Informática

>> Este livro trata de um campo de vanguarda na ciência. Falamos do computador do futuro, dos reflexos que a física e a mecânica quântica projetam na filosofia, da busca da realidade e das novas tecnologias da computação e comunicações. Tratamos, ainda, do desenvolvimento do código e do algoritmo. Em circuitos, avançamos para uma escala nanométrica, indo ao mundo das moléculas, dos átomos e das partículas.

>> Escrevemos sobre implementações da computação quântica e da linguagem de programação universal com base em um conjunto de portas lógicas e demonstramos o uso dos pacotes de desenvolvimento dos principais fabricantes. Executamos os programas em modo de simulação e também passamos para o código compilado diretamente executado em processadores quânticos verdadeiros.

>> Em uma demonstração clara e simples, são descritos a montagem dos ambientes de desenvolvimento, os componentes de tecnologia padrão e código aberto e as principais interfaces da atualidade, tais como ferramentas para cálculo numérico, matrizes, visualização gráfica, aprendizado de máquina (ML), inteligência artificial (AI) e computação em nuvem (cloud).

>> Falamos da harmonia e das oportunidades que permitem um canal de contato entre a humanidade e o Universo, e, por fim, desorganizamos os fatos e levantamos algumas dúvidas.

ALTA BOOKS
EDITORA
www.altabooks.com.br
/altabooks
/altabooks

“Eu tento dar sentido ao que vejo e me pergunto sobre o que faz o Universo existir. Quando jovem, em lugares bastante montanhosos, observei o firmamento com milhares de estrelas brilhando. Recentemente eu mergulhei na teoria quântica para espiar o infinito Universo em sua menor escala. Com todas essas experiências, nunca me canso de querer saber o que há além. O que importa é que eu não desisto nessa busca.”

CLAUDE FALBRIARD

“Aquele que não parou e colaborou com o tempo verificará mais tarde que está tão adiante que jamais poderá ser alcançado, e que não tem volta! O passado não existe, uma luz o chama, o presente voa, a informação é valiosa, volumosa, veloz num tempo infinito, levando ao futuro num quantum.”

INES BROSSO

AGRADECIMENTOS

Agradecemos à Rosana Arruda pelas sugestões e horas dedicadas a este projeto, e à Editora Alta Books por acreditar neste livro.

Para nossa pesquisa, tivemos apoio e suporte de empresas como IBM, Rigetti, Intel e Thorlabs. Foi um trabalho de colaboração profissional e acadêmico para a utilização de cloud e socorro aos obstáculos encontrados nos acessos.

Também tivemos incentivo de professores, que com seus trabalhos de pesquisa na área de redes de computadores e internet sempre nos motivaram a continuar, como a professora doutora Graça Bressan e o professor doutor Wilson Vicente Ruggiero, do LARC (Laboratório de Arquitetura de Redes de Computadores) da Escola Politécnica da USP, e dos professores doutores Demi Getszcko e Daniel Gatti, da Pontifícia Universidade Católica de São Paulo, que ajudaram na criação de um laboratório de pesquisas em Segurança na Computação Quântica em 2018, na Faculdade de Ciências Exatas, que existe desde 1917 e foi berço da primeira Escola de Física do Brasil, hoje tombada como patrimônio histórico e cultural e que caminha para ser a pioneira em pesquisas em segurança em computação quântica e internet quântica.

SOBRE OS AUTORES

A professora doutora **Ines Brosso, brasileira**, tem doutorado em engenharia elétrica pela Escola Politécnica da Universidade de São Paulo, no Departamento de Engenharia da Computação e Sistemas Digitais no Laboratório de Arquitetura e Redes de Computadores (LARC). Tem bacharelado e licenciatura em matemática pela PUC/SP e faz pós-doutorado na Pontifícia Universidade Católica de São Paulo, no Programa de Pós-graduação em Tecnologias da Inteligência e Design Digital. Atuou no desenvolvimento de sistemas e projetos de segurança de TI em empresas de grande porte, como ABB, Banco BCN e Banco Bradesco S.A. por mais de 36 anos. Publicou vários artigos, livros e registros de software. Atua como consultora na área de segurança de TI. É membra consultiva do Comitê de Segurança da Informação da ABNT/SP e Desenvolvimento Seguro do Chapter da OWASP/SP. Linhas de pesquisa: segurança em tecnologia da informação; desenvolvimento seguro de aplicativos; mecanismos de autenticação contínua; sistemas biométricos; políticas de segurança adaptativas; criptografia; segurança na computação quântica.

Currículo Lattes em: http://lattes.cnpq.br/6036666021206431

Contato LinkedIn em: https://www.linkedin.com/in/ines-brosso-16331b

Claude Falbriard, suíço, é mestre com certificado profissional da OpenGroup, especialista em tecnologia da informação e telecom, com 47 anos de profissão junto a empresas multinacionais como ABB e IBM. É autor dos livros *Redes Banda Larga* e *Protocolos e Aplicações para Redes de Computadores*, pela Editora Érica. Detém diversas patentes registradas, tais como "Método e Sistema para Identificação de Materiais Recicláveis", "Dispositivo de 'Middleware' Conectável em Nuvem" e "Etiqueta Reflexiva e Sensor de Luz Polarizada para Transmitir Informações". É especializado na construção de código aberto e engenharia de sistemas IBM de grande porte e orientador das práticas e metodologias de inovação. É também estudioso em tecnologias de vanguarda (ciência de dados, blockchain e quantum).

Contato LinkedIn em: https://www.linkedin.com/in/claudefalbriard

Claude e Ines trabalharam juntos na ABB, no Brasil, de 1980 a 1990, e sempre tiveram uma afinidade muito grande em relação à pesquisa e a redes de computadores. Mesmo distantes e afastados das rotinas profissionais, nunca deixaram de manter contato e estreitar a troca de informações sobre inovações, até que surgiu, em 2018, a ideia de escrever este livro.

PREFÁCIO

Prezado leitor, vivemos um momento especial e único! O século XXI apresenta infinitas possibilidades e desafios, e novas tecnologias e abordagens devem ser utilizadas na identificação, exploração e implementação de soluções para problemas de natureza cada vez mais complexa e caótica.

Nas últimas décadas, o poder do processamento convencional dobrou a cada dois anos. A disrupção na indústria e sociedade, fomentada pelo desenvolvimento e pela aplicação da inteligência artificial, caminha a passos largos, mas no campo científico, com cenários complexos, ainda nos deparamos com a limitação do clássico modelo binário. A ciência moderna busca resolver problemas complexos de otimização matemática, modelagem molecular, descobrimento de novos medicamentos, entre outros, cuja exploração e busca por soluções são limitadas pela computação digital.

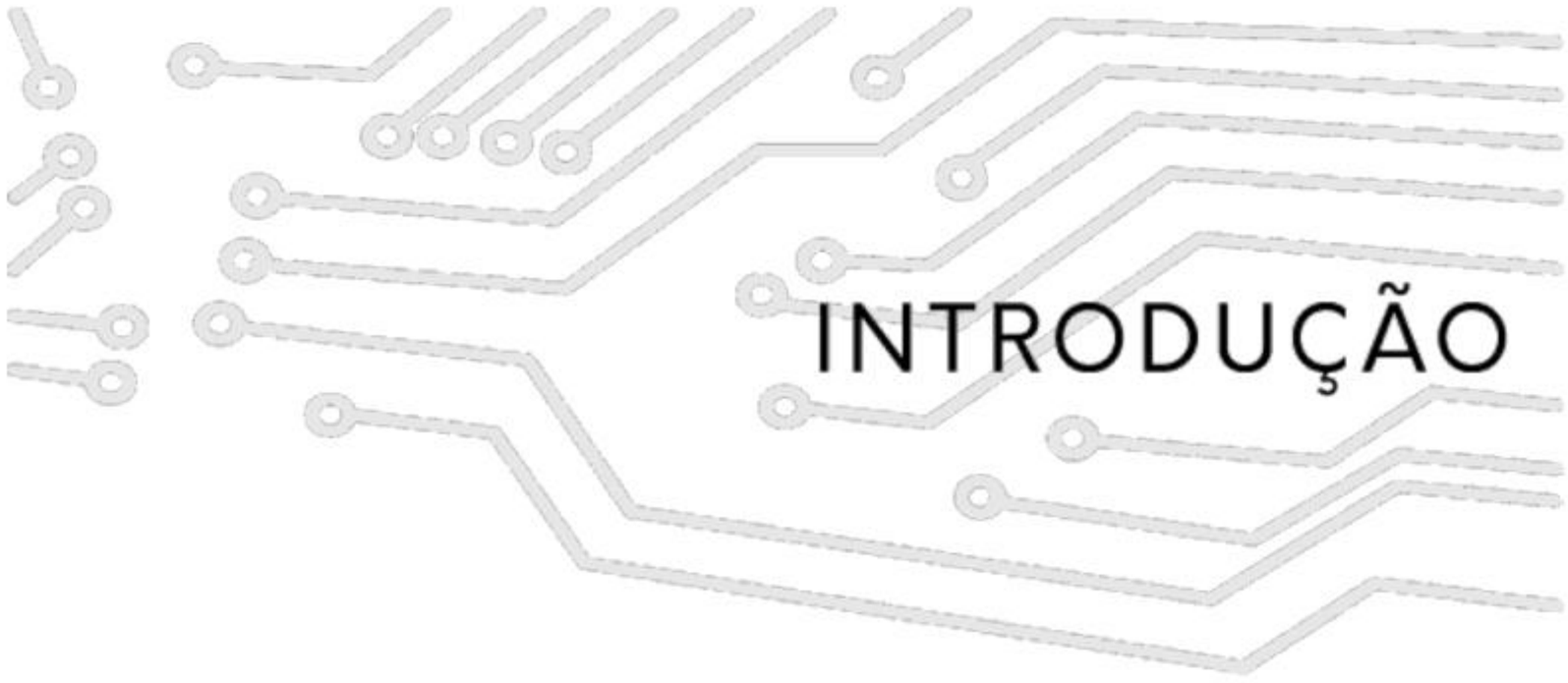
Nesse cenário, a exploração da computação quântica e sua respectiva aplicabilidade apresentam novos horizontes e abrem caminho para uma disrupção tecnológica e econômica sem precedentes. Com base nos fundamentos da física quântica, os computadores quânticos apresentam propriedades únicas (sobreposição, emaranhamento e qubit),que podem ser utilizados na resolução de problemas de natureza complexa, potencializando o poder exploratório científico e econômico.

Os autores Ines Brosso e Claude Falbriard nos brindam de forma intuitiva, didática e magistral com as possibilidades desse maravilhoso mundo da computação quântica. De questões filosóficas à sua aplicabilidade na indústria, os autores preparam o leitor por meio de conceitos fundamentais e descrevem os passos na preparação de recursos dedicados em sistemas de comunicação, segurança, tarefas de cálculos científicos e democratização do tema. Desejo a todos uma excelente leitura.

Rafael Castro de Oliveira, Estrategista de Agilidade, Inovação e Tecnologias na IBM Cingapura

LISTAS DE FIGURAS

SUMÁRIO



INTRODUÇÃO

Bem-vindo ao dinâmico mundo da computação quântica, a realidade de uma nova era, a ciência que estuda as teorias e propriedades da física quântica e da mecânica quântica aplicadas à ciência da computação, abrangendo desde o hardware do computador quântico, o metal que compõe suas baterias, o software, a segurança, até a tecnologia de comunicação de dados.

Este livro apresenta tecnologias de computação quântica de ponta para desenvolvedores, pesquisadores e profissionais que queiram se aprofundar no assunto. Cada capítulo apresenta conceitos, definições e exemplos dos assuntos tratados de forma a dar uma visão geral das tecnologias e da lógica da computação quântica — uma nova era que se inicia na tecnologia.

O objetivo deste livro é reduzir os mistérios que envolvem a computação quântica e a lógica de processamento dos computadores desta nova geração.

Hoje já existe uma competição entre grandes empresas fabricantes de computadores quânticos e suas plataformas, o que tem levado à rápida inovação e à queda nos preços. A concorrência entre os vários fabricantes impulsiona a inovação de hardwares, softwares e serviços quânticos.

Este livro não é um tutorial. Apesar de apresentar uma parte introdutória muito abrangente e explicativa, ao longo do texto e com o avanço dos capítulos ele exigirá do leitor conhecimentos e experiência em matemática, criptografia, física e linguagem de programação. Ou seja, o público-alvo deve ser técnico e especializado em computação.

As plataformas de computação quântica utilizadas foram: Alibaba CAS; D-Wave; IBM; Microsoft; Rigetti e Xanadu.

Os autores

CAPÍTULO 1
COMPUTAÇÃO QUÂNTICA, SUA HISTÓRIA E ORIGEM

INTRODUÇÃO

Na computação clássica, o computador é baseado na arquitetura de Von Neumann, com unidades de bits e bytes (0,1), ou seja, em um sistema binário, que distingue elementos de processamento e armazenamento de dados, pois tem processador e memória destacados por um barramento de comunicação, em um processamento sequencial.

Entretanto, os computadores atuais têm limitações; com a evolução tecnológica, o aumento do volume de dados e a necessidade de aumento da velocidade de processamento, algumas aplicações não são suportadas nessa arquitetura de computadores, e percebe-se que, com o tempo, não existirá hardware com potência ou velocidade de processamento suficiente para suportar aplicativos mais avançados.

Neste contexto surgiu a necessidade da criação de um computador alternativo aos atuais e que, com poder de processamento e armazenamento muito alto e extremamente veloz, com outros materiais e em altíssima velocidade, resolvesse problemas matemáticos complexos para simulação de problemas quânticos.

