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

Contexto e objetivos

- Apresentar a base matemática para descrever sistemas quânticos:
  - Espaços de Hilbert
  - Operadores lineares
  - Produto tensorial
- Introduzir o modelo de computação quântica a partir dos postulados
- Implementar e discutir os algoritmos:
  - **Algoritmo de Grover** (busca não-estruturada);
  - **QAOA** aplicado ao **MaxCut**.

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:

$$\langle\phi|\psi\rangle$$

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

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

A base computacional

No caso de um qubit:

$$\mathcal{H} = \mathbb{C}^2.$$

A base computacional é definida por:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Propriedades:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \quad \langle 0|1\rangle = \langle 1|0\rangle = 0.$$

Ou seja, $\{|0\rangle, |1\rangle\}$ é uma base ortonormal.

Espaços de Hilbert

Um **espaço de Hilbert** $\mathcal{H}$ é um espaço vetorial com produto interno $\langle\cdot|\cdot\rangle$ e que é completo na norma induzida:

$$\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}.$$

Exemplo (qubit): $\mathcal{H} = \mathbb{C}^2$ com base $\{|0\rangle, |1\rangle\}$ e produto interno canônico.

$$|\psi\rangle = a|0\rangle + b|1\rangle, \qquad |a|^2 + |b^2| = 1.$$

Operadores lineares

Um **operador linear** $A : \mathcal{H} \to \mathcal{H}$ satisfaz

$$A(\alpha|\psi\rangle + \beta|\phi\rangle) = \alpha A|\psi\rangle + \beta A|\phi\rangle.$$

Adjunto: Dada a representação matricial de A temos

$$A^\dagger = (A^T)^* = (A^*)^T$$

Classes importantes:

- **Hermitiano:** $A = A^\dagger$.
- **Unitário:** $U^\dagger U = I$.
- **Projeção:** $P^2 = P$ e $P^\dagger = P$.

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):

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

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

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 $|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle \ldots$

Operadores em espaços tensoriais

Se A atua em $\mathcal{H}_A$ e B atua em $\mathcal{H}_B$, define-se $A \otimes B$ por:

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

Aplicação típica: portas que atuam em um qubit de um registrador:

$$U_k = I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I.$$

Produto de Kronecker

O **produto de Kronecker** é a representação matricial do produto tensorial.

Se $A \in \mathbb{C}^{m\times n}$ e $B \in \mathbb{C}^{p\times q}$, define-se

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \in \mathbb{C}^{mp\times nq}.$$

Exemplo (2 qubits):

$$X \otimes I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Interpretação física: aplicar X no primeiro qubit e identidade no segundo.

Postulado 1 - Espaço de estados

Postulado 1. A um sistema físico 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 1 - Qubit e parametrização (Esfera de Bloch)

Para um qubit, $\mathcal{H} = \mathbb{C}^2$, na base computacional $\{|0\rangle, |1\rangle\}$:

$$|\psi\rangle = a|0\rangle + b|1\rangle, \qquad |a|^2 + |b|^2 = 1.$$

Removendo a fase global, pode-se escrever (a menos da equivalência):

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \quad 0 \leq \theta \leq \pi,\ 0 \leq \varphi < 2\pi.$$

Leitura geométrica: o par (θ, φ) identifica um ponto na Esfera de Bloch, com vetor

$$\vec{r} = (\sin\theta\cos\varphi,\ \sin\theta\sin\varphi,\ \cos\theta).$$

Postulado 1 - Qubit e parametrização (Esfera de Bloch)

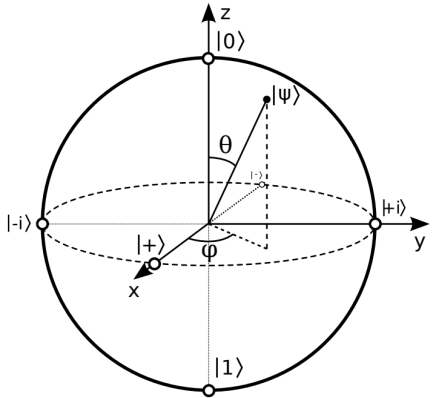

Figura 1: Estado $|\psi\rangle$ representado na Esfera de Bloch.

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 2 - Exemplos e evolução contínua

Exemplos (Pauli).

