Computação Quânica: O básico

Teo Haeser Gallarza

March 27, 2020

Índice

Algebra Linear

Autômato Finito

- Espaço Vetorial
  - Vetores assumem a notação de Dirac:

$$|\psi\rangle = (z_0, z_1, \ldots, z_{n-1}) = \begin{bmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{bmatrix}$$

- Base e Dimensão
  - Base canônica ou base computacional:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} , \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} , \quad \cdots , \quad |n-1\rangle^{=} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} .$$

- Bases para 1 qubit:

$$\begin{aligned}
\mathcal{I} = \mathcal{Z} &= \{\, |0\rangle \;,\; |1\rangle \,\} \\
\mathcal{X} &= \left\{ |+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \;,\; |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\} \\
\mathcal{Y} &= \left\{ |+i\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), |-i\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle) \right\}
\end{aligned}$$

- Matriz de mudança de base e Hadamard:

$$H = [I]_{\mathcal{X}}^{\mathcal{I}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Mudanças de bases com Hadamard:

$$H|0\rangle = |+\rangle \qquad H|+\rangle = |0\rangle$$
$$H|1\rangle = |-\rangle \qquad H|-\rangle = |1\rangle$$

- Produto interno:

$$(\,|\phi\rangle\,,|\psi\rangle\,) = \langle\phi|\psi\rangle = \begin{bmatrix} {w_0}^* & {w_1}^* & \cdots & {w_{n-1}}^* \end{bmatrix} \cdot \begin{bmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{bmatrix} = \sum_{k=0}^{n-1} {w_k}^* z_k$$

- Definição de $\langle\phi|$:

$$\langle\phi| = |\phi\rangle^\dagger = \begin{bmatrix} w_0 \\ \vdots \\ w_{n-1} \end{bmatrix}^\dagger = \begin{bmatrix} {w_0}^* & {w_1}^* & \cdots & {w_{n-1}}^* \end{bmatrix}$$

- Outros conceitos importantes
  - Norma

$$\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle} \geq 0$$

  - Base Ortogonal
  - Transformação Linear
  - Autovetores e autovalores

- Produto tensorial

$$
\begin{aligned}
|00\rangle &= |0\rangle\,|0\rangle = |0\rangle \otimes |0\rangle \\
|01\rangle &= |0\rangle\,|1\rangle = |0\rangle \otimes |1\rangle \\
|10\rangle &= |1\rangle\,|0\rangle = |1\rangle \otimes |0\rangle \\
|11\rangle &= |1\rangle\,|1\rangle = |1\rangle \otimes |1\rangle
\end{aligned}
$$

- Produto de Kronecker

$$|v\rangle \otimes |w\rangle = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{bmatrix} = \begin{bmatrix} a_0 |w\rangle \\ a_1 |w\rangle \\ \vdots \\ a_{n-1} |w\rangle \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ \vdots \\ a_0 b_{m-1} \\ a_1 b_0 \\ a_1 b_1 \\ \vdots \\ a_{n-1} b_{m-1} \end{bmatrix}$$

Mecânica Quântica

Postulados

- Postulado 1
  - Um sistema fısico isolado e descrito por uma espaco de Hilbert H com escalares complexos. Esse espaco vetorial e chamado espaço de estados. Um estado do sistema é descrito pelo chamado vetor de estado, um vetor unitario no espaco de estados do sistema.
- Postulado 2
  - A evoluçao temporal de um sistema fısico fechado e dada por um operador linear unitario no seu espaço de estados H. Em símbolos: $|\phi_f\rangle = U\left|\phi_j\right\rangle$

- Postulado 3:
  - possıveis resultados da medida do observável
- Valor esperado de um Observável
- Postulado 4:
  - A composiçao de sistemas dados por H_1, H_2, ..., H_N e descrita pelo produto tensorial

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_N$$

Exemplo

$$
\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\
|\psi_2\rangle &= |0\rangle \ .
\end{aligned}
$$

A composição dos dois qubits é modelada pelo espaço de Hilbert $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = \mathbb{C}^2 \otimes \mathbb{C}^2$, e o estado do sistema composto é descrito por

$$
\begin{aligned}
|\psi\rangle_{1,2} &= |\psi_1\rangle_1 \otimes |\psi_2\rangle_2 \\
&= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)_1 \otimes |0\rangle_2 \\
&= \frac{1}{\sqrt{2}}|0\rangle_1 \otimes |0\rangle_2 + \frac{1}{\sqrt{2}}|1\rangle_1 \otimes |0\rangle_2 \\
&= \frac{1}{\sqrt{2}}|0\rangle_1 |0\rangle_2 + \frac{1}{\sqrt{2}}|1\rangle_1 |0\rangle_2 \\
&= \frac{1}{\sqrt{2}}|00\rangle_{1,2} + \frac{1}{\sqrt{2}}|10\rangle_{1,2} \\
&= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \ .
\end{aligned}
$$

