RAMOS, Reinaldo Augusto de Oliveira: SILVA, Fabiana Raulino da; ROSETTI, Rafael Diogo. Limites e possibilidades da complexidade computacional quântica. *TECCOGS — Revista Digital de Tecnologias Cognitivas*, n. 29-30, p. 108-130, 2024.

Recebido em: 3 dez. 2024
Aprovado em: 23 dez. 2024

dx.doi.org/10.23925/1984-3585.2024i2930p108-130

Limites e possibilidades da complexidade computacional quântica

Reinaldo Augusto de Oliveira Ramos[1]

Fabiana Raulino da Silva[2]

Rafael Diogo Rossetti[3]

Resumo: O artigo explora o impacto da computação quântica na teoria da complexidade computacional, com destaque para as classes *P* e *BQP*, abordando como os paradigmas quânticos desafiam as categorizações clássicas de problemas. Ao examinar os algoritmos de Shor e Grover, o estudo discute a maneira como esses algoritmos ampliam o escopo de problemas considerados resolvíveis, o que anteriormente era inviável em termos de tempo polinomial em sistemas clássicos. A análise apresenta uma revisão histórica das classes de complexidade, abordando o surgimento e a importância das classes *P* e *NP* e a relevância de algoritmos quânticos em problemas intratáveis. Além disso, o artigo aborda a introdução de teorias híbridas que integram métodos clássicos e quânticos, como o Variational Quantum Eigensolver (*VQE*) e o Quantum Annealing, destacando a eficiência dessas abordagens para resolver problemas de otimização complexos. As discussões

1 É aluno do pós-doutorado, Doutor e Mestre em Tecnologias da Inteligência e Design Digital pela PUC-SP. Especialista em Jogos Digitais pelo SENAC SP. Desenvolvedor Sênior na empresa inglesa Anything World e vice coordenador do Bacharelado em Jogos Digitais da PUC SP. É professor de Jogos Digitais e Data Analytics na ESPM. Orcid: https://orcid.org/0000-0002-8150-6163. E-mail: raoramos@pucsp.br.

2 Fabiana Raulino é doutoranda em Tecnologias da Inteligência e Design Digital pela PUC-SP, com mestrado em Engenharia de Produção pela UFSCAR e especialização em Ergonomia de Sistemas de Produção pela USP. Atua como professora de Inteligência Artificial na Pós-graduação em Animação e Jogos Digitais pela FAAP Digital e professora do MBA Executivo em Inteligência Artificial da Faculdade XP. Orcid: https://orcid.org/0000-0002-8150-6163. E-mail: fabi.ergonomia@gmail.com e fabianaraulino@trampolean.net.

3 Rafael Diogo Rossetti é doutorando em Tecnologias das Inteligências do Design Digital pela PUC SP, com Mestrado em Negócios Internacionais (UCES) e Mestrado Profissional em Desenvolvimento de Jogos (PUC SP). Graduado em Marketing e Desenvolvimento de Jogos, ele também conta com cursos de aperfeiçoamento em instituições renomadas como Israel, MIT, FGV, ESPM e Saint Paul School. Sócio-fundador da Messier Data & Creative Ltda, Rafael é Diretor de Ciência e Tecnologia da Associação dos Diplomados da Escola Superior de Guerra – SP, além de Vice-líder de Pesquisa da Marinha e professor universitário. Orcid: https://orcid.org/0009-0007-5263-0636. E-mail: rossetti@messier.com.br.

sobre as classes probabilísticas *BPP* e *PP* também são centrais para compreender o papel da probabilidade em algoritmos quânticos, uma característica intrínseca ao modelo de computação quântica. O estudo justifica-se pela necessidade de uma reavaliação contínua das bases da teoria da complexidade frente aos avanços quânticos, que redefinem limites teóricos e práticos. Embora a computação quântica ainda enfrente desafios, como a estabilidade dos qubits, as propostas de paradigmas híbridos oferecem caminhos promissores para resolver problemas de alta complexidade, sinalizando uma transição para uma era computacional mista, com potencial para revolucionar a resolução de problemas no século XXI.

Palavras-chave: computação quântica; complexidade computacional; classes *P* e *BQP*; algoritmos quânticos; paradigma híbrido.

Limits and possibilities of quantum computational complexity

Abstract: This paper explores the impact of quantum computing on computational complexity theory, with a focus on the classes *P* e *BQP*, examining how quantum paradigms challenge classical problem categorizations. By analyzing Shor's and Grover's algorithms, the study discusses how these quantum algorithms expand the scope of solvable problems, previously considered intractable within polynomial time for classical systems. The analysis provides a historical review of complexity classes, covering the emergence and significance of classes P and NP and the importance of quantum algorithms for traditionally intractable problems. Additionally, the article addresses the introduction of hybrid theories that integrate classical and quantum methods, such as the Variational Quantum Eigensolver (*VQE*) and Quantum Annealing, highlighting the efficiency of these approaches in solving complex optimization problems. Discussions on probabilistic classes *BPP* and *PP* are also central to understanding the role of probability in quantum algorithms, an intrinsic feature of the quantum computing model. The study is justified by the ongoing need to reevaluate the foundations of complexity theory considering quantum advancements, which redefine theoretical and practical boundaries. While quantum computing still faces challenges, such as qubit stability, hybrid paradigm proposals offer promising paths to address high-complexity problems, signaling a transition toward a mixed computational era with the potential to revolutionize problem-solving in the 21st century.

Keywords: quantum computing; computational complexity; P and BQP classes; quantum algorithms; hybrid paradigm.

Introdução

A teoria da complexidade computacional é uma área central da ciência da computação que busca classificar problemas computacionais de acordo com o esforço necessário para resolvê-los em termos de tempo, espaço e outros recursos. Tradicionalmente, os problemas são classificados em classes como (problemas resolvíveis em tempo polinomial) e NP (problemas verificáveis em tempo polinomial). No entanto, o advento da computação quântica introduziu novas classes de complexidade, como *BQP* (*Bounded-error Quantum Polynomial time*), que se referem à capacidade de resolver problemas com algoritmos quânticos em tempo polinomial, com uma margem de erro aceitável (Watrous, 2008, p. 2; Bernstein; Vazirani, 1993, p. 11).

Embora a computação clássica tenha dominado o campo por décadas, a computação quântica propõe uma mudança de paradigma ao aproveitar os princípios da superposição e do entrelaçamento quântico, possibilitando o processamento de informações de maneiras que a computação clássica não pode replicar (Watrous, 2008, p. 2). Esses princípios resultam em modelos de computação radicalmente diferentes, que desafiam a categorização tradicional dos problemas. Em particular, a computação quântica pode resolver certos problemas, como a fatoração de números grandes, mais eficientemente do que qualquer algoritmo clássico conhecido, como demonstrado pelo algoritmo de Shor (Watrous, 2008, p. 2).

