Sobre Computação Quântica – Uma Breve Introdução

Prof. M.Sc. Rodrigo Hagstrom

São Paulo, fevereiro de 2025

Introdução à Computação Quântica e Álgebra Linear

Este documento apresenta conceitos fundamentais da mecânica quântica e sua aplicação em computadores quânticos, abordando álgebra linear necessária para compreender os cálculos quânticos.

Alguns Conceitos Fundamentais da Mecânica Quântica

1. Quantização de Energia

- A energia de sistemas quânticos aparece em quantidades discretas (quanta).

- A energia de sistemas quânticos não é contínua, mas aparece em quantidades discretas chamadas *quanta*.
- No modelo do átomo de Bohr, por exemplo, os elétrons só podem ocupar órbitas específicas, e os saltos entre elas envolvem a emissão ou absorção de fótons.

2. Dualidade Onda-Partícula

- Partículas podem se comportar como ondas e vice-versa.

- Partículas subatômicas apresentam comportamento de onda e de partícula simultaneamente.
- O experimento da **dupla fenda** demonstrou que elétrons e fótons podem interferir consigo mesmos como ondas, mas também podem ser detectados como partículas.

3. Princípio da Incerteza de Heisenberg

- Não podemos conhecer simultaneamente a posição e o momento de uma partícula com precisão absoluta.

- Não é possível conhecer simultaneamente a posição e o momento linear (*quantidade de movimento*) de uma partícula com precisão absoluta.
- A relação matemática dessa incerteza é dada por:

$$\Delta x \cdot \Delta p \geq \hbar/2$$

- onde Δx é a incerteza na posição, Δp a incerteza no momento, e $\hbar$ é a constante de Planck reduzida ($h/2\pi$).

4. Função de Onda e Probabilidade

- O estado de uma partícula é descrito por uma função de onda $\Psi(x,t)$.

O quadrado do módulo dessa função, $|\Psi(x,t)|^2$, representa a **probabilidade** de encontrar a partícula em uma posição específica.

5. Colapso da Função de Onda

- A medição faz com que a função de onda colapse para um único valor.

- Antes da medição, a partícula está em uma superposição de estados possíveis.
- Quando medimos a posição, por exemplo, a função de onda "colapsa" para um único valor, e a incerteza desaparece nesse instante.

Matemática Básica da Mecânica Quântica

Espaço de Estados e Vetores de Estado

- O estado de um sistema quântico é representado por um vetor $|\psi\rangle$.

- O estado de um sistema quântico é representado por um vetor em um **espaço de Hilbert**[1].
- Esse vetor é chamado de **ket** e denotado como $|\psi\rangle$.
- O seu dual, chamado **bra**, é denotado como $\langle\psi|$.
- O produto interno entre dois estados $|\psi\rangle$ e $|\phi\rangle$ é escrito como: $\langle\psi|\phi\rangle$ e fornece uma medida da sobreposição entre os dois estados.

Operadores e Observáveis

- Grandezas físicas são representadas por operadores hermitianos.

- Grandezas físicas como **energia**, **momento** e **posição** são representadas por **operadores hermitianos**.

---

1 Um **espaço de Hilbert** é um **espaço vetorial complexo com produto interno**, usado para descrever estados quânticos.
No caso de um qubit, o espaço de Hilbert tem **duas dimensões** e a base $\{|0\rangle,|1\rangle\}$.
Para **n qubits**, o espaço de Hilbert tem $\mathbf{2^n}$ **dimensões**.
A **medição em um espaço de Hilbert** projeta um estado sobre uma base, dando probabilidades quânticas.

- Um operador A^ age sobre um vetor de estado $|\psi\rangle$ e pode ter autovalores a: $\hat{A}|\psi\rangle = a|\psi\rangle$ Isso significa que, ao medir a grandeza correspondente a A^, o único resultado possível será um dos autovalores a.

Equação de Schrödinger

A evolução temporal de um sistema quântico é governada pela **Equação de Schrödinger**:

$$i\hbar\frac{\partial}{\partial t}\Psi(x,t) = \hat{H}\Psi(x,t)$$

onde:

- $\hbar$ é a constante de Planck reduzida,
- H^ é o operador Hamiltoniano (energia total do sistema),
- Ψ(x,t) é a função de onda do sistema.

