Um Estudo sobre Computação Quântica

Márcio Dias de Oliveira Junior

Universidade Federal de Minas Gerais (UFMG)
Instituto de Ciências Exatas (ICEx)
Especialização em Matemática

Orientador: Prof. Dr. Csaba Schneider

Belo Horizonte – MG
2026

Roteiro

1. Base matemática
2. Postulados da mecânica quântica
   - Postulado 1 - Espaço de estados
   - Postulado 2 - Evolução
   - Postulado 3 - Medição quântica
   - Postulado 4 - Sistemas compostos
3. Circuitos quânticos
4. Exemplos de algoritmos quânticos
   - Algoritmo de Grover
   - QAOA

Notação Bra-Ket

A notação $|\psi\rangle$ (ket) foi introduzida por Paul Dirac.

Interpretação:

- $|\psi\rangle$ representa um vetor em um espaço de Hilbert $\mathcal{H}$.
- $\langle\psi|$ representa o funcional linear associado (vetor dual) relativo ao produto interno.

Produto interno:

$$\langle\varphi|\psi\rangle$$

Assumindo um base ortonormal de $\mathcal{H}$ e com produto interno canônico podemos identificar:

$$|\psi\rangle = \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \end{bmatrix} \quad \text{e} \quad \langle\psi| = [\psi_0^*, \psi_1^*, \ldots].$$

Operadores em base ortonormal (matriz)

Fixe bases ortonormais $\{|i\rangle\}_{i=1}^{n}$ e $\{|j\rangle\}_{j=1}^{n}$.

Componentes (elementos de matriz):

$$A_{ij} = \langle i|A|j\rangle.$$

Expansão do operador (forma *ket por bra*):

$$A = \sum_{i,j}^{n} \langle i|A|j\rangle \; |i\rangle\langle j| = \sum_{i,j}^{n} A_{ij}|i\rangle\langle j|.$$

Relação de completude:

$$\sum_{i=0}^{n} |i\rangle\langle i| = I$$

Produto tensorial

Dados dois espaços de Hilbert $\mathcal{H}_A$ e $\mathcal{H}_B$ podemos construir o espaço tensorial (que também é um espaço de Hilbert):

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B.$$

Dimensão:

$$\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = \dim(\mathcal{H}_A) \cdot \dim(\mathcal{H}_B) = n \cdot m.$$

Exemplo (2 qubits): $\mathbb{C}^2 \otimes \mathbb{C}^2 \simeq \mathbb{C}^4$ com base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, onde $|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle \ldots$

Postulado 1 - Espaço de estados

Postulado 1. A um sistema quântico isolado associa-se um **espaço de Hilbert complexo** $\mathcal{H}$, chamado *espaço de estados* do sistema. O estado do sistema é completamente descrito por um **vetor unitário** $|\psi\rangle \in \mathcal{H}$.

Equivalência (a menos de uma fase global). Estados que diferem por uma fase global representam o mesmo estado:

$$|\psi\rangle \sim e^{i\alpha}|\psi\rangle.$$

Postulado 2 - Evolução

Postulado 2. A evolução temporal de um sistema quântico **fechado** é descrita por uma **transformação unitária**. Se o estado no instante t_1 é $|\psi\rangle$, então no instante t_2:

$$|\psi'\rangle = U|\psi\rangle,$$

onde U depende apenas do sistema e dos instantes t_1, t_2, e satisfazendo

$$U^\dagger U = UU^\dagger = I.$$

Consequências:

- Preservação de norma: $\||\psi'\rangle\| = \||\psi\rangle\|$.
- Reversibilidade: $U^{-1} = U^\dagger$.
- Portas quânticas em circuitos são operadores unitários.

