

Computação Quântica e o Ano Internacional da Ciência e Tecnologia Quânticas

Quantum Computing and the International Year of Quantum Science and Technology

Caio M. Porto,^a  Nelson H. Morgon^{a,*} 

^a Universidade Estadual de Campinas,
Instituto de Química, Departamento de
Físico-Química, Campinas-SP, CEP
13083-970, Brasil

*E-mail: nhmorgon@unicamp.br

Submissão: 24 de Julho de 2025

Aceite: 12 de Dezembro de 2025

Publicado online: 18 de Dezembro de 2025

Quantum computing represents one of the most promising frontiers in contemporary science and technology, built upon the counterintuitive and fascinating principles of quantum mechanics. While classical computers process information using bits that take on definitive values of 0 or 1, quantum computers leverage the unique properties of quantum systems—such as superposition, entanglement, and interference - to manipulate qubits that can simultaneously exist in multiple states. The theoretical advancements in quantum mechanics, developed throughout the 20th century, laid the conceptual groundwork necessary to envision and subsequently build computational devices that operate according to these fundamental principles of nature. From the earliest discoveries about the dual nature of light to the modern implementations of quantum algorithms, this journey reveals how a deep understanding of quantum physics paved the way for a computational revolution. This revolution promises to transform fields like cryptography, molecular simulation, optimization, and artificial intelligence.

Keywords: Mecânica quântica; bits - qubits; computação quântica.

1. Introdução

A trajetória histórica da computação quântica revela uma evolução fascinante desde descobertas fundamentais da compreensão dos fenômenos microscópicos até implementações tecnológicas concretas que prometem revolucionar a computação. Os avanços da mecânica quântica forneceram não apenas a base conceitual necessária, mas também as ferramentas matemáticas e as percepções profundas e claras que tornaram possível imaginar e posteriormente construir dispositivos computacionais que operam segundo princípios quânticos.¹ Esta jornada continua a acelerar, com desenvolvimentos recentes em correção de erros quânticos, algoritmos híbridos e aplicações em otimização, simulação molecular e criptografia, sugerindo que estamos no limiar de uma nova era computacional fundamentalmente diferente e potencialmente transformadora. A mecânica quântica, nascida no início do século XX, revolucionou profundamente nossa compreensão do universo em escalas subatômicas. Conceitos radicalmente contra-intuitivos, como por exemplo: a superposição (a capacidade de uma partícula existir em múltiplos estados simultaneamente) ou o entrelaçamento quântico (uma conexão instantânea entre partículas que persiste mesmo à distância), desafiaram as noções clássicas de realidade. Embora inicialmente focada em explicar fenômenos atômicos e subatômicos, a profundidade e o poder desses princípios logo sugeriram aplicações além da física fundamental.²

Foi a percepção visionária de Richard Feynman, numa palestra no MIT em 1981, onde ele propôs a simulação de sistemas quânticos com outros sistemas quânticos, essencialmente lançando a ideia de um “simulador quântico”. Em 1982 explicitamente apontou para a necessidade de computadores baseados nessas leis quânticas para simular eficientemente sistemas quânticos complexos – uma tarefa proibitivamente difícil para computadores clássicos.¹ Esta percepção marcou o nascimento conceitual da computação quântica, um campo que promete revolucionar áreas como criptografia, descoberta de materiais e inteligência artificial ao aproveitar o paralelismo inerente e as correlações únicas oferecidas pelo mundo quântico.³

A linha do tempo abaixo traça os marcos cruciais, desde os fundamentos teóricos até os avanços práticos recentes, que pavimentaram o caminho para esta tecnologia transformadora.

1.1. Ascensão dos fundamentos quânticos (1900-1965)

- **1900:** *Max Planck*, físico alemão considerado o pai da mecânica quântica, introduz

o conceito revolucionário de quantização da energia na interpretação da radiação emitida por objetos aquecidos, onde a energia não era emitida ou absorvida de forma contínua, mas sim em pacotes discretos, ou “quanta”, proporcional à sua frequência.⁴⁻⁶

- **1905:** *Albert Einstein* explica o efeito fotoelétrico, propondo que a luz seja quantizada em partículas discretas de energia, os fótons. Este trabalho valida as observações de Planck lançando as bases para a teoria quântica.⁴

- **1924:** *Louis de Broglie* propõe o conceito da dualidade onda-partícula para a matéria, expandindo a ideia de Einstein de que a luz (que classicamente era vista como onda) também poderia se comportar como partícula (fóton). Max Born cunha pela primeira vez o termo “mecânica quântica” (*Quantenmechanik*) para descrever a nova física emergente que explicava o comportamento do mundo atômico.⁴

- **1925:** *Werner Heisenberg*, juntamente com Max Born e Pascual Jordan, formula a mecânica matricial, a primeira versão completa e matematicamente consistente da mecânica quântica, descrevendo sistemas físicos através de matrizes.⁷

- **1926:** *Erwin Schrödinger*, considerado o pai da mecânica ondulatória, oferece uma descrição alternativa à mecânica matricial de Heisenberg para o comportamento dos sistemas quânticos. Sua contribuição mais famosa e crucial foi a Equação de Schrödinger, publicada em uma série de artigos.⁸

- **1925-1927:** *Niels Bohr* e *Werner Heisenberg* desenvolvem a interpretação de Copenhague. Esta visão dominante enfatiza a natureza probabilística da mecânica quântica, a importância do ato de medição (que “colapsa” a função de onda) e o princípio da complementaridade, tornando-se o paradigma padrão por décadas.^{9,10}

- **1930:** *Paul Dirac* publica *The Principles of Quantum Mechanics*, uma obra monumental que unifica a mecânica matricial e a mecânica ondulatória de Schrödinger em uma estrutura teórica elegante e poderosa, introduzindo a notação de *bra-ket* e tratando de forma consistente a relatividade e a teoria quântica. Permanece um texto fundamental.¹¹

- **1935:** *Albert Einstein*, *Boris Podolsky* e *Nathan Rosen* (EPR) publicam seu famoso artigo de desafio, argumentando que a mecânica quântica, devido às suas previsões de entrelaçamento (correlações instantâneas à distância), deve ser incompleta. Eles propuseram a existência de “variáveis ocultas” locais para restaurar o realismo e a localidade.²

- **1935:** Em resposta ao paradoxo EPR, *Erwin Schrödinger* desenvolve o célebre experimento mental do gato de Schrödinger, ilustrando dramaticamente o conceito de superposição quântica (o gato está simultaneamente vivo e morto) e formaliza o termo “entrelaçamento quântico” (*Verschränkung*).¹²

