##### REPORT 3

**Sumário e Primeiro Capítulo Teórico**

##### IDENTIFICAÇÃO

|  |  |  |  |
| --- | --- | --- | --- |
| **NO** | **NOME** | **e-mail** | **Telefone** |
| **1** | **Luis Felipe dos Santos Gianoni** | **lfelipe2305@hotmail.com.br** | **15981420688** |
| **2** | **Marcos Favoretti Jr** | [**marcos.junior@ethos.ind.br**](mailto:marcos.junior@ethos.ind.br) | **15991642814** |
| **3** | **Patrick Nunes de Souza** | **patrick.n.souza@outlook.com** | **15991459102** |

**TÍTULO:**

Algoritmo de busca em grafos utilizando computação quântica

**LÍDER DO GRUPO:**

Patrick Nunes de Souza

**ORIENTADOR:**

Marcos Fabio Jardini

Data da Entrega: 24 / 04 /2025

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Visto do Orientador

**Sumário**

1. **INTRODUÇÃO**
2. **O CAIXEIRO VIAJANTE**

**2.1 Contextualização do Problema com Grafos**

**2.2 Complexidade NP e P**

**2.3 Soluções da atualidade**

**2. CATEGORIAS DE RECOMENDAÇÃO**

Todo o título deve estar com letras maiúsculas. Texto explicando os tipos que serão abordados no capítulo, a importância dos mesmos e suas vantagens.

**2.1 Baseado em Conteúdo e Filtragem Colaborativa**

Apenas a primeira letra de cada palavra em maiúsculo. Texto sobre o assunto.

2.1.1 Sistemas híbridos

Apenas a primeira letra de cada palavra em maiúsculo e sem negrito. Texto sobre o assunto.

2.1.2 Exemplos de aplicação

Apenas a primeira letra da primeira palavra em maiúsculo e sem negrito. Texto sobre o assunto.

(Utilizar o template do TCC)

**1º CAPÍTULO TEÓRICO (item 2 da Monografia)**

O documento deve conter:

- Lista de Figuras (se for o caso: mais de 5 itens)

- Lista de Tabelas (se for o caso: mais de 5 itens)

- Lista de Abreviaturas e Siglas (se for o caso – ordem alfabética)

- Lista de Símbolos (se for o caso – ordem alfabética)

- SUMÁRIO

- Item 2 da monografia, visto que o item 1 é a INTRODUÇÃO

- Referências

**IMPORTANTE:** Usar fonte Arial, tamanho 12, espaço entrelinhas 1,5, folha A4.

**2 O CAIXEIRO VIAJANTE:**

Nesse projeto será tratado o problema do Caixeiro Viajante, conhecido como “*Travelling Salesman Problem”* (TSP), é um dos problemas mais estudados na área de otimização combinatória e teoria dos grafos. Sua formulação clássica propõe encontrar o caminho mais curto que permite a um caixeiro visitar um conjunto de cidades, passando por cada uma exatamente uma vez e retornando ao ponto de partida. O nome tem origem em uma analogia com os vendedores ambulantes do século XIX, que percorriam diferentes localidades para comercializar seus produtos e, por isso, precisavam planejar rotas eficientes para reduzir tempo e custos.

Segundo Perkins (2021), as origens do Problema do Caixeiro Viajante, ou TSP, remontam ao início do século XIX, mas foi formalizado matematicamente pela primeira vez por um indivíduo chamado Merrill M. Flood em 1930, que tentava resolver um problema de roteamento de ônibus escolares. Posteriormente, adotado por Hassler Whitney em Princeton sob o apelido de "problema dos 48 estados", no qual a rota mais curta era considerada para visitar todos os 48 Estados Unidos contíguos, recebeu finalmente a expressão atual "TSP" em um relatório da RAND Corporation de 1949.

