Computação Quântica

*Ronan Damasco**

A computação quântica, assunto antes restrito aos meios acadêmicos, ganhou espaço na mídia especializada em tecnologia e inovação. Ela traz o potencial de revolucionar a computação e criar possibilidades que, no momento, nem conseguimos imaginar. Os especialistas no tema divergem sobre a data precisa na qual teremos um computador quântico totalmente operacional. O consenso gira em torno de 5 a 10 anos. Se ainda estamos tão longe, por que falar desse assunto agora? E por que esse assunto ganhou tanta relevância recentemente? Para responder a essas perguntas, gostaria de compartilhar aqui a minha jornada de estudo e aprendizado sobre o tema.

* *Microsoft.*

1 Meu primeiro contato com a computação quântica

A primeira vez que ouvi falar de computação quântica foi em janeiro de 2018, em um evento interno da Microsoft realizado na sede da empresa em Redmond, Seattle, nos Estado Unidos. Na ocasião, uma representante da área de pesquisa da empresa mencionou uma impressionante informação: a de que um problema que levaria 1 bilhão de anos para ser resolvido por meio da computação clássica poderia ser resolvido em apenas 100 segundos utilizando-se a computação quântica. Dois pontos me chamaram a atenção nessa afirmação. O primeiro foi o termo "computação clássica". Fiquei surpreso em saber que a tecnologia de computação eletrônica digital tão avançada que usamos hoje já está sendo chamada dessa maneira. O segundo ponto foi a enorme diferença entre o tempo empregado para resolver o problema usando as duas tecnologias. De onde teriam saído esses números tão díspares? Por que tal superioridade de *performance* da computação quântica? Vim a aprender depois que essa estimativa de tempos vem da redução do grau de complexidade de um problema, conceito matemático que define como um problema escala sua complexidade, de forma exponencial ou polinomial, por exemplo. A experiência vivida naquele dia foi suficiente para despertar minha curiosidade e, a partir de então, procurei ler, estudar e fazer cursos para me aprofundar no tema da computação quântica.

2 O que é a computação quântica?

A computação quântica é uma nova forma de computação, baseada em fenômenos da mecânica quântica. A mecânica quântica é um tema muito controverso e complexo e que foi exaustivamente contestado no século passado. O próprio Albert Einstein, um dos físicos mais conhecidos pelo público em geral, foi um grande adversário da mecânica quântica. Com frases famosas como: "Deus não joga dados", para questionar o uso da estatística na mecânica quântica e "*Spooky effect at distance*", para se referenciar ao entrelaçamento de partículas, em inglês, *entanglement*, Albert Einstein não concordava com os conceitos pregados pela mecânica quântica e acreditava que existiam variáveis desconhecidas, ou ocultas, que explicariam esses fenômenos de forma mais ordenada. Após muitas décadas de discussão e inúmeros experimentos de comprovação, os físicos concluíram que não valia mais a pena discutir o entendimento dos fenômenos da mecânica quântica e, em vez disso, resolveram simplesmente aceitá-los. A famosa frase "*Shut-up and calculate*", atribuída ao físico David Mermin, reflete o fato de que a matemática comprova o que não conseguimos entender completamente. Nós, brasileiros, podemos usar outra frase, a do personagem Chicó da obra "Auto da Compadecida", do escritor Ariano Suassuna: "Sei não... só sei que foi assim...". Para sepultar de vez a discussão entre a física clássica e a mecânica quântica, em 2015, na Universidade de Delft, na Holanda, foi feita a demonstração, considerada sem brechas, ou furos, e assim, definitiva, do experimento proposto em 1964 pelo físico irlandês John Stewart Bell, conhecido como "Desigualdade de Bell". O experimento realizado na Holanda confirmou que a natureza é randômica como quer a mecânica quântica e não determinística como dizia a física clássica.

Atribui-se a criação do conceito de computação quântica ao físico e professor Richard Feynman, do Instituto de Tecnologia da Califórnia (Caltech), que afirmou, em 1985, que calcular a evolução de um sistema quântico usando computação clássica é ineficiente e demanda um computador de mesma natureza do problema, ou seja, um computador quântico. A computação quântica não é só uma computação mais rápida ou eficiente, ela é uma nova maneira de fazer computação que requer um modelo diferente para representar os problemas e solucioná-los usando fenômenos da mecânica quântica.

E que fenômenos são esses? Basicamente três: a superposição, a interferência da medição e o entrelaçamento.

