Notas sobre Computação Quântica

Henrique Hepp

18 de outubro de 2021

Nesse trabalho apresentamos conceitos elementares referentes a álgebra linear, mecânica quântica e computação quântica. O conteúdo das seções baseia-se principalmente nos livros de Kaye et al. (2007) e de Nielsen e Chuang (2011).

1 Álgebra linear

Os objetos básicos da álgebra linear são os *espaços vetoriais*. Na computação quântica os espaços vetoriais nos quais estamos interessados são os espaços vetoriais complexos com dimensão finita com produto interno, que nomeamos como *espaços de Hilbert*. Neste texto usamos as letras $\mathcal{H}, \mathcal{V}, \mathcal{W}$ para denotar espaços de Hilbert. Para denotar os vetores de um espaço de Hilbert usamos a *notação de kets*, ou seja, um vetor $\boldsymbol{v}$ é denotado como $|v\rangle$.

Uma maneira alternativa de descrever os estados é por meio de matrizes. Nesse caso, um vetor $|v\rangle = \alpha_1 |v_1\rangle + \alpha_2 |v_2\rangle + \cdots + \alpha_N |v_n\rangle$, em que $|v_1\rangle, |v_2\rangle, \cdots, |v_n\rangle$ são vetores unitários linearmente independentes, é expresso como

$$|v\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

Para denotar o vetor transposto conjugado de $|v\rangle$ usamos a notação *bra*, ou seja,

$$\langle v| = \begin{bmatrix} \alpha_1^* & \alpha_2^* & \cdots & \alpha_N^* \end{bmatrix},$$

onde os coeficientes α_i^* são os complexos conjugados de α_i.

O *produto interno* entre dois vetores $|v\rangle = \alpha_1 |v_1\rangle + \cdots + \alpha_n |v_n\rangle$ e $|w\rangle = \beta_1 |v_1\rangle + \cdots + \beta_n |v_n\rangle$ é definido e denotado por

$$\langle v|w\rangle = \alpha_1^* \beta_1 + \cdots + \alpha_n^* \beta_n .$$

Observe que $\langle v|w\rangle = \langle w|v\rangle^*$. Se o produto interno entre dois vetores é igual a zero, esses dois vetores são *ortogonais*. A *norma de um vetor* $|v\rangle \in \mathcal{V}$ é

$$\| |v\rangle \| = \sqrt{\langle v|v\rangle} .$$

Um vetor é *unitário* se tiver norma igual a um. Vetores unitários ortogonais são chamados de *ortonormais*.

Dado um espaço de Hilbert $\mathcal{H}$ com dimensão $2^n = N$, um conjunto de N vetores $B = \{|b_m\rangle\} \subseteq \mathcal{H}$ é uma *base ortonormal* de $\mathcal{H}$ se

$$\langle b_n|b_m\rangle = \delta_{n,m} \quad \forall b_m, b_n \in B$$

e todo $|\psi\rangle \in \mathcal{H}$ pode ser escrito como

$$|\psi\rangle = \sum_{b_n \in B} \alpha_n |b_n\rangle \qquad \text{para algum } \alpha_n \in \mathbb{C} \ .$$

Os valores de α_n satisfazem $\alpha_n = \langle b_n|\psi\rangle$ e são chamados de coeficientes de $|\psi\rangle$ com respeito à base $\{|b_n\rangle\}$.

Um *operador linear* entre $\mathcal{V}$ e $\mathcal{W}$ é qualquer função $A : \mathcal{V} \to \mathcal{W}$ que seja linear, ou seja,

$$A\left(\sum_i \alpha_i |v_i\rangle\right) = \sum_i \alpha_i A |v_i\rangle \ .$$

Dado um espaço de Hilbert $\mathcal{H}$, denotamos por $\mathbf{L}(\mathcal{H})$ o conjunto de operadores lineares $A : \mathcal{H} \to \mathcal{H}$.