- **1944:** *John von Neumann* publica *Mathematical Foundations of Quantum Mechanics*, estabelecendo um arcabouço matemático rigoroso e abstrato para a teoria, incluindo a teoria de operadores em espaços de Hilbert e o postulado do colapso da função de onda. Sua estrutura

tornou-se essencial para a formalização posterior da computação quântica.¹³

- **1957:** *Hugh Everett III* propõe a radical interpretação de muitos mundos (MWI). Contrária à de Copenhague, a MWI sugere que todas as possibilidades contidas na superposição quântica realmente ocorrem, mas em ramos separados e não comunicantes de um universo que se ramifica constantemente. Oferece uma visão determinística sem colapso da função de onda.¹⁴

- **1961:** *Rolf Landauer* demonstra uma conexão fundamental entre informação e termodinâmica: O Princípio de Landauer. Ele prova que apagar um bit de informação clássica dissipa uma quantidade mínima de energia ($kT \ln 2$), estabelecendo um limite físico para a eficiência energética da computação clássica e sugerindo que a reversibilidade é crucial para a computação de baixo consumo.¹⁵

- **1965:** *John Stewart Bell* formula e prova o Teorema de Bell. Ele demonstra matematicamente que nenhuma teoria de variáveis ocultas locais pode reproduzir todas as previsões da mecânica quântica, particularmente as correlações fortes previstas pelo entrelaçamento. O teorema forneceu uma receita experimental (as desigualdades de Bell) para testar a natureza não-local da mecânica quântica contra teorias locais realistas.¹⁶

1.2. Semeando as sementes da Computação Quântica (1973-1991)¹⁷

- **1973:** *Alexander Holevo* estabelece um limite fundamental na capacidade de informação dos sistemas quânticos: o Teorema de Holevo (ou Limite de Holevo). Ele prova que n qubits (bits quânticos) não podem transmitir mais do que n bits clássicos de informação, apesar de seu vasto espaço de estados. Este resultado é crucial para entender o poder e também as limitações da comunicação quântica.¹⁸

- **1980:** *Paul Benioff* propõe o primeiro modelo teórico explícito de uma Máquina de Turing Quântica, demonstrando que era possível, em princípio, construir um computador cujas operações fossem governadas pelas leis da mecânica quântica, mantendo a reversibilidade e evitando a dissipação de calor prevista por Landauer para operações irreversíveis.¹⁹

- **1981:** Em uma palestra seminal, *Richard Feynman* argumenta que simular sistemas quânticos complexos em computadores clássicos é intrinsecamente ineficiente (“a natureza não é clássica, caramba!”). Ele propõe explicitamente a construção de um computador quântico como a única maneira eficaz de simular a natureza, lançando assim o desafio fundamental que impulsiona o campo.¹

- **1982:** *David Deutsch* generaliza o modelo de Benioff e formula o conceito de um Computador Quântico Universal. Ele demonstra que tal máquina poderia simular qualquer outro sistema físico com eficiência, estabelecendo a computação quântica como um paradigma computacional fundamentalmente novo e poderoso.²⁰

- **1984:** *Charles Bennett* e *Gilles Brassard* inventam o BB84, o primeiro protocolo prático de Distribuição Quântica de Chaves (QKD). Ele permite que duas partes (Alice e Bob) gerem uma chave secreta compartilhada e provavelmente segura, cuja segurança é garantida pelas leis fundamentais da física quântica (princípio da incerteza e teorema da não-clonagem), detectando qualquer tentativa de espionagem (Eva).²¹

- **1985:** *David Deutsch* e *Richard Jozsa* desenvolvem o algoritmo de Deutsch-Jozsa. Embora resolva um problema artificial, este algoritmo demonstra provavelmente pela primeira vez uma vantagem quântica exponencial sobre os melhores algoritmos clássicos para uma classe específica de problemas, ilustrando o poder do paralelismo quântico.²²

- **1991:** *Artur Ekert* propõe um protocolo alternativo de QKD, o E91, baseado especificamente na violação das Desigualdades de Bell por pares de partículas entrelaçadas. A segurança aqui está diretamente ligada à presença e detecção do entrelaçamento.²³

1.3. Aceleração Quântica: algoritmos e implementações (1992-2007)¹⁷

- **1992:** *David Deutsch* e *Richard Jozsa* refinam seu algoritmo, apresentando formalmente a versão generalizada para múltiplas entradas, consolidando o Algoritmo de Deutsch-Jozsa como um marco conceitual.²²

- **1994:** *Peter Shor* descobre o revolucionário algoritmo de Shor. Ele demonstra como um computador quântico poderia fatorar números inteiros grandes em tempo polinomial, uma tarefa para a qual não se conhece algoritmo clássico eficiente. Isso ameaça diretamente a segurança do amplamente utilizado sistema de criptografia RSA, catapultando a computação quântica para o centro das atenções da segurança da informação e do financiamento de pesquisa.²⁴

- **1996:** *Lov Grover* inventa o algoritmo de Grover. Este algoritmo fornece uma vantagem quadrática para buscas em bancos de dados não estruturados, encontrando um item específico entre N itens com apenas $O(\sqrt{N})$ consultas, em contraste com $O(N)$ consultas no caso clássico. Tem aplicações amplas em problemas de busca e otimização.²⁵

- **1997:** *Isaac Chuang*, *Neil Gershenfeld* e *Mark Kubinec* realizam a primeira implementação experimental do algoritmo de Shor (fatorando o número 15) usando uma técnica de Ressonância Magnética Nuclear (RMN) em moléculas líquidas. Esta prova de conceito crucial demonstrou a viabilidade prática de executar algoritmos quânticos complexos, embora em escalas minúsculas.^{26,27}

- **1998:** Pesquisadores da IBM implementam o algoritmo de Grover usando RMN, encontrando uma solução em um espaço de busca com 4 elementos usando apenas uma consulta, demonstrando a vantagem quântica prevista por Grover em um experimento controlado, embora modesto.²⁶

- **2000:** *David DiVincenzo* estabelece os Critérios de DiVincenzo, uma lista de cinco requisitos físicos essenciais para a realização de um computador quântico prático: 1) sistema físico escalonável com qubits bem caracterizados; 2) capacidade de inicializar os estados dos qubits; 3) tempos de coerência quântica suficientemente longos; 4) conjunto universal de portas quânticas e 5) capacidade de medir qubits específicos. Estes critérios continuam a guiar o projeto de hardware quântico.²⁸

