

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/370325361>

Introdução à Computação Quântica

Article · April 2023

CITATION

1

READS

655

2 authors, including:



[Emilio Silva](#)

FLETRONICS INSTITUTO DE TECNOLOGIA

2 PUBLICATIONS 1 CITATION

SEE PROFILE

Introdução à Computação Quântica

Eng. Emilio Luciano de Miranda e Silva
Flextronics Instituto de Tecnologia

30 de abril de 2022

Resumo

Quantum computing is developing in areas where classical computing does not offer adequate performance: molecular simulation for the development of new materials or chemical compounds, climate prediction, cryptography, machine learning, among others. This article presents the fundamentals of the qubit, its notation and mathematical characterization. The Bloch sphere is presented, as well as its usefulness in the study of qubit behavior. Quantum computing itself – or the behavior of the qubit when acted upon by a quantum gate – is described in a separate section. The quantum measurement and its consequences are also described, as well as the special quantum states: superposition and entanglement. A basic architecture of a quantum computer is shown. IBM's program development platform, Qiskit, and its basic manipulation are presented.

*

A computação quântica está se desenvolvendo em áreas as quais a computação clássica não oferece performance adequada: simulação de moléculas para desenvolvimento de novos materiais ou compostos químicos, previsão do clima, criptografia, aprendizado de máquina entre outros. Este artigo apresenta os fundamentos do qubit, sua notação e caracterização matemática. A esfera de Bloch é apresentada, bem como sua utilidade no estudo do comportamento do qubit. A computação quântica em si – ou o comportamento do qubit quando sob ação de uma porta quântica – é descrita em uma seção à parte. A medida quântica e suas consequências também são descritas, bem como os estados quânticos especiais: superposição e emaranhamento. Uma arquitetura básica de um computador quântico é mostrada. A plataforma de desenvolvimento de programas da IBM, o Qiskit, e sua manipulação básica são apresentadas.

Palavras-chaves: qubit, computação quântica, qiskit, estados quânticos, portas quânticas, circuitos quânticos, notação dirac, medida quântica, artigo técnico.

Introdução

A mecânica quântica, disciplina da física introduzida por Max Plank em 1900, pode ser intimidadora. Porém, não se está sozinho nessa perplexidade. O modo como parte do mundo natural funciona, o mundo em que vivemos fisicamente, não nos parece lógico se o olharmos pela lente da mecânica quântica. Isso decorre, em parte, por causa da limitação de nossos sentidos que nos leva a crer que o mundo que nos cerca é aquele que sentimos. Mas, não é assim. A natureza pode ser para nós bem incompreensível quando a observamos com mais cuidado. O mundo natural pode ser assustador, e ao mesmo tempo instigante quando visto pela lente da mecânica quântica. Nesse sentido, a natureza, através da computação quântica, nos fornece um conjunto de regras que podem ser utilizadas em algoritmos que resolvem problemas difíceis de serem solucionados pelas regras da álgebra booleana da computação clássica, tais como simulação molecular para criação de novos compostos químicos ou materiais, previsão do clima mais acurada entre outros. É disto que trata a computação quântica: um conjunto de regras de funcionamento retiradas da mecânica quântica, o qual é transformado, através da matemática, em portas quânticas que modelam o qubit, que é o bit quântico, e possibilitam a criação de algoritmos que resolvem problemas.

Do Bit ao Qubit

Iniciaremos a nossa jornada dando uma olhada no bit da álgebra booleana. Apesar de ser uma abstração matemática, o bit existe na natureza em forma de claro-escuro, presente-ausente, etc. De maneira arbitrária, podemos representar o bit como dois vetores defasados em 180° .

$$0 \longleftarrow o \longrightarrow 1$$

Figura 1 – Representação geométrica do *bit*

Observa-se que, nessa representação arbitrária e geométrica, os valores do bit recaem sobre uma linha. O bit então pode ser representado geometricamente através de um plano unidimensional com dois valores excludentes entre si: 1 ou 0. Já o qubit, que é o bit da computação quântica, pode ser representado por um ponto em uma superfície de uma esfera.

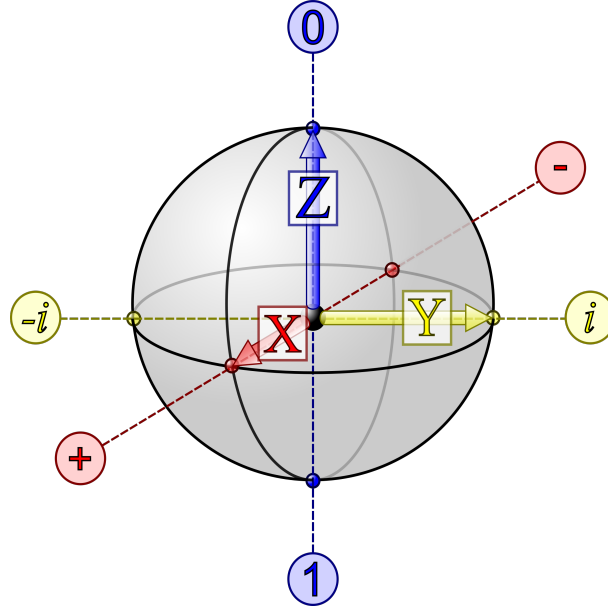


Figura 2 – Bit booleano na esfera de Bloch - (GCROSS, 2022).

