



Introdução à computação quântica

Alexandre C. Ricardo
Amanda G. Valério
Tiago de S. Farias



Sumário

Parte 1: Fundamentos Teóricos (~1h30)


- Recapitulação de mecânica quântica
- Computação clássica e mecânica quântica
- Portas lógicas
- Execução de algoritmos quânticos
- Pós-processamento
- Software & Hardware quânticos

Parte 2: Algoritmos quânticos na prática ~(1h30 - 2h)

- Geração de Estados de Bell
- Teleportação quântica
- Algoritmos Variacionais e Quantum Machine Learning

Mecânica quântica





Recapitulando: Equação de Schrödinger, Estados Quânticos e Notação de Dirac

Equação de Schrödinger dependente do tempo:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H}|\psi(t)\rangle$$

- Vetor de estado $|\psi\rangle$ (ket) descreve o sistema quântico.
- Vetor dual $\langle\psi|$ (bra). Produto interno: $\langle\psi|\phi\rangle$
- Evolução unitária: Existe $U(t)$ unitária que satisfaz $|\psi(t)\rangle = U(t)|\psi(0)\rangle$
- Evolução unitária preserva probabilidade entre os estados estacionários
- Equação linear: Combinação linear de soluções também é solução
- Base de soluções estacionárias $\{|\psi_n\rangle\}_{n=1,2,\dots}$



O qubit e a base computacional

O qubit é um sistema quântico de dois níveis, representando a versão quântica do bit clássico.

A base computacional é a base na qual representamos as operações em computação quântica.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Estado geral de um qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathcal{C}, |\alpha|^2 + |\beta|^2 = 1$$



Superposição

Superposição é representada pela combinação linear de **estados da base**.

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

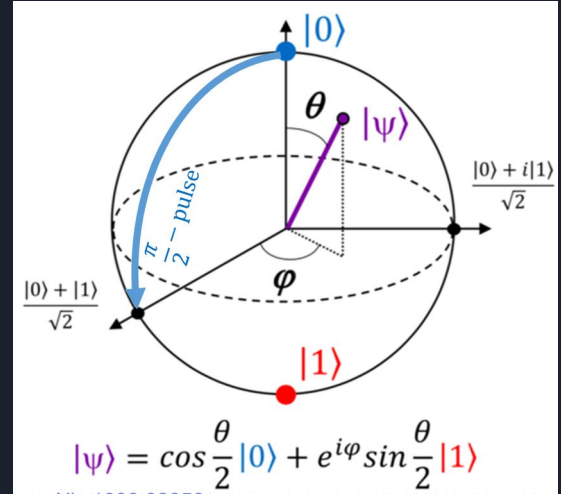
NÃO significa que a partícula *está* nos dois estados da base ao mesmo tempo, mas sim que existe uma **distribuição de amplitudes de probabilidade não nulas** entre os dois estados da base.

Esfera de Bloch

Ferramenta visual para visualizar estados de um único qubit.

Estado de um único qubit:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$$



[arXiv:1908.02656](https://arxiv.org/abs/1908.02656)

Pode ser visto como uma esfera de raio unitário parametrizada pelos ângulos $\{\theta, \phi\}$



Emaranhamento

Adicionando mais uma partícula ao nosso sistema:

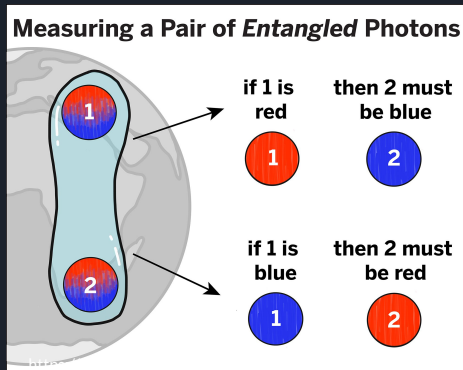
$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

Emaranhamento ocorre quando não existem bases nas quais podemos fatorar o estado em produtos tensoriais.

Emaranhamento

Exemplo de estado emaranhado: Estados de Bell.

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Exemplo de estado não-emaranhado: Superposição uniforme

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \end{aligned}$$



Interferência

Operações unitárias podem gerar interferência entre estados quânticos.

Recurso em computação quântica importante para diversos algoritmos (Deutsch-Jozsa, Shor, Grover)

Probabilidade clássica: Sempre real e positiva

Amplitudes de estados quânticos: números complexos -> podem se cancelar ou amplificar



Medida

Medida colapsa o estado do sistema

Exemplo:

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

Pode retornar :


- $|0\rangle$ com probabilidade $|\alpha|^2$
- $|1\rangle$ com probabilidade $|\beta|^2$

Computação Clássica

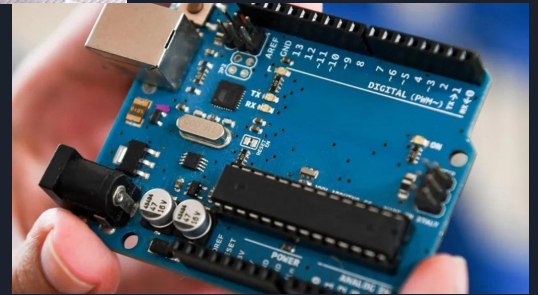




Níveis de Programação

- 
- Linguagens de programação
 - Assembly
 - Microcontroladores/Nível eletrônico