O primeiro fenômeno, a superposição, estabelece que uma partícula pode – ou tem probabilidade de – estar em vários estados ao mesmo tempo. É como se disséssemos que uma maçã é verde e vermelha ao mesmo tempo. Só vamos saber se ela é vermelha ou verde quando a medirmos ou a observarmos. A maçã não é vermelha ou verde até que a observemos e descubramos sua cor. Ela é, ao mesmo tempo, verde e vermelha, com probabilidades diferentes de ser cada uma dessas cores. Esse é um conceito não intuitivo, curioso e estranho, com o qual não estamos acostumados no mundo ao nosso redor, mas que acontece com as partículas atômicas. A superposição confere à computação quântica o chamado paralelismo quântico que, por sua vez, permite o chamado "*super-dense coding*". Uma boa analogia, sempre usada para ilustrar o paralelismo quântico, é a solução de um labirinto. Em vez de se testar cada um dos possíveis caminhos para descobrir qual é o correto, na computação quântica, testamos todos os caminhos ao mesmo tempo usando a superposição.

O segundo fenômeno, a medição do estado quântico, destrói a superposição, fazendo com que a partícula assuma um estado definido. A medição tem um papel importante na mecânica quântica, diferentemente da física clássica, onde as propriedades de um objeto independem da sua observação. A unidade de processamento na computação quântica é o chamado *bit* quântico, ou QUBIT. Diferentemente do *bit* clássico, que pode assumir os valores 0 ou 1, o QUBIT pode assumir uma infinidade de valores, ou probabilidades de ser 0 ou 1, até que seja medido. Quando medido, o QUBIT será 0 ou 1. Nesse ponto, você pode estar se perguntando:

se o resultado da leitura do QUBIT é 0 ou 1, por que não usar o *bit* clássico que conhecemos, evitando um modelo de computação tão complexo? Na computação clássica, durante o processamento, são efetuadas somente operações sobre os valores 0 e 1. Com os QUBITs, operamos com valores em múltiplos estados, ou probabilidades, ou seja, a mágica acontece durante o processamento, com a chamada interferência quântica. Uma boa metáfora, usada frequentemente para explicar a interferência quântica, é quando jogamos pedras num lago. Cada pedra forma ondas concêntricas. Essas ondas interferem umas nas outras, podendo se anular ou dobrar de tamanho quando coincidem. Ao tirar uma foto do lago, é como se fizéssemos uma medição e obtivéssemos o resultado do processamento.

O último fenômeno é o entrelaçamento. Afirma-se que duas partículas estão entrelaçadas quando elas agem como se estivessem se comunicando, ou como se fossem irmãs gêmeas. Quando medimos uma das partículas, sabemos que a outra está em estado análogo, mesmo encontrando-se afastada a grande distância. Teoricamente, cada uma poderia estar num canto do universo. As partículas entrelaçadas ocorrem espontaneamente na natureza ou podem ser forçadas a esse estado por meio de diferentes técnicas. O experimento feito pela Universidade de Delft, citado anteriormente, por exemplo, usou partículas entrelaçadas geradas por meio de aprisionamento de fótons em defeitos, chamados de buracos de nitrogênio, existentes em diamantes criados artificialmente.[1]

3 Como está sendo implementada a computação quântica na atualidade?

Várias tecnologias estão sendo estudadas e testadas para a produção dos *bits* quânticos, entre elas: o uso de elétrons, *spin* nuclear, íons aprisionados por campos eletromagnéticos, tecnologias óticas (fótons), supercondutores ou semicondutores. Esta última tecnologia encontra-se em um estágio muito desenvolvido e que nos permite a fabricação de *microchips*

1 YouTube. Disponível em: https://www.youtube.com/watch?v=AE8MaQJkRcg. Acesso em: nov. 2019.

contendo dezenas de bilhões de transistores no espaço de uma unha do dedo. Grandes empresas comerciais, como Microsoft, Google e IBM, entre outras, concorrem numa corrida desenfreada para disponibilizar comercialmente seus computadores quânticos. O grande desafio para essas implementações é manter a estabilidade dos *bits* quânticos. O ruído, que pode ser eletromagnético ou mesmo a variação de temperatura, tem forte impacto nos QUBITs. Os computadores quânticos em desenvolvimento no momento são mantidos em ambientes muito controlados, com temperaturas da ordem de milli-Kelvins, o que é aproximadamente cem vezes mais frio que o espaço sideral.

Vale aqui fazer uma ressalva sobre a diferença entre computação quântica e os computadores quânticos. Enquanto os computadores quânticos estão ainda em desenvolvimento, a computação quântica, realizada por meio de simulação em computadores clássicos, principalmente por meio da computação em nuvem, já está disponível há alguns anos. A simulação, entretanto, é limitada a poucas dezenas de QUBITs devido ao aumento exponencial de capacidade da computação quântica. Para aumentar o número de QUBITs disponíveis, temos que escalar muito a capacidade de processamento de um computador clássico. Estima-se, por exemplo, que para simular 160 QUBITs seriam necessários todos os átomos de silício do planeta.