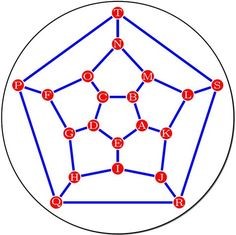
De acordo com Zhou et al. (2019), o TSP tornou-se um paradigma importante na ciência da computação por ser um problema NP-difícil, ou seja, para o qual não se conhece um algoritmo eficiente que resolva todas as instâncias em tempo polinomial, no capítulo 2.3 será abordado mais especificamente sobre problema NP-difícil. Entre as curiosidades que envolvem o TSP, destaca-se o fato de que ele possui aplicações em áreas inesperadas, como na genética (por meio do sequenciamento de DNA), na robótica (planejamento de trajetórias) e até na arte computacional.

2.1 Contextualização do Problema com Grafos

De acordo com Silva, Oliveira e Costa (2022), grafos são estruturas matemáticas fundamentais nas áreas de matemática discreta e estrutura de dados, amplamente utilizadas na ciência da computação para modelar relações e interações entre elementos. Formalmente, um grafo é composto por um conjunto de vértices (ou nós) e por um conjunto de arestas que conectam pares desses vértices. Essa estrutura permite representar, de maneira abstrata, diversos sistemas do mundo real, como redes de transporte, redes de comunicação, redes sociais, entre outros. Por exemplo, em um sistema de transporte, os vértices podem representar cidades e as arestas, as estradas que as conectam. Na área de estrutura de dados, os grafos são essenciais para o desenvolvimento de algoritmos que resolvem problemas como busca em profundidade e largura, detecção de ciclos, caminhos mínimos e otimização de rotas.

Dentro do estudo dos grafos, destaca-se o conceito de ciclo hamiltoniano, que é um caminho fechado que passa por todos os vértices do grafo exatamente uma vez, retornando ao ponto de origem. De acordo com Marcelo de Souza Santos (2016), esse tipo de ciclo foi nomeado em homenagem ao matemático irlandês William Rowan Hamilton, que introduziu a ideia no século XIX por meio de um jogo matemático conhecido como "Icosian Game", como mostrado na figura 1.

Figura 1- tabuleiro do Icosian Game



fonte: disponível em: <https://fr.pinterest.com/pin/465559680219761838>. Acesso em 20 de Abr. 2025.

Segundo Santos, Marcelo de Souza (2016), Esse problema teve origem em 1850 e o adjetivo hamiltoniano foi dado devido ao trabalho do matemático irlandês William R. Hamilton. Hamilton inventou o Icosian Game, um jogo no qual o mundo foi baseado em um grafo dodecaedro. Os vértices desse grafo foram rotulados como cidades e o objetivo do jogo era que um viajante visitasse todas as 20 cidades sem repetir alguma cidade já visitada.

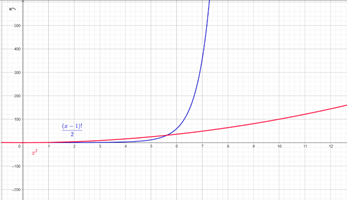
 A existência de um ciclo hamiltoniano em um grafo está diretamente relacionada a diversos problemas práticos, sendo um dos elementos centrais no problema do Caixeiro Viajante.

2.2 Complexidade NP e P

O problema do Caixeiro Viajante está inserido na classe dos chamados problemas NP-difíceis (Non-deterministic Polynomial-time hard), sendo considerado NP-completo em sua versão de avaliação do caminho, onde se busca determinar se existe um percurso com custo inferior ou igual a um valor previamente definido, retornando apenas se é verdadeiro ou falso. A classificação como NP-completo implica que o problema pertence ao conjunto NP (tempo polinomial não determinístico), ou seja, ainda que não exista um algoritmo conhecido que resolva o problema em tempo polinomial para todas as instâncias, qualquer solução proposta pode ser verificada com eficiência, isto é, em tempo polinomial.

