difíceis de aprender e inacessível para quem não possui sólida formação em CTEM[1]. Essa visão elitista da ciência é problemática e traz consequências negativas, contribuindo para a proliferação de ideias erradas sobre as tecnologias quânticas. Por isso é importante que a sociedade seja educada sobre a ciência moderna, a fim

1 Ciência, Tecnologia, Engenharia e Matemática.

de compreender o potencial e as limitações da tecnologia, e dessa forma tomar decisões sensatas quanto à alocação de recursos.

Em primeiro lugar, é importante esclarecer que a computação quântica não é capaz de resolver problemas que são impossíveis para computadores clássicos. Há, de fato, problemas matemáticos que são provadamente impossíveis de se resolver mesmo pelos computadores mais sofisticados – são os problemas chamados „incomputáveis". Um exemplo típico é o problema da parada, estudado por Alan Turing, e nem mesmo um computador quântico conseguiria resolvê-lo. Portanto, a primeira distinção importante que devemos fazer é entre eficiência e computabilidade. A promessa da computação quântica é ser mais eficiente, porém não faz sentido prometer a resolução de problemas incomputáveis.

Um segundo mito que precisa ser combatido é de que a computação quântica irá resolver qualquer problema com facilidade, ou que será mais eficiente que a computação clássica em todos os aspectos. Na verdade, nem tudo pode ser resolvido eficientemente na computação quântica. E além disso, muitos problemas para os quais a computação clássica já possui soluções eficientes não podem ser melhorados no mundo quântico. Dessa forma, é esperado que a computação quântica sempre coexista com a computação clássica, e que unidades de processamento quânticas sejam usadas para resolver problemas específicos.

Outro engano comum é pensar que seja trivial desenvolver algoritmos quânticos a partir de ideias conhecidas da computação clássica. A realidade é que a maioria dos algoritmos quânticos são altamente contra-intuitivos e o seu desenvolvimento possui muitas particularidades que requerem habilidades diversas daquelas de desenvolvedores clássicos. Testar um software quântico, por exemplo, é muito mais difícil, pois não se pode observar estados intermediários do cálculo sem causar seu colapso e a perda de propriedades quânticas.

Para obter vantagem a partir de algoritmos quânticos precisamos de hardware quântico, cujo desenvolvimento ainda é um grande desafio tecnológico. Já existem computadores quânticos, porém todos são ainda

muito limitados e sujeitos a erros, de modo que ainda não são capazes de resolver problemas práticos de forma mais eficiente que os clássicos. Alguns desses computadores quânticos podem ser acessados gratuitamente na nuvem, com algumas limitações, sendo boas ferramentas para treinamento e pesquisa acadêmica. No entanto, a maioria dos computadores quânticos atualmente é acessada mediante pagamento por tempo de uso. Também é possível comprar computadores quânticos para uso exclusivo, porém isso ainda requer um altíssimo investimento nos dias de hoje.

Neste artigo, algumas noções essenciais de mecânica quântica e computação quântica são apresentados na Seção 1, sem entrar em detalhes técnicos e sem usar notação matemática avançada. As principais aplicações da computação quântica são apresentadas na Seção 2. Os principais obstáculos para o desenvolvimento da computação quântica são apresentados na Seção 3. Os progressos recentes e as perspectivas de médio e longo prazo, são apresentados na Seção 4. Finalmente, as discussões finais e conclusões são apresentadas na Seção 5.

1. Fundamentos de computação quântica

Na computação digital clássica, a unidade básica de informação é o bit, termo cunhado por Claude Shannon na década de 1940 como abreviação de *binary digit*, ou dígito binário. Portanto, o bit é uma variável que pode assumir a cada instante somente um dentre dois valores possíveis, usualmente denotados por 0 ou 1. É importante observar que o bit não é uma mera idealização matemática, mas pode também possuir uma realização física. Basicamente qualquer sistema físico clássico com dois estados bem definidos e facilmente distinguíveis é apto a representar um bit. Pode-se utilizar para representar os bits 0 e 1, por exemplo, dois níveis de tensão de uma corrente elétrica, ou duas polarizações perpendiculares de um fóton, ou a carga armazenada de um capacitor.