Este artigo se propõe a trazer reflexões sobre o estado atual da teoria da complexidade computacional, comparando as classes de complexidade quânticas e clássicas. A análise focará nas classes *P* e *BQP*, discutindo os limites teóricos, algoritmos representativos e os impactos práticos da computação quântica. Também serão explorados novos paradigmas emergentes que propõem reformulações das bases da teoria da complexidade, buscando integrar a computação quântica de maneira mais coerente ao cenário computacional como um todo. Desta forma, pergunta-se: como a introdução da computação quântica desafia e redefine os paradigmas da teoria da complexidade computacional, e quais são os limites teóricos e práticos das classes *BQP* e *P* na resolução de problemas computacionais complexos?

Os objetivos são discutir as definições formais dessas classes, sua relevância e os principais algoritmos que as representam, com uma análise comparativa entre computação quântica e clássica; explorar como algoritmos quânticos, como o de Shor e o de Grover, alteram a classificação de

problemas em relação às abordagens clássicas, discutindo se problemas anteriormente classificados como intratáveis (em termos de tempo polinomial) podem ser resolvidos eficientemente com algoritmos quânticos; e refletir sobre propostas recentes de teorias híbridas que integram características quânticas e clássicas.

A computação quântica, embora ainda em seus estágios iniciais, promete revolucionar a maneira como problemas computacionais são resolvidos, especialmente aqueles considerados intratáveis pelos modelos clássicos. Uma nova geração de dispositivos quânticos está agora sendo imaginada e realizada, nos quais os estados de objetos quânticos individuais (por exemplo, átomos, elétrons, fótons) são controlados e manipulados de formas que, em décadas anteriores, só eram sonhadas. O entrelaçamento de estados quânticos, anteriormente visto como um aspecto "assustador" da física quântica que parecia demandar uma teoria mais completa, agora é aceito como o mecanismo essencial pelo qual grande parte da tecnologia quântica opera (Raymer e Monroe, 2019, p. 1).

A introdução de novas classes de complexidade, como *BQP*, abre caminho para uma compreensão mais profunda da computação além do paradigma clássico, mas também desafia os fundamentos estabelecidos da teoria da complexidade. Portanto, é crucial revisar essas bases à luz do novo modelo quântico e propor novas direções para a pesquisa em complexidade computacional Shor (Watrous, 2008, p. 11).

O presente estudo justifica-se devido à crescente maturidade da tecnologia quântica, em que a compreensão profunda da relação entre computação quântica e clássica, em termos de complexidade, torna-se não apenas um campo teórico de grande valor, mas também uma área com impactos diretos em aplicações práticas como criptografia, otimização e simulação de sistemas complexos. Este trabalho justifica-se como uma contribuição crítica para a reestruturação das fundações da computação no século XXI.

Teoria da complexidade computacional: contextualização histórica e técnica

A teoria da complexidade computacional é um ramo da ciência da computação que emerge como uma forma de entender as limitações fundamentais dos algoritmos e das máquinas que os executam. Seu principal objetivo é classificar problemas de acordo com a quantidade de recursos computacionais (como tempo e espaço) necessários para resolvê-los. No centro dessa teoria estão duas questões principais: "Quais problemas podem ser resolvidos eficientemente?" e "Quais são os limites do que as máquinas conseguem computar?" (Watrous, 2008, p. 1).

A origem da teoria da complexidade computacional remonta à década de 1930, com a formalização da noção de computação através dos trabalhos de Alan Turing e Alonzo Church, que introduziram modelos matemáticos de máquinas e funções computáveis. A Máquina de Turing, proposta por Turing, se tornou o modelo abstrato universal para descrever a execução de algoritmos. A partir desse modelo, a ciência da computação formalizou a ideia de decidibilidade – se um problema pode ou não ser resolvido por uma máquina (Freire; Greca, 2013, p. 17).

A teoria da recursividade – um campo que estuda quais problemas podem ser resolvidos através de algoritmos – geralmente representa problemas como conjuntos de números naturais. Um problema é decidível se existe um método algorítmico que pode, em tempo finito, determinar se um dado número pertence ao conjunto (ou seja, responde "sim" ou "não" para cada número; Margenstern, 2000, p. 217).

Entretanto, resolver um problema não é suficiente: a eficiência com que ele é resolvido também é de grande importância. Foi apenas com a evolução dos computadores modernos que a preocupação com a eficiência, em termos de tempo de execução e espaço de memória, ganhou maior relevância. A distinção entre problemas fáceis (resolvidos em tempo eficiente) e problemas difíceis (que podem requerer tempos de execução impraticavelmente longos) começou a ser formalizada com o desenvolvimento das classes de complexidade, sendo a classe P uma das primeiras e mais fundamentais (Margenstern, 2000, p. 217).

O algoritmo de Shor, proposto por Peter Shor em 1994, trouxe uma contribuição fundamental ao resolver o problema de fatoração de inteiros em tempo polinomial, com complexidade $O((\log N)3$; Hey, 1999, p. 109)

Na computação clássica, a fatoração de inteiros grandes é um problema da classe *NP* (não determinístico polinomial), sem um algoritmo conhecido que o resolva em tempo polinomial. Em sistemas clássicos, a fatoração rápida torna-se impraticável para números com milhares de dígitos, exigindo tempo exponencial para decompor um número nos seus fatores primos. Essa característica fundamenta a segurança de muitos sistemas criptográficos modernos, como o RSA, que se baseia na dificuldade da fatoração para garantir a integridade dos dados (*ibid.*).

Com o algoritmo de Shor, a computação quântica altera radicalmente essa percepção. A possibilidade de fatoração eficiente subverte a classificação do problema como intratável, ao menos para entradas de tamanhos grandes, mas que permanecem praticáveis com a capacidade de um computador quântico suficientemente poderoso (Arora; Barak, 2007, p.

422). Esse resultado não apenas coloca o problema de fatoração na classe *BQP*, mas também sugere que outros problemas de natureza semelhante, envolvendo estrutura matemática específica, possam ser abordados com a mesma eficiência na computação quântica (Watrous, 2008, p. 12). O impacto dessa reclassificação é duplo: enquanto redefine a tratabilidade de problemas, ela também coloca em xeque os sistemas criptográficos que dependem da complexidade da fatoração (Arora; Barak, 2007, p. 423).

Outro avanço relevante trazido pela computação quântica é o algoritmo de Grover, que realiza buscas em listas ou bancos de dados desordenados com complexidade $O(\sqrt{N}$; Aaronson, 2021, p. 3). Esse algoritmo representa uma abordagem eficiente para o problema de busca, que no modelo clássico requer $O(N)$ operações para ser resolvido de maneira exaustiva. Embora o ganho de eficiência do algoritmo de Grover não seja exponencial, ele oferece uma redução quadrática, o que ainda é significativo em cenários em que o tamanho da entrada N é muito grande (*ibid.*).

