Universidade Federal de Campina Grande
Departamento de Sistemas e Computação
Pós-Graduação em Informática

Introdução a Circuitos Quânticos

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

Campina Grande, 16 maio de 2005

Resumo

A Computação Quântica é uma área recente e combina três outras áreas bastante conhecidas: matemática, física e computação. Este trabalho apresenta um estudo introdutório aos circuitos utilizados na Computação Quântica, porém apenas os aspectos matemáticos e computacionais serão abordados. O principal objetivo deste é fornecer uma compreensão básica sobre o tema e possibilitar um estudo mais aprofundado sobre a computação quântica.

Conteúdo

Lista de Figuras

Lista de Tabelas

1 Introdução

O conceito de computador quântico teve inicio quando, em 1982, Feynman propôs que sistemas quânticos não seriam eficientemente modelados em sistemas clássicos, pois estes só poderiam ser modelados eficientemente por outro sistema quântico.

Deutsch [Deu85] propôs em 1985 um modelo para computação quântica universal, seria o correspondente a Máquina de Turing(MT) para computação clássica, este modelo adicionava algumas características à MT, as quais permitia a representação de sobreposições.

Porém o modelo inicialmente proposto era bastante complexo, assim Deutsch criou uma representação mais simples para a computação quântica que era bastante semelhante ao modelo de circuitos clássicos. Por serem de fácil compreensão os circuitos quânticos vêm sendo cada vez mais utilizados.

Só em 1994, quando Shor publicou seu algoritmo quântico para fatoração de números inteiros grandes é que a computação quântica despertou interesse geral, pois a fatoração é a base para os atuais sistemas de criptografia. O algoritmo de Shor resolve o problema de fatoração de primos em tempo polinomial, enquanto a solução clássica só é obtida em tempo exponencial.

A principal técnica utilizada para aumentar a velocidade dos computadores clássicos é a miniaturização de circuitos, o que torna possível a utilização de números cada vez maiores de circuitos nos processadores.

Porém devido ao limite de De Broglie, que diz que os atuais circuitos poderão progredir até o tamanho de 20 nanômetros sem sacrifício funcional, após este limite os elétrons deixam de agir como partículas e passam a agir como ondas, quando obedecem então as leis da física quântica [Cab04].

Os computadores quânticos não serão apenas mais velozes que as máquinas atuais, eles torna rão possível uma nova forma de computação.

Os circuitos quânticos fornecem uma forma simples para que se possa compreender o funcionamento de computadores quânticos. Os circuitos aqui apresentados são bastante simples e para compreender como estes funcionam é necessário apenas um conhecimento matemático básico. Todos os conceitos matemáticos necessários serão também apresentados.

Este trabalho está organizado da seguinte maneira: na seção seguinte é realizada uma revisão matemática; a Seção 3 apresenta a notação comumente utilizada na computação quântica; a Seção 4 exibe o conceito de q-bit; portas quânticas são apresentadas na Seção 5; a Seção 6 apresenta os circuitos quânticos; finalmente na seção 7 são apresentadas as conclusões finais deste trabalho.

2 Revisão Matemática

Diversos conceitos matemáticos são necessários para que se possa compreender o funcionamento dos circuitos quânticos. Nesta seção será realizada uma breve revisão matemática sobre estes conceitos, os quais são de fácil compreensão.

2.1 Números Complexos

Para o conjunto dos números reais, representado por $\mathbb{R}$, equações como $x^2+1=0$ não possuem solução, pois números negativos não possuem raízes reais, caso o índice da raiz seja par. No entanto tomando o conjunto dos números complexos, representado por $\mathbb{C}$, tal equação possui solução como veremos a seguir.

Um número complexo pode ser expresso como $z = a + bi$ onde $a \epsilon R$, $b \epsilon R$ e $i = \sqrt{-1}$, sendo i chamado de unidade imaginária [FY95], então temos:

$$C = \{z = a + bi | a \in R, b \in R, i = \sqrt{-1} \tag{1}$$

Tomando como universo o conjunto dos números complexos temos uma solução para a equação $x^2 + 1 = 0$, assim temos:

$$x^2 + 1 = 0 \Rightarrow x^2 = -1 \Rightarrow x = \sqrt{-1} \Rightarrow x = i \tag{2}$$

Todos os números reais podem ser representados com um número complexo, para isto basta fazer b = 0 restando z = a. Caso a = 0 temos um número complexo z = bi, denominado imaginário puro [FY95].

2.1.1 Adição e subtração de complexos

As definições das operações de soma, subtração, multiplicação e divisão de complexos exibidas aqui se baseiam nas definições apresentadas em [FY95].