A *norma de um operador* $A \in \mathbf{L}(\mathcal{H})$, para todo vetor $|v\rangle \in \mathcal{H}$, é

$$\|A\| = \sup_{|v\rangle \neq 0} \frac{\|A|v\rangle\|}{\||v\rangle\|} \ .$$

Sejam $|v\rangle \in \mathcal{V}$ e $|w\rangle \in \mathcal{W}$. O *produto diádico* denotado por $|w\rangle\langle v|$ é um operador linear de $\mathcal{V}$ para $\mathcal{W}$ cuja ação é definida por:

$$(|w\rangle\langle v|)(|v'\rangle) = |w\rangle\langle v|v'\rangle \ .$$

Observe que: $|w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$. Em sua forma matricial, o *produto diádico* entre entre dois vetores $|w\rangle = \alpha_1|1\rangle + \cdots + \alpha_n|n\rangle$ e $|v\rangle = \beta_1|1\rangle + \cdots + \beta_n|n\rangle$ para uma base ortogonal $\{|i\rangle\} \in \mathcal{H}$ é

$$|w\rangle\langle v| = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{bmatrix} \begin{bmatrix} \beta_1^* & \beta_2^* & \beta_3^* & \cdots & \beta_n^* \end{bmatrix} .$$

Seja $\{|i\rangle\}$ uma base ortogonal para $\mathcal{V}$, como um vetor $v \in \mathcal{V}$ pode ser escrito como $|v\rangle = \sum_i \alpha_i |i\rangle$, para algum conjunto de números complexos $\{\alpha_i\}$ e como $\langle i|v\rangle = \alpha_i$, temos:

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle = \sum_i \alpha_i |i\rangle = |v\rangle \ . \tag{1}$$

Como (1) vale para todo v, obtemos a equação conhecida como *relação de completude*:

$$\sum_i |i\rangle\langle i| = \mathbb{1} \ .$$

Dado um operador linear A em $\mathcal{H}$, o *operador adjunto* ou *Hermitiano conjugado* de A, denotado por $A^\dagger$, é definido como

$$A^\dagger = (A^*)^T \ .$$

Observe que

$$(\langle v| A |w\rangle)^* = \langle w| A^\dagger |v\rangle \quad \forall\, |v\rangle, |w\rangle \in \mathcal{H} \ .$$

Por convenção,

$$|v\rangle^\dagger = \langle v| \ .$$

A operação adjunta tem as seguintes propriedades:

- $(AB)^\dagger = B^\dagger A^\dagger$;
- $(|w\rangle \langle v|)^\dagger = |v\rangle \langle w|$;
- $(A^\dagger)^\dagger = A$;
- $(\sum_i \alpha_i A_i)^\dagger = \sum_i \alpha_i^* A_i^\dagger$.

Na mecânica quântica é comum o uso dos seguintes operadores lineares.

- Um operador N é *normal* se $NN^\dagger = N^\dagger N$. Denotamos o conjunto de todos operadores normais em $\mathcal{H}$ como $\mathbf{Norm}(\mathcal{H})$.
- Um operador H é *hermitiano* se $H = H^\dagger$. Denotamos o conjunto de todos operadores hermitianos em $\mathcal{H}$ como $\mathbf{Herm}(\mathcal{H})$.
- Um operador P é *positivo* ou *positivo semidefinido* se é hermitiano e para qualquer vetor $|v\rangle$, temos $\langle v| P |v\rangle \geq 0$, e $\langle v\rangle P |v\rangle \in \mathbb{R}$. Denotamos o conjunto de todos operadores positivos em $\mathcal{H}$ como $\mathbf{Pos}(\mathcal{H})$.
- Um operador Π é *projetor ortogonal* se é hermitiano, e satisfaz $\Pi^2 = \Pi$. Denotamos o conjunto de todos operadores projetores ortogonais em $\mathcal{H}$ como $\mathbf{Proj}(\mathcal{H})$.
- Um operador $U \in \mathbf{L}(\mathcal{H})$ é *unitário* se $U^\dagger U = \mathbb{1}$. Denotamos o conjunto de todos operadores unitários em $\mathcal{H}$ como $\mathbf{U}(\mathcal{H})$. A definição também implica que:
  1. $U^\dagger = U^{-1}$, onde U^{-1} é a inversa de U;
  2. U preserva o produto interno, $\langle Uv|Uw\rangle = \langle v|w\rangle$ para todo $|v\rangle, |w\rangle \in \mathcal{H}$;
  3. U preserva a norma: $\|U|v\rangle\| = \||v\rangle\|$ para todo $|v\rangle \in \mathcal{H}$;
  4. se $\||v\rangle\| = 1$ então $\|U|v\rangle\| = 1$ para todo $|v\rangle \in \mathcal{H}$.