Se substituirmos esses sistemas clássicos por sistemas quânticos com dois níveis de energia bem distinguíveis, de modo que possamos

controlá-los e medi-los, teremos uma realização física para um *bit quântico*, ou abreviadamente *qubit*. Enquanto o bit pode assumir a cada instante somente um valor dentre dois possíveis, o qubit pode existir em um estado que é uma combinação destes dois. Intuitivamente, podemos pensar que o qubit vale 0 e 1 ao mesmo tempo, com certos pesos associados. Chamamos a esse estado de *superposição quântica*.

Ainda de modo intuitivo, podemos considerar o que teríamos ao juntar dois qubits. As superposições possíveis nesse caso envolveriam os estados 00, 01, 10 e 11, com seus respectivos pesos. A propriedade da superposição dá origem ao *paralelismo quântico*. A ideia é que ao efetuarmos uma operação sobre uma superposição de estados, essa operação é aplicada simultaneamente a todos os termos da superposição. Com dois qubits, conseguimos realizar paralelamente operações sobre quatro termos distintos. Com três qubits, o paralelismo atua sobre oito termos. E assim por diante, com crescimento exponencial.

Uma outra consequência muito curiosa do princípio da superposição quântica envolvendo dois ou mais qubits é o *emaranhamento*. Um exemplo de emaranhamento seria a superposição envolvendo dois qubits na qual somente os estados 00 e 11 possuem algum peso. Uma pergunta que podemos fazer nesse caso é como escrever o estado de cada qubit individualmente. A resposta é que não podemos fazê-lo, pois os dois qubits estão muito fortemente correlacionados. Se observamos o primeiro qubit colapsando-o para o estado 0, então nesse caso o segundo também necessariamente terá colapsado para 0. E, da mesma forma, se o primeiro qubit colapsa para o estado 1, então o segundo qubit também colapsa para 1. E curiosamente isso é verdade mesmo que os dois qubits correspondam a partículas quânticas muito distantes entre si – uma na Terra e outra em Marte, digamos. Trata-se de um fenômeno dos mais contra-intuitivos da mecânica quântica e sem paralelos diretos no nosso cotidiano.

Somente o paralelismo quântico e o emaranhamento não são suficientes para garantir ganhos expressivos de desempenho nos computadores quânticos. Um erro comum transmitido com frequência é dizer

que o computador quântico é mais rápido porque tenta todas as soluções possíveis em paralelo. Na verdade, somente com o paralelismo mas sem a *interferência quântica*, não seria possível ter vantagem por meio da computação quântica. A interferência é o efeito que permite a alguns termos de uma superposição serem amplificados enquanto outros são atenuados – de modo semelhante aos padrões de interferência que vemos nas ondas em um lago, ao se lançar pedras sobre o mesmo. Para desenvolver algoritmos quânticos eficientes, além de explorar o paralelismo precisamos também garantir que os termos correspondentes à solução desejada sejam amplificados por meio de interferência construtiva, enquanto os demais termos sejam atenuados por interferência destrutiva.

Uma importante diferença entre computadores clássicos e quânticos é o momento de ler o resultado. A medição na mecânica quântica implica necessariamente um colapso aleatório e irreversível do estado quântico. Devido à forma como se dá a medição em sistemas quânticos, os computadores quânticos são particularmente sensíveis a interferências do ambiente. Por um lado, precisamos controlar o computador de modo que realize o cálculo que desejamos, portanto ele precisa interagir com o meio externo de alguma forma. Por outro lado, essa interação pode agir como uma medição, ainda que involuntária, causando a degradação do estado quântico e consequentemente do cálculo que se desejava realizar. Essa perda das propriedades quânticas chamada de *descoerência* é um dos maiores desafios para construção de computadores quânticos hoje.

