Minicurso de Introdução à Computação Quântica

IX Semana da Computação (SECOMP - 2022)

Prof. Charles F. de Barros
Departamento de Ciência da Computação
UFSJ

O mundo quântico

- Universo na escala subatômica
- Fenômenos estranhos e contra-intuitivos ocorrem
- Partículas podem se encontrar em dois estados simultaneamente
- Partículas separadas por quilômetros de distância podem interagir instantaneamente
- A observação de um sistema interfere diretamente em seu estado

Por que estudar Computação Quântica?

- Tamanho e complexidade dos problemas computacionais
- Para muitos problemas não são conhecidas soluções eficientes
- Potencial de revolucionar a forma como resolvemos problemas

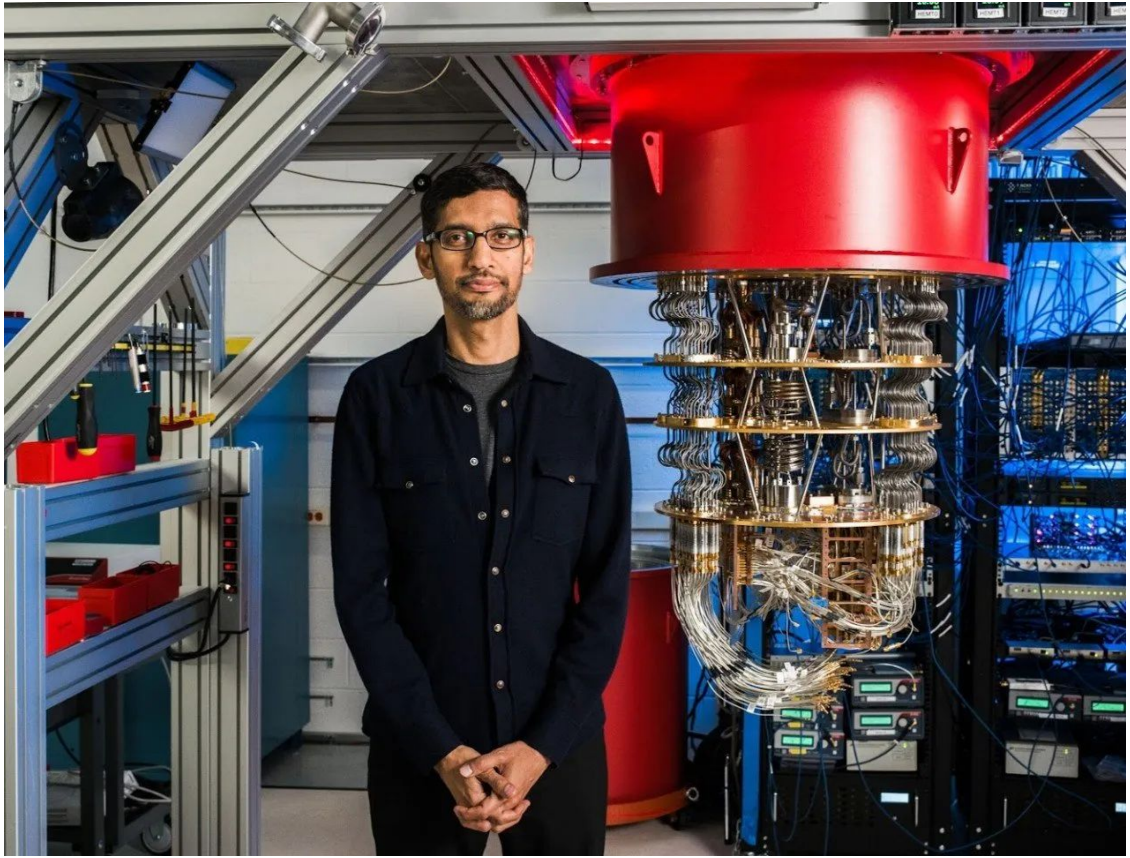
O que um computador quântico faz

- Resolve certos problemas de forma mais eficiente
- Explora fenômenos da Mecânica Quântica
- Superposição
- Emaranhamento

O que um computador quântico não faz

- Resolver qualquer problema de forma mais eficiente do que um computador clássico
- Há problemas para os quais não se conhece nenhuma solução eficiente, nem mesmo utilizando computadores quânticos
- Substituir o computador clássico

Computador quântico da IBM



Computador quântico da Google e Sundar Pichai, CEO da Alphabet Inc.

Computador quântico DWave

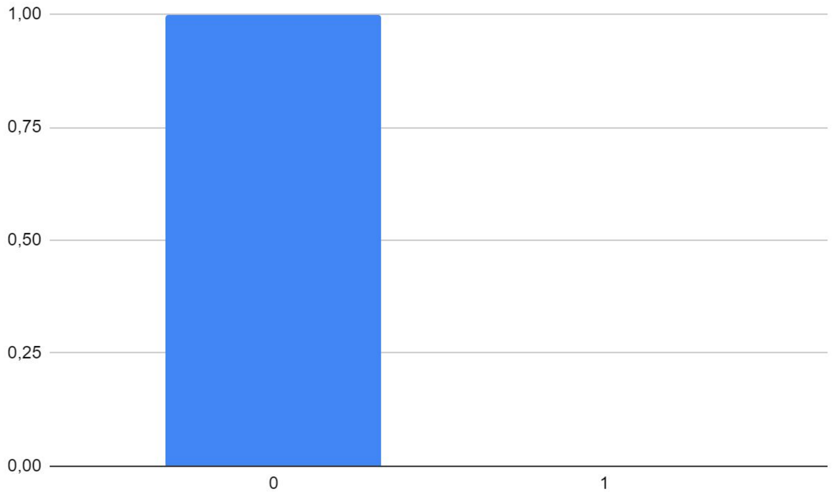
SpinQ Gemini: o primeiro desktop quântico?

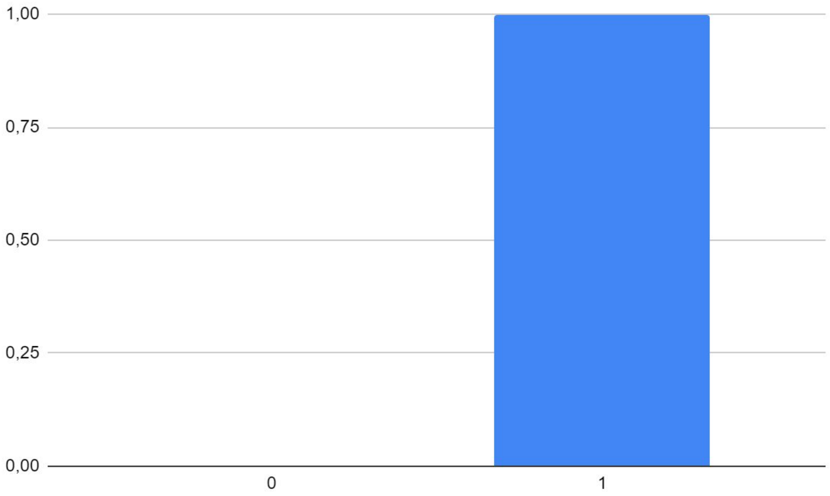
A unidade fundamental de informação em um computador quântico