A relação entre os operadores lineares é ilustrada na Figura 1.
Um vetor $|\psi\rangle$ é nomeado de *autovetor* de um operador T se, para alguma constante λ, temos:

$$T|\psi\rangle = \lambda|\psi\rangle \ .$$

A constante λ é nomeada como *autovalor* de T correspondente ao autovetor $|\psi\rangle$.

Teorema 1 (O Teorema Espectral)**.** *Qualquer operador **normal** M sobre um espaço de Hilbert $\mathcal{H}$ pode ser escrito como:*

$$M = \sum_i \lambda_i |i\rangle \langle i| \ ,$$

onde λ_i são os autovalores de M, $\{|i\rangle\}$ é uma base ortonormal para $\mathcal{H}$, e cada $|i\rangle$ é um autovetor de M com autovalor λ_i.

Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços de Hilbert com dimensões n e m respectivamente. P*produto tensorial* entre $\mathcal{V}$ e $\mathcal{W}$, denotado por $\mathcal{V} \otimes \mathcal{W}$, é um espaço de Hilbert com dimensão $n \times m$. Sejam $\{|b_i\rangle\}_{i\in\{1,\cdots,n\}}$ uma base ortonormal para $\mathcal{V}$ e $\{|c_j\rangle\}_{j\in\{1,\cdots,m\}}$ uma base ortonormal para $\mathcal{W}$. Então,

$$\{|b_i\rangle \otimes |c_j\rangle\}_{i\in\{1,\cdots,n\}, j\in\{i,\cdots,m\}}$$

é uma base ortonormal para $\mathcal{V} \otimes \mathcal{W}$.

O produto tensorial entre dois vetores $|v\rangle \in \mathcal{V}$ e $|w\rangle \in \mathcal{W}$ é um vetor em $\mathcal{V} \otimes \mathcal{W}$ denotado por $|v\rangle \otimes |w\rangle$. O produto tensorial é caracterizado pelos seguintes axiomas.

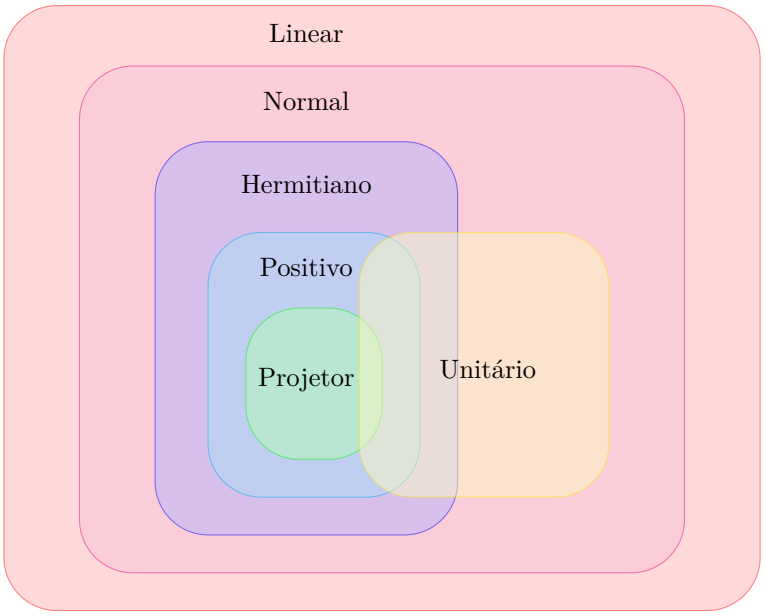

Figura 1: Tipos de operadores lineares.

