

Expectativa e Realidade da Computação Quântica

Alexandre Alves Coelho¹, Bruno Vieira¹, Juliana Lara Lavorenti¹, Vinicius Ceron¹.

¹Estudantes do curso de Análise e Desenvolvimento de Sistemas da IFSP Piracicaba.

Resumo: Desde que foi criada, a área da computação foi uma das que mais evoluíram em tecnologia. Diversas áreas da ciência já contribuíram com inovações, porém nenhuma dessas áreas despertem mais expectativas no imaginário coletivo como a física quântica. E faz sentido quando se lida com uma das vertentes mais exóticas da própria física. Por isso, diversos mitos foram criados a partir da ideia dos “computadores quânticos” e o que eles podem fazer. Este artigo mostrará a real aplicação desses conceitos e o porquê, realmente, a computação quântica será uma das maiores inovações tecnológicas da computação.

Palavras chaves: Computação Quântica; Processadores; Superposição; Mitos.

1. Introdução

O computador como é popularmente conhecido é recente se comparar quando o conceito de “computador” foi criado. Se tornaram menores, mais rápidos e mais eficientes. Mas se algo se manteve, foi o seu principal propósito: executar cálculos. Até pode parecer algo simples, mas as aplicações dessa diretriz são vastas, sendo aplicadas em diversos campos, seja do usuário comum ou da ciência.

Hoje em dia é impossível imaginar a vida humana e suas relações sem os computadores, sejam eles em suas diversas formas (CPU's, notebooks, smartphones, entre outros). As ferramentas que eles contêm são usadas de incontáveis maneiras. No trabalho, principalmente administrativo, tornam a vida mais fácil e ágil. São eles que analisam o faturamento de uma empresa, a validade de produtos em estoque, saldo de uma conta ou até mesmo sua compatibilidade em um relacionamento com alguém de um signo ascendente. Tudo isso, desde que seja fornecido os dados, terá o resultado.

Simular experiências e padrões se tornou algo habitual do cotidiano de pesquisadores. Porém, mesmo com supercomputadores, muitas vezes o processamento dos dados se torna demorado, e isso por conta da limitação dos equipamentos. Quanto mais os computadores evoluem, mais complexas as pesquisas se tornam.

Ou seja, o computador é importante para o ser humano, desde tarefas simples do cotidiano, até simulações complexas da ciência. E é importante distinguir a exigência de cada situação quanto ao poder computacional disponível nos dias atuais, pois é essa questão que surge quando colocamos computadores quânticos nas aplicações do dia a dia: o computador quântico mudará a vida das pessoas?

2. Processadores convencionais

Antes de entender sobre computadores quânticos e superposição, deve-se entender como funciona os processadores atuais. Munidos de transistores, que atua como portas lógicas, a linguagem utilizada dentro do computador é o sistema binário. Logo, em um computador os dados são representados por 0 e 1. Essa representação dada pelos dígitos 0 e 1 é chamada de sistema binário, que é a base do sistema digital do mundo da informática. (CUNHA, 2017).

Nesse sistema binário com 0 e 1, ou “falso” e “verdadeiro”, se obtém o bit. O bit é a menor unidade da memória. São com os bits que se estrutura informações mais complexas como o byte (conjunto de 8 bits), até kilobytes, megabytes, gigabytes, terabytes e assim por diante, todos multiplicando seu antecessor por mil.

Os processadores são compostos de transistores, componentes eletrônicos responsáveis por determinar qual o valor do bit. Para distingui-los, o transistor pode escolher barrar a corrente elétrica ou deixar passar. Assim, quando não há eletricidade na passagem, é 0 (falso), e quando há alimentação, se torna 1 (verdadeiro).

Essa dualidade básica até os dias atuais tem sido o suficiente para inúmeras tarefas com maior agilidade graças a computadores e smartphones. No entanto, existem alguns desafios que a computação normal jamais será capaz de resolver, simplesmente por não haver poder suficiente para resolvê-los. Para isso, a ciência trabalha na evolução do computador quântico. (SANTINO, 2019).

