

Technical Report

Quamputabilidade ou Computabilidade quântica:
Sobre máquinas de Turing quânticas, máquinas quânticas
universais etc. (mais sobre etc.)

João Cândido Lima Dovicchi¹

Florianópolis – SC
2015

¹Prof. Associado do Departamento de Informática e Estatística da Universidade Fed. de Santa Catarina

Conteúdo

1	Introdução	3
1.1	Um pouco de álgebra	4
1.2	Uma breve visão do gato de Schrödinger	8
2	Qubits	10
2.1	Postulado 1	11
2.2	Postulado 2	12
2.3	Postulado 3	14
2.4	Postulado 4	17
3	Computando com qubits	18
3.1	Registradores Quânticos	19
3.2	Portas quânticas	20
3.3	Reversibilidade	22
4	Quantum-Turing	25
4.1	Algoritmos quânticos	25
4.2	Church-Turing-Deutsch	26
5	Anotações (Anexo)	30
5.1	A esfera de Bloch	30
5.2	Operador Hamiltoniano	33
5.3	Matrizes de Pauli	34
5.4	Portas quânticas e símbolos	36
5.5	Operações com portas quânticas	39

1 Introdução

Em muitas aulas tenho sempre chamado a atenção de meus alunos para o beco-sem-saída em que von Neumann nos meteu. Talvez ele até tenha sido incitado pelas máquinas lógicas universais de Turing mas nos deixou presos no determinismo da computação clássica: uma máquina de estado. O mais incrível é que von Neumann foi o primeiro a reconhecer a importância dos espaços vetoriais de Hilbert e propor bases para a mecânica quântica [1].

O intuito de escrever este *Technical Report* é mostrar que talvez exista uma saída para a “computação determinística”. Talvez os estados quânticos, apesar de apresentarem certas complexidades, possam modelar o mundo físico com maior precisão e proximidade dos modelos quânticos. Afinal, mesmo a física clássica poderia deixar de se contentar com as aproximações grosseiras dos zeros e uns do computador digital.

A compreensão da computação quântica depende do conhecimento de algumas bases teóricas da física quântica. A física quântica, por si, depende de conceitos matemáticos, principalmente da álgebra e assim por diante. Este *technical report* pressupõe alguns conhecimentos anteriores de álgebra linear, autovalores, autovetores e apresenta outros conceitos algébricos e como estes são utilizados no arcabouço matemático da mecânica quântica.

A questão da computabilidade, estabelecida por Alonso Church [2] e Alan Turing [3] em 1936, formou a base para a implementação dos computadores digitais de hoje. No entanto, existe um problema fundamental quando os sistemas físicos clássicos (analógicos) são modelados pela computação clássica (discreta). O maior problema está relacionado com nível de precisão científica necessária para uma representação do mundo analógico no modelo digital. Aí se encontra um grande problema de compatibilidade do que pode ou não ser computável.

Em um artigo de 1985, Deutsch [4] mostra a incompatibilidade da Máquina Universal de Turing clássica e a física clássica, mas faz uma ressalva:

“The fact that classical physics and the classical universal Turing machine do not obey the Church-Turing principle in the strong physical form is one motivation for seeking a truly quantum model. The more urgent motivation is, of course, that classical physics is false.”

O autor acaba por defender que isto não impede que a teoria quântica e computadores quânticos universais possam ser compatíveis com o princípio da computabilidade de Church-Turing. O que ele chama de “*strong physical form*” está relacionado com a tese que expande o princípio de Church-Turing:

“Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means”.

Aliás, Yao [5] também se preocupa com esta questão da compatibilidade entre os sistemas físicos e o princípio estendido da computabilidade de Church-Turing que em seu artigo é chamado de (*Extended Church-Turing Thesis*).

1.1 Um pouco de álgebra

Para podermos compreender os conceitos básicos da computação quântica e como funcionam os operadores sobre os *quantum bits* ou “qbits” é necessário compreender algumas bases da álgebra no espaço vetorial complexo e suas relações com os conceitos de “estado quântico” e “resultados”. Aqui, consideramos o termo “resultados” como relativo aos dados observáveis ou que podem ser medidos em um determinado estado do sistema.

Primeiramente vamos adotar uma notação conhecida como notação de Dirac [6] para vetores. Esta notação é amplamente utilizada na Teoria Quântica. Por exemplo, no lugar de representarmos um vetor v por \vec{v} , vamos representá-lo como $|v\rangle$. A representação usa os “brackets” para representar vetores ($\langle |$ e $| \rangle$), sendo que os vetores $\langle v|$ são comumente chamados de *bra-vectors* e os vetores $|v\rangle$ são chamados de *ket-vectors*. A notação $\langle u|v\rangle$ representa o produto interno de $\vec{u} \cdot \vec{v}$.

Em espaços vetoriais reais, não existe diferença entre “bras” e “kets” a não ser que podemos relacionar os *bra-vectors* com vetores representados por uma matriz linha ($M_{1,n}$) e os *ket-vectors* com vetores representados por colunas ($M_{n,1}$). Entretanto, no espaço vetorial complexo, os *bra-vectors* representam complexos conjugados. Ficará evidente, mais adiante, qual é a vantagem de representá-los nesta notação.

Espaços vetoriais finitos

Chamamos de espaço vetorial a um conjunto de vetores que podem ser operados por adição entre si ou multiplicados por escalares para gerar outros vetores. Se os escalares são números reais os espaços são denominados reais e são simbolizados por \mathbf{R}^n , onde n representa a dimensão do espaço. Para uma revisão destes conceitos veja um bom livro texto de álgebra linear, como o livro de Howard Anton [7], por exemplo.

Um vetor A pode ser gerado pelos seus componentes e um vetor normalizado (vetor unitário) \hat{u}_i qualquer. Por ex.:

$$A = \sum_i A_i \hat{u}_i$$

Usando-se a notação de Dirac, temos:

$$|A\rangle = \sum_i A_i |\hat{u}_i\rangle$$

No espaço \mathbf{R}^n os vetores podem ser representados por matrizes linha ou matrizes coluna. Por exemplo, considere no \mathbf{R}^2 os vetores \mathbf{A} e \mathbf{B} , tal que:

$$\mathbf{A} = (A_1 \quad A_2) \quad \text{e} \quad \mathbf{B} = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$

Na notação de Dirac \mathbf{A} é representado como um *bra-vector* ou $\langle A|$ e \mathbf{B} como um *ket-vector* ou $|B\rangle$. E o produto interno de $\mathbf{A} \cdot \mathbf{B}$:

$$\mathbf{A} \cdot \mathbf{B} \equiv (A_1 \quad A_2) \cdot \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \equiv \langle A|B\rangle$$

e, portanto, $\langle A|$ representa o vetor transposto de $|A\rangle$.

Quando os escalares são números complexos, o espaço vetorial é dito complexo e é representado por \mathbf{C}^n , sendo n a dimensão do espaço vetorial complexo. Assim, um vetor A no espaço \mathbf{C}^n pode ser representado por seus componentes:

$$|A\rangle = A_1 \hat{u}_1 + A_2 \hat{u}_2 + \dots + A_n \hat{u}_n$$

e o vetor complexo conjugado A^* , por:

$$\langle A| = A_1^* \hat{u}_1 + A_2^* \hat{u}_2 + \dots + A_n^* \hat{u}_n$$

onde cada escalar A_n pode ser complexo e A_n^* seu respectivo complexo conjugado.

Na representação matricial, o vetor $|A\rangle$, tem $\langle A|$ como complexo conjugado:

$$|A\rangle = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \quad \text{e} \quad \langle A| = (A_1^* \quad A_2^*)$$

Assim, o produto interno $\langle A|B\rangle$ é a soma dos componentes de B multiplicados pelos complexos conjugados de A . Ou seja:

$$\langle A|B\rangle = \sum_i A_i^* B_i$$

De onde podemos concluir que:

$$\langle A|B\rangle = \langle B|A\rangle^*$$

O complexo conjugado $\langle A|$ é chamado, também, de “transposto conjugado” ou de “conjugado hermitiano”. Dada uma matriz C , a conjugada hermitiana é descrita como a transposta conjugada.

