

UFCG - Universidade Federal de Campina Grande
DSC - Departamento de Sistemas e Computação

Introdução a Circuitos Quânticos

Alexandre de Andrade Barbosa
aab@dsc.ufcg.edu.br

Roteiro

- Introdução
- Revisão Matemática
- Q-Bits
- Portas Quânticas
- Circuitos Quânticos

Introdução

- A computação quântica é um domínio recente, engloba três áreas: física, computação e matemática.
- Por que um computador quântico é importante?
 - Devido ao limite de De Broglie.
 - Para resolução de problemas para os quais os computadores clássicos não possuem eficiência (fatoração, busca, etc.)
- O conceito de computador quântico foi apresentado por Feynman em 1982.
- Deutsch propôs um modelo para computação quântica universal.
- Em 1994 o Algoritmo de Shor mostrou que a computação quântica era mais que apenas curiosidade acadêmica.
- Circuitos quânticos são uma maneira eficiente de expressar a lógica existente na computação quântica.

Revisão Matemática

- Números complexos
- Matrizes
- Álgebra linear

Números Complexos

- Um número complexo “ z ” é pode ser escrito na fórmula $z = a + bi$, onde $a \in \mathbb{R}$, $b \in \mathbb{R}$ e $i^2 = -1$.
- O conjunto dos números complexos ($\mathbb{C}$) pode ser visto como uma extensão do conjuntos dos reais ($\mathbb{R}$).
- Sejam $z_1 = a_1 + b_1i$ e $z_2 = a_2 + b_2i$, podemos definir as operações como abaixo:

$$z_1 \pm z_2 = (a_1 + b_1i) \pm (a_2 + b_2i) = (a_1 \pm a_2) + (b_1 \pm b_2)i \quad (1)$$

$$z_1 \cdot z_2 = (a_1 + b_1i) \cdot (a_2 + b_2i) = (a_1a_2 + a_1b_2i + a_2b_1i - b_1b_2) \quad (2)$$

- Para definirmos a divisão precisamos definir o complexo conjugado de z , representado por $\bar{z}$

$$z_1 = a_1 + b_1i \Rightarrow \bar{z}_1 = a_1 - b_1i \quad (3)$$

$$z_1 / z_2 = (z_1 \cdot \bar{z}_2 / z_2 \cdot \bar{z}_2) \quad (4)$$

Matrizes

- Uma matriz é uma tabela onde seus elementos estão dispostos em linhas e colunas.
- Sejam $A_{2 \times 2}$ e $B_{2 \times 2}$ duas matrizes quaisquer, com mesmo número de linhas e colunas, podemos definir as operações abaixo:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \quad (5)$$

$$A \pm B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \pm \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} \pm b_{11} & a_{12} \pm b_{12} \\ a_{21} \pm b_{21} & a_{22} \pm b_{22} \end{pmatrix} \quad (6)$$

$$A \cdot B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \quad (7)$$

- Existem diversos tipos especiais de matrizes, dos quais destacamos:
 - Matriz quadrada - mesmo número de linhas e colunas
 - Matriz linha - possui apenas uma linha
 - Matriz coluna - possui apenas uma coluna

Matrizes

- Matriz transposta - troca-se as linhas por colunas

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad A^T = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \quad (8)$$

- Matriz identidade - todos os elementos da diagonal principal são iguais a 1, todos os outros são zero.

$$1 = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (9)$$

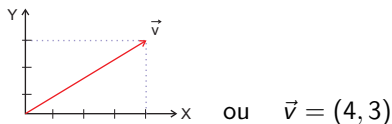
- Matriz conjugada - matriz onde todos seus elementos são conjugados da matriz original

$$A = \begin{pmatrix} a + bi & c + di \\ e + fi & g + hi \end{pmatrix} \quad A^* = \begin{pmatrix} a - bi & c - di \\ e - fi & g - hi \end{pmatrix} \quad (10)$$

- Matriz inversa - a inversa de uma matriz A é representada por A^{-1} e pode ser encontrada resolvendo-se a expressão $A.A^{-1} = A^{-1}.A = \mathbb{I}$
- Matriz unitária - matriz que satisfaz a condição $(A^*)^T = A^{-1}$

Álgebra Linear

- Para se obter uma boa compreensão da computação quântica é necessário possuir conhecimento básico sobre álgebra linear.
- Um vetor pode ser representado como um segmento de reta, com a notação matricial de suas coordenadas no espaço ou como $(v_1, v_2, \dots, v_n)$.