- **2007:** A empresa D-Wave Systems anuncia o que afirma ser o primeiro computador quântico comercial, baseado em quantum annealing (*annealing* quântico). Sua natureza e capacidade de resolver problemas práticos de otimização de maneira genuinamente quântica e vantajosa permanecem objeto de intenso debate e ceticismo na comunidade científica por vários anos. Enquanto o computador quântico foi anunciado em 2007, o artigo que demonstra a possibilidade de se utilizar um único átomo como qubit, provando que as características essenciais, como ser capaz de receber e recriar o qubit fotônico por exemplo, foram atingidas.²⁹

1.4. Da supremacia à escalabilidade (2019-presente)

- **2019:** A empresa Google, utilizando seu processador Sycamore de 53 qubits, anuncia ter alcançado a supremacia quântica. Eles afirmaram que seu processador executou uma tarefa específica de amostragem aleatória (verificar a saída de um circuito quântico aleatório) em aproximadamente 200 segundos, uma tarefa que levaria milhares de anos no supercomputador clássico mais avançado da época (Summit). Este marco, embora sobre uma tarefa artificial, demonstrou pela primeira vez que, um cálculo inalcançável pela computação clássica seria possível, dentro de um tempo razoável, utilizando computação quântica.³⁰

- **2020:** A empresa IBM responde ao marco do Google, demonstrando que a mesma simulação pode ser realizada em menos de três dias com fidelidade muito maior. A IBM também enfatizou seu roteiro de desenvolvimento contínuo e foco na escalabilidade e correção de erros, elementos críticos para a computação quântica prática.³¹

- **Dias atuais:** Hoje os computadores quânticos não são mais meras construções teóricas. Sistemas com centenas de qubits físicos operam em laboratórios e via nuvem (IBM Quantum, Azure Quantum, ...), enquanto máquinas tolerantes a falhas são o Santo Graal da indústria. Embora desafios de coerência quântica e correção de erros persistam, já se comprovou que algoritmos como o de Shor (fatoração) e Grover (busca) superaram radicalmente os limites clássicos. São vários os avanços recentes em plataformas quânticas: a) qubits supercondutores (IBM, Google) - sistemas em criogenia profunda (15 mK); b) íons aprisionados (Quantinuum) - átomos individuais controlados por laser e c) pontos quânticos (Intel) - "átomos artificiais" em semicondutores.^{32,33}

2. Metodologia Teórica

A Revolução Quântica - do Bit ao Qubit: Na computação clássica, o bit representa o alicerce fundamental de todo processamento de informação. Como unidade elementar de dados, um bit existe em um de dois estados mutuamente exclusivos - convencionalmente representados como 0 e 1. Esta dualidade binária espelha a natureza dos sistemas físicos que implementam a computação tradicional. Por exemplo, em circuitos elétricos, o 0 corresponde a baixa tensão (tipicamente 0V) e o 1 a alta tensão (como +5V em sistemas históricos ou valores menores em tecnologias modernas).^{34,35} Este paradigma binário, embora extraordinariamente bem-sucedido na revolução digital, opera sob uma limitação fundamental: cada bit sempre existe em um estado definido e único a qualquer momento. Um bit de memória RAM ou um transistor em um CPU é inequivocamente 0 ou 1, sem ambiguidade ou sobreposição possível. Toda a complexidade computacional emerge da combinação sequencial destas unidades discretas através de operações lógicas booleanas (AND, OR, NOT). A Tabela 1 apresenta a relação fundamental entre a quantidade de estados discerníveis e os bits necessários para codificá-los em um sistema clássico de informação. Esta relação é exponencial e determinística, sendo a base de toda a computação e comunicação digital como a conhecemos. Partindo do princípio de que um bit é uma unidade binária que pode assumir apenas um de dois estados (0 ou 1), observa-se que com 2 bits é possível representar exatamente 4 configurações únicas, como 00, 01, 10 e 11. Da mesma forma, ao adicionar mais um bit, elevando o total para 3, a capacidade de representação salta para 8 estados distintos, que vão de 000 a 111. Este padrão é regido pela fórmula $m = 2^n$, onde 'm' é o número total de estados e 'n' é o número de bits. Este comportamento exponencial significa que cada bit adicional dobra o espaço de estados disponível, permitindo que uma quantidade relativamente pequena de bits represente uma vasta gama de informações, sendo este o princípio que rege a codificação de tudo, desde textos simples até imagens complexas, em qualquer dispositivo computacional clássico.^{34,35}

Tabela 1. Relação entre a quantidade de estados e bits necessários para codificar informações em sistemas clássicos e quânticos

| Estados (m) | Bits (n) | Exemplo (binário) |
|-------------|----------|-------------------------|
| 4 | 2 | 00, 01, 10, 11 |
| 8 | 3 | 000, 001, 010, ..., 111 |

A computação quântica introduz uma unidade fundamental radicalmente nova - o qubit (*quantum bit*). Superficialmente, o qubit mantém uma semelhança formal com seu predecessor clássico - também possui dois estados de base, denotados na notação de Dirac como $|0\rangle$ e $|1\rangle$. Porém, esta aparente simplicidade esconde uma natureza profundamente diferente regida pelas leis da mecânica

quântica. Três propriedades quânticas fundamentais distinguem o qubit do bit tradicional:

- 1) *Superposição Quântica* - enquanto um bit clássico é sempre 0 ou 1, um qubit pode existir em uma combinação coerente simultânea de ambos os estados:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

onde α e β são amplitudes complexas (satisfazendo $|\alpha|^2 + |\beta|^2 = 1$) que representam probabilidades. Fisicamente, isto pode ser implementado por elétrons com spins em superposição ou átomos em múltiplos níveis energéticos simultâneos. Consequência computacional: um único qubit contém informação contínua (as amplitudes), enquanto n qubits podem representar 2^n estados simultaneamente.

- 2) *Emaranhamento Quântico* - qubits podem se correlacionar de formas impossíveis classicamente. Quando emaranhados, o estado de múltiplos qubits tornam-se interdependentes:

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (2)$$

Medir um qubit (obtendo 0 ou 1) determina instantaneamente o estado do outro, mesmo a distâncias cósmicas. Esta correlação não-local viola a intuição clássica.

