



**Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
Campus Sertãozinho**

Guilherme Santos da Silveira, Victoria de Oliveira Spagiari

Aplicação de Sistemas Inteligentes para a Detecção de Fraudes em Redes Elétricas

Sertãozinho

2024

1 INTRODUÇÃO

1.1 Histórico da computação

2 REFERENCIAL TEÓRICO

2.1 Computação: fundamentos e evolução histórica

2.1.1 Definição geral de computação

De forma ampla, a computação pode ser definida como o conjunto de processos pelos quais um sistema recebe entradas, realiza algum tipo de processamento sobre essas informações e produz saídas (KAISER; GRANADE, 2021). Essa definição independe da natureza física do sistema computacional, sendo válida tanto para dispositivos mecânicos quanto eletrônicos ou digitais. O processamento pode envolver operações aritméticas, lógicas, simbólicas ou algorítmicas, desde que exista uma transformação bem definida entre os dados de entrada e os resultados obtidos na saída.

Sob essa perspectiva, a computação não se restringe aos computadores modernos, mas abrange qualquer mecanismo capaz de executar regras sistemáticas para manipulação de informação. Essa visão permite compreender a computação como um conceito anterior e mais amplo do que os próprios computadores digitais.

2.1.2 Computação antes dos computadores digitais

Muito antes do surgimento dos computadores eletrônicos, diferentes ferramentas e métodos foram desenvolvidos para auxiliar o ser humano em tarefas computacionais (CAMPBELL-KELLY et al., 2023). Um dos exemplos mais antigos é o ábaco, utilizado por diversas civilizações como instrumento para realizar operações aritméticas básicas. Embora simples, o ábaco já incorpora a ideia fundamental de representação e manipulação sistemática de informações.

Durante os séculos seguintes, surgiram dispositivos mecânicos mais sofisticados, como as máquinas de cálculo de Blaise Pascal e Gottfried Wilhelm Leibniz, capazes de executar automaticamente somas, subtrações e, em alguns casos, multiplicações e divisões. Paralelamente, grande parte dos cálculos científicos e de engenharia continuava sendo realizada manualmente, frequentemente com o auxílio de tabelas matemáticas e métodos numéricos.

Esses exemplos evidenciam que a computação, entendida como processamento de informação, antecede a computação digital moderna, sendo impulsionada por necessidades práticas nas áreas de comércio, ciência, engenharia e navegação.

2.1.3 Surgimento dos computadores digitais

O avanço tecnológico do século XX possibilitou a transição da computação mecânica para a computação eletromecânica e, posteriormente, eletrônica. Os primeiros computadores eletromecânicos utilizavam relés para implementar operações lógicas e aritméticas, enquanto os computadores eletrônicos passaram a empregar válvulas a vácuo, permitindo velocidades de processamento significativamente maiores.

Um exemplo histórico emblemático é o uso de máquinas computacionais no contexto da Segunda Guerra Mundial, especialmente nos esforços de criptoanálise. A máquina Enigma, utilizada para cifrar comunicações militares, representava um problema computacional de grande complexidade para a época ([HODGES, 2014](#)). O desenvolvimento de métodos sistemáticos e máquinas especializadas para quebrar suas cifras ilustra de forma clara como a computação passou a desempenhar um papel estratégico na resolução de problemas reais de alta relevância prática.

Esse período marca o início da computação digital como uma ferramenta central para lidar com problemas que extrapolavam a capacidade do cálculo manual ou puramente mecânico.

Após o surgimento dos primeiros computadores eletrônicos, a computação clássica passou por uma evolução acelerada, impulsionada principalmente por avanços no hardware. As válvulas a vácuo foram gradualmente substituídas por transistores, que ofereciam maior confiabilidade, menor consumo de energia e maior densidade de integração. Posteriormente, o desenvolvimento dos circuitos integrados permitiu a miniaturização e a integração de um número crescente de componentes em um único chip.

Esse avanço tecnológico é frequentemente associado à chamada Lei de Moore ([MOORE et al., 1965](#)), que observa o crescimento aproximadamente exponencial do número de transistores em circuitos integrados ao longo do tempo. Como consequência, houve um aumento contínuo no poder computacional disponível, tanto em termos de velocidade quanto de capacidade de armazenamento.

Além do aumento da densidade de componentes, a computação clássica também evoluiu por meio do paralelismo, explorando arquiteturas com múltiplos núcleos, processamento vetorial e sistemas distribuídos. Essas estratégias permitiram ganhos adicionais de desempenho, especialmente para aplicações que podem ser decompostas em tarefas paralelas.

2.1.4 Limitações da computação clássica

Apesar dos avanços expressivos, a computação clássica enfrenta limitações fundamentais quando aplicada a determinados tipos de problemas. Em muitos casos, o número de estados possíveis cresce exponencialmente com o tamanho do problema, tornando

inviável a exploração exaustiva de todas as soluções em tempo razoável.

A teoria da complexidade computacional formaliza essas limitações por meio de classes como P, NP, NP-difícil e NP-completo (SIPSER, 1996). Problemas pertencentes à classe P admitem soluções eficientes em tempo polinomial, enquanto problemas NP-completos, embora fáceis de verificar, não possuem algoritmos conhecidos que os resolvam eficientemente em computadores clássicos.

Exemplos práticos incluem problemas de otimização combinatória, como o problema do caixeiro viajante, a fatoração de grandes números inteiros e certos problemas de simulação de sistemas físicos complexos. Na prática, mesmo com hardware moderno e técnicas avançadas de paralelismo, esses problemas rapidamente se tornam intratáveis à medida que sua dimensão aumenta.

As limitações da computação clássica motivam a busca por novos paradigmas computacionais capazes de lidar de forma mais eficiente com problemas de alta complexidade. Em particular, há classes de problemas cuja estrutura sugere que abordagens baseadas exclusivamente em bits clássicos e operações determinísticas podem não ser suficientes.

Nesse contexto, surgem modelos alternativos de computação, como a computação quântica, que exploram princípios físicos distintos para representar e processar informações. Esses modelos não substituem a computação clássica, mas oferecem novas ferramentas conceituais e práticas para enfrentar problemas que “pedem” um novo tipo de tratamento computacional, abrindo caminho para avanços em áreas como criptografia, otimização e simulação de sistemas complexos.