Postulado 3 - Medição

Postulado 3. Medições quânticas são descritas por um conjunto de operadores $\{M_i\}_{i=1}^m$ (operadores de medição) que satisfazem a **relação de completude**:

$$\sum_{i=1}^{m} M_i^\dagger M_i = I.$$

Se o sistema está no estado $|\psi\rangle$:

- **Probabilidade** do resultado i:

$$p(i) = \langle\psi|M_i^\dagger M_i|\psi\rangle.$$

- **Estado pós-medida** (condicionado ao resultado i):

$$|\psi'\rangle = \frac{M_i|\psi\rangle}{\sqrt{p(i)}}.$$

Intuição: A medição, em geral, introduz aleatoriedade.

Postulado 4 - Sistemas compostos

Postulado 4. O espaço de estados de um sistema composto por dois subsistemas A e B é o **produto tensorial** dos espaços individuais:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B.$$

Se $\{|j\rangle\}_{j=1}^{n}$ é base de $\mathcal{H}_A$ e $\{|k\rangle\}_{k=1}^{m}$ é base de $\mathcal{H}_B$, então $\{|j\rangle \otimes |k\rangle\}_{i=j=1}^{j=n,k=m}$ é base de $\mathcal{H}_{AB}$.

Dimensão:

$$\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = \dim(\mathcal{H}_A) \cdot \dim(\mathcal{H}_B).$$

Operadores em sistemas compostos:

$$(A \otimes B)(|\psi\rangle \otimes |\varphi\rangle) = A|\psi\rangle \otimes B|\varphi\rangle.$$

Circuitos quânticos

A computação quântica no modelo de circuitos é descrita por:

Estado inicial $\longrightarrow$ **Portas unitárias** $\longrightarrow$ **Medição**

Formalmente:

$$|\psi_{\text{out}}\rangle = U_k \cdots U_2 U_1 |\psi_{\text{in}}\rangle$$

onde cada U_i é unitário.

Componentes fundamentais:

- Registradores de qubits.
- Portas unitárias.
- Medição na base computacional.

Emaranhamento: Estados de Bell

Construção a partir de $|00\rangle$:

Aplicando H no primeiro qubit e depois $\text{CNOT}_{1,2}$:

$$\begin{aligned}
|00\rangle &\xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\
&\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= |\beta_{00}\rangle.
\end{aligned}$$

Medição no modelo de circuitos

Ao final do circuito, mede-se na base computacional:

$$\{|x\rangle\langle x|\}_{x\in\{0,1\}^n}.$$

Probabilidade de obter x:

$$P(x) = |\alpha_x|^2.$$

Resultado clássico produzido pelo circuito:

$$x \in \{0,1\}^n.$$

Um circuito quântico implementa uma **distribuição de probabilidade** sobre sequências binárias.

Teleporte quântico

Objetivo: transferir um qubit desconhecido

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

de Alice para Bob sem um canal de comunicação quântica.

Cenário:

- Alice e Bob compartilham previamente um par EPR (assuma $|\beta_{00}\rangle$).
- Anos depois, Alice precisa entregar o estado $|\psi\rangle$ a Bob.
- Alice pode enviar apenas **informação clássica** para Bob.

Ideia: usar emaranhamento + 2 bits clássicos + operações locais em Bob.

Circuito do teleporte

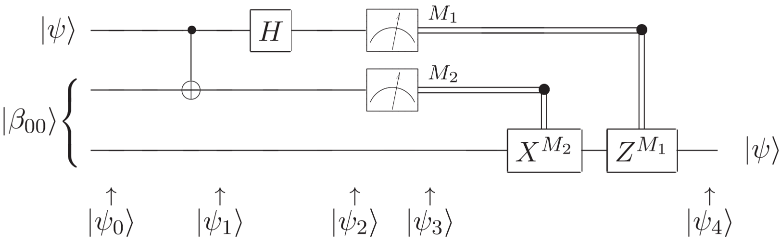

Figura 1: Circuito quântico para teleporte de um qubit.

Resumo operacional:

- Alice aplica CNOT e Hadamard em seus qubits, mede e obtém dois bits.
- Alice envia os 2 bits a Bob (canal clássico).
- Bob aplica uma correção I, X, Z ou XZ.