Clássico vs. Quântico

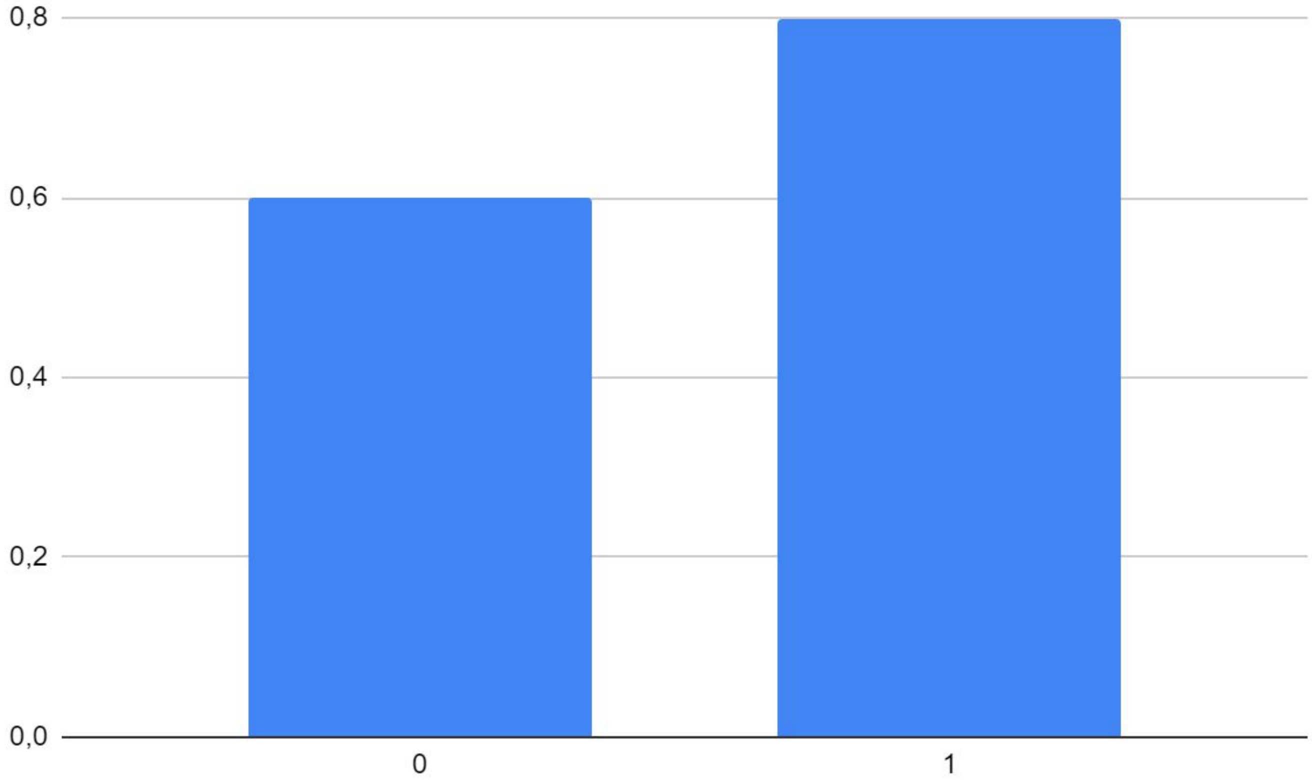
- No computador clássico, a unidade fundamental de informação é o **BIT**
- Dois estados possíveis: 0 ou 1
- Apenas um estado de cada vez

- No computador quântico é o **QUBIT**
- Dois estados possíveis
- Qualquer **SUPERPOSIÇÃO DESSES ESTADOS**
- “0 e 1 ao mesmo tempo”