De acordo com Perkins (2021), a principal distinção entre problemas de tempo polinomial (polynomial time), como ordenações e buscas simples (com complexidades como O(n), O(n log n), O(n²)), e os de tempo não polinomial (non-polynomial time), como muitos problemas combinatórios, está na escalabilidade da solução. Problemas NP-difíceis, como o Caixeiro Viajante, tendem a apresentar crescimento exponencial ou fatorial no número de possibilidades a serem analisadas por exemplo, com n cidades, existem (n − 1)!/2 rotas possíveis distintas, abaixo na imagem 2 pode-se visualizar escalabilidade da solução entre um problema p e np-dificil. Isso significa que mesmo para instâncias com um número relativamente pequeno de cidades, a quantidade de combinações possíveis pode se tornar computacionalmente inviável de se percorrer por força bruta. Esse crescimento exponencial impõe uma limitação prática: enquanto um algoritmo de tempo polinomial é viável mesmo em grandes volumes de dados, algoritmos de tempo não polinomial tornam-se rapidamente impraticáveis com o aumento da entrada.

Figura 2- Comparação de escabilidade entre NP e P



fonte: autoria própria

2.3 Soluções da atualidade

Diante dessa complexidade, diversos métodos computacionais têm sido empregados para encontrar soluções viáveis ao problema. Os algoritmos exatos, como a técnica de programação dinâmica (ex.: algoritmo de Held-Karp) ou o método de branch and bound, garantem a obtenção da melhor solução possível, mas seu tempo de execução cresce rapidamente à medida que o número de vértices aumenta, o que restringe sua aplicação a instâncias de pequeno ou médio porte.

De acordo com Zhou et al. (2019), Como alternativa, surgem os algoritmos heurísticos e meta-heurísticos, que não garantem a solução ótima, mas produzem respostas satisfatórias em tempo razoável. Dentre esses, destacam-se os algoritmos genéticos, a colônia de formigas, a busca tabu e o simulated annealing, os quais baseiam-se em princípios inspirados na natureza, em processos de otimização probabilística e em estratégias adaptativas para explorar o espaço de soluções. Essas abordagens têm se mostrado especialmente eficazes em cenários reais, como logística, roteamento de veículos, planejamento de produção, redes de distribuição e bioinformática, onde a obtenção de uma solução ótima exata é menos relevante do que alcançar uma solução suficientemente boa dentro de um tempo computacional aceitável.

**3 Computação Quântica**

**A computação quântica é uma tecnologia em constante evolução que explora os princípios da mecânica quântica para processar informações de maneiras fundamentalmente distintas dos computadores clássicos. Enquanto os sistemas computacionais convencionais operam com bits que representam estados definidos (0 ou 1), os qubits, a unidade fundamental de informação quântica, possuem a capacidade de existir em superposição, ou seja, em múltiplos estados simultaneamente. Essa característica, junto ao fenômeno do entrelaçamento quântico, permite que os computadores quânticos manipulem exponencialmente mais informações e executem cálculos que ultrapassam a capacidade dos sistemas computacionais atuais, esses e mais alguns fundamentos serão mais bem explicados e definidos no próximo capítulo desse projeto. Como bem ressaltam Nielsen e Chuang (2010) em sua obra seminal "Quantum Computation and Quantum Information", "qualquer tarefa computacional que um computador clássico pode realizar, um computador quântico também pode, mas a recíproca não é verdadeira." De fato, essa tecnologia promissora visa solucionar problemas que complexos que para um computador clássico demandariam bilhões de anos de processamento.**

**3.1 Fundamentos e Princípios da Mecânica Quântica**

**Para compreender a computação quântica, é essencial ter uma noção dos principais princípios da mecânica quântica que a sustentam. Esse subcapitulo irá abordar os principais princípios.**

**3.1.1 Superposição**

**A superposição é um dos pilares fundamentais da computação quântica e um conceito que distingue os qubits dos bits clássicos. Em termos simples, a superposição permite que um qubit não se restrinja a um único estado binário (0 ou 1) a qualquer momento, mas sim que exista em uma combinação linear de ambos os estados simultaneamente. Imagine um bit clássico como um interruptor de luz que está ligado (1) ou desligado (0). Um qubit, por outro lado, pode ser visualizado como um interruptor que está, de alguma forma, ligado e desligado ao mesmo tempo, ou, mais precisamente, em uma proporção de ambos.**