Como os computadores quânticos são tão sensíveis, somente conseguiremos extrair todo seu potencial com a ajuda de sistemas que detectem e corrijam erros. A boa notícia é que a teoria para esse tipo de sistema já é bem conhecida há muitos anos, e novos códigos ainda mais avançados vêm sendo desenvolvidos nos últimos anos. No entanto, ainda há pelo menos dois grandes obstáculos para a implementação de uma computação quântica tolerante a falhas. Em primeiro lugar, o número de qubits disponíveis deve ser muito alto para compensar os que

são perdidos devido à necessidade de redundância. Em segundo lugar, a qualidade destes deve ser bem melhor que a atual para que os erros não sejam produzidos mais rapidamente do que podem ser corrigidos.

A discussão nesta seção foi propositalmente informal, dada a restrição de espaço. Para sermos mais formais, deveríamos usar recursos da álgebra linear, que é o ramo da matemática por trás da mecânica quântica e consequentemente da computação quântica. A álgebra linear ocupa-se do estudo de objetos chamados vetores e as operações que podemos realizar entre eles satisfazendo certas propriedades. Nesse formalismo matemático, os qubits são representados por vetores, e se precisarmos juntar vários qubits podemos fazê-lo por meio de uma operação chamada produto tensorial. Os algoritmos quânticos são representados matematicamente por sequências de matrizes que, operadas sobre os vetores de qubits, os vão transformando passo a passo até alcançar a solução para o problema. A medição dos qubits, ou seja, a leitura do resultado, é representada matematicamente por meio de projetores. O profissional que deseja se aprofundar na computação quântica deve buscar uma boa formação matemática, especialmente em álgebra linear.

Para uma introdução mais abrangente sobre os conceitos de computação quântica, o leitor pode consultar o livro de Marquezino, Portugal e Lavor (2019). Para continuar se aprofundando, o leitor pode estudar o livro de Wong (2022), que é mais extenso apesar de ainda adequado como introdução. Ambos os livros introduzem de forma concisa os principais conceitos e notações de álgebra linear.

2. Aplicações da computação quântica

Um erro comum cometido por quem se inicia na computação quântica e que é propagado por notícias exageradas, é a ideia de que computadores quânticos serão capazes de resolver todo tipo de problema exponencialmente mais rápido que os computadores clássicos. Há também quem pense que um algoritmo clássico ficaria automaticamente mais rápido apenas se fosse executado em um computador quântico.

Todas essas ideias são exageradas e não correspondem à realidade. Na verdade, há certos tipos de problemas que os computadores quânticos poderão resolver muito mais rapidamente que os clássicos, enquanto para outros não faria diferença. Por esse motivo, o mais provável é que no futuro computadores clássicos e quânticos co-existam.

Uma analogia é a forma como GPUs[2] não utilizadas hoje em dia como auxiliares para diversos problemas que envolvem cálculos intensos de matrizes. No futuro, é provável que além de GPUs, os centros de computação de alto desempenho lançarão mão também de QPUs[3] para resolver cálculos específicos. Não faz sentido utilizar um equipamento mais caro para resolver problemas com os quais processadores comuns e GPUs já lidam muito bem, então a tendência é que todos esses dispositivos trabalhem juntos nos futuro. Os computadores quânticos somente substituirão os clássicos um dia, se por algum motivo improvável eles se tornarem mais baratos que os clássicos – não necessariamente na sua construção, mas no consumo de energia ou manutenção, por exemplo. Sendo assim, é importante conhecer os tipos de problemas em que os processadores quânticos serão úteis.

A primeira aplicação pensada para a computação quântica foi a simulação de sistemas quânticos, conforme proposto por Feynman (1982). Ele sugeriu que seria mais eficiente usar um computador quântico para simular outros sistemas quânticos, algo que os computadores clássicos encontram extrema dificuldade em fazer. A simulação quântica tem importância central em áreas como o desenvolvimento de fármacos, permitindo a modelagem precisa de interações moleculares que podem levar à criação de novos medicamentos. Além disso, a descoberta de novos nanomateriais com propriedades personalizadas para aplicações tecnológicas é outro campo que pode ser revolucionado por essa tecnologia. Um exemplo prático é a simulação de catalisadores para aumentar a eficiência de processos industriais, como a produção de fer-

2 *Graphical Processing Unit*.