- Estado Emaranhado / Estado Separável

$$|\psi\rangle \neq |\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$$

Matrizes de Pauli

Notação	Ação na base $\|0\rangle, \|1\rangle$	Matriz na base $\|0\rangle, \|1\rangle$
$X = \sigma_x = \sigma_1$	$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
$Y = \sigma_y = \sigma_2$	$Y\|0\rangle = i\|1\rangle$ $Y\|1\rangle = -i\|0\rangle$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
$Z = \sigma_z = \sigma_3$	$Z\|0\rangle = \|0\rangle$ $Z\|1\rangle = -\|1\rangle$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Estados de Bell

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

$$|\beta_{01}\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

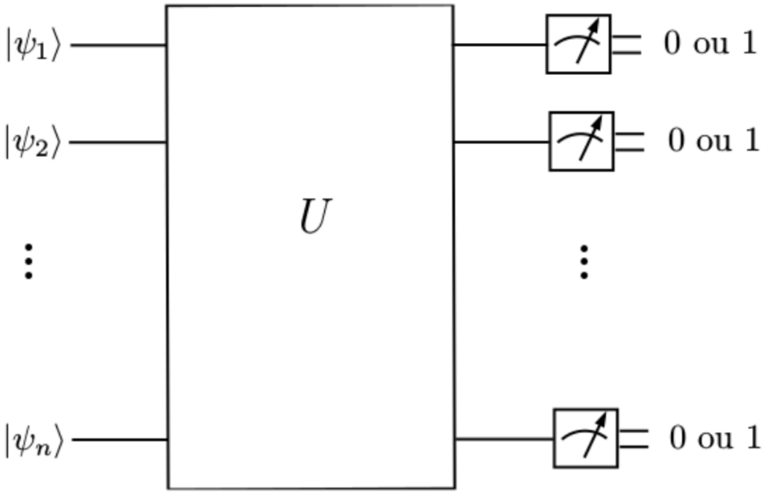
$$|\beta_{10}\rangle = |\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$$|\beta_{11}\rangle = |\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Computação Quântica

Modelos

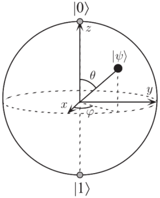
- Computação Quântica de Circuitos
- Computação Quântica Adiabática
- Máquina de Turing Quântica
- Caminhada Aleatória Quântica


$|\psi_1\rangle$
$|\psi_2\rangle$
$|\psi_n\rangle$
U
0 ou 1
0 ou 1
0 ou 1

- Número de entradas e saídas
- Reversibilidade

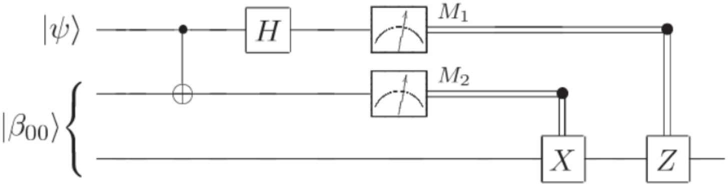
Fases

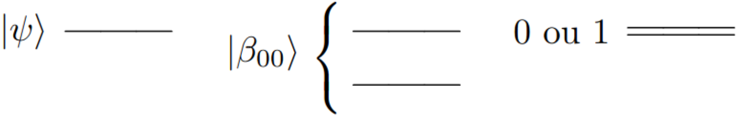
- Fases global
- Fase Relativa



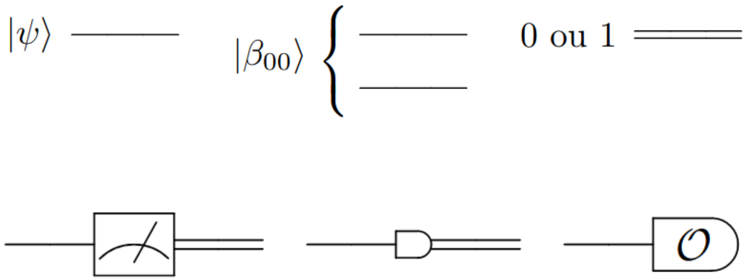
Ponto da esfera de Bloch			Estado $\|\psi\rangle$
$\hat{x} = (1,0,0)$	$\theta = \pi/2$	$\varphi = 0$	$\|+\rangle$
$-\hat{x} = (-1,0,0)$	$\theta = \pi/2$	$\varphi = \pi$	$\|-\rangle$
$\hat{y} = (0,1,0)$	$\theta = \pi/2$	$\varphi = \pi/2$	$\|+i\rangle$
$-\hat{y} = (0,-1,0)$	$\theta = \pi/2$	$\varphi = 3\pi/2$	$\|-i\rangle$
$\hat{z} = (0,0,1)$	$\theta = 0$		$\|0\rangle$
$-\hat{z} = (0,0,-1)$	$\theta = \pi$		$\|1\rangle$

Frame Title


$|\psi\rangle$
$|\beta_{00}\rangle$
H
M_1
M_2
X
Z


$|\psi\rangle$
$|\beta_{00}\rangle$
0 ou 1

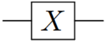
Frame Title



Portas 1 Qubit

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

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



$$X|b\rangle = |\bar{b}\rangle$$

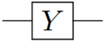
b=0,1 ; $\bar{b}$=NOT(b)