Computação Clássica





Computação Clássica

```
print( "Hello, World!" )
```

```
#include <stdio.h>

int main() {
    printf("Hello World\n");
    return 0;
}
```

Computação Clássica

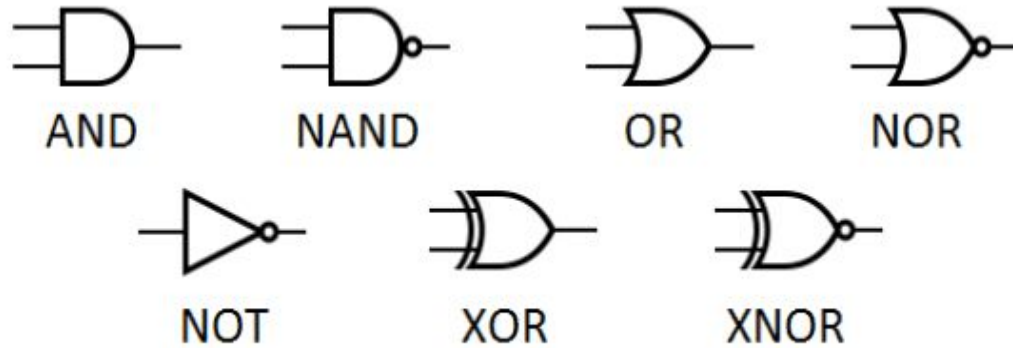
```
print("Hello, World!")
```

```
#include <stdio.h>
```

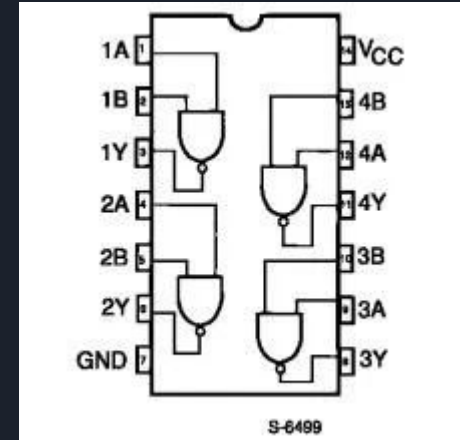
```
int main() {  
    printf("Hello World\n");  
    return 0;  
}
```

```
1  format ELF64 executable 3  
2  
3  segment readable executable  
4  
5  entry main  
6  
7  main:  
8      lea rdi, [msg]  
9      mov rax, 14  
10     mov rdx, rax  
11     mov rsi, rdi  
12     mov rdi, 1  
13     mov rax, 1  
14     syscall  
15     xor rdi, rdi  
16     mov rax, 60  
17     syscall  
18  
19     segment readable writable  
20  
21     msg db 'Hello world!', 10, 0  
22
```


Computação Clássica



<https://www.pontogpp.com.br/tecnicos/desvendando-as-portas-logicas>



<https://www.autocorerobotica.com.br/74hc00-ci-porta-logica-nand>

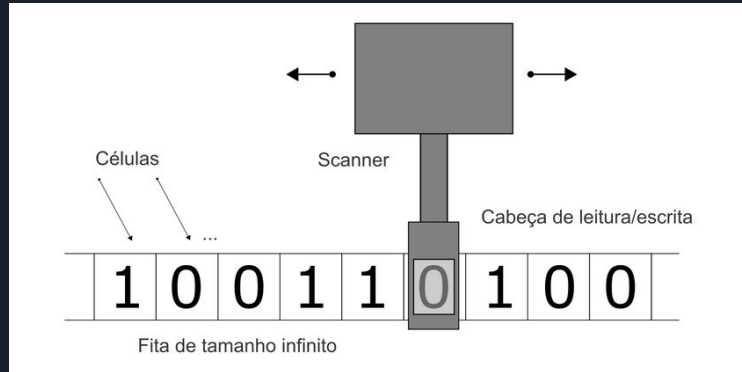


Teoria da Computação

- Toda a computação clássica pode ser realizada por um conjunto de portas clássicas
- Abstratamente, podemos definir modelos matemáticos universais de computação
 - Máquina de Turing

Teoria da Computação

- Toda a computação clássica pode ser realizada por um conjunto de portas clássicas
- Abstratamente, podemos definir modelos matemáticos universais de computação
 - Máquina de Turing





Teoria da Computação

- Toda a computação clássica pode ser realizada por um conjunto de portas clássicas
- Abstratamente, podemos definir modelos matemáticos universais de computação
 - Máquina de Turing
- Tese de Church-Turing:

Tudo que é computável, pode ser computado por
uma máquina de Turing



Teoria da Computação

- Toda a computação clássica pode ser realizada por um conjunto de portas clássicas
- Abstratamente, podemos definir modelos matemáticos universais de computação
 - Máquina de Turing
- Tese de Church-Turing:

Tudo que é computável, pode ser computado por
uma máquina de Turing



Vantagens da computação quântica

- Tempo de processamento:
 - exploração de problemas que já demandam muito tempo de processamento (classe NP)
- Custo energético
- Melhores soluções
- Exploração do comportamento de redes neurais
- Teorema da não-clonagem



Vantagens da computação quântica

- Tempo de processamento:
 - exploração de problemas que já demandam muito tempo de processamento (classe NP)
- Custo energético
- Melhores soluções
- Exploração do comportamento de redes neurais
- Teorema da não-clonagem

Emaranhamento + Superposição

- Permitem percorrer todo espaço de solução em menos passos
- “Paralelismo Quântico”

