A História da Computação Quântica

Bernardo Cunha Capoferri, Guilherme Dantas Rameh
Henrique Martinelli Frezzatti, Lívia Sayuri Makuta

18 de Novembro de 2021

Resumo

Será abordado neste artigo a história da computação quântica. Neste âmbito, será discutido como esta nova ciência surgiu, com quais propósitos, e o que é esperado para o seu futuro. Além disso, serão abordadas também as tecnologias decorrentes dessa ciência e o quanto podem alterar e melhorar a vida dos seres humanos em diversos ramos da tecnologia.

Palavras-chave: Computação Quântica; História; Aplicações; Presente; Futuro; Tecnologia; Ciência.

1 Introdução

No presente artigo serão tratados sobre tópicos importantes acerca do tema da computação quântica. Esse ramo, ultimamente, tem apresentado muitos avanços e promete revolucionar o futuro da computação, dessa forma, torna-se importante compreendê-lo. A fim de esclarecer os conceitos básicos desse tema, os momentos mais importantes de sua história e o que é esperado para o futuro com suas possíveis aplicações, é a razão pela qual este documento foi escrito.

2 Conceitos básicos da computação quântica

Para entender computação quântica, é necessário compreender alguns conceitos importantes e que provocaram grandes avanços para a teoria quântica. Também serão feitas algumas comparações com a computação clássica e atual, fazendo paralelos para ilustrar alguns dos conceitos.

Em computadores normais, o menor componente, e o mais essencial, é o transistor, cujo papel é permitir ou não que elétrons passem por ele. Assim,

ele pode assumir dois valores distintos (quando passam elétrons e quando não), ou seja, 1 ou 0. Na computação clássica, essa saída é chamada de "bits". Para a computação quântica, a menor unidade de informação é chamada de "qubits", que pode ser por exemplo um fóton, e os valores 0 e 1 podem ser a polarização vertical ou horizontal desse fóton. Porém, diferentemente de bits normais, um qubit não precisa se limitar apenas a esses dois valores. A partir da teoria quântica, um qubit pode estar em qualquer proporção entre esses dois estados, e isso é chamado de superposição. Enquanto o qubit não tiver seu valor testado, ele permanece em estado de superposição e, consequentemente, seu valor não é determinado, ou melhor, seu valor são todos os valores possíveis que ele pode assumir ao mesmo tempo. Todavia, assim que se verifica seu valor, ele é forçado ao seu real estado (no caso do fóton, verticalmente ou horizontalmente polarizado), 1 ou 0. Como os qubits podem estar em todas as possibilidades ao mesmo tempo, quanto mais qubits são usados em um sistema, as possibilidades crescem exponencialmente em potência de 2 [1].

Outro conceito fundamental que, em conjunto com a sobreposição, permite a evolução e importância da computação quântica é o *entanglement*, ou emaranhamento (em português) [2]. Esse conceito ilustra uma relação muito próxima entre diversos qubits, promovendo uma reação a mudanças de estado de seus qubits parceiros, instantaneamente. Dessa forma, ao medir - e, portanto, forçar uma determinação de estado - em apenas um qubit, é possível deduzir as propriedades de seus parceiros sem precisar determiná-los também.

O próximo passo para sistemas mais complexos é o uso de portas quânticas (equivalente a portas lógicas) e a manipulação de qubits e probabilidades. Portas lógicas na computação clássica recebem um conjunto de entradas e produzem uma saída determinada. Uma porta quântica recebe um conjunto de sobreposição, manipula probabilidades, e produz um outro conjunto de sobreposição como saída.

Portanto, um computador quântico pega um conjunto de qubits, aplica algumas portas quânticas, os emaranha e manipula as possibilidades para, por fim, medi-las e colapsar as superposições em uma sequência real de uns e zeros. Assim, é possível obter todas as possibilidades de resultados para essa operação ao mesmo tempo. Logo, ao se aproveitar de superposição e emaranhamento, é possível alcançar resultados - e verificá-los ao decorrer de diversas tentativas - muito mais rápido do que um computador normal conseguiria.

3 Breve introdução da história da computação quântica até os anos 2000

A ideia de um dispositivo computacional baseado na mecânica quântica foi explorada já na década de 1970 por físicos e cientistas da computação, e esta surgiu quando os cientistas estavam investigando os limites físicos fundamentais da computação. Se a tecnologia continuasse a obedecer à "Lei de Moore"[1], então o tamanho cada vez menor dos circuitos compactados em chips de silício acabaria por atingir um ponto em que os elementos individuais não seriam maiores do que alguns átomos [3]. Entretanto, uma vez que as leis físicas que governam o comportamento e as propriedades do circuito na escala atômica são inerentes à mecânica quântica por natureza, e não clássicas, surgiu a questão natural de saber se um novo tipo de computador poderia ser criado com base nos princípios da física quântica.

