

AS CONQUISTAS DA FÍSICA E O DESAFIO E AS POSSIBILIDADES DO COMPUTADOR QUÂNTICO

Entrevista com Fernando Brandão¹

A entrevista foi concedida à Profa. Maria Esperança de Paula²

SCI|AS – Fernando Brandão é professor catedrático do Instituto de Tecnologia da Califórnia, localizado em Pasadena, nos Estados Unidos da América, e Diretor de Ciência Aplicada na Amazon. Especialista em Física Quântica, atualmente é um dos líderes, naquela instituição, do projeto que visa à construção de computador quântico, de que os primeiros resultados já foram informados tanto em revistas especializadas quanto noticiados pela grande imprensa. O professor concedeu esta entrevista para SCI|AS. Educação. Comunicação e Tecnologia, abordando os aspectos principais da área em que atua, considerando a necessidade de que os professores de Física e de Ciências em geral possam transmitir aos estudantes – e não só no nível superior – informações seguras e atualizadas sobre o assunto de sua especialização em tecnologia quântica.

SCI|AS – Bom dia professor Fernando.

FB – Bom dia. É uma satisfação conversar com vocês da revista **SCI|AS. Educação. Comunicação e Tecnologia** da Faculdade de Educação da Universidade do Estado de Minas Gerais.

¹ Fernando Brandão. Doutor em Física pela Imperial College (Reino Unido). Professor de Física na Caltech Pasadena EUA. Diretor de Ciência Aplicada no Centro para Computação Quântica da Amazon Web Services. E-mail: fbrandao@caltech.edu

² Maria Esperança de Paula. Editora-Chefe da Revista SCI|AS – Educação, Comunicação e Tecnologia. Professora de Tecnologia Educacional na Faculdade de Educação da Universidade do Estado de Minas Gerais. FaE. UEMG. Mestrado em Educação pela Universidade do Estado do Rio de Janeiro (UERJ). E-mail: maria.esperanca@uemg.br

SCIAS – Professor, dando início a nossa conversa, o senhor poderia explicar o que é a física quântica?

FB - A física quântica, também chamada de mecânica quântica, é, na verdade, a teoria fundamental da natureza. Ela explica o mundo dos átomos, moléculas, fótons e tudo mais que é realmente muito pequeno. Objetos microscópicos se comportam de maneira diferente do que observamos em nossa experiência cotidiana, que é descrita pelo que chamamos de física clássica. A física clássica é a que aprendemos na escola, como as leis de Newton.

Você talvez já tenha ouvido que partículas quânticas podem estar em superposição em dois locais diferentes. Por exemplo, pense em um elétron orbitando o núcleo de um átomo. O elétron pode estar em uma superposição de diferentes locais — aqui e ali ao mesmo tempo. Você também pode ter ouvido que duas partículas quânticas, como dois elétrons em um átomo, podem estar emaranhadas, significando que suas propriedades estão correlacionadas tão fortemente que não existe paralelo na física clássica.

Eu sei que isso parece complicado. Pode acreditar que até os físicos acham. Mas é assim que a Natureza escolheu se comportar. Felizmente, você não precisa entender física quântica para saber como um computador quântico funciona em alto nível. Mas a lição aqui é que, como o mundo microscópico se comporta de forma bastante diferente, talvez devêssemos usá-lo para construir tecnologia.

SCIAS - A física quântica já foi usada em tecnologia antes?

FB - Sim. A física quântica já teve um grande impacto na tecnologia e em nossas vidas:

Para desenvolver lasers, precisamos da teoria quântica da luz. Para construir máquinas de ressonância magnética (MRI), precisamos da teoria quântica das moléculas. Para desenvolver o transistor – o elemento fundamental de todos os sistemas computacionais modernos – precisamos da teoria quântica do estado sólido. Podemos nos perguntar se a mecânica quântica terá um impacto ainda maior na tecnologia do século XXI. Eu acredito que sim, oferecendo uma forma radicalmente nova de computação

SCIAS - Como ela pode permitir esse novo tipo de computação?