3 *Quantum Processing Unit.*

tilizantes, que consome grandes quantidades de energia. A computação quântica poderá proporcionar enormes economias energéticas e benefícios ambientais significativos.

O primeiro algoritmo quântico com uma aplicação prática muito evidente mesmo para não-especialistas e com grande potencial de impacto na sociedade foi o algoritmo de Shor para fatoração de inteiros, apresentado em 1994. A capacidade de fatorar números inteiros grandes de forma eficiente tem como consequência a obsolescência de diversos métodos criptográficos que utilizamos amplamente para realizar compras na Internet ou para transações bancárias. Portanto, a notícia de que computadores quânticos poderiam decifrar esses códigos secretos causou uma revolução na forma como a computação quântica era vista. O que antes era uma curiosidade científica de físicos teóricos passou a ser tratado como um assunto de alta relevância prática mesmo por quem não era especialista. O algoritmo de Shor requer computadores quânticos tolerantes a falhas, que ainda estão muito distantes da realidade atual, como veremos mais adiante neste artigo. Portanto, os sistemas criptográficos atuais ainda permanecerão seguros por muitos anos. Ainda assim, setores que dependem de altíssima confidencialidade já estão investindo em métodos de criptografia *pós-quânticos*, mais sofisticados, e que permanecerão seguros mesmo quando tivermos computadores quânticos operando de acordo com seu pleno potencial.

Outro desenvolvimento que causou grande impacto na história da computação quântica foi o algoritmo de Grover, em 1996. Esse algoritmo apresentou um ganho de desempenho bem mais modesto que o de Shor, porém para um problema de aplicação muito mais geral. O algoritmo de Grover serve para encontrar um elemento em uma lista não ordenada ou sem uma estrutura. Por exemplo, encontrar uma palavra no dicionário é fácil pois as entradas estão em ordem alfabética. Se não estivessem, teríamos que procurar palavra por palavra, e no pior caso teríamos que consultar o livro inteiro. Com o algoritmo de Grover, o número de consultas é da ordem de raiz quadrada do número de palavras – não é um ganho exponencial como o algoritmo de Shor, mas ainda

assim é interessante. Talvez o resultado não pareça muito impressionante através dessa metáfora, pois dicionários sempre estão em ordem alfabética. No entanto, há muitos problemas práticos que não conseguimos resolver diretamente, mas conseguimos verificar se uma tentativa de solução que nos é apresentada está correta ou não. Podemos resolver esse tipo de problema por tentativa e erro, testando um candidato de cada vez. Essa abordagem é semelhante a procurar uma palavra específica em uma lista desordenada, o que certamente é muito ineficiente. Computadores quânticos, entretanto, podem tirar proveito da superposição de estados e da interferência, e dessa forma encontram a solução para o problema muito mais rapidamente.

A computação quântica tem grande potencial para resolver problemas de otimização combinatória, o que pode trazer benefícios significativos para a indústria. Muitos desses avanços são possíveis graças ao uso de algoritmos híbridos, que combinam o melhor dos computadores quânticos e clássicos. Nessa abordagem, parte dos cálculos ocorre em circuitos quânticos parametrizados, enquanto otimizadores clássicos ajustam esses parâmetros – de modo semelhante ao treinamento de uma rede neural artificial. Esse método permite que os circuitos sejam mais compactos, tornando-os mais adequados para a limitação dos dispositivos quânticos atuais. Além disso, a técnica de *annealing* quântico, que é análoga ao *simulated annealing* da computação clássica, também tem sido aplicada com sucesso em problemas de otimização. Essa técnica é particularmente útil em problemas onde a busca pela solução global ótima precisa navegar por um vasto espaço de soluções, sendo usada em campos como logística, planejamento e finanças.