Uma matriz hermitiana é uma matriz do espaço vetorial complexo igual à própria matriz conjugada complexa (A^* ou A^\dagger). Ou seja:

$$A = A^*$$

Por exemplo, seja:

$$A = \begin{pmatrix} 1 & i & 1+i \\ -i & -5 & 2-i \\ 1-i & 2+i & 3 \end{pmatrix}$$
$$A^* = \bar{A}^T$$

$$\bar{A} = \begin{pmatrix} 1 & -i & 1-i \\ i & -5 & 2+i \\ 1+i & 2-i & 3 \end{pmatrix}$$

e, portanto:

$$A^* = \begin{pmatrix} 1 & i & 1+i \\ -i & -5 & 2-i \\ 1-i & 2+i & 3 \end{pmatrix}$$

Considerando-se um operador hermitiano, \hat{H} , usando-se a notação de Dirac, podemos escrever que $\langle A|\hat{H}|A\rangle = \langle A|\hat{H}|A\rangle^*$

Um operador hermitiano deve satisfazer, então, que a matriz transposta conjugada seja igual à matriz original, ou seja:

$$A^\dagger = A$$

e ele é importante porque, em mecânica quântica, as propriedades observáveis (resultados) de um sistema em determinado estado têm que ser representadas por um operador hermitiano.

Sobre operadores hermitianos, podemos resumir [8]:

1. Todos os autovalores de um operador hermitiano são reais;
2. Todos os operadores hermitianos têm autovetores;
3. Dois diferentes autovalores de um operador hermitiano têm autovetores que são mutualmente ortogonais;
4. $\exists D = (\lambda_1 \dots \lambda_n)$ autovetores mutualmente ortogonais de um operador hermitiano; e
5. Autovetores de um operador hermitiano formam uma base ortogonal completa para o referido espaço de Hilbert sobre o qual age o operador.

Para uma revisão dos conceitos básicos sobre espaços de Hilbert, veja o livro online do Prof. João Carlos A. Barata [9], no capítulo 37.

Um operador A é chamado de anti-hermitiano se $A^\dagger = -A$ e, consequentemente, se A é hermitiano então iA é anti-hermitiano.

O espaço de Hilbert

Os bits quânticos ou quantum bits, chamados de *qubits* são vetores de um espaço de Hilbert bidimensional [1] e todas as medidas observáveis são baseadas neste espaço vetorial complexo conhecido como espaço \mathbf{L}^2 [10, 11, 12].

Considere dois vetores ortogonais. Por exemplo:

$$|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad |v\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Podemos dizer que $|u\rangle$ e $|v\rangle$ são ortogonais pois o produto interno $\langle u|v\rangle$ é igual a zero e, além disso tanto $|u\rangle$ quanto $|v\rangle$ têm norma unitária, ou seja:

$$\|u\| = \sqrt{\langle u|u\rangle} = 1$$

e, tanto $|u\rangle$ quanto $|v\rangle$ podem gerar uma base ortonormal. Outro exemplo pode ser dado pelos vetores $|s\rangle$ e $|t\rangle$:

$$|s\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{e} \quad |t\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

que são ortogonais e

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{e} \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

também geram uma base ortonormal.

Um outro conceito importante para a compreensão das operações com qubits é o conceito de **mapa unitário**. Um mapa unitário U é um operador no espaço de Hilbert que causa uma rotação ou mudança de uma base ortonormal. Por exemplo, se:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

geram, respectivamente,

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \quad \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$$

então, um operador chamado mapa unitário:

$$\hat{U} \equiv \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}$$

tal que:

$$\hat{U} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \alpha_1 a + \alpha_2 b \\ \beta_1 a + \beta_2 b \end{pmatrix}$$

1.2 Uma breve visão do gato de Schrödinger

Na mecânica clássica os estados são representações de uma variável em função do tempo e os resultados são medidas possíveis destes estados. Na mecânica quântica os estados de um sistema físico são representados por vetores em um espaço vetorial complexo denominado espaço de Hilbert (\mathbf{L}^n) que contém os vetores de cada estado e os resultados ou dados observáveis são representados por autovalores de um operador hermitiano sobre este espaço.

Podemos resumir da seguinte forma:

- Considera-se estados de um sistema as condições de entrada e não o que se mede. O que se mede são quantidades observáveis.
- Estados de um sistema são representados por vetores no espaço vetorial complexo (espaço de Hilbert ou \mathbf{L}).
- Quantidades observáveis são operadores lineares; e
- Operadores lineares que representam dados observáveis são operadores hermitianos;

Podemos dizer, então, que uma variável física qualquer² tem que ter retornar valores reais esperados (tais como autovalores de um operador hermitiano). Um operador hermitiano é seu próprio adjunto (auto-adjunto)

$$\hat{H}^\dagger = \hat{H}$$

então,

$$\langle \psi | \hat{H}^\dagger | \psi \rangle \equiv \langle \psi | \hat{H} | \psi \rangle = \langle \psi | \hat{H} | \psi \rangle^*$$

logo:

$$\langle \psi | \hat{H} | \psi \rangle =; \int_{-\infty}^{\infty} \psi^*(x) \psi(x) dx = \langle \psi | \hat{H} | \psi \rangle^* \quad (1)$$

Por exemplo, imagine um operador $\hat{\Omega}$ constante, digamos que $\hat{\Omega} = a + ib$, onde a e b são reais e $i = \sqrt{-1}$. Por definição, o operador hermitiano conjugado é dado por:

$$\langle \phi | \hat{\Omega} \psi \rangle = \langle \hat{\Omega}^\dagger \phi | \psi \rangle$$

Conclui-se, da integral 1, que:

$$\langle (a - ib) \phi | \psi \rangle = \langle \phi | (a + ib) \psi \rangle = (a + ib) \langle \phi | \psi \rangle$$

ou seja, o conjugado hermitiano de um operador constante é o seu complexo conjugado.

²Considere uma variável em um determinado sistema que possa ser descrito por um espaço vetorial complexo de Hilbert.

Na mecânica quântica, uma medida ou resultado observável é uma das possibilidades descritas pelo operador hermitiano sobre um estado (vetor do espaço \mathbf{L}) no qual o sistema foi preparado. Por exemplo: dado um estado qualquer, digamos $|A\rangle$, representado por autovalores

$$\lambda_1, \lambda_2, \dots, \lambda_n.$$

para cada autovalor, existe um autovetor $|\Lambda_n\rangle$.

Postula-se que: a probabilidade de se obter diferentes resultados para os autovalores de λ_1 até λ_n é calculado pelos componentes de $|A\rangle$ ao longo da base λ_n , tomado com seu complexo conjugado:

$$|\langle \lambda_n | A \rangle|^2 = \langle \lambda_n | A \rangle \langle A | \lambda_n \rangle = P(\lambda_n)$$

se o sistema foi preparado no estado $|A\rangle$.

Considerando-se a simples trajetória de uma partícula, um estado específico da trajetória x pode ser expresso como função do tempo, por exemplo, $x(t)$ do ponto de vista da mecânica clássica. Do ponto de vista quântico estado corresponde a um espaço vetorial complexo de funções $\psi(x)$:

$$\psi(x) \Rightarrow |\psi(x)\rangle$$

Se considerarmos duas funções desta mesma trajetória $|\phi(x)\rangle$ e $|\psi(x)\rangle$, o produto interno é equivalente a:

$$\langle \phi(x) | \psi(x) \rangle = \int \phi^*(x) \psi(x) dx$$

Suponha o operador do momentum de uma partícula, que na mecânica quântica é descrito por:

$$\frac{\partial}{\partial x} \left(\frac{\hbar}{i} \right) \tag{2}$$

o conjugado hermitiano do operador $\frac{\partial}{\partial x}$ pode ser deduzido usando-se a integral para derivar o resultado:

$$\left\langle \phi \left| \frac{\partial}{\partial x} \right. \right\rangle = \int_{-\infty}^{\infty} \phi^*(x) \frac{\partial \psi(x)}{\partial x} dx \tag{3}$$

Integrando 3 em partes, diferenciando ϕ e integrando para se obter ψ :

$$\left\langle \phi \left| \frac{\partial}{\partial x} \right. \right\rangle = [\phi^*(x) \psi(x)]_{-\infty}^{\infty} - \int_{-\infty}^{\infty} \frac{\partial \phi^*(x)}{\partial x} \psi(x) dx = \left\langle \frac{-\partial}{\partial x} \phi \left| \psi \right. \right\rangle$$

Portanto o hermitiano conjugado do operador $\frac{\partial}{\partial x}$ é $-\frac{\partial}{\partial x}$ e o operador de momentum, da equação 2 é:

$$\frac{-\partial}{\partial x} \left(\frac{\hbar}{-i} \right)$$

2 Qubits

Para se tratar de computação quântica é necessário entender sua entidade básica. Assim como a computação clássica tem como unidade fundamental uma abstração matemática, o *bit*, a computação quântica se baseia em uma abstração como unidade, o *qubit* ou quantum bit. O nome *qubit* foi criado por Benjamin Schumacher [13, 14] em 1995 para se referir ao bit quântico.