Uma das influências para isso nessa década de 70 foi o físico Stephen Wiesner, da *Columbia University*, o qual sugeriu que propriedades quânticas dos fótons poderiam ser usadas para gerar "dinheiro quântico" que seria impossível de falsificar. Essa visão, segundo ele, era armazenar algumas dezenas de fótons em armadilhas de luz em cada nota e garantir que a polarização desses fótons fosse conhecida apenas pelo banco. Uma vez que os estados quânticos eram impossíveis de copiar, a nota do banco então nunca poderia ser copiada e, quem quisesse verificar a nota, precisaria apenas levá-la ao banco emissor, o qual poderia usar o conhecimento prévio das polarizações para testar a veracidade da nota. Dessa forma, Wiesner propôs que o processamento quântico de informações seria uma possível maneira de realizar melhor as tarefas criptológicas, o que serviu de inspiração para a geração de físicos quânticos que desenvolveram a criptografia quântica, de maneira a enviar uma mensagem com uma segurança melhor [4].

Contudo, Wiesner apenas publicou seu trabalho *"Conjugate Coding"* [5] em 1983 pela *ACM SIGACT News*, enquanto os primeiros quatro artigos sobre informações quânticas foram publicados por Alexander Holevo (1973), Roman Pavlovich Poplavskii (1975) e Roman Ingarden (1976). A começar por Holevo, um matemático russo que fez contribuições substanciais nos fundamentos matemáticos da teoria quântica, estatística quântica e teoria da informação quântica, sendo que, nesse ano de 1973, quando publicou seu artigo *"Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel"* [6], obteve um limite superior para

[1] A observação feita em 1965 por Gordon Moore, cofundador da Intel, de que o número de transistores por polegada quadrada em circuitos integrados dobrou a cada 18 meses desde que o circuito integrado foi inventado.

a quantidade de informação clássica que pode ser extraída de um conjunto de estados quânticos (informação acessível) por medições quânticas, o que ficou conhecido como o "Teorema de Holevo" [7]. Já Poplavskii, em seu trabalho *"Thermodynamical models of information processing"* [8], mostrou a inviabilidade computacional de simular sistemas quânticos em computadores clássicos, devido ao princípio de superposição. Por sua vez, o físico e matemático polonês Ingarden, em 1976, publicou um artigo intitulado *"Quantum Information Theory"* [9], que descreveu uma das primeiras tentativas de criar uma teoria da informação quântica, mostrando que a teoria da informação clássica de Shannon [2] não pode ser diretamente generalizada para o caso quântico, mas sim que é possível construir uma teoria quântica da informação que é uma generalização da teoria de Shannon, isso através de uma mecânica quântica generalizada de sistemas abertos e um conceito generalizado de observáveis (os chamados semi-observáveis).

Entretanto, as contribuições mais conhecidas inicialmente foram feitas apenas no início dos anos 1980 por Paul A. Benioff do *Argonne National Laboratory* em Illinois, David Deutsch da *University of Oxford*, Richard Feynman do *California Institute of Technology* e Kazuhiro Igeta e Yoshihisa Yamamoto do Instituto de Tecnologia da Universidade de Tóquio. De início, temos Paul Benioff, o qual é considerado um dos patronos da computação quântica por ter sido o primeiro a descrever um modelo mecânico de um computador quântico em 1980. Em seu trabalho, intitulado *"The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines"* [10], foi demonstrado que um computador poderia operar de acordo com as leis da mecânica quântica, apresentando uma descrição da equação de Schrödinger das máquinas de Turing. Em maio de 1981, na primeira conferência sobre Física da Computação realizada no MIT *(Massachusetts Institute of Technology)* [11], Paul Benioff e Richard Feynman deram palestras sobre computação quântica. Ao assistir a palestra de Feynman, Benioff observou que parecia impossível simular com eficiência uma evolução de um sistema quântico em um computador clássico. Dois anos após essa conferência, Benioff desenvolveu seu modelo original de uma máquina de Turing a partir da mecânica quântica, sendo esse momento considerado o *"big bang"* da computação quântica. A partir dessa base na área da computação quântica, em 1985, David Deutsch em seu artigo *"Quantum theory, the Church-Turing principle and the universal quantum computer"* [12] relata que o primeiro computador quântico univer-

[2] A teoria de Shannon estudou as possibilidades de otimizar a transmissão das mensagens, entendidas como sequências de símbolos, deixando de lado a parte do significado. Além disso, definiu os componentes do modelo de comunicação, como por exemplo: emissor, receptor e canal.