Na computação quântica, o elemento central é qubit (abreviatura de bit quântico), que se diferencia por assumir o estado (0,1), ou seja, assume o estado 0, o estado 1, ou ambos ao mesmo tempo, e que, como pode trabalhar simultaneamente, aumenta consideravelmente a capacidade de processamento do computador.

Se na computação clássica o processamento é sequencial, na computação quântica ele é simultâneo.

EVOLUÇÃO HISTÓRICA

As pesquisas que evoluíram para o surgimento da computação quântica se iniciaram nos Estados Unidos no século XX, na década de 1950, baseando-se nas leis da física clássica e da mecânica quântica.

Trinta anos depois, mais precisamente em 1981, o físico Richard Feynman, em uma conferência no MIT, apresentou uma proposta para a utilização de sistemas quânticos que teriam, então, uma capacidade de processamento superior à dos computadores comuns, e os descreve como a energia livre que afeta as operações da computação e o elo entre nosso cérebro e a computação quântica.

Em 1985, na Universidade de Oxford, David Deutsch detalhou o primeiro computador quântico, uma Máquina de Turing quântica, na qual simulou outro computador quântico.

O professor de matemática aplicada Peter Shor, em 1994 — quase dez anos após o trabalho de Deutsch — apresentou um novo trabalho sobre computação quântica, em Nova Jersey, no Bell Labs da AT&T, em que desenvolveu o algoritmo de Shor, capaz de fatorar grandes números a uma velocidade muito superior à dos computadores convencionais, ou seja, um algoritmo capaz de fatorar que explora o paralelismo quântico por meio da execução repetida de funções.

Em 1996, Lov Grover, também da Bell Labs, desenvolveu o Speedup, o primeiro algoritmo para pesquisa de base de dados quânticos.

Também em 1996 foi proposto um modelo para a correção do erro quântico.

No MIT, em 1999, foram construídos os primeiros protótipos de computadores quânticos utilizando montagem térmica.

A partir do ano 2000, várias universidades norte-americanas, em cooperação com instituições de pesquisa, iniciaram a construção de circuitos eletrônicos e ópticos, para implementar todos os componentes requeridos para gerar um fluxo de lógica quântica, sobretudo os componentes conhecidos por "gates", componentes construtivos bastante análogos ao circuito, já conhecidos na computação clássica.

Em 2007 surgiu o Orion, um processador quântico de 16 qubits que foi desenvolvido pela empresa canadense D-Wave.

Em 2011, a D-Wave lançou o primeiro computador quântico para comercialização, o D-Wave One, que tinha um processador de 128 qubits. Porém o D-Wave One ainda não era totalmente independente, e precisava ser usado em conjunto com computadores convencionais, de forma híbrida.

Em 2017, a D-Wave Systems lançou comercialmente o 2000Q, um computador quântico de 2.000 qubits a módicos US$15 milhões. O computador quântico anterior da companhia tinha 1.000 qubits. O desenho da D-Wave é um "annealer" quântico executando algoritmos de computação quântica adiabática feitos exclusivamente para rotinas de otimização, e assim difere e não é comparável aos computadores quânticos universais e programáveis dos demais circuitos qubit em supercondutor.

Ainda em 2017, o físico brasileiro Guilherme Tosi, junto de uma equipe de pesquisadores da Universidade de Nova Gales do Sul, na Austrália, inventou uma nova arquitetura radical para a computação quântica baseada em "flip-flop qubits" que pôde ser usada em um novo

tipo de computador quântico, permitindo assim a fabricação de processadores quânticos em larga escala, tornando-se muito mais barata — e fácil — do que se pensava ser possível, sem a necessidade do processo complicado da colocação precisa dos átomos de silício no processador.

Outro fato importante em questão era o superaquecimento das máquinas, o que levou à procura por novos metais na composição dos computadores quânticos, tanto para as baterias quanto para a forma de propagação da energia.

Atualmente, na China, mais precisamente em Xangai, existe um grande centro de pesquisas e desenvolvimento de computadores quânticos. Xangai é a capital da computação quântica nos dias de hoje.

Ou seja, as pesquisas sobre computação quântica começaram nos Estados Unidos, e por conta da matéria-prima disponível em abundância na região e mão de obra mais barata, a prática está tendo seu berço na Ásia e se propagando pelo mundo inteiro via cloud computing.

No Brasil há diversos núcleos de pesquisas na área da computação quântica. Há um grupo no LNCC (Laboratório Nacional de Computação Científica), além de grupos pertencentes às instituições de ensino superiores, com destaque para universidades do Rio de Janeiro e da Paraíba, e estudos sobre a segurança no Laboratório de Redes de Computadores (LARC) na POLI /USP e PUC São Paulo.

PERSPECTIVAS FUTURAS

A computação quântica quebra inúmeros paradigmas da computação clássica ao basear-se nas teorias da mecânica quântica da física e nos elementos que mudam as estruturas clássicas e que vêm das mudanças que a física clássica trouxe. Físicos como Heisenberg, Bohr, Schrödinger e Einstein estudaram esses novos princípios.

Entre tais princípios, podemos destacar:

- Sobreposição quântica
- A experiência do gato de Schrödinger
- Entrelaçamento quântico
- Teletransporte quântico
- Espalhamento de Rutherford
- Existência de multiverso

Tais princípios possibilitaram o desenvolvimento da computação quântica — e serão abordados ao longo deste livro —, e com a evolução das pesquisas da superposição de estados e sobreposição quântica surgiram outras pesquisas, o que motivou os estudos para a verificação de dois estados diferentes ao mesmo tempo, sendo que a experiência mental do gato de Schrödinger deu um sentido intuitivo à evolução da computação quântica.

A computação quântica foi construída sobre a fundação da teoria física e da mecânica quântica, que apresentam as leis que descrevem o futuro da inteligência artificial (IA), iniciando essa jornada pelo descobrimento dos algoritmos e nos levando a uma nova geração de equipamentos físicos, os quais vão surgindo em forma de pequenos protótipos.

A computação quântica está prevista para estar disponível comercialmente a partir do ano de 2020, com evoluções previstas para 2050 e 2100, em aplicações de inteligência artificial.

Será a computação quântica a protagonista da próxima revolução tecnoeconômica? Veremos nos próximos capítulos!

CAPÍTULO 2
O MARAVILHOSO MUNDO DA FÍSICA QUÂNTICA E O COMPUTADOR DO FUTURO

INTRODUÇÃO

"O que é pouco provável, mas possível, pode ser feito em quantum."

INES BROSSO & CLAUDE FALBRIARD

"Observe as estrelas.
Ao observá-las, perceberá que a computação quântica inspira emoções, desperta a curiosidade e ainda possui mistérios. Hoje ninguém sabe de exato como tudo isto funciona."

DR. ILYAS KAHN

"Eu acho que posso dizer com segurança que ninguém entende a mecânica quântica."

RICHARD FEYNMAN

A última revolução no mundo tecnoeconômico foi certamente a Revolução Industrial, ensinando a levantar pesos com ajuda da mecânica, criando motores a vapor e combustíveis fósseis, criando máquinas voadoras e finalmente ajudando a traduzir o funcionamento da calculadora Abacus, representada por impulsos elétricos em estados definidos como on/off (bits) disponibilizados em circuitos transistorizados.

Alguns bilhões de circuitos transistorizados, juntos, ajudaram a criar os primeiros computadores digitais e dispositivos móveis conhecidos como smartphones.

A Revolução Industrial até ajudou a paralelizar as linhas de montagens nas fábricas dos automóveis, mas, em linhas gerais, prevaleceu o esquema em série dos processos, cada vez mais ágeis.

Na técnica dos circuitos integrados e supercondutores não existem barreiras para reduzirmos ainda mais o tamanho do circuito. Não há como escapar dessa lei, e os circuitos em breve alcançarão o tamanho exato do átomo, independentemente da velocidade de nosso progresso científico.

Analisando com objetividade, existem possibilidades do surgimento dos computadores moleculares, que usam circuitos transistorizados construídos com materiais compostos de carbono, grafeno, nióbio, alumínio e silício, e nos quais o menor circuito terá o tamanho exato de um átomo de carbono.

Os computadores quânticos devem assumir o papel da próxima geração de arquitetura de computação, sobretudo em tarefas bastante especializadas, tais como a criptografia. Eles têm um desenho diferente dos atuais computadores e uma maneira totalmente diferente de programação. Atuam sobre o átomo, em vez do bit de valor 0 ou 1, e têm valores às vezes 0, outras 1, ou qualquer valor intermediário entre 0 e 1. Para programá-los, precisamos agrupá-los em um campo magnético, alinhá-los e bombardeá-los com radiação magnética, para obtermos uma mudança da sua carga (flip) e assim poder medir o eco dessa operação. Devido às interferências externas, que tornam o átomo instável (decoerência) e fazem dos átomos um aglomerado que se altera aleatoriamente, o maior problema na engenharia desses computadores é a falta de estabilidade.

A lei de Moore, válida durante os últimos anos, prevê a multiplicação da potência dos computadores a cada 18 meses, entretanto já temos em vista sinais de um certo atraso nesse período previsto, ficando cada vez mais difícil manter esse ritmo evolutivo. O fato traz reflexos de mercado, em que os chips dos computadores e smartphones são vistos como motores da prosperidade. Em breve sairemos da era do silício, indo para a era pós-silício.

A FÍSICA QUÂNTICA NA VISÃO DE EINSTEIN

FIGURA 1: Albert Einstein sorrindo — Retrato do físico teórico Albert Einstein
FONTE: Os autores, 2018.

Einstein foi o primeiro físico a dizer que a descoberta do quantum, por Planck, exigiria uma reescrita das leis da física. Para apoiar seu ponto, em 1905 ele propôs que a luz às vezes age como uma partícula, que ele chamou de "quantum da luz".

A revolução quântica de meados da década de 1920 ocorreu sob a direção dos físicos Einstein e Bohr, e seus debates pós-revolucionários tratavam de dar sentido à mudança. Os choques para Einstein começaram em 1925, quando Werner Heisenberg introduziu equações matriciais que removeram os elementos newtonianos do espaço e do tempo de qualquer realidade subjacente. O choque seguinte veio em 1926, quando Max Born propôs

que a mecânica deveria ser entendida como uma probabilidade sem qualquer explicação causal.

Einstein rejeitou essa interpretação. Em uma carta de 1926 a Max Born, Einstein escreveu: "Eu, de qualquer forma, estou convencido de que Ele [Deus] não joga dados."

Einstein observou as teorias, mas não quis aceitar o ponto de vista defendido por diversos físicos defensores da mecânica quântica, tais como Bohr, Heisenberg e Schrödinger, abrindo, assim, um debate científico. O Universo naquele momento era regido pela equação perfeita: a teoria da relatividade.

FIGURA 2: Fórmula da Teoria da Relatividade, baseada em trabalhos de Einstein: energia = massa * velocidade da luz elevada ao quadrado
FONTE: Os autores, 2018.

"Se os fatos não se encaixarem na teoria, então mude os fatos."

Albert Einstein

Einstein tinha grande percepção da "não localidade" que ele qualificava de *spookiness* (ação fantasma, ou emaranhamento a distância) e do princípio da incerteza resultante da mecânica quântica. Durante décadas, ele não parou de buscar explicações ainda mais convincentes, indo além das teorias apresentadas pelos seus colegas de debate.

A simples pergunta "O que é real?" é um bom argumento para abrir nossa mente. Precisamos de humildade enquanto investigamos as inúmeras interpretações e narrativas que explicam os dados.

O telescópio espacial NASA Hubble detectou a primeira prova da existência do espaço curvado, em que a luz desvia do campo das galáxias antes de alcançar nossos olhos. O dispositivo analisa os ruídos das galáxias e o ajuste no espectro da luz, uma pesquisa que aponta para uma expansão do Universo a partir do Big Bang.

FIGURA 3: Telescópio Espacial Hubble
FONTE: Pixabay.com | Andrew-Art.

A figura a seguir ilustra um buraco negro em rotação, resultante dos efeitos do "Tempo Espaço" curvado.

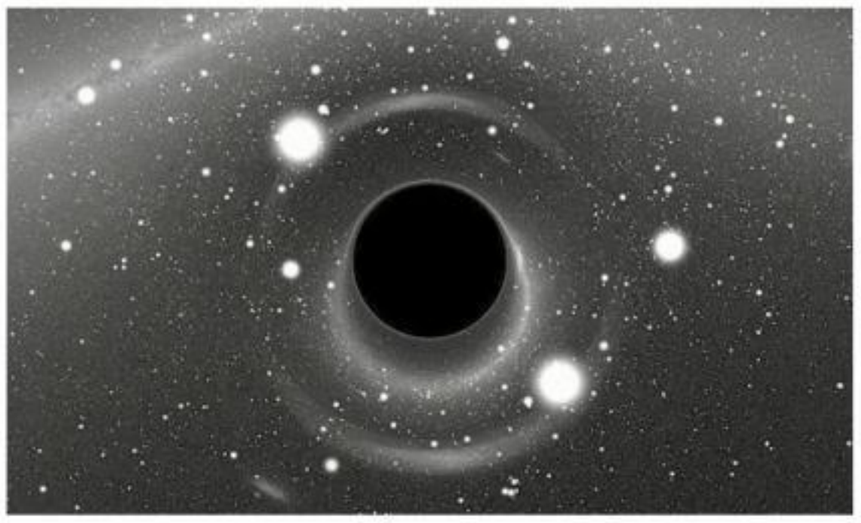


FIGURA 4: Modelo conceitual de um buraco negro rotativo
FONTE: Os autores, 2018.