Dados dois números complexos $z_1 = a_1 + b_1 i$ e $z_2 = a_2 + b_2 i$, a soma ou subtração de z_1 e z_2 são realizadas somando ou subtraindo a parte real de z_1 com a parte real de z_2 e a parte imaginária de z_1 com a parte imaginária de z_2, temos a adição definida na Equação 3 e a subtração definida na Equação 4:

$$z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i \tag{3}$$

$$z_1 - z_2 = (a_1 + b_1 i) - (a_2 + b_2 i) = (a_1 - a_2) + (b_1 - b_2)i \tag{4}$$

2.1.2 Multiplicação de complexos

Dados dois números complexos $z_1 = a_1 + b_1 i$ e $z_2 = a_2 + b_2 i$, a multiplicação de z_1 e z_2 é realizada como a multiplicação de binômios, sabendo que $i^2 = -1$, temos:

$$\begin{aligned} z_1.z_2 &= (a_1 + b_1 i).(a_2 + b_2 i) \\ &= (a_1.a_2) + (a_1.b_2 i) + (a_2.b_1 i) + b_1.b_2.i^2 \\ &= (a_1.a_2) + (a_1.b_2 i) + (a_2.b_1 i) - b_1.b_2 \end{aligned} \tag{5}$$

2.1.3 Conjugado de um complexo

Dado $z_1 = a_1 + b_1 i$, chamamos de conjugado de z_1, representado por $\bar{z}$, o número complexo $z_1 = a_1 - b_1 i$, ou seja aquele com o sinal de sua parte imaginária negado, assim temos:

$$z = a + bi \Longrightarrow \bar{z} = a - bi \tag{6}$$

O produto de um número complexo por seu conjugado é sempre um número real positivo, pois temos:

$$\begin{aligned} z.\bar{z} &= (a + bi).(a - bi) \\ &= a^2 + b^2 \end{aligned} \tag{7}$$

2.1.4 Divisão de complexos

Dados dois números complexos $z_1 = a_1 + b_1 i$ e $z_2 = a_2 + b_2 i$, a divisão de z_1 e z_2 é obtida multiplicando numerador e denominador pelo conjugado do denominador, assim temos:

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{(a_1+b_1 i)}{(a_2+b_2 i)} . \frac{(a_2-b_2 i)}{(a_2-b_2 i)} \\ &= \frac{(a_1.a_2 - a_1.b_2 i + a_2.b_1 i + b_1.b_2)}{a_2^2+b_2^2} \\ &= \frac{(a_1.a_2+b_1.b_2)+(a_2.b_1 i - a_1.b_2 i)}{a_2^2+b_2^2} \\ &= \frac{z_1.\bar{z_2}}{z_2.\bar{z_2}} \end{aligned} \tag{8}$$

2.2 Matrizes

Uma matriz é uma tabela onde os elementos estão dispostos em linhas e colunas. Toda matriz é indicada por uma letra maiúscula do alfabeto latino e pode ser representada em geral utilizando-se parênteses ( ) ou colchetes [ ] [FY95].

Seja $A_{m \times n}$ uma matriz, onde m representa o número de linhas e n o de colunas, um elemento qualquer de A é representado por a_{ij}, sendo i o índice para a linha do elemento e j o índice da coluna. Então seja $A_{2 \times 2}$ uma matriz qualquer, temos:

$$A_{2 \times 2} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

A ordem de uma matriz representa o número de linhas e colunas desta, assim se temos $A_{m \times n}$, A é dita uma matriz de ordem m por n.

Duas matrizes A e B quaisquer só podem ser iguais se e somente se possuírem a mesma ordem e todos seus elementos correspondentes forem iguais, ou seja $a_{11} = b_{11}$, $a_{12} = b_{12}$ e assim por diante [Ste75].

Existem diversos tipos especiais de matrizes, destacamos como os mais importantes tipos no contexto apresentado, as matrizes descritas abaixo:

Matriz quadrada - toda aquela que possui um número de linhas e colunas igual.

Matriz coluna - toda aquela que possui apenas uma coluna.

Matriz linha - toda aquela quando possui apenas uma linha.

Matriz transposta - obtida transformando as linhas em colunas e as colunas em linhas, como visto na Equação 9.

$$A_{3\times3} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \Rightarrow A^T_{3\times3} = \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \tag{9}$$

Matriz identidade - é uma matriz quadrada onde todos os elementos da diagonal principal são iguais a um e todos os outros iguais a zero.