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

Portas lógicas quânticas





Portas lógicas quântica





Portas lógicas quântica



$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$$



Portas lógicas quântica



$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \begin{bmatrix} \phi_0 \\ \phi_1 \end{bmatrix} = \begin{bmatrix} \psi_0 \\ \psi_1 \end{bmatrix}$$



Portas lógicas quântica





Portas de 1 qubit



Portas de 1 qubit

- Porta Hadamard



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

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

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

Portas de 1 qubit

- Portas de Pauli



$$\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle \end{aligned}$$

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

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Portas de 1 qubit

- Portas de rotação



$$RX(\theta) = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

$$RY(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

$$RZ(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

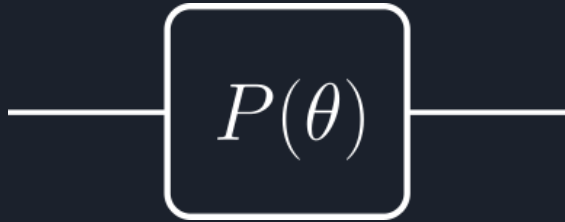
$$RX(\theta)|0\rangle = \cos(\theta/2)|0\rangle - i\sin(\theta/2)|1\rangle$$

$$RX(\theta)|1\rangle = -i\sin(\theta/2)|0\rangle + \cos(\theta/2)|1\rangle$$



Portas de 1 qubit

- Porta de fase / porta T



$$P(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

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

$$P(\theta)|0\rangle = |0\rangle$$

$$P(\theta)|1\rangle = e^{i\theta}|1\rangle$$



Portas de 2 qubits

Portas de 2 qubits

- CNOT (CX)



$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

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

$$CNOT_{1 \rightarrow 2} |00\rangle = |00\rangle$$

$$CNOT_{1 \rightarrow 2} |01\rangle = |01\rangle$$

$$CNOT_{1 \rightarrow 2} |10\rangle = |11\rangle$$

$$CNOT_{1 \rightarrow 2} |11\rangle = |10\rangle$$

Portas de 2 qubits

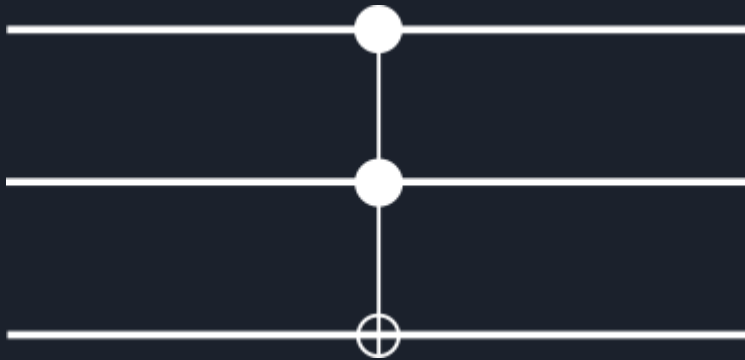
- SWAP



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

$$SWAP|\phi\rangle \otimes |\psi\rangle = |\psi\rangle \otimes |\phi\rangle$$

Porta Toffoli (CCNOT, CCX)



$$CCNOT_{1,2 \rightarrow 3} |110\rangle = |111\rangle$$



Universalidade

- Conjunto de portas que permite implementar qualquer algoritmo
- Qualquer unitária pode ser representada como uma composição de portas desse conjunto



Universalidade

- Conjuntos universais de portas

Universalidade

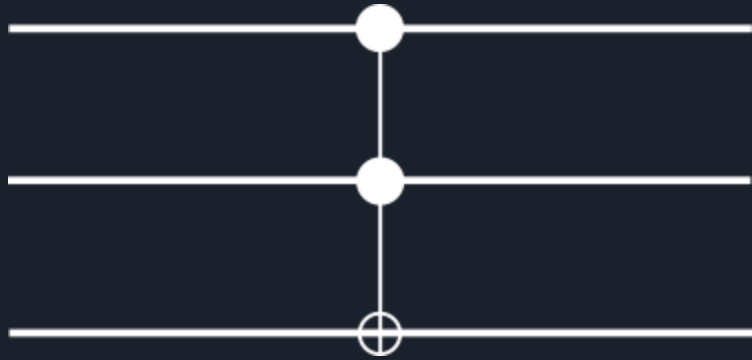
- Portas de Clifford (H, S, CNOT) + porta T



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

Universalidade

- Porta Toffoli + porta Hadamard





Universalidade

- Portas de rotação + CNOT





Decomposição

- Computadores quânticos não implementam todas as portas possíveis de forma direta
- Devemos decompor unitárias na combinação de portas disponíveis, desde que forme um conjunto universal, isso é eficiente?