3. Processadores quânticos e a Superposição

Se foi alcançado o poder de processamento máximo dos processadores atuais, como aumentar? A resposta é simples de se anunciar, mas complexa para se executar: adicionando uma nova posição. Mas não uma posição de valor diferente, pois no sistema binário, apenas 0 ou 1 são aceitos. Logo, a nova posição teria que ser 1 ou 0 sem ser um dos dois. Isso é possível com a superposição.

A superposição é um conceito da mecânica quântica, onde uma informação pode assumir dois valores ao mesmo tempo. Ou seja, em um sistema binário, essa nova posição seria 0 e 1, ao mesmo tempo. Um bom exemplo é o fóton, as partículas da luz. Em experimentos, o fóton pode assumir dois estados: o de onda ou o de partícula. Os dois estados coexistem, porém, ao se medir (ou observar, termo científico), o fóton vai assumir um dos estados.

Nesse caso, ao invés de 0 ou 1, teremos ambos ao mesmo tempo. Isso é, em uma cadeia de qubit (termo para o bit quântico). Seguindo essa lógica, se há dois bits existindo ao mesmo tempo em um qubit, possuindo uma cadeia de qubit, é possível obter, exponencialmente, muito mais resultados.

Porém, lembrando o comportamento do fóton, quando medido o resultado de um qubit, o mesmo se colapsa em apenas um dos resultados. Ou seja, em uma cadeia de qubits, com N resultados, ao registrar quais resultados, apenas um será apresentado, perdendo todos os outros. Assim, as aplicações do processamento quântico poderiam ser inúteis já que não se pode medir seus resultados.

Se não pode medir resultados, como achar os dados esperados dentro dos N resultados sem observá-los diretamente? Para isso, é usado a Interferência de Onda. A Interferência de Ondas (consiste em aumentar ou diminuir a intensidade de uma onda sobrepostas em outra, buscando anulá-las, interferência destrutiva, ou somá-las, interferência construtiva). Assim, pelo sinal da onda que contém a mesma intensidade que esteja procurando será o resultado. É como palavras-chaves utilizadas para pesquisar trechos dentre uma gigantesca quantidade de palavras. Desde que cruze ondas que se anulem, por exemplo, só significará que ambas possuem a mesma intensidade, ou seja, dados iguais.

4. Expectativas e Realidade da Computação Quântica

Quando se fala em poder de processamento, talvez o que mais venha à tona no imaginário das pessoas é: o quão rápido será a velocidade da internet? Quais aplicações serão possíveis rodar em computadores usuais? Para muitos, quando se depara com o poder que um processador quântico tem em relação ao clássico, as expectativas são altas. Dificilmente terá alguém que nunca teve dificuldade em usar alguma ferramenta do computador, ou várias de uma vez, por causa de lentidão e travamentos oriundos da limitação de processamento da mesma.

Sempre que há inovações tecnológicas, muitos desses avanços acabam refletindo no nosso dia a dia. Até mesmo desenvolvimento de materiais e equipamentos para astronautas acabam tendo implicações no cotidiano, como comida de bebês e os famosos “travesseiros para astronautas”. Porém, mesmo uma tecnologia direcionada a algo ligado a ferramentas casuais, dificilmente terá aplicações para estas. E os motivos são: inviabilidade e inutilidade.

Como mencionado nos capítulos 2 e 3, uma das principais características do qubit é quando medido, entra em colapso e perde um dos resultados sobrepostos. Com isso, para atividades corriqueiras dos usuários comuns, inviabiliza um comportamento tão abstrato. Se pensar nos usos dos computadores e smartphones, nota-se que são limitados a: pesquisas de resultados, cálculos exatos, download de arquivos específicos, visualização de vídeos e imagens previamente pesquisadas e assim por diante. Tudo isso exige exatidão de resultados e, mais importante, não exige mais do que a tecnologia atual permite.