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \Rightarrow \quad X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle.$$

Exemplo (Hadamard).

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle.$$

Postulado 2 - Evolução Contínua

A dinâmica contínua é governada pela **equação de Schrödinger dependente do tempo**:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle,$$

onde: $H(t)$ é o **Hamiltoniano** (operador hermitiano) e $\hbar$ é a constante de Planck.

Caso independente do tempo:

$$U(t_2, t_1) = \exp\left(-\frac{i}{\hbar}H(t_2 - t_1)\right).$$

Caso dependente do tempo:

$$U(t_2, t_1) = \mathcal{T}\exp\left(-\frac{i}{\hbar}\int_{t_1}^{t_2} H(s)\,ds\right),$$

onde $\mathcal{T}$ é o operador de ordenação temporal.

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 3 - Medição projetiva

Medição projetiva. Um caso importante ocorre quando $M_i = P_i$ são projetores ortogonais:

$$P_i^2 = P_i, \quad P_i^\dagger = P_i, \quad P_i P_j = 0 \ (i \neq j), \quad \sum_i P_i = I.$$

Exemplo: medição na base computacional.

$$M_0 = |0\rangle\langle 0|, \qquad M_1 = |1\rangle\langle 1|, \qquad I = M_0 + M_1.$$

Se

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

então:

$$p(0) = |a|^2, \quad p(1) = |b|^2, \qquad |\psi_0\rangle = |0\rangle, \ |\psi_1\rangle = |1\rangle.$$

Em outras palavras: Ao medir "colapsamos" o estado para um autovetor compatível com o resultado obtido.

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 $\{|i\rangle \otimes |j\rangle\}$ 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:

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

Postulado 4 - Estados separáveis e emaranhamento

Estados produto (separáveis). Um estado é separável se pode ser escrito como

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle.$$

Emaranhamento. Existem estados do sistema composto que *não* podem ser escritos como produto tensorial. Exemplo (estado de Bell):

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \in \mathbb{C}^2 \otimes \mathbb{C}^2.$$

Ideia da prova (esboço): assumindo $|\beta_{00}\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$, os coeficientes exigiriam simultaneamente $ac = \frac{1}{\sqrt{2}}$, $bd = \frac{1}{\sqrt{2}}$, e $ad = bc = 0$, o que é impossível.

Circuitos quânticos

A computação quântica no modelo de circuitos é descrita por:

$$\textbf{Estado inicial} \longrightarrow \textbf{Portas unitárias} \longrightarrow \textbf{Medição}$$

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

Registradores e estados iniciais

Um circuito com n qubits atua sobre:

$$\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$$

Estado inicial padrão:

$$|0\rangle^{\otimes n} = |00\cdots0\rangle$$

Estado geral:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \quad \text{com} \quad \sum_x |\alpha_x|^2 = 1.$$

Dimensão do espaço:

$$\dim(\mathcal{H}) = 2^n.$$

Portas de 1 qubit

Uma porta de 1 qubit é um operador unitário $U : \mathbb{C}^2 \to \mathbb{C}^2$.

Exemplos:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

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

Aplicação em n qubits:

$$H_k = I \otimes \cdots \otimes H \otimes \cdots \otimes I.$$

Portas de múltiplos qubits

Portas que atuam simultaneamente em dois ou mais qubits introduzem correlações.

Exemplo: **CNOT**

$$\mathrm{CNOT}|x, y\rangle = |x, y \oplus x\rangle.$$

Matriz:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Emaranhamento: Estados de Bell

Construção a partir de $|00\rangle$:
Aplicando H no primeiro qubit e depois $\text{CNOT}_{1,2}$:

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

Os quatro estados de Bell:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Profundidade do circuito

Profundidade: número máximo de camadas de portas que devem ser aplicadas sequencialmente.
O circuito a baixo tem profundidade 2.

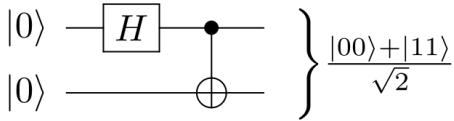

Figura 2: Circuito para geração do estado $|\beta_{00}\rangle$.

Universalidade

Um conjunto de portas é **universal** se pode aproximar qualquer operador unitário com precisão arbitrária.