- 3) *Interferência Quântica* - operações aplicadas a qubits (portas quânticas) manipulam as fases relativas das amplitudes. Por exemplo, a porta quântica Hadamard é um operador unitário no espaço de Hilbert das funções de base $|0\rangle$ e $|1\rangle$, e pode ser escrita como:

$$\hat{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \quad (3)$$

Sua ação sobre os vetores da base computacional é a de transformar as bases ou numa superposição de igual probabilidade de ambos os estados:

$$\hat{H}|0\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \hat{H}|1\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (4)$$

Seu uso frequente se dá pois permite criar interferência construtiva (reforçando estados desejados) e destrutiva (suprimindo estados indesejados), possibilitando otimizações algorítmicas impossíveis classicamente. Esta natureza radicalmente diferente habilita novos paradigmas computacionais trazendo vantagens quânticas. Enquanto um computador clássico com n bits processa uma configuração por vez, um sistema com n qubits processa 2^n configurações simultaneamente. Por exemplo: 50 qubits representam mais estados ($1,125 \times 10^{15}$) que o número de grãos de areia na Terra. No entanto, a implementação prática enfrenta obstáculos significativos como os descritos na Tabela 2.

Tabela 2. Principais desafios na computação quântica³⁶

| Desafio | Descrição |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Decoerência | Qubits perdem informação ao interagir com o ambiente (tipicamente em microssegundos) |
| Correção de Erros | Requer redundância quântica (≈10 a 100 e 100 a 1,000 qubits físicos por qubit lógico, para qubits supercondutores e íons aprisionados respectivamente) |
| Controle de Precisão | Operações exigem acurácia extrema (erros < 10 ⁻⁴) |

De um modo geral, o qubit não é meramente uma evolução tecnológica, mas uma revolução conceitual que redefine a própria natureza da informação e computação. Enquanto o bit reflete uma visão determinística e discreta do mundo, o qubit incorpora a essência probabilística e contínua da realidade quântica. Esta transição do binário absoluto para o espectro probabilístico representa não apenas um salto computacional, mas uma transformação epistemológica que ressignifica nossa compreensão de informação, causalidade e realidade física. O ato de medição em sistemas quânticos constitui uma interação física irreversível que projeta o estado quântico original em um autoestado do operador medido, destrói superposições quânticas relacionadas ao observável e introduz uma assimetria temporal fundamental na evolução do sistema. Na Tabela 3 observa-se uma comparação entre medições clássicas e quânticas.

A análise dos processos de medição em mecânica quântica revela uma divergência radical em relação à física clássica, estabelecendo novos princípios fundamentais para a compreensão da realidade física. Enquanto sistemas clássicos possuem propriedades definidas independentemente da medição, expressas como funções determinísticas do estado físico, sistemas quânticos exibem uma natureza profundamente diferente manifestada através das relações de incerteza ($\Delta x \cdot \Delta p \geq \hbar/2$) e de comutação ($[\hat{x}, \hat{p}] = i\hbar$), onde observáveis complementares não podem ser simultaneamente bem-definidos. Na computação quântica, a natureza delicada do estado durante a medição exige algoritmos que protejam as superposições durante o processamento, enquanto extraem resultados úteis através de interferência construtiva. Sensores quânticos de última geração exploram precisamente a sensibilidade do colapso quântico para detectar variações mínimas em campos magnéticos, forças gravitacionais e outras grandezas físicas com precisão fundamental.^{34,35,38,39}

3. Resultados e Discussão

3.1. A Computação Quântica e a Química

Computadores quânticos, que aproveitam propriedades como superposição, interferência e emaranhamento de bits quânticos, prometem superar os computadores clássicos na resolução de diversas classes de problemas complexos. Na química, o desenvolvimento de algoritmos quânticos é particularmente promissor para resolver desafios atualmente intratáveis, como cálculos de estrutura eletrônica, dinâmica quântica, espectroscopia e quimioinformática. Apesar do grande potencial, a implementação física de computadores quânticos ainda está em fase inicial e ainda não superou os computadores clássicos em tarefas úteis. No entanto, o desenvolvimento de software quântico para aplicações químicas é uma área de pesquisa extremamente ativa. Esta análise resume o progresso recente em algoritmos, hardware e software de computação quântica e discute os desafios restantes para implementações práticas na química.³³

3.2. Estado atual da Computação Quântica no Brasil

A ONU declarou 2025 como o Ano Internacional da Ciência e Tecnologia Quânticas, o que coloca essa área em destaque global. Segundo dados do IDC (*International Data Corporation*), os investimentos no mercado de computação quântica devem atingir cerca de US\$ 16,4 bilhões até o final de 2027, demonstrando a magnitude econômica desta revolução tecnológica.⁴⁰ Este contexto internacional evidencia a urgência para que países como o Brasil estabeleçam estratégias robustas para não ficarem à margem desta transformação tecnológica fundamental. Iniciativas de apoio institucional têm aparecido, mesmo que ainda timidamente. Merece destaque o fato de que durante a 5ª Conferência Nacional de Ciência, Tecnologia e Inovação,

Tabela 3. Comparação entre medições clássicas e quânticas.³⁷

| Aspecto | Mecânica Clássica | Mecânica Quântica |
|-------------------|---------------------------------|-----------------------------------|
| Efeito da medição | Não altera o estado do sistema | Altera irreversivelmente o estado |
| Previsibilidade | Determinística | Probabilística |
| Reversibilidade | Processo reversível | Colapso irreversível |
| Exemplo | Medir temperatura de um líquido | Medir spin de um elétron |

especialistas brasileiros reivindicaram infraestrutura compatível com o potencial nacional, destacando que o país acumula 25 anos de pesquisa consolidada na área de tecnologias quânticas. O Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) aprovou projetos específicos de “Pesquisa e Desenvolvimento em Computação Quântica”, estabelecendo parceria estratégica entre universidades brasileiras, demonstrando o reconhecimento institucional da importância desta área. Em 2024 a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) lançou um programa abrangente de pesquisa para promover o progresso das tecnologias quânticas, com objetivos múltiplos visando: impulsionar o desenvolvimento de startups especializadas, atrair investimentos globais para o ecossistema paulista, trazer talentos internacionais para São Paulo, bem como fortalecer a base de pesquisa existente. Criação do Laboratório de Tecnologias Quânticas do CBPF em 2025 com investimento de R\$ 30 milhões e do Centro de Competência em Tecnologias Quânticas (Embrapii) com foco em comunicação quântica, com investimento inicial de R\$ 60 milhões. Essas são algumas iniciativas promissoras, mas há muito a se fazer. Por exemplo, na Tabela 4 tem-se uma comparação dos investimentos de alguns países selecionados.⁴¹

O Brasil está teoricamente bem posicionado no cenário da computação quântica, com uma base de pesquisa sólida e reconhecida internacionalmente. No entanto, para não ficar para trás na corrida quântica global que se intensifica rapidamente, o país precisa: aumentar significativamente os recursos destinados à infraestrutura quântica, estabelecer colaborações estratégicas com líderes internacionais, expandir programas de formação em todos os níveis educacionais, facilitar a transferência de tecnologia para aplicações comerciais e criar marcos regulatórios e incentivos específicos para o setor. A janela de oportunidade para o Brasil se estabelecer como um player relevante na computação quântica ainda está aberta, mas requer ação coordenada e investimentos estratégicos imediatos. O sucesso nesta área pode posicionar o país como líder tecnológico em setores estratégicos como agronegócio, energia e segurança cibernética.