Um bit quântico pode ser representado em dois estados quânticos $|0\rangle$ e $|1\rangle$ e, portanto, são vetores no espaço vetorial bidimensional complexo (espaço de Hilbert), formando combinações lineares chamadas “superposições” representadas por $|\psi\rangle$, onde:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Enquanto um bit pode assumir 2 estados $\{0, 1\}$, um qubit pode estar em um outro estado que não $|0\rangle$ ou $|1\rangle$. Os estados $|0\rangle$ e $|1\rangle$ formam uma base ortonormal deste espaço vetorial e são conhecidos como bases quânticas computacionais [15], que podem ser expressas no \mathbf{L}^2 como:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Os escalares α e β são números complexos e

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

Podemos representar os qubits em um espaço vetorial complexo como na esfera de Bloch, conforme a figura 1 (veja também as Anotações 5.1).

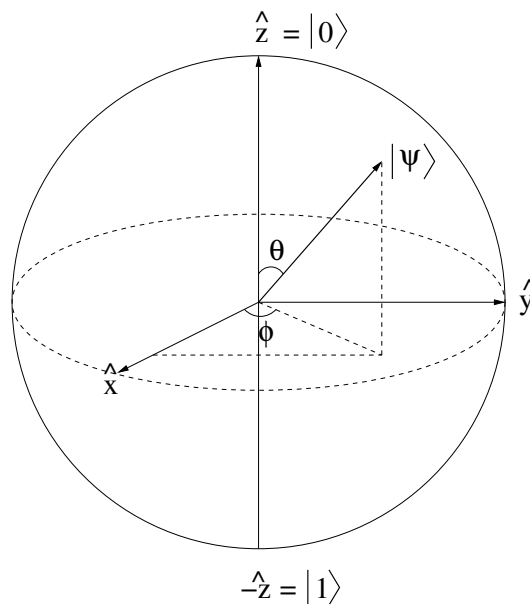


Figura 1: Representação do qubit na esfera de Bloch

Formalmente, podemos representar o estado de um qubit como um vetor unitário no espaço \mathbf{C}^2 — mais precisamente, no espaço de Hilbert \mathbf{L}^2 — e mais facilmente em um círculo unitário (vide fig 2).

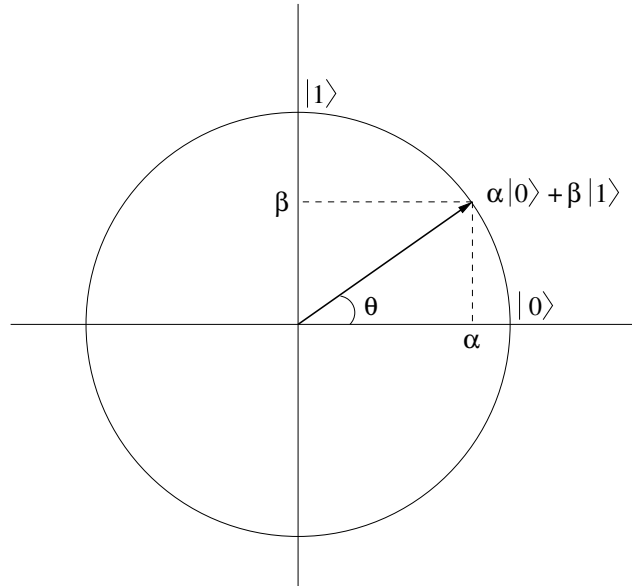


Figura 2: Representação do qubit no plano bidimensional

Qualquer tentativa de medir o estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ resultará em $|0\rangle$ com probabilidade $|\alpha|^2$ e $|1\rangle$ com probabilidade $|\beta|^2$. Qualquer outra tentativa de se medir o estado, resultará no mesmo valor, ou seja, o sistema está no estado “medido”. Podemos extrair apenas um bit de informação do estado de um qubit. Uma explicação muito clara sobre este aparente paradoxo pode ser encontrada no primeiro capítulo do livro de Leonard Susskind “Quantum Mechanics, The Theoretical Minimum” [16].

O processo de medida ou o dispositivo utilizado para medir determinam uma base quântica. Assim, se dois vetores $|\phi\rangle, |\psi\rangle \in \mathbf{C}^2$ são linearmente independentes eles podem servir como uma base vetorial:

$$\alpha|0\rangle + \beta|1\rangle = \alpha'|\phi\rangle + \beta'|\psi\rangle$$

$|0\rangle$ e $|1\rangle$ formam uma base ortonormal que podemos chamar de “base computacional quântica”.

Podemos, agora, escrever quatro postulados básicos da mecânica quântica que nos interessam especialmente para a computação quântica [15].

2.1 Postulado 1

O primeiro deles é chamado de postulado de estado e é formalmente descrito assim:

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system’s state space.

Ou seja, todo sistema físico é descrito por um espaço vetorial complexo com produto interno (um espaço de Hilbert); e é completamente descrito em um determinado tempo por um vetor de estado que é um vetor unitário no referido espaço vetorial do estado.

Uma vez que a mecânica quântica não especifica qual o estado para determinado sistema físico, podemos descrever um qubit em qualquer espaço de estado em \mathbf{C}^2 , por exemplo a orientação de um fóton ou o spin de um elétron.

Embora um estado quântico possa requerer sistemas com espaço dimensional infinito, na computação quântica temos que considerar sistemas dimensionalmente finitos.

2.2 Postulado 2

O segundo postulado conhecido como *Evolution Postulate* [15] é formalmente enunciado como:

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2 .

O segundo postulado é relativo à equação de Schrödinger para a evolução temporal de um sistema quântico fechado, descrita por um operador hermitiano fixo, chamado de **hamiltoniano** que representaremos por $\hat{\mathbf{H}}$ (como um operador hermitiano, mas em negrito):

$$\hat{\mathbf{H}}|\psi\rangle = i\hbar \frac{d}{dt}|\psi\rangle \quad (4)$$

onde, $\hat{\mathbf{H}}$ é um operador hamiltoniano³ e \hbar é a constante de Plank $h/2\pi$.

Podemos enunciar o segundo postulado de forma mais clara:

“O estado $|\psi\rangle$ de um sistema quântico fechado em um tempo t_1 é relacionado a um estado $|\psi'\rangle$ no tempo t_2 por um operador unitário \hat{U} dependente de t_1 e t_2 .”

³O operador hamiltoniano está descrito nas anotações no final deste TR (veja Anotações 5.2)

$$|\psi'\rangle = \hat{U}|\psi\rangle \quad (5)$$

onde,

$$\hat{U}(t_1, t_2) = \exp \left[\frac{-i\hat{H}(t_2 - t_1)}{\hbar} \right]$$

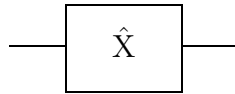
Note que este postulado é relativo à conservação da energia de um sistema quântico. Ainda, se o operador hamiltoniano \hat{H} é hermitiano e \hat{U} é um operador unitário, então a equação 5 implica em:

$$\| |\psi'\rangle \| = \| \hat{U}|\psi\rangle \| = \| |\psi\rangle \| = 1$$

Na computação quântica, a maioria dos operadores são unitários e podem ser representados por matrizes onde cada coluna é um vetor unitário e com colunas emparelhadas que são mutuamente ortogonais.

Podemos abstrair a idéia e representar estes operadores como portas de circuitos (*gates*). Considere os operadores unitários em \mathbf{L}^2 que podem representar 1 qubit, por exemplo, usando as portas de Pauli para spins de elétrons como base⁴.

A porta:



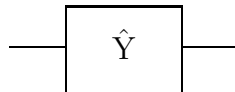
pode ser descrita pelo operador \hat{X} , tal que:

$$\hat{X}|0\rangle = |1\rangle \text{ e } \hat{X}|1\rangle = |0\rangle$$

onde,

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

A porta:



pode ser descrita pelo operador \hat{Y} , tal que:

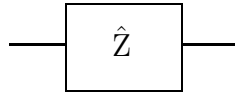
$$\hat{Y}|0\rangle = i|1\rangle \text{ e } \hat{Y}|1\rangle = -i|0\rangle$$

onde,

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

A porta:

⁴*Pauli Gates* são relativas às matrizes de Pauli que são matrizes complexas 2×2 , hermitianas e unitárias (veja Anotações 5.3).