Exemplo de conjunto universal:

$$\{H, T, \text{CNOT}\}$$

onde

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

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:

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

Assim, um circuito quântico implementa uma **distribuição de probabilidade** sobre sequências binárias.

Teorema da Não clonagem

Theorem (Teorema da não clonagem para um qubit)

Não existem $|s\rangle \in \mathbb{C}^2$ *e* $U : \mathbb{C}^4 \to \mathbb{C}^4$, *um operador unitário, tais que* $U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$ *para todo* $|\psi\rangle \in \mathbb{C}^2$. *Em outras palavras, não é possível construir um circuito quântico que realize a cópia de um qubit arbitrário* $|\psi\rangle$.

Teorema da Não clonagem

Se a cópia funciona para os estados $|\psi\rangle$ e $|\varphi\rangle$, temos

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle.$$

Ao tomar o produto interno das equações acima temos

$$\begin{aligned}\langle U(|\psi\rangle \otimes |s\rangle) | U(|\varphi\rangle \otimes |s\rangle)\rangle &= \langle (|\psi\rangle \otimes |s\rangle) | (|\varphi\rangle \otimes |s\rangle)\rangle \\ &= \langle \psi|\varphi\rangle \\ &= \langle (|\psi\rangle \otimes |\varphi\rangle) | (|\psi\rangle \otimes |\varphi\rangle)\rangle \\ &= \langle \psi|\varphi\rangle^2,\end{aligned}$$

portanto,

$$\langle \psi|\varphi\rangle = \langle \psi|\varphi\rangle^2 \implies \langle \psi|\varphi\rangle = 0 \text{ ou } \langle \psi|\varphi\rangle = 1,$$

que só é possível se $|\varphi\rangle = |\psi\rangle$ ou se $|\varphi\rangle$ e $|\psi\rangle$ são ortogonais.

Teleporte Quântico: cenário e objetivo

Objetivo: transferir um qubit desconhecido

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

de Alice para Bob sem um canal de comunicação quântica entre eles.

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.

Pontos importantes

Dificuldades fundamentais:

- Alice possui *apenas uma cópia* de $|\psi\rangle$.
- Pelo **teorema da não-clonagem**, ela não pode copiar $|\psi\rangle$.
- Uma medição direta altera o estado, pois o estado pós-medida depende do resultado.

Mesmo que Alice conhecesse $|\psi\rangle$, descrevê-lo exatamente exigiria especificar parâmetros em um conjunto contínuo.

Solução: explorar o par EPR compartilhado para reconstruir $|\psi\rangle$ em Bob.

Circuito do teleporte

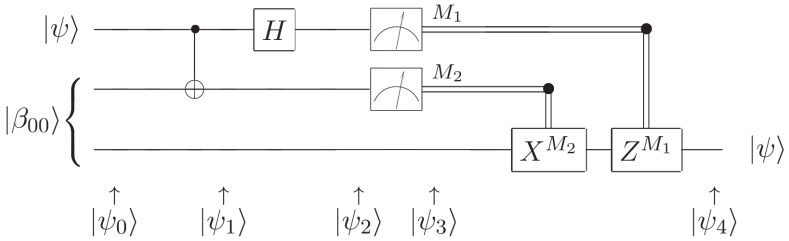

Figura 3: Circuito quântico para teleporte de um qubit.

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.

Estado de entrada e aplicação do CNOT

Assuma $|\psi\rangle = a|0\rangle + b|1\rangle$ e o par EPR $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Estado de entrada:

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle \\ &= \frac{1}{\sqrt{2}}\Big(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)\Big). \end{aligned}$$

Convenção: os dois primeiros qubits são de Alice e o terceiro é de Bob.

Após CNOT (controle = qubit $|\psi\rangle$; alvo = metade do EPR de Alice):

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|10\rangle + |01\rangle)\Big).$$

Aplicação do Hadamard e decomposição em 4 casos

Após aplicar Hadamard no primeiro qubit de Alice:

$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}\Big(a(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + b(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle)\Big) \\
&= \frac{1}{2}\Big(\\
&\quad + |00\rangle(a|0\rangle + b|1\rangle) \\
&\quad + |01\rangle(a|1\rangle + b|0\rangle) \\
&\quad + |10\rangle(a|0\rangle - b|1\rangle) \\
&\quad + |11\rangle(a|1\rangle - b|0\rangle) \\
&\Big).
\end{aligned}
$$

Os qubits de Alice determinam um dentre quatro termos (resultados clássicos $00, 01, 10, 11$).