Os buracos negros rotativos e os computadores quânticos usam fenômenos da mecânica quântica para processar as informações, formando assim um tópico que fascina os amantes da ciência há décadas, e até mesmo os pensadores mais inovadores raramente os posicionariam juntos. Encontramos entre os pesquisadores o doutor Stephen Hawking, que sugere de que raios X emitidos por esses buracos negros têm propriedades que os tornam portadores ideais das informações para o processamento da computação quântica. Na relatividade geral, um buraco branco é uma região hipotética do espaço-tempo que não pode ser penetrada do exterior, embora a matéria e a luz possam escapar dele.

FIGURA 5: Modelo conceitual do buraco negro e buraco branco no espaço-tempo
FONTE: Os autores, 2018.

Quantum, A Física Paralela

Na teoria, a ideia de uma física paralela oposta à física clássica nasceu pelos experimentos de Max Plank, Albert Einstein, Werner Heisenberg e pela teoria do átomo escrita por Niels Bohr, resultando em uma interpretação conhecida como interpretação de Copenhague (1927). Essa visão, sobretudo no teorema de Bell, contestava a validade das equações de Albert Einstein, colocando a física quântica em evidência.

Resumidamente, a Interpretação de Copenhague afirma que, em certo sentido, o átomo não medido não é real, sendo seus atributos criados ou realizados no ato da medição.

O teorema de Bell é fácil de entender, porém deveras difícil de acreditar. Ele informa que a realidade não deve ser local. No modelo da perturbação, os atributos medidos do átomo são determinados não apenas pelos eventos que estão ocorrendo no local da medição, mas

também por eventos arbitrariamente distantes. A prova matemática de Bell afirma e comprova que a realidade não é local. Influências não locais não enfraquecem com a distância. O teorema de Bell afirma categoricamente: "*Se é local, é uma bobagem*".

Kant definiu três termos — aparência, realidade e teoria — e denominava a realidade pelo termo "*a coisa em si*". A teoria é um pensamento humano que abrange tanto as aparências como a realidade, e as aparências estão profundamente ligas ao universo intelectual, sensorial e à natureza humana. Essa visão é um tanto imprecisa sobre a realidade. Na ciência realista, como Einstein diz, é a física que conduz a realidade.

O físico John von Neumann foi quem redefiniu, em 1932, a lógica clássica de acordo com o entendimento da física quântica, propondo uma nova lógica, descrita no livro *Mathematical Foundations of Quantum Mechanics* [A Fundação Matemática da Mecânica do Quantum, em tradução livre], e assim nasceu a lógica quântica.

A lógica tange tanto o campo da filosofia quanto o da matemática e, especialmente hoje, também o campo das ciências de computação.

O advento da teoria e os paradoxos quânticos geram um impacto profundo no campo da física. Os físicos basicamente sofreram a perda do domínio da realidade e do controle da situação, e a teoria quântica assumiu seu posto.

A teoria quântica foi criada para lidar com um problema: a interação da luz com os átomos. Os elétrons têm certas propriedades inatas, tais como massa, que servem para distingui-los das outras partículas, e eles adquirem e têm seus atributos dinâmicos, como a carga e o spin, que parecem terem sido criados pelo contexto da mensuração.

A ciência foi avançando durante as décadas de 1950 e 1960, com as primeiras viagens ao espaço, a ida do homem à Lua e a exploração dos planetas do Sistema Solar. O homem alcançou as menores partículas, chegando a desmontar os átomos com o acelerador e colisor de partículas (LHC da organização multinacional, no CERN). Os computadores evoluíram e apoiaram a ciência para desvendar os mistérios por meio da matemática e física. Novos conceitos foram postos à prova mental e comprovação física, e chegou-se à conclusão de que a física quântica é ascendente.

DIFERENÇAS ENTRE COMPUTADOR QUÂNTICO E O SISTEMA DE COMPUTAÇÃO CLÁSSICO

Vamos pegar como exemplo o maior computador comercial hoje construído, que é o sistema mainframe IBM Z14, tendo 6,1 bilhões de circuitos transistorizados e 1.832 MIPs, e assim podemos estimar que um computador de tecnologia quântica terá um acréscimo de potência em aproximadamente 1 bilhão de vezes.

O computador quântico tenta explorar a natureza imprevisível da física quântica, criando novas maneiras de programação, e explorar processos paralelos que permitem acelerar certos tipos de cálculo.

Em sistemas de tamanho reduzido dos átomos, observaremos o comportamento descrito pela física quântica, e não mais as leis da física clássica. Entretanto, a observação causará uma decoerência involuntária do sistema!

Será que seria preciso deixar de lado a observação? Ou como podemos evitá-la?

Atualmente ainda não sabemos por certo se a computação quântica em grande escala de um computador universal realmente é uma possibilidade, ou se a natureza poderia rejeitar a complexidade desenhada e até nos retornar uma resposta de decoerência. Talvez o quantum seja algo reservado à escala extremamente minúscula.

TECNOLOGIA DOS COMPUTADORES QUÂNTICOS

O acréscimo na capacidade certamente refletirá no suporte do paralelismo em algoritmos.

Outro benefício endereçará a eficiência energética dessa nova linha de computadores. Os circuitos transistorizados da atual geração de computadores apresentam basicamente o seguinte esquema, quando as novas tecnologias endereçam a eficiência energética, de modo similar ao *modus operandi* de nosso cérebro:

- Computadores clássicos (esquentam em operação):
  Input [Dados, Energia Elevada] => Processamento [Perda de Energia] => Informação
- Nosso cérebro (é desenhado para intervalos de sono e uma carga contínua):
  Input [Dados, Energia Baixa] => Processamento [Pouca Energia] => Informação e Oxigênio
- Computadores quânticos (desenhados para operação contínua):
  Input [Dados, Energia Baixa] => Processamento [Retroalimentação] => Informação

As aplicações na visibilidade imediata para a tecnologia do quantum podem estar no campo da quebra da criptografia ou em melhorias na geração das chaves de segurança utilizadas. A tecnologia das chaves RSA levaria bilhões de anos para ser quebrada em processos de computação clássica, mas em sistemas da geração quântica teríamos como quebrá-la em poucos instantes, talvez em menos de um minuto.

Há perspectivas amplas que preveem o uso da computação quântica em áreas como a pesquisa e criação de novos remédios, com sua eficácia cada vez mais elevada, ou o mapeamento completo do genoma humano, ou novas formas para armazenar a energia, ou então a criação de sementes e adubos mais produtivos. E é possível simular computadores quânticos por meio de software executado em computadores clássicos.

Software de Simulação Disponível para Computação Quântica

1. Quantum IO Monad

   O Quantum IO Monad é uma biblioteca para definir cálculos quânticos em Haskell. Pode ser pensado como uma linguagem incorporada dentro do Haskell e vem com funções para simular a execução dessas computações quânticas. A distribuição contém muitos cálculos de exemplo escritos em QIO, incluindo uma implementação do algoritmo de Shor (HASKELL, 2018).

2. QuTip – Quantum

   O QuTiP é um software de código aberto para simular a dinâmica de sistemas quânticos abertos. A biblioteca QuTiP, escrita em Python, depende dos pacotes numéricos Numpy, Scipy e Cython. Além disso, a saída gráfica é fornecida pelo Matplotlib (QuTip, 2018).

3. QISKIT – Quantum

   O Quantum Information Science Kit (Qiskit, abreviado) é um kit de desenvolvimento de software (SDK) para desenvolver aplicações de computação quântica e trabalhar com computadores NISQ (Noisy-intermidate Scale Quantum), como o IBM Q. O Qiskit é composto de elementos que funcionam juntos para permitir a computação quântica. Um desses elementos é o Terra, que é a base sobre a qual o resto do Qiskit é construído (QISKIT, 2018).

4. pyQuil da Rigetti Forest – Quantum

   O pyQuil é parte do kit de ferramentas Rigetti Forest para programação quântica na nuvem. Trata-se de é uma biblioteca Python de código aberto desenvolvida na Rigetti Computing que constrói programas para computadores quânticos. Mais concretamente, o pyQuil produz programas na Linguagem de Instrução Quantum (Quil) e cria um ambiente de execução de nuvem (Forest) (PYQUIL, 2018).

As simulações da computação quântica fornecem técnicas que ajudam a ilustrar o funcionamento da computação quântica e seus efeitos regidos pela lógica e pela mecânica quântica.

O uso de algoritmo com paralelismo cria um peso significativo, que torna seu processamento em circuitos clássicos um tanto ineficiente, e objetivamente se espera uma possível degradação exponencial.

Entretanto, a compreensão desse processo abrirá uma perspectiva valiosa para explorar plenamente o potencial dos computadores quânticos hoje disponíveis em laboratórios, tais como os processadores das marcas D-Wave, Rigetti, IBM e Google, e os recursos de computação quântica podem ser acessados experimentalmente por meio dos APIs disponíveis em sistemas de computação em nuvem.

A Teoria do Tudo e A Geometria Universal

É bom saber que por trás dos mistérios da mecânica quântica pode existir um belo mundo de geometria ordenada no mais baixo nível das partículas subatômicas, e a visualização da física é capaz de produzir um trabalho de arte.

Aqui segue uma sugestão inspiradora para todos os estudiosos em computação quântica.

FIGURA 6: Modelo conceitual em Geometria Lie – Rotação quasicristalina
FONTE: Quantum Gravity Research, 2018.

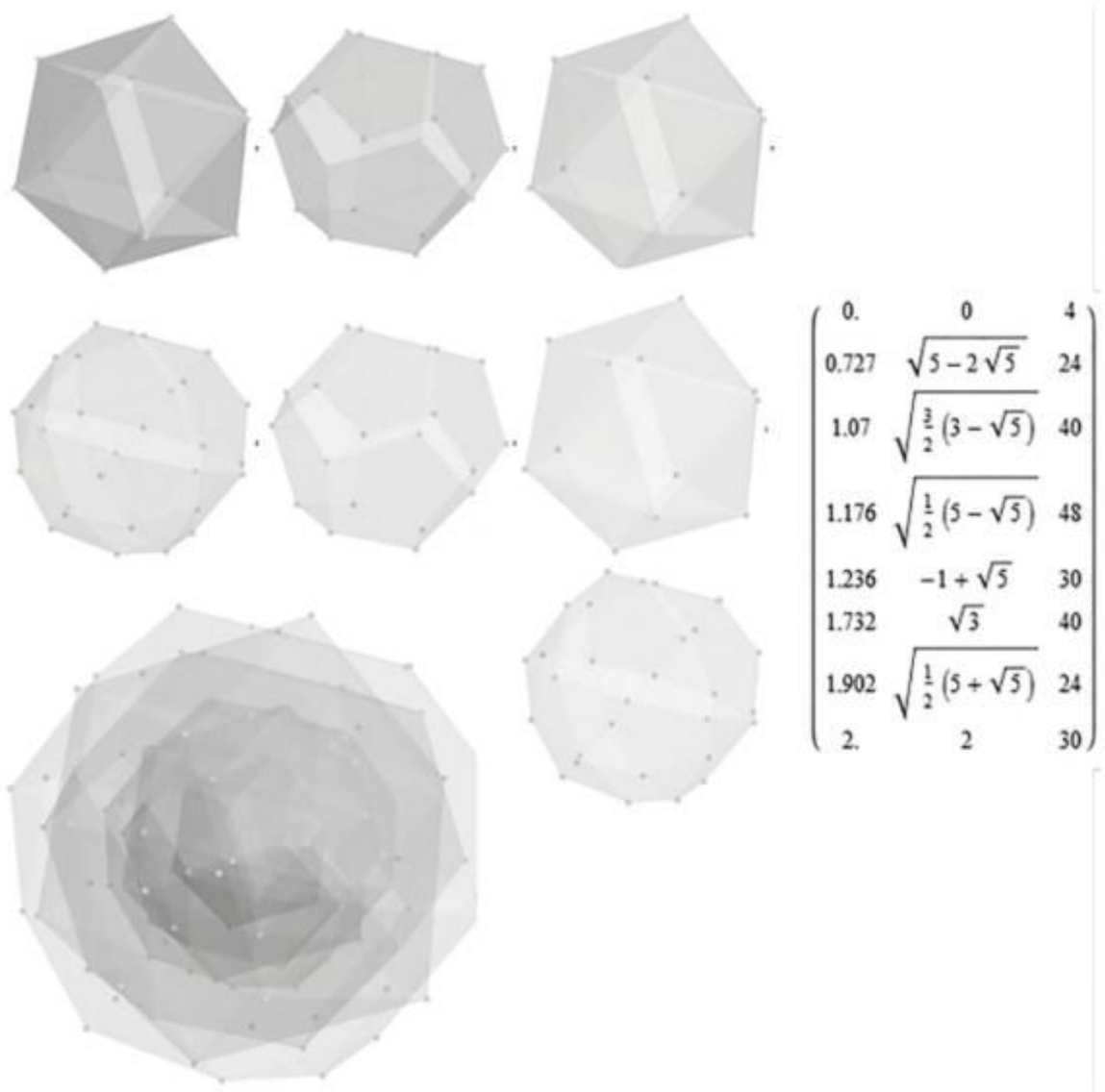
Geometria Lie E8

O grupo Lie E8 é um objeto perfeitamente simétrico de 248 dimensões e possivelmente a estrutura subjacente a tudo em nosso Universo. No século XIX, o matemático Sophus Lie criou fórmulas algébricas para descrever a forma de objetos simétricos, chamadas campos de Lie. Sua obra foi construída por matemáticos sucessores, e, na década de 1890, Wilhelm Killing encontrou um conjunto de campos de Lie que descrevia talvez a forma mais complexa em nosso Universo, o grupo E8. Trata-se de um objeto simétrico inter-relacionado 248-dimensional que é extremamente complexo.

Podemos admirá-lo e simulá-lo em modelos e desenhos tais como o modelo matemático Lie E8 ou em redes de rotação quasicristalinas.

Veja na figura a seguir o Lie E8 e suas explicações.