A busca não estruturada, comumente encontrada em aplicações como reconhecimento de padrões, análise de dados e resolução de quebra-cabeças combinatórios, era considerada impraticável em situações de tempo polinomial em sistemas clássicos devido à necessidade de checar cada item individualmente (Bernstein; Vazirani, 1993, p. 12). O algoritmo de Grover muda essa classificação, propondo uma alternativa mais rápida que, em sistemas práticos, pode reduzir o tempo de busca de maneira substancial. Isso não altera a classificação do problema de busca em uma classe polinomial estrita, mas desloca sua resolução para um domínio mais eficiente, tornando-o acessível em um número de passos menor do que seria possível classicamente (Aaronson, 2021, p. 3).

Esses avanços exemplificados pelos algoritmos de Shor e Grover evidenciam que a introdução de métodos quânticos de cálculo não apenas modifica a tratabilidade de problemas, mas também provoca uma reinterpretação dos limites teóricos estabelecidos pela complexidade computacional clássica (Freire Junior; Greca, 2013, p. 20). A redefinição de problemas anteriormente intratáveis tem implicações profundas: enquanto a computação clássica considera problemas de fatoração e de busca em certas condições como intransponíveis em tempo polinomial, a computação quântica, ao operar na classe *BQP*, oferece soluções mais acessíveis, que colocam esses problemas em um novo patamar de viabilidade (Aaronson, 2021, p. 3).

Essa nova classificação sugere que problemas com alta simetria ou estrutura oculta – características que algoritmos quânticos são especial-

mente aptos a explorar – poderão ser reavaliados à medida que novas técnicas quânticas surgirem (Mohr, 2014, p. 3). Problemas que antes eram percebidos como limiares de complexidade intransponível, agora se tornam potenciais candidatos a soluções eficientes, ao menos em teoria (Bernstein; Vazirani, 1993, p. 12). No entanto, para que esses algoritmos realmente se tornem ferramentas práticas, ainda é necessária uma infraestrutura de computação quântica robusta e uma superação das barreiras técnicas atuais, como a correção de erros e a estabilidade dos qubits (Aaronson, 2021, p. 2).

O surgimento das classes de complexidade

O surgimento das classes de complexidade foi motivado pela necessidade de organizar problemas computacionais de acordo com a quantidade de recursos – em particular, tempo e espaço – necessários para resolvê-los (Arora; Barak, 2007, p. 66). Essa classificação visa definir a viabilidade prática de resolver problemas, identificando aqueles que podem ser resolvidos de forma eficiente e aqueles para os quais soluções eficientes permanecem desconhecidas (Gill *et al.*, 2021, p. 70). As classes de complexidade estabeleceram um *framework* teórico fundamental na ciência da computação, que não apenas organiza o estudo dos algoritmos e problemas em diferentes categorias, mas também permite análises rigorosas das limitações computacionais (Arora; Barak, 2007, p. 29).

A primeira classe de complexidade amplamente estudada foi *P*, que engloba problemas resolvíveis em tempo polinomial por uma máquina de Turing determinística (Stockmeyer, 1987, p. 4). A classe *P* representa o conjunto de problemas considerados tratáveis, ou seja, problemas que podem ser resolvidos em um tempo razoável conforme o tamanho da entrada aumenta (Arora; Barak, 2007, p. 27). A definição de tempo polinomial (representado como $O(n^k)$ para algum inteiro k) foi escolhida por representar uma expansão moderada de recursos à medida que o problema cresce, o que sugere que esses problemas são resolvíveis em prática por computadores clássicos (Arora; Barak, 2007, p. 68).

Em paralelo ao tempo polinomial, a classe de complexidade de espaço – *PSPACE* – surgiu para abordar problemas baseados na quantidade de memória necessária para resolução. *PSPACE* é definida como o conjunto de problemas que podem ser resolvidos por uma máquina de Turing determinística com uma quantidade polinomial de memória (Aaronson, 2021, p. 2). Esse conceito é importante em áreas como lógica e

verificação de modelos, em que o espaço ocupado é mais relevante que o tempo, especialmente em problemas que envolvem estruturas complexas de dados e lógica (Aaronson, 2021, p. 5).

Com o desenvolvimento da classe *P*, surgiu uma questão crucial: muitos problemas pareciam difíceis de resolver diretamente, mas suas soluções podiam ser verificadas de forma eficiente (Mohr, 2014, p. 3). Isso levou à definição da classe *NP* (Nondeterministic Polynomial time), que engloba problemas cuja solução pode ser verificada em tempo polinomial (Arora; Barak, 2007, p. 39). A classe *NP* inclui problemas como o Caixeiro Viajante e o Problema da Satisfatibilidade Booleano (*SAT*), que podem não ter algoritmos de resolução em tempo polinomial conhecidos, mas têm verificações que podem ser feitas em tempo polinomial (Arora; Barak, 2007, p. 40).

O problema do Caixeiro Viajante (Traveling Salesman Problem –) envolve um vendedor (ou "caixeiro viajante") que deve visitar um conjunto de cidades, passando por cada uma exatamente uma vez e retornando à cidade de origem. O objetivo é determinar a rota mais curta possível que completa esse percurso. Este problema pode ser formalizado como uma questão de minimização sobre um grafo completo, em que as cidades representam os nós e as distâncias entre elas representam as arestas ponderadas do grafo (Arora; Barak, 2007, p. 54).

O *TSP* é um problema *NP*-difícil, uma vez que se encontra fora da classe *P* – para tamanhos de entrada muito grandes, os algoritmos conhecidos demandam tempo exponencial. Além disso, o *TSP* pertence à categoria dos problemas *NP*-completos em sua versão de decisão, e aqui a questão não é encontrar a rota mais curta, mas determinar se existe uma rota que não excede uma determinada distância $\boldsymbol{D}$ (Arora; Barak, 2007, p. 54). A complexidade do *TSP* está no crescimento exponencial do número de rotas possíveis conforme o número de cidades aumenta: para $\boldsymbol{n}$ cidades, existem $(\boldsymbol{n-1})!/\boldsymbol{2}$ possíveis rotas, o que torna inviável uma solução exata por força bruta para grandes valores de *n* (Arora; Barak, 2007, p. 54).

O Problema *P* versus *NP*, uma das maiores questões abertas na ciência da computação, questiona se todos os problemas em *NP* também estão em P, ou seja, se a solução de todos os problemas verificáveis em tempo polinomial poderia ser encontrada em tempo polinomial (Mohr, 2014, p. 3).

A descoberta da classe *NP* e do problema *P* versus *NP* gerou um marco no campo, pois introduziu um nível de incerteza sobre a viabilidade de resolver algoritmos complexos (Mohr, 2014, p. 3). Esse problema é de importância fundamental não só na ciência da computação teórica, mas também em áreas aplicadas como criptografia, em que muitos siste-

mas de segurança dependem da suposição de que problemas *NP*-difíceis não podem ser resolvidos em tempo polinomial (Mohr, 2014, p. 4).