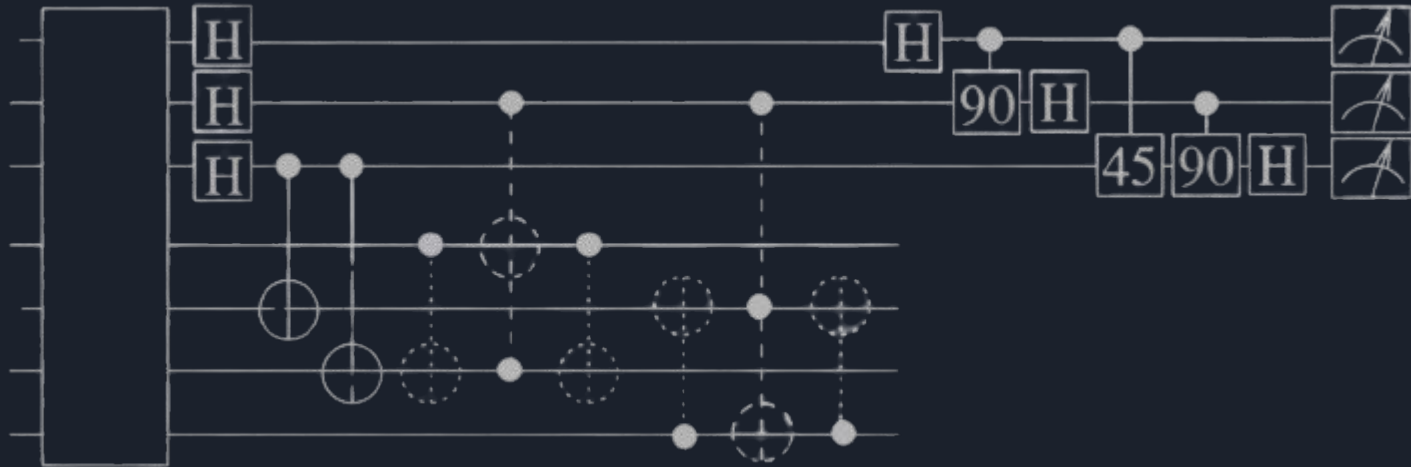
Decomposição

- Teorema de Solovay-Kitaev:

Qualquer unitária pode ser decomposta eficientemente em portas básicas com precisão polilogarítmica

$$O(4^n \text{polylog}(1/\epsilon))$$

Circuitos quânticos



Vandersypen, Lieven M. K., et al. "Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance." *Nature*, vol. 414, no. 6866, Dec. 2001, pp. 883–87

Execução de algoritmos quânticos





Como Executar um Algoritmo Quântico?

Simulação de algoritmos quânticos
(computação clássica):

- Cálculo numérico
- Simuladores especializados (Qiskit's Aer, PennyLane's Lightning, Cirq's Simulator, etc.)

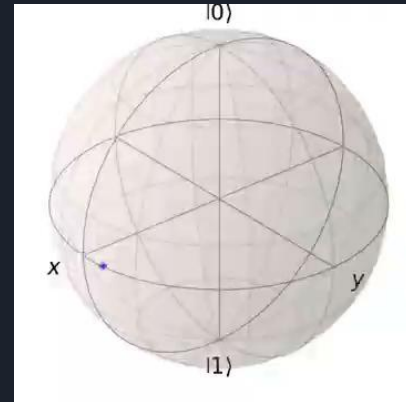
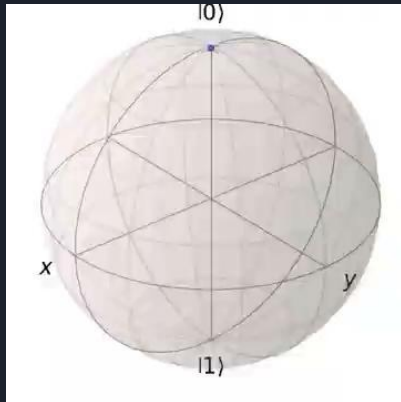
Execução por Hardware Quântico:

- Execução do circuito no computador quântico
- Requerem pagamento (exceto alguns casos)

Ruído e decoerência

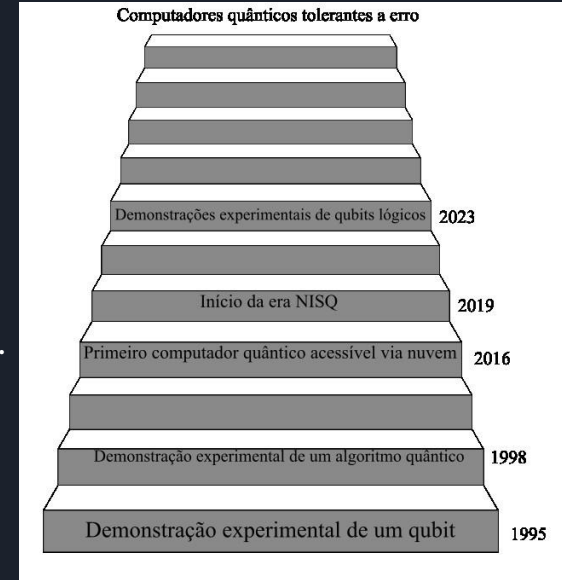
A Eq. de Schrödinger descreve a dinâmica de **sistemas quânticos fechados**. Na prática:

- Sistemas quânticos não são 100% isolados, gerando baixa **interação com o ambiente**.
- A interação com o ambiente leva a perda da informação dos qubits para o ambiente.
- Efeitos comuns de decoerência são o decaimento e a defasagem:



NISQ: Noisy Intermediate-Scale Quantum

- *Noisy*: Computadores quânticos com erros.
- *Intermediate-Scale*: Escala intermediária (50 - 1000 qubits).
 - Muitos qubits -> impossível simular classicamente.
 - Número de qubits, ainda assim, pequeno demais para protocolos de correção de erros
- Podem retornar bons resultados com circuitos rasos.
- Existe potencial para “benefício quântico” em tarefas específicas, sem comprovação.



