Technical Report

Alguns bits de qubits:
Uma introdução sobre bits quânticos.

João Cândido Lima Dovicchi[1]

Florianópolis – SC
2015

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

1 Introdução

O grande problema da computação determinística é que estamos presos em um "beco sem saída". A chamada "lei de Moore" está se concretizando, já que estamos chegando ao nível atômico dos semicondutores e, mais recentemente de supercondutores [1]. A computação clássica, determinística e baseada em máquinas de estado está com seus dias contados. O mais curioso é que a máquina de estado foi implementada de forma determinística por von Neumann e ele foi o primeiro a reconhecer a importância dos espaços vetoriais de Hilbert e propor bases para a mecânica quântica [2].

As bases da mecânica clássica foram violentamente abaladas quando foi descoberto que no nível atômico, as partículas não se comportavam como era esperado e a teoria criada para explicar os estados delas hoje é conhecida como teoria quântica. Era de se esperar que os computadores, ao atingir o nível atômico dos "transistores" formados por supercondutores em condições especiais, operando em camadas atômicas e em condições de baixa temperatura também poderiam operar de acordo com a teoria quântica. E é o que acontece, na verdade [3].

Este *Technical Report* pertence a uma série de TRs que podem facilitar a compreensão da computação quântica e mostrar que, talvez, a saída para escapar da computação determinística está próxima. Em outro artigo de interesse, são explorados os elementos principais da álgebra linear necessária para a compreensão de operadores lineares usados na mecânica quântica [4].

Os estados quânticos apresentam certas complexidades — quando se trada de "emaranhamento" (*entanglement*) de "superposição" dos estados (*superposition*) — mas a computação quântica pode modelar o mundo físico com muito mais precisão e realidade. Mesmo os cálculos da física e da engenharia poderiam ser menos grosseiros como fruto das aproximações e arredondamentos dos zeros e uns do computador clássico 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 conceitos algébricos e como estes são utilizados no arcabouço matemático da mecânica quântica. Para uma revisão da álgebra veja o relatório técnico já citado [4].

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 [5, 6] em 1995 para se referir ao bit quântico.

O estado computacional quântico — que vamos chamar de $|\psi\rangle$ — é um

vetor[2] que representa uma superposição de dois estados $|0\rangle$ e $|1\rangle$ que é uma combinação linear tal que:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Um bit quântico pode, então, 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" representados aqui 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 [8], que podem ser expressas no $\mathbf{L}^2$ como:

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

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.

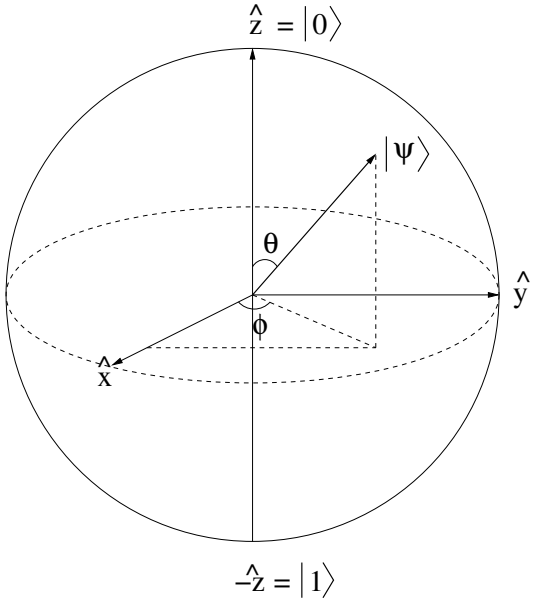


Figura 1: Representação do qubit na esfera de Bloch

[2]A notação vetorial usada neste documento é a notação de Dirac [7].

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).

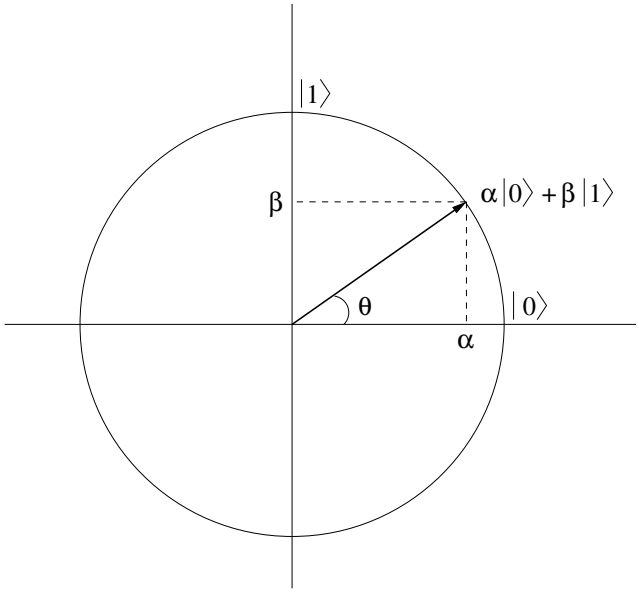


Figura 2: Representação do qubit no plano bidimensional

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 iformação 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" [9].

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".

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 fótom 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.

A 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):

$$\hat{\mathbf{H}}|\psi\rangle = i\hbar \frac{\mathrm{d}}{\mathrm{d}t}|\psi\rangle \tag{1}$$

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

Podemos dizer que 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.

$$|\psi'\rangle = \hat{U}|\psi\rangle \tag{2}$$

onde,

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

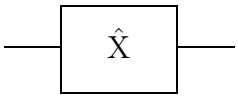
Note $\hat{U}(t_1, t_2)$ é relativo à conservação da energia de um sistema quântico. Ainda, se o operador hamiltoniano $\hat{\mathbf{H}}$ é hermitiano e $\hat{U}$ é um operador unitário, então a equação 2 implica em:

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

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 mutualmente 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 base.

