Introdução a Computação Quântica

Evandro Chagas Ribeiro da Rosa

IATe
GCQ-UFSC

Setembro de 2019

Conteúdo programático

Bit Quântico

Qubit

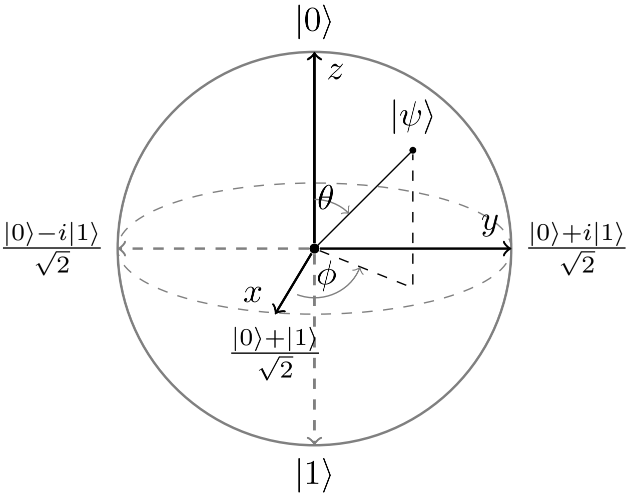


Figura: Esfera de Bloch.

Circuitos quântico

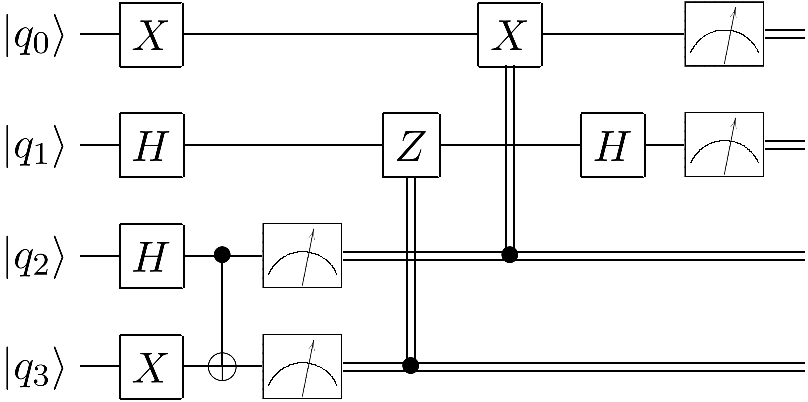


Figura: Exemplo de circuito quântico.

Notação de Dirac

Notação braket

- $|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_n \end{bmatrix}$
- $\langle\psi| = |\psi\rangle^\dagger = \begin{bmatrix} \alpha_0^* & \cdots & \alpha_n^* \end{bmatrix}$
- $\langle\psi|\varphi\rangle = \begin{bmatrix} \alpha_0 & \cdots & \alpha_n \end{bmatrix} \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_n \end{bmatrix} = z$
- $|| \, |\psi\rangle \, || = \sqrt{\langle\psi|\psi\rangle}$

Postulado 1
Espaço do sistema

Postulado 1: Associado a cada sistema quântico fechado há um espaço de Hilbert, e o estado do sistema é totalmente representado por um vetor unitário pertencente a esse espaço.

Base Computacional

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad ||\,|\psi\rangle\,|| = \sqrt{\alpha^2 + \beta^2} = 1$$

Postulado 4

Sistemas composto

Postulado 4: O estado de um sistema composto é dado pelo produto tensorial dos seus componentes, ou seja, um sistema composto por n sistemas quânticos, nos estados $|\psi_0\rangle$, $|\psi_1\rangle$, . . . , $|\psi_{n-1}\rangle$, tem seu estado total representado por $|\psi_0\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_{n-1}\rangle$.

Produto tensorial

$$|\psi\rangle \otimes |\varphi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} \\ \alpha_1 \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_2 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{bmatrix}$$

Postulado 2

Evolução do sistema

Postulado 2: A evolução de um sistema quântico fechado é descrita pela aplicação de um *operador unitário*, ou seja, a transição de um estado $|\psi\rangle^0$ no tempo t_0 para o estado $|\psi\rangle^1$ no tempo t_1 pode ser totalmente descrita por um operador unitário U, sendo $U|\psi\rangle^0 = |\psi\rangle^1$.