**Essa analogia com a moeda girando no ar, popularizada para ilustrar o conceito, é bastante intuitiva: enquanto a moeda está girando, ela não é nem "cara" nem "coroa", ela está em um estado de incerteza que abrange ambas as possibilidades. Somente quando a moeda pousa e seu movimento cessa é que seu estado se torna definido. Da mesma forma, um qubit em superposição existe em uma combinação de 0 e 1, com certas probabilidades associadas a cada estado. Conforme explicam Nielsen e Chuang (2010), o estado de um qubit pode ser representado matematicamente como α∣0⟩+β∣1⟩, onde α e β são amplitudes de probabilidade complexas, e ∣α∣^2+∣β∣^2=1. Isso significa que o qubit tem uma probabilidade ∣α∣^2 de ser medido como 0 e uma probabilidade ∣β∣^2 de ser medido como 1.**

**O ato de medição é o que "colapsa" o estado do qubit de sua superposição para um estado clássico definido (0 ou 1). Antes da medição, todas as possibilidades de estado coexistem, mas no momento da observação, apenas uma é revelada probabilisticamente. Essa capacidade intrínseca de existir em múltiplos estados simultaneamente é o que confere aos computadores quânticos um poder inerente de processamento paralelo massivo. Em vez de processar cada estado sequencialmente, um sistema de qubits em superposição pode explorar simultaneamente um número exponencialmente maior de caminhos computacionais. Como destaca Deutsch (1985) em seu trabalho sobre a universalidade de um computador quântico, essa superposição é a base para a aceleração de certos algoritmos, permitindo que eles resolvam problemas em tempo polinomial onde algoritmos clássicos exigiriam tempo exponencial.**

* **Imagem de tempo polinominal**

**3.1.2 Entrelaçamento Quântico**

**O entrelaçamento quântico é absolutamente crucial para o poder computacional dos sistemas quânticos. Ele descreve uma conexão profunda entre dois ou mais qubits, onde seus estados se tornam ligados de tal forma que o estado de um qubit não pode ser descrito independentemente dos outros, mesmo que estejam fisicamente separados por grandes distâncias.**

**Para ilustrar, imagine um par de luvas: se você tem uma luva esquerda, sabe instantaneamente que a outra luva é uma luva direita, independentemente de onde ela esteja. No mundo quântico, o entrelaçamento é muito mais profundo. Quando qubits estão entrelaçados, a medição do estado de um deles determina instantaneamente o estado do(s) outro(s) qubit(s) correlacionado(s), independentemente da distância. Não é uma mera correlação baseada em informação preexistente, mas uma interdependência quântica. Como enfatizam Nielsen e Chuang (2010), o entrelaçamento é um recurso computacional essencial, permitindo que a informação seja distribuída de uma forma que não tem análogo clássico.**

**Essa correlação instantânea e robusta entre qubits entrelaçados é fundamental para a criação de algoritmos quânticos que exploram a interdependência dos qubits para resolver problemas complexos. Por exemplo, no algoritmo de Shor para fatoração de números primos, o entrelaçamento permite que o computador quântico explore múltiplas possibilidades simultaneamente e encontre a resposta de forma eficiente (Shor, 1994). O entrelaçamento é a base para o processamento de informações que transcende as capacidades dos computadores clássicos, possibilitando que as operações em um qubit afetem e revelem informações sobre outros qubits entrelaçados, o que é vital para a eficiência de certas operações quânticas e para a exploração de espaços de solução vastos.**

**3.1.3 Interferência Quântica**

**A interferência quântica é um princípio fundamental que capacita os algoritmos quânticos a extraírem informações úteis das superposições de estados. Essencialmente, ela permite que as probabilidades de diferentes resultados de um cálculo sejam seletivamente reforçadas ou canceladas. Esse fenômeno é análogo à forma como as ondas (como ondas de luz ou som) interagem: quando duas ondas se encontram, elas podem se somar para criar uma onda de maior amplitude (interferência construtiva) ou se anular mutuamente (interferência destrutiva).**