Pós-processamento





Fazendo medidas em circuitos quânticos

- Medir qubits -> colapso da função de onda em estados da base computacional
- Após medir os resultados de um computador quântico, temos bits clássicos
- Resultados probabilísticos
- Muitos *shots* -> Estatística do sistema

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

$$P(|0\rangle) = |\alpha|^2$$

$$P(|1\rangle) = |\beta|^2$$



Pauli strings

- Operadores de Pauli: $\{I, X, Y, Z\}$
- Pauli String: Produto Tensorial de Operadores de Pauli através dos qubits
- Qualquer observável pode ser decomposto em Pauli Strings
- Importante para obter informações do sistema. Reconstrução de fase relativa:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$$



Pauli strings

- Reconstrução de fase relativa:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

Medindo somente a base computacional (0s e 1s):

$$P(0) = \cos^2(\theta/2) \qquad P(1) = \sin^2(\theta/2)$$

Pauli strings

- Reconstrução de fase relativa:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

Medindo somente a base computacional (0s e 1s):

$$P(0) = \cos^2(\theta/2) \qquad P(1) = \sin^2(\theta/2)$$

Sem informação sobre a fase relativa.





Pauli strings

- Reconstrução de fase relativa:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

Medindo somente os valores esperados de X e Y:

$$\langle X \rangle = \langle \psi | X | \psi \rangle = (\cos(\theta/2)\langle 0 | + e^{-i\phi}\sin(\theta/2)\langle 1 |) (\cos(\theta/2)|1\rangle + e^{i\phi}\sin(\theta/2)|0\rangle) = \sin\theta \cos\phi$$

$$\langle Y \rangle = \langle \psi | Y | \psi \rangle = (\cos(\theta/2)\langle 0 | + e^{-i\phi}\sin(\theta/2)\langle 1 |) (i\cos(\theta/2)|1\rangle - ie^{i\phi}\sin(\theta/2)|0\rangle) = \sin\theta \sin\phi$$

$$\phi = \arctan(\langle Y \rangle / \langle X \rangle)$$

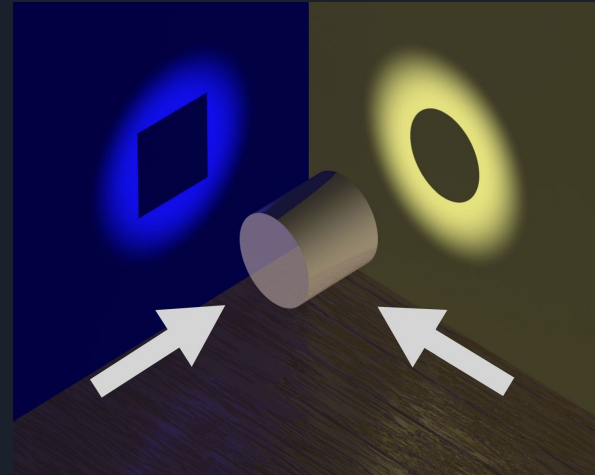


Tomografia de estados quânticos

- Reconstrução do estado quântico completo
- Requer medidas em todas as bases (Pauli Strings)
- Custo exponencial
- Útil apenas em baixa escala, para prova de conceito

Tomografia de estados quânticos

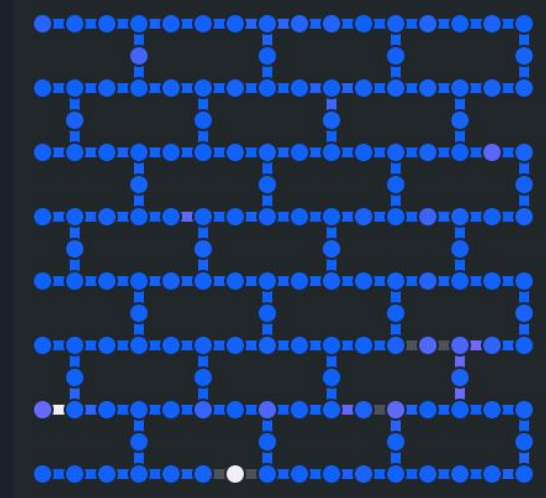
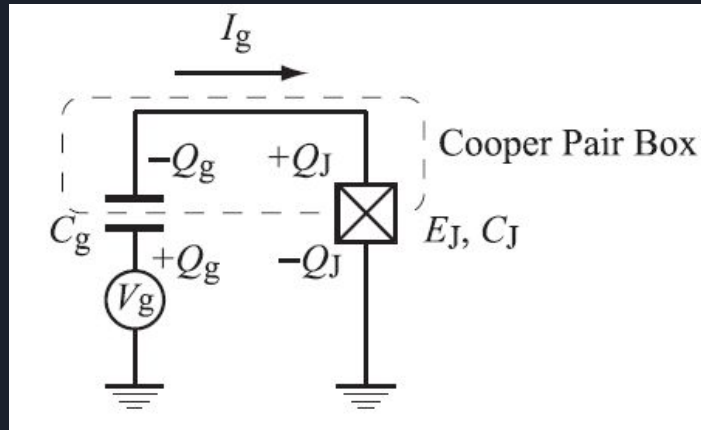
- Reconstrução do estado quântico completo
- Requer medidas em todas as bases (Pauli Strings)
- Custo exponencial
- Útil apenas em baixa escala, para prova de conceito
- Alternativa: shadow tomography