De maneira diferente do bit, o qubit pode ser representado por infinitos valores que correspondem aos infinitos pontos sobre a superfície dessa esfera. O qubit também possui valores 0 e 1, que ficam nos extremos superior e inferior da esfera, e que podem ser associados ao bit lógico – de fato, os dois valores do bit booleano integram o conjunto de infinitos valores na superfície da esfera. Por inspeção, podemos ver na esfera uma característica fundamental do qubit: ele pode assumir simultaneamente valores entre 0 e 1 – quando o vetor estiver no plano médio desta (QUANTUM, 2022b). Esse estado especial do qubit denomina-se superposição que o distingue do bit e faz parte das características quânticas de partículas atômicas. É essa característica de superposição que diferencia, primariamente, o qubit do bit.

A Notação de Dirac

A notação de Dirac, físico inglês do séc. XX, é utilizada para a manipulação dos estados quânticos. Um vetor de duas dimensões pode ser representado, na álgebra linear, através de uma letra em negrito ou de uma letra com uma flecha em cima (FARIAS, 2020).

$$\vec{v} = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} \quad (1)$$

Dirac propôs que a notação do vetor fosse modificada desta maneira.

$$|v\rangle = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} \quad (2)$$

A notação pode ser expandida para vetores multidimensionais, bastando adicionar linhas ao vetor da equação (2), mas para o escopo deste artigo um vetor de duas dimensões é o suficiente. Essa notação vetorial pode ser estendida para caracterizar o dual do vetor $|v\rangle$, ou seu conjugado complexo.

$$\langle v| = \begin{bmatrix} a_{11}^* & a_{21}^* \end{bmatrix} \quad (3)$$

O produto escalar entre dois vetores bidimensionais (produto vetorial cujo resultado é um número) pode ser escrito da seguinte forma na notação de Dirac.

$$|v\rangle = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix}, \quad |w\rangle = \begin{bmatrix} b_{11} \\ b_{21} \end{bmatrix} \quad (4)$$

$$\langle v|w\rangle = \sum_{i=1}^n a_i^* b_i \quad (5)$$

$$\langle v|w\rangle = a_{11}^* b_{11} + a_{11}^* b_{21} + a_{21}^* b_{11} + a_{21}^* b_{21} \quad (6)$$

Também se pode caracterizar a multiplicação matricial na notação de Dirac da maneira a seguir.

$$|v\rangle\langle w| = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} \cdot \begin{bmatrix} b_{11}^* & b_{21}^* \end{bmatrix} \quad (7)$$

$$|v\rangle\langle w| = \begin{bmatrix} a_{11}b_{11}^* & a_{11}b_{21}^* \\ a_{21}b_{11}^* & a_{21}b_{21}^* \end{bmatrix} \quad (8)$$

Adicionalmente, a notação de Dirac fornece, de maneira simples e extensível, a caracterização associada de dois ou mais vetores. A representação de dois qubits, por exemplo, pode ser feita da seguinte forma (QUANTUM, 2022b).

$$\langle vv| = a_{00} + a_{01} + a_{10} + a_{11} = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} \quad (9)$$

Se tomarmos dois qubits diferentes $|a\rangle$ e $|b\rangle$, eles podem ser representados pelo produto tensorial ou Kronecker (QUANTUM, 2022b).

$$a = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}, \quad b = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \quad (10)$$

$$|ba\rangle = |b\rangle \otimes |a\rangle = \begin{bmatrix} b_0 \otimes \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \\ b_1 \otimes \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} b_0a_0 \\ b_0a_1 \\ b_1a_0 \\ b_1a_1 \end{bmatrix} \quad (11)$$

Denomina-se *ket* o vetor $|v\rangle$ e *bra* o seu conjugado complexo $\langle v|$. O termo *bra-ket* é dado ao produto escalar $\langle v|v\rangle$.

Estado Quântico

O estado quântico do qubit pode ser caracterizado, de maneira particular, através de um vetor de dimensão n . Se se quer representar, por exemplo, o dia de terça-feira como o dia em que este artigo começou a ser escrito, um dado vetor $|s\rangle$ com $n = 5$ poderia ser assim caracterizado.

$$|s\rangle = \begin{bmatrix} seg \\ ter < - \\ qua \\ qui \\ sex \end{bmatrix} \quad (12)$$

$$|s\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (13)$$

É possível afirmar então, que este tipo de caracterização pode ser interpretado como uma probabilidade, dado que a marcação 1 em (13) indica a probabilidade de 100% do artigo ter se iniciado na terça-feira – o que, evidentemente, exclui os outros dias. Este tipo de marcação de estado quântico para o qubit embute algumas vantagens evidentes. Uma delas é que o qubit pode ser representado através da notação de Dirac para possibilitar o cálculo da atuação das portas quânticas no qubit através da álgebra linear. Uma outra é que se pode normalizar o vetor de representação para ter o seu comprimento igual a 1, o que possibilita a utilização desse vetor para o cálculo de probabilidade - que é o resultado da computação quântica para um qubit.

Caracterização do QUBIT

A notação do qubit usa probabilidade em sua caracterização. Esta é uma ideia chave que é preciso ter em mente. Outra ideia chave é: o qubit tem dois tipos de existência, antes e depois de uma leitura. Antes de uma leitura o estado quântico do qubit é tipo uma nuvem em torno da superfície de uma esfera, como descrito na seção anterior. Ele está simultaneamente em lugares específicos escolhidos ao acaso. Depois da leitura, o qubit assume um valor fixo que pode ser lido. E, finalmente, o resultado de uma leitura do qubit é firme, ou seja, para um dado instante da leitura o valor do vetor de estado lido é consistente com o estado físico do qubit naquele instante. Esta característica é importante tanto para entender o qubit, como, para entender o resultado de uma computação quântica.