**No contexto da computação quântica, os algoritmos são projetados para manipular os qubits de tal maneira que os "caminhos" que levam às soluções corretas para um problema experimentem interferência construtiva, aumentando suas probabilidades de serem medidos. Em contra partida, os "caminhos" que levariam a soluções incorretas são submetidos à interferência destrutiva, diminuindo drasticamente suas probabilidades. Como descrevem Nielsen e Chuang (2010), a interferência é o mecanismo que permite aos algoritmos quânticos "navegar" no vasto espaço de superposições de maneira eficiente, amplificando as amplitudes de probabilidade dos estados desejados e minimizando as dos indesejados.**

**Esse controle preciso sobre as amplitudes de probabilidade é o que confere aos computadores quânticos sua capacidade de resolver certos problemas de forma mais eficiente do que os computadores clássicos. Por exemplo, no algoritmo de Grover para busca em bancos de dados não ordenados, a interferência é usada para amplificar a probabilidade de encontrar o item desejado, reduzindo significativamente o número de passos de busca em comparação com qualquer algoritmo clássico (Grover, 1996). Assim, a interferência quântica atua como um filtro poderoso, destacando as soluções corretas em meio a um oceano de possibilidades.**

**3.2 Aplicações Potenciais da Computão Quântica**

**A computação quântica é um campo em rápida evolução, e desdobrar mais assuntos significa aprofundar em seus fundamentos, aplicações, desafios e o ecossistema que a rodeia.**

**3.2.1 Otimização e o Problema do Caixeiro Viajante**

**Um dos campos mais promissores para a aplicação da computação quântica é a otimização. Problemas dessa natureza, como o clássico Problema do Caixeiro Viajante (PCV), que busca a rota mais eficiente entre múltiplos pontos, são classificados como NP-difíceis, ou seja, sua complexidade computacional cresce exponencialmente com o tamanho do problema, tornando-os inviáveis para computadores clássicos em larga escala. A computação quântica, por meio de algoritmos como o Quantum Approximate Optimization Algorithm (QAOA), oferece uma abordagem promissora para explorar o espaço de soluções de forma significativamente mais eficiente. Conforme demonstrado por Farhi et al. (2014), o QAOA pode ser aplicado a problemas de otimização combinatória, mostrando potencial para encontrar soluções ótimas ou quase ótimas. Essa capacidade tem implicações diretas para otimizar rotas de entrega e logística, cadeias de suprimentos complexas e até mesmo a distribuição de recursos em redes de comunicação ou energia, conforme discutido por Montanaro (2016) sobre as aplicações gerais de algoritmos quânticos.**

**3.2.2 Descoberta de Materiais e Farmacologia**

**No campo da química e ciência dos materiais, a capacidade da computação quântica de simular com precisão o comportamento de moléculas e reações químicas em nível atômico é um avanço notável. Isso se deve à natureza quântica fundamental das interações moleculares, que computadores clássicos simulam com dificuldade crescente à medida que a complexidade da molécula aumenta. Como apontado por Aspuru-Guzik e Walther (2005), a simulação quântica pode acelerar significativamente a descoberta de novos materiais com propriedades desejadas, como supercondutores e catalisadores, e o desenvolvimento de novos medicamentos, ao permitir um entendimento mais profundo de como as moléculas interagem com alvos biológicos em um nível fundamental.**

**3.2.3 Criptografia e Segurança da Informação**

**A computação quântica tem implicações profundas para a criptografia e a segurança da informação. O advento de algoritmos quânticos como o de Shor (Shor, 1994) demonstra a capacidade de fatorar números primos grandes de forma eficiente, o que representa uma ameaça direta à segurança dos sistemas de criptografia de chave pública amplamente utilizados atualmente, como o RSA. Essa perspectiva tem impulsionado intensas pesquisas em criptografia pós-quântica, que visa desenvolver e implementar métodos de segurança que sejam resistentes a ataques de computadores quânticos em larga escala (Chen et al., 2016).**