2.2 Limites da computação clássica e motivação para novos paradigmas

2.2.1 Limitações tecnológicas versus limitações teóricas

Ao longo da história da computação, muitos obstáculos foram superados por meio de avanços tecnológicos, como o aumento da velocidade dos processadores, a miniaturização dos componentes eletrônicos e o aprimoramento das arquiteturas computacionais. Essas limitações, de natureza tecnológica, estão associadas a restrições práticas de engenharia e tendem a ser mitigadas com o progresso científico e industrial.

Porém, nem todas as limitações enfrentadas pela computação clássica podem ser superadas por avanços tecnológicos, existem barreiras de natureza teórica, intrínsecas ao próprio modelo computacional clássico, baseado na manipulação de bits e em operações determinísticas ou probabilísticas.

Essas limitações persistem mesmo quando se considera um computador ideali-

zado, capaz de executar operações em tempo arbitrariamente pequeno e com memória ilimitada. Nesses casos, o fator limitante não é a velocidade de cada operação individual, mas o crescimento do número total de operações necessárias para resolver determinados problemas.

Um exemplo paradigmático é o problema do logaritmo discreto (SHOR, 1994). Dado um grupo finito, um gerador g e um elemento h , o objetivo é encontrar o expoente x tal que $g^x = h$. Apesar de sua formulação simples, não existem algoritmos clássicos conhecidos que resolvam esse problema em tempo polinomial, mesmo considerando paralelismo clássico extremo. O melhor desempenho clássico conhecido ainda apresenta crescimento subexponencial, tornando o problema intratável para instâncias de grande porte. Assim, a dificuldade do logaritmo discreto ilustra um limite estrutural do modelo clássico de computação, e não apenas uma limitação tecnológica.

2.2.2 Crescimento exponencial do espaço de estados e exemplos computacionais

O crescimento exponencial do espaço de estados está no cerne de diversos problemas computacionais relevantes. Na teoria da complexidade, esse fenômeno aparece de forma clara em problemas pertencentes às classes NP-difícil e NP-completo (SIPSER, 1996), nos quais o número de soluções candidatas cresce combinatorialmente com o tamanho do problema.

O problema do caixeiro viajante (*Traveling Salesman Problem* – TSP) é um exemplo clássico. Dado um conjunto de cidades e as distâncias entre elas, o objetivo é encontrar o caminho de menor custo que visite cada cidade exatamente uma vez. A versão de decisão do problema é NP-completa, e a versão de otimização é NP-difícil. Na prática, instâncias de grande porte são tratadas por meio de heurísticas e algoritmos aproximados, como algoritmos genéticos ou *simulated annealing* (KIRKPATRICK; JR; VECCHI, 1983), que produzem boas soluções, mas sem garantia de otimalidade global.

Outro exemplo de grande relevância é o problema da fatoração de números inteiros grandes, base de sistemas criptográficos como o RSA (RIVEST; SHAMIR; ADLEMAN, 1978). Embora não se saiba se esse problema é NP-completo, ele não admite algoritmos clássicos eficientes conhecidos. Nesse caso, a computação quântica oferece uma vantagem estrutural: o algoritmo de Shor (SHOR, 1994) demonstra que a fatoração pode ser realizada em tempo polinomial em um computador quântico, evidenciando que o obstáculo não está apenas no hardware, mas no modelo computacional utilizado.

Essas dificuldades tornam-se ainda mais pronunciadas na simulação de sistemas físicos quânticos. Um sistema composto por n partículas quânticas requer a descrição de um estado em um espaço de dimensão proporcional a 2^n . Como consequência, a simulação

exata desses sistemas em computadores clássicos torna-se rapidamente inviável, mesmo para valores modestos de n , reforçando a ideia de que certos problemas apresentam uma incompatibilidade fundamental com o paradigma clássico de computação.

2.2.3 Computação não-clássica e a motivação física de Feynman

Diante dessas limitações estruturais, surgem propostas de paradigmas de computação não-clássica, que buscam explorar modelos físicos alternativos para representar e processar informação. A computação analógica utiliza grandezas contínuas e a dinâmica natural de sistemas físicos para realizar cálculos, enquanto a computação neuromórfica inspira-se na organização do cérebro, explorando paralelismo massivo e adaptação.

Entre esses paradigmas, a computação quântica se destaca por sua fundamentação direta nas leis da mecânica quântica. Em vez de tentar simular sistemas quânticos por meio de bits clássicos, a computação quântica propõe utilizar sistemas quânticos controlados como elementos computacionais, explorando propriedades como superposição, interferência e emaranhamento.

Essa ideia foi articulada de forma pioneira por Richard Feynman ([FEYNMAN, 2018](#)), ao observar que a dificuldade de simular sistemas quânticos em computadores clássicos não é acidental, mas resulta do fato de que a natureza não opera segundo as regras da computação clássica. Assim, a computação quântica surge não apenas como uma alternativa tecnológica, mas como um novo paradigma conceitual, alinhado à própria estrutura física dos sistemas que se deseja estudar.

2.3 Fundamentos de Mecânica Quântica para Computação

Este capítulo apresenta os conceitos essenciais da mecânica quântica necessários para a compreensão da computação quântica. O objetivo não é desenvolver a teoria completa da mecânica quântica, mas introduzir apenas os elementos matemáticos e conceituais que fundamentam o modelo computacional quântico, conforme apresentado em referências clássicas como ([NIELSEN; CHUANG, 2010](#)) e ([WATROUS, 2018](#)).

2.3.1 Espaços Vetoriais Complexos

A formulação matemática da mecânica quântica é baseada em espaços vetoriais complexos. Em computação quântica, os estados físicos de sistemas quânticos são representados por vetores em um espaço vetorial complexo de dimensão finita, usualmente um espaço de Hilbert.

Um espaço vetorial complexo é definido sobre o corpo dos números complexos \mathbb{C} ,

permitindo combinações lineares do tipo

$$\alpha |v\rangle + \beta |w\rangle, \quad \alpha, \beta \in \mathbb{C}. \quad (2.1)$$

Além disso, esse espaço é equipado com um produto interno, que permite definir normas, ângulos e projeções, elementos fundamentais para a interpretação probabilística da teoria quântica.