- Uma base é o conjunto mínimo de vetores que gera todos os outros vetores do espaço.
- Um vetor $\vec{v} = (5, 6)$ pode ser escrito como combinação linear dos vetores da base do espaço, para o $\mathbb{R}^2$ a base canônica é $\vec{i} = (1, 0)$ e $\vec{j} = (0, 1)$.

$$\vec{v} = 5\vec{i} + 6\vec{j} = 5(1, 0) + 6(0, 1).$$

(11)

Álgebra Linear

- Dados dois vetores $\vec{v} = (v_x, v_y, v_z)$ e $\vec{u} = (u_x, u_y, u_z)$, podemos definir as operações abaixo:

- Soma ou subtração:

$$\vec{v} \pm \vec{u} = (v_x, v_y, v_z) \pm (u_x, u_y, u_z) = (v_x \pm u_x, v_y \pm u_y, v_z \pm u_z) \quad (12)$$

- Produto interno ou produto escalar:

$$\vec{v} \cdot \vec{u} = (v_x, v_y, v_z) \cdot (u_x, u_y, u_z) = v_x u_x + v_y u_y + v_z u_z \quad (13)$$

- Produto externo ou produto vetorial:

$$\vec{v} \times \vec{u} = (v_x, v_y, v_z) \times (u_x, u_y, u_z) = \begin{vmatrix} i & j & k \\ v_x & v_y & v_z \\ u_x & u_y & u_z \end{vmatrix} \quad (14)$$

- Produto tensorial:

$$\vec{v} \otimes \vec{u} = (v_x, v_y, v_z) \otimes (u_x, u_y, u_z) = (v_x u_x, v_x u_y, v_x u_z, v_y u_x, v_y u_y, v_y u_z, v_z u_x, v_z u_y, v_z u_z) \quad (15)$$

Notação de Dirac

- A notação mais utilizada na computação quântica é a notação de Dirac, nesta notação um vetor $\vec{v}$ é representado como $|v\rangle$, temos:

$$\vec{v} = (v_x, v_y) \Rightarrow |v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \quad (16)$$

- Nesta notação todo $|v\rangle$ possui um dual definido como seu transposto conjugado e representado por $\langle v|$, assim temos:

$$|v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \Rightarrow \langle v| = \begin{bmatrix} v_x^* & v_y^* \end{bmatrix} \quad (17)$$

- Dados $|v\rangle$ e $|u\rangle$ abaixo, podemos representar as operações vetoriais como a seguir.

$$|v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \quad |u\rangle = \begin{bmatrix} u_x \\ u_y \end{bmatrix} \quad (18)$$

Notação de Dirac

- Soma ou subtração:

$$|v\rangle \pm |u\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \pm \begin{bmatrix} u_x \\ u_y \end{bmatrix} = \begin{bmatrix} v_x \pm u_x \\ v_y \pm u_y \end{bmatrix} \quad (19)$$

- Produto interno ou produto escalar:

$$\langle u|v\rangle \equiv (u, v) = \begin{bmatrix} u_x^* & u_y^* \end{bmatrix} \begin{bmatrix} v_x \\ v_y \end{bmatrix} = v_x u_x^* + v_y u_y^* \quad (20)$$

- Produto externo ou produto vetorial:

$$|v\rangle \langle u| = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \begin{bmatrix} u_x^* & u_y^* \end{bmatrix} = \begin{bmatrix} v_x u_x^* & v_x u_y^* \\ v_y u_x^* & v_y u_y^* \end{bmatrix} \quad (21)$$

- Produto tensorial:

$$|v\rangle \otimes |u\rangle \equiv |vu\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \otimes \begin{bmatrix} u_x \\ u_y \end{bmatrix} = \begin{bmatrix} v_x u_x \\ v_x u_y \\ v_y u_x \\ v_y u_y \end{bmatrix} \quad (22)$$

Q-Bits

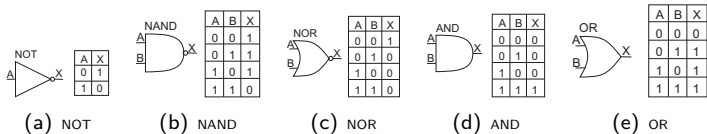
- Na computação clássica o bit é o conceito fundamental, para computação quântica o conceito análogo é o q-bit.
- Q-Bits aqui serão descritos como objetos matemáticos e não físicos.
- O bit clássico é representado por 0 ou 1, os q-bits análogos seriam os estados $|0\rangle$ e $|1\rangle$, porém q-bits podem estar em outros estados além destes.
- Um q-bit pode ser uma combinação linear de outros estados, estes estados são chamados de superposições, como exibido abaixo:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad (23)$$

- O estado de um q-bit é um vetor de duas dimensões em um espaço complexo.