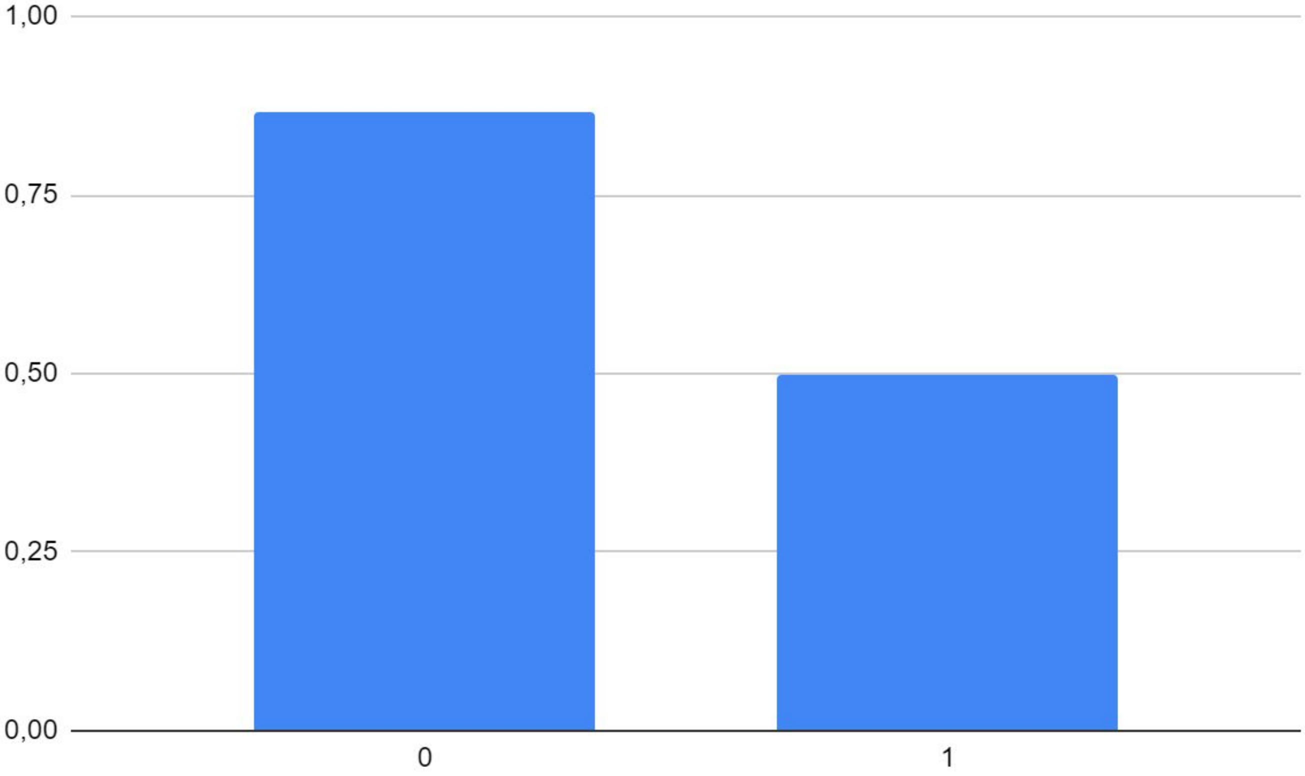




Estados de um bit



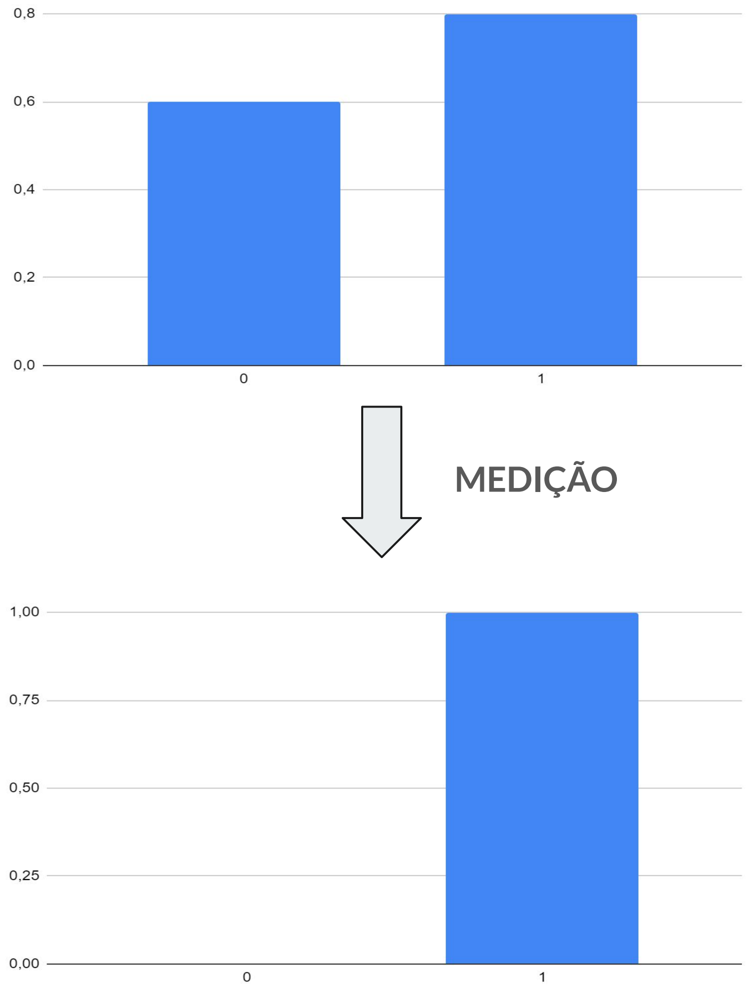
Estado possível de um qubit



Estado possível de um qubit

Medição

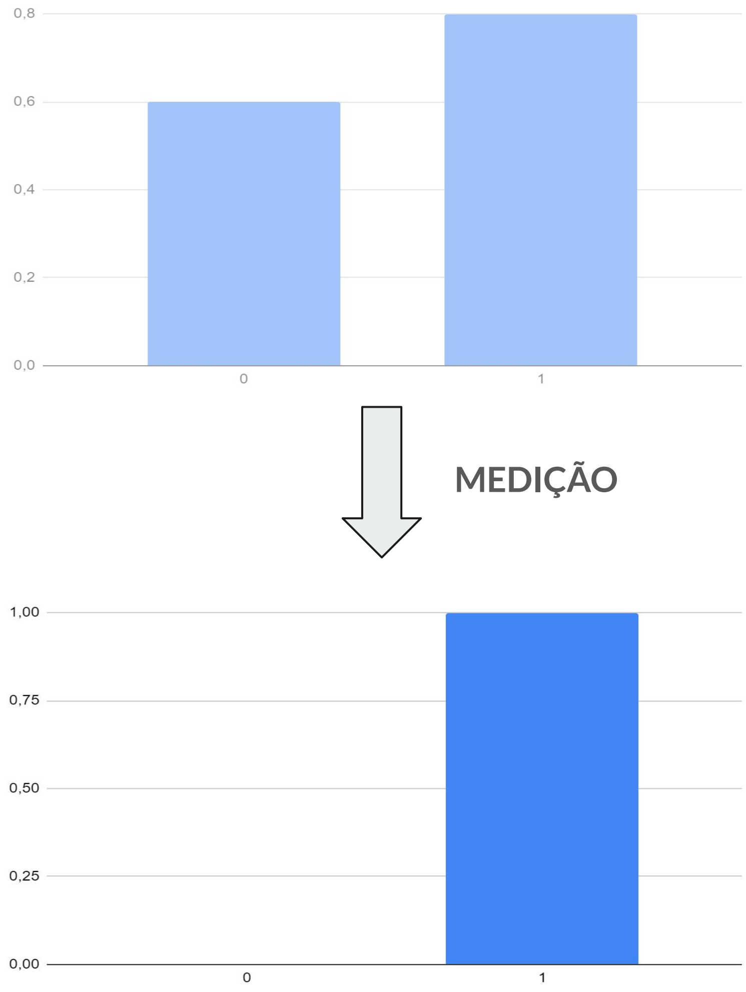
- A superposição só existe em nível quântico
- É preciso efetuar uma **MEDIÇÃO**
- Após a medição, o qubit colapsa para um dos estados possíveis
- Ao observar um sistema, nós interferimos nele
- Para cada estado possível há uma certa **PROBABILIDADE**



Medição

- A superposição só existe em nível quântico
- É preciso efetuar uma **MEDIÇÃO**
- Após a medição, o qubit colapsa para um dos estados possíveis
- Ao observar um sistema, nós interferimos nele
- Para cada estado possível há uma certa **PROBABILIDADE**

Isto irá ocorrer com probabilidade 64%



Descrição matemática do qubit

- Cada estado possível é representado por um **VETOR**

NOTAÇÃO DE DIRAC

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

- **Esses vetores formam a BASE de um ESPAÇO VETORIAL**

BASE COMPUTACIONAL

Descrição matemática do qubit

- Todo qubit é uma **COMBINAÇÃO LINEAR** dos vetores da base:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \alpha, \beta \in \mathbb{C}$$

- Condição:

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

Descrição matemática do qubit

- O qubit é um **VETOR UNITÁRIO**

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$$

Descrição matemática do qubit

$$\alpha = \text{Amplitude do estado } |0\rangle$$
$$|\alpha|^2 = \text{Probabilidade do estado } |0\rangle$$

$$\beta = \text{Amplitude do estado } |1\rangle$$
$$|\beta|^2 = \text{Probabilidade do estado } |1\rangle$$

Exemplo 1:

$$|\psi\rangle = 0,6\,|0\rangle + 0,8\,|1\rangle = \begin{pmatrix} 0,6 \\ 0,8 \end{pmatrix}$$

$$\mathrm{Prob}[|0\rangle] = 0,6^2 = 36\%$$

$$\mathrm{Prob}[|1\rangle] = 0,8^2 = 64\%$$

Exemplo 2:

$$|\psi\rangle = \frac{1}{2}|0\rangle + \left(\frac{1}{2} + \frac{i}{\sqrt{2}}\right)|1\rangle$$

$$\text{Prob}[|0\rangle] = \left(\frac{1}{2}\right)^2 = 25\%$$

$$\text{Prob}[|1\rangle] = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 75\%$$