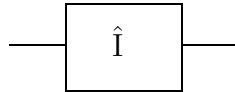
pode ser descrita pelo operador \hat{Z} , tal que:

$$\hat{Z}|0\rangle = |0\rangle \text{ e } \hat{Z}|1\rangle = -|1\rangle$$

onde,

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

Podemos, ainda, incluir uma porta para o operador de identidade \hat{I} :



pode ser descrita pelo operador \hat{I} , tal que:

$$\hat{I}|0\rangle = |0\rangle \text{ e } \hat{I}|1\rangle = |1\rangle$$

onde,

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2.3 Postulado 3

O terceiro postulado [15], conhecido como postulado de medição, é enunciado como:

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment.

Com o intuito de tornar mais claro, podemos enunciar-lo, como:

“As leituras de um sistema quântico podem ser representadas por probabilidades p de saídas representadas operadores \hat{P}_m de um conjunto M de vetores hermitianos $\{\hat{P}_m : m \in M\}$ que descrevem os estados do sistema.”

De fato já dissemos que os estados do sistema quântico são representados por vetores do espaço de Hilbert e que as leituras são obtidas por operadores hermitianos sobre este espaço vetorial.

Se o estado de um sistema for, digamos, $|\psi\rangle$ antes de medido, a possibilidade de saída $p(m)$ é dada por:

$$p(m) = \langle \psi | P_m^\dagger \cdot P_m | \psi \rangle$$

e, depois de medido, o estado é dado por:

$$\frac{P_m |\psi\rangle}{\sqrt{\langle \psi | P_m^\dagger \cdot P_m | \psi \rangle}}$$

Os operadores de leitura (medidas) têm que satisfazer a equação de complementariedade, onde:

$$\sum_{m \in M} P_m^\dagger \cdot P_m = I$$

o que garante que a soma das probabilidades de saída seja 1. Assim,

$$\sum_m p(m) = \sum_m \langle \psi | P_m^\dagger \cdot P_m | \psi \rangle = \langle \psi | \hat{I} | \psi \rangle = 1$$

Na computação quântica, o principal interesse é nos operadores que são projeções numa base ortonormal particular do espaço chamado de “base computacional”. Então, podemos representar as medidas de um bit como sendo:

$$\hat{P}_0 = |0\rangle\langle 0| \text{ e } \hat{P}_1 = |1\rangle\langle 1|$$

que resulta em $\alpha|0\rangle + \beta|1\rangle$, ou seja, $p(0) = |\alpha|^2$ e $p(1) = |\beta|^2$.

Por exemplo, se $\hat{P}_0 = |0\rangle\langle 0|$, então:

$$\hat{P}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

e, evidentemente:

$$\hat{P}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Observe que $\hat{P}_0^\dagger \hat{P}_0 + \hat{P}_1^\dagger \hat{P}_1 = I$. E aqui é bom lembrar que, se temos uma base ortonormal no espaço de Hilbert,

$$\begin{aligned} |\psi\rangle &= \sum_{i \in \mathbf{N}} \langle a_i | \psi \rangle |a_i\rangle \\ &= \sum_{i \in \mathbf{N}} |a_i\rangle \langle a_i | \psi \rangle \end{aligned}$$

e, portanto,

$$\sum_{i \in \mathbb{N}} |a_i\rangle\langle a_i| = \hat{1}$$

é um operador unitário.

Dado o estado de um sistema $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, a probabilidade de se medir $|0\rangle$ pode ser escrita como:

$$p(0) = \langle\psi|\hat{P}_0^\dagger\hat{P}_0|\psi\rangle$$

já que $\hat{P}_0^\dagger\hat{P}_0 = \hat{P}_0$ podemos escrever:

$$\begin{aligned} p(0) = \langle\psi|\hat{P}_0|\psi\rangle &= \begin{pmatrix} a^* & b^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= \begin{pmatrix} a^* & b^* \end{pmatrix} \begin{pmatrix} a \\ 0 \end{pmatrix} = |a|^2 \end{aligned}$$

Na mecânica quântica o fator da fase global da função de onda não tem significado físico, ou seja, numa onda contínua não existe o ponto inicial para se medir a fase absoluta. O que realmente interessa é a fase relativa.

Um operador \hat{P}_m de medida independe da fase global ou do fator de fase global⁵(veja capítulo VII:I do livro de Albert Messiah) [17]. Assim, para qualquer estado $|\psi\rangle$ e qualquer fase θ , podemos obter o vetor $e^{i\theta}|\psi\rangle$. Então, qualquer operador unitário \hat{U} :

$$\hat{U}e^{i\theta}|\psi\rangle = e^{i\theta}\hat{U}|\psi\rangle$$

e, para qualquer operador de medida \hat{P}_m ,

$$\langle\psi|e^{-i\theta}\hat{P}_m^\dagger\hat{P}_me^{i\theta}|\psi\rangle = \langle\psi|\hat{P}_m^\dagger\hat{P}_m|\psi\rangle$$

Entretanto, considerando-se dois estados $|\psi_1\rangle$ e $|\psi_2\rangle$, tal que:

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

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

medidos na base computacional, resultam na mesma probabilidade de saída, enquanto que se forem medidos numa outra base ortonormal, o resultado é diferente.

Além disso, se

⁵Chamamos de “fase global” ou “fator de fase global” ao fator exponencial complexo $e^{i\theta}$ de qualquer número complexo escrito na forma polar. Este termo também pode ser chamado de “fasor”. O ângulo θ é chamado de fase e uma função de onda multiplicada pelo fasor $e^{i\theta}$ soma a fase da onda do valor θ . Na mecânica quântica o fasor é um número complexo unitário, isto é, de valor absoluto 1.

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

então,

$$H|\psi_1\rangle = |0\rangle \text{ e } H|\psi_2\rangle = |1\rangle$$

2.4 Postulado 4

O quarto postulado ou *composition postulate* é enunciado por Nielsen [15] da seguinte maneira:

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n , and system number i is prepared in the state ρ_i , then the joint state of the total system is $\rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n$.

Isto quer dizer que o estado de um sistema composto é formado pelo produto tensor dos estados individuais dos componentes, ou seja, um sistema $|\psi_{1,2}\rangle$ formado pelos componentes dos sistemas $|\psi_1\rangle$ e $|\psi_2\rangle$ será o produto tensor entre eles:

$$|\psi_{1,2}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

O Produto tensor ou produto de Kronecker é o produto de cada elemento de um vetor pelo outro vetor. Por exemplo, seja:

$$|A\rangle = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \text{ e } |B\rangle = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

o produto tensor ou produto de Kronecker entre eles será dado por:

$$|A\rangle \otimes |B\rangle = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_1 b_3 \\ a_2 b_1 \\ a_2 b_2 \\ \vdots \\ a_3 b_3 \end{pmatrix}$$

Por exemplo, as bases $|0\rangle$ e $|1\rangle$ podem ser usadas para formar as bases $|00\rangle \dots |11\rangle$:

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

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

Estas bases formam as bases computacionais de um sistema de dois qubits. Um par de qubits também pode existir em superposições deste quatro estados que envolve um coeficiente complexo — algumas vezes chamado de amplitude — descrito pelo vetor $|\psi\rangle$ tal que: state, such that the state vector describing the two qubits is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

onde as condições de probabilidade de cada coeficiente somam 1, ou seja:

$$\sum_{x \in \{0,1\}^2} |\alpha_x|^2 = 1$$

Nem todos os estados combinados podem ser separados em produtos tensores dos componentes individuais. Ele é separável se puder ser expresso como um produto tensor dos componentes. Por exemplo:

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

Dois estados de um sistema de 2-qubits não podem ser separados nas partes componentes⁶:

$$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \text{ e } \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

3 Computando com qubits

O que é um computador quântico? Bem, podemos dizer que é um computador que opera algumas transformações, sob condições bem controladas e governadas pelas leis da mecânica quântica. Mermin [18] define:

⁶Separação não implica em separabilidade. Duas partículas podem estar fisicamente separadas mas continuam ligadas (*entangled*).

“A quantum computer is one whose operation exploits certain very special transformations of its internal state, (...). The laws of quantum mechanics allow these peculiar transformations to take place under very carefully controlled conditions.”