O polítopo E8 4_21 é projetado para 3D usando três filas da matriz de dobragem E8 a H4 dando simetria H3. Os vértices são classificados e contados por sua norma 3D. A geração do casco cada vez mais transparente de cada conjunto de normas mostra: 1) quatro pontos na origem; 2) dois icosaedros; 3) dois dodecaedros; 4) quatro icosaedros; 5) um icosadodecaedro; 6) dois dodecaedros; 7) dois icosaedros; e 8) um icosadodecaedro, com um total de 240 vértices. Isto é, naturalmente, dois conjuntos concêntricos de cascos da simetria H4 do w: 600 células dimensionadas pela razão áurea.



0.	0	4
0.727	$\sqrt{5-2\sqrt{5}}$	24
1.07	$\sqrt{\frac{3}{2}\left(3-\sqrt{5}\right)}$	40
1.176	$\sqrt{\frac{1}{2}\left(5-\sqrt{5}\right)}$	48
1.236	$-1+\sqrt{5}$	30
1.732	$\sqrt{3}$	40
1.902	$\sqrt{\frac{1}{2}\left(5+\sqrt{5}\right)}$	24
2.	2	30

FIGURA 7: Geometria dos polítopos do grupo Lie
FONTE: Quantum Gravity Research, 2018.

O pesquisador Garrett Lisi, físico teórico, afirma:

> Cada partícula elementar conhecida é identificada por suas cargas em relação às forças eletromagnética, fraca, forte e gravitacional. Os elétrons têm carga elétrica -1, quarks acima de 2/3, quarks abaixo de -1/3 e neutrinos 0, com antipartículas com cargas elétricas opostas. No modelo-padrão, essas cargas elétricas são uma combinação da hipercarga das partículas, Y, e carga fraca, W.
>
> Essas cargas correspondem à geometria dos grupos de Lie, e os modelos unificados de física de partículas correspondem a como os grupos de Lie do modelo-padrão e a gravidade incorporam-se a grupos de Lie maiores, até o maior grupo de Lie excepcionalmente simples, E8.

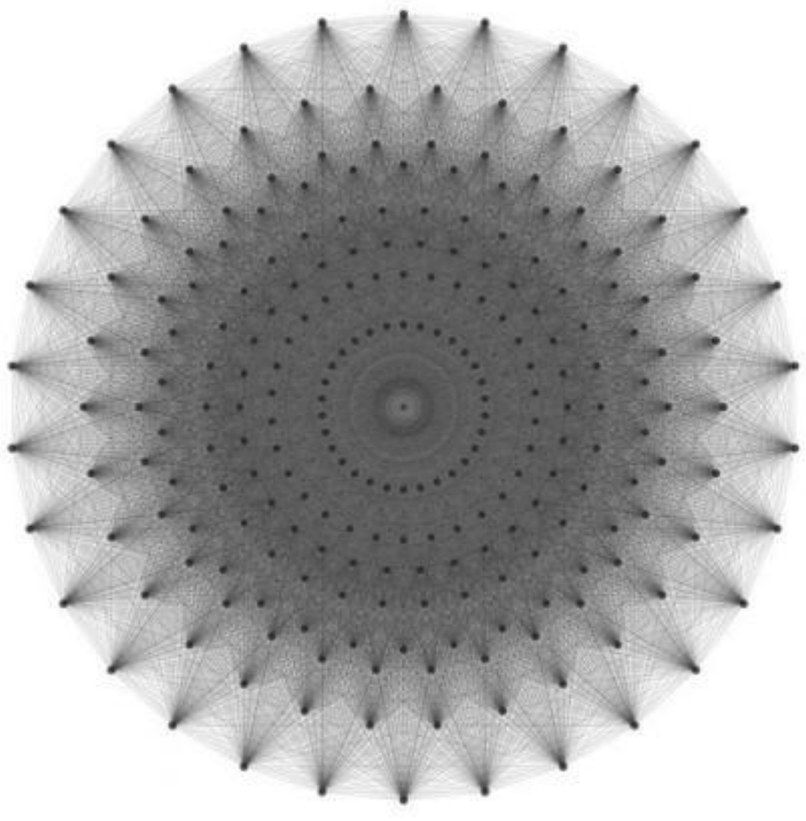


FIGURA 8: Geometria Lie grupo E8
FONTE: Quantum Gravity Research, 2018.

Embora a proposta de Lisi, “a teoria de tudo”, tenha aspectos empolgantes, ela não ganhou aceitação no mundo da física. Hoje a teoria está sendo amplamente, mas não inteiramente, ignorada. Talvez seja um trabalho ainda em progresso e, quase como toda nova proposta teórica é apresentada de uma maneira defeituosa e incompleta, com questões abertas que precisam ser preenchidas.

Quasicristais

O cristal quasiperiódico, ou quasicristal, é uma estrutura ordenada, mas não periódica, portanto é um padrão quasicristalino que preenche continuamente todo o espaço disponível, mas sem simetria translacional. Na figura encontra-se um programa gerador escrito em linguagem Python que executa uma simulação da visualização 2D da geometria dos quasicristais (programa: QuasiCrystalGenerator.ipynb).

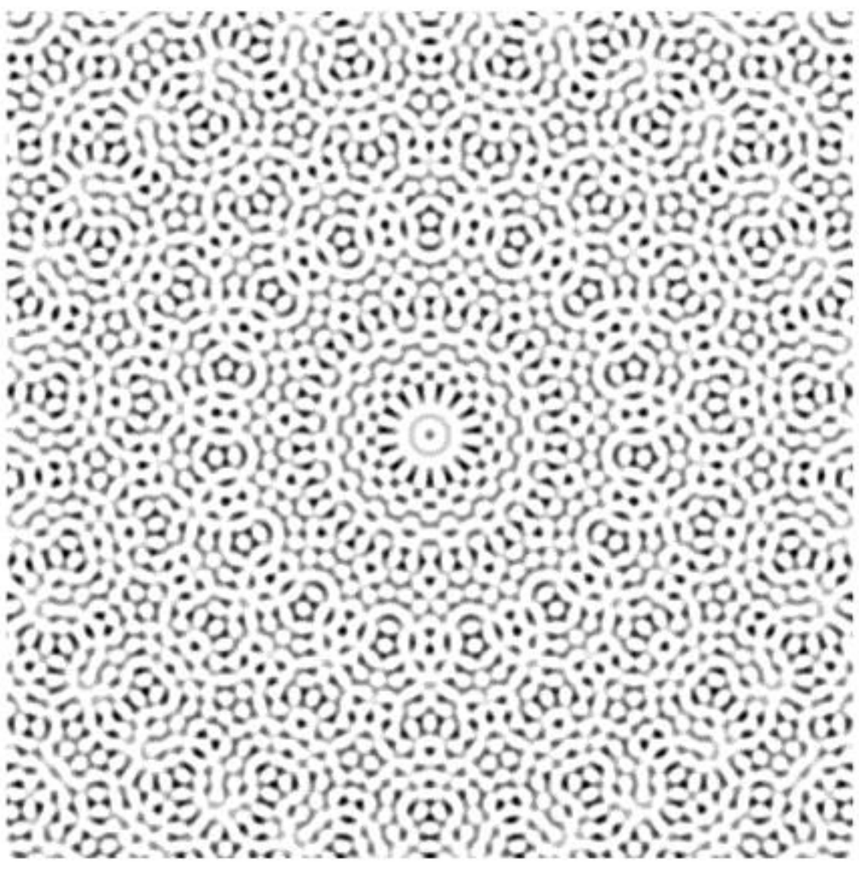


FIGURA 9: Estruturas de quasicristais
FONTE: Os autores, 2018.

LÓGICA QUÂNTICA E O PARADIGMA DA INCERTEZA

A lógica quântica foi introduzida por John von Neumann como uma alternativa à lógica clássica, a fim de reconciliar a aparente inconsistência entre a lógica proposicional clássica e os desenvolvimentos mais recentes da mecânica quântica, a partir da equação de Schrödinger.

O nascimento oficial da lógica quântica (QL) foi produzido com o artigo seminal de 1936 “A Lógica da Mecânica Quântica”, em que Birkhoff e von Neumann fizeram a proposta de uma lógica não clássica para a teoria, argumentando que o problema de saber se o formalismo espacial de Hilbert, de estrutura lógica, pode ser útil para o entendimento da mecânica quântica. Na introdução do artigo, eles enfatizam:

> Um dos aspectos da teoria quântica que atraiu a atenção geral é a novidade das noções lógicas que pressupõe. Afirma que mesmo uma descrição matemática

> completa de um sistema físico S, em geral, não permite predizer com certeza o resultado de um experimento em S e que em particular nunca se pode prever com certeza tanto a posição quanto o momento de S (o princípio da incerteza de Heisenberg). Além disso, afirma que a maioria dos pares de observações não pode ser feita simultaneamente em S (princípio da não comutatividade das observações).

A lógica quântica, em essência, pode ser pensada como um casamento entre lógica proposicional quântica e cálculo de probabilidade do quantum.

Projeções podem ser vistas como proposições sobre observáveis físicos. Uma vez que seu espectro está contido no conjunto de dois pontos, {0, 1}, eles podem ser verdadeiros ou falsos. Como operadores autoadjuntos podem ser representados em termos de projeções, segue-se que os observáveis na mecânica quântica podem ser representados em termos de proposições com valores de verdade 0 ou 1.

A principal diferença entre a lógica clássica e a lógica quântica é o fracasso dessa lei como resultado do princípio da incerteza de Heisenberg, e assim, enquanto redes booleanas são o pano de fundo para a lógica clássica, na lógica quântica exigimos a rede ortodôntica, ou rede Hilbert.

> *"Como pode a natureza ser tão absurda quanto se nos mostra nessas experiências atômicas?"*
>
> **Weiner Heisenberg**

Por outro lado, antes é preciso dizer que o nome "lógica quântica" é um pouco enganador: "Pela lógica quântica padrão, usualmente se entende a rede ortomodular completa baseada nos subespaços fechados em um espaço de Hilbert." É desnecessário observar que tal terminologia, que identifica uma lógica com um exemplo particular de uma estrutura algébrica, acaba sendo um pouco enganosa do ponto de vista estritamente lógico.

Diferentes formas da lógica quântica (QL) podem ser obtidas pela construção de semântica algébrica, ou kripkeana (de acordo com o filósofo Saul Aaron Kripke), sobre a estrutura algébrica do espaço de Hilbert.

A física quântica descreve a mecânica do mundo ainda oculto em primeira vista fugindo de nossa lógica de verdadeiro e falso, da verdade e da mentira. A nova física descreve uma lógica de possibilidades infinitas, tão infinitas que ainda não foram exploradas por nossa mente, e nem podem ser detectadas por nossa vida e nossos sentidos.

Podemos tentar aplicar a antiga lista de operadores de lógica sobre essa nova visão e perceber que ela não seria o suficiente para descrever todos os estados. A unidade básica, o nosso bit do mundo digital, sim, é bastante similar, exceto que ele possui um ou outro estado, ou ambos, ou todos os vetores possíveis em um espaço.

Como assim "ou ambos"? Quer dizer que o bit, na visão quântica, poderá ter os valores 0 e 1 ao mesmo tempo? Sim, e justamente essa sobreposição (*superposition*) é que qualifica nosso novo componente na lógica do mundo quântico, o qubit, como algo versátil e equipado com superpoderes.

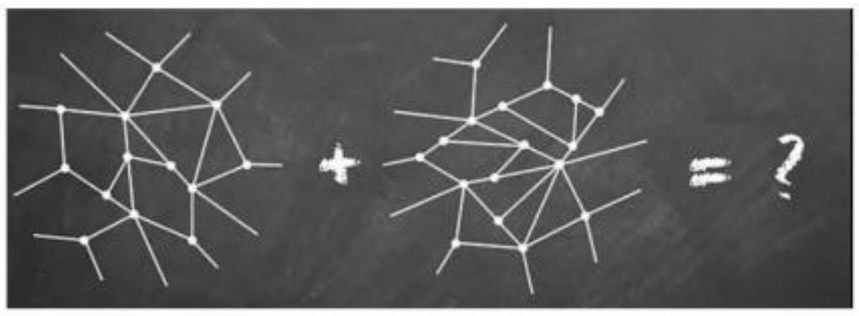


FIGURA 10: O desafio da adição de duas redes neuronais
FONTE: Os autores, 2018.

Operações de Lógica

A lógica quântica (QL) foi desenvolvida como uma tentativa de construir uma estrutura proposicional que permitisse descrever os eventos de interesse na mecânica quântica (QM). A QL substituiu a estrutura booleana, que, embora adequada para o discurso da física clássica, era inadequada para representar o domínio atômico.

De fato, a QM tem sido relacionada à modalidade desde 1926, quando Max Born interpretou a função de onda quântica Ψ em termos de uma densidade de probabilidade.

No entanto, ficou claro desde o início que essa nova possibilidade quântica era algo completamente diferente daquela considerada nas teorias clássicas.

O conceito é o da onda de probabilidade (a mecânica quântica era algo inteiramente novo na física teórica desde Newton), e probabilidade, em matemática ou em mecânica estatística, significa uma declaração sobre nosso grau de conhecimento da situação real.

Ao jogar dados, não conhecemos os detalhes do movimento de nossas mãos que determinam a queda dos dados e, portanto, dizemos que a probabilidade de lançar um número especial é apenas uma em seis. A função de onda de probabilidade, no entanto, significava mais do que isso: significava uma tendência para algo. De acordo com Werner Heisenberg, o conceito da onda de probabilidade "era uma versão quantitativa do antigo conceito de *potentia* na filosofia aristotélica. Introduziu algo entre a ideia de um evento e o evento real, um estranho tipo de realidade física, apenas entre a possibilidade e a realidade".