Uma aplicação importante da computação quântica é a resolução de sistemas lineares de equações, problema recorrente em diversas áreas, desde a física até a economia, e para o qual os algoritmos quânticos oferecem um ganho exponencial de eficiência em relação aos métodos clássicos. No entanto, utilizar esse tipo de algoritmo em computadores quânticos não é tão simples quanto na computação clássica, pois o resultado final é codificado em estados de superposição, impossibilitando

uma medição direta como fazemos em sistemas clássicos. Apesar desse desafio, várias propostas têm sido desenvolvidas para aplicar essa técnica na solução de equações diferenciais, o que abre portas para aplicações em áreas como a simulação da dinâmica de fluidos, onde a precisão e a rapidez na resolução de sistemas lineares são essenciais. Esses avanços mostram o potencial de algoritmos quânticos para resolver problemas matemáticos complexos, possibilitando simulações mais rápidas e precisas em diversas áreas da ciência e da engenharia.

Para uma exposição mais completa e mais técnica das aplicações da computação quântica o leitor pode consultar Dalzell *et al.* (2024). Os leitores que já possuem certa experiência em programação de computadores podem se aprofundar nessas aplicações e até mesmo executá-las em computadores quânticos reais, estudando algum kit de desenvolvimento como o IBM Qiskit (JAVADI-ABHARI *et al.*, 2024).

3. Principais desafios atuais

Apesar de todo o entusiasmo recente em torno da computação quântica, deve-se ter em mente que ainda há grandes desafios a serem superados antes que a computação quântica avance da fase experimental para aplicações comerciais. Conhecer esses desafios é importante para manter as expectativas alinhadas com a realidade.

3.1 Desafios tecnológicos

Um primeiro obstáculo para o avanço da computação quântica ainda é a qualidade dos qubits e a escalabilidade dos sistemas. Os qubits atuais, apesar de terem melhorado recentemente, ainda possuem um nível de ruído elevado. Além disso, a construção de computadores com milhares ou milhões de qubits, que seriam necessários para resolver problemas práticos, ainda é uma meta distante. A dificuldade em controlar muitos qubits de forma estável, sem comprometer a coerência e introduzir erros, impõe limites ao crescimento dos sistemas quânticos.

Soma-se a isso o fato de não termos ainda uma direção clara de implementação física dos qubits. Há muitas propostas diferentes – como supercondutores, armadilhas de íons, átomos neutros, fótons, dentre outros – cada qual com suas vantagens e desvantagens.

Devido à extrema sensibilidade dos qubits ao ambiente externo, até mesmo mínimas interações podem gerar erros que, se não corrigidos, comprometem o resultado final dos cálculos. Diferente da computação clássica, onde bits errôneos podem ser facilmente detectados e corrigidos, a correção de erros em sistemas quânticos é muito mais complexa. No entanto, para atingir todo o potencial da computação quântica é necessário ainda avançar em sistemas de correção de erros até finalmente atingir o marco da computação quântica tolerante a falhas. Apesar de avanços significativos, implementar esses mecanismos em larga escala continua a ser um desafio (CAMPBELL, 2024).

Para mais detalhes sobre os desafios da computação quântica no estágio atual, em que somente temos à disposição computadores com poucos qubits e muito ruído, o leitor pode consultar Bharti *et al.* (2022). Para mais detalhes sobre a construção de computadores quânticos, existe o recente livro de Majidy, Wilson e Laflamme (2024).

3.2. Desafios econômicos

O custo de desenvolvimento e implementação de computadores quânticos é extremamente elevado, o que restringe sua disponibilidade a poucos centros de pesquisa e grandes empresas tecnológicas. A criação de ambientes econômicos que permitam o investimento contínuo nessa área será crucial para que a computação quântica tenha impacto global. Programas de cooperação internacional e incentivos governamentais serão fundamentais para democratizar o acesso à computação quântica e garantir que o progresso tecnológico seja amplamente distribuído.

Países em desenvolvimento como o Brasil estão aproveitando o acesso a plataformas de computação quântica via nuvem, fornecidas por grandes empresas como IBM e Amazon, para avançar na pesquisa

e no desenvolvimento sem a necessidade de construir hardware próprio. Esse modelo de colaboração internacional permite que pesquisadores brasileiros explorem as potencialidades da computação quântica e apliquem algoritmos quânticos a problemas locais. Através de parcerias com empresas globais, o Brasil pode acelerar seu acesso à tecnologia quântica, superando as limitações econômicas e tecnológicas que ainda impedem a construção de computadores quânticos próprios.