A classe *P* refere-se ao conjunto de problemas que podem ser resolvidos por uma máquina de Turing determinística em tempo polinomial (Watrous, 2008, p. 3). Em termos práticos, um algoritmo pertence à classe *P* se o número de passos necessários para resolver o problema cresce de forma polinomial com o tamanho da entrada. Isso significa que, para qualquer problema em *P*, existe um algoritmo eficiente que pode ser executado dentro de limites razoáveis de tempo (Watrous, 2008, p. 2).

Em contrapartida, foi definida a classe *NP* (Non-deterministic Polynomial time), que contém problemas para os quais uma solução, se fornecida, pode ser verificada em tempo polinomial por uma máquina determinística (Watrous, 2008, p. 3). O conceito de não determinismo surge como uma forma teórica de representar sistemas que podem, em certo sentido, "adivinhar" soluções corretas entre várias possibilidades. No entanto, a existência de algoritmos que resolvam esses problemas em tempo polinomial (ou seja, pertencentes a *P*) ainda é um mistério não resolvido na teoria da complexidade, formulado na famosa questão $P = NP$? (Bernstein; Vazirani, 1993, p. 11).

Ao longo das décadas de 1970 e 1980, essa questão se tornou central na ciência da computação teórica, levando à criação de uma hierarquia mais sofisticada de classes de complexidade, como *NP*-completo (um subconjunto de *NP* para o qual se acredita que não existe solução polinomial), EXP (problemas que requerem tempo exponencial) e *PSPACE* (problemas que podem ser resolvidos usando espaço polinomial; Aaronson, 2021, p. 5). Essas classes permitiram uma classificação mais granular dos problemas computacionais, facilitando o entendimento de suas dificuldades relativas (Arora; Barak, 2007, p. 54).

A teoria da complexidade computacional busca entender os limites e as capacidades dos algoritmos em função dos recursos computacionais necessários para resolver problemas, sendo essencial para categorizar problemas em classes baseadas em suas complexidades temporais e espaciais (Stockmeyer, 1987, p. 5). Uma dessas classes fundamentais é a classe *P*, que inclui todos os problemas que podem ser resolvidos em tempo polinomial por uma máquina de Turing determinística, e que, portanto, são considerados tratáveis computacionalmente dentro de um contexto clássico (Stockmeyer, 1987, p. 4). Este conceito é crucial, pois delimita o que a computação clássica pode resolver de maneira prática, com recursos finitos e em um tempo razoável.

Em contraste, a computação quântica introduz uma nova classe, conhecida como Bounded-Error Quantum Polynomial Time (*BQP*), que representa problemas resolvidos por computadores quânticos em tempo polinomial com um grau aceitável de erro probabilístico (Watrous, 2008, p. 11). A classe *BQP* inclui problemas que podem ser resolvidos mais rapidamente em um sistema quântico do que em um sistema clássico, demonstrando uma vantagem teórica que pode, potencialmente, ser concretizada com o desenvolvimento de computadores quânticos de grande escala (Mohr, 2014, p. 4).

Para compreender as diferenças entre *P* e *BQP*, é essencial analisar algoritmos que exemplifiquem a capacidade única dos sistemas quânticos. Um exemplo clássico é o algoritmo de Shor, que resolve o problema de fatoração em tempo polinomial para números grandes, enquanto a melhor solução conhecida na computação clássica exige tempo exponencial (Mohr, 2014, p. 4). Esse avanço é significativo, pois a fatoração rápida desafia os fundamentos da criptografia moderna, sugerindo que problemas considerados intratáveis em *P* podem, sob o paradigma quântico, tornar-se tratáveis (Bernstein; Vazirani, 1993, p. 14). Da mesma forma, o algoritmo de Grover ilustra a capacidade dos computadores quânticos de realizar buscas não estruturadas em $\boldsymbol{O(\sqrt{N})}$, em contraste com o tempo linear necessário em uma máquina clássica (Aaronson, 2021, p. 5). Estes exemplos não só demonstram a eficiência teórica da *BQP*, mas também levantam questões sobre o alcance dessa vantagem em cenários práticos (Freire Junior; Greca, 2013, p. 20).

Os limites teóricos de BQP em comparação com P ainda são tema de intensos debates na comunidade científica, pois não se sabe com certeza se *BQP* engloba *P*, ou se ambas são classes disjuntas. Estudos indicam que a *BQP* pode incluir uma ampla gama de problemas que não estão na classe *P*, porém sem uma demonstração formal da relação exata entre essas classes, o campo permanece aberto para especulações (Aaronson, 2021, p. 5).

Os desenvolvimentos na computação quântica desafiam as bases da teoria da complexidade ao introduzirem a possibilidade de uma hierarquia de classes que inclua operações e capacidades fora do alcance das máquinas de Turing clássicas (Watrous, 2008, p. 2). Pesquisas recentes discutem o potencial de paradigmas alternativos, como a computação adiabática e o *quantum annealing*, como novos frameworks que podem modificar a definição de tratabilidade computacional, especialmente para problemas de otimização (Gill *et al.*, 2021, p. 68). Estes métodos propõem reformulações dos próprios fundamentos da teoria da complexidade, su-

gerindo que classes como *BQP* possam vir a incorporar novos critérios, ou até mesmo novas classes surgirem para abarcar os avanços teóricos e práticos da computação quântica (Aaronson, 2021, p. 5).

Esses novos paradigmas abrem caminho para a revisão de conceitos tradicionais de complexidade e eficiência, ampliando o escopo para além das máquinas determinísticas e abordando problemas que exigem a exploração do paralelismo quântico. Essa abordagem aponta para uma possível revolução na teoria da complexidade, na qual a computação quântica não seria apenas um complemento, mas uma força motriz para a reestruturação da teoria como um todo (Gill *et al.*, 2021, p. 70).

Se a classe *P* delimita os problemas considerados "facilmente resolvíveis" com algoritmos eficientes em sistemas computacionais clássicos, em contraste, a classe *BQP*, "Bounded-Error Quantum Polynomial Time", inclui problemas de decisão que podem ser resolvidos por uma máquina de Turing quântica em tempo polinomial com uma probabilidade de erro menor que 1/3 (Arora; Barak, 2007, p. 429). Essencialmente, a máquina quântica explora superposição e interferência quântica para testar múltiplos estados simultaneamente, o que a torna especialmente eficiente para certos problemas em que uma busca exaustiva clássica seria inviável (Aaronson, 2021, p. 4). *BQP* é uma classe probabilística; mesmo que o resultado não seja garantido, ele pode ser refinado por múltiplas execuções do algoritmo, o que reduz a probabilidade de erro para níveis arbitrariamente baixos (Bernstein; Vazirani, 1993, p. 20).

A relevância de *P* e *BQP* reside na diferença entre problemas resolvíveis de maneira prática em um computador clássico versus um computador quântico (Bernstein; Vazirani, 1993, p. 20). A computação clássica, ao limitar-se a uma análise sequencial dos dados, enfrenta barreiras consideráveis quando se trata de problemas como fatoração de números grandes, cujo tempo de execução aumenta exponencialmente com o tamanho da entrada (Freire Junior; Greca, 2013, p. 17). Por outro lado, a computação quântica, por meio de *BQP*, promete resolver tais problemas em tempo polinomial, explorando fenômenos quânticos como o entrelaçamento e a superposição (Arora; Barak, 2007, p. 430). Esse salto em capacidade computacional não apenas redefine o conceito de tratabilidade, mas também provoca uma reconsideração das fronteiras de segurança e criptografia que dependem da dificuldade de certos problemas no contexto clássico (Freire Junior; Greca, 2013, p. 17).