Matriz inversa - a inversa de uma matriz A é representada por A^{-1} e pode ser encontrada resolvendo-se a expressão $A.A^{-1} = A^{-1}.A = \mathbb{I}$. Assim se temos uma matriz

$$A = \begin{pmatrix} 1 & 4 & 0 \\ -1 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix} \tag{10}$$

sua inversa é dada por

$$A^{-1} = \begin{pmatrix} 4 & -8 & 8 \\ 2 & 2 & -2 \\ 0 & 0 & 6 \end{pmatrix} \tag{11}$$

pois podemos ver nas Equações 12 e 13 que $A.A^{-1} = \mathbb{I}$ e $A^{-1}.A = \mathbb{I}$, respectivamente.

$$A.A^{-1} = \begin{pmatrix} 1 & 4 & 0 \\ -1 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \\ \frac{1}{6} & \frac{1}{6} & -\frac{1}{6} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{12}$$

$$A^{-1}.A = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \\ \frac{1}{6} & \frac{1}{6} & -\frac{1}{6} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 4 & 0 \\ -1 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{13}$$

Matriz unitária - matriz que satisfaz a condição $(A^*)^T = A^{-1}$, como observado na Equação 14.

$$A = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \Rightarrow (A^*)^T = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = A \tag{14}$$

2.2.1 Adição e subtração de matrizes

Para que duas matrizes A e B quaisquer possam ser adicionadas ou subtraídas, é necessário que estas tenham o mesmo número de linhas e colunas (sejam da mesma ordem), ou seja $A_{m\times n}$ só pode ser adicionada ou subtraída por $B_{p\times q}$ se m=p e n=q [Ste75].

Dadas as matrizes $A_{2\times 2}$ e $B_{2\times 2}$:

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

Então $A \pm B = (a_{ij} \pm b_{ij})$ como pode ser visto abaixo:

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

2.2.2 Multiplicação de matrizes

Para que duas matrizes A e B quaisquer possam ser multiplicadas é necessário que o número de colunas de A seja igual ao número de linhas de B, ou seja $A_{m\times n}$ só pode ser multiplicada por $B_{p\times q}$ se n=p [Ste75].

Seja C a matriz resultante da multiplicação da matriz $A_{2\times 3}$ pela matriz $B_{3\times 2}$, então C será uma matriz 2×2 onde $c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + ... + a_{in}b_{nk}$, como pode ser observado abaixo:

Dadas as matrizes A e B:

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

Então a multiplicação é definida como abaixo:

$$A.B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} . \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}.b_{11} + a_{12}.b_{21} & a_{11}.b_{12} + a_{12}.b_{22} \\ a_{21}.b_{11} + a_{22}.b_{21} & a_{21}.b_{12} + a_{22}.b_{22} \end{pmatrix}$$

2.3 Álgebra Linear

Para compreender diversos aspectos da computação quântica é bastante desejável o conhecimento de conceitos básicos da álgebra linear, os conceitos necessários para compreensão de circuitos quânticos são apresentados nas subseções seguintes.

2.3.1 Vetores no R^n

Um vetor pode ser representado como um segmento de reta orientado em um plano ou espaço, como pode ser visto na Figura 1. As componentes do vetor podem ainda ser definidas utilizando um sistema de coordenadas cartesianas,

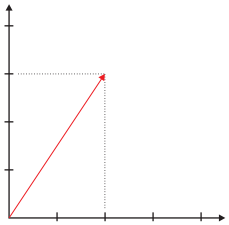


Figura 1: Representação gráfica de um vetor no R^2

sendo (v_1, v_2) a representação do ponto final do vetor e a origem (0,0) o ponto inicial do mesmo. Assim, o vetor da Figura 1 seria representado por (2,3) [SW87].

Um vetor pode também ser representado por uma matriz linha ou coluna, seja um vetor $\vec{v} = (v_1, v_2, v_3)$ este pode ser representado como abaixo:

$$\vec{v} = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

Utilizando as coordenadas cartesianas a adição, subtração e multiplicação por um escalar podem ser facilmente definidas, assim se temos dois vetores quaisquer $\vec{v} = (v_1, v_2)$ e $\vec{u} = (u_1, u_2)$ e um escalar α, as operações são definidas em [SW87] como abaixo:

- Adição: $\vec{v} + \vec{u} = (v_1, v_2) + (u_1, u_2) = (v_1 + u_1, v_2 + u_2)$
- Subtração: $\vec{v} - \vec{u} = (v_1, v_2) - (u_1, u_2) = (v_1 - u_1, v_2 - u_2)$
- Multiplicação por escalar: $\alpha\vec{v} = \alpha(v_1, v_2) = (\alpha v_1, \alpha v_2)$

2.3.2 Produto interno ou escalar

O produto interno entre dois vetores é representado por "$.$", assim se temos dois vetores quaisquer $\vec{v} = (v_1, v_2)$ e $\vec{u} = (u_1, u_2)$, o produto interno de $\vec{v}$ e $\vec{u}$, representado por $\vec{v}.\vec{u}$ e pode ser obtido como abaixo:

- $\vec{v}.\vec{u} = (v_1, v_2).(u_1, u_2) = v_1.u_1 + v_2.u_2$

2.3.3 Produto externo ou vetorial

O produto externo entre dois vetores é representado por "$\times$", assim se temos dois vetores quaisquer $\vec{v} = (v_1, v_2, v_3)$ e $\vec{u} = (u_1, u_2, u_3)$, o produto externo de $\vec{v}$ e $\vec{u}$, representado por $\vec{v} \times \vec{u}$ pode ser obtido resolvendo-se

$$\vec{v} \times \vec{u} = (v_1, v_2, v_3) \times (u_1, u_2, u_3) = \det \begin{bmatrix} \vec{i} & \vec{j} & \vec{k} \\ v_1 & v_2 & v_3 \\ u_1 & u_2 & u_3 \end{bmatrix} \tag{15}$$

onde i=(1,0,0), j=(0,1,0) e k=(0,0,1).

Por exemplo sejam $\vec{v} = (1, 3, 2)$ e $\vec{u} = (2, 1, 1)$, o produto vetorial, $\vec{v} \times \vec{u}$, é dado por

$$det \begin{bmatrix} \vec{i} & \vec{j} & \vec{k} \\ 1 & 3 & 2 \\ 2 & 1 & 1 \end{bmatrix} = (3\vec{i} + 4\vec{j} + \vec{k}) - (\vec{j} + 2\vec{i} + 6\vec{k}) = \vec{i} + 3\vec{j} - 5\vec{k} = (1, 3, -5) \quad (16)$$

2.3.4 Produto tensorial

O produto tensorial entre dois vetores é representado por "$\otimes$", assim se temos dois vetores quaisquer $\vec{v} = (v_1, v_2, ..., v_m)$ e $\vec{u} = (u_1, u_2, ..., u_n)$, o produto tensorial de $\vec{v}$ e $\vec{u}$, representado por $\vec{v} \otimes \vec{u}$ e pode ser obtido como abaixo:

$$\begin{aligned} \vec{v} \otimes \vec{u} &= (v_1, v_2, ..., v_m) \otimes (u_1, u_2, ..., u_n) \\ &= (v_1u_1, v_1u_2, ..., v_2u_1, v_2u_2, ..., v_mu_1, v_mu_2, ..., v_mu_n) \end{aligned} \quad (17)$$

2.3.5 Base e Combinação linear

Seja $\vec{v} = (4, 3)$ um vetor no espaço R^2, $\vec{v}$ pode ser escrito como combinação linear de outros vetores, como exemplificado na Equação 18.

$$\vec{v} = (4, 3) = 4(1, 0) + 3(0, 1) \quad (18)$$

De modo mais geral uma combinação linear em um espaço R^n é definida em [Sho04] como uma soma de um conjunto de vetores não nulos tal como,

$$\alpha_1\vec{v_1} + \alpha_2\vec{v_2} + ... + \alpha_n\vec{v_n} \quad (19)$$

onde $\alpha_1, \alpha_2, ..., \alpha_n \in R^n$.

Um conjunto de vetores pode ser chamado linearmente independente se a única solução para a equação

$$\alpha_1\vec{v_1} + \alpha_2\vec{v_2} + ... + \alpha_n\vec{v_n} = 0 \quad (20)$$

for $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$. Conjuntos de vetores que não são linearmente independentes são chamados linearmente dependentes.

Uma base para um espaço vetorial é definida em [Sho04] como o conjunto de vetores linearmente independentes que geram o espaço. A grosso modo pode se entender a definição de base como o conjunto mínimo de vetores do espaço que pode criar todos os outros vetores deste espaço através de combinação linear.

Como exemplo de base podemos citar a base canônica (i,j) para o espaço R^2, onde i=(1,0) e j=(0,1). Note que qualquer vetor do espaço R^2 pode ser escrito como combinação linear de (i,j).

3 Notação de Dirac

Na computação quântica é comumente utilizada a notação de Dirac para representar estados quânticos, essa notação é utilizada devido a praticidade de representar estados quânticos e transformações [VNB04]. Na literatura a notação de Dirac pode também ser encontrada como notação *braket*, devido a sua forma de representação de vetores.