2.3.2 Estados Quânticos e Notação de Dirac

Estados quânticos puros são representados por vetores normalizados em um espaço de Hilbert complexo. A notação mais comum para representar esses vetores é a notação de Dirac, ou notação bra-ket.

Um vetor de estado é denotado por um *ket*, como $|\psi\rangle$, enquanto seu conjugado transposto é denotado por um *bra*, $\langle\psi|$. O produto interno entre dois estados é escrito como

$$\langle\phi|\psi\rangle. \quad (2.2)$$

No contexto da computação quântica, o sistema mais básico é o *qubit*, cujo estado geral pode ser escrito como

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (2.3)$$

onde $\alpha, \beta \in \mathbb{C}$ e satisfazem a condição de normalização

$$|\alpha|^2 + |\beta|^2 = 1. \quad (2.4)$$

2.3.3 Superposição

A superposição é uma das características centrais da mecânica quântica e não possui análogo direto na computação clássica. Enquanto um bit clássico assume apenas os valores 0 ou 1, um qubit pode estar em uma combinação linear desses dois estados.

Essa propriedade permite que sistemas quânticos representem simultaneamente múltiplos estados clássicos, o que é fundamental para o paralelismo quântico explorado por algoritmos quânticos.

É importante ressaltar que a superposição não implica que o sistema possui simultaneamente ambos os valores clássicos de forma observável, mas sim que seu estado físico é descrito por uma combinação coerente desses estados.

2.3.4 Probabilidade e Amplitudes

Diferentemente da computação clássica, na qual probabilidades são atribuídas diretamente aos estados, na mecânica quântica as probabilidades são obtidas a partir das amplitudes complexas associadas aos estados.

Dado um estado

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (2.5)$$

a probabilidade de obter o resultado $|0\rangle$ em uma medição é $|\alpha|^2$, enquanto a probabilidade de obter $|1\rangle$ é $|\beta|^2$.

As amplitudes complexas permitem fenômenos exclusivamente quânticos, como interferência construtiva e destrutiva, que desempenham papel central em algoritmos quânticos como o de Shor e o de Grover.

2.3.5 Medição e Colapso do Estado

A medição em mecânica quântica é um processo fundamentalmente probabilístico. Ao medir um sistema quântico, o estado do sistema colapsa para um dos estados da base associada ao observável medido.

No caso de um qubit medido na base computacional $\{|0\rangle, |1\rangle\}$, o estado $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ colapsa para $|0\rangle$ com probabilidade $|\alpha|^2$ ou para $|1\rangle$ com probabilidade $|\beta|^2$.

Após a medição, a superposição é destruída, e medições subsequentes produzem o mesmo resultado com probabilidade unitária. Esse comportamento distingue claramente a evolução unitária dos sistemas quânticos do processo de medição.

2.3.6 Sistemas Compostos e Produto Tensorial

Para descrever sistemas quânticos compostos por múltiplos subsistemas, utiliza-se o produto tensorial de espaços vetoriais. Se dois sistemas possuem espaços de estados \mathcal{H}_A e \mathcal{H}_B , o espaço de estados do sistema composto é dado por

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B. \quad (2.6)$$

No caso de dois qubits, os estados base do sistema composto são

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}. \quad (2.7)$$

O produto tensorial é essencial para representar correlações quânticas entre subsistemas e constitui a base matemática para o estudo do emaranhamento.

2.3.7 Emaranhamento Quântico

O emaranhamento é um fenômeno exclusivamente quântico no qual o estado de um sistema composto não pode ser escrito como o produto tensorial dos estados de seus subsistemas.

Um exemplo clássico de estado emaranhado é o estado de Bell

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (2.8)$$

Nesse estado, nenhuma descrição individual dos subsistemas é suficiente para caracterizar o sistema completo. Medições realizadas em um subsistema afetam instantaneamente as probabilidades associadas ao outro, independentemente da distância entre eles.

O emaranhamento é um recurso fundamental para a computação quântica, sendo explorado em protocolos como teleportação quântica, correção de erros quânticos e aceleração algorítmica.

2.4 Qubits e Informação Quântica

Esta seção tem como objetivo formalizar o conceito de qubit e introduzir os fundamentos da informação quântica. Embora conceitos como superposição e medição já tenham sido apresentados anteriormente, aqui eles são tratados de forma mais sistemática, estabelecendo a base conceitual necessária para o estudo de circuitos quânticos, algoritmos e canais quânticos.

2.4.1 Definição Formal de Qubit

O bit quântico (*quantum bit*), ou qubit, é a unidade fundamental de informação na computação quântica. Matematicamente, um qubit é definido como um vetor unitário pertencente a um espaço de Hilbert complexo bidimensional, usualmente denotado por \mathbb{C}^2 .

Escolhendo a base computacional $\{|0\rangle, |1\rangle\}$, qualquer estado puro de um qubit pode ser escrito como

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (2.9)$$

onde $\alpha, \beta \in \mathbb{C}$ e satisfazem a condição de normalização

$$|\alpha|^2 + |\beta|^2 = 1. \quad (2.10)$$

Essa definição formal diferencia o qubit de um bit clássico. Enquanto o bit clássico assume um valor determinístico 0 ou 1, o qubit é descrito por amplitudes complexas, cuja interpretação física está associada às probabilidades de resultados de medições.

2.4.2 Representação Geométrica: Esfera de Bloch

A representação geométrica dos estados de um qubit é frequentemente feita por meio da Esfera de Bloch. Nessa representação, todo estado puro de um qubit corresponde a um ponto sobre a superfície de uma esfera unitária.

Qualquer estado $|\psi\rangle$ pode ser parametrizado como

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle, \quad (2.11)$$

com $\theta \in [0, \pi]$ e $\phi \in [0, 2\pi)$.

Os polos da esfera correspondem aos estados da base computacional, com $|0\rangle$ no polo norte e $|1\rangle$ no polo sul. Estados em superposição correspondem a pontos intermediários, enquanto a fase relativa ϕ representa rotações em torno do eixo z .

A Esfera de Bloch fornece uma visualização intuitiva para operações unitárias de um único qubit, que se manifestam como rotações da esfera.