3.3. A Computação Quântica em Química

As áreas de química teórica, química computacional, quimioinformática e aprendizagem de máquina aplicada

à química, são as principais e diretamente as que mais se beneficiarão do aumento da capacidade de computação prometidos pela computação quântica, tanto por lidarem com sistemas quânticos complexos, como pelo aprimoramento de algoritmos clássicos como aprendizagem de máquina e otimização. No caso da química quântica, tem-se a promessa da simulação eficiente de funções de onda de forma que sistemas maiores e/ou altamente correlacionados possam ser modelados com precisão.³⁵

Atualmente, estamos na era da computação quântica conhecida como NISQ (*Noisy Intermediate-Scale Quantum*), que significa computadores quânticos de escala intermediária e com erros.⁴³ Essa definição é utilizada para o período de tempo em que os computadores quânticos apresentam até alguns milhares de qubits, o que permite a aplicação e estudo de circuitos não triviais e que tem o poder de demonstrar a vantagem quântica, que apresentam uma quantidade de ruído significativa a ponto de limitar a quantidade de portas que podem ser utilizadas num determinado circuito (profundidade do circuito) e que são propensos a decoerência. Além disso, não possuem ainda a capacidade contínua de correção de erros.

Atualmente o algoritmo que apresenta a maior potencialidade de implementação e utilização é o algoritmo quântico variacional (*Variational Quantum Eigensolver - VQE*),⁴⁴ que utiliza o princípio variacional para cálculos de estrutura eletrônica de átomos e moléculas. Este é um algoritmo híbrido quântico-clássico, no qual o computador quântico é utilizado com um circuito parametrizado que é minimizado através de um otimizador no computador clássico. Ele tem como vantagem produzir circuitos mais rasos, ou seja, com menor quantidade de *gates*, de forma que podem estar mais próximos do tempo de decoerência dos computadores quânticos atuais. Além disso, algoritmos variacionais apresentam uma certa tolerância ao ruído, devido ao fato de que o otimizador pode aprender ou adaptar os parâmetros do circuito de forma a reduzir o ruído.⁴⁵

Dois pontos devem ser resolvidos para que cálculos de estrutura eletrônica possam ser realizados utilizando o VQE: o mapeamento do problema fermiônico nos qubits e a parametrização do circuito. Atualmente existem diversas estratégias para o mapeamento, as quais podem utilizar simetria, paridade, redução no número de Pauli *strings*, entre outras, de forma a facilitar a resolução do problema. O mapeamento mais simples é o de Jordan-Wigner, o qual considera cada qubit como um spin-orbital do sistema

Tabela 4. Investimentos globais em tecnologias quânticas (em 2025).⁴²

| País | Investimento (US\$) | Foco Principal |
|-------------|---------------------|-----------------------------------------------------------------------|
| Brasil | 16 mi | Infraestrutura e recursos humanos. |
| China | 15,3 bi | Sensores, comunicação e computação |
| Reino Unido | 4,7 bi | Estratégia nacional integrada |
| Canadá | 1,9 bi | Pesquisa básica e aplicada |
| EUA | 7,7 bi | Liderança tecnológica, segurança nacional e competitividade econômica |

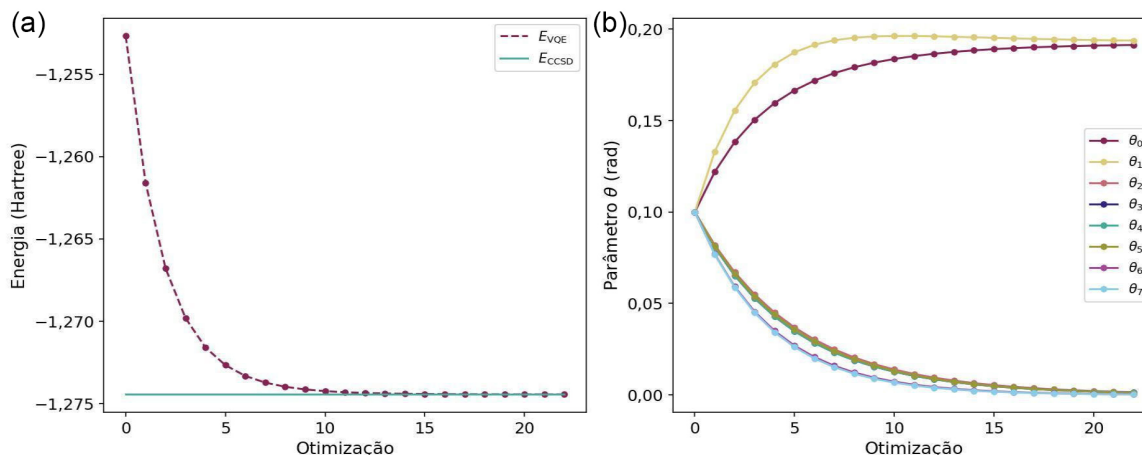


Figura 1. Curva (a) da energia em relação ao passo da otimização, mostrada em relação à energia calculada através do computador clássico, e (b) dos parâmetros das portas do circuito durante a otimização

a ser estudado, e os inicializa em $|1\rangle$ ou $|0\rangle$, caso estes spin-orbitais estejam ocupados ou não, respectivamente. No caso da parametrização do circuito, esta pode ser relativamente simples, como no caso do *ansatz* eficiente para *hardware* (HEA).⁴⁶ No entanto, este é genérico ao extremo, o que pode necessitar uma quantidade muito grande de camadas de forma que o mínimo desejado se encontre no espaço gerado pelo circuito, no limite sendo o espaço de Hilbert completo. Por isso, a parametrização é em geral construída de forma a ser inspirada em métodos de química quântica como o *coupled cluster* (CC). A versão unitária do CC,⁴⁷ que não é utilizada de forma geral em computadores clássicos devido a seu alto custo computacional, tem a vantagem de ser variacional e poder ser implementada no *hardware* quântico através de matrizes de Pauli. Outra vantagem é que o método CC, especialmente com excitações simples, duplas e triplas iterativas, apresenta uma excelente precisão. Devido a essas vantagens, o método CC unitário com excitações simples e duplas (UCCSD) e suas variações são métodos com ampla utilização em computação quântica.⁴⁸