O qubit possui dois estados básicos e eles são derivados dos estados do bit booleano. Tomemos o bit booleano 0 inicialmente.

$$0 \longleftarrow o$$

O qubit q no estado quântico 0 é caracterizado pelo seguinte vetor na notação de Dirac.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (14)$$

Assim se segue que o mesmo qubit q no estado quântico 1 tem este vetor na notação de Dirac.

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (15)$$

O que fizemos foi deduzir, a partir dos bits booleanos 0 e 1, dois vetores $|0\rangle$ e $|1\rangle$, respectivamente, que representam agora dois estados quânticos ([QUANTUM, 2022b](#)).

A notação dos estados quânticos para $|0\rangle$ e $|1\rangle$ é arbitrária. Não se deve procurar entender por que o estado quântico $|0\rangle$ está com o 1 marcado na primeira linha do vetor. Ao se deparar com o estado quântico $|0\rangle$ devemos fazer a seguinte interpretação: a probabilidade de o qubit estar no estado $|0\rangle$ é 100% – isso parece óbvio, mas a ênfase é na adoção extensiva da probabilidade na caracterização do qubit.

O qubit, por suposto, assume mais valores que esses dois estados. De fato, qualquer estado do qubit pode ser caracterizado pelo seguinte vetor ([BARDIN DANIEL SANK; JEFFREY, August 2020](#)).

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad \therefore |\alpha|^2 + |\beta|^2 = 1 \rightarrow \alpha, \beta \in \mathbb{C} \quad (16)$$

A análise da equação 14 mostra que o estado quântico de um qubit ψ pode ser representado por um vetor com duas probabilidades α e β e que essas probabilidades pertencem ao conjunto dos números complexos. Ela nos mostra também que a soma dos módulos das duas probabilidades α e β tem de ser obrigatoriamente 1. Então, se nos depararmos com um resultado de uma computação do qubit, por exemplo, no ambiente QISKIT da IBM, de 70% de chance de ψ ser 1, o resultado aparecia assim.

$$|\psi\rangle = \begin{bmatrix} 0 + 0j \\ 0.7 + 0j \end{bmatrix} \quad (17)$$

Uma outra forma de se escrever a equação de estado do qubit, e por isso é importante conhecê-la, é a que segue ([POLACK, 2011](#)).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (18)$$

A representação do estado quântico do qubit, através de uma equação de soma ou um vetor bidimensional cujo os módulos de seus elementos têm soma 1, pode parecer simples. Mas não se deixe enganar pela simplicidade. Pois ela embute uma sofisticação que suporta o comportamento imprevisível do qubit antes de uma medida, bem como o resultado firme após essa. A computação quântica é complexa por natureza logo em seu elemento mais básico, o qubit. No entanto, a álgebra linear vem em nosso auxílio nesse primeiro contato.

O qubit deve ser caracterizado então, como um vetor no espaço tridimensional com comprimento 1 e centrado no ponto de origem dos três eixos $[x; y; z]$. O qubit tem natureza instável com relação à sua posição. Ele pode estar simultaneamente em todas as posições ao redor de seu ponto central. No entanto, o seu estado pode ser definido como probabilidade de $p < 0$ e $p > 1$ depois de uma leitura. Esse comportamento do qubit, de se estabilizar depois de uma leitura, possibilita a computação através das suas características quânticas.¹

Características Matemáticas dos Vetores de Estados Quânticos

Os vetores $|0\rangle$ e $|1\rangle$ podem ser somados com outros vetores ou entre si (QUANTUM, 2022b).

$$|\psi\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}, \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (19)$$

$$|\psi\rangle + |0\rangle = \begin{bmatrix} a_0 + 1 \\ a_1 + 0 \end{bmatrix} \quad (20)$$

Os vetores $|0\rangle$ e $|1\rangle$ podem ser multiplicados por um número escalar.

$$x|0\rangle = \begin{bmatrix} x \cdot 1 \\ x \cdot 0 \end{bmatrix} \quad (21)$$

Os dois vetores são ortogonais² porque a multiplicação entre eles dá como resultado zero.

$$|0\rangle \cdot |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1 \cdot 0 + 0 \cdot 1 \quad (22)$$

Os vetores $|0\rangle$ e $|1\rangle$ são normalizados, o que significa que o seus respectivos comprimentos, ou suas normas ou módulos, são iguais a 1. Os módulos dos vetores $|0\rangle$ e $|1\rangle$ são assim calculados.

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

$$\|0\rangle\| = \sqrt{1^2 + 0^2} \quad (24)$$

$$\|0\rangle\| = 1 \quad (25)$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (26)$$

$$\|1\rangle\| = \sqrt{0^2 + 1^2} \quad (27)$$

$$\|1\rangle\| = 1 \quad (28)$$

¹ Nesse ponto, é recomendável se fazer uma revisão da álgebra linear. Uma boa referência para esse tópico é <<https://www.mat.ufmg.br/ead/wp-content/uploads/2016/08/Introducao-a-Algebra-Linear.pdf>>.

² O ângulo entre eles é 90°.

Eles também são linearmente independentes entre si, ou seja, eles não podem ser descritos matematicamente em função um do outro.