De acordo com a axiomatização de QM de John von Neumann, a interpretação matemática de um sistema físico é um espaço Hilbert separável do complexo H, e um estado puro é representado por um raio em H. Diferentemente do esquema clássico, grandezas físicas são representadas por autoadjunto, operadores em H que, em geral, não comutam sob multiplicação. Os valores que qualquer magnitude pode tomar são os autovalores (valor eigen), operador correspondente, e cada um dos quais vem com o seu autoestado (estado eigen) associado. A não comutatividade dos operadores tem consequências interpretativas problemáticas, pois é então difícil afirmar que as

magnitudes quânticas assim representadas são simultaneamente preexistentes à observação.

A evolução do estado é dada pela equação de Schrödinger, que, devido à sua linearidade, implica a existência formal de superposições quânticas de estados. O fato de que estados podem ser linearmente combinados proíbe o uso de meros subconjuntos como representantes de proposições; eles são bem representados por subespaços fechados de H.

As Treliças Lógicas

Para figurar a estrutura de várias lógicas, os matemáticos utilizam um diagrama chamado de treliça, que mostra em um relance todas as relações de E/OU entre os atributos. A treliça ordena os atributos do sistema de acordo com sua abrangência, com o elemento mais abrangente sendo posicionado no topo da estrutura. A estrutura lógica dos atributos de polarização é mostrada na Figura 11. Como vimos, a estrutura de atributo de cor booleana, [operação E], envolve um movimento descendente, enquanto a [operação OU] envolve um movimento ascendente.

Portanto, (H OU D = Todos) quando (H E D = Nenhum).

Os atributos são conectados por meio de linhas que mostram como cada par de atributos mais baixos se junta para formar um novo atributo mais alto. A treliça das cores é um exemplo de diagrama da lógica clássica e apresenta as relações lógicas existentes entre as cores primárias e secundárias. As cores primárias (vermelho, verde e azul) são a base para misturas aditivas de cores, com as quais formam as imagens da TV colorida. A impressão em cores (processo substrativo) também é baseada em misturas de cores (processo substrativo) e demonstra a mistura de cores complementares, tais como amarelo, magenta e ciano. Como exemplo, a operação AND para azul resulta da adição das cores ciano (azul esverdeado) e magenta, na ordem de cima para baixo.

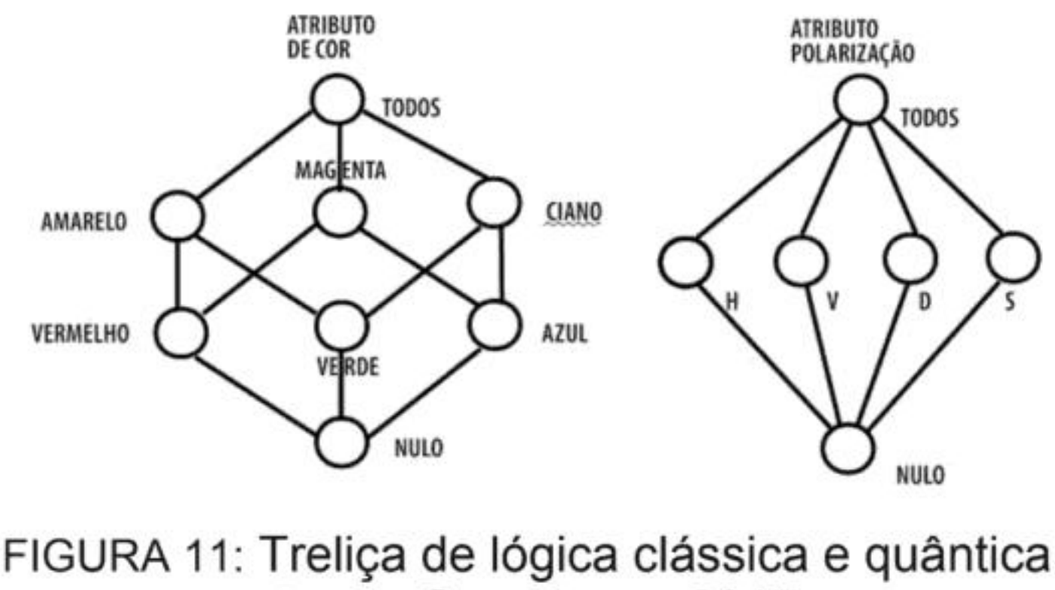


FIGURA 11: Treliça de lógica clássica e quântica
FONTE: Os autores, 2017.

Exemplos de polarização:

H OU D = TODOS (superposição)

H E D = NULO (nenhum raio passará um filtro óptico)

A lei distributiva é válida para qualquer treliça. Aqui um exemplo com três atributos:

A OU (B E C) = (A OU B) E (A OU C)

É uma regra que vale em geral, exceto para as treliças de lógica quântica, em que a lei da distribuição não é aplicada:

H OU (D E CD) = H OU N = H

(H OU D) E (H OU CD) = T E T = T

Os atributos de polarização P(0) e P(45) formam uma treliça não distributiva.

Para calcular o resultado da operação E (AND) de qualquer par de atributos A-B, procura-se o atributo comum mais alto, que pode ser encontrado seguindo-se as linhas de cima para baixo, partindo de A e B.

Para calcular o resultado da operação OU (OR) de qualquer par de atributos A e B, procura-se o atributo comum mais baixo, que pode ser encontrado seguindo-se as linhas de baixo para cima partindo de A e B.

Essas relações E e OU são mais do que conexões lógicas abstratas; elas correspondem às operações físicas reais. As treliças lógicas quânticas seguem todas as regras booleanas. A entidade quântica não está completamente aberta para observação. Seus atributos são somente visíveis e representam apenas uma parte de sua faixa de possibilidades. O restante da treliça quântica contém relações ocultas que distinguem uma entidade quântica do objeto clássico.

Conceito de Polarização

A direção da oscilação da luz em seu campo elétrico determina o estado de polarização da luz. Considerando as oscilações das ondas elétricas da luz como uma onda de água propagante, dizemos que a luz é polarizada verticalmente quando a oscilação da onda (elétrica) sobe e desce na direção vertical. Se, por outro lado, a oscilação (elétrica) da onda é horizontal, então dizemos que a luz é polarizada horizontalmente. Qualquer outra direção de polarização, então, é apenas uma combinação linear dessas polarizações planas. Chamamos essas polarizações em que o plano de oscilação permanece fixo de polarização linear do espaço. Se, por outro lado, podemos ter uma situação na qual o plano de oscilação gira de uma vertical para uma horizontal e de volta para uma direção vertical à medida que a luz viaja no espaço, isso leva a uma polarização elíptica, ou circular, que pode ser esquerda ou destra.

A polarização da luz não afeta nem sua energia, nem seu momento, mas determina de que maneira a onda de luz pode conduzir sua influência. Por exemplo, cargas que só podem oscilar em uma direção vertical não serão afetadas por uma luz polarizada horizontalmente, porque essa luz só pode causar oscilações na direção vertical. Assim, uma luz polarizada verticalmente passaria inalterada através de tal meio. No caso de uma luz polarizada elipticamente caindo sobre a mesma carga, ela terá apenas o componente

vertical de sua oscilação elétrica absorvido; o componente horizontal permanecerá inalterado.

Quando reduzimos a intensidade da luz ao seu menor nível possível, estamos lidando com um único fóton, a luz quantizada. No nível de fótons, a polarização está relacionada ao seu chamado momento angular (intrínseco) — spin. Fótons, descobriu-se, vêm em duas variedades: o momento angular canhoto ou destro. Esse estado quantificado do fóton é referido como sua helicidade ou seu spin. Então, na realidade, a polarização intrínseca do fóton é puramente circular; polarização circular direita (estado R) ou esquerda (estado L).

Como consequência, a luz polarizada linear deve ser feita de uma combinação de fótons polarizados circulares esquerdo e direito. Mas é agora que vem a questão preocupante: o que acontece quando reduzimos a intensidade de um feixe de luz linearmente polarizado mais e mais até o ponto em que acabamos "com um fóton de cada vez"? Seu estado de polarização, sabemos, deve ser medido para saber se é uma polarização circular esquerda ou direita, mas a polarização do feixe (linear) precisa ser uma mistura de ambos!

Os experimentos que lidam com essa forma de fóton único consideram o seguinte como verdadeiro: o fóton é polarizado circularmente com uma probabilidade igual à mistura dessas polarizações, necessária para compensar a polarização do feixe de luz original. Por exemplo, se nosso feixe original fosse linearmente polarizado, poderíamos construir essa polarização com um número igual de fótons de estado R e L. Em seguida, a probabilidade de um único fóton ser polarizado circularmente para a esquerda ou para a direita é de 50%. O que é interessante, no entanto, é que experimentos verificaram que, na verdade, essa probabilidade de 50% não é a probabilidade do conjunto (coleção de fótons), mas a probabilidade de cada fóton individualmente! Isso significa que cada fóton nessa luz linearmente polarizada está em uma mistura igual dos estados de spin intrinsecamente puro de R e L!

Conceito do Giro (Spin)

Além dos fótons, outras partículas elementares, como elétrons, prótons e até mesmo nêutrons, também têm a propriedade ou atributo que chamamos de spin. Não há uma explicação clara para essa propriedade na física clássica. É, como no caso dos fótons, relacionada às propriedades do tipo momento angular. O estado de spin do fóton está ligado à sua direção de propagação, então um fóton que entra na página é medido para ser R ou L. Se estiver no estado R, seu momento angular é anti-horário, enquanto, se acontecer de estar no estado L, seu momento angular é no sentido horário. O spin do elétron também é quantizado, mas a direção da quantização não tem nada a ver com a direção do movimento do elétron. Mais especificamente, seu spin pode ter três direções separadas independentes, como nos eixos x, y e z. É a direção de um campo magnético externo que decide as direções de rotação quantificadas. Um campo magnético externo orientado verticalmente faz com que os elétrons que interagem com esse campo tenham seu ponto de spin para cima ou para baixo, isto é, o sentido de polarização do spin torna-se vertical. (Isso

ocorre porque o momento magnético do elétron interage com o campo magnético externo.) Direções de quantização semelhantes são ditadas por direções do campo magnético externo para outras partículas, incluindo as de nêutrons.

Conceito do Estado Misto

Já discutimos esse conceito no contexto da polarização de fótons. Evidentemente, sistemas microscópicos, como partículas elementares e átomos, comportam-se como se qualquer uma de suas propriedades fosse feita de uma "mistura" que não é diretamente mensurável. O que podemos medir é um estado (valor quantizado da propriedade) ou o outro, mas não a mistura. No entanto, evidências experimentais mostram que a mistura existe! Um exemplo disso é demonstrado na experiência "qual caminho". De fato, esses experimentos parecem sugerir que, nesses casos, a causalidade pode ser violada. Para ver como isso pode acontecer, vamos examinar o experimento de Schneider e LaPuma envolvendo polarização de fótons.

Essa experiência utiliza um interferômetro do tipo Mach-Zehnder para criar franjas de interferência de uma fonte laser polarizada aleatoriamente no plano (isto é, polarizada circularmente). Esse tipo de interferômetro é composto de dois divisores de feixe e dois espelhos, que primeiro dividem um feixe de laser em dois feixes separados e depois sobrepõem esses dois feixes para criar um padrão de interferência em uma tela (aqui, uma câmera de vídeo). Além dos divisores de feixe e da tela, são usados nesse experimento existem dois polarizadores e um analisador. As polarizações são usadas de maneira cruzada em cada perna do interferômetro, e o analisador é colocado logo antes da tela.

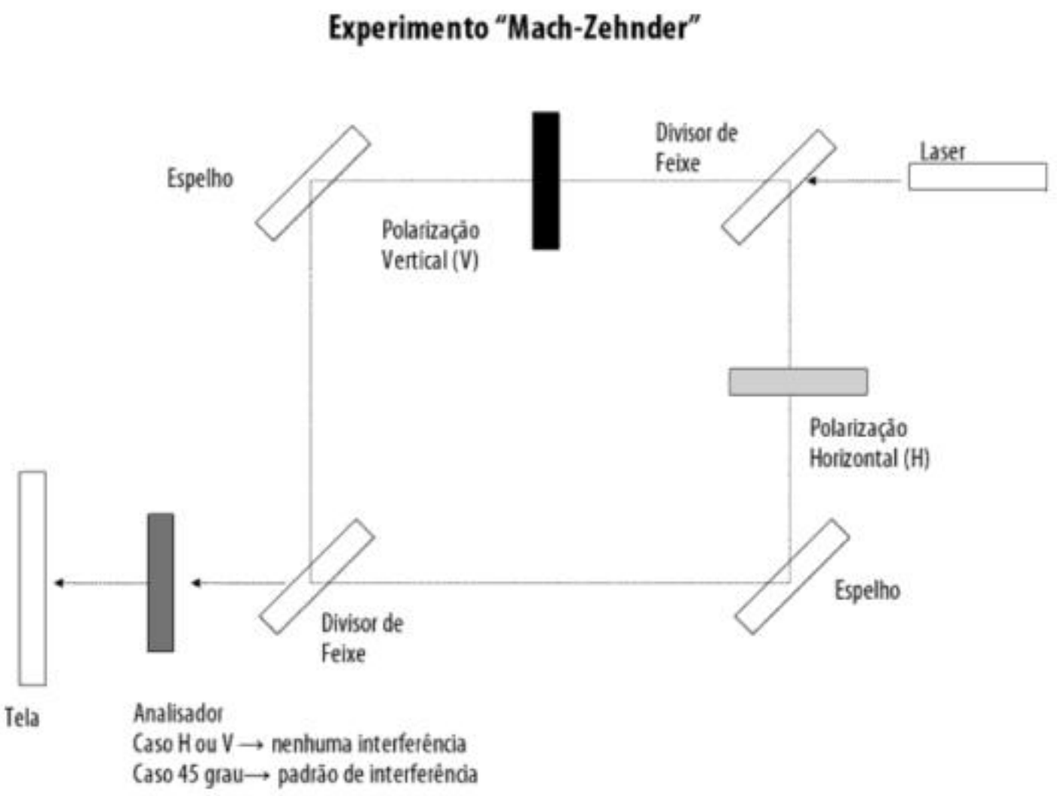


FIGURA 12: Bancada ótica para o experimento Mach-Zehnder
FONTE: Os autores, 2018.