Ferramentas de desenvolvimento para computação quântica já existem há algum tempo. O *Quantum Development Kit* da Microsoft,[2] por exemplo, está disponível desde 2017. Esse *kit* de desenvolvimento disponibiliza a linguagem Q#, que pode ser instalada na popular ferramenta aberta *Visual Studio Code*.[3] A Microsoft investe na computação quântica com uma abordagem arrojada e inovadora, que pode ser encontrada em: https://cloudblogs.microsoft.com/quantum/2018/09/25/microsoft-advances-quantum-computing-vision-and-helps-tackle-real-world-challenges/.

2 Microsoft. Disponível em: https://www.microsoft.com/en-us/quantum/development-kit. Acesso em: nov. 2019.
3 Visual Studio Code. Disponível em: https://code.visualstudio.com/. Acesso em: nov. 2019.

4 Em que ponto está o desenvolvimento da computação quântica?

Antes de apresentar o desenvolvimento da computação quântica, queria destacar uma área que utiliza tecnologia quântica e tem avançado muito: os dispositivos quânticos e, mais especificamente, os sensores. Dispositivos quânticos estão em uso desde os anos 1950. Os relógios atômicos que sincronizam nossas redes, computadores e celulares usam fenômenos quânticos para determinar o tempo com enorme precisão. Estima-se que, se um relógio atômico estivesse funcionando no *Big Bang*, há aproximadamente 13,8 bilhões de anos, ele estaria marcando o tempo hoje com uma precisão dentro de um segundo. Essa mesma precisão, ou supersensibilidade, tem sido aplicada em sensores de altitude, aceleração e vibração de grande precisão que poderão ser usados na indústria automobilística, por exemplo. Na área médica, esses sensores permitirão exames de ressonância quarenta vezes mais rápidos, menores e custando um quarto do preço dos atuais equipamentos usados para esse fim. Na área militar, o *ghost imaging*, que utiliza fótons entrelaçados e permite observar à distância o que acontece num campo de batalha, por exemplo, foi testado em 2013 com alcance de 2km.

Na computação quântica propriamente dita, a chamada computação quântica de anelamento, ou, no inglês, *annealing*, baseada no conceito de computação quântica adiabática, é a que mais avança. O anelamento tem aplicações em problemas de otimização e combinações numéricas. Um exemplo de aplicação é na área financeira, na otimização de formação de carteiras de investimento (portfólios). Fabricantes de computadores quânticos de anelamento disponibilizam máquinas com algumas dezenas de milhares de QUBITs. Alguns puristas, entretanto, não consideram o anelamento como computação quântica, e sim como uma variação da computação clássica que usa técnicas quânticas.

A discussão atual é se já atingimos ou não a chamada "supremacia quântica". Aliás, esse termo tem sido paulatinamente substituído pelo mais politicamente correto "vantagem quântica". Nesse ponto, a computação quântica é capaz de resolver um problema que seria

impraticável ou praticamente impossível de ser resolvido num computador clássico. A simples discussão sobre se já atingimos ou não a supremacia quântica perde a importância frente ao fato de já estarmos, nesse momento, discutindo esse assunto, o que demonstra o estado avançado de desenvolvimento da computação quântica.

5 Que tipos de problema a computação quântica resolve?

Em teoria, poderíamos afirmar que a computação quântica pode ser aplicada a qualquer tipo de problema, e esperamos que no futuro isso acabe acontecendo. Entretanto, devido à complexidade da modelagem matemática necessária para resolver problemas de maneira quântica, ou se beneficiar da vantagem quântica, apenas algumas classes de problema têm utilizado a computação quântica de maneira eficiente. Temos que considerar que estamos há mais de um século resolvendo nossos problemas de computação por meio de algoritmos, e uma mudança de padrão mental ainda vai levar algum tempo.

O primeiro tipo de problema, e talvez o que despertou todo interesse e preocupação para a computação quântica, foi a criptografia. A proteção da informação necessária para manter nossa privacidade e segurança é baseada em algoritmos criptográficos. Em 1994, Peter Shor, pesquisador da Bell *Laboratories* e hoje professor do MIT, demonstrou um algoritmo quântico capaz de encontrar com muita rapidez o período de uma função. Esse algoritmo cria uma solução rápida para o problema de fatoração de grandes números primos, que é a base da criptografia. O trabalho do professor Shor despertou a necessidade da criação de novos algoritmos de criptografia que seriam resistentes à computação quântica, a chamada criptografia pós-quântica.