Outro obstáculo significativo é a escassez de profissionais capacitados para trabalhar com computação quântica. Apesar de as universidades e centros de pesquisa estarem começando a oferecer mais programas de estudo sobre o tema, o número de especialistas ainda é insuficiente para atender à crescente demanda. Desenvolver um ecossistema de talentos que vá além dos cientistas e engenheiros quânticos, abrangendo também desenvolvedores de software e profissionais de TI capazes de integrar as tecnologias quânticas aos sistemas clássicos, será essencial para que a computação quântica tenha um impacto sustentável a longo prazo.

4. Progressos recentes e perspectivas

Nos últimos anos, a pesquisa em computação quântica avançou significativamente, com vários grupos reivindicando a chamada supremacia quântica – o ponto em que um dispositivo quântico supera até o melhor supercomputador clássico em uma tarefa específica, não necessariamente de interesse prático. O experimento mais notório, apesar de um tanto controverso, foi realizado pela Google em 2019, quando seu processador *Sycamore* completou um cálculo em cerca de 200 segundos, o que de acordo com eles levaria cerca de 10.000 anos usando o supercomputador clássico mais rápido do mundo. No entanto, a IBM contestou essa afirmação, sugerindo que a mesma tarefa poderia ser realizada por um supercomputador clássico em poucos dias, desde que utilizando uma abordagem melhorada. Desde então, outros grupos também realizaram experimentos que alcançaram supremacia quântica, motivando o desenvolvimento de algoritmos clássicos que os superaram. A

supremacia quântica, portanto, ainda é um alvo em movimento. Apesar das controvérsias desses resultados, principalmente devido aos aspectos de marketing envolvidos, eles são importantes por marcarem uma tendência de progresso contínuo da área, demonstrando o potencial da computação quântica em resolver problemas que seriam inviáveis para sistemas clássicos.

Apesar dos grandes desafios tecnológicos ainda existentes, a produção de computadores quânticos têm acelerado não somente em quantidade, mas também em qualidade. Diversas empresas têm estabelecido *roadmaps* ousados para o desenvolvimento de hardware quântico e os têm cumprido razoavelmente bem até aqui, com progressos significativos. Uma parceria entre os finlandeses VTT e IQM tem sido muito bem sucedida, tendo atingido recentemente a marca de 30 computadores quânticos produzidos e a capacidade de produzir até 20 computadores por ano. A Quantinuum espera ter computadores quânticos universais e tolerantes a falhas até 2030, e possui um histórico recente de muitos marcos importantes de desenvolvimento atingidos, inclusive na área de códigos de correção de erros. A IBM planeja entregar já em 2029 computadores quânticos de 200 qubits, com correção de erros, e capacidade de executar um total de 100 milhões de operações.[4]

Portanto, a computação quântica tem um enorme potencial econômico. Jean-François *et al.* (2024), do Boston Consulting Group, projetam que a computação quântica poderá gerar entre US$ 450 bilhões e US$ 850 bilhões em valor econômico, com um mercado na faixa de US$ 90 bilhões a US$ 170 bilhões até 2040. Valores semelhantes também são previstos pelo *Quantum Technology Monitor 2024* de McKinsey & Company[5], que inclui na análise outras tecnologias quânticas correlacionadas, como comunicação e sensores quânticos. Os investimentos

4 O *roadmap* completo está disponível em https://www.ibm.com/roadmaps/quantum/2024/. Acesso em 21 de outubro de 2024.

5 Disponível em https://www.mckinsey.com/featured-insights/the-rise-of-quantum-computing. Acesso em 21 de outubro de 2024.

públicos no setor têm sido bastante elevados em países como China, Alemanha, Reino Unido e Estados Unidos da América.