Para uma partícula livre, a equação se reduz a:

$$-\frac{\hbar^2}{2m}\frac{d^2\Psi}{dx^2} + V(x)\Psi = E\Psi$$

Essa equação é fundamental para descrever sistemas como átomos, moléculas e semicondutores.

Funções de Onda e Probabilidades

A função de onda Ψ(x) deve ser **normalizada**, ou seja, a soma das probabilidades sobre todo o espaço deve ser 1:

$$\int |\Psi(x)|^2 dx = 1$$

A probabilidade de encontrar uma partícula em um intervalo $a \leq x \leq b$ é dada por:

$$P(a \leq x \leq b) = \int_a^b |\Psi(x)|^2 dx$$

Conceitos Fundamentais dos Computadores Quânticos

Os **computadores quânticos**, conforme propostos por **Richard Feynman** em 1982, utilizam os princípios da **Mecânica Quântica** para realizar cálculos de maneira fundamentalmente diferente dos computadores clássicos.

A motivação de Feynman foi que **sistemas quânticos são difíceis de simular em computadores clássicos** devido à complexidade exponencial das interações quânticas.

A seguir, vamos explorar os conceitos fundamentais dos **computadores quânticos** e sua matemática com base nos princípios da mecânica quântica.

1. Qubits

- Diferente dos bits clássicos, os qubits podem estar em superposição.

- Nos computadores clássicos, a unidade de informação é o **bit**, que pode assumir valores **0 ou 1**.
- Nos computadores quânticos, a unidade de informação é o **qubit**, que pode estar em um estado **0, 1 ou em uma superposição de ambos**:

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$$

onde α e β são números complexos que representam as amplitudes de probabilidade, obedecendo à relação de normalização:

$$|\alpha|^2+|\beta|^2=1$$

- A superposição é uma característica fundamental no que pode ser considerado o modelo de funcionamento dos algoritmos e computadores quânticos.

2. Entrelaçamento Quântico (**Entanglement**)

- Qubits entrelaçados têm estados correlacionados.

- Quando dois ou mais qubits estão entrelaçados, suas propriedades se tornam **correlacionadas** independentemente da distância entre eles.
- Um estado entrelaçado famoso é o **estado de Bell**:

$$|\Phi^+\rangle=1/\sqrt{2}\,(|00\rangle+|11\rangle)$$

- Isso significa que **medir um qubit afeta instantaneamente o estado do outro entrelaçado**, mesmo que estejam separados por grandes distâncias.

3. Interferência Quântica

- Permite amplificar probabilidades corretas e eliminar erradas.

- Nos computadores quânticos, operações podem causar **interferência construtiva ou destrutiva** nas amplitudes de probabilidade dos qubits.

- Essa interferência permite **amplificar** os estados corretos e **destruir** os errados, o que é essencial para algoritmos quânticos como o de Shor (fatoração de números primos) e o de Grover (busca em bases de dados).

Computadores Quânticos

Os computadores quânticos são descritos matematicamente usando **álgebra linear e operadores unitários**.

1. Estados e Espaço de Hilbert

- O estado de um **único qubit** é representado por um vetor em um espaço de Hilbert bidimensional:

  $$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$$

  onde

  $$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ e } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}.$$

- Para um **sistema de dois qubits**, o estado é um vetor em um espaço de Hilbert **4-dimensional**:

  $$|\psi\rangle=\alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle$$

  com a normalização:

  $$|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1$$

2. Portas Lógicas Quânticas

Nos computadores clássicos, usamos **portas lógicas** como AND, OR e NOT. Em computadores quânticos, as operações são feitas com **portas quânticas**, que são **transformações unitárias** representadas por **matrizes**.

Porta Hadamard (H)

Cria **superposição** a partir de um estado puro:

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

Se aplicada ao estado $|0\rangle$, resulta em:

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

Isso coloca o qubit em uma superposição de **0 e 1**.