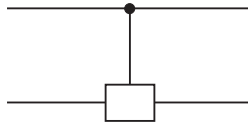
Portas Quânticas

- Nos computadores clássicos o processamento da informação ocorre através de circuitos lógicos (agrupamento de portas lógicas).
- Portas lógicas realizam operações sobre o(s) bit(s) de entrada gerando uma saída correspondendo a uma tabela verdade:



- Portas quânticas também são agrupadas para formar circuitos quânticos, no entanto algumas considerações e convenções devem ser apresentadas.

Notações e convenções



- Linhas horizontais - representam a evolução do q-bit.
- Sentido - a evolução do q-bit ocorre da esquerda para direita.
- Linhas verticais - não representam copia e sim que o circuito atua sobre os dois q-bits.
- Controle - o símbolo • indica controle, ou seja a porta só realiza sua operação se o q-bit da entrada de controle for $|1\rangle$.

Portas Quânticas de um Q-bit

- Uma porta quântica aplica uma operação unitária sobre um q-bit.
- Toda matriz unitária 2×2 pode ser uma porta quântica de um q-bit.
- As portas quânticas de um q-bit mais utilizadas são:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = 1/\sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad (24)$$

- Podemos observar a execução de algumas portas sobre q-bits:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle, X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \quad (25)$$

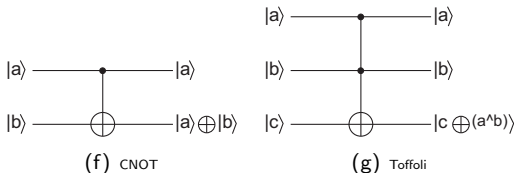
$$Z|\psi\rangle = Z(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \left(\begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} \right) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} \quad (26)$$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (27)$$

$$S|\psi\rangle = S(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ i\beta \end{bmatrix} = \alpha|0\rangle + i\beta|1\rangle \quad (28)$$

Portas Quânticas de múltiplos Q-Bits

- O conjunto de portas quânticas de um q-bit apesar de infinito não é universal.
- É preciso utilizar portas quânticas de múltiplos q-bits para representar operações quânticas sobre um número qualquer de q-bits.
- Como exemplo de portas quânticas de múltiplos q-bits temos a porta CNOT ou NOT-controlada e a porta Toffoli.

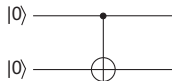


Porta CNOT

- A operação executada por CNOT nega o q-bit alvo apenas se o q-bit de controle estiver “ligado”, assim temos...

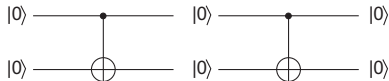
Porta CNOT

- A operação executada por CNOT nega o q-bit alvo apenas se o q-bit de controle estiver “ligado”, assim temos...



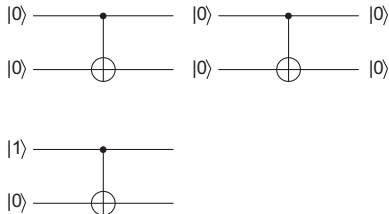
Porta CNOT

- A operação executada por CNOT nega o q-bit alvo apenas se o q-bit de controle estiver “ligado”, assim temos...



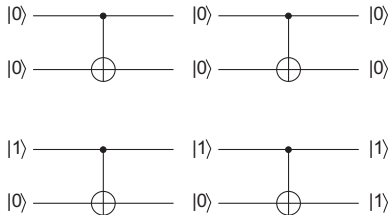
Porta CNOT

- A operação executada por CNOT nega o q-bit alvo apenas se o q-bit de controle estiver “ligado”, assim temos...



Porta CNOT

- A operação executada por CNOT nega o q-bit alvo apenas se o q-bit de controle estiver “ligado”, assim temos...

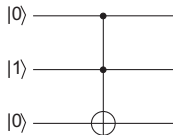


Porta Toffoli

- A operação executada por Toffoli é bastante semelhante a CNOT, esta porta nega o q-bit alvo apenas se os q-bits de controle estiverem “ligados”, assim temos...