5. Considerações finais

Em conclusão, a computação quântica apresenta um potencial transformador em várias áreas estratégicas, incluindo a saúde, segurança da informação, finanças, logística e otimização de processos industriais. Aplicações como a simulação de sistemas quânticos e o desenvolvimento de novos fármacos demonstram o alcance dessa tecnologia, que pode impactar desde a produção de fertilizantes até a indústria farmacêutica. Embora os recentes avanços sejam promissores, é crucial alinhar as expectativas à realidade. A computação quântica não substituirá os sistemas clássicos; em vez disso, coexistirá com eles, fornecendo soluções específicas para alguns problemas. Além disso, os computadores quânticos ainda enfrentam desafios tecnológicos significativos, como a correção de erros, a estabilidade dos qubits e a escalabilidade dos sistemas. Somente quando esses obstáculos forem superados poderemos atingir todo seu potencial.

Também é essencial destacar o papel das considerações políticas e sociais no avanço dessa tecnologia. Uma vez que a computação quântica pode impactar profundamente tantos setores estratégicos para uma nação, não é prudente manter o país em alta dependência de soluções estrangeiras. Os investimentos do Brasil no setor ainda são baixos, tanto no setor público quanto no privado. Finalmente, é importante destacar que além de pesquisa e desenvolvimento, é essencial investir também na formação de profissionais qualificados para garantir que os benefícios dessa tecnologia sejam plenamente alcançados.

Referências

BHARTI, Kishor; CERVERA-LIERTA, Alba; KYAW, Thi Ha; *et al*. Noisy intermediate-scale quantum (NISQ) algorithms. **Reviews of Modern Physics**, v. 94, n. 1, p. 015004, 2022.

CAMPBELL, Earl. A series of fast-paced advances in Quantum Error Correction. **Nature Reviews Physics**, v. 6, n. 3, p. 160–161, 2024.

DALZELL, Alexander M.; MCARDLE, Sam; BERTA, Mario; *et al*. Quantum algorithms: A survey of applications and end-to-end complexities. 2023. Disponível em: <http://arxiv.org/abs/2310.03011>. Acesso em: 10 outubro 2024.

FEYNMAN, Richard P. Simulating physics with computers. **International Journal of Theoretical Physics**, v. 21, n. 6, p. 467–488, 1982.

JAVADI-ABHARI, Ali; TREINISH, Matthew; KRSULICH, Kevin; *et al*. Quantum computing with Qiskit. 2024. Disponível em: <http://arxiv.org/abs/2405.08810>. Acesso em: 10 outubro 2024.

JEAN-FRANÇOIS, Bobier; MATT, Langione; CASSIA, Naudet-Baulieu; *et al*. **The Long-Term Forecast for Quantum Computing Still Looks Bright**. BCG Global. Disponível em: <https://on.bcg.com/3ye4ey2>. Acesso em: 18 outubro 2024.

MAJIDY, Shayan; WILSON, Christopher; LAFLAMME, Raymond. **Building Quantum Computers: A Practical Introduction**. Cambridge: Cambridge University Press, 2024.

MARQUEZINO, Franklin de Lima; PORTUGAL, Renato; LAVOR, Carlile. **A Primer on Quantum Computing**. 1. ed. [s.l.]: Springer, 2019.

WONG, Thomas G. **Introduction to classical and quantum computing**. Omaha, Nebraska: Rooted Grove, 2022.

Franklin de Lima Marquezino · Bacharel em Ciência da Computação pela Universidade Católica de Petrópolis (UCP). Mestre e Doutor em Modelagem Computacional pelo Laboratório Nacional de Computação Científica (LNCC). Professor Associado da Universidade Federal do Rio de Janeiro (UFRJ), atuando no Núcleo Multidisciplinar de Pesquisa em Computação (NUMPEX-Comp) do Campus Duque de Caxias Prof. Geraldo Cidade, e no Programa de Engenharia de Sistemas e Computação (PESC) do Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia (COPPE). Em 2011, sua tese de doutorado sobre Computação Quântica recebeu o Prêmio CAPES como melhor tese do Brasil na Área Interdisciplinar. Em 2024 foi Pesquisador Visitante no Centre for Quantum Computer Science da Universidade da Letônia. É membro do corpo editorial do periódico Theoretical Computer Science (TCS-C: Theory of Natural Computing).