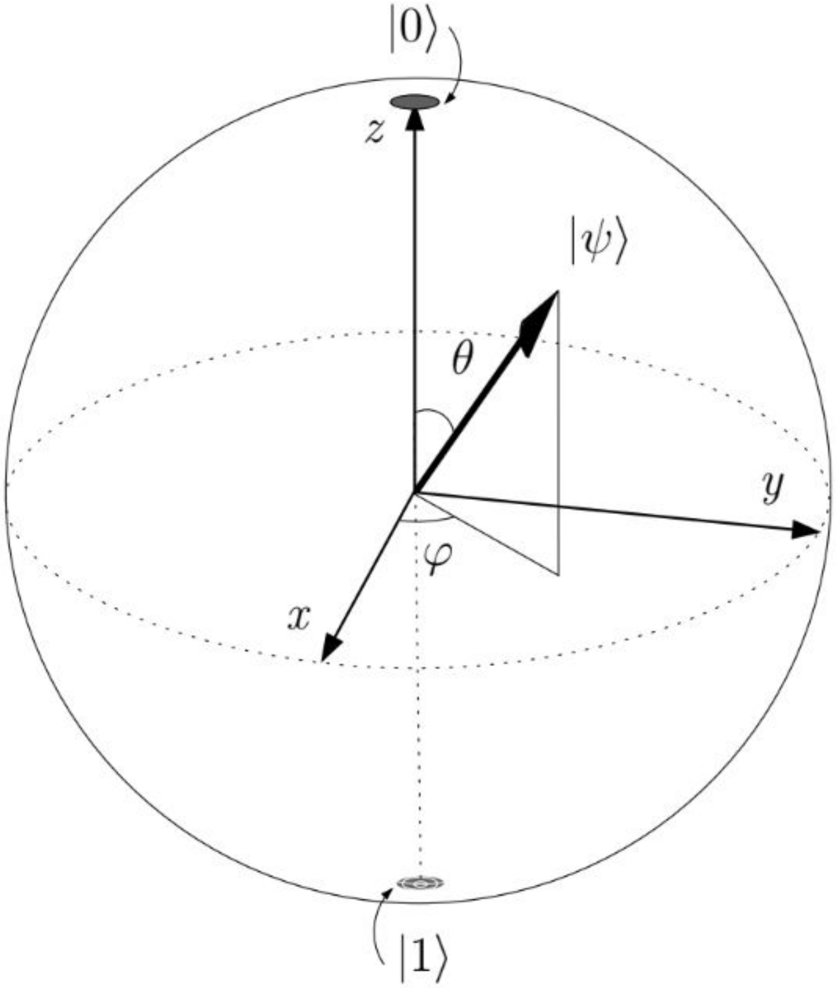
Esfera de Bloch

- Visualização do qubit em 3 dimensões
- Representação polar do qubit

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\mathrm{sen}\,\frac{\theta}{2}|1\rangle$$

$$0 \leq \theta \leq \pi$$

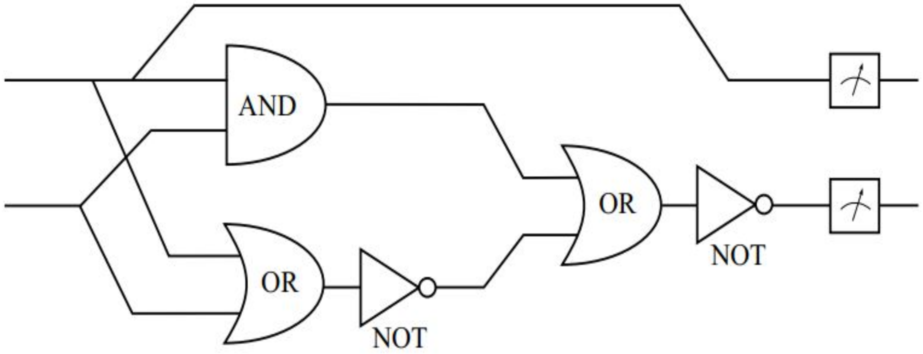
$$0 \leq \varphi < 2\pi$$



Portas quânticas

Portas e circuitos

- Um computador é uma máquina que executa funções sobre um conjunto de bits de entrada
- Estas funções são descritas por sequências de operações
- Cada operação é representada por uma **PORTA LÓGICA**



Portas quânticas

- Descrevem operações realizadas sobre um ou mais qubits
- Toda porta quântica pode ser descrita por um **OPERADOR UNITÁRIO**
- **Transforma um vetor unitário em outro vetor unitário**
- “A evolução no tempo de um sistema quântico isolado será descrita por uma transformação unitária”

Operadores unitários

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

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

Operador adjunto

Conjugada complexa

$$U = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$U^* = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

$$U^\dagger = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Porta bit-flip (Pauli-X)

- Rotação em torno do eixo X da esfera de Bloch
- Atuação sobre os vetores da base:

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

Representação matricial

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

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

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

Atuação da porta Pauli-X sobre um qubit genérico

$$\begin{aligned} X(\alpha|0\rangle + \beta|1\rangle) &= \alpha X|0\rangle + \beta X|1\rangle \\ &= \beta|0\rangle + \alpha|1\rangle \end{aligned}$$

Exercício:

1) Quais são os autovetores da porta Pauli-X?

Porta Pauli-Y

- Rotação em torno do eixo Y da esfera de Bloch
- Atuação sobre os vetores da base:

$$Y|0\rangle = i|1\rangle$$

$$Y|1\rangle = -i|0\rangle$$

Representação matricial

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

$$Y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix}$$

$$Y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix}$$

Atuação da porta Pauli-Y sobre um qubit genérico

$$Y(\alpha|0\rangle + \beta|0\rangle) = -i\beta|0\rangle + i\alpha|1\rangle$$

Tem um erro aqui, é 1 e não 0

Exercício:

1) Quais são os autovetores da porta Pauli-Y?

Porta Pauli-Z (phase-flip)

- Rotação em torno do eixo Z da esfera de Bloch
- Atuação sobre os vetores da base:

$$Z|0\rangle = |0\rangle$$

$$Z|1\rangle = -|1\rangle$$

Representação matricial

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

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

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

Atuação da porta Pauli-Z sobre um qubit genérico

$$Z(\alpha |0\rangle + \beta |0\rangle) = \alpha |0\rangle - \beta |1\rangle$$

Tem um erro aqui, é 1 e não 0

Exercício:

1) Quais são os autovetores da porta Pauli-Z?