Na Figura 12, o cinza-claro polarizado é ajustado para polarização horizontal, e o preto, para polarização vertical. Quando o analisador cinza-escuro é orientado para polarização horizontal (ou para polarização vertical), nenhuma interferência é observada. No entanto, quando é orientado a 45 graus, uma das chamadas orientações de borracha, a interferência aparece. Isso demonstra que quando as combinações polarizador-analisador executam o

experimento para determinar a direção de polarização da luz (fóton) que passa em cada caminho, então o estado de "mistura" se torna definido. No entanto, quando o analisador está na orientação "borracha", apesar do fato de as luzes cruzadas não interferirem, o padrão de interferência aparece. Isso mostra claramente que os fótons estão em estado misto até serem detectados. Para obter detalhes sobre esse experimento e os resultados obtidos, faça uma busca no Google por "Photon Quantum Eraser Experiment".

Um conceito interessante que não tem analogia em nosso mundo macroscópico, mas que existe no mundo microscópico e é descrito pela teoria da mecânica quântica, é o do entrelaçamento. Pares de fótons emaranhados são criados no laboratório usando-se o método de down conversion em um cristal não linear. Nesse processo, uma intensa luz laser cria dois fótons com a metade da energia de um único fóton no laser. Nesse sentido, a frequência do fóton é reduzida pela metade ou convertida para baixo. Da mesma forma, existem processos atômicos que criam elétrons entrelaçados.

INTERFERÊNCIAS ONDULATÓRIAS

A interferência de ondas consiste na superposição de duas ondas no espaço. Esse fenômeno pode ser classificado de duas formas: interferência construtiva ou destrutiva. Quando duas ondas superpõem-se na mesma região do espaço, ocorre a interferência, que resulta em outra onda com intensidade diferente.

Duas ondas e amplitudes se somam em fase:

1 + 1 = 2

Duas ondas e amplitudes se cancelam fora de fase:

1 + 1 = 0

Duas ondas e amplitudes têm fase arbitrária:

1 + 1 = 0 a 2

ONDAS E SONS

O teorema da transformada de Fourier fornece métodos e osciladores em semicondutor para a criação de novos timbres, sons impossíveis de se criar por meios mecânicos (o mesmo conceito aplicado nos sintetizadores do Robert Moog).

As partículas apresentam características ondulatórias, e, ao mesmo tempo, as ondas apresentam características de partículas.

Probabilidade = (Possibilidade) ao quadrado, em que a possibilidade representa a onda.

Quon	Massa	Carga	Spin
Elétron	1	-1	½
Próton	1836	1	½

Fóton	0	0	1

FIGURA 13: Atributos quânticos em partículas elementares.
FONTE: Herbert, 1985.

TEORIAS DA REALIDADE

A seguir relacionamos as principais teorias da realidade que são importantes para a ciência física e, em uma visão mais ampla, também à compreensão do Universo.

Um dos mais bem guardados segredos da ciência é o fato de que os físicos perderam seu pulso sobre a realidade. O que fecha a porta ao público é, em parte, a barreira da linguagem. O formalismo matemático que facilita a comunicação entre cientistas é incompreensível para os leigos. O livro escrito pelo autor Nick Herbert ajuda a compreender como os físicos lidam, ou não conseguem lidar, com a realidade e examina cada uma das realidades descritas a seguir:

- Realidade quântica 1: Não existe nenhuma realidade profunda (Copenhague).
- Realidade quântica 2: A realidade é criada pela observação (Copenhague).
- Realidade quântica 3: A realidade é um todo indiviso.
- Realidade quântica 4: A interpretação dos mundos múltiplos.
- Realidade quântica 5: A lógica quântica.
- Realidade quântica 6: O mundo é construído de objetos comuns.
- Realidade quântica 7: A consciência cria a realidade.
- Realidade quântica 8: O mundo duplo.

Esperamos que os físicos saibam determinar experimentalmente o tipo de mundo em que vivemos e possam confirmar uma ou múltiplas teorias expostas. Todas elas podem, no entanto, estar erradas (HERBERT, 1985).

SALTO QUÂNTICO

Definição:

> *É uma transição abrupta (como de um elétron, um átomo ou uma molécula) de um estado de energia discreto para outro.*

O termo tenta explicar como os elétrons podem transitar instantaneamente entre os níveis de energia dentro de um átomo. Geralmente podemos observar três estados:

- Estado do solo (o estado-padrão), denominado “g” (órbita menor).
- Estado exitado (um estado frágil), denominado “e” (órbita maior).
- Metaestado (duração prolongada), denominado “m” (orbita intermediária).

Caso houver uma alimentação de energia, por exemplo, por meio de uma luz laser, o elétron saltará do estado de "ground" para "excitado", e isso ocorre instantaneamente, proporcionando ao observador a noção de que um salto acontece sempre aleatoriamente. No caso do hidrogênio, esse momento ocorre repetidamente de 10 a 11 vezes por segundo.

Para observar esse salto, os físicos prendem um átomo em uma câmara de vácuo e observam-no através de uma janela. Muitos fótons são emitidos durante o experimento e podem ser vistos a olho nu. Após ter trocado de estado (de "g" para "e" e depois de volta a "g") e, ao receber energia, o átomo poderá mudar para um estado "m" (estado metaestável) e ficar nele por algum tempo. Isso gera um resultado imprevisível para o observador: a luz, a emissão dos fótons, liga e desliga aleatoriamente.

Além da emissão de energia (fótons), o átomo, ao colapsar seu estado para o estado "g", também absorve energia.

Quantum Leap foi uma série de televisão norte-americana de ficção científica que foi ao ar entre 1989 e maio de 1993. Nela temos o Dr. Sam Beckett, físico que atravessa o espaço-tempo durante um experimento em viagem no tempo, tomando temporariamente o lugar de outras pessoas para corrigir erros históricos.

De fato, o "salto quântico" é mais uma façanha da física, tornando essa expressão popular, descrevendo assim uma mudança brusca em direção a uma nova meta com um efeito um tanto positivo.

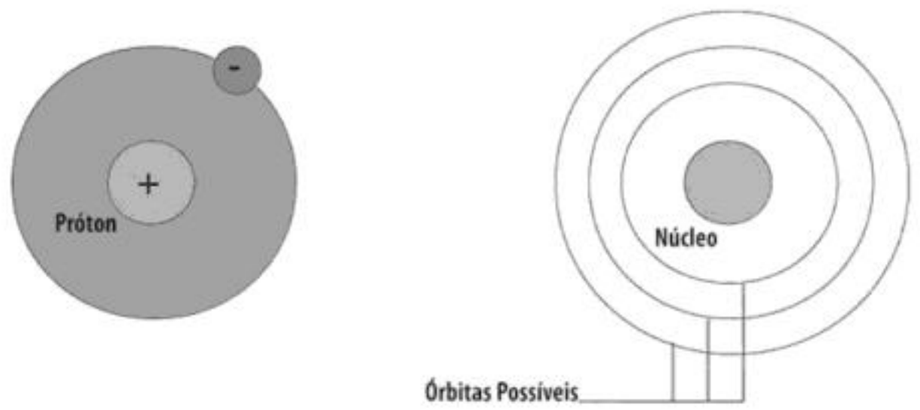


FIGURA 14: Modelo do átomo descrito por Niels Bohr/Órbitas possíveis do elétron
FONTE: Os autores, 2018.

Da soma das teorias populares já abordadas, ficou em evidência uma simples pergunta: será que as conexões não locais permitiriam transportar sinalizações mais rápidas do que a luz? Se o mundo realmente está ligado por conexões mais rápidas do que a luz, não poderíamos explorar essas ligações enviando mensagens? Seria, de fato, uma nova era para humanidade, agora senhora do espaço e do tempo?

O ponto de vista da ciência é o de que o observador poderá, sim, enviar mensagens mais rápidas do que a luz, mas o observador não poderá decifrá-las. Essas ligações constituem linhas privadas acessíveis somente à natureza interditada ao uso humano por um indecifrável embaralhamento decorrente do perfeito estado aleatório quântico.

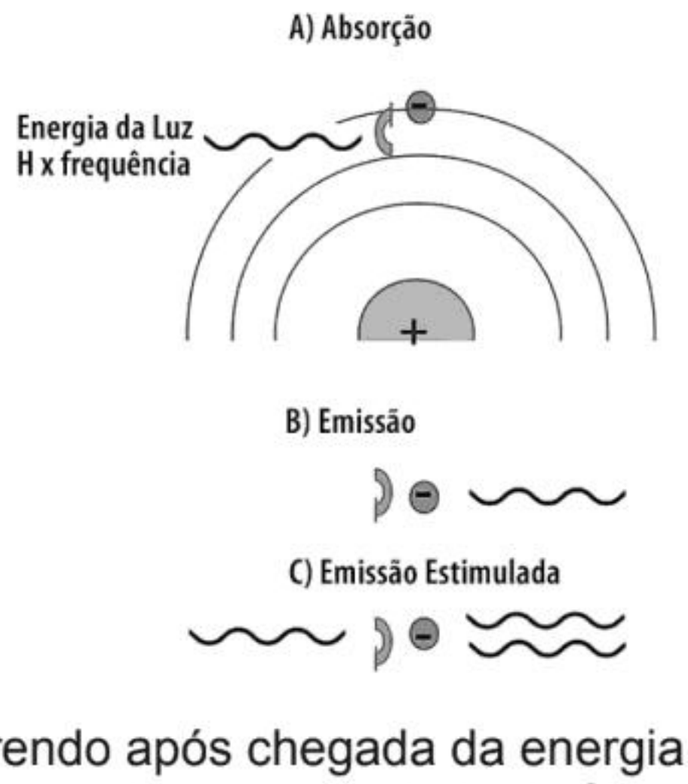


FIGURA 15: Salto quântico ocorrendo após chegada da energia de luz (laser), absorção, emissão e emissão estimulada de fótons
FONTE: Os autores, 2018.

A teoria quântica descreve a divisão do mundo em duas partes: o "sistema" e o "instrumento M". O mundo é um todo, sem linhas divisórias, embora o primeiro passo de qualquer computação quântica seja o rompimento dessa unidade.

No tempo-espaço, o mundo torna-se um espaço tetradimensional (Einstein). Na teoria quântica, precisamos descrever o mundo como sendo uma sobreposição simultânea de todas as possibilidades, mas, como humanos, percebemos o mundo apenas como uma sequência de realidades definidas, descritas pela física clássica.

MECÂNICA QUÂNTICA E A LÓGICA QUÂNTICA EM SISTEMAS DE COMPUTAÇÃO

Em níveis subatômicos, tudo o que sabemos sobre física clássica é rompida, não apenas por uma pequena margem, mas, sim, em escala maciça. Bem-vindo ao mundo da mecânica quântica e esteja pronto para se surpreender.

Antes de começarmos a falar sobre computação quântica, devemos ter uma boa noção do que é a mecânica quântica, o que é especial nela e como seus fenômenos nos ajudam a realizar cálculos avançados.

Pesquisas iniciais sobre mecânica quântica podem ser datadas do século XVII, quando os cientistas propuseram a teoria da luz das ondas (a luz pode exibir tanto uma teoria de ondas quanto uma de partículas ao mesmo tempo). A existência de um quantum de luz foi proposta por Max Planck em 1900, e foi reforçada por Albert Einstein, afirmando que a luz é composta de pequenas partículas chamadas fótons, e cada fóton tem energia. Em geral, a mecânica quântica lida com o comportamento da matéria e suas interações com a energia na escala de átomos e partículas subatômicas.

Com o advento da mecânica quântica, a mecânica newtoniana (ou mecânica clássica) começou a diminuir em níveis fundamentais. Alguma natureza específica da luz em si não pôde ser explicada pela física clássica. Na série espectral do hidrogênio, por exemplo, quando o gás hidrogênio é aquecido em um tubo e a luz emitida é observada, pode ser

notado que o espectro de emissão do hidrogênio atômico contém número de séries espectrais, em vez de apresentar uma emissão contínua de luz (ou radiação eletromagnética). Sim, é mais como bandas de cores e diferente da expectativa da física clássica.

O físico dinamarquês Niels Bohr veio com uma explicação para isso. Segundo o modelo de Bohr, o átomo é como um pequeno núcleo carregado positivamente, cercado por elétrons que viajam em órbitas circulares ao redor do núcleo — semelhante à estrutura do Sistema Solar. Cada órbita corresponde a um nível de energia diferente. Mudanças de energia, como a transição de um elétron de uma órbita para outra em torno do núcleo de um átomo, são feitas em quantas discretos. O termo "salto quântico" refere-se ao movimento abrupto de um nível discreto de energia para outro, sem transição suave. Não há "entre".

O salto quântico era especial porque o movimento do elétron não era progressivo — apenas desaparecia de uma órbita e aparecia na próxima órbita sem estado intermediário e emitia (ou absorvia) uma quantidade específica de energia. Bem, isso torna as coisas interessantes. Bohr explicou que a quantidade de energia nesse nível não pode ser subdividida e é chamada quanta, uma quantidade mínima específica de energia. Foram as primeiras percepções desse tipo de níveis de energia e, como foram fornecidas por um físico chamado Planck, chamamos isso de constante de Planck. Assim, em geral, a energia do elétron em um átomo é quantizada.