Ecosistema de plataformas quânticas

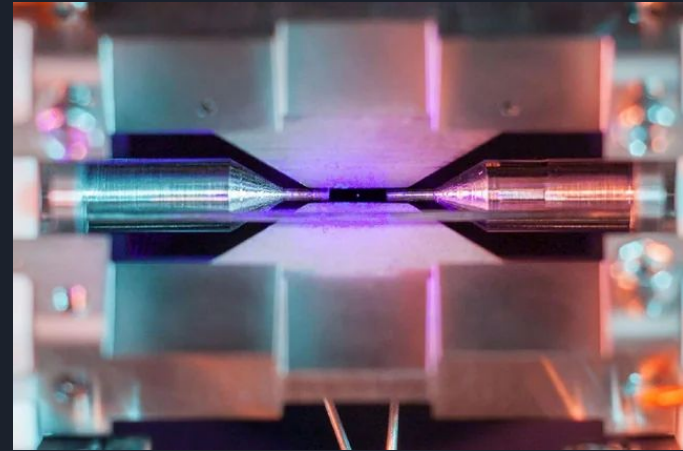
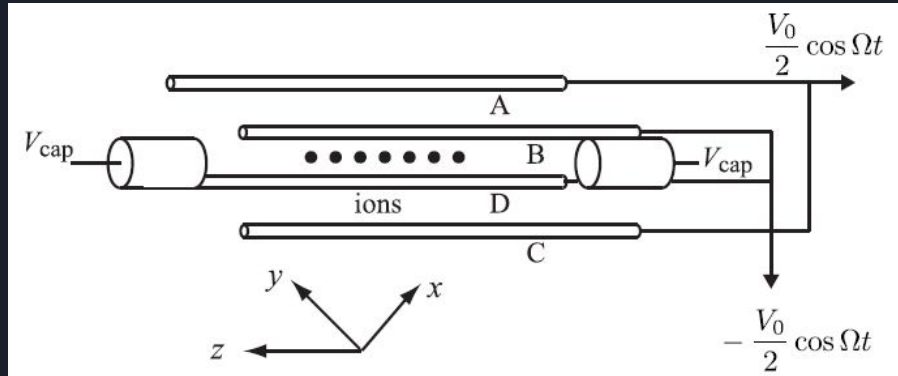
Hardware - Qubits Superconductores



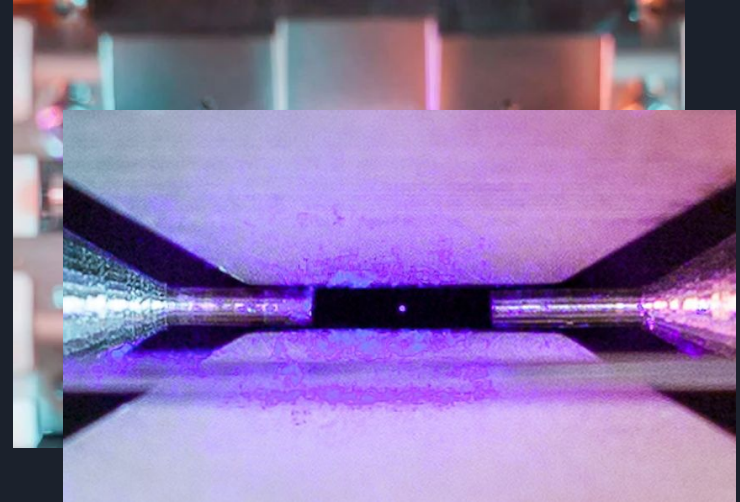
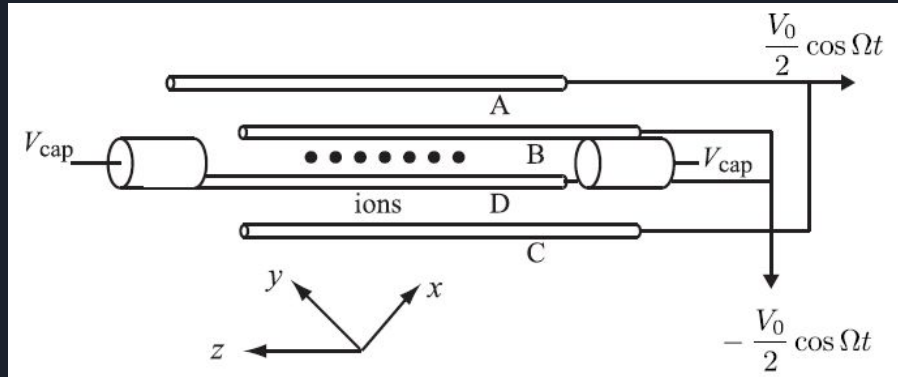
ibm_kingston