As capacidades atuais dos processadores convencionais são mais que necessários para as tarefas da maioria da população conectada. Por mais que a demanda por mais processamento aumente, os centros de pesquisas já usam equipamentos, sem ser quântico, muito mais poderosos do que os usados nas casas e centros comerciais. Seria trivial pensar nas aplicações de algo tão exclusivo para ações genéricas.

Pela Lei de Moore, onde Gordon E. Moore projetou que a cada dois anos, a quantidade de transistores dobraria mantendo o mesmo custo. Essa lei vem se mantendo desde 1975 e, segundo as projeções do próprio Moore, o limite tecnológico dos computadores clássicos deverá ser atingido em 2025. Mesmo que esse limite esteja próximo, as limitações diretas da falta de processamento demorarão ainda muito mais para que seja sentida.

De qualquer forma, não é completamente restrita, no futuro, que os computadores quânticos adentrem em escritórios e lares comuns. Porém, hoje, não há real necessidade de usá-los nas atividades virtuais que são utilizadas diariamente.

5. O Poder e Aplicações dos Computadores Quânticos

Um dos maiores desafios das pesquisas científicas hoje é a simulação. Simular variáveis e situações em busca de resultados refletem grande parte do uso de supercomputadores por parte dos pesquisadores e cientistas. Se o qubit se mostra inútil quanto a resultados exaltados, tudo muda no campo da probabilidade.

Em dezembro de 2001, o algoritmo de Shor, desenvolvido por Peter Shor em 1994, foi implementado em um computador quântico de sete qubits. Este computador foi criado por cientistas do Centro de Pesquisas da IBM. O computador foi utilizado para fatoração do número 15 e, como esperado, o resultado foi $15 = 3 \times 5$, por mais simples que seja, mostrou que computadores quânticos podem existir realmente. E operações que levariam bilhões de anos para serem resolvidas por um computador clássico poderão ser resolvidas rapidamente pelos computadores quânticos (figura 1). A tabela a seguir mostra estimativas de tempo de fatoração em algoritmos quânticos e comuns (OLIVEIRA, 2003).

COMPRIMENTO DO NÚMERO A SER FATORADO (EM BITS)	TEMPO DE FATORAÇÃO POR ALGORITMO CLÁSSICO	TEMPO DE FATORAÇÃO COM O ALGORITMO DE SHOR
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quadrilhões de anos	4,8 horas

Figura 2 - Comparação do tempo de fatoração de números inteiros (OLIVEIRA, 2003).

São estudados também as aplicações no ramo da segurança, onde cada vez mais é necessário novos meios seguros de realizar transações, movimentações monetárias, conversas em redes sociais e assim por diante. Nesse caso, não é problema o resultado da superposição se perder na observação, já que nesse caso, o mais importante a preservar é o caminho percorrido pela informação.

Em 2019, a IBM lançou seu primeiro computador quântico comercial e trouxe atualizações sobre novas conquistas relacionadas a computação quântica em janeiro desse ano,, segundo a revista CIO, A IBM Q NETWORK (Rede criada para avanços na computação quântica) recebeu 4 aliados fortes na trilha do caminho para um futuro possível nesse meio, a Delta Air Lines, Anthem, Goldman Sachs e Wells Fargo. De acordo com Rahul Samant, CIO da Delta, a companhia planeja explorar como a computação quântica pode ajudar na superação de desafios durante as viagens aéreas. Já a Anthem procurará formas de otimizar o uso do seu armazenamento de dados de saúde, desenvolvendo opções de tratamento personalizadas e melhorando a previsão das condições de saúde dos seus segurados.

5.1. Casos ativos de computação quântica

Algumas empresas já estão utilizando equipamentos de computação quântica da IBM para resolver problemas reais, incluindo a montadora Daimler, que implementou a solução para modelar o comportamento de moléculas que contêm lítio. Seu objetivo é desenvolver baterias com melhor desempenho para veículos elétricos.