sal, assim como uma máquina de Turing universal, pode simular qualquer outra máquina de Turing, porém, com uma melhor eficiência, com propriedades notáveis não reproduzíveis por nenhuma máquina de Turing, o que foi chamado de princípio de Church-Turing-Deutsch. O computador quântico universal conseguiria simular qualquer outro computador quântico com, no máximo, uma desaceleração polinomial. Por fim, foi apenas em 1988 que Yoshihisa Yamamoto e Kazuhiro Igeta publicaram o artigo *"Quantum mechanical computers with single atom and photon fields"* [13] e propuseram a primeira realização física de um computador quântico, incluindo a porta CNOT de Feynman, com uma abordagem que utiliza átomos e fótons e é progenitora da computação quântica moderna e dos protocolos de rede que usam fótons para transmitir qubits e átomos para realizar operações de dois qubits.

No que concerne o progresso nos algoritmos quânticos, tem-se que esse começou na década de 1990, com a descoberta do algoritmo Deutsch-Josza em 1992, o que foi apresentado no artigo: *"Rapid solutions of problems by quantum computation"* [14] por David Deutsch and Richard Jozsa. O algoritmo de Deutsch-Josza foi descoberto por David Deutsch e Richard Jozsa que propuseram uma classe de problemas que podiam ser resolvidos com melhor desempenho pelo algoritmo que formularam em um computador quântico, mas que seria muito mais difícil para qualquer algoritmo clássico determinístico, o qual poderia apresentar falhas e erros no processo, sendo este talvez o primeiro resultado na complexidade computacional dos computadores quânticos, provando que eles eram capazes de realizar algumas tarefas computacionais bem definidas com melhor performance do que qualquer computador clássico. Em 1993, por sua vez, foi descoberto por Daniel Simon, da *Montreal University*, o algoritmo de Simon, descrito por ele em: *"On the Power of Quantum Computation"* [15]. Esse acontecimento teve gênese quando Simon inventou um problema de oráculo para o qual um computador quântico seria exponencialmente mais rápido do que o melhor algoritmo clássico de um computador convencional [16] e, com isso, ofereceu evidências convincentes de que o modelo quântico pode ter um poder teórico de complexidade significativamente maior do que a máquina de Turing probabilística. Esse algoritmo foi base para o algoritmo de Shor, descoberto por Peter Shor do Bell Labs da AT&T em Nova Jersey em 1994 e relatado em sua obra: *"Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"* [17]. Esse algoritmo permite que um computador quântico fatore grandes números inteiros rapidamente. Dessa forma, resolve o problema de fatoração e o problema de logaritmo discreto, sendo que pode teoricamente quebrar muitos dos criptossistemas em uso atualmente. Como consequência, essa invenção despertou um enorme

interesse em computadores quânticos, mesmo fora da comunidade física.

Nesse mesmo ano de 1994, Cirac e Zoller propuseram a realização experimental da porta quântica CNOT com íons aprisionados, a qual se tornou uma pesquisa intitulada *"Quantum Computations with Cold Trapped Ions"* [18]. Um ano depois, Peter Shor e Andrew Steane propuseram (de maneira independente) o primeiro esquema para correção de erros quânticos, tendo Shor publicando o artigo: *"Good Quantum Error-Correcting Codes Exist"* [19] e Steane publicando: *"Multiple-Particle Interference and Quantum Error Correction"* [20]. No ano de 1996, seguindo a proposta de Cirac e Zoller, Christopher Monroe e David Wineland no NIST (Boulder, Colorado) realizaram experimentalmente a primeira porta lógica quântica (a porta NOT controlada (CNOT)) com íons presos. Ainda em 1996, Lov Grover, da Bell Labs inventou um algoritmo de busca quântica descrito em: *"A fast quantum mechanical algorithm for database search"* [21], que usa o fenômeno de paralelismo quântico para buscar soluções para o problema de busca. Esse algoritmo apresenta uma melhoria quadrática em relação ao algoritmo clássico e, embora essa melhoria quadrática não tenha sido tão relevante quanto a melhoria para fatoração, registros discretos ou simulações físicas, o algoritmo pode ser aplicado a uma variedade muito maior de problemas [22]. Por fim, apenas um ano depois, no final dos anos 90, o primeiro modelo para computação quântica baseado em técnicas de ressonância magnética nuclear (RMN) foi proposto, sendo que esta técnica foi realizada em 1998 com um registro de 2 qubits sendo aumentada para 7 qubits no *National Laboratory of Los Alamos*, em 2000. Além disso, em 31 de julho de 2000, Arun K. Pati e Samuel L. Braunstein provaram a teoria que era impossível de se apagar uma cópia de um estado quântico [23].