Teleporte quântico (Qiskit)

Implementação em Qiskit (`quantum-teleportation.ipynb`).

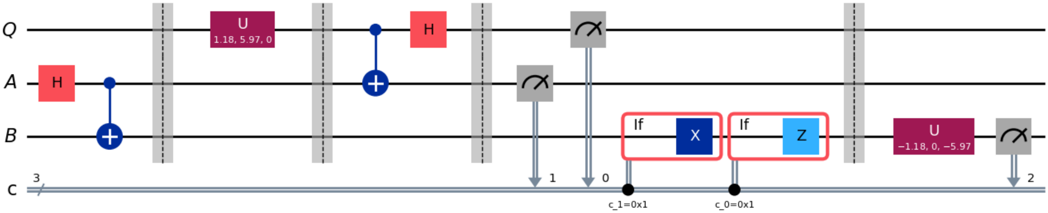

Figura 2: Diagrama do circuito para o teleporte quântico.

Comparativo

Computação Clássica

- Unidade básica: bit (0 ou 1)
- Estados discretos em $\{0, 1\}^n$
- Funções booleanas
- Operações podem ser irreversíveis
- Cópia de bits
- Medição não altera o estado

Computação Quântica

- Unidade básica: qubit ($|0\rangle, |1\rangle$)
- Espaço de Hilbert de dimensão 2^n
- Operadores unitários
- Todas as operações são reversíveis
- Não clonagem de qubits
- Medição colapsa o estado

Problema de Busca Não-Estruturada

Seja $N = 2^n$ e o conjunto de estados computacionais

$$\{x \mid x \in \{0,1\}^n\}.$$

Desejamos encontrar $x^\star$ tal que

$$f(x^\star) = \begin{cases} 1, & \text{se } x = x^\star \\ 0, & \text{caso contrário.} \end{cases}$$

Oráculo quântico:

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle.$$

- U_f aplica fase -1 apenas no estado marcado.
- Não há estrutura conhecida em f.
- Busca clássica: $O(N)$.

Estado inicial

Aplicamos Hadamard em todos os qubits:

$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

Definimos o estado ortogonal ao estado marcado:

$$|x_\perp^\star\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x^\star} |x\rangle.$$

O estado $|s\rangle$ pertence ao subespaço V gerado por $\{|x^\star\rangle, |x_\perp^\star\rangle\}$:

$$|s\rangle = \operatorname{sen}(\theta)|x^\star\rangle + \cos(\theta)|x_\perp^\star\rangle, \qquad \operatorname{sen}(\theta) = \frac{1}{\sqrt{N}}, \quad \cos(\theta) = \sqrt{\frac{N-1}{N}}.$$

Ação do Oráculo no subespaço

No subespaço V:

$$U_f = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad |s\rangle = \begin{bmatrix} \operatorname{sen}\theta \\ \cos\theta \end{bmatrix}$$

- Inverte o sinal do estado marcado.
- Mantém os demais estados invariantes.
- A dinâmica ocorre apenas em um espaço de dimensão 2.

Operador difusor

Definimos no subespaço V

$$D = 2|s\rangle\langle s| - I. = \begin{bmatrix} -\cos(2\theta) & \text{sen}(2\theta) \\ \text{sen}(2\theta) & \cos(2\theta) \end{bmatrix}.$$

Como $|s\rangle\langle s| = \big(H^{\otimes^n}|0\rangle\big)\big(\langle 0|H^{\otimes^n}\big)$, podemos implementar D como:

$$D = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}.$$

Interpretação: reflexão em torno de $|s\rangle$.

Iteração de Grover

Definimos:

$$G = DU_f.$$

No subespaço V:

$$G = \begin{bmatrix} \cos(2\theta) & \operatorname{sen}(2\theta) \\ -\operatorname{sen}(2\theta) & \cos(2\theta) \end{bmatrix}.$$

- G é uma rotação no plano V.
- A cada iteração, a amplitude do estado marcado aumenta.