Porta CNOT (Controlled-NOT)

Entrelaça dois qubits:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Se aplicada ao estado $|00\rangle$, não muda nada, mas aplicada ao estado $|10\rangle$, ela o transforma em $|11\rangle$, criando **entrelaçamento**.

Porta de Fase (S e T)

Aplicam uma fase complexa ao estado quântico:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

Algoritmos Quânticos

Os computadores quânticos são promissores porque podem resolver problemas mais rapidamente do que os clássicos. Alguns algoritmos quânticos fundamentais incluem:

Algoritmo de Shor (Fatoração de Números Primos)

- Baseia-se na **transformada quântica de Fourier** para encontrar os fatores primos de um número rapidamente.
- Importante para **criptografia**, pois ameaça sistemas como RSA.

Algoritmo de Grover (Busca em Banco de Dados)

- Usa **interferência quântica** para encontrar um item em um banco de dados **em tempo quadrático melhor que o clássico**.
- Enquanto um algoritmo clássico precisa de O(N) passos, o **Grover faz em O(√N)**.

Simulação de Sistemas Quânticos[2]

- Feynman propôs os computadores quânticos inicialmente para simular **sistemas físicos quânticos** que seriam inviáveis de calcular em computadores clássicos.

Exemplo da Redução do Custo de Tempo com Computação Quântica

O problema

Dado uma função $f:\{0,1\}^n \rightarrow \{0,1\}$, queremos determinar se ela é:

1. **Constante** – retorna sempre 0 ou sempre 1 para todas as entradas.
2. **Balanceada** – retorna 0 para metade das entradas e 1 para a outra metade.

A solução clássica

- No pior caso, precisamos testar $\mathbf{2^{n-1}+1}$ valores para garantir que a função é constante.
- Isso significa que, se n=100, precisamos testar mais de 2^{99} entradas!

A solução quântica

O **Algoritmo de Deutsch-Jozsa** resolve o problema **em apenas UMA chamada à função f** usando **superposição e interferência**.

Passo a Passo do Algoritmo:

1 - **Criar n+1 qubits e inicializá-los em $|0\rangle$**

No início, todos os qubits estão no estado $|0\rangle$:

$$|\,00\ldots0\rangle\,|\,1\rangle$$

Mas o último qubit, chamado de **qubit auxiliar**, é colocado no estado $|\,1\rangle$:

$$|\,00\ldots0\rangle\,|\,1\rangle$$

2 - **Aplicar a Porta de Hadamard a todos os qubits**

A **Porta Hadamard (H)** cria uma **superposição quântica**, transformando:

$$|\,0\rangle \rightarrow 1/\sqrt{2}\,(\,|\,0\rangle + |\,1\rangle)$$

Para n+1 qubits, obtemos:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

2 É a "razão de existir" dos computadores quânticos.

Isso coloca os **primeiros n qubits em uma superposição de todas as entradas possíveis**.

3 - **Aplicar a função f(x) (Oráculo)**

A função f(x) é implementada como um **oráculo quântico**, que transforma o estado da seguinte forma:

$$|x\rangle |y\rangle \rightarrow |x\rangle \ |y \oplus f(x)\rangle$$

Como y estava inicialmente em $1/\sqrt{2}\ (|0\rangle - |1\rangle)$, obtemos um fator de fase:

$$|x\rangle \rightarrow (-1)^{f(x)} |x\rangle$$

Ou seja, a função **marca os estados com um fator de fase**.

4 - Aplicar a Porta Hadamard novamente

A segunda Hadamard converte a fase aplicada pelo oráculo em interferência:

$$H^{\otimes n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

→ Se f(x) for **constante**, todos os termos interferem construtivamente, e o resultado será **$|0\rangle$**.

→ Se f(x) for **balanceada**, a interferência destrói a amplitude de $|0\rangle$, produzindo um estado diferente.

- O algoritmo quântico resolve o problema com **uma única chamada** à função f(x).
- O método clássico exigiria **exponencialmente mais chamadas**.