2.4.3 Estados Puros e Estados Mistos

Estados quânticos podem ser classificados em estados puros e estados mistos. Estados puros são aqueles que podem ser descritos por um único vetor de estado $|\psi\rangle$, conforme apresentado anteriormente.

Estados mistos surgem quando há incerteza clássica sobre qual estado puro descreve o sistema ou quando o sistema está correlacionado com um ambiente externo. Esses estados são descritos formalmente pelo operador densidade ρ , definido como

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|, \quad (2.12)$$

onde $\{p_i\}$ é uma distribuição de probabilidades clássica.

Estados puros correspondem a operadores densidade do tipo $\rho = |\psi\rangle \langle \psi|$, enquanto estados mistos satisfazem $\text{Tr}(\rho^2) < 1$. A formulação por operadores densidade é essencial para a descrição de sistemas abertos, ruído e canais quânticos.

2.4.4 Medidas Projetivas

A medição em mecânica quântica é descrita formalmente por operadores de medição. No caso mais simples, consideram-se medidas projetivas, associadas a um conjunto de projetores ortogonais $\{P_i\}$ que satisfazem

$$P_i P_j = \delta_{ij} P_i, \quad \sum_i P_i = I. \quad (2.13)$$

A probabilidade de obter o resultado associado ao projetor P_i , quando o sistema está no estado ρ , é dada pela regra de Born:

$$p(i) = \text{Tr}(P_i \rho). \quad (2.14)$$

Após a medição, o estado do sistema colapsa para

$$\rho' = \frac{P_i \rho P_i}{\text{Tr}(P_i \rho)}. \quad (2.15)$$

No contexto da computação quântica, a medição mais comum é realizada na base computacional, correspondendo aos projetores $|0\rangle\langle 0|$ e $|1\rangle\langle 1|$.

2.4.5 Comparação entre Bit Clássico e Qubit

A diferença entre um bit clássico e um qubit não se limita à possibilidade de superposição. Um bit clássico pode ser descrito completamente por uma variável binária ou, em contextos probabilísticos, por uma distribuição de probabilidades clássica.

O qubit, por sua vez, é descrito por amplitudes complexas, o que permite fenômenos como interferência quântica. Além disso, estados quânticos não podem ser copiados arbitrariamente, conforme estabelecido pelo teorema da não clonagem, e a medição altera inevitavelmente o estado do sistema.

Essas diferenças impõem restrições e, simultaneamente, oferecem novos recursos computacionais que não possuem análogos clássicos.

2.4.6 Informação Clássica versus Informação Quântica

A distinção entre informação clássica e informação quântica vai além da forma de representação dos dados, estando profundamente ligada às leis físicas que governam cada modelo computacional. Na computação clássica, a informação é codificada em bits que assumem valores bem definidos, 0 ou 1, e podem ser copiados, lidos e manipulados sem alterar seu conteúdo.

Em contextos probabilísticos clássicos, a incerteza está associada apenas à falta de conhecimento do observador, sendo possível descrever completamente o sistema por meio de distribuições de probabilidade sobre estados determinísticos.

Na computação quântica, por outro lado, a informação é armazenada em estados quânticos, descritos por vetores de estado ou operadores densidade. Esses estados podem existir em superposição e apresentar correlações não clássicas, como o emaranhamento. Diferentemente do caso clássico, a incerteza quântica é intrínseca ao sistema e não pode ser interpretada apenas como desconhecimento do observador.

Além disso, a informação quântica está sujeita a restrições fundamentais. O teorema da não clonagem estabelece que não é possível copiar arbitrariamente um estado quântico desconhecido, e o processo de medição altera inevitavelmente o estado do sistema, causando o colapso da superposição.

Essas características impõem novos paradigmas computacionais. Algoritmos quânticos devem ser cuidadosamente projetados para explorar propriedades como superposição, interferência e emaranhamento, ao mesmo tempo em que minimizam medições intermediárias que destruiriam a informação quântica relevante antes da obtenção do resultado final.

2.4.6.1 Entropia Quântica

A entropia quântica, conhecida como entropia de von Neumann, generaliza a entropia de Shannon para estados quânticos. Ela é definida como

$$S(\rho) = -\text{Tr}(\rho \log \rho). \quad (2.16)$$

Para estados puros, a entropia é nula, refletindo a ausência de incerteza. Para estados mistos, a entropia é positiva e quantifica o grau de mistura ou incerteza do estado.

2.4.6.2 Canal Quântico

Um canal quântico descreve a evolução mais geral possível de um estado quântico, incluindo efeitos de ruído e interação com o ambiente. Formalmente, um canal quântico é uma aplicação linear completamente positiva e preservadora de traço, que mapeia operadores densidade em operadores densidade.

Canais quânticos são fundamentais para o estudo de comunicação quântica, correção de erros e limitações físicas da computação quântica em sistemas reais.

2.5 Portas Lógicas Quânticas e Circuitos Quânticos

Esta seção apresenta como a computação quântica é operacionalizada na prática por meio de portas lógicas quânticas e circuitos quânticos. Enquanto capítulos anteriores introduziram os fundamentos físicos e matemáticos dos estados quânticos, aqui o foco recai sobre os mecanismos que permitem manipular esses estados de forma controlada para realizar computação.

2.5.1 Portas Quânticas como Operadores Unitários

Na computação quântica, a manipulação da informação é realizada por meio de portas lógicas quânticas, que correspondem a operadores lineares unitários atuando sobre o espaço de estados do sistema. A evolução de um sistema quântico isolado é descrita por operadores unitários U que satisfazem

$$U^\dagger U = U U^\dagger = I. \quad (2.17)$$

A unitariedade garante a preservação da norma do vetor de estado, assegurando que as probabilidades associadas aos resultados de medição permaneçam normalizadas. Diferentemente das portas clássicas, que operam sobre valores discretos, portas quânticas transformam amplitudes complexas, permitindo interferência construtiva e destrutiva.

Portas de múltiplos qubits são responsáveis por criar correlações quânticas entre subsistemas, incluindo o emaranhamento, e não possuem equivalente direto na computação clássica. De forma geral, todo operador linear que atua em um espaço vetorial de dimensão n pode ser representado por uma matriz $n \times n$.