Um vetor $\vec{v}$ é representado na notação de Dirac como $|v\rangle$ (lê-se "ket vê"), assim temos:

$$\vec{v} = (v_1, v_2) \Rightarrow |v\rangle = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \tag{21}$$

Nesta notação tem-se ainda o vetor representado por $\langle v|$ (lê-se "bra vê"), o qual é o transposto conjugado de $|v\rangle$, assim temos:

$$|v\rangle = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \Rightarrow \langle v| = \begin{bmatrix} v_1^* & v_2^* \end{bmatrix} \tag{22}$$

Dados $|v\rangle$ e $|u\rangle$

$$|v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \quad |u\rangle = \begin{bmatrix} u_x \\ u_y \end{bmatrix} \tag{23}$$

podemos representar as operações vetoriais como é mostrado abaixo:

- Adição:

$$|v\rangle + |u\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} + \begin{bmatrix} u_x \\ u_y \end{bmatrix} = \begin{bmatrix} v_x + u_x \\ v_y + u_y \end{bmatrix} \tag{24}$$

- Subtração:

$$|v\rangle - |u\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} - \begin{bmatrix} u_x \\ u_y \end{bmatrix} = \begin{bmatrix} v_x - u_x \\ v_y - u_y \end{bmatrix} \tag{25}$$

- Multiplicação por escalar:

$$\alpha|v\rangle = \alpha \begin{bmatrix} v_x \\ v_y \end{bmatrix} = \begin{bmatrix} \alpha v_x \\ \alpha v_y \end{bmatrix} \tag{26}$$

Utilizando a notação de Dirac temos novos meios para representar os produtos entre vetores, os quais são apresentadas nas subseções seguintes.

3.1 Produto interno ou escalar na notação de Dirac

O produto interno entre dois vetores é representado na notação de Dirac por "(v,v)" ou "$\langle v|v\rangle$", sendo a segunda maneira mais utilizada. Assim dados dois vetores $|v\rangle$ e $|u\rangle$

$$|v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \quad |u\rangle = \begin{bmatrix} u_x \\ u_y \end{bmatrix} \tag{27}$$

o produto interno de $|u\rangle$ e $|v\rangle$ pode ser obtido como abaixo:

$$\langle u|v\rangle = \begin{bmatrix} u_x^* & u_y^* \end{bmatrix} \begin{bmatrix} v_x \\ v_y \end{bmatrix} = u_x^* v_x + u_y^* v_y \tag{28}$$

3.2 Produto externo ou vetorial na notação de Dirac

O produto externo entre dois vetores v e u quaisquer é representado na notação de Dirac por "$|v\rangle\langle u|$". Assim se temos dois vetores

$$|v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \quad |u\rangle = \begin{bmatrix} u_x \\ u_y \end{bmatrix} \tag{29}$$

o produto externo de $\vec{v}$ e $\vec{u}$ pode ser obtido como abaixo:

$$|v\rangle\langle u| = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \begin{bmatrix} u_x^* & u_y^* \end{bmatrix} = \begin{bmatrix} v_x u_x^* & v_x u_y^* \\ v_y u_x^* & v_y u_y^* \end{bmatrix} \tag{30}$$

3.3 Produto tensorial na notação de Dirac

O produto tensorial entre dois vetores também é representado na notação de Dirac por "$\otimes$", assim se temos dos vetores

$$|v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} \quad |u\rangle = \begin{bmatrix} u_x \\ u_y \end{bmatrix} \tag{31}$$

o produto tensorial de $|v\rangle$ e $|u\rangle$, representado por $|v\rangle \otimes |u\rangle$ ou em sua forma abreviada $|vu\rangle$ e pode ser obtido como abaixo:

$$|v\rangle \otimes |u\rangle \equiv |vu\rangle = \begin{bmatrix} v_1 \\ v_2 \\ \cdots \\ v_m \end{bmatrix} \otimes \begin{bmatrix} u_1 \\ u_2 \\ \cdots \\ u_n \end{bmatrix} = \begin{bmatrix} v_1 u_1 \\ v_1 u_2 \\ \cdots \\ v_2 u_1 \\ v_2 u_2 \\ \cdots \\ v_m u_1 \\ v_m u_2 \\ \cdots \\ v_m u_n \end{bmatrix} \tag{32}$$

4 Bits quânticos

Para a computação clássica o conceito fundamental é o *bit*, para a computação quântica o conceito análogo é o *bit quântico* [NC00]. Na literatura as referências aos bits quânticos freqüentemente são realizadas de maneira abreviada QuBit ou ainda q-bit. Neste trabalho os bits quânticos serão referenciados como q-bits, tal como em [PLCM04] e descritos puramente como objetos matemáticos, tal como em [NC00].

Um bit clássico possui apenas dois estados possíveis os quais são representados por 0 ou 1, q-bits possuem como possíveis estados os vetores $|0\rangle$ e $|1\rangle$, que podem ser ditos equivalentes aos estados clássicos 0 e 1 e representados como

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad e \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{33}$$

porém um q-bit pode estar em um estado chamado superposição, onde este é uma combinação linear de estados [NC00].