Dado que os vetores $|0\rangle$ e $|1\rangle$ atendem a estes requisitos básicos de multiplicação escalar, adição vetorial, ortogonalidade, normalidade e independência linear, eles formam uma base. Desta maneira, eles podem descrever qualquer vetor um um espaço bidimensional (QUANTUM, 2022b).

Esfera de Bloch

A esfera de Bloch é uma representação gráfica em três dimensões do qubit. Ela não deve ser confundida com a representação do estado quântico do qubit que é um vetor de estado bidimensional (QUANTUM, 2022b). A esfera de Bloch utiliza o sistema de coordenadas esféricas $[r; \psi; \theta]$ para o mapeamento em três dimensões.

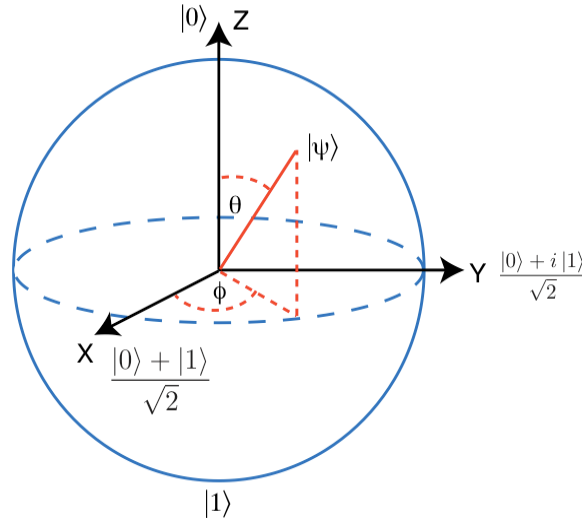


Figura 3 – Esfera de Bloch - (QUANTUM, 2022b)

A transposição do vetor de estado do qubit para coordenadas esféricas é realizada tomando a forma algébrica de um qubit $|q\rangle$ para fazer duas transformações: a primeira transforma α e β em números reais e a segunda adiciona uma fase no qubit $|1\rangle$ (QUANTUM, 2022b). Partindo da fórmula geral do qubit.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha, \beta \in \mathbb{C} \quad (29)$$

Dado que o vetor do qubit é normalizado, como descrito na seção anterior, poderemos utilizar uma identidade trigonométrica para transformar α e β em números reais.

$$r = \sqrt{\alpha^2 + \beta^2} \therefore r = 1 \rightarrow \alpha, \beta \in \mathbb{C} \quad (30)$$

$$r = \sqrt{\cos^2\theta + \sin^2\theta} \therefore r = 1 \rightarrow \theta \in \mathbb{R} \quad (31)$$

$$r = \cos\frac{\theta}{2} + \sin\frac{\theta}{2} \therefore r = 1 \rightarrow \theta \in \mathbb{R} \quad (32)$$

Podemos reescrever a equação (29) em função do ângulo θ que é um número real e faz o qubit girar em torno do eixo Z.

$$\psi = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \rightarrow \theta \in \mathbb{R} \quad (33)$$

Finalmente, adicionamos um ângulo ϕ utilizando a fórmula de Euler $e^{ix} = \cos(x) + i \sin(x)$ para inserir uma rotação no plano xy (WELLSTOOD, 2016).

$$\psi = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \rightarrow \theta, \phi \in \mathbb{R} \quad (34)$$

A utilidade da esfera de Bloch, como já foi dito, é visualizar o comportamento do qubit. Nesse âmbito, ela constitui uma valiosa ferramenta de suporte ao aprendizado³. Mas, ela não se aplica à computação dos qubits que é feita exclusivamente pelas portas quânticas e cujo resultados são expressos pelos vetores de estado quântico na forma $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

O Computador Quântico

O computador quântico é um dispositivo híbrido. A parte de controle e tratamento dos resultados das computações quânticas é realizada por um computador clássico. A outra parte, onde residem os qubits, é quântica e por isso trabalha em temperatura muito fria, em torno do 0° absoluto – 10-20mK°(BRANDL, August 2017).

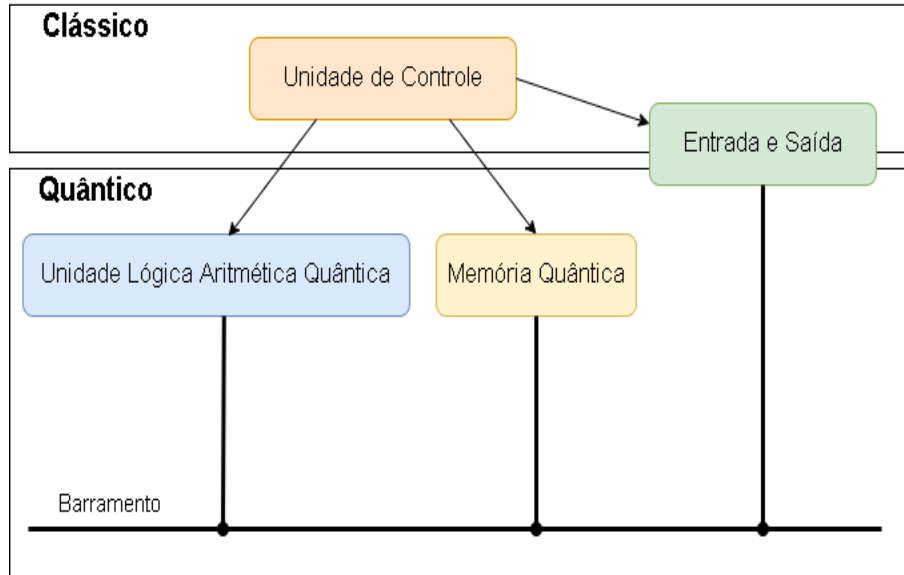


Figura 4 – Computador quântico

A seção clássica do computador quântico controla o estado quântico do qubit, através da rotação do seu vetor de estado. No fim da manipulação do qubit, a seção clássica