FB - Antes de explicar exatamente como, vamos dar um passo atrás e olhar a história do que chamamos de computação clássica, ou seja, de todos os sistemas computacionais modernos que temos hoje. Conforme a Lei de Moore, o poder computacional em um chip dobra a cada dois anos. Essa lei se manteve assim por mais de 70 anos. Hoje podemos ter centenas de bilhões de transistores em um chip – uma quantidade incrível de capacidade computacional. Mas, apesar desse sucesso extraordinário da computação clássica, alguns problemas importantes continuam fora de alcance.

Uma classe desses problemas é a simulação de sistemas quânticos. Se você olhar para o uso do maior supercomputador do mundo, verá que 5 das 6 principais áreas dizem respeito a simular sistemas quânticos complexos: química, ciência dos materiais, energia de fusão, física nuclear e física de altas energias.

SCIAS - Por que simular sistemas quânticos é difícil para computadores?

FB - Sem entrar em muitos detalhes, isso se faz em vista do emaranhamento quântico, uma das características da mecânica quântica que mencionei antes. O emaranhamento implica que o custo computacional de simular um sistema quântico cresce exponencialmente com o número de partículas. Precisamos de um supercomputador para modelar apenas 50 partículas quânticas. E já está completamente fora do alcance dos computadores clássicos modelar algo como 100 partículas.

Isso é decepcionante para a física computacional. Mas podemos observar esse fato de um ponto de vista mais otimista. O primeiro a pensar nessa possibilidade foi o físico vencedor do Nobel e professor do Caltech, Richard Feynman. Em 1981, Feynman afirmou, de um modo bem humorado [FEYNMAN18]:

“A Natureza não é clássica, puxa, e se você quer simular a Natureza é melhor fazê-lo nos padrões da mecânica quântica — e, caramba, esse é um problema maravilhoso, porque não parece nada fácil.”

Essa é a ideia original de um computador quântico.

SCIAS - E o que é um computador quântico?

FB - Se pudermos engenhar sistemas quânticos com muitas partículas e um alto nível de controle, poderemos criar um novo tipo de computador, que deve superar os computadores clássicos pelo menos na tarefa de simular a própria Natureza. Vamos destrinchar isso com calma.

Primeiro, voltando à computação clássica: nossos computadores armazenam dados em bits, que podem ser 0 ou 1. Fisicamente, usamos carga elétrica em transistores para armazenar bits. Bits são processados por portas lógicas, que agem em um ou dois bits por vez. Há apenas algumas portas desse tipo, que são blocos fundamentais de circuitos digitais.

Você pode pensar em qualquer computação como um jogo de Lego, em que as portas são as peças. No jogo, você recebe uma tarefa e seu objetivo é conectar as portas em um circuito que resolva essa tarefa. Quanto menor o circuito, melhor. Você irá precisar de menos tempo para resolver o problema. Essa é a essência do desenvolvimento de algoritmos.

Nossos computadores rodam, a cada segundo, circuitos com bilhões de portas. Essa enorme complexidade é o que dá poder aos sistemas computacionais modernos.

SCIAS - Como isso funciona no caso do computador quântico?

FB- Podemos pensar em um computador quântico de forma similar a essa. Em vez de bits, temos *qubits*. Qubits são construídos a partir de qualquer sistema quântico com duas configurações diferentes. Por exemplo, um qubit pode ser formado por dois níveis de energia de um elétron em um átomo.

Dizemos que o qubit está no estado 0 se estiver no nível de energia mais baixo. Até aí, igual ao bit. Mas, por causa da superposição, o elétron pode estar em uma superposição dos dois níveis de energia.

Dizemos que o estado do qubit é uma superposição de 0 e 1. Quando medimos a energia do elétron, só obtemos um dos dois valores: 0 ou 1. Nunca observamos a superposição diretamente, Mas podemos observá-la indiretamente.

Em um computador quântico também aplicamos portas lógicas aos qubits. Mas agora essas portas são quânticas e temos uma classe mais rica de escolhas. Podemos implementá-las enviando sinais aos qubits, como lasers ou voltagens.

Por exemplo, ao iluminar um átomo com um laser na frequência certa, podemos mover o qubit de 0 para 1, ou o contrário. Mas, mudando o pulso do laser, também podemos levá-lo para uma superposição de 0 e 1. Essa porta quântica não existe na computação clássica.