3.1 Registradores Quânticos

Os registradores são a parte fundamental do processador na computação clássica. Todo e qualquer processamento de um algoritmo é realizado nos registradores de um processador. Na computação quântica, os registradores, quando medidos, são formados por uma cadeia de bits que tem o tamanho da informação armazenada. No estado de superposição, cada registrador é uma superposição de n qubits relativos aos 2^n cadeias possíveis das superposições de $|0\rangle$ e $|1\rangle$. Ou seja,

$$|\psi_n\rangle = \sum_{k=0}^{2^n-1} a_k |k\rangle$$

Por exemplo, considere um registrador de 3-qubits. O sistema pode ser representado por:

$$|\psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \dots + \alpha_6|110\rangle + \alpha_7|111\rangle$$

Cada uma das configurações possíveis destas superposições podem ser obtidas pelos produtos tensores dos qubits componentes, ou seja:

$$\begin{aligned} |000\rangle &= |0\rangle \otimes |0\rangle \otimes |0\rangle \\ &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0) \end{aligned}$$

$$\begin{aligned} |001\rangle &= |0\rangle \otimes |0\rangle \otimes |1\rangle \\ &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= (0\ 1\ 0\ 0\ 0\ 0\ 0\ 0) \end{aligned}$$

$$\begin{aligned} |010\rangle &= |0\rangle \otimes |1\rangle \otimes |0\rangle \\ &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= (0\ 0\ 1\ 0\ 0\ 0\ 0\ 0) \end{aligned}$$

$$= \dots$$

Cada uma, em termos de bases computacionais dos componentes, podemos representar por:

$$|\psi\rangle = \alpha_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_4 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_5 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_6 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_7 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

3.2 Portas quânticas

Na computação clássica, as portas lógicas são implementadas eletronicamente e a informação da entrada é manipulada e retorna um estado convertido pelo circuito. Assim, por exemplo, um circuito que pode inverter a entrada é um circuito chamado de “porta not” ou simplesmente NOT. Neste caso, o estado de um bit de entrada o circuito produz o bit inverso na saída como esquematizado na figura 3.



Figura 3: Representação esquemática da porta NOT

Na computação quântica, era de se esperar que a inversão acontecesse nos vetores de estado $|0\rangle$ e $|1\rangle$. Entretanto, apenas a inversão dos estados não evidencia a superposição dos qubits $|0\rangle$ e $|1\rangle$. A porta NOT quântica⁷ troca o estado:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{por} \quad |\neg\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

onde $\neg\psi$ — leia-se *not-psi* — é o inverso do sistema $|\psi\rangle$. A porta quântica NOT pode ser representada pelo operador \hat{X} de Pauli (ver Anotações 5.3 no final deste relatório).

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

Se o estado quântico é $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, então:

$$\hat{X} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

⁷Aqui os termos porta e operador são usados um pelo outro, dependendo da abordagem: se for algébrica, usaremos o termo operador e se for computacional, usaremos porta.

Enquanto na computação clássica temos apenas a porta NOT como uma porta simples e unitária, na computação quântica os operadores \hat{Z} e \hat{H} (Hadamard) também podem ser usadas. Por exemplo, a porta

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

mantém o estado $|0\rangle$ inalterado e inverte o sinal do estado $|1\rangle$ resultando em $-|1\rangle$. Ou seja:

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

A porta Hadamard

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

converte cada estado em metade do caminho entre $|0\rangle$ e $|1\rangle$:

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

Observe no diagrama em esfera de Bloch (veja figura 1) que a porta de Hadamard é equivalente a rotacionar o eixo \hat{y} de 90° , seguida pela rotação no eixo \hat{x} de 180° .

Na computação clássica, as portas AND, OR, XOR, NAND e NOR são portas que recebem dois bits e retornam um bit como resultado da operação. Na computação quântica também podemos ter portas que recebem dois qubits e, assim temos muitas possibilidades de operações executadas por estas portas, já que o total seria $4! = 24$ operações. Mas tomemos como primeiro exemplo um operador emprestado da mecânica quântica sobre spins $\hat{S}_{m,n} = \hat{S}_{n,m}$ que sobre um par $\{x, y\}$ inverte os elementos do par. Por exemplo:

$$\begin{aligned} \hat{S}|xx\rangle &= |xx\rangle \\ \hat{S}|xy\rangle &= |yx\rangle \\ \hat{S}|yx\rangle &= |xy\rangle \\ \hat{S}|yy\rangle &= |yy\rangle \end{aligned}$$

Então podemos escrever o operador como:

$$\hat{S} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

e observe que se o estado $|\psi\rangle$ for dado por:

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

então, podemos dizer que o operador \hat{S} sobre $|\psi\rangle$ resulta em:

$$\hat{S}|\psi\rangle = \alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|11\rangle$$

onde, \hat{S} é o operador que representa a porta lógica quântica *Swap*.

Existem várias possibilidades de operadores que podem representar as portas de circuitos quânticos e algumas delas são fundamentais (ver Nielsen [15], Mermin [18] e alguns exemplos nas Anotações 5.4). As operações computacionais das portas quânticas podem, desta forma ser resultados observáveis de estados quânticos (superposições) produzidos por estes operadores. Por exemplo, os circuitos podem ser combinados para operar sobre os estados e cada um representa um operador unitário U que produz uma superposição diferente dos estados que pode ser medida por um autovalor de M (veja figura 4).

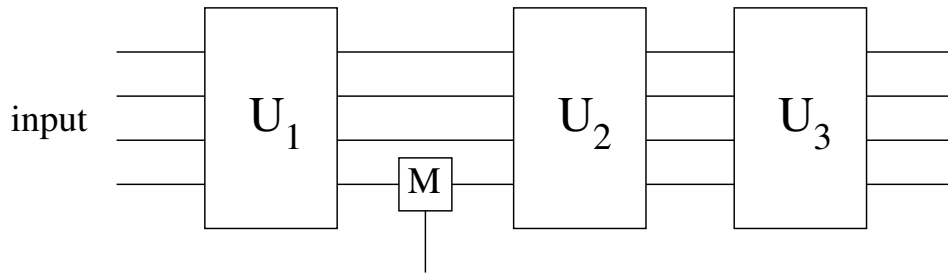


Figura 4: Exemplo abstrato de um circuito quântico. Cada operador \hat{U}_i é descrito por uma matriz $2^n \times 2^n$ (Modificado de Dawar [19])

Em suma, a operação que uma porta quântica executa, nada mais é do que a transformação linear feita por uma matriz multiplicada pela entrada para calcular uma saída. Por exemplo:

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

e esta operação é determinística. No entanto, se tivermos um estado do sistema, representado por $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, a transformação será sobre as possibilidades $(\alpha \beta)^T$, ou seja:

$$\neg \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

que resulta na negação: $\neg|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$.

3.3 Reversibilidade

Algumas portas lógicas podem ser revertidas, isto é, o operador aplicado duas vezes, retorna o estado inicial. Estas portas são chamadas de portas universais. Por exemplo, considere o sistema $|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$ e o operador \hat{C}_{NOT} (*controled-NOT*), tal que:

$$\hat{C}_{NOT} |\psi\rangle = |\psi'\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|11\rangle + \alpha_3|10\rangle$$

podemos dizer que \hat{C}_{NOT} é inversível pois sua operação troca apenas as possibilidades dos estados, cujo primeiro qubit seja 1 e, portanto, é uma porta universal pois $\hat{C}_{NOT} |\psi'\rangle = |\psi\rangle$.

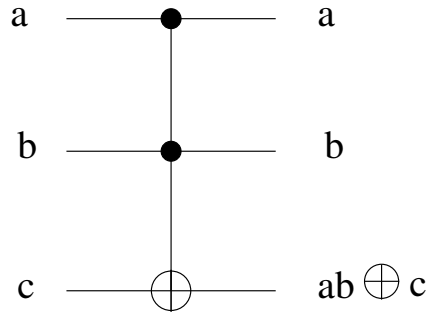


Figura 5: Esquema de um circuito lógico quântico Toffoli (fonte: Nielsen [15])

O mesmo acontece com a porta de Toffoli [20] que também pode ser usada em computação quântica. seja, por exemplo:

$$|\psi\rangle = \alpha_0|000\rangle + \dots + \alpha_7|110\rangle + \alpha_8|111\rangle \quad (6)$$

a porta de Toffoli (veja figura 5) pode ser representada pelo mapa unitário:

$$T \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

e o operador \hat{T} sobre o sistema $|\psi\rangle$ da equação 6 resulta em:

$$\hat{T} |\psi\rangle = \alpha_0|000\rangle + \dots + \alpha_7|111\rangle + \alpha_8|110\rangle$$

Neste caso, se $\hat{T} |\psi\rangle = |\psi'\rangle$, então $\hat{T} |\psi'\rangle = |\psi\rangle$. Claramente, o operador é inversível.