Seja $|\psi\rangle$ um q-bit genérico ele pode então ser escrito como:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{34}$$

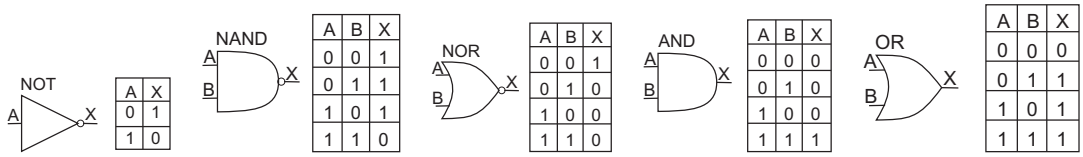
onde α e β são números complexos, $|\psi\rangle$ é denominado superposição de estados.

Um q-bit pode ser definido matematicamente como um vetor unitário no espaço $\mathbb{C}^2$. Os vetores $|0\rangle$ e $|1\rangle$ são denominados base computacional pois qualquer outro vetor pode ser criado através de uma combinação linear destes [PLCM04].

5 Portas Quânticas

Nos computadores clássicos o processamento da informação ocorre através de circuitos lógicos que são agrupamentos de portas lógicas as quais executam operações sobre bits [Cab04].

Para os circuitos clássicos cinco portas lógicas são os principais blocos construtores, tais portas obedecem a álgebra booleana e podem ter suas entradas e saídas descritas em tabelas verdade [Tan00], como é exibido na Figura 2.



A	X
0	1
1	0

(a) NOT

A	B	X
0	0	1
0	1	1
1	0	1
1	1	0

(b) NAND

A	B	X
0	0	1
0	1	0
1	0	0
1	1	0

(c) NOR

A	B	X
0	0	0
0	1	0
1	0	0
1	1	1

(d) AND

A	B	X
0	0	0
0	1	1
1	0	1
1	1	1

(e) OR

Figura 2: Portas clássicas

Os circuitos da computação quântica também são agrupamentos de portas quânticas, as quais realizam operações unitárias sobre q-bits [Cab04]. Assim

portas quânticas podem ser vistas como operadores ou matrizes unitárias, este fato é de grande importância pois assim todas as matrizes unitárias 2×2 podem representar portas quânticas de um q-bit [NC00].

Como exemplo de portas quânticas temos as matrizes de Pauli, vistas em sua representação matricial na Equação 35 e em uma representação visual na Figura 3.

$$X = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{35}$$

(a) X (b) Y (c) Z

Figura 3: Portas de Pauli

5.1 Portas Quânticas de um Q-Bit

O conjunto de portas quânticas que realizam operações unitárias sobre um q-bit é infinito, pois as matrizes unitárias 2x2 são infinitas. Entre as portas de um q-bit mais utilizadas estão as portas de Pauli já citadas, a porta Hadamard ou Hadamard-Walsh e a porta S. As operações realizadas por estas portas são explicadas nas seções seguintes.

5.1.1 Porta de Pauli X

A porta de Pauli X definida como

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{36}$$

corresponde a porta clássica NOT, pois $X|0\rangle = |1\rangle$ e $X|1\rangle = |0\rangle$, como pode ser visualizado mais detalhadamente nas Equações 37 e 38.

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \tag{37}$$

$$X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \tag{38}$$

Uma outra representação da porta quântica NOT pode ser vista na Figura 4.

Figura 4: Porta NOT quântica

5.1.2 Porta de Pauli Y

O operador unitário abaixo representa a porta Y

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{39}$$

que ao ser aplicada em um q-bit genérico $|\psi\rangle = |0\rangle + |1\rangle$ resulta em

$$Y|\psi\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} = i(|1\rangle - |0\rangle) \tag{40}$$

5.1.3 Porta de Pauli Z

A matriz que representa a porta Y é

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{41}$$

que ao ser aplicada a um estado genérico $|\psi\rangle = |0\rangle + |1\rangle$ resulta em

$$Z|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = |0\rangle - |1\rangle \tag{42}$$

5.1.4 Porta Hadamard ou Hadamard-Walsh

A porta de um q-bit hadarmard é definida pelo operador

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{43}$$

e leva um estado a uma superposição, como podemos observar nas equações seguintes

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{44}$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{45}$$

5.1.5 Porta de fase

A matriz que representa a porta S é

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{46}$$

assim aplicando S a um estado genérico $|\psi\rangle = |0\rangle + |1\rangle$ obtemos

$$S|\psi\rangle = S(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & i\beta \end{bmatrix} = \alpha|0\rangle + i\beta|1\rangle \tag{47}$$

5.2 Portas Quânticas de múltiplos Q-Bits

Apesar de infinito, o conjunto de portas de um q-bit não é universal, assim para realizar operações sobre n q-bits é necessário utilizar portas com mais de um q-bit. Serão mostradas aqui as portas quânticas CNOT e Toffoli as quais realizam operações sobre 2 e 3 q-bits respectivamente.