1. Para quaisquer $c \in \mathbb{C}$, $|v\rangle \in \mathcal{V}$ e $|w\rangle \in \mathcal{W}$,

$$c(|v\rangle \otimes |w\rangle) = (c\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c\,|w\rangle)\,;$$

2. Para quaisquer $|v_1\rangle, |v_2\rangle \in \mathcal{V}$ e $w \in \mathcal{W}$,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle\ ;$$

3. Para quaisquer $|v\rangle \in \mathcal{V}$ e $|w_1\rangle, |w_2\rangle \in \mathcal{W}$,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle\ .$$

As seguintes notações são equivalentes:

$$|i\rangle \otimes |j\rangle = |i, j\rangle = |ij\rangle\ ;$$
$$|i, j\rangle_{AB} = |i\rangle_A \otimes |j\rangle_B = |i\rangle_A\,|j\rangle_B\ .$$

Uma identidade útil é

$$|ij\rangle\langle kl| = |i\rangle\langle k| \otimes |j\rangle\langle l|\ .$$

Sejam A e B operadores lineares em $\mathcal{V}$ e $\mathcal{W}$, respectivamente. Então $A \otimes B$ é o operador linear em $\mathcal{V} \otimes \mathcal{W}$ definido por

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A\,|v\rangle \otimes B\,|w\rangle\,.$$

O produto tensorial também pode ser representado matricialmente. Dadas as matrizes A com dimensão $m \times n$ e B com dimensão $p \times q$, o *produto de Kronecker*, denotado por $A \otimes B$, é a matriz $mp \times nq$ dada por

$$A \otimes B = \begin{bmatrix} A_{11}[B] & A_{12}[B] & \cdots & A_{1n}[B] \\ A_{21}[B] & A_{22}[B] & \cdots & A_{2n}[B] \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}[B] & A_{m2}[B] & \cdots & A_{mn}[B] \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} A_{11}B_{11} & \cdots & A_{11}B_{1q} & \cdots & \cdots & A_{1n}B_{11} & \cdots & A_{1n}B_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{11}B_{p1} & \cdots & A_{11}B_{pq} & \cdots & \cdots & A_{1n}B_{p1} & \cdots & A_{1n}B_{pq} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{m1}B_{11} & \cdots & A_{m1}B_{1q} & \cdots & \cdots & A_{mn}B_{11} & \cdots & A_{mn}B_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{m1}B_{p1} & \cdots & A_{m1}B_{pq} & \cdots & \cdots & A_{mn}B_{p1} & \cdots & A_{mn}B_{pq} \end{bmatrix} .$$

O *traço* de um operador A sobre um espaço de Hilbert $\mathcal{H}$ é

$$\operatorname{tr}(A) = \sum_{b_n} \langle b_n | A | b_n \rangle ,$$

onde $\{b_n\}$ é qualquer base ortonormal para $\mathcal{H}$. Em sua representação matricial o traço é a soma dos elementos da diagonal principal.

Dados os operadores lineares $A, B \in \mathbf{L}(\mathcal{H})$ e $U \in \mathbf{U}(\mathcal{H})$, a função traço tem as seguintes propriedades:

- (Propriedade cíclica). $\operatorname{tr}(AB) = \operatorname{tr}(BA)$;
- (Linearidade) $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$;
- $\operatorname{tr}(zA) = z \operatorname{tr}(A)$ com $z \in \mathbb{C}$;
- $\operatorname{tr}(UAU^\dagger) = \operatorname{tr}(U^\dagger UA) = \operatorname{tr}(A)$ (o traço não depende da base) ;
- $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \operatorname{tr}(B)$.

Dados dois vetores $|\psi\rangle \in \mathcal{H}$ e $|\phi\rangle \in \mathcal{H}$, o traço do produto tensorial $|\psi\rangle \langle\phi|$ é:

$$\operatorname{tr}(|\psi\rangle \langle\phi|) = \sum_i \langle i|\psi\rangle \langle\phi|i\rangle = \sum_i \langle\phi|i\rangle \langle i|\psi\rangle = \langle\phi|\psi\rangle .$$

2 Mecânica quântica

A mecânica quântica pode ser vista como um arcabouço matemático e conceitual usado para descrever um sistema físico. Podemos nomear um conjunto de postulados como base da mecânica quântica, mas observamos que não existe um consenso sobre o conteúdo e forma dos postulados.

Postulado 1. *A todo sistema físico isolado está associado um espaço de Hilbert $\mathcal{H}$, conhecido por **espaço de estados** do sistema. O sistema é descrito por um **estado (puro)**, que é um vetor unitário em $\mathcal{H}$.*

Um estado $|\psi\rangle$ em um espaço com N dimensões, $\mathbb{C}^N$, pode ser descrito pela combinação linear de N estados linearmente independentes

$$|\psi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle + \cdots + \alpha_N |N\rangle \ ,$$

onde $\alpha_1, \cdots \alpha_N$ são números complexos. Como $|\psi\rangle$ é um vetor unitário, temos que $\sum_i |\alpha_i|^2 = 1$. Podemos também dizer que o estado quântico $|\psi\rangle$ é a *superposição* dos N estados, e os números $\alpha_1, \cdots \alpha_N$ também são chamados de *amplitudes* dos estados.