Como exemplo da utilização atual de computadores quânticos, será mostrado o cálculo da energia da molécula de H_3^+ através do método VQE, utilizando o *ansatz* UCCSD, com função de base mínima STO-3G e mapeamento Jordan-Wigner. Apesar de existirem computadores quânticos com centenas até pouco mais de mil qubits, a simulação de sistemas maiores tem como limitação o ruído e a profundidade do circuito.³⁴ No caso de simulações, o limite é o custo computacional elevado de se simular qubits em computadores clássicos. O sistema foi estudado utilizando o pacote PennyLane⁴⁹ e os simuladores de computadores quânticos presentes neste pacote. Não foram adicionados ruídos de forma a simplificar a apresentação, no entanto, estes podem ser simulados através de calibrações de computadores quânticos reais. A Figura 1 mostra os resultados para energia em relação ao passo da otimização. Apesar da energia iniciar alta, pode-se ver que o resultado final tem excelente concordância com o valor calculado

no computador clássico, sendo o erro da ordem de 10^{-6} . Também se pode notar que dois parâmetros tendem a aproximadamente 0,19 rad enquanto os outros tendem a zero. Igualmente, tem-se que o estado final, retirando os estados cujas amplitudes eram menores que 10^{-3} , para os qubits foi:

$$|\psi\rangle = -0,096|000011\rangle - 0,96|001100\rangle + 0,991|110000\rangle \quad (5)$$

o qual demonstra que a função de onda é composta principalmente pelos qubits no estado fundamental ($|110000\rangle$), junto com uma contribuição das excitações duplas ($|000011\rangle$ e $|001100\rangle$).

Em seguida, foi realizada a otimização da molécula, partindo da estrutura distorcida de forma a aumentar a distância entre os átomos (Figura 2). Uma vantagem da utilização do VQE é que tanto as distâncias interatômicas quanto os parâmetros do circuito podem ser otimizados simultaneamente.

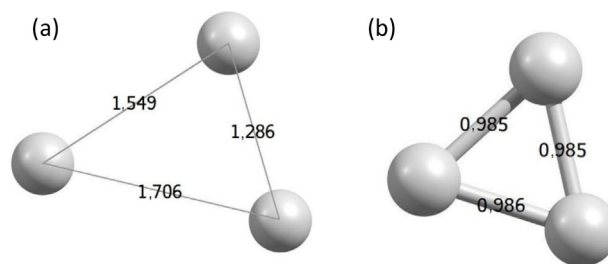


Figura 2. Estrutura para a molécula de H_3^+ (a) antes da otimização, e (b) após ser otimizada, com distâncias de ligação em Å

A Figura 3 apresenta os resultados para a otimização. Pode-se notar que, na ausência de ruído, o otimizador consegue diminuir a variação na energia entre passos da otimização até valores menores que 0,005 mEh e de gradiente menor que 0,004 Eh/bohr. As distâncias de ligação obtidas também estavam em excelente concordância com os resultados obtidos classicamente. Tais resultados, bem como a implementação relativamente direta dos métodos

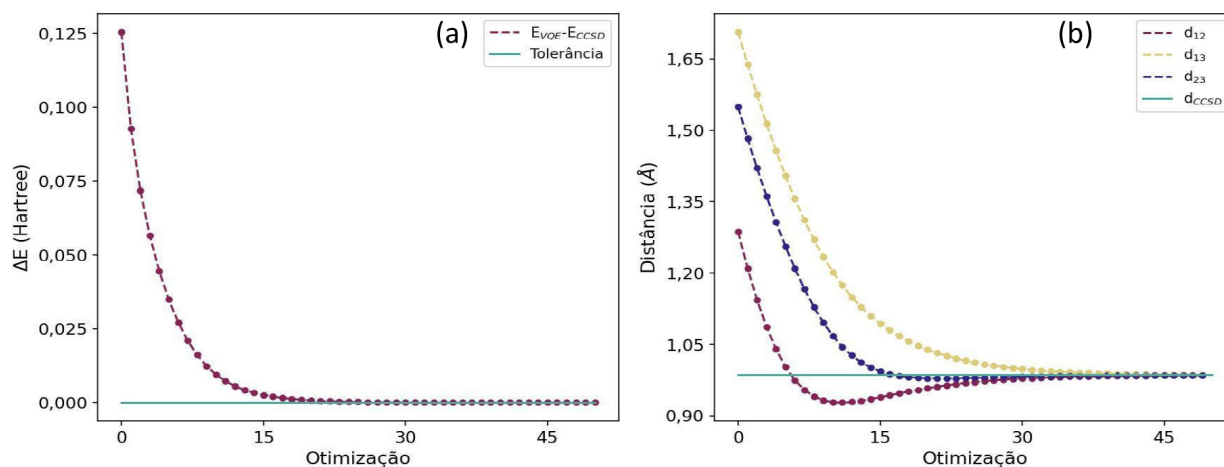


Figura 3. Gráficos da (a) diferença entre a energia calculada através do computador clássico e a energia do VQE, e (b) das distâncias interatômicas, em Å, em relação ao passo da otimização

e algoritmos utilizados, mostram o quanto a computação quântica avançou em pouco tempo, não apenas na construção de hardwares maiores e mais resilientes a ruído, mas também no desenvolvimento de pacotes, algoritmos e estratégias para a utilização destes *hardwares*.