Para exemplificar as capacidades de *P* e *BQP*, podemos citar algoritmos específicos que ilustram o potencial de cada classe. No âmbito da classe *P*, o algoritmo de ordenação de mergesort é um exemplo clássico,

operando em tempo *O(n log n)* e demonstrando a eficiência da resolução de problemas estruturados (Cheng; Wang, 2006, p. 4). Outro exemplo relevante na computação clássica é o algoritmo de Dijkstra, utilizado para resolver o problema de caminho mínimo em grafos ponderados, com complexidade temporal de O(V2) em implementações tradicionais, em um cenário em que *V* representa o número de vértices (Li *et al.*, 2022, p. 8).

Na computação quântica, dois algoritmos se destacam: o algoritmo de Shor para fatoração e o algoritmo de Grover para busca não estruturada. O algoritmo de Shor, que resolve a fatoração de inteiros em tempo polinomial *O(log N)3)*, exemplifica a vantagem quântica ao abordar um problema que, na computação clássica, requer tempo exponencial. Essa característica é um marco na complexidade quântica, ameaçando a segurança de sistemas criptográficos baseados em fatoração (Shor, 1997). Já o algoritmo de Grover representa uma busca quadrática sobre um conjunto de dados não estruturados, reduzindo a complexidade de *O(N)* para *O(√N)*, o que, embora não seja exponencial, ainda representa uma melhora significativa para cenários específicos, como criptografia simétrica (Arora; Barak, 2007, p. 27).

Análise comparativa entre computação quântica e clássica

A comparação entre as abordagens clássica e quântica revela não apenas uma diferença na capacidade de processamento, mas também na maneira como a informação é manipulada e interpretada.

A computação clássica, baseada em bits binários (0 ou 1), opera de forma determinística, seguindo um fluxo sequencial ou, no máximo, paralelismo em multiprocessadores para ganhos de desempenho (Gill *et al.*, 2021, p. 69). Em contraste, a computação quântica utiliza qubits, que podem estar em múltiplos estados simultaneamente, representando um espaço de busca exponencialmente maior a cada qubit adicionado (Gill *et al.*, 2021, p. 70). Essa diferença torna a computação quântica particularmente eficaz para problemas nos quais a simultaneidade das soluções gera um ganho significativo, ao contrário dos problemas estruturados, que ainda são resolvidos com mais eficiência em máquinas clássicas para entradas de tamanho moderado (Gill *et al.*, 2021, p. 71).

As limitações da computação quântica, contudo, ainda são significativas; atualmente, os computadores quânticos enfrentam desafios técnicos, como a manutenção da coerência dos qubits e a correção de erros, o que não diminui as muitas possibilidades para o futuro, como podemos ver em Gill *et al.* (2021).

O artigo intitulado "Quantum Computing: A Taxonomy, Systematic Review, and Future Directions" (Gill *et al.*, 2021) apresenta uma revisão abrangente sobre o estado atual da computação quântica, propondo uma taxonomia que categoriza os desenvolvimentos tecnológicos, algoritmos e ferramentas de software no campo. A metodologia empregada é uma revisão sistemática da literatura, na qual os autores analisam a pesquisa existente e destacam áreas de lacunas e desafios. O estudo identifica quatro categorias principais de características da computação quântica: características básicas, algorítmicas, de tempo/portas e outras, fornecendo uma estrutura para mapear os estudos conforme a tecnologia avança. Como resultado, os autores apontam desafios críticos, como a decoerência quântica e as dificuldades de conectividade entre qubits, especialmente em dispositivos da era NISQ (Quantum de Escala Intermediária e Ruidoso), e enfatizam a necessidade de desenvolvimento em criptografia pós-quântica e hardware escalável. O artigo sugere direções futuras para pesquisa, incluindo algoritmos de aprendizado de máquina quântica e avanços na computação segura, ambos promissores, mas ainda limitados por obstáculos técnicos e de implementação

Assim, enquanto a classe *BQP* promete resolver problemas intransponíveis na computação clássica, a implementação prática, de acordo com os autores acima citados ainda depende de avanços tecnológicos substanciais para que essas promessas se tornem aplicáveis a grande escala.

Esse panorama entre as classes *P* e *BQP*, ancorado em algoritmos representativos e nas diferenças entre as abordagens computacionais, permite uma visão aprofundada dos potenciais e limitações de cada paradigma (Mohr, 2007, p. 4). Embora a computação quântica represente um avanço teórico promissor, a complexidade computacional continua a evoluir em direção a um futuro em que o híbrido entre as abordagens clássica e quântica possa ser uma via de exploração científica (Aaronson, 2021, p. 5).

A discussão sobre teorias híbridas que integram características de computação quântica e clássica está ganhando força, especialmente em resposta aos desafios práticos e teóricos que emergem com a introdução de paradigmas quânticos na computação (Gill *et al.*, 2021, p. 15). Essas abordagens híbridas visam explorar o melhor dos dois mundos, aproveitando a estabilidade e a familiaridade dos métodos clássicos juntamente com a eficiência e as capacidades paralelas oferecidas pelos algoritmos quânticos (*ibid.*, p. 17). Em um cenário em que a computação quântica pura ainda enfrenta barreiras técnicas significativas, como a correção de

erros e a manutenção da coerência quântica, as teorias híbridas surgem como uma alternativa viável para resolver problemas complexos de maneira mais eficiente (*ibid.*, 2021, p. 28).

Uma das abordagens mais promissoras na teoria híbrida é o Quantum-Classical Hybrid Algorithm, que utiliza uma estrutura em que partes de um problema são processadas por algoritmos quânticos, enquanto outras são abordadas por métodos clássicos (Gill *et al.*, 2021, p. 12). Um exemplo emblemático dessa abordagem é o algoritmo de otimização Variational Quantum Eigensolver (*VQE*), que aplica uma rotina quântica para a resolução de parte do problema e, em seguida, utiliza um algoritmo clássico para ajustar os parâmetros do circuito quântico, criando um loop iterativo entre os métodos quânticos e clássicos (Gill *et al.*, 2021, p. 2). Esse processo permite que sistemas quânticos de tamanho limitado, como os atualmente disponíveis, contribuam para resolver problemas complexos, enquanto a parte clássica estabiliza e processa o output quântico.

Modelos híbridos, como o Variational Quantum Eigensolver (*VQE*), aplicam sub-rotinas quânticas para explorar espaço de soluções de alta complexidade e métodos clássicos para refinamento e ajuste. Esse método é fundamental na química quântica computacional, em que a simulação de estados moleculares requer uma combinação de precisão e complexidade que apenas sistemas híbridos podem fornecer com eficiência (Gill *et al.*, 2021, p. 2).