Porta Hadamard

- Cria uma superposição uniforme
- Atuação sobre os vetores da base:

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

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

Representação matricial

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

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

Atuação da porta Hadamard sobre um qubit genérico

$$H(\alpha|0\rangle + \beta|1\rangle) = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|1\rangle$$

Exercício:

1) Provar a igualdade acima.
2) Provar que o resultado é um vetor unitário
3) **Quais são os autovetores do operador Hadamard?
4) Localize na esfera de Bloch os resultados da atuação da porta Hadamard sobre os vetores da base computacional

Representação de portas em circuitos quânticos

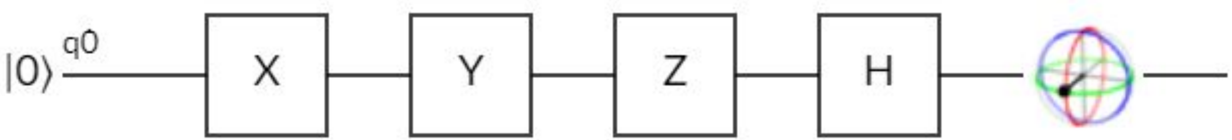
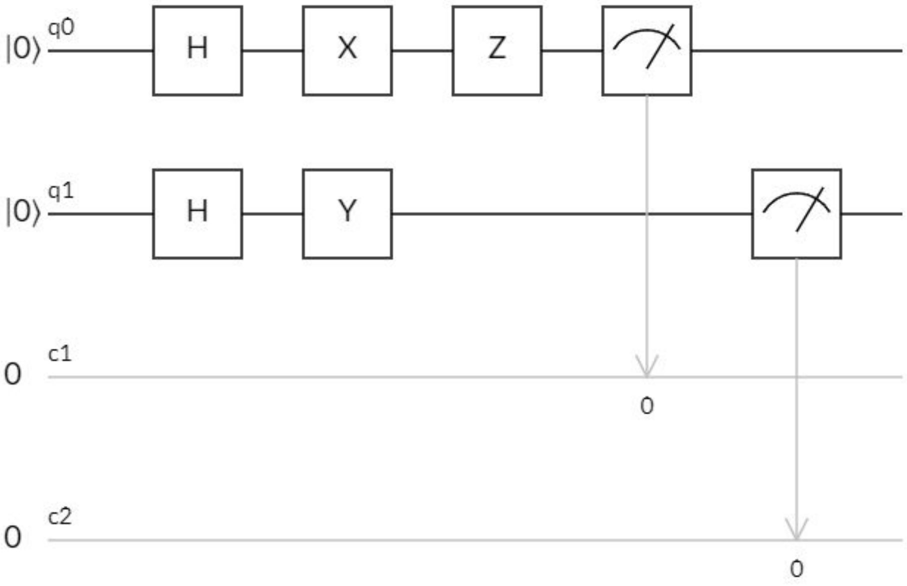


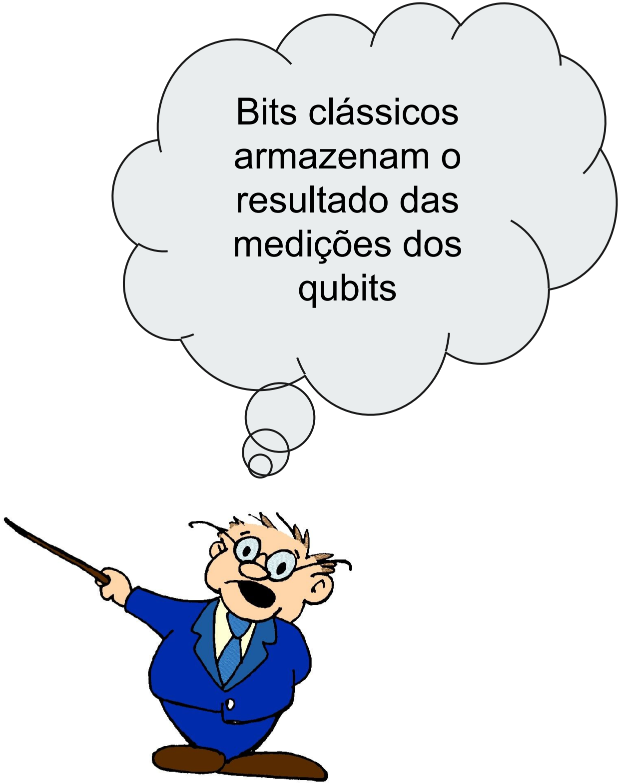
Imagem extraída de **quantum-circuit.com**

Como descrever um estado de dois ou mais qubits?

- Circuitos quânticos descrevem a evolução de um conjunto de qubits, denominado **REGISTRADOR**
- Portas quânticas podem atuar sobre dois ou mais qubits
- Estados com dois ou mais qubits são representados matematicamente pelo **PRODUTO TENSORIAL**

Um circuito com 2 qubits





Produto tensorial

Definição

- Utilizado para representar matematicamente um conjunto de dois ou mais qubits em superposição
- Também representa portas que atuam sobre mais de um qubit
- É uma operação recebe como entrada dois estados, com m e n linhas respectivamente, e retorna um estado de mn linhas

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \Longrightarrow |0\rangle \otimes |0\rangle = |00\rangle$$

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \Longrightarrow |0\rangle \otimes |1\rangle = |01\rangle$$

Produto tensorial dos qubits da base computacional

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \Longrightarrow |1\rangle \otimes |0\rangle = |10\rangle$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \Longrightarrow |1\rangle \otimes |1\rangle = |11\rangle$$

Produto tensorial dos qubits da base computacional

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) =$$

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

Produto tensorial de dois qubits genéricos

Descrição genérica de um estado de 2 qubits

$$|\psi\rangle = x\,|00\rangle + y\,|01\rangle + z\,|10\rangle + w\,|11\rangle$$

$$|x|^2 + |y|^2 + |z|^2 + |w|^2 = 1$$

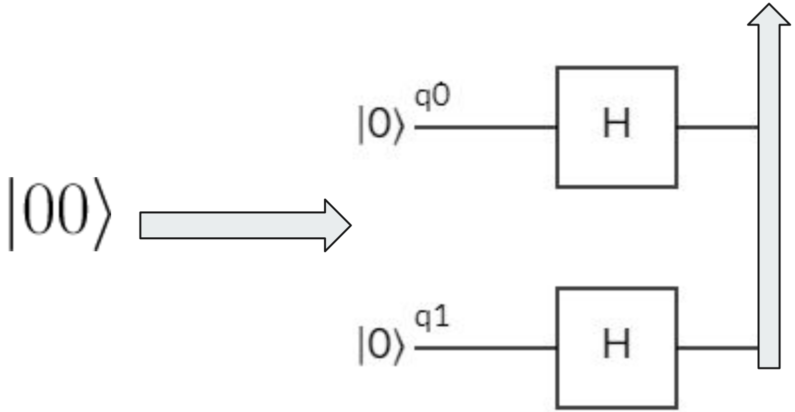
Descrição genérica de um estado de 2 qubits

- É um **VETOR UNITÁRIO**

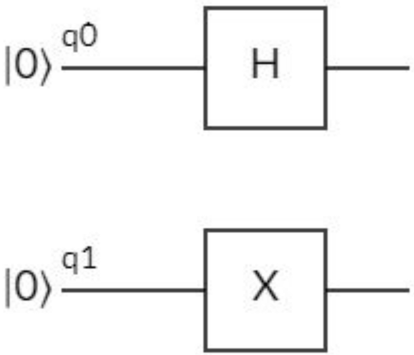
$$\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} \in \mathbb{C}^4$$

Exemplo:

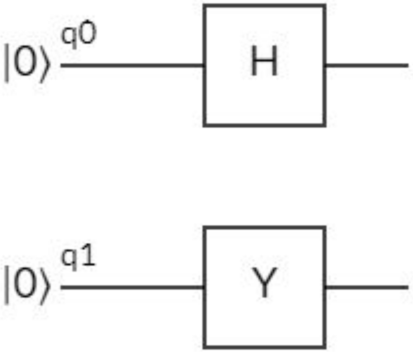
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$