4. Conclusões

A computação quântica (CQ) é uma fronteira tecnológica promissora, baseada nos fascinantes princípios da mecânica quântica, como superposição e emaranhamento. Ao contrário dos computadores clássicos, que usam bits 0 ou 1, os computadores quânticos manipulam qubits, que podem existir em múltiplos estados simultaneamente. O século XX forneceu a base teórica para essa revolução, que promete transformar áreas como criptografia, simulação molecular, otimização e inteligência artificial. Neste trabalho aplicaram-se os princípios da CQ na simulação ilustrativa do cálculo da energia da molécula de H_3^+ utilizando o método VQE com o *ansatz* UCCSD, conjunto de funções de base mínima STO-3G e mapeamento Jordan-Wigner. Esses resultados mostram uma excelente concordância com os cálculos clássicos, apesar das limitações dos computadores quânticos atuais. Isso demonstra o potencial da tecnologia, mesmo enquanto a pesquisa continua a superar os obstáculos para sistemas maiores e mais robustos.

Agradecimentos

Os autores gostariam de agradecer ao Instituto de Química da UNICAMP, ao Conselho Nacional de Desenvolvimento Científico (CNPq) (310665/2021-3), à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) (2019/18445-5 e 2021/11039-1) e à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES - Código de Financiamento 001) pelo apoio financeiro.

Referências Bibliográficas

1. Feynman, R. P.; Simulating physics with computers. *International Journal of Theoretical Physics* **1982**, 21, 467. [\[Link\]](#)
2. Einstein, A.; Podolsky, B.; Rosen, N.; Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review* **1935**, 47, 777. [\[Crossref\]](#)
3. Feynman, R. P.; Quantum mechanical computers. *Foundations of Physics* **1986**, 16, 507. [\[Crossref\]](#)
4. Mehra, J.; Rechenberg, H.; *The Probability Interpretation and the Statistical Transformation Theory, the Physical Interpretation, and the Empirical and Mathematical Foundations of Quantum Mechanics 1926–1932*, Springer: New York, 2001.
5. Thompson, R. F.; Effect of acquisition level upon the magnitude of stimulus generalization across sensory modality. *Journal of Comparative and Physiological Psychology* **1959**, 52, 183. [\[Crossref\]](#)
6. Delfi, O.; *History of Quantum Mechanics*, Discovery Publishing House: New Delhi, 2023.
7. Heisenberg, W.; Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen. *Zeitschrift für Physik* **1925**, 33, 879. [\[Crossref\]](#)
8. Schrödinger, E.; Quantisierung als Eigenwertproblem. *Annalen der Physik* **1926**, 384, 361. [\[Crossref\]](#)
9. Heisenberg, W.; Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik* **1927**, 43, 172. [\[Crossref\]](#)
10. Bohr, N.; The Quantum Postulate and the Recent Development of Atomic Theory¹. *Nature* **1928**, 121, 580. [\[Crossref\]](#)
11. Dirac, P. A. M.; *The Principles of Quantum Mechanics*, Oxford University Press: Nova York, 2010.
12. Schrödinger, E.; Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften* **1935**, 23, 807. [\[Crossref\]](#)
13. Von Neumann, J.; *Mathematical Foundations of Quantum Mechanics*, Princeton University Press: New Jersey, 2018.
14. Everett, H.; ‘Relative State’ Formulation of Quantum Mechanics. *Reviews of Modern Physics* **1957**, 29, 454. [\[Crossref\]](#)