A porta:



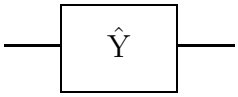
pode ser descrita pelo operador $\hat{X}$, tal que:

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

onde,

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

A porta:



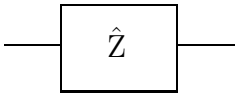
pode ser descrita pelo operador $\hat{Y}$, tal que:

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

onde,

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

A porta:



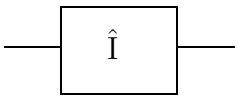
pode ser descrita pelo operador $\hat{Y}$, tal que:

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

onde,

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

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



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

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

onde,

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

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,

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

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 global[3](veja capítulo VII:I do livro de Albert Messiah) [10]. 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 $\hat{P}_m$,

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

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

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

então,

[3]Chamamos 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.

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

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:

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

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

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

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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 componentes[4]:

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

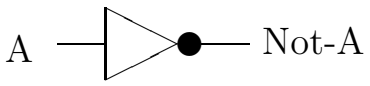
[4]Separação não implica em separabilidade. Duas partículas podem estar fisicamente separadas mas continuam ligadas (*entangled)*

2 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 [11] define:

> "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."

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.



A	Not-A
0	1
1	0

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` quântica[5] 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.

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

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

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

[5]Aqui 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^o, seguida pela rotaçao no eixo $\hat{x}$ de 180^o.

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 $\{x, y\}$ inverta 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:

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

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 [8], Mermin [11]). 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).

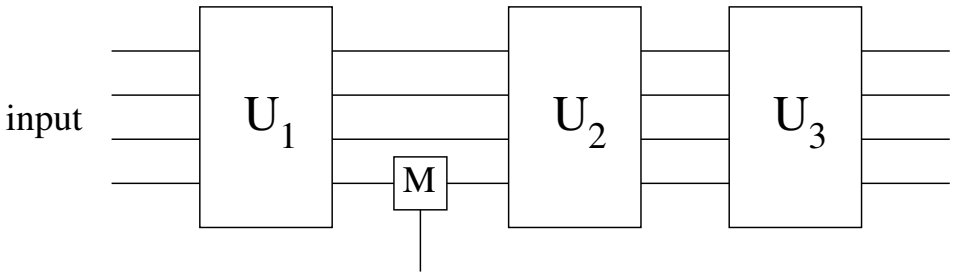


Figura 4: Exemplo abstrato de um circuito quântico. Cada operador $\hat{U}_i$ é descrito por uma matriz $2^n \times 2^n$ (Modificado de Dawar [12])

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

2.1 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 $\hat{C}_{NOT}\,|\psi'\rangle = |\psi\rangle$.

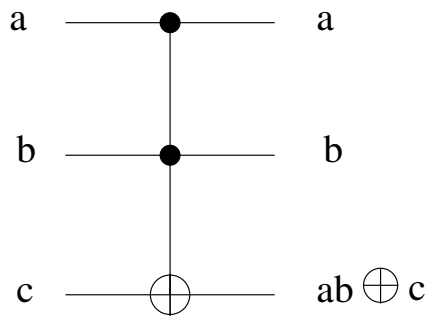


Figura 5: Esquema de um circuito lógico quântico Toffoli (fonte: Nielsen [8])

O mesmo acontece com a porta de Toffoli [13] que também pode ser usada em computação quântica. seja, por exemplo:

$$|\psi\rangle = \alpha_0|000\rangle + ... + \alpha_7|110\rangle\,\alpha_8|111\rangle \tag{3}$$

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 3 resulta em:

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

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 $\sqrt{\texttt{NOT}}$ ou SRN (*square root not*) [14]. Este operador, quando aplicado a um quantum bit gera a superposição (randomizando o qubit) e, no entanto a aplicação combinada de duas portas $\sqrt{\texttt{NOT}}$ 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 `NOT`[6]. 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 qbits:

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

Podemos considerar então que, com base nestas propriedades das portas quânticas e o "paradoxo de Zeno" [15], todo sistema lógico clássico pode ser simulado em um computador quântico.

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

Referências

[1] WIKIPEDIA. *Atomic layer deposition — Wikipedia, The Free Encyclopedia*. 2015. [Online; accessed 3-March-2015]. Disponível em: <http://en.wikipedia.org/w/index.php?title=Atomic_layer_deposition&oldid=648966699>.

[2] 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).

[3] EKINO, T. et al. d-wave superconductivity and s-wave charge density waves: Coexistence between order parameters of different origin and symmetry. *Symmetry*, v. 3, n. 4, p. 699–749, 2011. ISSN 2073-8994. Disponível em: <http://www.mdpi.com/2073-8994/3/4/699>.

[4] 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>.

[5] 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>.

[6] SCHUMACHER, B.; WESTMORELAND, M. *Quantum Processes Systems, and Information*. New York, NY, USA: Cambridge University Press, 2010. ISBN 052187534X, 9780521875349.

[7] 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>.

[8] 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.

[9] 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>.

[10] MESSIAH, A. *Quantum Mechanics*. Amsterdam, Netherlands: North-Holland Pub. Company, 1967. ISBN 0486409244.

[11] 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>.

[12] DAWAR, A. *Quantum Computing Course Notes*. Cambridge, UK: [s.n.], 2014. Disponível em: <http://www.cl.cam.ac.uk/teaching/1415/QuantComp/notes.pdf>.

[13] 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.

[14] 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.

[15] 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>.