

CLAUDE FALBRIARD E INES BROSSO

COMPUTAÇÃO QUÂNTICA

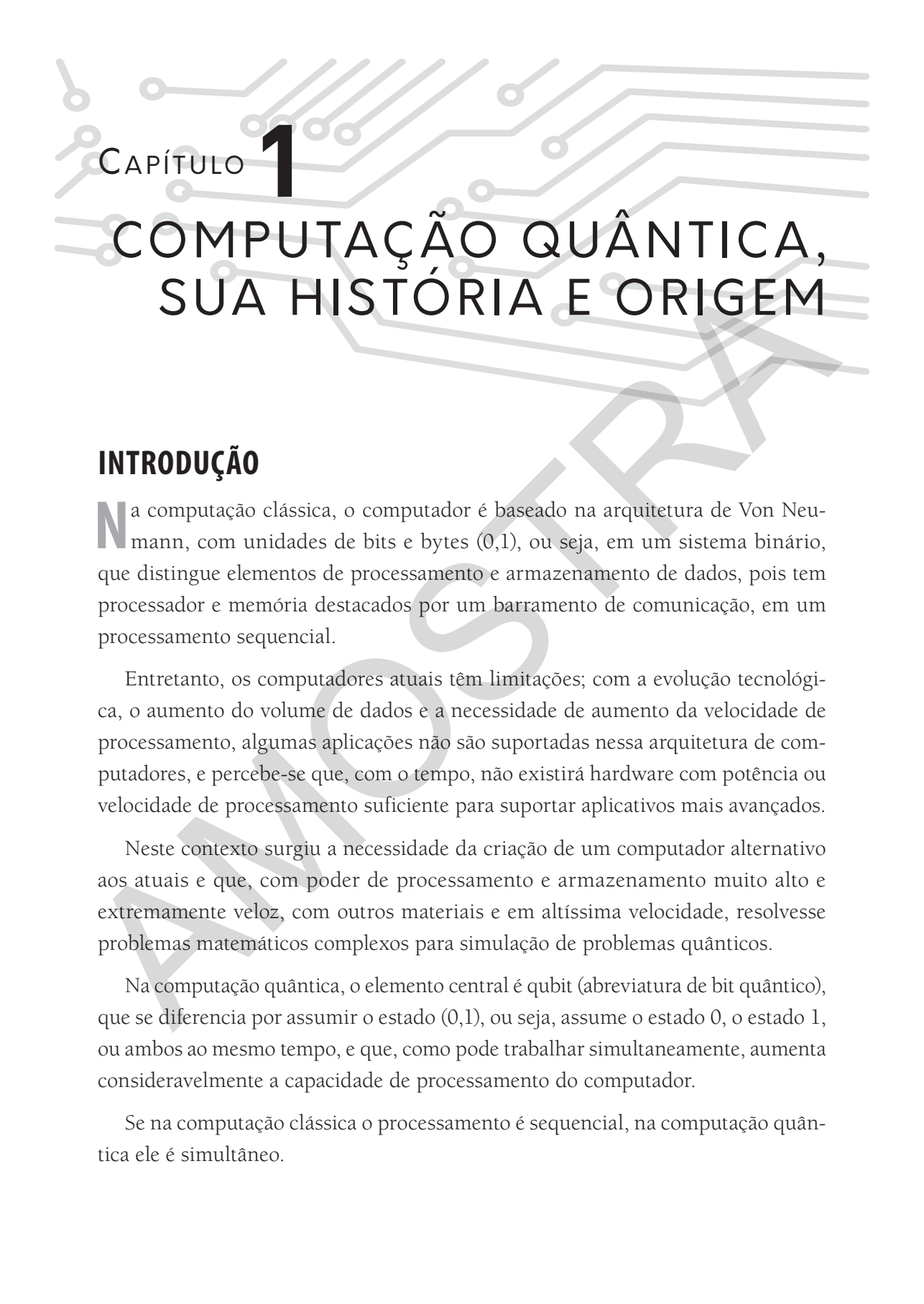
A REALIDADE DE UMA NOVA ERA



ALTA BOOKS
EDITORA
Rio de Janeiro, 2020

SUMÁRIO

Introdução	1
CAPÍTULO 1: Computação Quântica, Sua História e Origem	3
CAPÍTULO 2: O Maravilhoso Mundo da Física Quântica e o Computador do Futuro	7
CAPÍTULO 3: A Presença da Realidade Quântica e Seus Reflexos na Filosofia	49
CAPÍTULO 4: Pesquisas Aplicadas, Tecnologia e Fabricantes	63
CAPÍTULO 5: Desafios e Perspectivas da Comunicação Quântica	103
CAPÍTULO 6: Como Preparar um Computador Dedicado para Tarefas de Cálculo Científico e Simulação Quântica	137
CAPÍTULO 7: O Ruído do Universo e Números Perfeitamente Aleatórios	253
CAPÍTULO 8: A Harmonia do Universo	279
CAPÍTULO 9: Fatos e Enigmas sobre a Computação Quântica	283
Conclusão	297
Referências	299
Lista de Siglas, Acrônimos e Nomes	315
Anexo A – Tabelas e Equações	323
Índice	327



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.

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.

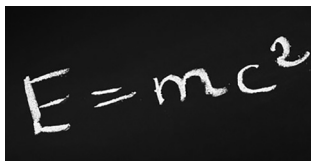

$$E=mc^2$$

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.

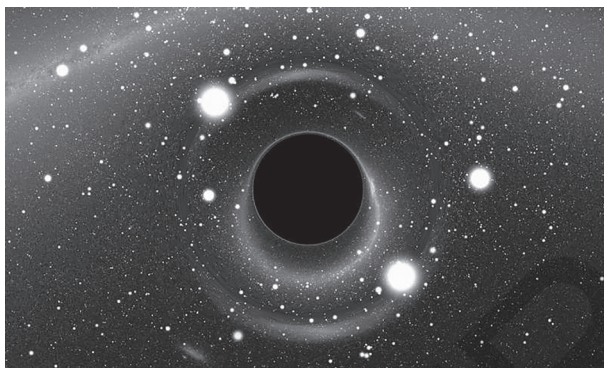


FIGURA 4: Modelo conceitual de um buraco negro rotativo

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.

Buraco Negro



Buraco Branco

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-intermediate 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 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.