4 Computação quântica no século XXI

No primeiro ano da virada do século XXI, os cientistas Emanuel Knill, Raymond Laflamme, e Gerard Milburn do departamento de energia do *National Laboratory of Los Alamos* e do *Centre for Quantum Computing Technology of University of Queensland*, avançaram na busca por um computador quântico funcional, explorando a tecnologia existente de uma maneira nova e inesperada. Foi demonstrado pelos cientistas que a computação quântica óptica é possível com fontes de apenas um fóton, *beam splitter*, *phase shifters* e detectores de fótons, abrindo o caminho para mais experimentos computacionais nesta área, já que a análise de distúrbios em fótons é atrativa devido a simplicidade de ser observada [24]. Ainda nesse ano, passando do campo da óptica para o eletromagnético, Michael N. Leuenberger e Daniel Loss pu-

blicaram o artigo: *"Quantum computing in molecular magnets"* [25], no qual propuseram uma implementação do algoritmo de Grover, o qual usa ímãs moleculares que são sistemas de estado sólido com um grande spin, de tal forma que seus próprios estados de spin os tornam candidatos naturais para sistemas de partícula única. Dessa forma, mostraram que, teoricamente, os ímãs moleculares podem ser usados para construir dispositivos de memórias densos e eficientes baseados no algoritmo de Grover.

No ano de 2004, um grupo de trabalho de Rainer Blatt, físico experimental alemão-austríaco, em conjunto com uma equipe do *National Institute of Standards and Technology in Boulder*, Colorado, EUA, conseguiu pela primeira vez transferir a informação quântica de um átomo em uma maneira totalmente controlada para outro átomo (teletransporte) [26]. A revista científica Nature relatou esses experimentos que foram conduzidos separadamente e deu-lhes um lugar de destaque na capa. Nesse experimento, relatado no artigo: *"Deterministic quantum teleportation of atomic qubits"* [27], três partículas foram posicionadas em uma armadilha de íons segmentada que auxilia o endereçamento de qubits individuais e, ao final do experimento, alcançaram uma fidelidade média de 78 por cento, o que superou a fidelidade de outros protocolos que não utilizavam essa técnica de emaranhamento. Além disso, dois anos depois, o grupo de trabalho de Blatt já conseguiu emaranhar até oito átomos de maneira controlada de forma a criar o primeiro computador quântico com 8 qubits que foi apresentado na *Innsbruck University* [28].

Já em 2007, físicos do *National Institute of Standards and Technology* (NIST) transferiram informações entre dois "átomos artificiais"por meio de vibrações eletrônicas em um cabo de alumínio micro fabricado, demonstrando um novo componente para potenciais computadores quânticos ultrapoderosos do futuro [29]. A configuração lembra uma versão em miniatura de uma linha de transmissão de televisão à cabo, mas com alguns recursos adicionais poderosos, que incluem circuitos de supercondutores com uma resistência elétrica igual a 0 e bits de dados multitarefa que obedecem às regras incomuns da física quântica. Um ano depois, em 2008, uma equipe de cientistas da *Princeton University* em New Jersey, da *Oxford University* no Reino Unido e do *Lawrence Berkeley National Laboratory* do *Energy Department of California*, apoiados em parte pela *National Science Foundation*, relataram na revista Nature que conseguiram armazenar informações no núcleo de um átomo [30]. No experimento que fizeram, o sistema fazia uso do núcleo e dos elétrons de um átomo de fósforo embutido em um cristal de silício, sendo que tanto o elétron quanto o núcleo se comportavam como minúsculos ímãs quânticos capazes de armazenar informações quânticas. A partir disso, os pesquisadores moveram as informações para o núcleo, onde sobreviveram

por muito mais tempo - cerca de 3 a 4 segundos -, o que se tornou uma descoberta significativa, já que antes dessa técnica ser desenvolvida, o maior tempo que conseguiam preservar a informação quântica no silício era menos de um décimo de segundo.

Em 2009, uma equipe do NIST liderada por Jonathan Home revelou o primeiro dispositivo de pequena escala que fazia uso de íons *ultracold* para demonstrar separadamente todas as etapas necessárias para a computação quântica, o que envolve inicializar os qubits, armazená-los em íons, realizar uma operação lógica em um ou dois qubits, transferir a informação entre diferentes locais no processador e ler os resultados do qubit individualmente [31]. Essa configuração de Home tinha uma precisão geral de 94 por cento, algo impressionante para um dispositivo quântico, mas não boa o suficiente para ser usada em um computador quântico de grande escala. Por sua vez, em 2010, físicos da Universidade Johannes Gutenberg de Mainz liderados pelo Dr. Arno Rauschenbeutel, desenvolveram uma interface quântica que conecta partículas de luz a átomos [32]. A interface é baseada em uma fibra de vidro ultrafina e é adequada para a transmissão de informações quânticas, o qual é um pré-requisito essencial para a comunicação quântica que, segundo Rauschenbeutel, pode ser utilizada para a transmissão segura de dados por meio de criptografia quântica e também para os computadores quânticos.