**3.2.4 Inteligência Artificial e Aprendizado de Máquina**

**A convergência da computação quântica com a inteligência artificial (IA) e o aprendizado de máquina (ML), conhecida como aprendizado de máquina quântico, é uma área emergente com grande potencial. Algoritmos quânticos podem, em tese, acelerar o treinamento de modelos de aprendizado de máquina, otimizar redes neurais e processar grandes volumes de dados de maneiras que os computadores clássicos não conseguem. Conforme explorado por Biamonte et al. (2017), essa combinação pode abrir novas fronteiras para a análise de dados, reconhecimento de padrões e até mesmo para o desenvolvimento de IA mais avançada, aproveitando a capacidade dos computadores quânticos de explorar espaços de dados complexos de forma mais eficiente.**

**3.3 Desafios atuais**

**Apesar de seu imenso potencial transformador, a computação quântica ainda se encontra em seus estágios iniciais de desenvolvimento, confrontando desafios significativos que precisam ser superados para sua plena materialização e aplicação em larga escala.**

**3.3.1 Decoerência e Correção de Erros Quânticos**

**Um dos maiores obstáculos enfrentados na construção de computadores quânticos robustos é a decoerência. Esse fenômeno refere-se à perda das propriedades quânticas dos qubits devido à interação indesejada com o ambiente, como flutuações de temperatura ou campos eletromagnéticos (Preskill, 1998). A sensibilidade dos qubits ao ruído ambiental limita drasticamente a vida útil de seus estados quânticos coerentes e, consequentemente, restringe o tempo de execução dos algoritmos quânticos. Para mitigar os efeitos da decoerência e permitir a computação quântica de grande escala, são indispensáveis técnicas de correção de erros quânticos (QEC). No entanto, essas técnicas são extraordinariamente complexas e exigem um número substancial de qubits físicos redundantes para codificar um único qubit lógico tolerante a falhas, o que representa um desafio complexo em termos de engenharia e escalabilidade (Gottesman, 1997).**

**3.3.2 Escalabilidade e Desenvolvimento de Hardware Quântico**

**A construção de computadores quânticos que possuam um grande número de qubits de alta qualidade e com baixas taxas de erro permanece um desafio de engenharia monumental. Atualmente, diversas tecnologias de hardware estão sendo ativamente exploradas, incluindo qubits supercondutores (Arute et al., 2019), íons presos (Cirac & Zoller, 1995), átomos neutros (Saffman et al., 2010) e qubits topológicos (Kitaev, 2003), cada qual apresentando vantagens e desvantagens distintas em termos de escalabilidade, coerência e conectividade. A fase tecnológica atual é frequentemente referida como a era NISQ (Noisy Intermediate-Scale Quantum). Essa denominação, cunhada por Preskill (2018), caracteriza os dispositivos quânticos existentes por possuírem um número limitado de qubits (tipicamente entre 50 e 100) e serem intrinsecamente suscetíveis a erros, o que impõe restrições significativas sobre a complexidade e a profundidade dos algoritmos que podem ser executados com fidelidade.**

**3.3.3 Desenvolvimento de Algoritmos Quânticos Práticos e Vantagem Quântica**

**Embora existam algoritmos quânticos teóricos que prometem acelerações exponenciais sobre seus equivalentes clássicos, como o algoritmo de Shor para fatoração de números primos (Shor, 1994) e o algoritmo de Grover para busca em bancos de dados não ordenados (Grover, 1996), o desenvolvimento de algoritmos quânticos práticos que demonstrem uma vantagem quântica (quantum advantage) real e convincente para problemas de relevância no mundo real ainda está em fase de intensa pesquisa e desenvolvimento. Muitas das pesquisas atuais concentram-se em identificar e otimizar algoritmos que possam explorar as capacidades dos dispositivos NISQ para resolver classes específicas de problemas onde os computadores clássicos enfrentam limitações severas (Bharti et al., 2021). A demonstração de uma vantagem quântica inequívoca para um problema útil e não-trivial é um marco crucial para a validação e o avanço contínuo do campo.**