Medição de Alice, comunicação clássica e correções de Bob

Estado de Bob condicionado ao resultado de Alice:

$$
\begin{aligned}
00 &\mapsto |\psi_3(00)\rangle = a|0\rangle + b|1\rangle \\
01 &\mapsto |\psi_3(01)\rangle = a|1\rangle + b|0\rangle \\
10 &\mapsto |\psi_3(10)\rangle = a|0\rangle - b|1\rangle \\
11 &\mapsto |\psi_3(11)\rangle = a|1\rangle - b|0\rangle
\end{aligned}
$$

Correção em Bob:

- 00: I (não faz nada)
- 01: aplica X
- 10: aplica Z
- 11: aplica X e depois Z

Teleporte quântico (Qiskit)

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

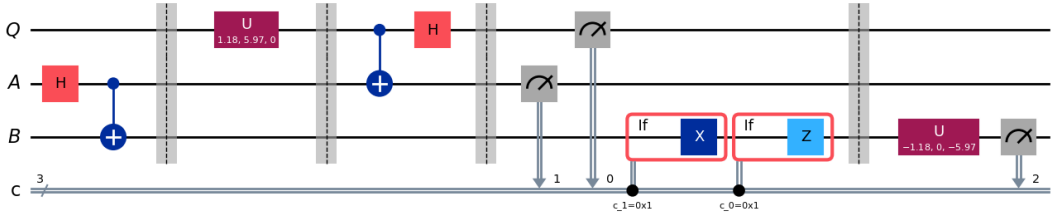

Figura 4: Diagrama do circuito para o teleporte quântico.

Teleporte quântico (Qiskit)

Qubit teleportado sempre aparece com resultado $|0\rangle$.

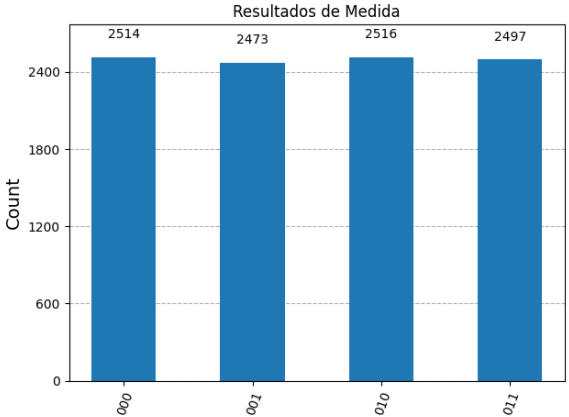

Figura 5: Histograma para simulação de medições no circuito do teleporte quântico.

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:

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

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

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

Ação do Oráculo no subespaço

No subespaço V:

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

- 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

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

Como $|s\rangle\langle s| = \left(H^{\otimes n}|0\rangle\right)\left(\langle 0|H^{\otimes n}\right)$, 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:

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

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

Evolução Após r iterações

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

Probabilidade de medir o estado marcado:

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

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.

Caso com M Soluções

Definimos

$$|x^\star\rangle = \frac{1}{\sqrt{M}} \sum_{f(x)=1} |x\rangle, \qquad |x^\star_\perp\rangle = \frac{1}{\sqrt{N-M}} \sum_{f(x)=0} |x\rangle.$$

Assim,

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle = \frac{M}{N}|x^\star\rangle + \frac{N-M}{N}|x^\star_\perp\rangle.$$

Tomando $\operatorname{sen}\theta = \sqrt{M/N}$ obtemos de forma análoga

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

Algoritmo de Grover (Qiskit)

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

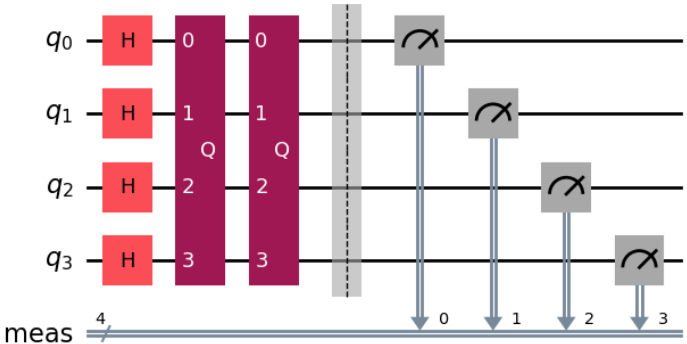

Figura 6: Diagrama do circuito quântico para o algoritmo de Grover para quatro qubits.