No entanto, foi apenas em 2017, com a IBM, que dois grandes passos foram dados na área através do desenvolvimento de um computador quântico universal de 17 qubits, ou seja, tendo capacidade de realizar diversos problemas quânticos ao contrário de outros modelos muito mais especializados [33]. Além disso, no final desse mesmo ano, já anunciaram o desenvolvimento do primeiro computador com 50 qubits [34][35][36], um marco importante, já que esse era o maior número de bits quânticos estimado para os melhores supercomputadores simularem, preparando o horizonte para novos avanços na área quântica. Porém, vale notar que esse computador não provou o conceito.

Em janeiro de 2019, a IBM continuou demonstrando sua dominância na área quando revelou o *"Q system one"* , o primeiro computador quântico a poder ser acessado pela nuvem e já vir embutido com os avançados sistemas de refrigeração [37]. No mesmo ano, pesquisadores da *Google* declararam a tão desejada "supremacia quântica" quando o chip da empresa de 53 qubits chamado de *"Seycamore"* levou, aproximadamente, 200 segundos para realizar uma operação que levaria os melhores computadores clássicos mais de 10.000 anos [38].

Apesar de ainda não ser tão desenvolvida quanto a tecnologia dos computadores clássicos, até por ser considerada recente, a tecnologia de computadores quânticos está chegando mais e mais perto do livre acesso ao público. Em 2021, a empresa privada IBM, em conjunto com Fraunhofer-Gesellschaft, pôs

em operação o primeiro computador quântico comercial [39]. Antes disso, o público só tinha acesso ao universo da computação quântica a partir de processamentos pela nuvem. Nesse sentido também, o governo alemão liberou uma verba de 2 bilhões de euros [40] para garantir o escalonamento de qubits em cada supercomputador, na tentativa de precaver já que aos poucos o desenvolvimento de supercomputadores está chegando ao seu limite físico. Outro passo importante tomado neste ano foi pela companhia canadense D-wave, que vem trabalhando na integração de computadores tradicionais e quânticos. Eles utilizaram um sistema chamado quantum annealer, uma versão mais limitada de um computador quântico [39].

Ainda em 2021, em 16 de novembro, a IBM revelou o computador quântico mais poderoso do mundo [41]. Esse computador, chamado de Eagle, funciona com 127 qubits e, segundo a empresa, tem o dobro da potência do Zuchongzhi, o computador quântico chinês de 56 qubits, que foi revelado em julho e que foi considerada a máquina mais poderosa do mundo em sua categoria, capaz de resolver, em 70 minutos, uma tarefa que supercomputadores clássicos demorariam pelo menos 8 anos para calcular. Zaira Nazario, gerente técnica de Teoria da Computação Quântica e Aplicações da IBM afirmou para o jornal El País que o Eagle é um marco por ultrapassar a barreira dos 100 qubits, e acredita que já atingiu o limite de tal forma que seu poder de computação não pode mais ser simulado com computadores clássicos, já que, segundo a IBM, o número de bits clássicos precisos para igualar o poder de computação desse novo processador excede o número de átomos existentes nas mais de 7,5 bilhões de pessoas vivas atualmente [42].

5 O futuro da computação quântica

"Desde a otimização de rotas de aviões ao aperfeiçoamento de trajetórias de robôs, os problemas que, até então, parecem impossíveis para as tecnologias atuais, serão possíveis com o uso da computação quântica e sua disseminação com o passar dos anos. Em todas as indústrias, a computação quântica irá abordar uma vasta gama de problemas, desde a otimização à simulação e à aprendizagem automática", é o que diz a multinacional *Honeywell* [43].

Dessa forma, pode-se compreender que a computação quântica tem um grande futuro próspero e repleto de possíveis inovações, tanto na vida das grandes empresas quanto no cotidiano. Essa nova ciência terá influências em diversas áreas da tecnologia, como na aeronáutica, química, saúde, robótica e nas finanças.

Com relação à área da aeronáutica, tem-se que a computação quântica po-

derá ajudar, e muito, com a determinação das melhores rotas para um avião de acordo com as diversas variáveis existentes do meio ambiente e condições de temperatura e clima, evitando tempestades ou maus tempos, limitando e evitando perturbações. Além disso, essa nova tecnologia permitirá que seja possível determinar os melhores aeroportos para se distribuir, previamente, componentes de reposição para aviões, além de atribuir e distribuir recursos para toda a tripulação, passageiros etc, afetando minimamente os horários de manutenção.