Outra área de aplicação da computação quântica é a comunicação. Por meio de algoritmos inovadores baseados em fenômenos quânticos, foram testadas transferências financeiras na Áustria em 2004, e parte do resultado de eleições na Suíça, em 2007, foi transmitida

usando redes quânticas. No ano passado, foi quebrado o recorde de distância na transmissão quântica que ocorreu via satélite entre a Áustria e a China, na distância de 7.600km.[4] Devido à destruição do estado quântico que ocorre pela medição, não se pode clonar um *bit* quântico, o chamado "*No cloning theorem*". Sendo assim, a comunicação quântica não pode ser interceptada ou copiada, pois destruiria a mensagem originalmente enviada. Em teoria, as comunicações quânticas são 100% seguras, exceto por ataque aos equipamentos de transmissão que já foram demonstrados. Avalia-se que, no futuro, parte da internet será quântica, formando uma rede para aplicações especiais que necessitam de segurança forte.

Hoje se usa a computação quântica para simular moléculas, no momento com poucos átomos apenas, modelando de forma perfeita como a natureza funciona, dispensando modelos complexos de aproximação que usamos na computação clássica. Espera-se que, no futuro, possamos compreender integralmente processos como a fotossíntese, para aperfeiçoar as baterias, ou a fixação do nitrogênio que é feita por bactérias em condições normais de temperatura e pressão na natureza e que consome aproximadamente 2% da energia global para a fabricação de amônia, usada em fertilizantes para esse fim.

Finalmente a área de inteligência artificial, principalmente o aprendizado de máquina, *machine learning* e *deep learning* são outras áreas de foco da computação quântica.

6 Como se preparar para essa nova realidade?

Dadas as mudanças que a computação quântica trará, fica clara a pressão, pelo menos no profissional de computação, para se adequar à nova tecnologia. Os algoritmos e linguagens que hoje utilizamos serão substituídos por uma nova abordagem, baseada em álgebra linear e linguagens quânticas. Em suma, o profissional de Tecnologia da Informação (TI) terá que reaprender a computação. Para isso, dezenas de cursos já estão disponíveis na internet. Artigos e livros também são uma boa fonte de aprendizagem. A Microsoft mantém uma vibrante comunidade no GitHub chamada "Quantum Katas".[5] Interessados no tema da computação quântica encontrarão inúmeras referências para estudo nessa comunidade. Algumas empresas de tecnologia disponibilizam também acesso *on-line* a computadores quânticos, reais ou simuladores, para aprendizado da computação quântica. Uma boa dica sobre o estudo da computação quântica é evitar aprofundar-se em mecânica quântica ou álgebra linear, o que pode tornar o estudo complexo e árido. Costumo fazer uma comparação com a computação clássica: a quase totalidade dos analistas e programadores não tem conhecimento sobre microeletrônica e dos princípios de construção dos *chips* dos computadores, e alguns tampouco conhecem a arquitetura dos computadores a fundo. Nem por isso são impedidos de programar eficientemente em linguagens de alto-nível e criar sistemas e soluções computacionais.

4 Science. Disponível em: https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance. Acesso em: nov. 2019.

5 GitHub. Disponível em: https://github.com/microsoft/QuantumKatas. Acesso em: nov. 2019.

7 Reflexão final

Durante a evolução da computação ao longo da história contemporânea, o modelo de computação atual, sequencial e implementado em dispositivos eletrônicos, não foi o único que utilizamos. O modelo conceitual que usamos na computação moderna evoluiu a partir de outras proposições, como a máquina proposta pelo matemático Turing, que usava conceitos bem diferentes da computação atual. A base matemática da nossa computação de hoje, a álgebra Booleana, é bem antiga, data de 1847. Além disso, tivemos máquinas mecânicas muito antes dos computadores eletrônicos, cuja primeira implementação utilizava válvula e depois transistores. Cada salto tecnológico levou, aproximadamente, 50 anos. Foi uma longa caminhada até chegarmos aos dispositivos móveis avançados que temos hoje. Pensar na complexidade da computação quântica e no tamanho e dificuldade para manter um computador quântico atual me faz lembrar que o Eniac, primeiro computador eletrônico, ocupava um espaço de 140 metros quadrados, com 40 gabinetes de quase 3 metros de altura que pesavam 30 toneladas. Imagino que ele era capaz de fazer operações matemáticas tão simples que se acanharia diante de uma calculadora de bolso comum. Usando nossa experiência passada, e com a aceleração exponencial da tecnologia que vivenciamos nos últimos anos, podemos ser surpreendidos com a computação quântica tornando-se realidade muito antes do que imaginamos. Vamos viver tempos realmente interessantes!