Um comportamento bem diferente das portas lógicas clássicas é o caso da porta $\sqrt{\text{NOT}}$ ou SRN (*square root not*) [21]. Este operador, quando aplicado a um quantum bit gera a superposição (randomizando o qubit) e, no entanto a aplicação combinada de duas portas $\sqrt{\text{NOT}}$ é determinística pois é equivalente a uma porta NOT.

A porta $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ é chamada de “raíz quadrada do NOT” porque:

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

e $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, em relação aos qubits, é equivalente à porta NOT⁸. Este tipo de comportamento não tem paralelo nas portas lógicas da computação clássica.

Existem ainda outras portas lógicas quânticas que podem ser usadas para propósitos específicos, tais como, uma porta de rotação do qubit, ou seja, uma porta que toma o vetor unitário de entrada e rotaciona o qubit de um ângulo θ com outro ângulo de valor constante ϕ , por exemplo:

$$\hat{P}_{\theta,\phi} = \begin{pmatrix} \cos(\theta) & \sin(\theta)e^{i\phi} \\ -\sin(\theta)e^{-i\phi} & \cos(\theta) \end{pmatrix}$$

E ainda, podemos citar portas que mudam a fase (*phase shift gate*) que podem ser usadas para deslocar a fase de um ângulo ϕ qualquer para alinhar fases de qubits com a finalidade de alinhar a superposição ou qualquer outro tipo de interferência em outros qubits:

$$\hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Veja mais detalhes sobre operações com qubits e portas quânticas, nas Anotações 5.5 no final deste relatório.

Podemos considerar então que, com base nestas propriedades das portas quânticas e o “paradoxo de Zeno” [22], todo sistema lógico clássico pode ser simulado em um computador quântico. Mas voltaremos a isto mais adiante.

⁸Note que, como operador algébrico, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ é diferente de $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

4 Quantum-Turing

A discussão sobre a validação das máquinas lógicas universais de Turing — que nós conhecemos simplesmente como “máquinas de Turing” — já é bastante antiga na área da computação quântica. Já na década de 70, Ingarden publicou um artigo que discutia a teoria da informação de Shannon [23] do ponto de vista da teoria quântica, mostrando que é possível generalizar a teoria de Shannon dentro do formalismo da teoria quântica usando o conceito de “observáveis” (*observables*) e que ele denominou de *semi-observables* [24].

Feynman em sua famosa palestra “There’s Plenty of Room at the Bottom” [25] mostrou que parecia impossível simular um sistema quântico em um computador clássico de forma eficiente. Ele propôs, depois, um modelo de simulação de qualquer sistema em um espaço vetorial com um estado de dimensões finitas equivalente a um computador que era capaz destas simulações se fosse preparado em um estado adequado [26].

O modelo de computação quântica descrito por Benioff [27] talvez seja a primeira proposta de uma estrutura para um computador quântico. No entanto, o modelo ainda é clássico, uma vez que o final de cada passo computacional é determinístico e, portanto, perfeitamente simulável por uma máquina de Turing clássica.

O trabalho de Deutsch [4] descreve um modelo computacional completamente quântico com forte influência do trabalho sobre “Autômatos Quânticos” de Albert [28]. Os Autômatos de David Albert possuíam estados que representavam as soluções de equações de movimento da mecânica quântica, considerando as suas capacidades de medir, saber e prever as suas propriedades físicas.

4.1 Algoritmos quânticos

Antes de compreender o algoritmo de Deutsch [4] é necessário compreender algumas diferenças entre os algoritmos clássicos e os algoritmos quânticos. As diferenças são, basicamente:

- Os algoritmos quânticos são muito mais rápidos que os clássicos.
- Algoritmos quânticos podem resolver mais problemas relativos ao mundo real que os algoritmos clássicos.
- Um algoritmo quântico pode calcular uma função $f(x)$ para vários valores de x simultaneamente.

Por exemplo, vamos considerar duas entradas x e y e um algoritmo que compute x e $y \oplus f(x)$. Esta “máquina” pode ser esquematizada como na figura 6.

Neste exemplo, se a entrada x for $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e a entrada $y = |0\rangle$, então, a saída $|\psi\rangle$ será:

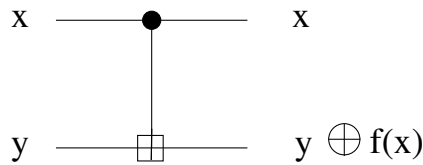


Figura 6: Exemplo de um algoritmo quântico

$$\begin{aligned}
 |\psi\rangle &= \frac{|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle}{\sqrt{2}} \\
 &= \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}
 \end{aligned}$$

Podemos considerar que, fisicamente, as entradas estariam nos registros de dados e a saída $|\psi\rangle$ seria medida no registro de destino.

4.2 Church-Turing-Deutsch

David Deutsch foi um dos primeiros a formular uma descrição formal para uma máquina de Turing quântica e um algoritmo fundamental para um programa de computador quântico.

Quando Deutsch [4] defende que:

‘Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means’.

ou seja, “todo sistema físico finito pode ser perfeitamente simulável por uma máquina de estado universal que opera por meios finitos”, ele defende que este postulado é mais físico é mais bem definido que o próprio postulado clássico de Turing. Junte-se a isso a terceira lei da termodinâmica, ou seja: “nenhum processo finito pode reduzir a entropia ou a temperatura a zero de um sistema físico finito”.

Em seu artigo, ele mostra que, com base na terceira lei da termodinâmica, a teoria quântica obedece ao citado princípio estendido de Church-Turing supra citado.

Uma afirmação importante deste artigo é que a hipótese de Church-Turing, vista como um princípio da física não torna a ciência da computação — ou a computação quântica — um ramo da física, mas torna a física experimental um ramo da ciência da computação.

Além disso, a computação quântica levanta problemas interessantes sobre a modelagem de linguagens de programação quânticas. Hoje muitas linguagens voltadas para algoritmos quânticos têm sido criadas [29]e, certamente, será assunto para outro *technical report* no futuro.

Referências

- [1] HILBERT, D.; NEUMANN, J. von; NORDHEIM, L. Über die Grundlagen der Quantenmechanik. (German) [On the foundations of quantum mechanics]. *Mathematische Annalen*, v. 98, p. 1–30, 1927. ISSN 0025-5831 (print), 1432-1807 (electronic).
- [2] CHURCH, A. An unsolvable problem of elementary number theory. *Amer. J. Math.*, v. 58, p. 345–363, 1936.
- [3] TURING, A. M. On computable numbers with an application to the Entscheidungsproblem. *Proc. London Math. Soc. (3)*, v. 42, p. 230–265, 1936. A correction, 43:544–546.
- [4] DEUTSCH, D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, v. 400, p. 97–117, 1985. Disponível em: <<http://www.davidddeutsch.org.uk/wp-content/deutsch85.pdf>>.
- [5] YAO, A. C.-C. Classical physics and the church–turing thesis. *J. ACM*, ACM, New York, NY, USA, v. 50, n. 1, p. 100–105, jan. 2003. ISSN 0004-5411. Disponível em: <<http://doi.acm.org/10.1145/602382.602411>>.
- [6] DIRAC, P. A. M. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, v. 35, p. 416–418, 7 1939. ISSN 1469-8064. Disponível em: <http://journals.cambridge.org/article_S0305004100021162>.
- [7] ANTON, H.; RORRES, C. *Algebra Linear com Aplicações*. Bookman, 2001. ISBN 9788573078473. Disponível em: <<http://books.google.com.br/books?id=pOaaSKP9IcMC>>.
- [8] DOVICCHI, J. *Uma pequena introdução à álgebra para mecânica quântica*. [S.l.], 2014. Disponível em: <<http://www.inf.ufsc.br/~dovicchi/papers-jcd/qalgebra.pdf>>.
- [9] BARATA, J. C. A. *Curso de Física Matemática*. 2014. Livro online. Disponível em: <http://denebola.if.usp.br/~jbarata/Notas_de_aula/notas_de_aula.html>.
- [10] DANOS, V.; KASHEFI, E.; PANANGADEN, P. *1-qubit versus 2-qubit measurement-based quantum computation*. 2005. Manuscript. Disponível em: <<http://www.pps.jussieu.fr/danos/pdf/teleport.pdf>>.
- [11] DANOS, V.; KASHEFI, E. Determinism in the one-way model. *Physical Review A*, v. 74, p. 052310, 2006. Also arXiv:quant-ph/0506062. Disponível em: <<http://dx.doi.org/10.1103/PhysRevA.74.052310>>.