Como o espaço de estados de um sistema composto por n qubits possui dimensão 2^n , as portas lógicas quânticas que atuam sobre esse sistema podem ser representadas, de forma genérica, por matrizes unitárias $2^n \times 2^n$. Esse crescimento exponencial da dimensão do espaço de estados é uma característica central da computação quântica e está diretamente relacionado ao seu potencial computacional.

A figura 1 contém a representação gráfica, além da representação matricial de algumas das portas lógicas quânticas mais comuns, que serão detalhadas nas subseções a seguir

2.5.2 Portas de Um Qubit

Portas de um qubit correspondem a operadores unitários 2×2 e podem ser interpretadas geometricamente como rotações da Esfera de Bloch.

2.5.2.1 Porta Pauli-X

A porta Pauli-X atua como o análogo quântico da porta NOT clássica, trocando os estados $|0\rangle$ e $|1\rangle$. Sua representação matricial é

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2.18)$$

Na Esfera de Bloch, essa porta corresponde a uma rotação de π em torno do eixo x .

2.5.2.2 Porta Pauli-Y

A porta Pauli-Y combina uma inversão de estado com uma mudança de fase, sendo representada por

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (2.19)$$

Essa porta corresponde a uma rotação de π em torno do eixo y da Esfera de Bloch.

2.5.2.3 Porta Pauli-Z

A porta Pauli-Z não altera as probabilidades associadas aos estados da base computacional, mas modifica a fase relativa entre eles. Sua matriz é

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.20)$$

Geometricamente, essa operação corresponde a uma rotação de π em torno do eixo z .

2.5.2.4 Porta de Hadamard

A porta de Hadamard desempenha um papel central na computação quântica, pois cria superposição a partir de estados da base computacional. Sua representação matricial é

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2.21)$$

Aplicada ao estado $|0\rangle$, a porta Hadamard produz

$$H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad (2.22)$$

e aplicada a $|1\rangle$, resulta em

$$H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (2.23)$$

Essa capacidade de gerar interferência controlada torna a porta Hadamard essencial em algoritmos quânticos.

2.5.2.5 Portas de Fase (S e T)

As portas de fase modificam exclusivamente a fase relativa dos estados quânticos. A porta S é definida por

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad (2.24)$$

enquanto a porta T , também conhecida como porta $\pi/8$, é dada por

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \quad (2.25)$$

Essas portas são essenciais para a universalidade da computação quântica, pois permitem a geração de rotações que não podem ser obtidas apenas com portas de Clifford.

2.5.3 Portas de Múltiplos Qubits

Portas de múltiplos qubits são responsáveis por criar correlações quânticas entre subsistemas, incluindo o emaranhamento, e não possuem equivalente direto na computação clássica.

2.5.3.1 Porta CNOT

A porta CNOT (Controlled-NOT) atua sobre dois qubits, um de controle e um alvo. O qubit alvo é invertido se, e somente se, o qubit de controle estiver no estado $|1\rangle$.

Em notação matricial, a porta CNOT pode ser representada por uma matriz 4×4 que atua sobre a base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Essa porta é fundamental para a criação de estados emaranhados e para a universalidade da computação quântica.

2.5.3.2 Porta CZ

A porta CZ (Controlled-Z) aplica uma mudança de fase ao estado $|11\rangle$, mantendo os demais estados inalterados. Embora seu efeito seja puramente de fase, a porta CZ também é capaz de gerar emaranhamento quando combinada com portas de um qubit.

2.5.3.3 Porta SWAP

A porta SWAP troca os estados de dois qubits. Embora não gere emaranhamento por si só, ela é importante para reorganizar qubits em arquiteturas físicas onde a conectividade é limitada.

2.5.3.4 Porta Toffoli

A porta Toffoli, ou CCNOT, é uma porta controlada por dois qubits que atua sobre um terceiro. Ela desempenha um papel central na computação reversível e estabelece uma ponte conceitual entre circuitos clássicos reversíveis e circuitos quânticos.

2.5.4 Construção de Circuitos Quânticos

Circuitos quânticos são representações gráficas que descrevem a sequência de portas aplicadas a um conjunto de qubits. Cada linha representa um qubit, e o tempo evolui da esquerda para a direita.

A computação quântica ocorre pela aplicação sequencial de operadores unitários, seguida por uma etapa de medição. Durante a execução do circuito, o sistema evolui de forma determinística segundo a mecânica quântica; a indeterminação surge apenas no momento da medição.











Operator	Gate(s)	Matrix
Pauli-X (X)	 \oplus	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Figura 1 – Conjunto de portas lógicas quânticas comumente utilizadas, incluindo portas de um qubit e de múltiplos qubits, suas representações em circuitos e respectivas matrizes unitárias.

2.5.5 Universalidade da Computação Quântica

Um conjunto de portas quânticas é dito universal se qualquer operador unitário pode ser aproximado arbitrariamente bem por uma sequência finita dessas portas.

Um exemplo de conjunto universal amplamente utilizado é composto por todas as portas de um qubit combinadas com a porta CNOT. Esse resultado é fundamental, pois garante que circuitos quânticos podem implementar qualquer computação quântica fisicamente realizável.

2.5.6 Circuitos Clássicos versus Circuitos Quânticos

Embora haja similaridade estrutural entre circuitos clássicos e quânticos, as diferenças conceituais são profundas. Circuitos clássicos operam sobre bits determinísticos e implementam funções booleanas irreversíveis.

Circuitos quânticos, por sua vez, devem ser reversíveis e são descritos por operadores unitários. Além disso, estados intermediários não podem ser observados sem alterar o resultado da computação, o que exige um planejamento cuidadoso da estrutura do circuito.

2.5.7 Medição ao Final do Circuito

Em um circuito quântico típico, a medição é realizada apenas ao final do processo computacional. Essa estratégia permite que a superposição e a interferência atuem

plenamente durante a execução do algoritmo.

A medição projeta o estado final do sistema em estados da base computacional, produzindo uma saída clássica que pode ser interpretada como o resultado da computação quântica.

2.6 Modelos de Computação Quântica e Algoritmos

Esta seção tem como objetivo conectar os fundamentos teóricos da computação quântica ao seu poder computacional. Para isso, são apresentados os principais modelos formais de computação quântica, seguidos pela descrição detalhada dos algoritmos quânticos mais representativos, destacando como propriedades específicas da mecânica quântica são exploradas para obter vantagens em relação à computação clássica.