Agora vamos implementar esse algoritmo usando **Qiskit**, uma biblioteca da IBM para simulação de computadores quânticos em Python.

```
from qiskit import QuantumCircuit, Aer, execute

# Definição da Função Deutsch-Jozsa (oráculo para uma função balanceada)
def balanced_oracle(n):
    qc = QuantumCircuit(n+1)
    for qubit in range(n):
        qc.cx(qubit, n)  # Aplica CNOT para criar a função balanceada
    return qc


# Criando um circuito para o Algoritmo de Deutsch-Jozsa
n = 3  # Número de qubits de entrada
```

```
qc = QuantumCircuit(n+1, n)

# Passo 1: Inicialização
qc.x(n)  # Define o qubit auxiliar em |1>
qc.h(range(n+1))  # Aplica Hadamard a todos os qubits

# Passo 2: Aplicar o Oráculo (Usamos uma função balanceada)
oracle = balanced_oracle(n)
qc.append(oracle.to_instruction(), range(n+1))

# Passo 3: Aplicar Hadamard novamente
qc.h(range(n))

# Passo 4: Medição dos primeiros n qubits
qc.measure(range(n), range(n))

# Simulação
simulator = Aer.get_backend('qasm_simulator')
result = execute(qc, simulator, shots=1024).result()
counts = result.get_counts()
print(counts)
```

Oráculo Quântico?

Uma **função de oráculo quântico** é uma função especial utilizada em algoritmos quânticos para processar informações sem revelar diretamente sua estrutura. Ela age como uma "caixa preta" que recebe um estado quântico como entrada e aplica uma transformação específica ao estado, geralmente adicionando uma **fase** a determinados estados (os chamados **estados marcados**).

Esses estados marcados são aqueles que possuem uma propriedade especial que queremos identificar, e o oráculo os distingue alterando a fase da função de onda sem colapsar o estado. Isso permite que, através da interferência quântica, algoritmos como o de Grover amplifiquem as probabilidades dos estados desejados, tornando a busca por informações mais eficiente do que em um sistema clássico.

Imagine que você tem **quatro caixas fechadas**, e apenas **uma delas contém um prêmio**. Em um sistema clássico, você precisaria abrir as caixas **uma por uma** até encontrar o prêmio. Agora, no mundo quântico, podemos usar um **oráculo quântico** para marcar a caixa certa sem precisar abri-las diretamente.

No computador quântico, cada caixa é representada por um **estado quântico**, e podemos colocá-los todos em uma **superposição**, onde cada caixa tem **a mesma probabilidade de conter o prêmio**:

$$½ (| 00⟩+ | 01⟩+ | 10⟩+ | 11⟩)$$

Aqui, os dois bits quânticos ($| 00⟩$, $| 01⟩$, $| 10⟩$, $| 11⟩$) representam quatro caixas.

Agora, vamos supor que o prêmio está na **caixa $|10⟩$**. O **oráculo quântico** atua como um "juiz", identificando essa caixa sem olhar dentro dela. Mas, em vez de dizer diretamente **"aqui está o prêmio"**, ele **modifica a fase** do estado correspondente, multiplicando-o por -1:

$$½ (| 00⟩ + | 01⟩ − | 10⟩ + | 11⟩)$$

Note que o estado $| 10⟩$ foi marcado com uma fase negativa, mas **o resto permaneceu o mesmo**.

Agora, podemos usar **interferência quântica** para amplificar a probabilidade de medir a caixa correta. Esse é o truque do **Algoritmo de Grover**: a fase negativa interfere com os outros estados, realçando a probabilidade de que o prêmio esteja em $| 10⟩$ quando fizermos uma medição.

Importante:

- O **oráculo quântico** não dá a resposta diretamente, mas **marca os estados corretos alterando a fase**.
- Isso permite que a **interferência quântica amplifique a resposta correta**.
- Em algoritmos como o **de Grover**, isso permite encontrar respostas **muito mais rápido** do que a busca clássica.

Esse é um dos motivos pelos quais os **computadores quânticos podem ser exponencialmente mais rápidos para certos problemas**!

Como o Oráculo "Escolhe" a Caixa Certa?

Em um computador clássico, uma função pode ser programada para verificar se um número atende a determinada condição. Da mesma forma, o **oráculo quântico** é uma função implementada como um circuito quântico, que recebe um estado quântico de entrada e **aplica uma modificação apenas no estado correto**.