Quando trata-se da área da química, é possível que haja diversas aplicações dessa nova ciência nesse ramo, podendo simular propriedades e comportamentos de novas estruturas moleculares. Logo, com essa tecnologia em mãos, será possível prever e simular novas substâncias e moléculas, evitando possíveis problemas que poderiam surgir com esses novos componentes, além de aumentar exponencialmente o universo criativo para o surgimento de novas substâncias inovadoras, tornando esse ramo cada vez mais inovador.

No ramo da saúde e da farmácia, a computação quântica será responsável por acelerar, significativamente, o processo desde o descobrimento de um novo tratamento médico até chegar às mãos do paciente, tornando os avanços na saúde como um todo cada vez mais rápidos, seguros e responsivos com a realidade em que se vive, evitando possíveis problemas, como novas pandemias, de forma mais rápida e eficaz. Não só isso, com essa nova ciência será possível reduzir os custos do processo de descobrimento e fabricação de um novo tratamento médico, tornando-os mais acessíveis à população.

Na área da logística e da robótica, essa nova tecnologia quântica será fundamental por ajudar na localização, montagem e posicionamento de sensores os quais são os responsáveis por receber dados e integrá-los no robô, permitindo o *machine learning* e fazendo com que este tome decisões mais significativas e precisas; assim, a computação quântica irá acelerar, aprimorar e tornar esse processo mais eficaz e preciso, além de determinar os melhores percursos de locomoção dos robôs pelas fábricas e armazéns.

Por fim, no ramo das finanças, essa combinação da mecânica quântica com a computação poderá gerar os melhores investimentos possíveis, analisando diversas variáveis que influenciam na variância dos preços das ações e lucros gerados. Ademais, também será possível identificar, de forma mais rápida, possíveis fraudes e transações em anonimato, aumentando a segurança ainda mais de transações e contas bancárias.

Em suma, pode-se afirmar que há diversas áreas da tecnologia em que a computação quântica poderia ser ou será extremamente ativa e benéfica para o avanço destas, além do aumento da eficácia e aprimoramento da segurança digital. No entanto, para que seja possível atingir esses objetivos de avanço tecnológico será necessário cerca de, pelo menos, 5 a 10 anos para os

avanços mais simples ocorrerem e se tornarem, de fato, viáveis à sociedade e às grandes empresas.

Além disso, há alguns desafios a serem enfrentados pela engenharia da computação para que essa tecnologia seja, de fato, viável e utilizada em larga escala; alguns desses desafios são a perda de informação e de memória dos qubits em supercondução pois, nessas condições, os qubits perdem frequentemente, em torno de nanossegundos, informações num geral; um outro grande desafio é a grande taxa de erros geradas pelos computadores quânticos, uma vez que é de extrema dificuldade criar um deste com baixas taxas de erros, além do fato de que a instabilidade do ambiente e a falta de materiais fazem perder dados quânticos, o que reduz o período de utilidade de um qubit. Ademais, também há a necessidade de realizar funções lógicas enquanto se trabalha com os qubits para reduzir possíveis interferências sonoras eletromagnéticas, o que pode diminuir a coerência de um qubit [2]. Logo, corrigir erros na computação quântica, ao se comparar com a computação clássica, é desafiador, uma vez que os erros são contínuos e difíceis de se identificar, além de que pode ocorrer a perda de dados salvos em qubits.

Sendo assim, há diversas áreas de atuação e um futuro muito próspero para a computação quântica, porém, para viabilizar essas inovações e novas tecnologias, tornando-as reais, será necessário ultrapassar diversas dificuldades e desafios dessa nova ciência, criando a necessidade de se compreender cada vez mais o uso e problemas dos qubits e como contorná-los.

Referências

[1] Kurzgesagt - In a Nutshell: "Computadores Quânticos Explicados - Limites da Tecnologia Humana". Publicado em: 08/12/2015. Acessado: 21/11/2021 às 16:22. Acesso disponível em <shorturl.at/mpCGS >;

[2] Sukhpal S. G., Adarsh K., Singh H., Singh M., Kaur K., Usman M., Buyya R.: "Quantum Computing: A Taxonomy, Systematic Review and Future Directions". Publicado em: 09/2020. Acessado: 18/11/2021 às 13:47. Acesso disponível em <https://arxiv.org/ftp/arxiv/papers/2010/2010.15559.pdf >;

[3] Hagar A., Cuffaro M.: "Quantum Computing". Atualizado em: 30/09/2019. Acessado: 18/11/2021 às 14:30. Acesso disponível em <shorturl.at/hsuGH >;