2.6.1 Modelo de Circuitos Quânticos

O modelo de circuitos quânticos é o paradigma mais utilizado para descrever computações quânticas, especialmente em contextos experimentais e de implementação prática. Nesse modelo, a computação é representada por um circuito composto por três elementos principais: preparação do estado inicial, aplicação de uma sequência de portas quânticas unitárias e medição final.

Inicialmente, os qubits são preparados em um estado conhecido, tipicamente $|0\rangle^{\otimes n}$. Em seguida, portas quânticas são aplicadas de forma sequencial, promovendo a evolução unitária do sistema. Por fim, realiza-se a medição dos qubits, convertendo o estado quântico final em uma saída clássica.

Esse modelo é particularmente adequado para descrever algoritmos quânticos, pois torna explícito o papel da superposição, da interferência e do emaranhamento durante o processo computacional.

2.6.2 Máquina de Turing Quântica

A Máquina de Turing Quântica é uma generalização do modelo clássico de Máquina de Turing, na qual as transições são descritas por operadores unitários. Embora esse modelo seja fundamental do ponto de vista teórico, ele é menos utilizado na prática do que o modelo de circuitos.

Do ponto de vista computacional, ambos os modelos são equivalentes em termos de poder computacional. A importância da Máquina de Turing Quântica reside principalmente na formalização da classe de complexidade BQP (*Bounded-Error Quantum Polynomial Time*), que caracteriza os problemas eficientemente resolvíveis por computadores quânticos.

2.6.3 Algoritmos Quânticos

Algoritmos quânticos exploram propriedades específicas da mecânica quântica para resolver determinados problemas de forma mais eficiente do que qualquer algoritmo clássico conhecido. Entre essas propriedades destacam-se a superposição, a interferência e o emaranhamento.

2.6.3.1 Algoritmo de Shor

O algoritmo de Shor é um dos resultados mais emblemáticos da computação quântica, pois demonstra que um computador quântico pode fatorar números inteiros em tempo polinomial, enquanto os melhores algoritmos clássicos conhecidos requerem tempo subexponencial.

O problema da fatoração de inteiros pode ser reduzido ao problema da determinação do período de uma função. Dado um inteiro N a ser fatorado e um inteiro a coprimo com N , define-se a função

$$f(x) = a^x \bmod N. \quad (2.26)$$

Essa função é periódica, e a determinação eficiente de seu período permite extrair fatores não triviais de N com alta probabilidade.

A principal contribuição do computador quântico no algoritmo de Shor é a determinação do período da função $f(x)$. Para isso, o algoritmo utiliza um registrador quântico preparado em superposição de todos os valores possíveis de x , explorando o paralelismo quântico para avaliar a função simultaneamente para múltiplas entradas.

Em seguida, aplica-se a Transformada de Fourier Quântica (QFT), que explora interferência quântica para amplificar as amplitudes associadas aos estados que codificam informações sobre o período da função. A medição final fornece, com alta probabilidade, um valor a partir do qual o período pode ser inferido por métodos clássicos.

O ganho computacional do algoritmo de Shor decorre diretamente da capacidade do computador quântico de:

- Representar exponencialmente muitos valores simultaneamente por meio da superposição;
- Manipular fases complexas de forma controlada;
- Explorar interferência para extrair informação global sobre a função.

2.6.3.2 Algoritmo de Grover

O algoritmo de Grover aborda o problema da busca não estruturada. Dado um conjunto não ordenado de N elementos, deseja-se encontrar um elemento que satisfaça uma

determinada condição. Classicamente, esse problema requer, em média, $O(N)$ consultas.

O algoritmo de Grover resolve esse problema em $O(\sqrt{N})$ iterações, oferecendo uma aceleração quadrática em relação à computação clássica.

O algoritmo inicia preparando uma superposição uniforme de todos os estados possíveis:

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \quad (2.27)$$

Em seguida, aplica-se repetidamente o operador de Grover, composto por duas etapas: a aplicação de um oráculo quântico que inverte a fase do estado solução e a aplicação do operador de difusão, que realiza uma reflexão em torno da média das amplitudes.

Cada iteração do operador de Grover aumenta a amplitude do estado solução e reduz as amplitudes dos estados não desejados. Após aproximadamente $\pi\sqrt{N}/4$ iterações, a probabilidade de medir o estado correto torna-se próxima de 1.

O algoritmo de Grover explora de forma explícita a interferência quântica, utilizando inversões de fase e reflexões geométricas no espaço de estados para amplificar a solução desejada.

2.6.4 Noção de Vantagem Quântica

A vantagem quântica refere-se à capacidade de computadores quânticos resolverem determinados problemas de forma mais eficiente do que computadores clássicos. É importante destacar que essa vantagem não é universal, mas específica a certos problemas e algoritmos.

Algoritmos como os de Shor e Grover demonstram que, para classes específicas de problemas, a computação quântica oferece ganhos assintóticos claros. No entanto, muitos problemas computacionais permanecem igualmente difíceis ou até mais complexos no modelo quântico.

2.6.5 Limitações Práticas dos Algoritmos Quânticos

Apesar do potencial teórico dos algoritmos quânticos, sua implementação prática enfrenta limitações significativas. Entre elas destacam-se o ruído, a decoerência e a necessidade de correção de erros quânticos.

Além disso, algoritmos como o de Shor exigem um número elevado de qubits lógicos e circuitos profundos, o que ainda está além das capacidades dos dispositivos quânticos atuais. Essas limitações reforçam a distinção entre o potencial teórico da computação quântica e sua realização prática no estado atual da tecnologia.

2.7 Implementações Práticas e Ferramentas

Esta seção tem como objetivo discutir como a computação quântica é acessada na prática, quais são as limitações dos dispositivos atuais e quais ferramentas são utilizadas para a implementação e execução de circuitos quânticos.

2.7.1 Computação Quântica em Nuvem

Diferentemente da computação clássica, computadores quânticos ainda não são amplamente acessíveis como dispositivos locais. Atualmente, o principal meio de acesso a hardware quântico real é por meio de plataformas de computação em nuvem, oferecidas por empresas e instituições de pesquisa.