1 - O oráculo recebe um estado superposto

Antes de chamar o oráculo, colocamos todos os possíveis estados (caixas) em **superposição**, por exemplo:

$$½ (| 00⟩ + | 01⟩ + | 10⟩ + | 11⟩)$$

Aqui, temos **quatro caixas** representadas por **quatro estados quânticos diferentes**.

2- O oráculo é uma função programada com a resposta

O oráculo é projetado com a informação de qual estado (caixa) contém o prêmio. Ele **não descobre a resposta por si só**, mas sim **sabe de antemão** qual é a solução do problema. Ele então **marca** esse estado adicionando uma **fase negativa**:

Se o prêmio estiver na caixa **$|10⟩$**, o oráculo aplica a seguinte transformação:

$$| x⟩ \rightarrow (-1)^{f(x)} | x⟩$$

onde:

- $f(x)=0$ para estados que **não são a solução** (deixando-os inalterados).
- $f(x)=1$ para o **estado correto** (multiplicando-o por -1).

Isso resulta no seguinte estado:

$$½ (| 00⟩+ | 01⟩− | 10⟩+ | 11⟩)$$

Agora, o estado correto **foi marcado com uma fase negativa**.

3 - O algoritmo usa interferência quântica para amplificar a resposta

Depois de chamar o oráculo, usamos **interferência quântica** para amplificar a probabilidade de medirmos o estado correto. Isso é feito aplicando uma combinação de **portas Hadamard e reflexões**, como no **Algoritmo de Grover**.

O resultado final é que, ao medir o sistema, **a probabilidade de encontrar a caixa correta será muito maior** do que a dos outros estados, resolvendo o problema em muito menos tentativas do que um computador clássico faria.

Logo:

1. **O oráculo já sabe qual estado é o correto** (ele é programado com essa informação antes da execução).
2. **Ele não descobre a resposta**; apenas aplica uma **marca de fase negativa** ao estado correto.
3. **A interferência quântica amplifica esse estado**, aumentando a chance de que, ao medir, encontremos a resposta correta rapidamente.

Problemas – Os Motivos de Sua Não Adoção

Porque ainda não adotamos, já que são tão bons?

Apesar do potencial, ainda existem desafios técnicos:

1. **Decoerência Quântica:**
    - O ambiente externo pode **destruir a superposição** dos qubits, tornando as operações imprecisas.
    -
2. **Correção de Erros Quânticos:**
    - Como os qubits são frágeis, técnicas de correção de erro precisam ser desenvolvidas para garantir que os cálculos sejam confiáveis.

Lutar contra estes fatores ambientais e de manutenção da informação tem exigido, por exemplo, operar em temperaturas próximas do 0 absoluto, uso de supercondutores escudos magnéticos e outras técnicas extremamente caras.

Além disso, é preciso estabelecer comunicação entre os sistemas quânticos e os controles de sistemas eletrônicos para viabilizar a correta operação e manutenção da informação. Essa interface não é facilmente realizada, tornando-se um desafio a mais.

3. **Escalabilidade:**
    - Ainda estamos longe de construir **computadores quânticos de larga escala**, pois manipular um grande número de qubits é extremamente difícil pelas razões que já apontamos acima neste material.

Hoje os computadores quânticos operam apenas na casa de uma ou poucas centenas de bits (algumas vezes até menos). Com esta quantidade de informação representada as aplicações práticas são na verdade poucas.

Entretanto, experimentos e investimentos em como aproveitar melhor este pontencial tem sido feitos, promovendo a esperança de maiores quantidades de informações no futuro (próximo?).

Para entender **a matemática da computação quântica**, é essencial ter uma base sólida em **Álgebra Linear**, pois os qubits e operações quânticas são representados por vetores e matrizes em espaços vetoriais complexos.

Conceitos Fundamentais para Revisar:

- Vetores e espaços vetoriais
- Produto interno e normalização
- Matrizes unitárias e hermitianas
- Autovalores e autovetores
- Portas lógicas quânticas
- Produto tensorial
- Medidas e projeções

//