Esse é apenas o começo, onde a previsibilidade da física clássica foi superada pela potencialidade da física quântica. E isso foi muito preocupante para muitos físicos da época. Por que um elétron segue órbitas quantizadas e não tem estados intermediários?

A tese de Louis de Broglie em 1923 respondeu a essa questão. Ele explicou que a matéria pode exibir tanto a natureza de uma partícula quanto a de ondas, como a da luz. E a natureza ondulatória dos elétrons insiste em que eles obtenham certos comprimentos de onda que lhes permitam se encaixar em uma órbita. Mas, com essa órbita, o elétron existe em todos os lugares, não apenas em um ponto específico, devido à sua natureza ondulatória. Isso é fundamentalmente diferente do exposto pela física clássica, mas foi comprovado experimentalmente, porque a matéria com massa mais alta, como nós humanos, tem um alto momento, e o comprimento de onda de tais assuntos será consideravelmente menor, já que a massa é inversamente proporcional ao comprimento de onda de Broglie. Assim, o efeito da explicação de Broglie diminui nos níveis macroscópicos.

O experimento da dupla fenda, conduzido por Davisson e Germer em 1927, provou que a luz e a matéria podem exibir propriedades de ondas e de partículas classicamente definidas. Uma forma semelhante, porém mais simples, do experimento de dupla fenda foi realizada por Thomas Young em 1801. A luz, quando passada através de duas fendas em uma barreira, pode ser de padrão de interferência na tela do outro lado (a luz passando pela fenda dupla não forma um padrão de banda dupla na tela). A parte interessante desses

experimentos é que, mesmo se passarmos um elétron/fóton um de cada vez, o padrão de interferência se acumula na tela/detector. Como diabos isso é possível?

Isso significa que, se enviarmos um único elétron de uma fonte através de uma dupla fenda (e não soubermos por qual fenda o elétron passa), o lugar na tela (ou detector) em que o elétron aparece no outro lado é probabilístico (pode ser qualquer lugar em um padrão de interferência). E, se enviarmos uma quantidade considerável de elétrons, ela formará o padrão de interferência do outro lado. Isso significa que cada único elétron deve exibir a propriedade de uma onda, caso contrário ele não estará interferindo com qualquer outra coisa. A única onda de elétrons em um lado da barreira produzirá duas ondas no outro lado da barreira de dupla fenda (como uma única onda de água passada por dois buracos pode formar duas ondas do outro lado), e essas duas ondas interagem uma com a outra para formar um padrão de interferência.

Erwin Schrödinger publicou uma equação que descreve o elétron em movimento como uma onda que se espalha. A equação é também conhecida como equação de Schrödinger, que o ajudou a ganhar o Prêmio Nobel de Física em 1933.

O físico e matemático alemão Max Born formulou a função de densidade de probabilidade, que descreve tudo isso como uma possibilidade de encontrar elétrons como ondas. Isso aconteceu depois de seus estudos sobre as órbitas de elétrons do modelo de Bohr, que ajudaram a formular a representação da mecânica da matriz da mecânica quântica juntamente com Werner Heisenberg. Mais tarde, Heisenberg propôs o princípio da incerteza de Heisenberg, que determina que a posição e a velocidade de uma partícula não podem ser medidas exatamente ao mesmo tempo, mesmo em teoria.

Werner Heisenberg e Niels Bohr criaram a interpretação de Copenhague da mecânica quântica, que afirma que os sistemas físicos geralmente não têm propriedades definidas antes de serem medidos, e a mecânica quântica só pode prever as probabilidades de que as medições produzirão certos resultados. O ato de medir resultará em um colapso da função de onda, alterando as probabilidades em um valor possível.

Albert Einstein respondeu:

> *Deus não joga dados com o Universo.*

Niels Bohr respondeu:

> *Pare de dizer a Deus o que fazer com seus dados.*

A coisa toda da física quântica era difícil de digerir, mesmo para a mente mais brilhante de todos os tempos. Mas ficou evidente no experimento da dupla fenda que, se tentarmos descobrir por qual fenda o elétron passa, colocando um dispositivo de medição em qualquer uma das fendas, o padrão de interferência desaparece.

Portanto, não tem sentido atribuir a realidade ao Universo na ausência de observação. Nos intervalos entre as medições, os sistemas quânticos realmente existem como uma

mistura difusa de todas as propriedades possíveis. Essa é a sobreposição quântica, o Universo material normal tem significado apenas no momento da medição.

No caso de nosso elétron, a sobreposição pode ser descrita como a possibilidade de o elétron estar em posição diferente ao mesmo tempo. Isso também pode ser aplicado ao spin (que é uma forma intrínseca do momento angular) do elétron, conforme o princípio da incerteza. O elétron pode girar em todas as direções até medirmos seu giro, pois, quando medimos o spin, ele será alinhado na direção da medição ou na direção oposta. Isso também é chamado de *spin up* ou *spin down*.

Caso um computador quântico precise executar uma adição de **0+1**, o sistema também adicionará **1+0** e **1+1** e um **0+0**, e todas as operações executarão ao mesmo tempo, formando a sobreposição. Assim, a solução de problemas numéricos teoricamente poderia ser executada bem mais rapidamente.

As coisas são diferentes no sistema quântico e também difíceis de entender à primeira vista. A fim de relaxar, talvez seja necessário conhecer a teoria do gato. E quanto ao gato de Schrödinger?

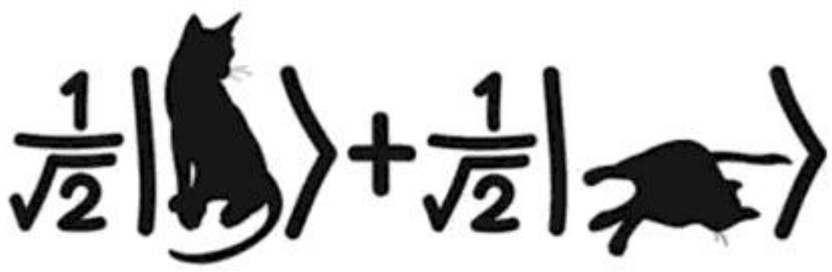


FIGURA 16: Experimento de pensamento do gato de Schrödinger
FONTE: Os autores, 2018.

Resumidamente, um gato em uma caixa fechada com algo (digamos, um explosivo) que pode ou não matá-lo está em sobreposição, o que significa que o gato pode estar vivo ou morto para o mundo exterior. Então, até abrirmos a caixa e observarmos o gato, metade da probabilidade é a de que ele esteja morto, e a outra metade da probabilidade é a de ele estar vivo.

Há mais uma implicação importante para esse experimento, que é o que acontece na caixa fechada. Se o gato sentir a explosão, então ele estará morto; se não sentir a explosão, ele estará vivo. O estado do gato é um pouco ligado ao do explosivo. No mundo quântico, isso é descrito como entrelaçamento quântico.

Emaranhamento quântico é o fenômeno pelo qual mais de uma partícula gerada em conjunto ou intimamente interagida pode iniciar um relacionamento, e o estado quântico de cada partícula não pode ser descrito independentemente (se o gato está morto, o explosivo explodiu/se o explosivo explodiu, o gato está morto). Assim, a partícula não pode ser descrita independentemente, ela se torna um sistema conectado, e a medição de um afeta o estado de outro. Essa propriedade será preservada mesmo quando separadas por grande distância.

Por exemplo, considere dois elétrons que estão emaranhados. Consideraremos que os spins (posição ou momento pode ser considerado, tomaremos o spin que é momento angular) dos elétrons somam zero quando são gerados. Agora podemos separar esses elétrons por qualquer distância e medi-los independentemente. Se o primeiro elétron mede um giro, então o outro será sempre girado para baixo, e vice-versa. E o efeito da medição acontece instantaneamente, o que significa mais rápido do que a velocidade da luz.

A ideia é que partículas quânticas emaranhadas existem em um estado de probabilidades e só perderão a sobreposição se uma das partículas for medida — e a outra partícula será afetada instantaneamente, mesmo que separadas por qualquer distância.

Muitos cientistas da época ficaram loucos devido a essa afirmação, inclusive Einstein, que se referiu a isso como sendo uma "ação fantasmagórica a distância". Ele chegou a pensar no paradoxo do EPR, que diz que duas partículas interagem para formar relacionamentos profundos e trocar informações codificadas em alguns "parâmetros ocultos" sobre os possíveis estados. Assim como um elétron diz "se alguém me medir, eu vou girar", outro diz que vai girar, caso contrário ele quebrará a teoria da relatividade enviando informações mais rapidamente do que a velocidade da luz.

Alain Aspect refutou o paradoxo da EPR em 1980 usando o experimento do teste de Bell baseado no teorema de Bell, proposto por John Stewart Bell em 1964. Sim, o mundo quântico é real e existem ações assustadoras.

Agora vamos recapitular cada tópico tendo em perspectiva a computação quântica.

A computação quântica estuda sistemas teóricos de computação que fazem uso direto de fenômenos da mecânica quântica, como sobreposição e emaranhamento, para realizar operações em dados.

No computador clássico, transformamos qualquer dado em zeros e uns, chamados bits.

Na verdade, a passagem da alta tensão com baixa voltagem para o processamento ocorre através de uma série de portas lógicas que podem manipular os dados para descobrir o resultado. Portas lógicas como AND, OR, NOT, XOR etc. podem ser organizadas de diferentes maneiras para processar os bits e produzir a saída. Elas podem fazer operações simples como uma adição ou operações complexas como a criptografia, e são fisicamente realizadas usando-se transistores, que hoje em dia dependem das propriedades dos semicondutores de silício para realizar a operação, evitando o uso de chaves mecânicas.

Uma razão para isso é que as portas quânticas são diferentes das portas clássicas, e que devem sempre ser reversíveis. Isso praticamente significa que os portais AND nem mesmo existem no mundo quântico (pelo menos, não no mesmo sentido de uma porta AND clássica). Em vez disso, há um conjunto diferente de portas, tais como CNOT (1982), TOFFOLI (1980), FREDKIN (1969) e outros, que permitem fazer tudo o que é possível pela computação quântica sem quebrar a condição de reversibilidade.

A outra questão é que qubits podem ser ambos, em 0 e 1, e a porta quântica deve cuidar disso. Mas isso não é um problema, apenas significa que a saída deve ser uma sobreposição de 0 e 1. Por exemplo, vamos pegar um simples gate NOT. Se a entrada é uma "sobreposição" de 30% 0 e 70% 1, então a saída se torna 70% de 0 e 30% de 1. É claro que esta é uma explicação muito superficial e bastante imprecisa, mas a ideia é exatamente essa.

Os computadores clássicos são rápidos e eficientes, mas não são bons em problemas que envolvem complexidade exponencial, como a fatoração de números inteiros (*integer*), especialmente a fatoração primária, quando os números inteiros são restritos a números primos (*semiprime*). Basicamente, é fácil encontrar o produto de dois grandes números primos, mas é preciso muita computação com computadores clássicos para encontrar os números que o produziram, dado o produto. De fato, essa complexidade é a base de muitos sistemas criptográficos, incluindo o funcionamento do padrão RSA.

Então, como computadores quânticos lidam com esse problema?

Na computação quântica, a unidade computacional básica é um qubit, que pode representar a informação. Um qubit tem algumas semelhanças com o bit normal, tal como pode ser medido como 0 ou 1, mas seu poder reside em suas propriedades mecânicas quânticas, como sobreposição e emaranhamento — um qubit pode estar em estado 0 e em um estado 1 ao mesmo tempo. Os estados de um qubit são representados usando-se a notação "ket 0" e "ket 1" e são escritos como |0> e |1>, e o estado medido básico é semelhante ao clássico 0 e 1.

O que exatamente pode ser um qubit em um computador quântico real? Bem, pode ser um elétron com um spin; um fóton com polarização; spins de impurezas; íons aprisionados; átomo neutro; um circuito semicondutor etc.

A superposição do qubit simples pode ser representada usando-se abaixo da esfera de Bloch.

Pode parecer um pouco complexo, mas o ponto principal que precisamos ter em mente é que o single qubit a qualquer momento pode estar em uma superposição de |0> e |1> e pode ser expresso como:

$$a\,|0\rangle + b\,|1\rangle$$

em que a e b são as amplitudes (proporcionais às probabilidades) do qubit sendo medido para 0 e 1 respectivamente, e:

$$a^2 + b^2 = 1$$

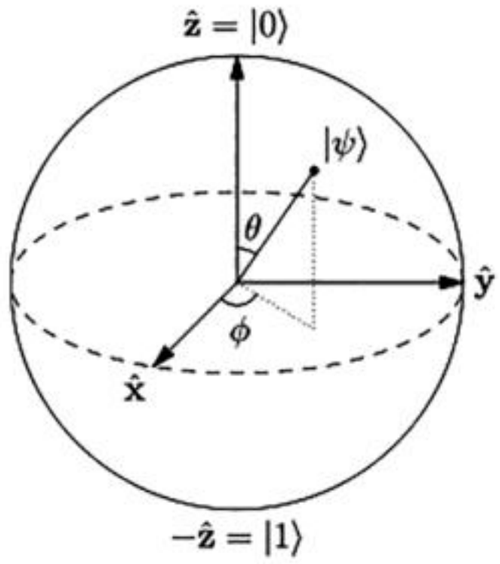


FIGURA 17: Visualização em qutip, 2018. Esfera de Bloch e seus eixos em orientação 3D (x, y, z)
FONTE: Os autores, 2018.

Assim, um qubit pode estar na superposição de dois estados e, uma vez medido, retornará um dos dois estados com base nas probabilidades de cada um deles. Assim, medir um qubit em si tem um efeito sobre o sistema, então a medição de um qubit é similar a um gate que afeta o estado do qubit.