Chamamos essa porta de porta H (ou *Hadamard*). Ela mapeia 0 para a superposição $0+1$ e 1 para a superposição $0-1$. Ainda não expliquei o sinal de menos, mas chegarei lá. Acontece que adicionar a porta H às portas clássicas é tudo que precisamos para obter todo o poder da computação quântica.

SCIAS – E como funcionam os circuitos com essa nova porta quântica?

FB - Assim como no caso clássico, você pode pensar na computação quântica como um jogo de Lego, mas agora com uma peça extra: a porta H .

Dado um problema, o objetivo é encontrar um circuito quântico que o resolva. Quanto menor o número de portas quânticas, melhor, pois você obtém o resultado mais rápido. Como temos mais tipos de portas, às vezes precisamos de menos portas quânticas do que de portas clássicas.

Note que não é que computadores quânticos rodem os mesmos algoritmos clássicos mais rápido. Na verdade, todas as implementações conhecidas de portas quânticas são mais lentas que portas clássicas. A vantagem vem do fato de que podemos escrever novos algoritmos, que usam fenômenos quânticos e não existem na computação clássica.

SCIAS - Como podemos usar essa classe mais rica de algoritmos?

FB - A afirmação principal da computação quântica é: *Computadores quânticos podem resolver alguns problemas com exponencialmente menos portas do que computadores clássicos.*

Então, não é que os computadores quânticos sejam duas vezes mais rápidos, ou 10 vezes mais rápidos do que os clássicos. Mas sim que eles conseguem resolver problemas que *para sempre* permaneceriam fora do alcance da computação clássica.

SCIAS – Que problemas seriam esses?

FB - Você está perguntando por que realmente queremos construir computadores quânticos. É uma boa pergunta. Uma grande área de aplicação dos computadores quânticos é o que chamamos de “simulações quânticas”. Essa é a ideia original de Feynman de usar computadores quânticos para simular a natureza. Diferentemente dos computadores clássicos, computadores quânticos podem simular de forma fiel sistemas quânticos complexos. Isso é crucial, porque permitiria inovações em muitas indústrias.

Um exemplo interessante é a produção de fertilizantes mais eficientes. Amônia é um ingrediente-chave dos fertilizantes. A produção de amônia industrial consome muita energia e emite muito carbono, cerca de 1,8% das emissões globais de CO₂. Mas algumas bactérias produzem amônia de forma muito mais eficiente. O processo central envolve uma molécula enorme chamada FeMoCo, com 120 elétrons ativos. Computadores clássicos *não conseguem* simular FeMoCo bem. Mas um computador quântico conseguiria, abrindo caminho para fertilizantes mais limpos e eficientes.

De forma mais geral, computadores quânticos desbloqueariam uma abordagem *ab initio* – isto é, do início – para o design molecular, nuclear e de materiais, evitando a necessidade de experimentos empíricos caros e demorados, ou de depender de aproximações fracas, que conseguimos em computadores clássicos. Eu acredito que o impacto para novas tecnologias poderia ser imenso. Pense no valor para a sociedade da invenção da máquina de MRI, do laser e do transistor. Tudo isso exigiu que a sociedade desenvolvesse a física quântica. Mas a física quântica usada nesses casos é fácil de modelar, porque tais sistemas têm baixo nível de emaranhamento e complexidade.

Os três exemplos de que falei antes são sistemas quânticos de alta complexidade/emaranhamento, além do limite do que nossos computadores clássicos conseguem fazer. Não sabemos ao certo, mas temos razões para acreditar que ser possível simulá-los em computadores quânticos poderia desbloquear tecnologias tão transformadoras quanto as máquinas de MRI, lasers e transistores. Há ainda mais exemplos, que vão de explorar reatores de fusão mais eficientes até algumas abordagens em design de fármacos.

Mas por que parar apenas nos casos que conhecemos hoje? Há uma nova fronteira da natureza que poderíamos explorar sistematicamente com computadores quânticos: a dos sistemas quânticos complexos. Provavelmente há muitas ideias transformadoras que hoje nem conseguimos imaginar!

SCIAS - Existem aplicações do computador quântico fora da física quântica?