Evolução Após r iterações

$$G^r|s\rangle = \operatorname{sen}((2r+1)\theta)|x^\star\rangle + \cos((2r+1)\theta)|x^\star_\perp\rangle.$$

Probabilidade de medir o estado marcado:

$$P(r) = \operatorname{sen}^2((2r+1)\theta).$$

Objetivo: maximizar $P(r)$.

Número ótimo de iterações

Queremos:

$$(2r+1)\theta \approx \frac{\pi}{2}.$$

Logo,

$$r \approx \frac{\pi}{4\theta} - \frac{1}{2}.$$

Como $\theta \approx \frac{1}{\sqrt{N}}$:

$$r \approx \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor.$$

O algoritmo encontra $x^\star$ com alta probabilidade usando $O(\sqrt{N})$ invocações do oráculo.

Algoritmo de Grover (Qiskit)

Implementação em Qiskit (`grovers-algorithm.ipynb`).

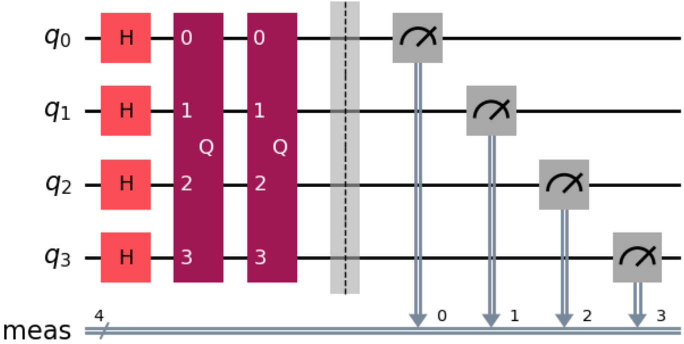

Figura 3: Diagrama do circuito quântico para o algoritmo de Grover para quatro qubits.

Problemas de Otimização Combinatória

Seja $X = \{0,1\}^n$ o conjunto de soluções $z = z_1 z_2 \cdots z_n \in \{0,1\}^n$ (sequências binárias). Um problema de otimização combinatória é dado por funções locais

$$C_\alpha : X \to \{0,1\}, \qquad \alpha = 1, \dots, m,$$

e pela função objetivo

$$C(z) = \sum_{\alpha=1}^{m} C_\alpha(z).$$

- Objetivo: encontrar z que maximize $C(z)$ (solução ótima).
- Otimização aproximada: buscar z com $C(z)$ próximo do máximo.
- Hipótese de *localidade*: cada C_α é implementável com $O(1)$ portas.

Mapeamento para um espaço de Hilbert

Considere o espaço de Hilbert gerado pelas sequências binárias de comprimento n

$$\mathcal{H} = \{|z\rangle : z \in X\}, \qquad \dim(\mathcal{H}) = 2^n,$$

com decomposição

$$\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n,$$

onde cada H_i tem dimensão 2 (um qubit).
A função objetivo define um operador diagonal (hermitiano) na base computacional:

$$C = \sum_{z \in X} C(z)|z\rangle\langle z|.$$

Logo, $|z\rangle$ são autovetores de C:

$$C|z\rangle = C(z)|z\rangle.$$

Operador de custo

Como C é hermitiano, definimos o operador unitário de custo:

$$U(C,\gamma) = \prod_{\alpha=1}^{m} e^{-i\gamma C_\alpha} = e^{-i\gamma C}, \qquad \gamma \in [0, 2\pi).$$

- Em geral, produtos de exponenciais podem não comutar.
- Aqui, cada C_α é diagonal na base computacional $\Rightarrow$ comutam entre si.
- Implementação em circuito: profundidade máxima $O(m)$ (uma camada por termo local).