Operador unitário

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

Portas lógicas quântica

Portas de Pauli

$$-\boxed{X}- \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{matrix} X\left|0\right\rangle = \left|1\right\rangle \\ X\left|1\right\rangle = \left|0\right\rangle \end{matrix}$$

$$-\boxed{Z}- \qquad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \begin{matrix} Z\left|0\right\rangle = \left|0\right\rangle \\ Z\left|1\right\rangle = -\left|1\right\rangle \end{matrix}$$

$$-\boxed{Y}- \qquad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \begin{matrix} Y\left|0\right\rangle = i\left|1\right\rangle \\ Y\left|1\right\rangle = -i\left|0\right\rangle \end{matrix}$$

Portas lógicas quântica

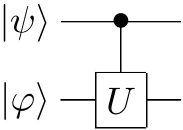
Portas de fase e Hadamard

$$-\boxed{S}- \qquad \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad \begin{aligned} S\left|0\right\rangle &= \left|0\right\rangle \\ S\left|1\right\rangle &= i\left|1\right\rangle \end{aligned}$$

$$-\boxed{T}- \qquad \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \qquad \begin{aligned} T\left|0\right\rangle &= \left|0\right\rangle \\ T\left|1\right\rangle &= \tfrac{1+i}{\sqrt{2}}\left|1\right\rangle \end{aligned}$$

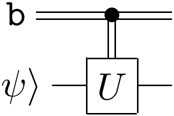
$$-\boxed{H}- \qquad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \begin{aligned} H\left|0\right\rangle &= (\left|0\right\rangle + \left|1\right\rangle)/\sqrt{2} \\ H\left|1\right\rangle &= (\left|0\right\rangle - \left|1\right\rangle)/\sqrt{2} \end{aligned}$$

Portas controlada



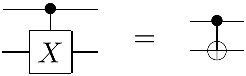
$|\psi\rangle$

$U\,|\varphi\rangle$ `if` $|\psi\rangle$ `==` $|1\rangle$ `else` $|\varphi\rangle$



b

$U\,|\psi\rangle$ `if b == 1 else` $|\psi\rangle$



Postulado 3: Uma medida quântica é descrita por um conjunto de *operadores de medida* $\{M_m\}$, onde o índice m indica o possível resultado da medida. Sendo $|\psi\rangle$ o estado logo antes da medida, a probabilidade de medir m é

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{1}$$

E o estado logo após a medida igual a

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{2}$$

Os operadores de medida precisam satisfazer a seguinte *equação de completude*

$$\sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1. \tag{3}$$

Medida na Base Computacional

Operadores de medida

- $M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$
- $M_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

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

$$p(0) = |\alpha|^2 \Rightarrow \frac{\alpha}{|\alpha|} |0\rangle$$

$$p(1) = |\beta|^2 \Rightarrow \frac{\beta}{|\beta|} |1\rangle$$

Estados de Bell

Exemplos de circuitos

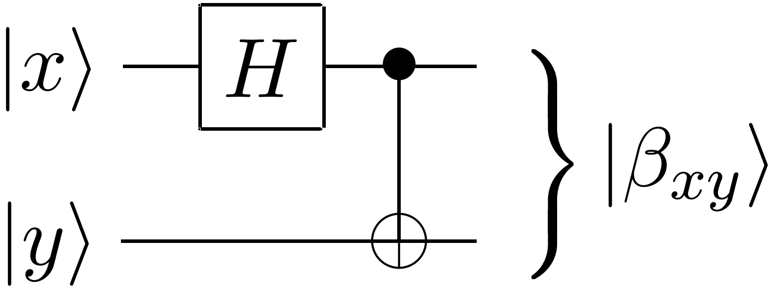
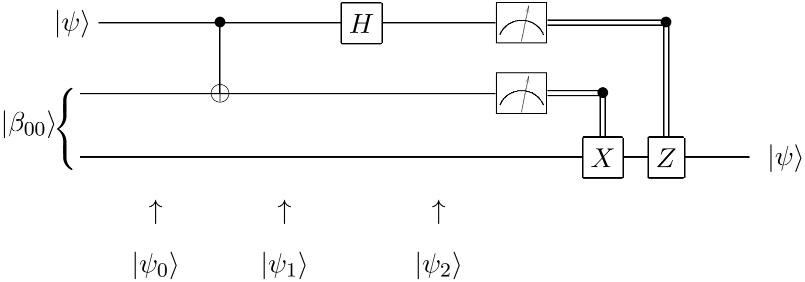