FB - Pouco mais de uma década após a primeira ideia de Feynman sobre o computador quântico, Peter Shor, que era pesquisador na AT&T naquela época, revolucionou a computação quântica [SHOR94]. Ele inventou um algoritmo quântico eficiente para quebrar a criptografia RSA. Enquanto quebrar uma chave RSA de 2048 bits levaria 1 bilhão de anos com um computador clássico, um computador quântico com 6000 qubits poderia fazer isso em 100 segundos.

SCIAS - Mas o que é a criptografia RSA?

FB - É o sistema de criptografia de chave pública mais usado hoje. Sempre que compramos algo online, estamos usando RSA. O algoritmo de Peter Shor é o exemplo mais claro de como o computador quântico pode superar massivamente o computador clássico em problemas de grande interesse para a sociedade.

Por causa desse risco severo para a segurança global, muitas pessoas estão trabalhando para substituir RSA por um esquema que seria seguro mesmo contra computadores quânticos. Isso se chama *criptografia pós-quântica*. Há alguns esquemas promissores e o NIST, no mês passado, selecionou alguns dos principais para padronização. Mas pesquisadores quânticos, incluindo Peter Shor, continuam tentando quebrar os novos esquemas, às vezes chegando perto. Então o resultado ainda é incerto.

SCIAS - Você falou de aplicações em simulações físicas e criptografia. Existem mais?

FB - O que sabemos aqui é mais especulativo, mas há razões para sermos otimistas.

Um problema que muitas empresas precisam resolver todos os dias é o *problema de roteamento de veículos*, no qual você tenta encontrar o conjunto ideal de rotas para uma frota de veículos entregar encomendas a um determinado conjunto de clientes. Como há muitos endereços e muitos veículos, esse é um problema de otimização bem difícil. Tentamos construir algoritmos para encontrar a melhor rota possível, dadas as restrições, como tempo e número de

unidades de computação disponíveis para o algoritmo. Se de alguma forma conseguirem um algoritmo que dê uma solução até mesmo 10% melhor que o estado da arte atual, isso será um grande avanço!

Problemas similares de otimização relacionados a logística, pesquisa operacional e alocação de recursos aparecem em todas as indústrias. O computador quântico pode ajudar a acelerar a busca por boas soluções de otimização [BRANDAO17]. Então, otimização pode potencialmente constituir uma aplicação ampla dos computadores quânticos para a indústria. Mas o que sabemos é mais especulativo, porque não temos certeza de quão grande pode ser na prática o ganho dos recursos quânticos para otimização.

Otimização também é fundamental para inteligência artificial. Então, computadores quânticos também podem potencialmente ajudar nessa área. Ainda mais, para certos conjuntos de dados, computadores quânticos podem aprender melhor, significando que modelos quânticos podem ser exponencialmente melhores que modelos clássicos. A ressalva é que não sabemos para quais conjuntos de dados os modelos quânticos podem ajudar. E, por causa do tamanho massivo dos dados na inteligência artificial, precisaríamos de computadores quânticos com bilhões de qubits ou mais.

SCIAS - Você mencionou aplicações de mecânica quântica em física, química e ciência dos materiais. E também, de forma mais surpreendente, em criptografia e até otimização. Mas que tipo de computador quântico precisamos para rodar essas aplicações?

FB - Um fato interessante é que você não precisa de tantos qubits para rodar essas aplicações. Você começa a obter valor já na faixa de centenas a milhares, dependendo da aplicação. Bem, exceto no caso de ML. Você precisa de mais portas quânticas, porém, na faixa de dezenas de milhões a dezenas de bilhões. Isso faz sentido, porque você quer rodar algoritmos quânticos sofisticados que superem amplamente todos os algoritmos clássicos. E isso requer muitas portas quânticas.

Tudo isso parece muito animador para a computação quântica. Mas infelizmente, há algo mais que sinto que preciso revelar?

SCIAS - O que é?