Algoritmo de Grover (Qiskit)

Estados marcados aparecem com maior frequência.

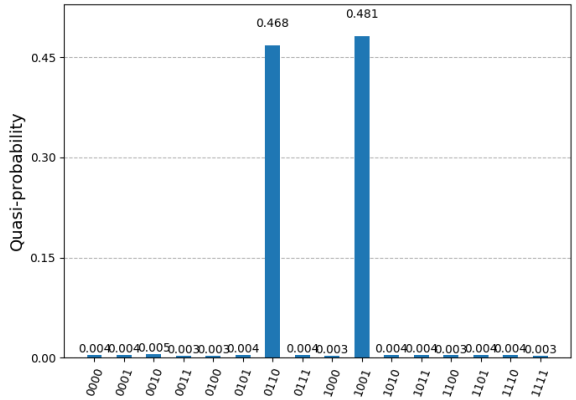

Figura 7: Histograma de medição para o algoritmo de Grover.

Problemas de Otimização Combinatória

Seja $X = \{0,1\}^n$ o conjunto de soluções (strings binárias)

$$z = z_1 z_2 \cdots z_n \in \{0,1\}^n.$$

Um problema de otimização combinatória é dado por funções locais

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

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

Ideia central: aproximar o ótimo aumentando 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:

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

Aplicando Lie–Trotter:

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

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

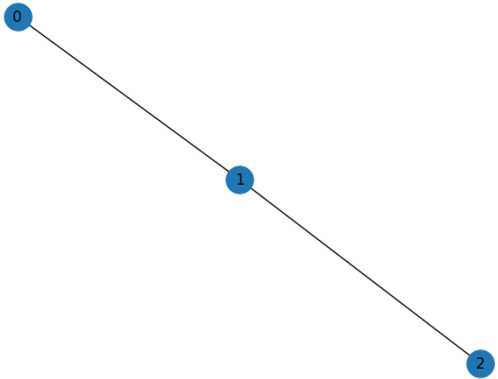

Figura 8: Grafo para uso no QAOA.

QAOA (Qiskit)

Implementação em Qiskit (`qaoa.ipynb`).

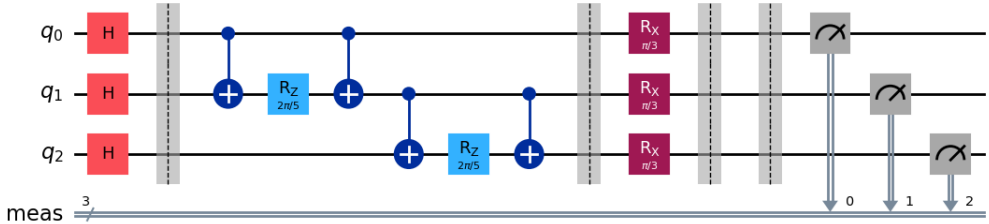

Figura 9: Circuito do QAOA.

QAOA (Qiskit)

Corte máximo aparece com maior frequência.

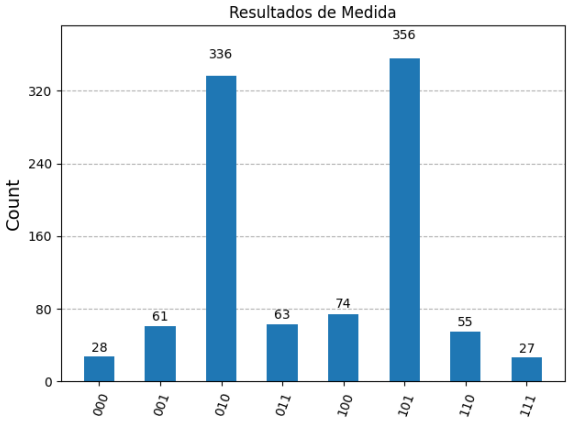

Figura 10: Histograma de medida com o resultado correto para o corte máximo.

Agradecimentos

Muito obrigado!