[4] Lutomirski A., Aaronson S., Farhi E., Gosset D., Hassidim A., Kelner J., Shor W. P.: "Breaking and making quantum money: toward a new

quantum cryptographic protocol". Publicado em: 23/12/2009. Acessado: 18/11/2021 às 14:18. Acesso disponível em <shorturl.at/hlDN2 >;

[5] Wiesner S.: "Conjugate Coding". Publicado em: 01/01/1983. Acessado: 18/11/2021 às 14:31. Acesso disponível em <shorturl.at/yDQZ8 >;

[6] Amaral B.: "A Cota de Holevo". Publicado em: 26/04/2021. Acessado: 20/11/2021 às 16:40. Acesso disponível em <shorturl.at/amDMZ >;

[7] Quantik: "The Holevo bound". Atualizado em: 18/08/2020. Acessado: 18/11/2021 às 21:25. Acesso disponível em <shorturl.at/ivyDL >;

[8] Poplavskiĭ P. R.: "Thermodynamic models of information processes". Publicado em: 29/11/2019. Acessado: 18/11/2021 às 14:10. Acesso disponível em <shorturl.at/buzDU >;

[9] Ingarden S. R.: "Quantum Information Theory". Publicado em: 13/12/1975. Disponível online em: 27/03/2002. Acessado: 20/11/2021 às 16:53. Acesso disponível em <shorturl.at/ptLOS >;

[10] Benioff P.: "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing Machines". Publicado em: 05/1980. Acessado: 20/11/2021 às 17:03. Acesso disponível em <shorturl.at/ajoA7 >;

[11] Wikipedia: "Timeline of quantum computing and communication". Atualizado em: 16/11/2021 às 20:35 (UTC). Acessado: 18/11/2021 às 14:03. Acesso disponível em <shorturl.at/fxJMY >;

[12] Deustch D.: "Quantum theory, the Church-Turing principle and the universal quantum computer". Publicado em: 13/07/1984. Acessado: 20/11/2021 às 17:10. Acesso disponível em <shorturl.at/xyTXY >;

[13] Yamamoto Y., Igeta K.: "Quantum mechanical computers with single atom and photon fields". Publicado em: 21/07/1988. Acessado: 21/11/2021 às 17:13. Acesso disponível em <shorturl.at/hH189 >

[14] Deutsch D., Jozsa R.: "Rapid Solutions of problems by quantum computation". Publicado em: 08/12/1992. Acessado: 20/11/2021 às 17:15. Acesso disponível em <shorturl.at/suxCW >;

[15] Simon R. D.: "On the power of quantum computation". Publicado em: 10/1997. Acessado: 20/11/2021 às 17:18. Acesso disponível em <shorturl.at/bdpzE >;

[16] Qiskit: "Simon 's Algorithm". Publicado em: Não disponível. Acessado: 18/11/2021 às 14:25. Acesso disponível em <shorturl.at/ntKS7 >;

[17] Shor W. P.: "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". Publicado em: 25/01/1996. Acessado: 20/11/2021 às 17:30. Acesso disponível em <shorturl.at/iFY12 >;

[18] Zoller P., Cirac I. J.: "Quantum Computations with Cold Trapped Ions". Publicado em: 15/05/1995. Acessado: 21/11/2021 às 17:13. Acesso disponível em <shorturl.at/nqF56 >.

[19] Shor W. P., Calderbank R. A.: "Good Quantum Error-Correcting Codes Exist". Publicado em: 16/04/1996. Acessado: 20/11/2021 às 17:48. Acesso disponível em <shorturl.at/gkxQX >;

[20] Steane A.: "Multiple-particle interference and quantum error correction". Publicado em: 08/11/1996. Acessado: 20/11/2021 às 17:43. Acesso disponível em <shorturl.at/jJRW4 >;

[21] Grover K. L.: "A fast quantum mechanical algorithm for database search". Publicado em: 01/07/1996. Acessado: 21/11/2021 às 15:40. Acesso disponível em <shorturl.at/nC079 >;

[22] Dillenburg F. R., Prado D. S.: "O Algoritmo de Grover". Publicado em: Não disponível. Acessado: 21/11/2021 às 16:01. Acesso disponível em <shorturl.at/juRSX >;

[23] Braunstein L. S., Pati K.A.: "Impossibility of deleting an unknown quantum state". Publicado em: 31/07/2000. Acessado: 21/11/2021 às 16:08. Acesso disponível em <shorturl.at/oAJS5 >;

[24] Knill, E., Laflamme, R. & Milburn, G.: "A scheme for efficient quantum computation with linear optics". Publicado em: 04/01/2021. Acessado: 18/11/2021 às 14:13. Acesso disponível em <shorturl.at/mwDV3 >;

[25] Loss D., Leuenberger N. M.: "Quantum computing in molecular magnets". Publicado em: 07/06/2001. Acessado: 21/11/2021 às 18:20. Acesso disponível em <shorturl.at/stKR8 >.