- [12] DANOS, V.; KASHEFI, E.; PANANGADEN, P. The measurement calculus. *Journal of the ACM*, v. 54, n. 2, 2007. Preliminary version in arXiv:quant-ph/0412135. Disponível em: <<http://doi.acm.org/10.1145/1219092.1219096>>.
- [13] SCHUMACHER, B. Quantum coding. *Phys. Rev. A*, American Physical Society, v. 51, p. 2738–2747, Apr 1995. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.51.2738>>.
- [14] SCHUMACHER, B.; WESTMORELAND, M. *Quantum Processes Systems, and Information*. New York, NY, USA: Cambridge University Press, 2010. ISBN 052187534X, 9780521875349.
- [15] NIELSEN, M.; CHUANG, I. *Quantum Computation and Quantum Information*. [S.l.]: Cambridge University Press, 2010. (Cambridge Series on Information and the Natural Sciences). ISBN 978-1-107-00217-3.
- [16] SUSSKIND, L.; FRIEDMAN, A. *Quantum Mechanics: The Theoretical Minimum*. Basic Books, 2014. (Theoretical Minimum, The). ISBN 9780465036677. Disponível em: <http://books.google.com.br/books?id=_b7WAgAAQBAJ>.
- [17] MESSIAH, A. *Quantum Mechanics*. Amsterdam, Netherlands: North-Holland Pub. Company, 1967. ISBN 0486409244.
- [18] MERMIN, N. D. *Quantum Computer Science*. New York, USA: Cambridge University Press, 2007. ISBN 978-0-521-87658-2. Disponível em: <<http://www.cambridge.org/9780521876582>>.
- [19] DAWAR, A. *Quantum Computing Course Notes*. Cambridge, UK: [s.n.], 2014. Disponível em: <<http://www.cl.cam.ac.uk/teaching/1415/QuantComp/notes.pdf>>.
- [20] TOFFOLI, T. Reversible computing. In: *Proceedings of the 7th Colloquium on Automata, Languages and Programming*. London, UK, UK: Springer-Verlag, 1980. p. 632–644. ISBN 3-540-10003-2.
- [21] VOS, A. D.; BEULE, J. D.; STORME, L. Computing with the square root of not. *SERDICA JOURNAL OF COMPUTING*, v. 3, n. 4, p. 359–370, 2009. ISSN 1312-6555.
- [22] Misra, B.; Sudarshan, E. C. G. The Zeno’s paradox in quantum theory. *Journal of Mathematical Physics*, v. 18, p. 756–763, abr. 1977. Disponível em: <<http://adsabs.harvard.edu/abs/1977JMP...18..756M>>.
- [23] SHANNON, C. A mathematical theory of communication. *Bell System Technical Journal*, v. 27, p. 379–423, 623–656, July, October 1948. Disponível em: <<http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf>>.

- [24] INGARDEN, R. S. Quantum information theory. *Reports on Mathematical Physics*, v. 10, n. 1, p. 43 – 72, 1976. ISSN 0034-4877. Disponível em: <<http://www.sciencedirect.com/science/article/pii/0034487776900057>>.
- [25] FEYNMAN, R. There is plenty of room at the bottom. *Caltech Engineering and Science*, v. 23, n. 5, p. 22 – 36, 1960. Disponível em: <<http://calteches.library.caltech.edu/47/2/1960Bottom.pdf>>.
- [26] FEYNMAN, R. P. Simulating physics with computers. *International journal of theoretical physics*, Springer, v. 21, n. 6, p. 467–488, 1982.
- [27] BENIOFF, P. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, Kluwer Academic Publishers-Plenum Publishers, v. 29, n. 3, p. 515–546, 1982. ISSN 0022-4715. Disponível em: <<http://dx.doi.org/10.1007/BF01342185>>.
- [28] ALBERT, D. Z. On quantum-mechanical automata. *Physics Letters A*, v. 98, n. 5–6, p. 249 – 252, 1983. ISSN 0375-9601. Disponível em: <<http://www.sciencedirect.com/science/article/pii/0375960183908630>>.
- [29] GAY, S. J. Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science*, v. 16, n. 4, 2006. Disponível em: <<http://www.dcs.gla.ac.uk/~simon/publications/QPLsurvey.pdf>>.
- [30] BLOCH, F. Nuclear induction. *Phys. Rev.*, v. 70, p. 460–474, 1946.
-

5 Anotações (Anexo)

5.1 A esfera de Bloch

A esfera de Bloch [30] é usada para representar as bases do espaço \mathbb{C}^2 correspondentes em uma esfera do \mathbb{R}^3 . Nesta esfera, um ponto com coordenadas esféricas (θ, ϕ) , onde:

$$r(\theta, \phi) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi} \sin\left(\frac{\theta}{2}\right) \end{pmatrix}$$

representa as bases computacionais formadas pelos vetores $|0\rangle$ e $|1\rangle$ e seus argumentos angulares.

Na figura 7 os pontos principais que representam as bases canônicas ortogonais para o bit quântico estão descritos na tabela 1.

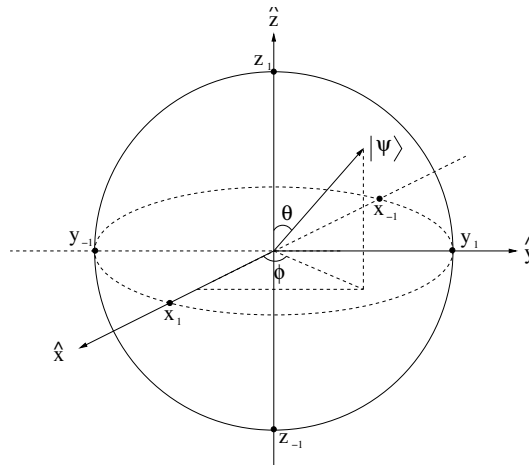


Figura 7: As bases canônicas na esfera de Bloch

De acordo com a tabela 1, as bases canônicas em cada eixo podem ser escritas como:

1. Bases do eixo z:

$$(|0_z\rangle, |1_z\rangle) = (|0\rangle, |1\rangle)$$

portanto:

$$(|0\rangle, |1\rangle)$$

forma as bases:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ e } \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

2. Bases do eixo x:

	Coord. 3D	Coord. esf.	Coord. \mathbb{C}^2
x_1	$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \pi/2 \\ 0 \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
x_{-1}	$\begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \pi/2 \\ \pi \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
y_1	$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \pi/2 \\ \pi/2 \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$
y_{-1}	$\begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} -\pi/2 \\ \pi/2 \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$
z_1	$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
z_{-1}	$\begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ \pi \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Tabela 1: Representações das bases canônicas da esfera de Bloch e suas correspondências em coordenadas cartesianas e esféricas.

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

portanto:

$$\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right), \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

forma as bases:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ e } \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

3. Bases do eixo y:

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

portanto:

$$\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ i \end{pmatrix} \right), \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ i \end{pmatrix} \right)$$

forma as bases:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \text{ e } \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

5.2 Operador Hamiltoniano

O operador Hamiltoniano é um tipo especial de operador hermitiano no espaço de Hilbert, aplicado ao princípio de Heisenberg. Muito “H” não é mesmo? Mas usaremos o mesmo operador $\hat{\mathbf{H}}$ (em negrito) para representá-lo, uma vez que é um operador hermitiano.

Podemos relacionar este operador à conservação da energia de um sistema e descrevê-lo como um operador resultante da soma de dois outros operadores:

$$\hat{\mathbf{H}} = \hat{E}_c + \hat{E}_p \quad (7)$$

onde \hat{E}_c é o operador de energia cinética e \hat{E}_p é o operador de energia potencial do sistema.

A energia potencial do sistema pode ser descrita como sendo:

$$E_p = \int_{t_1}^{t_2} F dt \quad (8)$$

Em termos de trajetória no plano cartesiano, podemos escrever que:

$$E_p = \int \nabla \varphi dx$$

onde,

$$\nabla \varphi = \left(\frac{\partial \varphi}{\partial x}, \frac{\partial \varphi}{\partial y}, \frac{\partial \varphi}{\partial z} \right)$$

Podemos, então, escrever:

$$\begin{aligned} \int \nabla \varphi(r) dr &= \int_a^b \nabla \varphi(r(t)) \cdot r'(t) dt \\ &= \int_a^b \frac{d}{dt} \varphi(r(t)) dt \\ &= \varphi(r(b)) - \varphi(r(a)) \\ &= \varphi(x_B) - \varphi(x_A) \end{aligned}$$

assim, se $v = dr/dt$ a equação 8 pode ser escrita como um operador de energia potencial:

$$\int_a^b F \cdot r dt = \hat{W}(r, t) \quad (9)$$

Nossa equação 7 pode, então ser escrita como:

$$\hat{\mathbf{H}} = \hat{E}_c + \hat{W}(r, t)$$

O operador de energia cinética (\hat{E}_c) pode ser descrito em termos da energia cinética:

$$E_c = \frac{1}{2}mv^2$$

ou em termos de momento $\rho(x, y, z)$ no plano cartesiano:

$$E_c = \frac{\rho^2}{2m}$$

onde m é a massa.