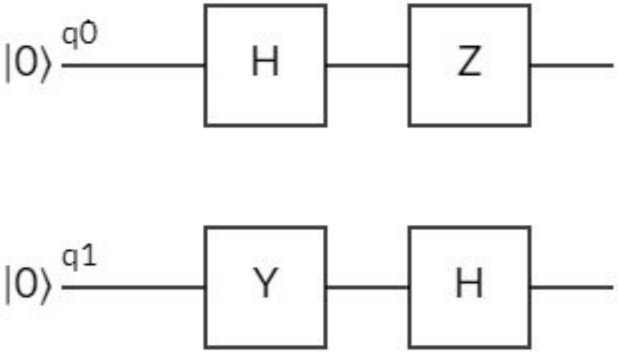
Exercício: descreva o estado resultante em cada circuito



(1)



(2)



(3)

Simplificação da notação

$$\{|00\rangle\,,|01\rangle\,,|10\rangle\,,|11\rangle\}$$

$$\{|0\rangle\,,|1\rangle\,,|2\rangle\,,|3\rangle\}$$

Base computacional do espaço $\mathbb{C}^4$

E se tivermos 3 qubits?

$$\begin{cases} |0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle = |0\rangle \\ |0\rangle \otimes |0\rangle \otimes |1\rangle = |001\rangle = |1\rangle \\ |0\rangle \otimes |1\rangle \otimes |0\rangle = |010\rangle = |2\rangle \\ |0\rangle \otimes |1\rangle \otimes |1\rangle = |011\rangle = |3\rangle \end{cases}$$

$$\begin{cases} |1\rangle \otimes |0\rangle \otimes |0\rangle = |100\rangle = |4\rangle \\ |1\rangle \otimes |0\rangle \otimes |1\rangle = |101\rangle = |5\rangle \\ |1\rangle \otimes |1\rangle \otimes |0\rangle = |110\rangle = |6\rangle \\ |1\rangle \otimes |1\rangle \otimes |1\rangle = |111\rangle = |7\rangle \end{cases}$$

Simplificação da notação

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

$$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle\}$$

Base computacional do espaço $\mathbb{C}^8$

Generalizando...

Um estado genérico de n qubits será representado por

$$\sum_{i=0}^{2^n-1} z_i \left|i\right\rangle$$

com a condição

$$\sum_{i=0}^{2^n-1} |z_i|^2 = 1$$

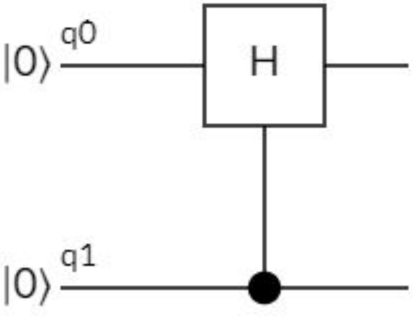
Portanto, um **VETOR UNITÁRIO**

$$\begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{2^n-1} \end{pmatrix} \in \mathbb{C}^{2^n}$$

Emaranhamento

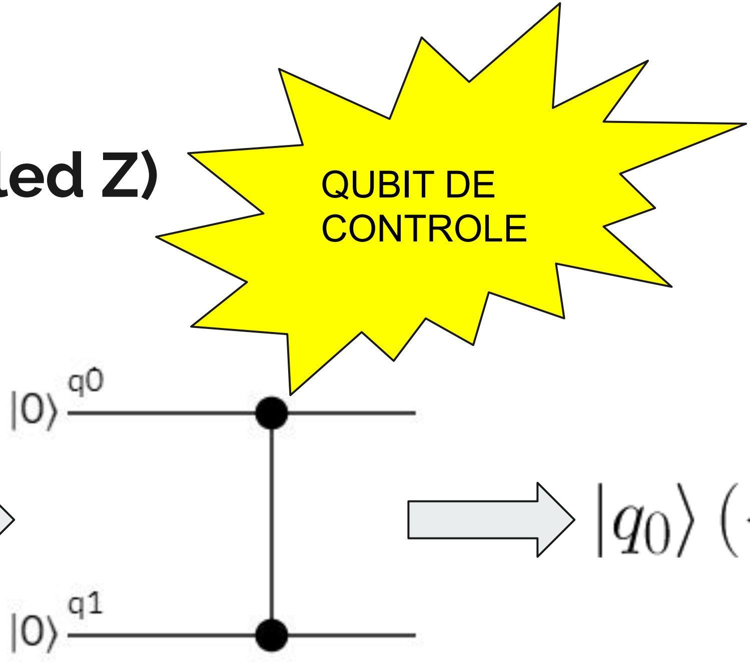
Portas controladas

- Bit/qubit de controle
- Qubit alvo
- A operação é realizada sobre o qubit alvo se o bit/qubit de controle for 1
- O bit/qubit de controle não é alterado



Porta Hadamard controlada

Porta CZ (Controlled Z)



$$|q_0 q_1\rangle \Rightarrow |q_0\rangle \, (-1)^{q_0 \wedge q_1} \, |q_1\rangle$$

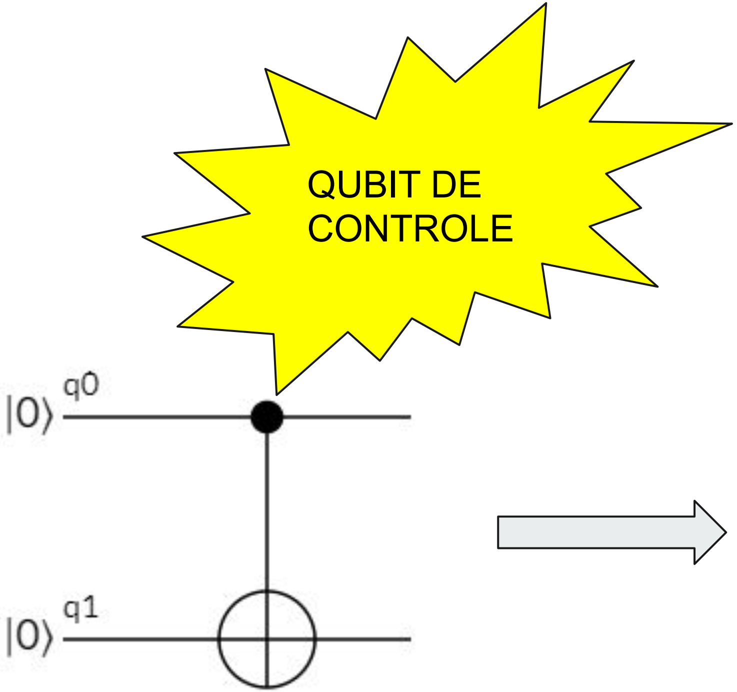
Atuação sobre os vetores da base computacional e representação matricial

$$\begin{cases} CZ\,|00\rangle = |00\rangle \\ CZ\,|01\rangle = |01\rangle \\ CZ\,|10\rangle = |10\rangle \\ CZ\,|11\rangle = -\,|11\rangle \end{cases}$$