³ <https://javafxpert.github.io/grok-bloch/>

o lê e mostra o resultado ao operador. Essa necessidade de uma máquina clássica na arquitetura do computador quântico advém do fato de a seção quântica em si ser muito instável. Por exemplo, o qubit deve operar em temperatura próxima ao zero absoluto de temperatura $-270C^\circ$. Se o congelador perder o controle da faixa de temperatura necessária para a operação do qubit – por exemplo, $10-20mK^\circ$ – o qubit poderá ficar instável e não operar como esperado.

Portas e Estados Quânticos

As portas quânticas são os operadores dos qubits. Elas são representadas por matrizes e operam o qubit através das operações da álgebra linear: produto escalar (produto interno) e multiplicação matricial (produto externo).

Portas Quânticas Simples - Portas de Pauli

As portas de Pauli operam sobre um qubit. Elas são compostas a partir dos produtos externos dos qubits $|0\rangle$ e $|1\rangle$. São matrizes quadradas 2×2 . Adotamos aqui a caracterização de cinco portas de Pauli de acordo com (POLACK, 2011).

A caracterização da porta quântica identidade I é a seguinte.

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| \quad (35)$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad (36)$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (37)$$

A porta Identidade é uma matriz quadrada neutra, pois qualquer matriz M multiplicada por ela, resulta na própria matrix M .

A porta X é caracterizada da seguinte forma.

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| \quad (38)$$

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \end{bmatrix} \quad (39)$$

$$= \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad (40)$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (41)$$

A porta X é uma inversora. Ela inverte o estado de um qbit $|0\rangle$ em $|1\rangle$, e vice-versa. Por exemplo, dado um qubit $\psi = |0\rangle$. Ao aplicarmos nele a porta X , o resultado ψ' será que o qubit irá para o estado $|1\rangle$.

$$|\psi'\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (42)$$

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (43)$$

Veja, a seguir, caracterização da porta quântica Z .

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| \quad (44)$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (45)$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad (46)$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (47)$$

A porta Z muda a fase relativa ϕ – no sistema de coordenadas esféricas – para a esfera de Bloch de um qubit, exceto o qubit $|0\rangle$. Por exemplo, a atuação da porta Z no qubit $\psi = |1\rangle$ é a que segue.

$$|\psi'\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (48)$$

$$= \begin{bmatrix} 0 \\ -1 \end{bmatrix} \quad (49)$$

A porta Y é caracterizada da seguinte forma.

$$Y = -|1\rangle\langle 0| + |0\rangle\langle 1| \quad (50)$$

$$= \begin{bmatrix} 0 \\ -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (51)$$

$$= \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad (52)$$

$$= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad (53)$$

A porta Y é uma combinação da negação da porta X com uma mudança de fase relativa da porta Z (POLACK, 2011). A aplicação da porta Y no qubit $\psi = |0\rangle$ desenvolve o seguinte resultado.

$$|\psi'\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad (54)$$

$$= \begin{bmatrix} 0 \\ -1 \end{bmatrix} \quad (55)$$

Medidas Quânticas no qubit

Se tomarmos um qubit $q\theta$ que sofreu uma operação de uma determinada porta quântica U resultando em um estado quântico ψ , dizemos que a medida de probabilidade do estado $|0\rangle$ em ψ é (QUANTUM, 2022b).

$$\psi = \langle q\theta | U \rangle \quad (56)$$

$$p(|0\rangle) = |\langle 0 | \psi \rangle|^2 \therefore p(|0\rangle) + p(|1\rangle) = 1 \quad (57)$$

Por exemplo, dado um determinado estado ψ do qubit $q\theta$, a medida de probabilidade de obtermos $|0\rangle$ no estado ψ então será.

$$|\psi\rangle = \frac{1}{3\sqrt{2}}|0\rangle + \frac{2i}{3\sqrt{2}}|1\rangle \quad (58)$$

$$\langle 0 | \psi \rangle = \langle 0 | \left(\frac{1}{3\sqrt{2}}|0\rangle + \frac{2i}{3\sqrt{2}}|1\rangle \right) \quad (59)$$

$$= \frac{1}{3\sqrt{2}} \langle 0 | 0 \rangle + \frac{2i}{3\sqrt{2}} \langle 0 | 1 \rangle \quad (60)$$

$$= \frac{1}{3\sqrt{2}} \cdot 1 + \frac{2i}{3\sqrt{2}} \cdot 0 \quad (61)$$

$$= \frac{1}{3\sqrt{2}} \quad (62)$$

$$|\langle 0 | \psi \rangle|^2 = \frac{1}{18} \quad (63)$$

Estado de Superposição

A porta Hadamard implementa o estado de superposição no qubit e em ambas as bases padrões, $|0\rangle$ e $|1\rangle$. O estado de superposição é inerente à mecânica quântica e não existe na álgebra booleana. Quando o qubit entra nesse estado, ele existe simultaneamente entre as bases $|0\rangle$ e $|1\rangle$. A caracterização da porta Hadamard é a seguinte (POLACK, 2011).