Embora ainda seja mais rápido executar esse tipo de cálculo em computadores convencionais, a Daimler e a IBM estão se preparando para o dia em que a computação quântica terá vantagem. Embora os computadores quânticos práticos permaneçam distantes da realidade, a potencial capacidade dessas máquinas já devem ser levadas em consideração por parte dos CIOs.

A programação no mundo quântico será fundamentalmente diferente da codificação para máquinas convencionais, envolvendo novos ambientes de desenvolvimento, novas linguagens e algoritmos inteiramente novos. Esses algoritmos quânticos não resolverão todos os problemas de computação atuais, mas a previsão é de que tenham uma vantagem significativa em relação às máquinas convencionais.

Pensando nisso, os CIOs já podem começar a trabalhar com equipes de P&D e engenharia para identificar se alguma das cargas de trabalho das suas organização pode ser adequada a uma abordagem quântica. O IBM Q Network oferece às empresas um ambiente de proteção para a execução dos experimentos, mas existe também a nuvem: a AWS possui o Amazon Braket e a Microsoft o Azure Quantum. O Google também está realizando pesquisas sobre computação quântica, mas, apesar de alguns avanços, ainda não oferece serviços hospedados na sua plataforma de nuvem.

6. Conclusão

Embora se crie muitas expectativas em torno na computação quântica, não significam que são altas demais para essa tecnologia que realmente é muito inovadora. Apenas são expectativas criadas em usos errados.

Avanços desse tipo nem sempre retornam em inovações diretas no cotidiano, mas sempre traz consequências ao redor e melhoram a qualidade de vida. Os efeitos dessa tecnologia trarão grandes avanços em diversas áreas, desde a física, farmacêutica, agrônômica e até financeira.

Ainda há muitos estudos a serem feitos para entender até onde pode se estender essas aplicações. E mesmo em cinco anos, quando se chegará ao limite dos computadores clássicos, o quão avançado não estará os computadores quânticos e suas prestações a tecnologia?

7. Referências

- CRISTO, F.; PREUSS, E.; FRANCISCATTO, R. Arquitetura de Computadores. Universidade Federal de Santa Maria, 2013.
- CUNHA, G.; MACEDO, R.; SILVEIRA, S. Informática Básica. Universidade Federal de Santa Maria, 2017.
- SANTINO, R. 2019. Entenda o que são computadores quânticos e como eles funcionam. Olhar Digital. São Paulo, SP, 2019. Disponível em: <<https://olhardigital.com.br/noticia/entenda-o-que-sao-computadores-quanticos-e-como-eles-funcionam/90692>>. Acesso em: 02 de setembro de 2020.

Computadores Quânticos Explicada. Canal Ciência Todo Dia, Youtube, 2020. Disponível em: <https://www.youtube.com/watch?v=92eSz2X0AIU&ab_channel=Ci%C3%AAnciaTodoDia>

MATTIELO, Felipe; SILVA, Gesiel Gomes; AMORIM, Ronni G. G.; SILVA, Washington Barbosa. Decifrando a Computação Quântica. UEFS, 2012.

<http://dfisweb.uefs.br/caderno/vol10n12/a4MattielCQuantica.pdf>

<https://exame.com/tecnologia/ibm-alcanca-novo-patamar-na-computacao-quantica-e-quer-dobrar-capacidade/>

<https://www.ibm.com/blogs/ibm-comunica/ibm-anuncia-primeiro-sistema-de-computacao-quantica-integrado-para-uso-comercial-no-mundo-o-ibm-q-system-one/>

<https://cio.com.br/rede-de-computacao-quantica-da-ibm-conquista-novos-usuarios-da-fortune-100/>

https://www.scielo.br/scielo.php?pid=S1806-11172017000100401&script=sci_arttext&lng=pt