15. Landauer, R.; Irreversibility and Heat Generation in the Computing Process. *IBM Journal of Research and Development* **1961**, *5*, 183. [\[Crossref\]](#)
16. Bell, J. S.; On the Einstein Podolsky Rosen paradox. *Physique Fizika* **1964**, *1*, 195. [\[Crossref\]](#)
17. Nielsen, M. A.; Chuang, I. L.; *Quantum Computation and Quantum Information*, Cambridge University Press: Cambridge, 2010.
18. Holevo, A. S.; *Statistical Structure of Quantum Theory*, Springer Berlin Heidelberg: Berlin, 2001.
19. Benioff, P.; The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics* **1980**, *22*, 563. [\[Crossref\]](#)
20. Deutsch, D.; Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London: Series A, Mathematical and Physical Sciences* **1985**, *400*, 97. [\[Crossref\]](#)
21. Bennett, C. H.; Brassard, G.; Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* **2014**, *560*, 7. [\[Crossref\]](#)
22. Deutsch, D.; Jozsa, R.; Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London: Series A, Mathematical and Physical Sciences* **1992**, *439*, 553. [\[Crossref\]](#)
23. Ekert, A. K.; Quantum cryptography based on Bell’s theorem. *Physical Review Letters* **1991**, *67*, 661. [\[Crossref\]](#)
24. Shor, P. W.; Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. *Society for Industrial and Applied Mathematics* **1997**, *26*, 1. [\[Link\]](#)
25. Grover, L. K.; Resumo da 28th annual ACM Symposium on Theory of Computing, Philadelphia, United States, 1996. [\[Link\]](#)
26. Chuang, I. L.; Gershenfeld, N.; Kubinec, M.; Experimental Implementation of Fast Quantum Searching. *Physical Review Letters* **1998**, *80*, 3408. [\[Crossref\]](#)
27. Vandersypen, L. M. K.; Steffen, M.; Breyta, G.; Yannoni, C. S.; Sherwood, M. H.; Chuang, I. L.; Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance. *Nature* **2001**, *414*, 883. [\[Crossref\]](#)
28. DiVincenzo, D. P.; The Physical Implementation of Quantum Computation. *Fortschritte der Physik* **2000**, *48*, 771. [\[Crossref\]](#)
29. Specht, H. P.; Nölleke, C.; Reiserer, A.; Uphoff, M.; Figueroa, E.; Ritter, S.; Rempe, G.; A single-atom quantum memory. *Nature* **2011**, *473*, 190. [\[Crossref\]](#)
30. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J. C.; Barends, R.; Biswas, R.; Boixo, S.; Brandao, F. G. S. L.; Buell, D. A.; Burkett, B.; Chen, Y.; Chen, Z.; Chiaro, B.; Collins, R.; Courtney, W.; Dunsworth, A.; Farhi, E.; Foxen, B.; Fowler, A.; Gidney, C.; Giustina, M.; Graff, R.; Guerin, K.; Habegger, S.; Harrigan, M. P.; Hartmann, M. J.; Ho, A.; Hoffmann, M.; Huang, T.; Humble, T. S.; Isakov, S. V.; Jeffrey, E.; Jiang, Z.; Kafri, D.; Kechedzhi, K.; Kelly, J.; Klimov, P. V.; Knysh, S.; Korotkov, A.; Kostitsa, F.; Landhuis, D.; Lindmark, M.; Lucero, E.; Lyakh, D.; Mandrà, S.; McClean, J. R.; McEwen, M.; Megrant, A.; Mi, X.; Michielsen, K.; Mohseni, M.; Mutus, J.; Naaman, O.; Neeley, M.; Neill, C.; Niu, M. Y.; Ostby, E.; Petukhov, A.; Platt, J. C.; Quintana, C.; Rieffel, E. G.; Roushan, P.; Rubin, N. C.; Sank, D.; Satzinger, K. J.; Smelyanskiy, V.; Sung, K. J.; Trevithick, M. D.; Vainsencher, A.; Villalonga, B.; White, T.; Yao, Z. J.; Yeh, P.; Zalcman, A.; Neven, H.; Martinis, J. M.; Quantum supremacy using a programmable superconducting processor. *Nature* **2019**, *574*, 505. [\[Crossref\]](#)
31. Pednault, E.; Maslov, D.; Gunnels, J.; Gambetta, J.; On “quantum supremacy”. Publicado no sítio da IBM em 22/10/2019. [\[Link\]](#)
32. Desdentado, E.; Calero, C.; Moraga, M. Á.; García, F.; Quantum computing software solutions, technologies, evaluation and limitations: a systematic mapping study. *Computing* **2025**, *107*, 110. [\[Crossref\]](#)
33. Weidman, J. D.; Sajjan, M.; Mikolas, C.; Stewart, Z. J.; Pollanen, J.; Kais, S.; Wilson, A. K.; Quantum computing and chemistry. *Cell Reports Physical Science* **2024**, *5*, 102105. [\[Crossref\]](#)
34. Porto, C. M.; Nome, R. A.; Morgon, N. H.; The influence of basis sets and ansatz building to quantum computing in chemistry. *Journal of Molecular Modeling* **2024**, *30*, 275. [\[Crossref\]](#)
35. Porto, C. M.; Fonseca, M. S.; Morais, G. S. T.; Villas-Boas, C. J.; Nome, R. A.; Morgon, N. H.; Computação Quântica em Química. *Química Nova* **2025**, *48*, e-20250072. [\[Crossref\]](#)
36. Gill, S. S.; Cetinkaya, O.; Marrone, S.; Claudino, D.; Haunschild, D.; Schlote, L.; Wu, H.; Ottaviani, C.; Liu, X.; Machupalli, S. P.; Kaur, K.; Arora, P.; Liu, J.; Farouk, A.; Song, H. H.; Uhlig, S.; Ramamohanarao, K.; Em *Quantum Computing*; Buyya, R.; Gill, S. S.; eds.; Elsevier, 2025, cap 2.
37. Griffiths, D. J.; *Introduction to Quantum Mechanics*, Cambridge University Press: Cambridge, 2018.
38. Motta, M.; Rice, J. E.; Emerging quantum computing algorithms for quantum chemistry. *WIREs Computational Molecular Science* **2022**, *12*, e1580. [\[Crossref\]](#)
39. Claudino, D.; The basics of quantum computing for chemists. *International Journal of Quantum Chemistry* **2022**, *122*, e26990. [\[Crossref\]](#)
40. Aarti Dhapte, A.; Market Research Future; Quantum Computing Market. [\[Link\]](#)
41. 5^a Conferência Nacional de Ciência, Tecnologia e Inovação. [\[Link\]](#)
42. Qureca; Overview of Quantum Initiatives Worldwide 2023. [\[Link\]](#)
43. Preskill, J.; Quantum Computing in the NISQ era and beyond. *Quantum* **2018**, *2*, 79. [\[Crossref\]](#)
44. Peruzzo, A.; McClean, J.; Shadbolt, P.; Yung, M. H.; Zhou, X. Q.; Love, P. J.; Aspuru-Guzik, A.; O’Brien, J. L.; A variational eigenvalue solver on a photonic quantum processor. *Nature Communications* **2014**, *5*, 4213. [\[Crossref\]](#)
45. Fontana, E.; Fitzpatrick, N.; Ramo, D. M.; Duncan, R.; Rungger, I.; Evaluating the noise resilience of variational quantum algorithms. *Physical Review A* **2021**, *104*, 022403. [\[Crossref\]](#)
46. Kandala, A.; Mezzacapo, A.; Temme, K.; Takita, M.; Brink, M.; Chow, J. M.; Gambetta, J. M.; Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature* **2017**, *549*, 242. [\[Crossref\]](#)
47. Kutzelnigg, W.; Error analysis and improvements of coupled-cluster theory. *Theoretica Chimica Acta* **1991**, *80*, 349. [\[Crossref\]](#)
48. Anand, A.; Schleich, P.; Alperin-Lea, S.; Jensen, P. W. K.; Sim, S.; Díaz-Tinoco, M.; Kottmann, J. S.; Degroote, M.; Izmaylov,

- A.F.; Aspuru-Guzik, A.; A quantum computing view on unitary coupled cluster theory. *Chemical Society Reviews* **2022**, *51*, 1659. [[Crossref](#)]
49. Bergholm, V.; Izaac, J.; Schuld, M.; Gogolin, C.; Ahmed, S.; Ajith, V.; Alam, M. S.; Alonso-Linaje, G.; AkashNarayanan, B.; Asadi, A.; Arrazola, J. M.; Azad, U.; Banning, S.; Blank, C.; Bromley, T. R.; Cordier, B. A.; Ceroni, J.; Delgado, A.; Di Matteo, O.; Dusko, A.; Garg, T.; Guala, D.; Hayes, A.; Hill, R.; Ijaz, A.; Isacsson, T.; Ittah, D.; Jahangiri, S.; Jain, P.; Jiang, E.; Khandelwal, A.; Kottmann, K.; Lang, R. A.; Lee, C.; Loke, T.; Lowe, A.; McKiernan, K.; Meyer, J. J.; Montañez-Barrera, J. A.; Moyard, R.; Niu, Z.; O’Riordan, L. J.; Oud, S.; Panigrahi, A.; Park, C.-Y.; Polatajko, D.; Quesada, N.; Roberts, C.; Sá, N.; Schoch, I.; Shi, B.; Shu, S.; Sim, S.; Singh, A.; Strandberg, I.; Soni, J.; Száva, A.; Thabet, S.; Vargas-Hernández, R. A.; Vincent, T.; Vitucci, N.; Weber, M.; Wierichs, D.; Wiersema, R.; Willmann, M.; Wong, V.; Zhang, S.; Killoran, N.; PennyLane: Automatic differentiation of hybrid quantum-classical computations. *ArXiv* **2022**. [[Crossref](#)]