Operador de mistura

Defina, para cada qubit j,

$$X_j = I \otimes \cdots \otimes I \otimes X \otimes I \otimes \cdots \otimes I,$$

e

$$B = \sum_{j=1}^{n} X_j.$$

O operador unitário de mistura é

$$U(B, \beta) = \prod_{j=1}^{n} e^{-i\beta X_j} = e^{-i\beta B}, \qquad \beta \in [0, \pi).$$

Além disso, podemos implementar $U(B, \beta)$ com $O(1)$ portas

$$U(B, \beta) = \bigotimes_{j=1}^{n} R_x(2\beta).$$

Inicialização: estado uniforme

Inicializamos em

$$|\psi\rangle = |0\rangle^{\otimes n},$$

e aplicamos $H^{\otimes n}$:

$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{z \in X} |z\rangle.$$

Estado variacional do QAOA (profundidade p)

Para $p \geq 1$, dados ângulos

$$\gamma_1, \ldots, \gamma_p, \qquad \beta_1, \ldots, \beta_p,$$

definimos o estado

$$|\gamma, \beta\rangle = U(B, \beta_p)U(C, \gamma_p) \cdots U(B, \beta_1)U(C, \gamma_1)|s\rangle.$$

Forma compacta:

$$|\gamma, \beta\rangle = \prod_{l=p}^{1} e^{-i\beta_l B} e^{-i\gamma_l C} \, |s\rangle.$$

- Cada camada aplica (custo) $\rightarrow$ (mistura).
- Profundidade máxima: $O(mp)$ (custo: $O(m)$; mistura: $O(1)$).

Função objetivo do QAOA

A qualidade do estado é medida pela expectativa ou média:

$$F_p(\gamma, \beta) = \langle \gamma, \beta | C | \gamma, \beta \rangle.$$

Definimos o melhor valor atingível com profundidade p:

$$M_p = \max_{\gamma,\beta} F_p(\gamma, \beta).$$

Monotonicidade:

$$M_p \geq M_{p-1},$$

pois é sempre possível escolher $\gamma_p = \beta_p = 0$ e "simular" a profundidade menor.

Limite superior via princípio variacional

Se C tem decomposição espectral

$$C = \sum_{i=1}^{m} c_i |e_i\rangle\langle e_i|, \qquad c_1 \geq c_2 \geq \cdots \geq c_m \geq 0,$$

então para qualquer estado normalizado $|\psi\rangle$:

$$\langle\psi|C|\psi\rangle \leq c_1, \quad \text{e} \quad \max_{\|\psi\|=1} \langle\psi|C|\psi\rangle = c_1.$$

- O valor ótimo é atingido no autoespaço do maior autovalor.
- No QAOA, os estados permitidos são restritos à família $|\gamma, \beta\rangle$.

Aumentando o número de passos p

Em geral, pode não existir (γ, β) tal que

$$|\gamma, \beta\rangle = |e_1\rangle.$$

No entanto, aumentando p, a família de estados variacionais enriquece e (sob hipóteses do artigo) obtém-se:

$$\lim_{p \to \infty} M_p = \max_{z \in X} C(z).$$

- Interpretação: maior expressividade do circuito com mais camadas.
- A seguir: conexão informal com evolução adiabática + discretização.

Fórmula de Lie–Trotter (ponte para discretização)

Para operadores hermitianos B e C,

$$e^{i(B+C)\Delta t} = e^{iB\Delta t}\, e^{iC\Delta t} \; + \; O(\Delta t^2),$$

onde o erro é entendido na norma de operadores:

$$\|e^{i(B+C)\Delta t} - e^{iB\Delta t}e^{iC\Delta t}\| \leq c\,\Delta t^2.$$

- Aproxima a exponencial do hamiltoniano somado por produto de exponenciais.
- Permite implementar evolução composta usando blocos simples (custo/mistura).