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|) \quad (64)$$

$$= \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \end{bmatrix} \right) \quad (65)$$

$$= \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right) \quad (66)$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (67)$$

Geometricamente, o que a função Hadamard da fórmula (55) faz é distribuir ou mapear igualmente $\frac{1}{\sqrt{2}}$ entre todas as combinações das bases $|0\rangle$ e $|1\rangle$. Esse mapeamento faz o vetor de estado ficar no plano médio entre as bases $|0\rangle$ e $|1\rangle$, que seria o plano x,y . Sendo $\frac{1}{\sqrt{2}}$ os catetos de um triângulo retângulo de hipotenusa 1, essa distribuição geométrica impõe a probabilidade de 50% de ocorrência para ambas as bases: $|0\rangle$ e $|1\rangle$. Esse estado de equilíbrio probabilístico entre as bases $|0\rangle$ e $|1\rangle$ é denominado superposição. Se aplicarmos a porta Hadamard em um qubit $\psi = |0\rangle$ o resultado será o seguinte.

$$|\psi'\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \quad (68)$$

$$= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (69)$$

Existem outras portas simples, mas elas devem ser estudadas depois do entendimento das demonstradas aqui.

Simbologia das Portas

Cada uma das portas quânticas tem um símbolo gráfico, que nada mais é que sua letra inicial maiúscula inscrita em um retângulo.

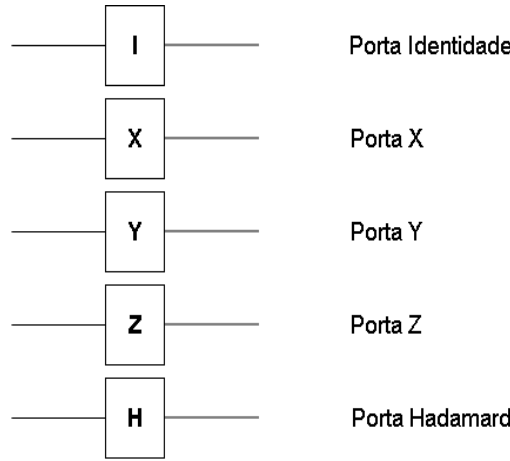


Figura 5 – Símbolos das portas quânticas

Portas Quânticas Múltiplas

As portas quânticas múltiplas operam em mais de um qubit. Elas são uma síntese conveniente de várias operações que portas quânticas simples fariam nesses qubits (BARDIN DANIEL SANK; JEFFREY, August 2020).

A porta negação-controlada C_{NOT} inverte um dado qubit $q1$ se o qubit $q0$ for igual a $|1\rangle$. Formalmente, a porta C_{NOT} é assim caracterizada (POLACK, 2011).

$$C_{NOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \quad (70)$$

$$= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \quad (71)$$

$$= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \quad (72)$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (73)$$

De onde se observa da fórmula (65) o mapeamento entrada-saída da porta C_{NOT} .

$$C_{NOT} : |00\rangle \rightarrow |00\rangle \quad (74)$$

$$|01\rangle \rightarrow |01\rangle \quad (75)$$

$$|10\rangle \rightarrow |11\rangle \quad (76)$$

$$|11\rangle \rightarrow |10\rangle \quad (77)$$

O símbolo da porta C_{NOT} é o seguinte.

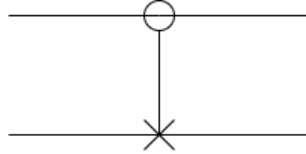


Figura 6 – Porta CNOT

O círculo do símbolo da porta C_{NOT} significa o qubit controlador e o X o qubit que é controlado. À primeira vista, pode-se presumir que a porta C_{NOT} não influi no qubit controlador após a sua ação. Isso não é verdade. Observe um circuito de dois qubits com duas portas Hadamard em cascata no qubit $q0$. O vetor de estado resultado ϕ' para $|00\rangle$ será este.

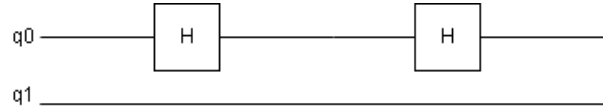


Figura 7 – Hadamard em série

$$\psi' = \begin{bmatrix} 1 + 0j \\ 0 + 0j \\ 0 + 0j \\ 0 + 0j \end{bmatrix} \quad (78)$$

Mas ao colocarmos uma porta C_{NOT} entre as portas Hadamard, o vetor de estado resultado ϕ'' para $q0 = |0\rangle; q1 = |0\rangle$ será outro.

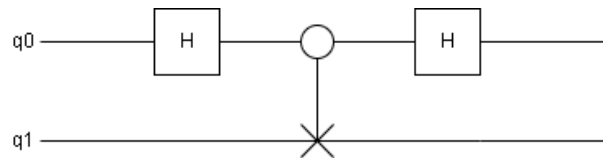


Figura 8 – CNOT entre Hadamards

$$\psi'' = \begin{bmatrix} 0,5 + 0j \\ 0,5 + 0j \\ 0,5 + 0j \\ -0,5 + 0j \end{bmatrix} \quad (79)$$

Isso ocorre porque $HH = I$. Sendo a matriz identidade neutra, o qubit – depois de aplicada a porta Hadamard duas vezes sucessivamente – permanece em seu estado original $|00\rangle$.