FB - Não temos ainda um hardware quântico bom o suficiente. O hardware atual é muito ruidoso. Sistemas quânticos interagem com o ambiente e sofrem decoerência. Mas acreditamos que existe um caminho plausível para um hardware de alta performance na próxima década, e há um enorme esforço global para construir computadores quânticos tolerantes a falhas, incluindo no nosso projeto no Centro de Computação Quântica da Amazon, onde estamos desenvolvendo hardware quântico com correção de erros usando qubits gatos de Schrödinger [PUTERMAN25].

SCIAS - Como sabemos sobre essas aplicações se computadores quânticos ainda não existem?

FB - Boa pergunta. Todos os algoritmos quânticos atuais -- inclusive o de Shor para fatoração -- foram criados com papel e lápis, escrevendo equações e circuitos quânticos. Mas isso é, na verdade, uma boa notícia: sugere que exploramos apenas uma pequena parte do espaço de aplicações possíveis, e que aplicações revolucionárias ainda podem ser descobertas assim que tivermos hardware de verdade.

SCIAS – Professor, tudo isso é um mundo muito novo, mas o novo sempre começa num ponto no presente. Então, como os professores de física e de ciências podem abrir a perspectiva de seus alunos para esse mundo novo, preparando-os para o futuro, visando uma Educação com apoio tecnológico quântico?

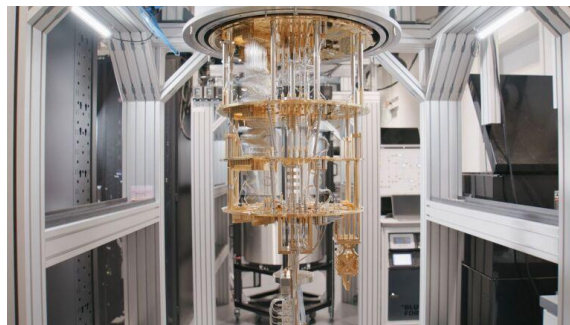
FB – Na educação, os processos como que reproduzem o desenvolvimento científico de uma área. Então, é preciso ter uma boa formação em física clássica, bem como um entendimento de como funcionam os computadores clássicos de que dispomos hoje em dia. Por outro lado, é preciso entender que o teórico e o aplicado não são esferas completamente dissociadas. Como eu disse antes, muito do que se vislumbra é desenhado com lápis e papel, pois é a partir desses exercícios de projeção daquilo que pode vir a ser que tornamos possível que de fato possam se realizar.

Muito importante em qualquer esfera do ensino é despertar a curiosidade dos alunos, de forma a interessá-los no que há de novo e gerar engajamento em

seguir por caminhos cada vez mais inovadores. E investir em inovação supõe compreender como a Natureza se apresenta e como age em diversos níveis, no da nossa experiência comum e no nível do que não se oferece a nossos olhos, mas interfere nos processos naturais e, portanto, na nossa vida.

É um grande desafio para os professores de hoje em dia. Mas não devemos esquecer duas coisas: a primeira, que os físicos que hoje trabalham na fronteira do conhecimento iniciaram seu percurso em escolas com a capacidade de produzir neles interesse e engajamento, pois se não fosse assim não se teriam tornado cientistas. A segunda coisa é que compreender como funciona a Natureza sempre foi um desafio para a humanidade e uma tarefa, sempre difícil, mas maravilhosa, com a capacidade de nos surpreender e nos abrir para a fruição do que o mundo nos oferece como maravilha. Fazer isso faz valer a pena ser professor.

SCIAS – Nossos sinceros agradecimentos, Prof. Fernando Brandão, por sua cordialidade e disponibilidade.



Computador quântico. Caltech. Pasadena, USA
(<https://www.aboutamazon.com/news/aws/quantum-computing-aws-ocelot-chip>)

Referências

[BRANDAO17] BRANDAO, Fernando G.S.L. et al. "Quantum speed-ups for solving semidefinite programs." *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2017.

[FEYNMAN18] FEYNMAN, Richard P. "Simulating physics with computers." **Feynman and computation**. cRc Press, 2018. 133-153.

[PUTERMAN25] PUTTERMAN, Harald, et al. "Hardware-efficient quantum error correction via concatenated bosonic qubits." **Nature** 638.8052 (2025): 927-934.

[SHOR94] SHOR, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." **Proceedings 35th annual symposium on foundations of computer science**. Ieee, 1994.