[26] Wikipedia.: “Rainer Blatt”. Atualizado em: 25/01/2021. Acessado: 27/11/2021 às 20:20. Acesso disponível em <shorturl.at/vxER0 >.

[27] Barrett, M., Chiaverini, J., Schaetz, T. et al.: “Deterministic quantum teleportation of atomic qubits”. Publicado em: 17/06/2004 . Acessado: 27/11/2021 às 19:29. Acesso disponível em <shorturl.at/ijwG4 >.

[28] Häffner, H., Hänsel, W., Roos, C. et al.: “Scalable multiparticle entanglement of trapped ions”. Publicado em: 01/12/2005. Acessado: 27/11/2021 às 20:13. Acesso disponível em <shorturl.at/gxAQR >.

[29] National Institute of Standards and Technology.: ”Superconducting Quantum Computing Cable Created.”Publicado em 27/09/2007. Acessado: 27/11/2021 20:37. Acesso disponível em <shorturl.at/hzY14 >.

[30] National Science Foundation: “World’s Smallest Storage Space... the Nucleus of an Atom”. Publicado em: 23/10/2008. Acessado: 18/11/2021 às 14:05. Acesso disponível em <shorturl.at/dqsFN >;

[31] Banks M.: “A decade of Physics World breakthroughs: 2009 - the first quantum computer”. Publicado em: 29/11/2019. Acessado: 18/11/2021 às 14:10. Acesso disponível em <shorturl.at/gpGJW >;

[32] E. Vetsch et al.: “Optical Interface Created by Laser-Cooled Atoms Trapped in the Evanescent Field Surrounding an Optical Nanofiber”. Publicado em: 20/05/2010. Acessado: 27/11/2021 às 20:55. Acesso disponível em: <shorturl.at/bpMUV >;

[33] Mitchell R.: “IBM to Sell Use of Its New 17-Qubit Quantum Computer over the Cloud”. Publicado em: 25/05/2017. Acessado: 21/11/2021 às 16:27. Acesso disponível em <shorturl.at/hszBO >;

[34] Knight W.: “IBM Raises the Bar with a 50-Qubit Quantum Computer”. Publicado em: 10/11/2017. Acessado: 21/11/2021 às 16:50. Acesso disponível em <shorturl.at/lxzES >;

[35] Galeon D.: “IBM Just Announced a 50-Qubit Quantum Computer”. Publicado em: 11/10/2017. Acessado: 21/11/2021 às 16:15. Acesso disponível em <shorturl.at/hDIW8 >;

[36] Summers N.: “This is what a 50-qubit quantum computer looks like”. Publicado em: 01/10/2018. Acessado: 21/11/2021 às 16:18. Acesso disponível em <shorturl.at/gCRY2 >;

[37] IBM.: “IBM unveils World’s First Integrated Quantum Computing system for Commercial Use”. Publicado em: 08/01/2019. Acessado: 21/11/2021 às 17:05. Acesso disponível em <shorturl.at/dpHP4 >;

[38] Arute, F., Arya, K., Babbush, R. et al.: “Quantum supremacy using a programmable superconducting processor”. Publicado em: 23/10/2019. Acessado: 21/11/2021 às 17:00. Acesso disponível em <shorturl.at/amEJ1 >;

[39] Infineon.: “Quantum computing - key technology of the 21st century”. Publicado em: Não disponível. Acessado: 18/11/2021 às 13:50. Acesso disponível em <shorturl.at/aqsET >;

[40] NIENABER, M.: “Germany to support quantum computing with 2 billions euros”. Publicado em: 11/05/2021. Acessado: 27/11/2021 às 21:35. Acesso disponível em: <shorturl.at/mpyGI >.

[41] Rigues R.: “IBM irá revelar computador quântico mais poderoso do mundo”. Atualizado em: 15/11/2021 às 15h41. Acessado: 20/11/2021 às 15:53. Acesso disponível em <shorturl.at/xMTW7 >;

[42] Collins H., Easterly K.: “IBM Unveils Breakthrough 127-Qubit Quantum Processor”. Atualizado em: 16/11/2021. Acessado: 20/11/2021 às 16:03. Acesso disponível em <shorturl.at/yHWX9 >;

[43] Honeywell: “Como a computação quântica irá transformar o futuro de 5 indústrias”. Atualizado em: 07/2020. Acessado: 18/11/2021 às 14:30. Acesso disponível em <shorturl.at/boLU2 >;