Notação alternativa

$$X = \sigma_x$$

$$X|+\rangle = |+\rangle$$
$$X|-\rangle = -|-\rangle$$

Portas 1 Qubit



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

Notação alternativa

$$Y = \sigma_y$$

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

$$Y|b\rangle = (-1)^b i|\bar{b}\rangle$$
$$b{=}0{,}1 \;;\; \bar{b}{=}\mathrm{NOT}(b)$$

$$Y|+\rangle = -i|-\rangle$$
$$Y|-\rangle = i|+\rangle$$

Portas 1 Qubit

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

$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

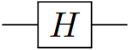
$$\underset{b=0,1}{Z|b\rangle = (-1)^b |b\rangle}$$

Notação alternativa

$$Z = \sigma_z$$

$$Z|+\rangle = |-\rangle$$
$$Z|-\rangle = |+\rangle$$

Portas 1 Qubit

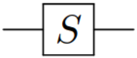


$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H\left|0\right\rangle = \left|+\right\rangle$$
$$H\left|1\right\rangle = \left|-\right\rangle$$

$$H\left|+\right\rangle = \left|0\right\rangle$$
$$H\left|-\right\rangle = \left|1\right\rangle$$

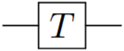
Portas 1 Qubit



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

$$S\left|0\right\rangle = \left|0\right\rangle$$
$$S\left|1\right\rangle = i\left|1\right\rangle$$

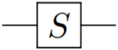
Portas 1 Qubit



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

$$T\,|0\rangle = |0\rangle$$
$$T\,|1\rangle = e^{i\frac{\pi}{4}}\,|1\rangle$$

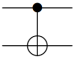
Portas 1 Qubit

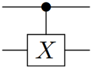


$$S(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

$$S|0\rangle = |0\rangle$$
$$S|1\rangle = e^{i\theta}|1\rangle$$

Portas 2 Qubit





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

$$\begin{aligned} \text{CNOT}\,|00\rangle &= |00\rangle \\ \text{CNOT}\,|01\rangle &= |01\rangle \\ \text{CNOT}\,|10\rangle &= |11\rangle \\ \text{CNOT}\,|11\rangle &= |10\rangle \end{aligned}$$

$$\begin{aligned} \text{CNOT}\,|0b\rangle &= |0b\rangle \\ \text{CNOT}\,|1b\rangle &= |1\bar{b}\rangle \end{aligned}$$

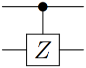
b=0,1 ; $\bar{b}$=NOT(b)

$$\text{CNOT}\,|a, b\rangle = |a, a \oplus b\rangle$$

a,b=0,1

$\oplus$=XOR=adição mod 2

Portas 2 Qubit

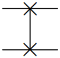


$$\mathrm{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\mathrm{CZ}\,|00\rangle = |00\rangle$$
$$\mathrm{CZ}\,|01\rangle = |01\rangle$$
$$\mathrm{CZ}\,|10\rangle = |10\rangle$$
$$\mathrm{CZ}\,|11\rangle = -\,|11\rangle$$

$$\mathrm{CZ}\,|0b\rangle = |0b\rangle$$
$$\mathrm{CZ}\,|1b\rangle = Z_2\,|1b\rangle = |1\rangle\,(Z\,|b\rangle)$$
$$b{=}0{,}1$$

Portas 2 Qubit

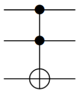


$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\text{SWAP}\,|00\rangle = |00\rangle$$
$$\text{SWAP}\,|01\rangle = |10\rangle$$
$$\text{SWAP}\,|10\rangle = |01\rangle$$
$$\text{SWAP}\,|11\rangle = |11\rangle$$

$$\text{SWAP}\,|ab\rangle = |ba\rangle$$
$$a,b=0,1$$

Portas 3 Qubit



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

$$\text{CCNOT}\,|00c\rangle = |00c\rangle$$
$$\text{CCNOT}\,|01c\rangle = |01c\rangle$$
$$\text{CCNOT}\,|10c\rangle = |10c\rangle$$
$$\text{CCNOT}\,|11c\rangle = |11\overline{c}\rangle$$

c=0,1 ; $\overline{c}$=NOT(c)

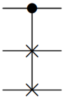
$$\text{CCNOT}\,|a, b, c\rangle = |a, b, (a \cdot b) \oplus c\rangle$$

a,b,c=0,1

$\cdot$ =AND

$\oplus$=XOR=adição mod 2

Portas 3 Qubit



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

$$\text{CSWAP}\,|0bc\rangle = |0bc\rangle$$
$$\text{CSWAP}\,|1bc\rangle = |1cb\rangle$$
$$b,c=0,1$$

Identidade de circuitos

$$X^2 = I \qquad XY = iZ$$

$$Y^2 = I \qquad YZ = iX$$

$$Z^2 = I \qquad ZX = iY$$

Pecurialidades da Computação Quântica

- Universsalidade de Portas Lógicas na Computação Quântica
- Teorema da não clonagem

Algoritmos e Tecnologias recentes