Essas estratégias híbridas são fundamentadas na noção de que a computação quântica é particularmente vantajosa para partes de problemas que envolvem grande paralelismo ou alta entropia, como a otimização de funções de energia ou a análise de estados complexos em física e química quântica (McClean *et al.*, 2016, p. 12). A parte clássica, por sua vez, continua essencial para funções que exigem precisão e para tarefas que se beneficiam de arquiteturas tradicionais de computação. Assim, os algoritmos híbridos representam uma solução que integra a vantagem de performance quântica sem depender completamente de sistemas quânticos que ainda estão em fase de desenvolvimento experimental (*ibid.*, p. 1).

Outra abordagem importante dentro da computação híbrida é o uso de *Quantum Annealing* junto com métodos de otimização clássica, como as redes neurais (Gill *et al.*, 2021, p. 2). O *Quantum Annealing*, utilizado principalmente em dispositivos como o D-Wave, permite a exploração de soluções quase-ótimas para problemas de otimização combinatória, como os encontrados em logística e aprendizado de máquina (*ibid.*, p. 31). Ao

combinar o *Quantum Annealing* com métodos clássicos, é possível refinar essas soluções quase-ótimas, reduzindo o espaço de busca para as partes mais promissoras do problema, e então refinar os resultados com algoritmos de aprendizagem clássicos (McClean *et al.*, 2016, p. 6).

Essa combinação é particularmente eficaz para problemas em que as estruturas de dados são muito complexas para serem tratadas com eficiência exclusivamente em um sistema quântico (Arora; Barak, 2007, p. 433). Em aprendizado de máquina, por exemplo, as arquiteturas híbridas são aplicadas para acelerar tarefas de treinamento e inferência, o que poderia ter um impacto significativo em áreas como análise de grandes volumes de dados, reconhecimento de padrões e diagnóstico médico (Gill *et al.*, 2021, p. 15). A partir dessa colaboração entre métodos clássicos e quânticos, o campo da complexidade computacional está, de fato, presenciando uma nova hierarquia de problemas que podem ser resolvidos de maneira otimizada através de abordagens mistas, desafiando as categorizações binárias anteriores entre tratável e intratável (Gill *et al.*, 2021, p. 17).

Embora promissoras, as abordagens híbridas também enfrentam desafios significativos, especialmente no que se refere à integração eficaz entre os sistemas quânticos e clássicos. Um dos principais problemas é a latência na comunicação entre os sistemas, pois o envio e processamento de dados entre unidades quânticas e clássicas pode introduzir atrasos que limitam a eficiência do processo híbrido (McClean *et al.*, 2016, p. 10). Além disso, a adaptação dos algoritmos clássicos para trabalhar de forma otimizada em conjunto com algoritmos quânticos ainda exige um desenvolvimento algorítmico e técnico profundo, principalmente em relação à correção de erros e à parametrização dos circuitos quânticos (*ibid.*, p. 11).

Outro desafio é a definição da classe de problemas que realmente se beneficiam dessas arquiteturas híbridas, já que muitas soluções ainda dependem de experimentação e ajustes. Enquanto métodos clássicos de machine learning podem ser melhorados com componentes quânticos, ainda há debate sobre a real extensão da vantagem quântica para algoritmos híbridos em larga escala. A própria teoria da complexidade computacional híbrida ainda está em seus estágios iniciais, e espera-se que novas classificações e frameworks sejam propostos para abordar a complexidade mista dos sistemas híbridos (Gill *et al.*, 2021, p. 15).

Os avanços em teorias híbridas abrem caminho para um cenário em que a computação quântica e clássica podem ser integradas em uma infraestrutura conjunta, permitindo que cada tipo de sistema seja utiliza-

do em sua capacidade máxima. Pesquisadores sugerem a possibilidade de uma "computação em camadas" para resolver problemas que seriam segmentados em subproblemas, com camadas específicas sendo destinadas a algoritmos quânticos e outras camadas a algoritmos clássicos. Esse modelo de segmentação modular ajudaria a superar limitações atuais, facilitando o uso simultâneo de várias arquiteturas computacionais em um único ambiente (Gill *et al.*, 2021, p. 25).

Assim, as teorias híbridas estão construindo a base para uma transformação nos paradigmas de complexidade computacional, ao permitir que características clássicas e quânticas coexistam, otimizando a resolução de problemas de alta complexidade. Embora ainda estejam emergindo, as propostas de integração híbrida oferecem uma visão para o futuro da computação, em que a colaboração entre métodos clássicos e quânticos permita expandir o escopo e a aplicabilidade da teoria da complexidade, promovendo uma revolução prática e teórica em como a computação enfrenta problemas complexos (Gill *et al.*, 2021, p. 28).

Além disso, o surgimento de novas classes de complexidade na computação quântica marca uma evolução fundamental no entendimento teórico e prático de problemas computacionais. A transição das classes clássicas de complexidade, como *P* e *NP*, para novas classes quânticas, como *QMA* (Quantum Merlin Arthur), e a reavaliação de classes probabilísticas clássicas, como *BPP* (Bounded-error Probabilistic Polynomial time) e *PP* (Probabilistic Polynomial time), abrem novas perspectivas para a análise e categorização de problemas específicos do domínio quântico (Watrous, 2008, p. 18).

A computação quântica introduz propriedades únicas, como a superposição e o entrelaçamento, que desafiam os limites das classes de complexidade tradicionais. Enquanto classes clássicas,como *P* e *NP* , são definidas pela capacidade dos algoritmos de resolver problemas em tempo polinomial ou verificar soluções em tempo polinomial, as máquinas quânticas podem explorar vastos espaços de soluções simultaneamente, operando em estados de probabilidade que requerem uma abordagem probabilística mais ampla (Bernstein; Vazirani, 1993, p. 12). Nesse cenário, surgem classes quânticas como *BQP* (Bounded-error Quantum Polynomial time), que representam problemas solúveis por computadores quânticos com uma probabilidade de erro limitada e que expandem as fronteiras do que é computacionalmente acessível (Bernstein; Vazirani, 1993, p. 14).

Classes de complexidade probabilística e verificação quântica: *QMA*, *BPP* e *PP*

QMA, ou Quantum Merlin Arthur, é uma classe de complexidade que adapta a classe *MA* (Merlin-Arthur) da teoria clássica para o contexto quântico. Em termos simples, um problema está em *QMA* se um "proponente" (Merlin) pode fornecer uma prova quântica para uma afirmação, e um verificador quântico (Arthur) pode validar essa prova com um erro limitado (Aaronson, 2021, p. 5). A *QMA* amplia a noção de verificabilidade para situações nas quais provas e verificações utilizam propriedades quânticas, criando possibilidades para problemas em que a validação de estados quânticos complexos é necessária (Watrous, 2008, p. 18).