O comportamento da porta quântica atuando no qubit só é previsível através da álgebra linear. Observe também que a porta Hadarmad, assim como algumas outras, introduziu um defasamento no último elemento do vetor ϕ'' . Apesar de o módulo desse elemento ser igual ao dos outros três. Todavia, esse defasamento será computado pela próxima porta. Enfim, o circuito quântico só pode ser computado com segurança através das operações da álgebra linear.

A porta permutadora *SWAP* troca os estados de dois qubits entre si, se esses estados são diferentes. Ela é um desdobramento da porta C_{NOT} . A sua matriz é a seguinte.

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (80)$$

O mapeamento entrada-saída da porta *SWAP* é o seguinte.

$$SWAP : |00\rangle \rightarrow |00\rangle \quad (81)$$

$$|01\rangle \rightarrow |10\rangle \quad (82)$$

$$|10\rangle \rightarrow |01\rangle \quad (83)$$

$$|11\rangle \rightarrow |11\rangle \quad (84)$$

O símbolo da porta *SWAP* é o que segue.



Figura 9 – Porta Swap

Circuitos Quânticos

A representação gráfica da aplicação das portas quânticas nos qubits é realizada através do circuito quântico.

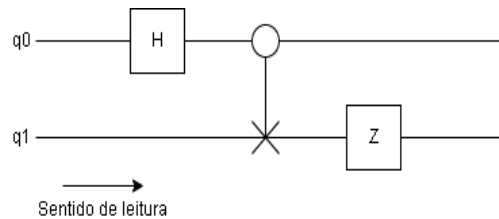


Figura 10 – Circuito quântico

Os estados do qubit são simbolizados por linhas. À esquerda dessas estão os rótulos dos qubits $q0, q1 \dots qn$. O sentido de leitura é da esquerda para a direita, sendo que a posição mais a esquerda é o estado inicial do qubit, o qual, se não sinalizado, assume-se que seja $|0\rangle$. As portas quânticas são aplicadas uma de cada vez para cada qubit. A linha imediatamente à direita da porta quântica retém o vetor de estado da ação da mesma. A resposta da computação de um circuito quântico é sempre um vetor de tamanho $2^n \therefore n = \text{qubits}$.

Estado de Emaranhamento

Quando aplicamos uma porta *CNOT* em dois qubits, essa operação os coloca em um estado quântico dito *emaranhamento*. Se essa operação é precedida pela aplicação de uma porta *Hadamard*, ambos os qubits assumem o estado $\psi = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

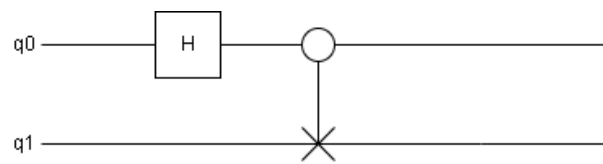


Figura 11 – Circuito que produz um emaranhamento

Esse estado de emaranhamento a partir da porta *Hadamard* é conhecido como estado de Bell. Esse estado não pode ser escrito separadamente em relação aos qubits envolvidos. Trata-se de um estado combinado entre qubits. Depois da leitura de um dos dois qubits, o resultado será $|00\rangle$ ou $|11\rangle$. Isso nos leva a conclusão de que o qubit não lido terá o mesmo estado do qubit lido (QUANTUM, 2022b) depois de uma leitura. É importante notar que o resultado da medida de um qubit é aleatório – a medida tem chances iguais de ser $|00\rangle$ ou $|11\rangle$ – e não é influenciado por qualquer manipulação no outro qubit. Esse comportamento intrigou os físicos quando descoberto, pois mesmo que os qubits emaranhados sejam afastados para uma distância muito grande, eles não perdem esse entrelaçamento.

Introdução ao QISKIT

O qiskit é um *framework* (um ambiente de programação) desenvolvido pela IBM para a programação de seus computadores quânticos. Ele é composto por uma coleção de bibliotecas em linguagem Python, um livro texto e outros recursos embutidos em uma página WEB ⁴. Ele pode ser instalado localmente ⁵, bem como ser utilizado no ambiente IBM Quantum ⁶. O ambiente IBM Quantum aceita contas do Gmail, do Github, do LinkedIn, do Twitter e do Instituto Fraunhofer para autenticação, o que torna o ingresso muito ágil.

O usuário tem à disposição muitas seções no IBM Quantum, dentre elas: Documents, System, Laboratory e Composer. A seção Documents contém toda a literatura necessária para o estudo da computação quântica. A seção System possui a lista de computadores quânticos disponíveis; somente aqueles com 5 qubits estão disponíveis para os iniciantes. A

⁴ <https://qiskit.org>

⁵ https://qiskit.org/documentation/getting_started.html

⁶ <https://quantum-computing.ibm.com>

seção Laboratory contém o ambiente de programação Qiskit que é compilado através de cadernos Jupyter.

O ambiente Composer deve ser utilizado pelo iniciante para estudar o qubit e seus circuitos.