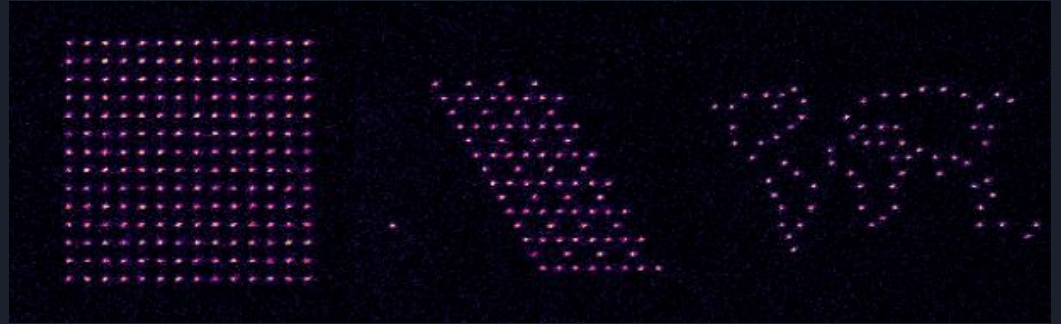
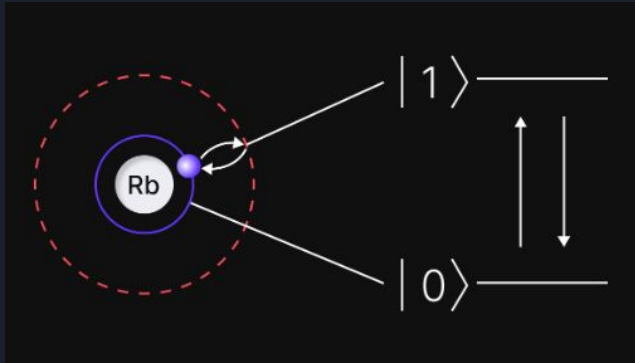
Hardware - Íons Aprisionados



Hardware - Íons Aprisionados



Hardware - Átomos Neutros



IQuEra>
Computing Inc.



Hardware

- Ressonância magnética nuclear
- Computação fotônica
- Quantum Dots
- Quantum Annealing





Software

 **CLASSIQ**



Cirq



QuForge



Qiskit



PENNYLANE

Algoritmos quânticos





Estados de Bell

- Estados maximamente entrelaçados

$$|\psi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\psi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\phi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\phi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

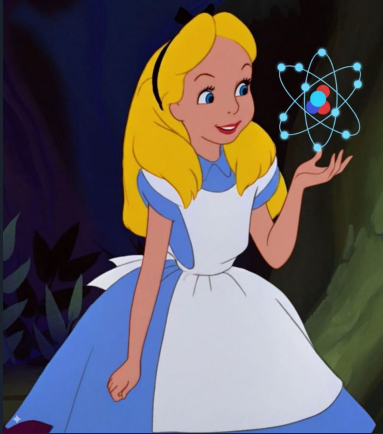


Estados de Bell

Teleportação quântica



Teleportação quântica



?





Teleportação quântica

Algoritmo quântico variacional

**QUANTUM DUCKY
LEARNS!**





$$|\phi\rangle \text{---} \boxed{RX(\theta)} \text{---} |\psi\rangle$$



Se pudermos controlar o ângulo da porta, podemos controlar o estado de saída.



Porta parametrizada



Se pudermos controlar o ângulo da porta, podemos controlar o estado de saída.



Aprendizado de máquina quântico: uma família de algoritmos

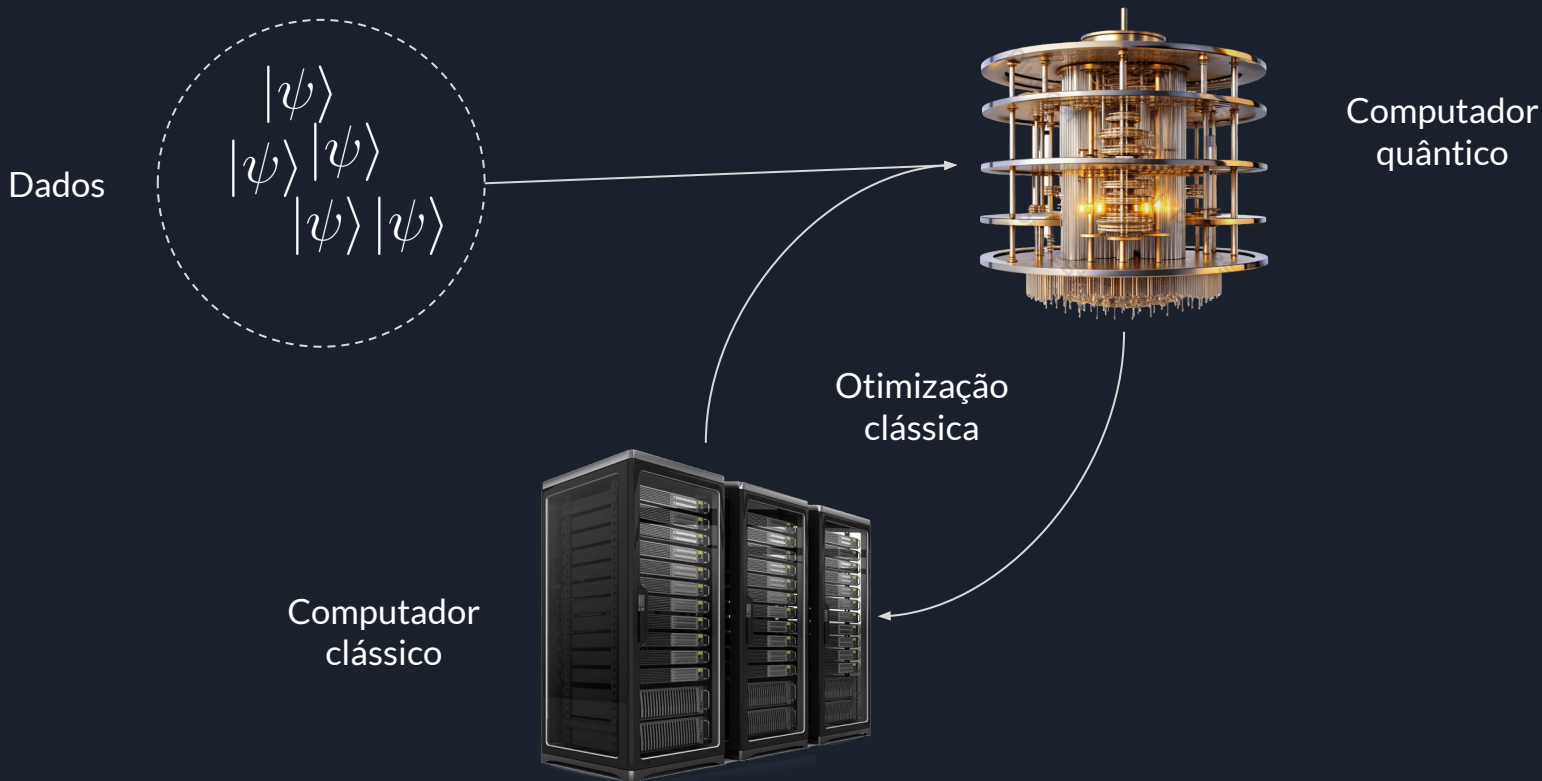
- Quantum kernel
- Quantum Feature Map
- Variational Quantum Algorithm
- Variational Quantum Eigensolver
- QAOA
- Quantum Support Vector Machine
- Quantum neural networks
- Quantum Boltzmann Machine
- Quantum annealing