Se considerarmos mais de um — digamos, dois — qubit, as coisas se tornam mais interessantes. O estado básico será 00, 01, 10, 11, mas os qubits podem estar em superposição de todos os estados ao mesmo tempo. Então, isso deve ser representado como:

a |00> + b |01> + c |10> + d |11>

A fim de representar dois qubits, precisamos de quatro probabilidades/amplitude (a, b, c, d). Se tivermos três qubits, precisaremos de oito. Então, se tivermos n qubits, precisaremos de 2 ** n números para representar o estado geral desse sistema quântico. Assim, com um pequeno aumento no número de qubits poderemos gerar sistemas capazes de representar estados enormes, e isso é diferente do que ocorre com computadores clássicos.

Mesmo que a quantidade de informação necessária para descrever a superposição cresça exponencialmente com o número de qubits, não poderemos acessar todas essas informações, por causa dos limites fundamentais da medição quântica. A rotação de um elétron em sobreposição pode ser em todas as direções, mas quando a medimos é somente em uma direção, para cima ou para baixo. Também não seremos capazes de prever a saída, pois ela é probabilística — com base na probabilidade associada ao estado (exemplo: metade das vezes acima e metade das vezes abaixo). Isso significa que, para usar todo o potencial do computador quântico, precisamos desenvolver algoritmos quânticos que explorem a existência de grande quantidade de informações armazenadas na sobreposição de qubits e, no final da computação, deixem o sistema em um dos estados-base que podemos detectar com uma certa clareza.

Em um computador quântico, é possível ter dois qubits com valores opostos, mas o valor dos qubits individuais é desconhecido até a medição. Isso é possível por causa do entrelaçamento quântico. Digamos que temos dois elétrons qubit que têm estado zero, então colocamos o primeiro elétron/qubit em sobreposição aplicando uma onda

eletromagnética, com uma certa frequência, que é proporcional à diferença de energia entre o estado 0 e o 1. Agora, quando tentamos ajustar o segundo elétron/qubit aplicando a onda eletromagnética de frequência que foi necessária quando o primeiro elétron/qubit estava no estado 0, o primeiro elétron/qubit na superposição terá um efeito na rotação do segundo qubit, e o segundo também se moverá para uma sobreposição (não um estado estável). Assim, o estado desses dois qubits será emaranhado, e, se medirmos primeiro um e começarmos a girar, o outro dará um spin para baixo e vice-versa. Esse emaranhamento será preservado a qualquer distância. Até medi-los, os dois qubits só podem ser considerados um único sistema com valores prováveis. Isso é impossível em computadores clássicos. Neles não se pode ter dois bits sem valor, exceto os valores opostos.

Assim, o aumento no número de qubits aumentará exponencialmente o número de possíveis estados emaranhados. Um ponto importante a ser observado é que o emaranhamento quântico pode ser muito frágil (a decoerência quântica), e qualquer sistema que utilize isso deve ter uma interferência externa mínima.

Os blocos de construção dos circuitos quânticos (modelo para computação quântica) são a porta lógica quântica. Eles são como portas lógicas do mundo da computação clássica, mas, ao contrário de muitos portais lógicos clássicos, *as portas da lógica quântica são reversíveis.* Isso ocorre porque a mecânica quântica exige um sistema quântico para nunca perder informações ao longo do tempo, e deve sempre ser possível reconstruir o passado.

Você consegue pensar em algum portal clássico que alcança o mundo quântico?

O AND gate não fará isso, já que ambos **1 AND 0, 0 AND 1** dão saída como valor 0.

Por ser uma comparação lógica reversível, o NOT pode chegar ao mundo quântico:

NOT 0 = 1, NOT 1 = 0

Isso será reversível se a saída for 0, então a entrada será 1; e se a saída for 1, a entrada será zero. Essa porta é conhecida pelo nome de porta **Pauli-X** no mundo quântico. Ele mapeia **|0>** para **|1>** e **|1>** para **|0>**.

A porta de **Hadamard** também age em um único qubit e cria uma sobreposição, e a porta do "**troca troca**" usa dois qubits, isto é, **|10>** a **|01>** e assim por diante.

Portas controladas atuam em dois ou mais qubits, em que um ou mais qubits agem como um controle para alguma operação. Por exemplo, a porta **NOT** controlada (ou **CNOT**) atua em dois qubits e executa a operação NOT no segundo qubit somente quando o primeiro qubit é |1>, e, por outro lado, deixa-o inalterado.

Porta "CNOT":

TABELA 1: Estados quânticos antes e depois do NOT controlado

Antes		Depois	
Controle	Alvo	Controle	Alvo
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

FONTE: Os autores, 2018.

No caso da porta CNOT, também podemos ver que cada saída é distinta, não há ambiguidade e os estados podem ser restaurados.

Em um computador quântico baseado na rotação de elétrons, a porta **CNOT** pode ser facilmente implementada, já que o bit de controle e o bit de destino estão juntos, e os bits de controle têm algum efeito sobre o bit de destino, e este decide se podemos virar o alvo com certa onda eletromagnética.

A porta CNOT também pode ser usada para produzir o estado emaranhado de controle e alvo. Se aplicarmos a porta de Hadamard para controlar primeiro e, em seguida, aplicarmos a porta CNOT, tanto o controle quanto o alvo estarão em sobreposição e entrelaçados juntos. A porta CNOT é geralmente usada na computação quântica para gerar estados emaranhados.

CNOT, juntamente com a rotação arbitrária do qubit, pode implementar quaisquer funções lógicas em computadores quânticos.

Existem, ainda, outras portas quânticas.

A **medição** de um qubit também poderá alterar o estado do sistema e funciona de forma muito semelhante às portas, mas não é um portal quântico real.

Para que um computador quântico funcione, devemos ser capazes de alterar propriedades de qubits arbitrários e de executar portas lógicas quânticas em um ou mais qubits, fazendo interação entre eles.

Agora precisamos utilizar toda essa lógica para criar alguns algoritmos úteis. Não faz sentido usar um computador quântico para realizar operações computacionalmente simples, já que computadores clássicos podem fazer isso com uma taxa mais acessível. Devido ao fato de que a infraestrutura em si é complexa e os computadores quânticos podem lidar com grande número de estados ao mesmo tempo, o uso efetivo de computadores quânticos está confinado a áreas específicas, como encontrar os fatores primos, pesquisar grande quantidade de dados etc., que são computacionalmente intensivas.

O **algoritmo quântico** é um procedimento passo a passo no qual cada uma das etapas pode ser executada em um computador quântico, e isso envolverá propriedades quânticas, como sobreposição e emaranhamento. Existem diferentes algoritmos já disponíveis, e mais estão no *pipeline*.

O **algoritmo de Shor** para fatoração inteira é um dos mais famosos, por causa de sua implicação na criptografia.

O **algoritmo de Grover** também é bastante conhecido e usado para pesquisar um banco de dados não estruturado ou uma lista não ordenada.

Existem outros algoritmos interessantes disponíveis que você pode encontrar aqui. Vamos explorar uma pequena variante do algoritmo de Grover, o algoritmo quântico para pesquisa de dados.

Passo 1) Primeiro, considere uma lista de N números de telefones e nomes entre os quais precisamos encontrar o nome de um número específico.

Ao contrário dos algoritmos quânticos normais, que fornecem um aumento exponencial na velocidade, o algoritmo de Grover fornece apenas um aumento quadrático na velocidade. A complexidade será uma função da raiz quadrada do número de elementos possíveis, N. Isso é muito mais eficiente quando comparado com algoritmos clássicos, que podem apresentar complexidade. O trabalho do algoritmo de Grover usa a amplificação da amplitude.

Para o nosso exemplo, vamos considerar apenas quatro números, que podem ser representados usando-se dois qubits, e precisamos encontrar o nome associado a 10:

a |00> + b |01> + c |10> + d |11>

em que a, b, c e d são as amplitudes e a = b = c = d.

Este é o primeiro passo no algoritmo de Grover: colocar o qubit em superposição.

Passo 2) Aplicar uma função oracle que vira a amplitude do item que estamos procurando na direção oposta. Nesse caso, c se torna -c. Agora a = b = d, e c é diferente e negativo.

Passo 3) Aplicar uma função de amplificação que amplifique a diferença entre cada amplitude e dos estados de sobreposição iguais. Como o valor de -c está tendo muita diferença em relação à outra amplitude, o valor de c aumenta rapidamente em comparação com a, b ou d.

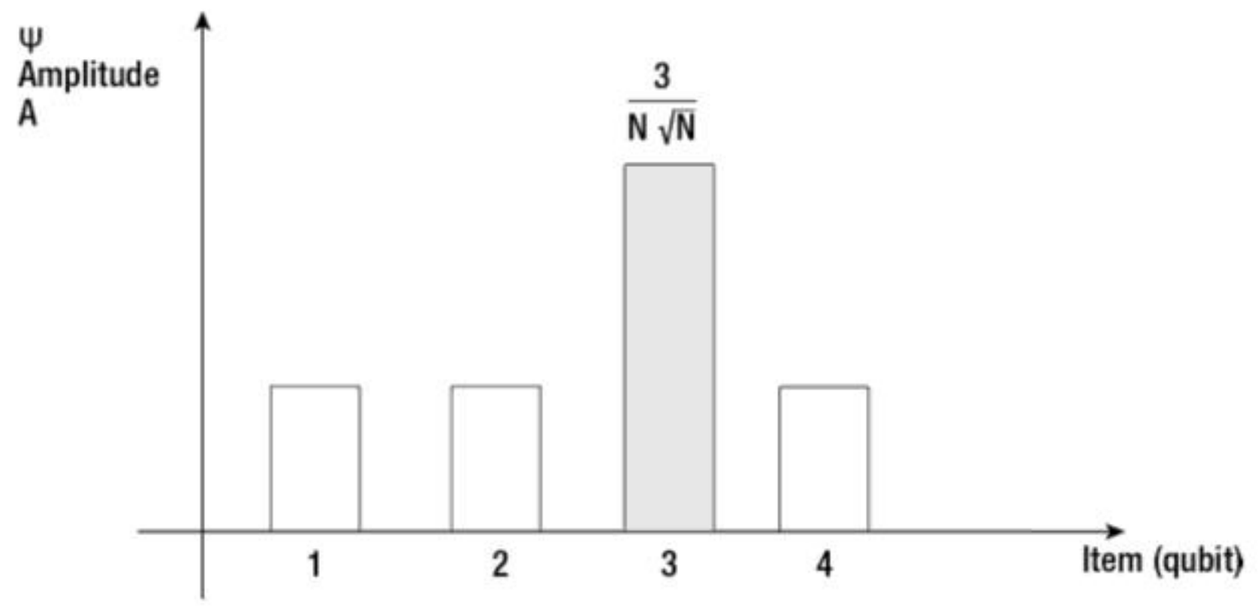


FIGURA 18: Medição da probabilidade, estado ψ em Colapso para o estado φ
FONTE: Os autores, 2018.

Agora, se medirmos os qubits, o terceiro estado será retornado com máxima probabilidade (os Passos 2 e 3 podem ser aplicados novamente para aumentar a probabilidade). Então, usando essa técnica, podemos resolver a busca carregando todos os valores disponíveis no qubit de uma só vez. Quanto maior o número de qubits disponíveis, maiores são os tamanhos de domínios com os quais podemos trabalhar.

Mas o que acontece com o hardware para executar tudo isso?

A implementação atual de computadores quânticos é baseada em semicondutores. Os qubits gerados a partir desses semicondutores devem ser mantidos longe de qualquer interferência externa. De outro modo, as propriedades quânticas mecânicas desses qubits serão perdidas. Assim, a temperatura desses computadores quânticos é mantida muito próxima do zero absoluto, e a configuração para isso, juntamente com os cálculos em níveis microscópicos, pode tornar os computadores quânticos extremamente caros. Ondas de micro-ondas/eletromagnéticas precisas podem ser usadas para modificar os estados de qubites.

É comum o caso de um computador clássico ser usado junto de um computador quântico para ajudar no processamento.

O centro de computação quântica da IBM, conhecido por IBM Q, é uma iniciativa pioneira para construir computadores quânticos universais comercialmente disponíveis para negócios e ciências. O IBM Q Experience nos permite executar algoritmos quânticos usando gratuitamente o compositor online ou sua biblioteca em linguagem Python. O número de qubits nesses sistemas é relativamente pequeno, mas aumentará rapidamente no decorrer dos próximos anos.

A D-Wave Systems é outra grande empresa nesse espaço, com seu computador quântico D-Wave 2000Q qubit 2000. Os produtos da D-Wave são amplamente utilizados por empresas como o Google, para executar o Quantum Artificial Intelligence Lab, e também pela NASA em suas pesquisas.

A máquina D-Wave usa o princípio do *recozimento quantum* para realizar suas operações. Isso é ótimo para otimizar soluções para problemas pesquisando rapidamente em um espaço e encontrando o mínimo global que se torna a solução. Essa abordagem pode ser mais rápida para determinados domínios problemáticos, mas um sistema que utiliza o recozimento quântico, em estado *hardwired* e de difícil uso programático, terá dificuldade em executar certos algoritmos, como o famoso algoritmo de Shor.

Por outro lado, a computação quântica universal oferecida pela IBM servirá a domínios de problemas amplos e nos permitirá projetar algoritmos complexos. Projetar esses algoritmos escritos especificamente para a computação quântica universal pode ser algo complexo e vem com seus próprios desafios no desenho do sistema.

A mecânica quântica é um campo da ciência que é inerentemente surpreendente, e as capacidades de computação oferecidas por ela são apenas a ponta do iceberg. A tecnologia