Figura: Circuito para gerar os estados de Bell

Teletransporte quântico

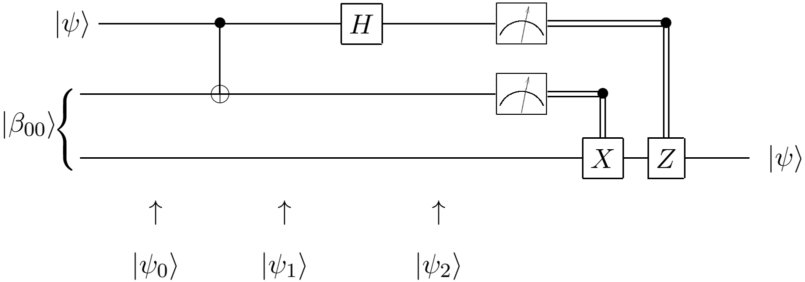
Exemplos de Circuitos



$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)]$$

Teletransporte quântico

Exemplos de Circuitos

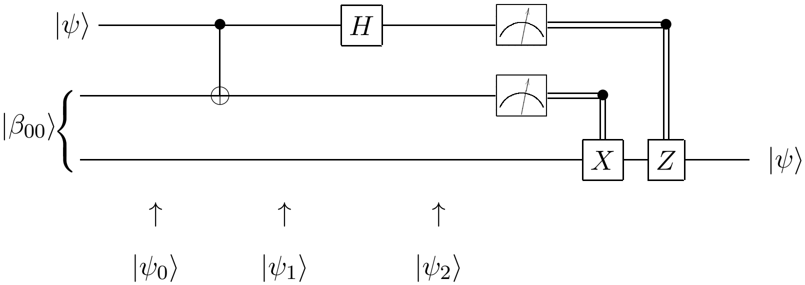


$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)]$$

Teletransporte quântico

Exemplos de Circuitos

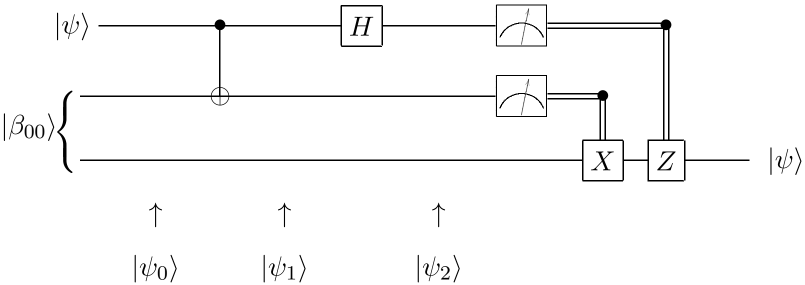


$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)]$$

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$$

Teletransporte quântico

Exemplos de Circuitos



$$
\begin{aligned}
|\psi_2\rangle = & \frac{1}{2}[|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) \\
& + |10\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)]
\end{aligned}
$$

QSystem

A quantum computing simulator for Python

- `pip install QSystem==1.2.0b1`
- `pip install jupyter`
- `jupyter notebook`

Algoritmo de Shor

Exemplos de circuito

Entrado: $n \in \mathbb{N}$ a ser fatorado

1. Selecione aleatoriamente um número a coprimo a n
2. Ache o período r da função $f(x) = a^x \mod n$

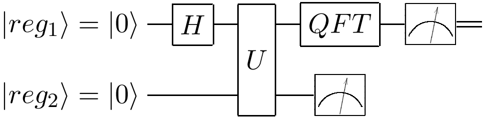


Figura: $U : |x\rangle\,|0\rangle \to |x\rangle\,|a^x \mod n\rangle$

3. $p = \gcd(a^{r/2}+1, n)$, $q = \gcd(a^{r/2}-1, n)$

Retorno: p, q

Obrigado