O operador \hat{E}_c pode, então, ser escrito como:

$$\hat{E}_c = \frac{\hat{\rho}\hat{\rho}}{2m} = -\frac{\hbar^2}{2m}\nabla^2$$

onde \hbar é a constante de Plank $h/2\pi$ e ∇^2 é o operador laplaciano (operador diferencial de segunda ordem):

$$\nabla^2 u = \frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2}$$

Nossa equação 7 pode então ser escrita como:

$$\hat{\mathbf{H}} = -\frac{\hbar^2}{2m}\nabla^2 + \hat{W}(r, t) \quad (10)$$

O operador hamiltoniano aplicado a um sistema gera os autovetores de $\hat{\mathbf{H}}$, ou seja:

$$\hat{\mathbf{H}}|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

Como o operador hamiltoniano é implementado como um operador hermitiano no espaço de Hilbert, os autovetores $|v\rangle$ de $\hat{\mathbf{H}}$ formam uma base ortonormal deste espaço:

$$\hat{\mathbf{H}}|v\rangle = E_v|v\rangle$$

Assim, os níveis de espectro de energia do sistema são dados pelos autovalores E_v e, uma vez que o hamiltoniano $\hat{\mathbf{H}}$ é um operador hermitiano, os valores de energia serão sempre representados por números reais.

5.3 Matrizes de Pauli

As matrizes de Pauli são matrizes complexas 2×2 hermitianas e unitárias. Elas são, em geral representadas pela letra grega $\sigma(\sigma_x, \sigma_y, \sigma_z)$ e formam o operador hamiltoniano que descreve o spin de uma partícula em um campo eletromagnético:

$$-i\hbar\frac{\partial}{\partial t}|\psi\rangle = \underbrace{\left[\frac{1}{2m}(\sigma \cdot (p - qA))^2 + q\phi \right]}_{\hat{\mathbf{H}}}|\psi\rangle$$

As matrizes de Pauli são:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Seus quadrados são iguais entre si, iguais à identidade e o produto delas por $-i$ também resulta na matriz identidade:

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = -i\sigma_x\sigma_y\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Como podemos encontrar os autovalores das matrizes de Pauli? Suponha uma matriz M qualquer, que possa satisfazer a equação

$$\alpha M^2 + \beta M + \gamma \mathbf{1} = 0$$

onde $\mathbf{1}$ é uma matriz unitária com as mesmas dimensões de M .

Assim, o autovalor λ de M sobre um vetor $|v\rangle$ é:

$$M|v\rangle = \lambda|v\rangle$$

e, portanto:

$$(\alpha M^2 + \beta M + \gamma \mathbf{1})|v\rangle = 0$$

se $M|v\rangle = \lambda|v\rangle$ e $M^2|v\rangle = \lambda^2|v\rangle$ logo,

$$(\alpha\lambda^2 + \beta\lambda + \gamma)|v\rangle = 0$$

Oras, o autovetor $|v\rangle$ não pode ser zero porque não faz sentido associar um autovetor zero a um autovalor que teria que ser zero, então, um autovetor não pode ser zero. Logo, podemos escrever que:

$$\alpha\lambda^2 + \beta\lambda + \gamma = 0$$

Assim, da mesma forma, se uma matriz de Pauli, $\sigma_n^2 = 1$ então $(\lambda_n)^2 = 1$ e $\lambda = \pm 1$.

A soma dos elementos da diagonal de uma matriz quadrada é chamado de **traço** de uma matriz e é denotado por $\text{tr } A$ se A for uma matriz quadrada.

$$\text{tr } A = \sum_i a_{i,i}$$

e o traço de uma matriz corresponde à soma de seus autovalores. No caso das matrizes de Pauli, $\text{tr } \sigma_n = 0$ e, portanto, os dois autovalores das matrizes de Pauli são 1 e -1 e seus autovetores:

$$|\psi\rangle = \begin{pmatrix} \psi^+ \\ \psi^- \end{pmatrix}$$

sendo que:

$$\begin{aligned}\psi_x^+ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & \psi_x^- &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\ \psi_y^+ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, & \psi_y^- &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \\ \psi_z^+ &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & \psi_z^- &= \begin{pmatrix} 0 \\ -1 \end{pmatrix}\end{aligned}$$

5.4 Portas quânticas e símbolos

As portas lógicas da computação quântica não são tão triviais como as da computação clássica porque envolvem estados quânticos dos bits e não apenas o valor observado de um bit individual. Nesta anotação vamos representar os principais operadores lógicos quânticos e suas matrizes unitárias equivalentes. As matrizes unitárias dos operadores são representadas em cada coluna, da esquerda para a direita e de cima para baixo, como $|00\dots 0\rangle, |00\dots 1\rangle$ até $|11\dots 1\rangle$.

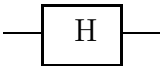
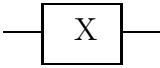
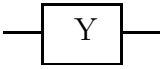
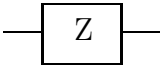
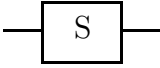
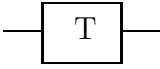
Hadamard		$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli-X		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y		$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z		$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Fase		$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\pi/8$		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Tabela 2: Portas lógicas de um qubit (fonte: Nielsen [15])

Note que $e^{i\pi/4} = \sqrt{i}$. Assim a porta S equivale à \sqrt{Z} e a porta $\pi/8$ equivale à \sqrt{S} . A partir destas pode-se conseguir outras portas quânticas lógicas, principalmente as portas controladas onde o primeiro estado serve como controle (veja tabela 3).

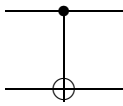
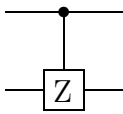
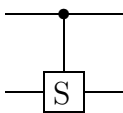
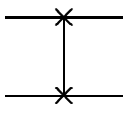
controled-NOT		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
controled-Z		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
controled-Phase		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$
Swap		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Tabela 3: Portas lógicas 2-qubit (fonte: Nielsen [15])

5.5 Operações com portas quânticas

Abaixo vamos detalhar alguns exemplos de operações com portas (*gates*) quânticas e mostrar que a implementação física de portas quânticas está vinculada à reversibilidade das operações, ou seja, têm que ser operações lineares unitárias.

Primeiramente temos que considerar a implementação física do qubit que representa o estado $|0\rangle$ e o estado $|1\rangle$. Claro que existem diversos materiais que podem ser usados para implementar o qubit, dentre eles a polarização de fótons, spins eletrônicos, estados moleculares à baixa temperaturas, interações com super-condutores etc. mas aqui, vamos considerar que temos o qubit $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e o qubit $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ e que podemos medir o resultado de uma operação. A implementação física é um problema de engenharia da computação.

O exemplo mais simples e fácil de se compreender a manipulação algébrica das portas lógicas quânticas, usando a álgebra linear, é a aplicação de um operador de identidade. Um circuito quântico que representa a identidade nada mas faz do que retornar, como saída a própria entrada. Este operador tem importância conceitual e pode ter aplicabilidade em algoritmos comparativos.

1. Operador identidade:

$$I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

e, portanto:

$$\hat{I}|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+0 \\ 0+0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

e, também:

$$\hat{I}|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0+0 \\ 0+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

que é, obviamente, inversível.

2. A porta NOT ou Pauli-X

$$N \equiv X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

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

3. A porta de Hadamard

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

$$\begin{aligned}\hat{H}|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+0 \\ 1+0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\end{aligned}$$

$$\begin{aligned}\hat{H}|1\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0+1 \\ 0-1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\end{aligned}$$

Note que, com relação à inversibilidade da porta de Hadamard, ela não é tão evidente, mas podemos demonstrar. Considere,

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+0 \\ 1+0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

então, para demonstrar que $\hat{H}(\hat{H}|0\rangle) = |0\rangle$ podemos escrever:

$$\hat{H}(\hat{H}|0\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+1 \\ 1-1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Tente demonstrar o mesmo para o qubit $|1\rangle$, ou seja que $\hat{H}(\hat{H}|1\rangle) = |1\rangle$.