Por exemplo, um problema como a verificação de um estado quântico emaranhado específico, essencial em protocolos de criptografia quântica e simulações moleculares, pertence a essa classe. *QMA* representa, portanto, uma extensão prática para problemas de decisão na computação quântica e aponta para uma taxonomia em que não apenas a resolução, mas também a verificabilidade de soluções quânticas, é considerada (*ibid.*, p. 19).

Classes probabilísticas como *BPP* e *PP* desempenham um papel essencial ao fornecer uma base para a compreensão da probabilidade em sistemas computacionais. *BPP*, que representa problemas solucionáveis em tempo polinomial com uma margem de erro limitada, é uma classe que se adapta ao ambiente quântico, em que o comportamento probabilístico é uma característica nativa (Arora; Barak, 2007, p. 68). Na computação quântica, os algoritmos frequentemente retornam respostas com uma probabilidade de erro intrínseca, tornando *BPP* um alicerce para a construção de novas classes de complexidade quântica (*ibid.*, 2007, p. 143).

Por outro lado, *PP* é uma classe que engloba problemas solucionáveis em tempo polinomial em que a probabilidade de sucesso pode ser superior a 50% (Arora; Barak, 2007, p. 173). *PP* é mais permissiva que *BPP*, uma vez que não impõe restrições rígidas à probabilidade de erro. Essa flexibilidade é relevante na computação quântica, especialmente em algoritmos em que a exatidão total é impossível ou desnecessária, mas uma solução com alta probabilidade de sucesso é suficiente. Isso se mostra valioso, por exemplo, em algoritmos quânticos de otimização e em certos tipos de simulações moleculares, em que as probabilidades podem ser manipuladas para maximizar as chances de uma solução próxima do ideal (*ibid.*).

As classes quânticas e probabilísticas delineiam uma taxonomia que abrange melhor os problemas da era quântica (Gill *et al.*, 2021, p. 25). Diferentes classes permitem separar problemas que são teoricamente resolvíveis de forma quântica daqueles que são apenas verificáveis, ou que dependem fortemente da probabilidade. A introdução dessas classes não apenas enriquece a teoria da complexidade, mas também permite categorizar problemas práticos da computação quântica dentro de um quadro compreensível, aproximando a teoria da prática (*ibid.*).

Por exemplo, a classe *QMA* completa, que contém problemas que são teoricamente difíceis mesmo para algoritmos quânticos, representa o limite da complexidade computacional para verificações quânticas (Aaronson, 2021, p. 5). Em contrapartida, problemas em BQP, mais acessíveis à solução quântica, sugerem a possibilidade de algoritmos eficientes para tarefas como a fatoração de números inteiros, demonstrada pelo famoso algoritmo de Shor. As interseções entre essas classes destacam a flexibilidade da computação quântica ao lidar com problemas com diferentes níveis de dificuldade e verificabilidade (Arora; Barak, 2007, p. 143). A criação de novas classes de complexidade quântica e a inclusão de classes probabilísticas na taxonomia quântica têm implicações profundas.

No plano teórico, elas permitem que a computação quântica seja compreendida de forma mais integrada e robusta dentro do campo da complexidade computacional. No contexto prático, essas classes auxiliam na identificação de problemas que, embora intratáveis por máquinas clássicas, podem ser viáveis de serem resolvidos ou verificados com o uso de algoritmos quânticos. Essa categorização é crucial para a transição da computação quântica do ambiente acadêmico para aplicações industriais, como segurança de dados, bioinformática e ciência dos materiais (Gill *et al.*, 2021, p. 3).

Classes como *QMA* fornecem um modelo para a validação de soluções quânticas, possibilitando que problemas de criptografia e otimização sejam mais bem compreendidos e abordados. Além disso, *BPP* e *PP* criam uma estrutura probabilística que suporta a criação de algoritmos híbridos, nos quais sistemas quânticos e clássicos podem operar em conjunto. Dessa forma, a complexidade quântica oferece uma ponte entre a teoria da computação e aplicações práticas, em que a probabilidade e a verificabilidade tornam-se elementos centrais no desenvolvimento de soluções (Watrous, 2008, p. 19).

Conclusões

A computação quântica, ao oferecer uma alternativa paradigmática aos sistemas clássicos, enfrenta complexos desafios técnicos, sobretudo no que tange à manutenção da coerência dos qubits. Este fenômeno, essencial para a execução de cálculos quânticos eficazes, é limitado pela fragilidade dos estados quânticos frente a interações externas, o que provoca a chamada decoerência. Em um sistema quântico, a interação com o ambiente pode introduzir flutuações que comprometem a superposição e o entrelaçamento, elementos fundamentais para o processamento quântico de informações. Com o aumento no número de qubits em dispositivos quânticos, a probabilidade de ocorrências de erro por decoerência cresce exponencialmente, tornando a preservação da coerência um dos principais obstáculos para a implementação prática em larga escala de algoritmos quânticos. Esta limitação não apenas restringe o tempo de vida dos qubits, mas também impõe barreiras substanciais à escalabilidade e à estabilidade dos sistemas quânticos, afetando a confiabilidade de suas operações.

A necessidade de correção de erros quânticos surge como uma tentativa de contornar os limites impostos pela decoerência, permitindo que a computação quântica mantenha a integridade da informação mesmo em face de erros inevitáveis. No entanto, a correção de erros quânticos traz seu próprio conjunto de desafios, uma vez que exige uma complexa arquitetura de redundância: cada qubit lógico deve ser sustentado por múltiplos qubits físicos, resultando em uma sobrecarga significativa de recursos. Esse aumento de complexidade arquitetural impacta diretamente a escalabilidade, tornando as implementações de larga escala ainda mais desafiadoras no contexto atual da tecnologia. A necessidade de um número expressivamente maior de qubits físicos para compor um único qubit lógico funcional implica em um consumo substancial de energia e requer níveis avançados de isolamento e controle térmico, o que por sua vez limita o uso da computação quântica fora de ambientes altamente controlados. A análise detalhada desses fatores é essencial para se compreender o caminho árduo e gradual que a computação quântica deve percorrer até alcançar um estágio de aplicabilidade ampla e efetiva.

A análise sobre as classes de complexidade quânticas e clássicas, particularmente focando em P e BQP, e a introdução de algoritmos quânticos como os de Shor e Grover, revela uma transformação fundamental na compreensão dos limites da computação e da teoria da complexidade. Tradicionalmente, a computação clássica enfrenta barreiras bem definidas

para problemas de alta complexidade, classificando muitos deles como intratáveis em termos de tempo polinomial. Entretanto, com o advento da computação quântica, alguns desses problemas tornam-se viáveis, mudando a definição de tratabilidade e introduzindo um novo paradigma para a resolução de problemas computacionais complexos.