Em circuitos clássicos o símbolo • representa uma cópia, no entanto na computação quântica não existe cópia quântica como é demonstrado em [VNB04]. A Figura 5 apresenta uma porta controlada onde o símbolo • representa um controle, e a linha vertical o alvo deste controle. As portas CNOT e Toffoli possuem um e dois q-bits de controle respectivamente e um q-bit alvo.

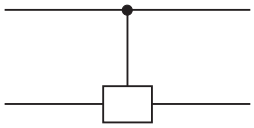


Figura 5: Porta controlada

5.2.1 Porta CNOT

A porta CNOT ou NOT-controlado é representada como na Figura 6 onde $\bigoplus$ pode ser vista a operação clássica XOR. A execução desta porta pode ser descrita da seguinte maneira, tendo o q-bit $|a\rangle$ como o controlador da negação do q-bit $|b\rangle$, ou seja $|b\rangle$ será negado se e somente se $|a\rangle = |1\rangle$ [dLJC03].

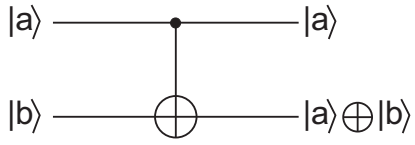


Figura 6: CNOT

5.2.2 Porta Toffoli

O funcionamento da porta Toffoli é bastante semelhante a CNOT, podemos visualizar sua representação na Figura 7. Seu funcionamento pode ser da seguinte maneira, caso os q-bits $|a\rangle$ e $|b\rangle$ sejam iguais a $|1\rangle$ o q-bit $|c\rangle$ será negado [dLJC03].

6 Circuitos Quânticos

Deustch [Deu85] propôs em 1985 um modelo para computação quântica universal, seria o correspondente a Máquina de Turing(MT) para computação clássica,

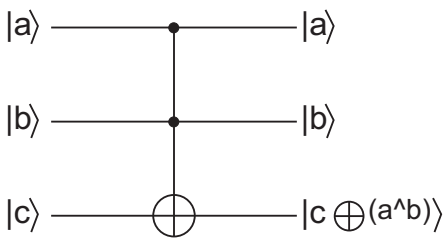


Figura 7: Toffoli

este modelo adicionava algumas características à MT, as quais permitia a representação de sobreposições.

Porém o modelo inicialmente proposto era bastante complexo, assim Deustch criou representação mais simples para a computação quântica que era bastante semelhante ao modelo de circuitos clássicos. Por serem de fácil compreensão os circuitos quânticos vem sendo cada vez mais utilizados.

Alguns circuitos quânticos serão aqui apresentados, como primeiro exemplo será apresentado o circuito quântico de swap e em seguida um circuito para realizar uma soma modulo 2.

6.1 Circuito swap

O circuito de swap pode ser visualizado na Figura 8, podemos observar que este circuito é formado por três portas CNOT.

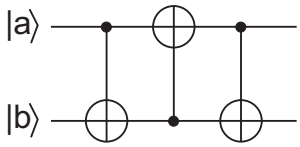


Figura 8: swap

A evolução deste circuito pode ser descrita da seguinte maneira, caso o q-bit de entrada $|a\rangle = |1\rangle$ e $|b\rangle = |0\rangle$, ao aplicarmos o primeiro CNOT aos dois q-bits, os q-bits de entrada para a segunda porta CNOT será $|a\rangle = |1\rangle$ e $|b\rangle = |1\rangle$, aplicando o segundo CNOT obtemos os estados $|a\rangle = |0\rangle$ e $|b\rangle = |1\rangle$, como o q-bit de controle para terceira porta CNOT é o q-bit $|0\rangle$, teremos a saída $|a\rangle = |0\rangle$ e $|b\rangle = |1\rangle$, a tabela 1 apresenta algumas entradas e saídas.

6.2 Circuito Somador de 2 bits

O circuito exibido na Figura 9 é apresentado em Menscher [Men97], este circuito realiza a soma de dois números de dois bits e obtém como resultado um número de 3 bits.

Tabela 1: Entradas e saídas para o circuito SWAP

Entradas		Saídas	
$\|a\rangle$	$\|b\rangle$	$\|a\rangle$	$\|b\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$

Podemos observar que o circuito somador apresentado é composto de portas CNOT e Toffoli exibidas como portas NOT quânticas controladas por um e dois q-bits respectivamente. A sétima porta é uma porta Toffoli com uma exibição alternativa, o q-bit só será negado se e somente se os q-bits de controlem forem iguais a $|1\rangle$.