Nesse modelo, usuários podem submeter circuitos quânticos para execução em processadores quânticos remotos, utilizando interfaces de programação de alto nível. Essa abordagem permite que pesquisadores e estudantes experimentem algoritmos quânticos reais sem a necessidade de infraestrutura física própria, ao custo de lidar com limitações impostas pelo hardware disponível.

2.7.2 Simuladores Clássicos versus Hardware Quântico Real

Ferramentas de computação quântica geralmente oferecem dois ambientes distintos para execução de circuitos: simuladores clássicos e dispositivos quânticos reais.

Simuladores clássicos reproduzem a evolução exata de estados quânticos ideais, sem ruído ou decoerência. Eles são extremamente úteis para validação de algoritmos, depuração de circuitos e análise conceitual. No entanto, o custo computacional de simular sistemas quânticos cresce exponencialmente com o número de qubits, tornando simulações exatas inviáveis para sistemas maiores.

Por outro lado, hardware quântico real opera sob condições físicas imperfeitas, estando sujeito a ruído, erros de porta e decoerência. Embora limitado em escala e fidelidade, o uso de hardware real é essencial para avaliar o comportamento de algoritmos quânticos em cenários práticos e compreender os desafios da computação quântica contemporânea.

2.7.3 Introdução ao Qiskit

O Qiskit é um dos principais frameworks de software para computação quântica, amplamente utilizado tanto em contextos acadêmicos quanto industriais. Ele fornece uma interface de alto nível para a construção, simulação e execução de circuitos quânticos em hardware real ou simulado.

2.7.3.1 Construção de Circuitos Quânticos

No Qiskit, circuitos quânticos são construídos de forma programática, utilizando abstrações que refletem diretamente o modelo de circuitos quânticos apresentado anteriormente. Qubits e bits clássicos são alocados explicitamente, e portas quânticas são aplicadas de maneira sequencial.

Essa abordagem facilita a tradução direta de diagramas de circuitos quânticos para código executável, mantendo uma correspondência clara entre teoria e implementação.

2.7.3.2 Execução de Circuitos

Após a construção do circuito, o Qiskit permite sua execução tanto em simuladores quanto em dispositivos quânticos reais. No caso de simuladores, o resultado corresponde à evolução ideal do circuito. No caso de hardware real, o circuito é submetido a um processador quântico remoto, respeitando restrições como conectividade entre qubits e profundidade máxima do circuito.

A execução em hardware real geralmente envolve múltiplas repetições do circuito, chamadas de *shots*, a fim de estimar distribuições de probabilidade a partir das medições.

2.7.3.3 Medições

As medições no Qiskit são explicitamente especificadas no circuito, refletindo o modelo teórico no qual a medição é realizada ao final da computação. O resultado da execução consiste em contagens associadas aos diferentes resultados possíveis, que podem ser interpretadas como estimativas empíricas das probabilidades de medição.

Esse processo evidencia a natureza estatística da computação quântica, na qual resultados individuais são aleatórios, mas distribuições globais carregam a informação relevante.

2.7.4 Ruído e Mitigação de Erros

Dispositivos quânticos atuais operam no regime conhecido como NISQ (*Noisy Intermediate-Scale Quantum*), caracterizado por um número limitado de qubits e pela presença significativa de ruído.

Entre as principais fontes de erro estão a decoerência, erros de porta e erros de leitura. Esses efeitos distorcem o estado quântico durante a execução do circuito, reduzindo a fidelidade dos resultados obtidos.

Como a correção completa de erros quânticos ainda não é viável em dispositivos atuais, estratégias de mitigação de erros são frequentemente empregadas. Essas técnicas

não eliminam o ruído, mas buscam reduzir seu impacto nos resultados finais, permitindo extrair informações úteis mesmo em hardware imperfeito.

A compreensão dessas limitações é essencial para a correta interpretação de experimentos quânticos e para a avaliação realista do desempenho de algoritmos quânticos na prática.

2.8 Possíveis Áreas de Aplicação da Computação Quântica

Após a apresentação dos fundamentos teóricos, modelos computacionais e ferramentas práticas da computação quântica, esta seção tem como objetivo apresentar um panorama das principais áreas nas quais essa tecnologia tem sido investigada como potencialmente vantajosa. O intuito não é aprofundar cada aplicação, mas delinear caminhos possíveis e contextualizar a relevância da computação quântica em diferentes domínios científicos e tecnológicos.

2.8.1 Otimização Combinatória

Problemas de otimização combinatória estão presentes em diversas áreas, como logística, planejamento, alocação de recursos e redes de transporte. Esses problemas geralmente envolvem a busca por uma solução ótima em um espaço de soluções que cresce exponencialmente com o tamanho do problema.

A computação quântica é investigada como uma possível alternativa para tratar esses problemas por meio de algoritmos quânticos e híbridos, que exploram superposição e interferência para navegar no espaço de soluções. Embora não exista, até o momento, uma aceleração quântica universal comprovada para todos os problemas de otimização, abordagens quânticas têm sido propostas como heurísticas promissoras, especialmente em arquiteturas NISQ.

2.8.2 Simulação de Sistemas Físicos

A simulação de sistemas físicos é uma das motivações originais da computação quântica. Muitos sistemas quânticos, como materiais fortemente correlacionados e sistemas de muitos corpos, são intratáveis para simulação exata em computadores clássicos devido ao crescimento exponencial do espaço de estados.

Computadores quânticos, por operarem segundo as mesmas leis físicas que os sistemas a serem simulados, oferecem uma plataforma natural para esse tipo de tarefa. Simulações quânticas podem, em princípio, reproduzir a dinâmica de sistemas físicos complexos de forma mais eficiente do que métodos clássicos.

2.8.3 Química Quântica

A química quântica é uma área intimamente relacionada à simulação de sistemas físicos, com foco específico em estruturas moleculares, energias eletrônicas e reações químicas. O cálculo preciso de propriedades moleculares é fundamental para o desenvolvimento de novos materiais, fármacos e catalisadores.

A computação quântica tem sido investigada como uma ferramenta para melhorar a precisão e a eficiência desses cálculos, especialmente em sistemas onde métodos clássicos exigem aproximações severas. Algoritmos quânticos podem, em princípio, calcular estados eletrônicos com maior fidelidade, embora limitações práticas ainda restrinjam aplicações em larga escala.