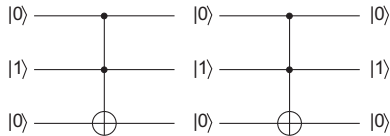
Porta Toffoli

- A operação executada por Toffoli é bastante semelhante a CNOT, esta porta nega o q-bit alvo apenas se os q-bits de controle estiverem “ligados”, assim temos...



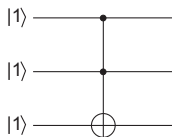
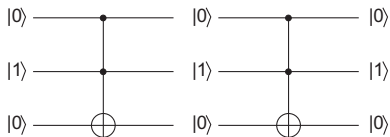
Porta Toffoli

- A operação executada por Toffoli é bastante semelhante a CNOT, esta porta nega o q-bit alvo apenas se os q-bits de controle estiverem “ligados”, assim temos...



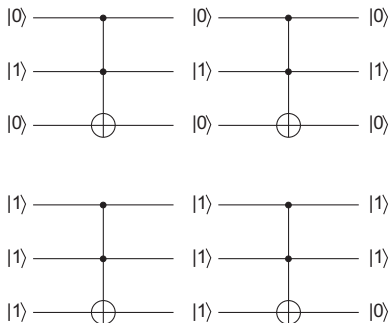
Porta Toffoli

- A operação executada por Toffoli é bastante semelhante a CNOT, esta porta nega o q-bit alvo apenas se os q-bits de controle estiverem “ligados”, assim temos...



Porta Toffoli

- A operação executada por Toffoli é bastante semelhante a CNOT, esta porta nega o q-bit alvo apenas se os q-bits de controle estiverem “ligados”, assim temos...

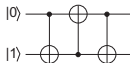


Circuitos Quânticos

- Circuitos quânticos facilitam a compreensão dos algoritmos quânticos.
- Circuitos quânticos são agrupamentos de portas quânticas, onde as portas realizam operações unitárias sobre q-bits.
- Como exemplo de circuito quântico podemos apresentar o circuito abaixo...

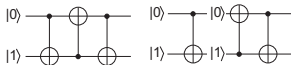
Circuitos Quânticos

- Circuitos quânticos facilitam a compreensão dos algoritmos quânticos.
- Circuitos quânticos são agrupamentos de portas quânticas, onde as portas realizam operações unitárias sobre q-bits.
- Como exemplo de circuito quântico podemos apresentar o circuito abaixo...



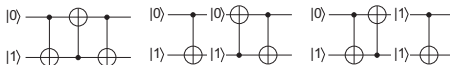
Circuitos Quânticos

- Circuitos quânticos facilitam a compreensão dos algoritmos quânticos.
- Circuitos quânticos são agrupamentos de portas quânticas, onde as portas realizam operações unitárias sobre q-bits.
- Como exemplo de circuito quântico podemos apresentar o circuito abaixo...



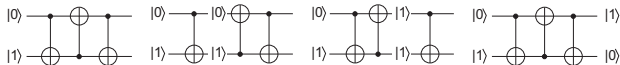
Circuitos Quânticos

- Circuitos quânticos facilitam a compreensão dos algoritmos quânticos.
- Circuitos quânticos são agrupamentos de portas quânticas, onde as portas realizam operações unitárias sobre q-bits.
- Como exemplo de circuito quântico podemos apresentar o circuito abaixo...



Circuitos Quânticos

- Circuitos quânticos facilitam a compreensão dos algoritmos quânticos.
- Circuitos quânticos são agrupamentos de portas quânticas, onde as portas realizam operações unitárias sobre q-bits.
- Como exemplo de circuito quântico podemos apresentar o circuito abaixo...



- ... vemos após sua execução que se trata de um circuito de troca ou *swap*.

Implementação de circuitos quânticos

- Diversas tecnologias vêm sendo propostas para implementação de circuitos quânticos, dentre elas:
 - íons aprisionados
 - eletrodinâmica quântica de cavidades (QED)
 - ressonância magnética nuclear (RMN)
- RMN foi utilizada na criação de sistemas de 2 e 3 q-bits, utilizados para mostrar que o problema de Deutsch e o algoritmo de Grover podem ser executados em hardware quântico.

Conclusões

- Computadores Quânticos trazem uma nova forma computação e não apenas mais velocidade.
- Diversos algoritmos quânticos já mostraram que a computação quântica é bem mais do que curiosidade acadêmica.
- Circuitos quânticos fornecem uma maneira mais simples para compreender a execução dos algoritmos.