O algoritmo de Shor exemplifica uma ruptura significativa na segurança criptográfica baseada em fatoração de grandes inteiros, mostrando que o que era considerado seguro e intransponível em um contexto clássico pode ser resolvido em tempo polinomial por sistemas quânticos. Da mesma forma, o algoritmo de Grover representa uma aceleração na busca de dados desestruturados, diminuindo significativamente o número de operações necessárias e abrindo novas possibilidades para áreas de big data e inteligência artificial. Essas capacidades ampliam o potencial prático da computação quântica em domínios aplicados e sublinham a necessidade de novos modelos de criptografia resistentes a ataques quânticos.

A introdução de modelos híbridos, como o *Variational Quantum Eigensolver* (*VQE*) e *Quantum Annealing* em conjunto com métodos de otimização clássicos, inaugura uma era em que a computação não será exclusivamente clássica ou quântica, mas uma fusão eficiente dos dois paradigmas. Essa abordagem híbrida é particularmente promissora para problemas de otimização e simulação molecular, em que a complexidade mista permite explorar um espaço de solução maior e com maior precisão, criando uma classe de problemas que apenas esses sistemas integrados podem resolver com eficácia.

A expansão da complexidade computacional para incluir classes específicas de problemas quânticos e probabilísticos representa um avanço crítico para a computação moderna. *QMA*, *BPP* e *PP* são exemplos de como a teoria da complexidade se adapta para lidar com os desafios e oportunidades da computação quântica, oferecendo uma estrutura que ajuda a distinguir diferentes tipos de problemas, desde os solucionáveis até os verificáveis e probabilisticamente resolvíveis. Essas classes não apenas ampliam o escopo teórico, mas também guiam o desenvolvimento de algoritmos e soluções práticas, impulsionando a computação quântica como uma ferramenta fundamental para a resolução de problemas de alta complexidade na sociedade moderna.

A relação entre *P* e *BQP* ainda é teórica e experimentalmente indefinida. Não há prova de que *BQP* engloba *P* ou vice-versa. Isso significa que problemas que são tratáveis na computação clássica podem não ter eficiência equivalente em sistemas quânticos e que problemas em *BQP* podem não ser resolvíveis por algoritmos determinísticos clássicos.

Essas descobertas apontam para uma expansão da teoria da complexidade computacional, que precisa evoluir para incluir uma taxonomia mais ampla e adaptativa de problemas, contemplando as classes de complexidade híbrida. A criação de novos frameworks para descrever essa complexidade mista é essencial, pois permitirá uma classificação mais precisa e previsível do que é viável ou intratável na computação moderna. Em última análise, a introdução de computação quântica e híbrida não só redefine os limites teóricos da complexidade, mas também traz um impacto prático significativo para a ciência, a segurança digital e o desenvolvimento de tecnologias avançadas, sinalizando uma revolução contínua na maneira como abordamos problemas computacionais.

Os limites teóricos e práticos de *P* e *BQP* apontam para a necessidade de abordagens híbridas, em que a computação clássica e quântica são utilizadas em conjunto, tirando proveito das forças de cada abordagem. A integração de algoritmos clássicos e quânticos, como no *Variational Quantum Eigensolver* (VQE) e em outras técnicas de otimização híbrida, visa utilizar a eficiência da computação clássica para problemas estruturados enquanto explora a computação quântica para resolver partes do problema que se beneficiam do paralelismo quântico (McClean *et al.*, 2016, p. 1). Esse tipo de arquitetura híbrida pode permitir que problemas classificados atualmente como intratáveis se tornem acessíveis, mesmo que parcialmente, em um futuro próximo.

Referências

AARONSON, Scott. Open problems related to quantum query complexity. *ACM Transactions on Quantum Computing*, v. 2, n. 4, p. 1–9, 31 dez. 2021. Disponível em https://arxiv.org/pdf/2109.06917. Acesso em 30 de outubro de 2024.

ARORA, Sanjeev; BARAK, Boaz. *Computational complexity:* A modern approach. Cambridge: Cambridge University Press, 2009.

BERNSTEIN, Ethan.; VAZIRANI, Umesh. *Quantum complexity theory. Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing – STOC '93*, p. 11-20, 1993. Disponível em: <https://doi.org/10.1137/S0097539796300921>. Acesso em 30 de outubro de 2024.

CHENG, Sheng-Tzong; WANG, Chun-Yen. Quantum switching and quantum merge sorting. *IEEE Transactions on Circuits and Systems I: Regular Papers*, v. 53, n. 2, p. 316-325, 2006. Disponível em: <https://ieeexplore.ieee.org/document/1593938>. Acesso em 30 de outubro de 2024.

FREIRE JUNIOR, Olival; GRECA, Ilena M. Informação e teoria quântica. *Scientiae Studia*, v. 11, n. 1, p. 11–33, jan. 2013. Disponível em: <https://www.scielo.br/j/ss/a/gx6mgj96M9q96XVkrkh7bSp>. Acesso em 30 de outubro de 2024.

GILL, Sukhpal Singh, *et al*. Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience*, 52, p. 66-114, 2021. Disponível em: <https://onlinelibrary.wiley.com/doi/epdf/10.1002/spe.3039>. Acesso em 30 out., 2024.

HEY, Tony. Quantum computing: an introduction. *Computing & Control Engineering Journal*, v. 10, n. 3, p. 105-112, 1999. Disponível em: https://www.researchgate.net/publication/3363605_Quantum_computing_An_introduction. Acesso em 30 de outubro de 2024.

LI, Jian *et al*. Fidelity-guaranteed entanglement routing in quantum networks, *IEEE Transactions on Communications*, v. 70, n. 10, p. 6748-6763, 2022. Disponível em: <https://arxiv.org/abs/2111.07764>. Acesso em 30 de outubro de 2024.

MARGENSTERN, Maurice. Frontier between decidability and undecidability: a survey. *Theoretical Computer Science*, v. 231, n. 2, p. 217-251, 2000. Disponível em: https://core.ac.uk/download/pdf/82133923.pdf. Acesso em 30 de outubro de 2024.

McCLEAN, Jarrod R. *et al*. The theory of variational hybrid quantum-classical algorithms. *New Journal of Physics*, v. 18, n. 2, 20 p, 2016. Disponível em: <https://arxiv.org/abs/1509.04279>. Acesso em 30 de outubro de 2024.

MOHR, Austin. Quantum computing in complexity theory and theory of computation, Carbondale IL, 2014, Disponível em: <http://austinmohr.com/work/files/complexity.pdf>. Acesso em 30 de outubro de 2024.

RAYMER, Michael G.; MONROE, Chistopher. The US National Quantum Initiative. *Quantum Science Technology*, v. 4, n. 20504, p. 1-6, 2019. Disponível em: <https://iopscience.iop.org/article/10.1088/2058-9565/ab0441>. Acesso em 30 de outubro de 2024.

STOCKMEYER, Larry. Classifying the computational complexity of problems. *Journal of Symbolic Logic*, v. 52, n. 1, p. 1-43, 1987. Disponível em: <https://www.jstor.org/stable/2273858>. Acesso 30 out., 2024.

WATROUS, John. Quantum computational complexity, 2008. Disponível em: <https://arxiv.org/abs/0804.3401>. Acesso em 30 de outubro de 2024.