2.8.4 Machine Learning Quântico

O *machine learning* quântico busca investigar como conceitos e algoritmos de aprendizado de máquina podem ser implementados ou acelerados utilizando computadores quânticos. Essa área explora tanto algoritmos quânticos inspirados em técnicas clássicas quanto modelos híbridos que combinam computação clássica e quântica.

Até o momento, não há consenso sobre a existência de uma vantagem quântica generalizada para tarefas de aprendizado de máquina. No entanto, o estudo dessa interseção tem contribuído para o desenvolvimento de novos modelos computacionais e para uma melhor compreensão dos limites entre aprendizado clássico e quântico.

2.8.5 Modelagem de Sistemas Complexos

Sistemas complexos caracterizam-se por interações não triviais entre múltiplos componentes, frequentemente resultando em comportamentos emergentes difíceis de prever. A computação quântica tem sido considerada uma possível ferramenta para a modelagem e análise desses sistemas.

2.8.5.1 Redes

Redes complexas aparecem em contextos diversos, como redes sociais, sistemas de comunicação e redes biológicas. A análise dessas estruturas frequentemente envolve problemas de grande escala e alta complexidade computacional. Abordagens quânticas têm sido propostas para a análise estrutural e dinâmica de redes, explorando paralelismo quântico e novas representações de estados.

2.8.5.2 Difusão

Processos de difusão em redes, como propagação de informações, falhas ou contaminações, são exemplos clássicos de dinâmicas complexas. Modelar e simular esses processos pode se tornar computacionalmente custoso em redes grandes e dinâmicas. A computação quântica surge como uma possibilidade para acelerar simulações ou oferecer novas formas de representação desses fenômenos.

2.8.5.3 Epidemiologia

A epidemiologia é um caso particular de modelagem de difusão em sistemas complexos, no qual se busca compreender e prever a propagação de doenças em populações. Modelos epidemiológicos frequentemente envolvem grandes espaços de estados e múltiplos parâmetros, tornando a simulação e otimização computacionalmente desafiadoras.

Nesse contexto, a computação quântica tem sido explorada como uma possível ferramenta para simulação de dinâmicas epidemiológicas, otimização de estratégias de intervenção e análise de cenários complexos, ainda que tais aplicações se encontrem, em grande parte, em estágio exploratório.

3 METODOLOGIA

O objetivo deste trabalho é treinar e aplicar o método inteligente *Support Vector Machine* (SVM) (??) para identificar clientes fraudulentos em um banco de dados de uma companhia distribuidora de energia elétrica. O SVM será treinado para diferenciar entre padrões de consumo legítimos e fraudulentos, auxiliando na detecção de fraudes com maior precisão.

A pesquisa adota uma abordagem quantitativa, focada na análise de dados históricos fornecidos por uma companhia distribuidora de energia elétrica e disponibilizados gratuitamente na plataforma *Kaggle* (??). Essa abordagem permite a aplicação de técnicas de aprendizado de máquina para modelagem preditiva e identificação de padrões associados ao furto de energia elétrica.

O desenvolvimento do projeto será conduzido utilizando a linguagem de programação *Python*, escolhida por sua robustez e extensa biblioteca de ferramentas para análise de dados e aprendizado de máquina. O método *Support Vector Machine* será implementado com a biblioteca *Scikit-Learn* (??). A metodologia possui as seguintes etapas: tratamento de dados, treinamento do modelo, avaliação da assertividade e escrita do trabalho.

Inicialmente, será realizado o tratamento do banco de dados com informações do consumo de energia, uma vez que é comum que esses dados apresentem problemas como informações faltantes, valores discrepantes e outras inconsistências. Essa etapa é essencial para garantir a qualidade do treinamento do modelo.

Após o tratamento, o banco de dados será dividido em duas partes: 80% dos dados serão utilizados para o treinamento do SVM, enquanto os 20% restantes serão reservados para a validação do modelo, cuja eficácia será avaliada utilizando o coeficiente de determinação R^2 (????).

Além disso, será realizada uma Análise Multivariada de Variância (MANOVA) (??????) para entender melhor os principais fatores que influenciam o furto de energia elétrica, permitindo uma análise mais detalhada dos dados e dos padrões detectados.

Por fim, a escrita da monografia será realizada com base nos dados e resultados obtidos ao longo do projeto. Para garantir a qualidade do texto, será utilizada uma ferramenta de Inteligência Artificial para correções ortográficas e ajustes gramaticais, proporcionando maior precisão e clareza na apresentação dos resultados.

REFERÊNCIAS

CAMPBELL-KELLY, M. et al. **Computer: A history of the information machine**. [S.l.]: Routledge, 2023. Citado na página 2.

FEYNMAN, R. P. Simulating physics with computers. In: **Feynman and computation**. [S.l.]: cRc Press, 2018. p. 133–153. Citado na página 6.

HODGES, A. **Alan Turing: The Enigma: The Book That Inspired the Film "The Imitation Game"**. [S.l.]: Princeton University Press, 2014. Citado na página 3.

KAISER, S. C.; GRANADE, C. **Learn quantum computing with python and Q#: A hands-on approach**. [S.l.]: Simon and Schuster, 2021. Citado na página 2.

KIRKPATRICK, S.; JR, C. D. G.; VECCHI, M. P. Optimization by simulated annealing. **science**, American association for the advancement of science, v. 220, n. 4598, p. 671–680, 1983. Citado na página 5.

MOORE, G. E. et al. **Cramming more components onto integrated circuits**. 1965. Citado na página 3.

NIELSEN, M. A.; CHUANG, I. L. **Quantum computation and quantum information**. [S.l.]: Cambridge university press, 2010. Citado na página 6.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, ACM New York, NY, USA, v. 21, n. 2, p. 120–126, 1978. Citado na página 5.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: IEEE. **Proceedings 35th annual symposium on foundations of computer science**. [S.l.], 1994. p. 124–134. Citado na página 5.

SIPSER, M. Introduction to the theory of computation. **ACM Sigact News**, ACM New York, NY, USA, v. 27, n. 1, p. 27–29, 1996. Citado 2 vezes nas páginas 4 e 5.

WATROUS, J. **The theory of quantum information**. [S.l.]: Cambridge university press, 2018. Citado na página 6.