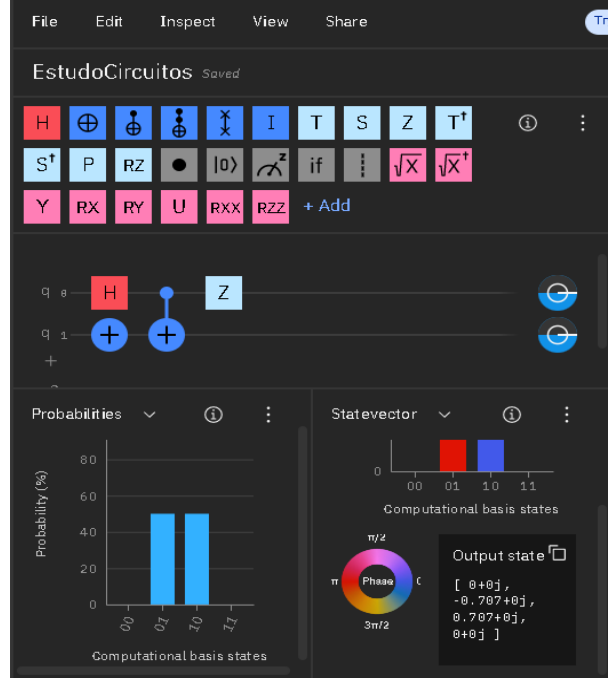


Figura 12 – Ambiente Composer do Qiskit - (QUANTUM, 2022a)

Por exemplo, faça o circuito acima arrastando e soltando as portas quânticas. Depois ajuste as duas janelas inferiores para mostrar *Probabilities* e *Statevector*. Você verá que o estado de Bell foi assim modificado.

$$\psi = -\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \therefore \frac{1}{\sqrt{2}} \cong 0,707 \quad (85)$$

O resultado acima aparece na janela *Statevector* como segue.

$$\psi = \begin{bmatrix} 0 & + & 0j \\ -0.707 & + & 0j \\ 0.707 & + & 0j \\ 0 & + & 0j \end{bmatrix} \quad (86)$$

Na janela de *Probabilities*, vemos as probabilidades como gráficos de barra. A quantidade de barras é $2^n \therefore n = \text{qubits}$. Nesse caso, elas indicam 50% para um dos dois estados $|01\rangle$ e $|10\rangle$. A cor vermelha no estado $|01\rangle$ indica que o qubit teve um giro na sua fase relativa. O valor desse giro é indicado pelo anel colorido que indica um giro de π ou 180° – cor vermelha na barra do estado $|01\rangle$.

Observa-se que a adição da porta inversora X trocou o estado de Bell inicial de $|00\rangle$ e $|11\rangle$ para $|01\rangle$ e $|10\rangle$ e a porta Z deu um giro de 180° no estado $|10\rangle$. Assim, pode-se indicar para o iniciante que utilize o ambiente *Composer* como uma calculadora para estudar o comportamento dos qubits em sua interação com as portas quânticas, sem a necessidade de se utilizar calculadoras para operações com matrizes ou como programas baseados na biblioteca *numpy* do Python.

Conclusão

Os fundamentos da computação quântica, a notação de Dirac, o qubit e suas portas de manipulação foram apresentadas de maneira parcial para facilitar o entendimento inicial da matéria – não foram mostradas todas as portas quânticas como, por exemplo, T , S , U e *Toffoli*. No entanto, a base matemática foi mostrada de maneira consistente para que o leitor tenha condições de entender o resultado das manipulações das portas quânticas no qubit, tanto através de equações de estado, como de simuladores como o *Composer* da IBM Quantum.

Agradecimentos

Este projeto foi apoiado pelo programa PPI Softex, Convênio nº 0200-08/2021/PPI/Softex/Fit/ResTIC3, financiado pelo Ministério da Ciência, Tecnologia e Inovações com recursos da Lei nº 8.248, de 23 de outubro de 1991.

Referências

- BARDIN DANIEL SANK, O. N. J. C.; JEFFREY, E. Quantum computing. IEEE Microwave Magazine, August 2020. Citado 2 vezes nas páginas 6 e 13.
- BRANDL, M. F. A quantum von neumann architecture for large-scale quantum computing. arXiv, August 2017. Citado na página 9.
- FARIAS, P. H. d. A. K. . R. R. S. D. M. *Álgebra Linear - Um Livro Colaborativo*. 2020. Disponível em: <<https://www.ufrgs.br/reatmat/AlgebraLinear/livro/s2-vetores.html>>. Acesso em: 2022-03-14. Citado na página 3.
- GCROSS. *Qubit Clipart*. 2022. URL na internet. Disponível em: <<https://openclipart.org/detail/142879/qubit-bloch-sphere>>. Acesso em: 2022-03-14. Citado na página 3.
- POLACK, E. R. . W. *Quantum Computing - A Gentle Introduction*. 1. ed. [S.l.]: Massachussets Institute of Technology, 2011. Citado 5 vezes nas páginas 6, 10, 11, 12 e 13.
- QUANTUM, I. *Ambiente programação IBM QUANTUM*. 2022. 2022-11-17. Disponível em: <<https://quantum-computing.ibm.com/>>. Acesso em: 2022-11-17. Citado na página 17.
- QUANTUM, I. *Qiskit Textbook - IBM QUANTUM*. 2022. URL na internet. Disponível em: <<https://qiskit.org/textbook/ch-states/introduction.html>>. Acesso em: 2022-03-14. Citado 7 vezes nas páginas 3, 4, 6, 7, 8, 12 e 16.

WELLSTOOD, F. *Notes About the Bloch Sphere*. 2016. Disponível em: <<http://physics.umd.edu/courses/Phys402/AnlageFall16/Bloch%20Sphere%20Notes%20by%20Fred%20Wellstood.pdf>>. Acesso em: 2022-03-21. Citado na página 9.