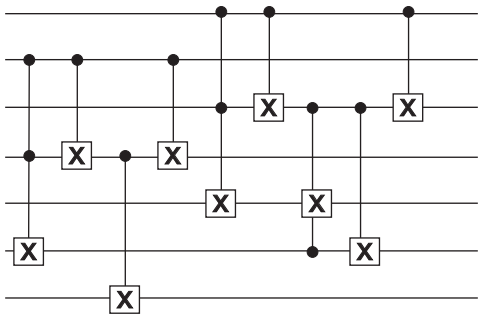


Figura 9: soma

A Tabela 2 apresenta o conjunto de q-bits de entrada, os q-bits de saída e os problemas de adição para os quais o circuito encontrou a solução.

6.3 Implementação de circuitos quânticos

Diversos estudos vêm sendo realizados para se conseguir construir um computador quântico [Pre]. Alguns requisitos para construção de uma máquina quântica são descritos em [Alv03], como abaixo:

- Armazenamento - Os q-bits precisam ser armazenados por períodos de tempo suficientes para completar computações interessantes.
- Isolamento - Os q-bits precisam estar isolados do ambiente, para minimizar erros por decoerência.
- Leitura - Os q-bits precisam permitir sua leitura de forma eficiente e confiável.

Estados de entrada	Estados de saída	Problema de adição equivalente
00 00 000	00 00 000	0+0=0
00 01 000	00 01 001	0+1=1
00 10 000	00 10 010	0+2=2
00 11 000	00 11 011	0+3=3
01 00 000	01 00 001	1+0=1
01 01 000	01 01 010	1+1=2
01 10 000	01 10 011	1+2=3
01 11 000	01 11 100	1+3=4
10 00 000	10 00 010	2+0=2
10 01 000	10 01 011	2+1=3
10 10 000	10 10 100	2+2=4
10 11 000	10 11 101	2+3=5
11 00 000	11 00 011	3+0=3
11 01 000	11 01 100	3+1=4
11 10 000	11 10 101	3+2=5
11 11 000	11 11 110	3+3=6

Tabela 2: Somador

- Portas lógicas - É necessário a possibilidade de manipulação de q-bits individuais. Deste modo, para permitir interações controladas entre q-Bits é necessário a construção de portas lógicas quânticas.
- Precisão - As portas lógicas quânticas precisam ser implementadas com alta precisão se o dispositivo for para cálculos confiáveis.

Diversas tecnologias vem sendo propostas para implementação de circuitos quânticos, como por exemplo:

- 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.

7 Conclusão

Computadores quânticos tornam possível uma nova forma de computação, eles não serão apenas mais velozes que os atuais, mas também resolverão problemas de maneira mais eficiente.

Os circuitos quânticos fornecem uma forma simples para que se possa compreender o funcionamento de computadores quânticos. Os circuitos aqui apresentados são bastante simples, esperamos que este trabalho forneça uma compreensão básica sobre o tema e que possibilite um estudo mais aprofundado sobre a computação quântica.

Referências

[Alv03] Flávio Luís Alves. Computação quântica fundamentos físicos e perspectivas, 2003.

[Cab04] Gustavo Eulalio M. Cabral. Uma ferramenta para projeto e simulação de circuitos quânticos. Master's thesis, Universidade Federal de Campina Grande, 2004.

[Deu85] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. Number 97, 1985.

[dLJC03] Aércio Ferreira de Lima, Bernardo Lula Júnior, and Gustavo Eulalio M. Cabral. Introdução à Computação Quântica. Technical Report 002, Universidade Federal de Campina Grande, junho 2003.

[FY95] Vicente Paz Fernandez and Antônio Nicolau Youssef. *Matemática para o segundo grau*. Editora scipione, 1995.

[Men97] D.P. Menscher. Modeling the quantum computer on the classical computer. Master's thesis, Brigham Young University, 1997.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[PLCM04] Renato Portugal, Carlile Campos Lavor, Luiz Mariano Carvalho, and Nelson Maculan. *Uma introdução à computação quântica*. SBMAC, 2004.

[Pre] John Preskill. Notas de aula do curso de computação quântica.

[Sho04] Salahoddin Shokranian. *Introdução à algebra linear*. Editora UNB, 2004.

[Ste75] G. Stephenson. *Introdução a matrizes conjutos e grupos*. Editora Edgard Blucher ltda, 1975.

[SW87] A. Steinbruch and Paulo Winterle. *Álgebra Linear e Geometria Analítica*. McGraw-Hill, 1987.

[Tan00] Andrew S. Tanenbaum. *Organização estruturada de computadores*. Livros Técnicos e Científicos Editora S.A., 2000.

[VNB04] André Luís Vignatti, Francisco Summa Netto, and Luiz Fernando Bittencourt. Uma introdução à computação quântica, fevereiro 2004.