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Porta CNOT

$$|q_0\rangle\,|q_1\rangle$$



$$|q_0\rangle\,|q_0 \oplus q_1\rangle$$

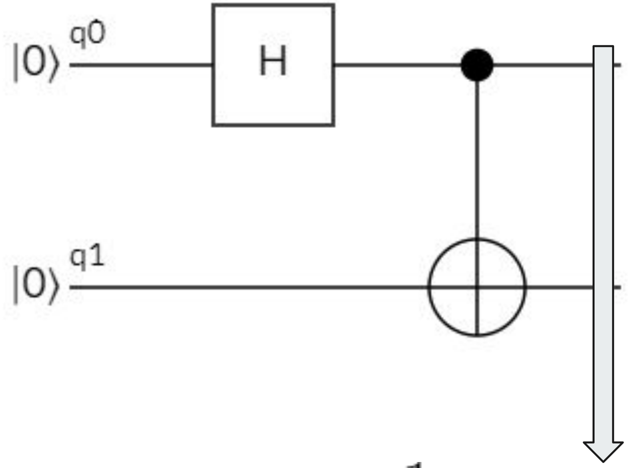
Atuação sobre os vetores da base computacional e representação matricial

$$\begin{cases} \mathrm{CNOT}\,|00\rangle = |00\rangle \\ \mathrm{CNOT}\,|01\rangle = |01\rangle \\ \mathrm{CNOT}\,|10\rangle = |11\rangle \\ \mathrm{CNOT}\,|11\rangle = |10\rangle \end{cases}$$

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

Determine o estado resultante

- Trata-se de um estado de 2 qubits
- Logo...



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

$$|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

$$\begin{cases} \alpha\gamma &= 1/\sqrt{2} \\ \alpha\delta &= 0 \\ \beta\gamma &= 0 \\ \beta\delta &= 1/\sqrt{2} \end{cases}$$

O sistema não tem solução

- Embora se trate de um estado de 2 qubits...
- É impossível descrever o estado de cada qubit isoladamente
- Este fenômeno é denominado **EMARANHAMENTO**
- Um estado emaranhado é aquele no qual não se pode descrever cada qubit de forma isolada
- A medição de um dos qubits fará o outro colapsar instantaneamente

Estados de Bell (emaranhamento máximo)

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

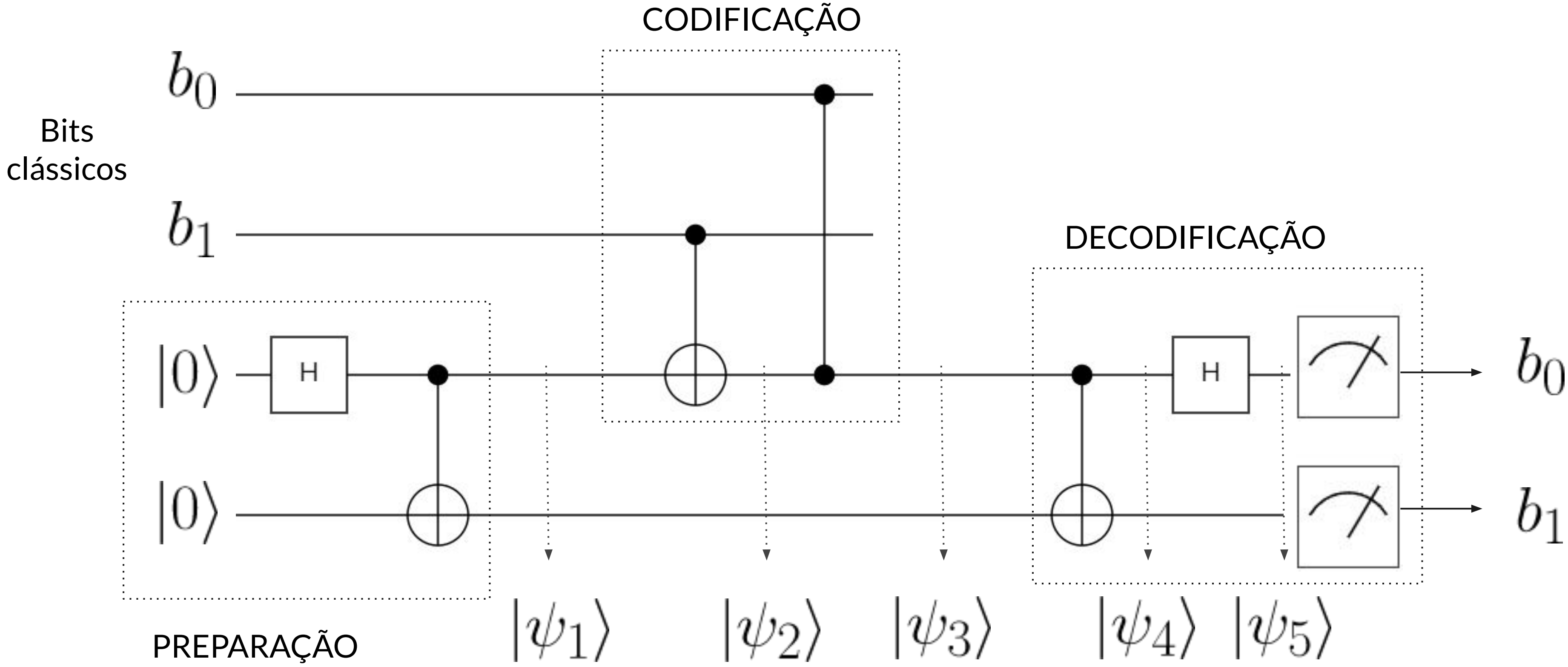
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Exercício: verifique que esses estados são, de fato, emaranhados

Aplicação: codificação superdensa

Objetivo: transmitir dois bits clássicos utilizando apenas 1 qubit

1. Preparação: pré-compartilhamento de um par de qubits emaranhados
2. Codificação: dois bits clássicos são "empacotados" no primeiro qubit
3. Decodificação: operador unitário + medição



Circuito para codificação superdensa

Preparação

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$$

Codificação

Notação simplificada do produto tensorial

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|b_1\rangle|0\rangle + |1 \oplus b_1\rangle|1\rangle)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}((-1)^{b_0 \wedge b_1}|b_1\rangle|0\rangle + (-1)^{b_0 \wedge (1 \oplus b_1)}|1 \oplus b_1\rangle|1\rangle)$$

Decodificação

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}((-1)^{b_0 \wedge b_1} |b_1\rangle |b_1\rangle + (-1)^{b_0 \wedge (1 \oplus b_1)} |1 \oplus b_1\rangle |b_1\rangle)$$

$$= \frac{1}{\sqrt{2}}((-1)^{b_0 \wedge b_1} |b_1\rangle + (-1)^{b_0 \wedge (1 \oplus b_1)} |1 \oplus b_1\rangle) |b_1\rangle$$