Aprendizado de máquina quântico: uma família de algoritmos

- Quantum kernel
- Quantum Feature Map
- Variational Quantum Algorithm
- Variational Quantum Eigensolver
- QAOA
- Quantum Support Vector Machine
- Quantum neural networks
- Quantum Boltzmann Machine
- Quantum annealing

Algoritmo quântico variacional





Algoritmo quântico variacional

- Preparar dados
- Executar circuito
- Obter medidas
- Otimizar parâmetros

Algoritmo quântico variacional

- Preparar dados



Algoritmo quântico variacional

- Preparar dados
 - Codificação de dados clássicos
 - Preparação de estados quânticos
 - QRAM

$$RY(\text{👨🎓})|0\rangle = |\phi\rangle$$

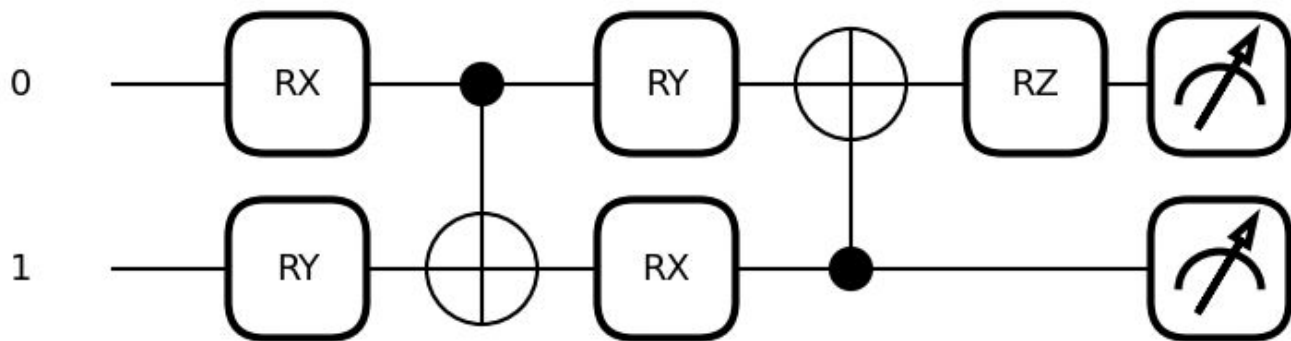
Algoritmo quântico variacional


- Executar circuito e realizar medida



Algoritmo quântico variacional

- Executar circuito e realizar medida






Algoritmo quântico variacional

- Otimizar parâmetros

medidas $\rightarrow \langle O \rangle$

função custo $\mathcal{L} = \mathcal{L}(\langle O \rangle, \langle \hat{O} \rangle)$


atualizar parâmetros $\theta \leftarrow \theta - \eta \frac{\partial \mathcal{L}}{\partial \theta}$



Algoritmo quântico variacional

- Otimizar parâmetros

função custo $\mathcal{L} = \frac{1}{2}(\langle \hat{O} \rangle - \langle O \rangle)^2$



Algoritmo quântico variacional

- Diferenciação automática → simulação clássica

$$|\psi\rangle = U_n(\theta_n)U_{n-1}(\theta_{n-1})\dots U_k(\theta_k)\dots U_1(\theta_1)|\phi\rangle$$

$$\frac{\partial |\psi\rangle}{\partial \theta_k} = U_n(\theta_n)U_{n-1}(\theta_{n-1})\dots \frac{\partial U_k(\theta_k)}{\partial \theta_k} \dots U_1(\theta_1)|\phi\rangle$$

- Regra do parameter-shift → computadores quânticos

$$\nabla_{\theta} \langle O \rangle = \frac{1}{2}(\langle O \rangle(\theta + \pi/2) - \langle O \rangle(\theta - \pi/2))$$

Algoritmo quântico variacional



Vamos ao código!

https://github.com/tiago939/minicurso_cq2025