Evolução adiabática: visão contínua (QAA)

Com $\hbar = 1$, a evolução temporal com hamiltoniano $H(t)$ é

$$U(t_1, t_2) = \mathcal{T} \exp\left(-i \int_{t_1}^{t_2} H(t)\, dt\right), \qquad |\psi(T)\rangle = U(T)|\psi(0)\rangle.$$

No QAA, usa-se interpolação linear:

$$H(t) = \left(1 - \frac{t}{T}\right) B + \frac{t}{T} C, \quad t \in [0, T],$$

com $H(0) = B$ e $H(T) = C$.
Teorema adiabático (ideia): para T grande e boa lacuna espectral,

$$|\psi(T)\rangle \approx \text{autovetor de maior autovalor de } C.$$

Discretização do QAA

Divida $[0,T]$ em p subintervalos de tamanho $\Delta t = T/p$ e pontos $t_l = l\Delta t$.

$$U(T) = \prod_{l=p-1}^{0} U(t_l, t_{l+1}).$$

Aproximando o hamiltoniano por seu valor em t_l:

$$U(t_l, t_{l+1}) \approx e^{-i\Delta t\big((1-s_l)B + s_l C\big)}, \qquad s_l = \frac{l}{p}.$$

Aplicando Lie–Trotter:

$$e^{-i\Delta t\big((1-s_l)B + s_l C\big)} \approx e^{-i\beta_l B}\, e^{-i\gamma_l C},$$

com

$$\beta_l = \Delta t(1 - s_l), \qquad \gamma_l = \Delta t\, s_l.$$

Discretização do QAA

Assim,

$$U(T)|s\rangle \approx \left(\prod_{l=p-1}^{0} e^{-i\beta_l B} e^{-i\gamma_l C} \right) |s\rangle = |\gamma, \beta\rangle.$$

- QAOA $\approx$ discretização de uma evolução adiabática contínua.
- Parâmetros (γ_l, β_l) codificam "passos" da interpolação.
- Para p grande (passos pequenos), aproxima-se a evolução contínua.

Considerações

- QAOA constrói estados variacionais com camadas alternadas:

$$U(C, \gamma_l) \text{ (custo)} \quad \text{e} \quad U(B, \beta_l) \text{ (mistura)}.$$

- Otimizando os $2p$ ângulos maximizamos

$$F_p(\gamma, \beta) = \langle \gamma, \beta | C | \gamma, \beta \rangle.$$

- Aumentar p aumenta expressividade e conecta-se ao limite adiabático:

$$\lim_{p \to \infty} M_p = \max_{z \in X} C(z).$$

QAOA (Qiskit)

Grafo para busca do corte máximo

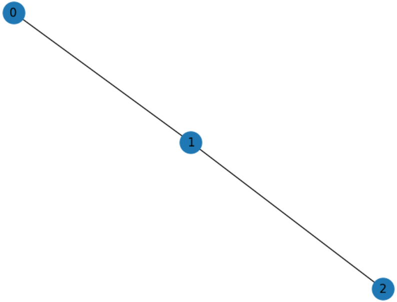

Figura 4: Grafo para uso no QAOA.

QAOA (Qiskit)

Implementação em Qiskit (`qaoa.ipynb`).

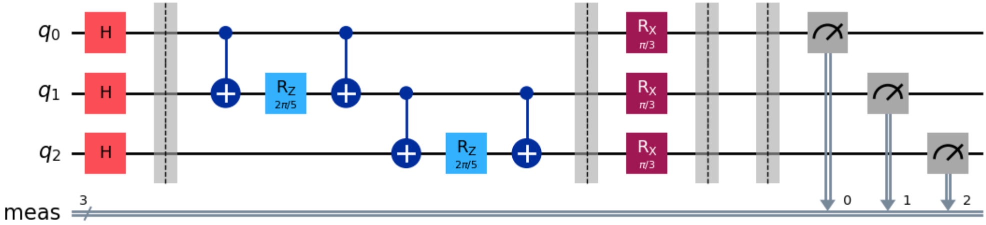

Figura 5: Circuito do QAOA.

Agradecimentos

Muito obrigado!