Decodificação

Hadamard sobre o primeiro qubit

- 1º caso: $b_0 = 0$

$$|\psi_5\rangle = \frac{1}{\sqrt{2}}(H|b_1\rangle + H|1 \oplus b_1\rangle)|b_1\rangle$$

$$= |0\rangle|b_1\rangle = |b_0\rangle|b_1\rangle$$

Decodificação

Hadamard sobre o primeiro qubit

- 2º caso: $b_0 = 1$ e $b_1 = 0$

$$|\psi_5\rangle = \frac{1}{\sqrt{2}}(H|b_1\rangle - H|1 \oplus b_1\rangle)|b_1\rangle$$

$$= \frac{1}{\sqrt{2}}\frac{2}{\sqrt{2}}|1\rangle|b_1\rangle = |b_0\rangle|b_1\rangle$$

Decodificação

Hadamard sobre o primeiro qubit

- 3º caso: $b_0 = 1$ e $b_1 = 1$

$$|\psi_5\rangle = \frac{1}{\sqrt{2}}(-H|b_1\rangle + H|1 \oplus b_1\rangle)|b_1\rangle$$

$$= \frac{1}{\sqrt{2}}\frac{2}{\sqrt{2}}|1\rangle|b_1\rangle = |b_0\rangle|b_1\rangle$$

Explorando o paralelismo quântico: o algoritmo de Deutsch

O problema

Considere uma função

$$f : \{0,1\} \to \{0,1\}$$

OBJETIVO: determinar o valor de

$$f(0) \oplus f(1)$$

Solução clássica

Calculamos o valor da função nas duas entradas possíveis.

FAZEMOS DUAS QUERIES À FUNÇÃO

Solução quântica: ALGORITMO DE DEUTSCH

A solução quântica consiste em resolver o mesmo problema fazendo **apenas uma query** à função.

O Oráculo ou “caixa preta”

Circuito que calcula o valor da função, mas não nos dá informação sobre o seu funcionamento interno

$$U_f : |x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle$$

Aplicando o oráculo sobre um estado em superposição

$$U_f\left(\frac{1}{\sqrt{2}}\left|0\right\rangle\left|0\right\rangle+\frac{1}{\sqrt{2}}\left|1\right\rangle\left|0\right\rangle\right)$$

Calculamos f(0) e f(1) “ao mesmo tempo”!!!

$$=\frac{1}{\sqrt{2}}\left|0\right\rangle\left|f(0)\right\rangle+\frac{1}{\sqrt{2}}\left|1\right\rangle\left|f(1)\right\rangle$$

O oráculo como porta controlada

$$\hat{U}_f \, |y\rangle = |y \oplus f(x)\rangle$$

Controlado pelo
primeiro qubit

Teorema:

Este operador tem como autovetor o estado

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

Prova:

$$\hat{U}_f \left|-\right\rangle = \frac{1}{\sqrt{2}}(\hat{U}_f \left|0\right\rangle - \hat{U}_f \left|1\right\rangle) = \frac{1}{\sqrt{2}}(\left|f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle)$$

$$f(x) = 0 \rightarrow \hat{U}_f \left|-\right\rangle = \left|-\right\rangle$$

$$f(x) = 1 \rightarrow \hat{U}_f \left|-\right\rangle = -\left|-\right\rangle$$

$$\Rightarrow \quad \hat{U}_f \left|-\right\rangle = (-1)^{f(x)} \left|-\right\rangle$$

AUTOVALOR

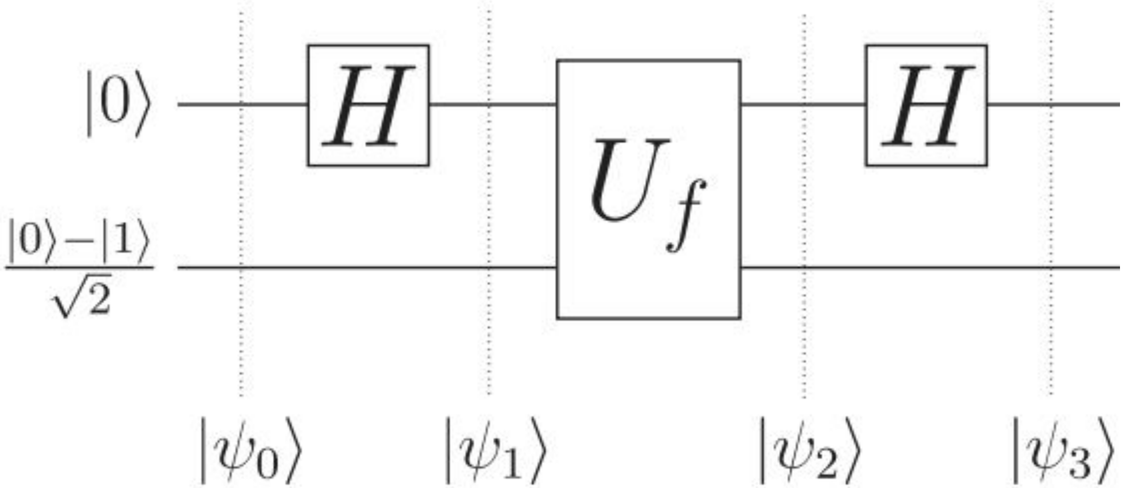
Portanto...

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

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

Phase
kick-back

O circuito para o algoritmo de Deutsch



Estado inicial

Pode ser preparado com uma porta Hadamard

$$|\psi_0\rangle = |0\rangle\,|-\rangle$$

Após a aplicação da primeira Hadamard

$$|\psi_1\rangle = |+\rangle\,|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |-\rangle$$

Após a aplicação do “Oráculo”

$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{\sqrt{2}}(U_f\,|0\rangle\,|-\rangle + U_f\,|1\rangle\,|-\rangle) \\
&= \frac{1}{\sqrt{2}}((-1)^{f(0)}\,|0\rangle\,|-\rangle + (-1)^{f(1)}\,|1\rangle\,|-\rangle) \\
&= \frac{1}{\sqrt{2}}((-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle)\,|-\rangle
\end{aligned}
$$

Isolamos
o 2º qubit

Aplicando Hadamard sobre o 1º qubit...

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)}H|0\rangle + (-1)^{f(1)}H|1\rangle)|-\rangle$$

1º caso: $f(0) \oplus f(1) = 0$

$f(0) \oplus f(1)$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(\pm H|0\rangle \pm H|1\rangle)|-\rangle$$

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

2º caso: $f(0) \oplus f(1) = 1$

$f(0) \oplus f(1)$

$$
\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{2}}(\pm H|0\rangle \mp H|1\rangle)|-\rangle \\
&= \frac{1}{\sqrt{2}}(\pm \frac{2}{\sqrt{2}}|1\rangle)|-\rangle = \pm|1\rangle|-\rangle
\end{aligned}
$$

Em ambos os casos, a medição do primeiro qubit nos dará o valor de

$$f(0) \oplus f(1)$$

Resumo

- A Computação Quântica apresenta um novo paradigma, através da exploração de fenômenos da Mecânica Quântica para resolver certos problemas de maneira mais eficiente
- Explora o paralelismo através do fenômeno da superposição, em que um qubit pode representar simultaneamente 0 e 1
- Explora ainda o fenômeno do emaranhamento, permitindo que partículas interajam de modo instantâneo, mesmo separadas por uma distância arbitrária

Obrigado!

Contato:
charlesbarros@ufsj.edu.br