Postulado 2. *A **evolução de um sistema quântico** no tempo é descrita pela equação de Schrödinger,*

$$i\hbar \frac{d\,|\psi\rangle}{dt} = H(t)\,|\psi\rangle \ ,$$

onde $\hbar$ é a constante de Planck e H é um operador hermitiano conhecido por Hamiltoniano.

Quando o sistema quântico é isolado, o Hamiltoniano é constante com relação ao tempo. Nesse caso a solução da equação de Schrödinger pode ser expressa por

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] |\psi(t_1)\rangle = U(t_1, t_2)\,|\psi(t_1)\rangle \ ,$$

onde definimos

$$U(t_1, t_2) = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] .$$

Como U é unitário e qualquer operador unitário pode ser expresso por $U = \exp(iK)$ para algum operador hermitiano K, podemos enunciar o segundo postulado como:

Postulado 2'. *A **evolução de um sistema quântico** isolado é descrita por uma **transformação unitária**. O estado $|\psi\rangle$ do sistema no tempo t_i está relacionado com o estado $|\psi'\rangle$ do sistema no tempo t_2 por meio de um operador unitário U que depende apenas dos tempos t_1 e t_2,*

$$|\psi'\rangle = U\,|\psi\rangle \ .$$

Postulado 3. *O **espaço de estado de um sistema físico composto** é o produto tensorial dos espaços de estados dos subsistemas. Se os sistemas forem numerados de 1 a n, o estado composto do sistema total é $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.*

Um estado puro $|\psi\rangle \in \mathcal{V} \otimes \mathcal{W}$ é um *produto estado*, se pode ser escrito como um produto tensorial de dois estados,

$$|\psi\rangle = |\psi_V\rangle \otimes |\psi_W\rangle \ ,$$

sendo $|\psi_V\rangle \in \mathcal{V}$ e $|\psi_W\rangle \in \mathcal{W}$. Caso não seja possível, esse estado é *emaranhado*. Quatro exemplos de estados emaranhados são os *estados de Bell*:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} ,$$
$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} ,$$
$$\frac{|10\rangle + |01\rangle}{\sqrt{2}} ,$$
$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} .$$

Postulado 4. *As **medições quânticas gerais** são descritas por uma coleção $\{M_i\}$ de operadores, chamados de operadores de medição, os quais satisfazem a equação de completude*

$$\sum_i M_i^\dagger M_i = \mathbb{1} \ .$$

Se o estado do sistema for $|\psi\rangle$ imediatamente antes da medição, então a probabilidade de ocorrer o resultado i é dado por

$$p(i) = \langle\psi| \, M_i^\dagger M_i \, |\psi\rangle \ ,$$

e o estado do sistema após a medição é

$$\frac{M_i \, |\psi\rangle}{\sqrt{\langle\psi| \, M_i^\dagger M_i \, |\psi\rangle}} \ .$$

A equação de completude expressa o fato que a soma das probabilidades é igual a 1,

$$1 = \sum_i p(i) = \sum_i \langle\psi| \, M_i^\dagger M_i \, |\psi\rangle \ .$$

Se os operadores de medição M_i são operadores projetivos Π_i, temos que a coleção $\{M_i\}$ pode ser expressa em termos da matriz

$$M = \sum_i m_i \Pi_i = \sum_i m_i \, |\varphi_i\rangle \, \langle\varphi_i| \ .$$

A probabilidade de obtermos o evento i é dada por

$$p(i) = \langle\psi| \, \Pi_i \, |\psi\rangle = \langle\psi|\varphi_i\rangle \, \langle\varphi_i|\psi\rangle \ ;$$

então, sendo $\alpha_i = \langle\varphi_i|\psi\rangle$,

$$p(i) = \langle\psi|\varphi_i\rangle \, \langle\varphi_i|\psi\rangle = \alpha_i^* \alpha_i = |\alpha_i|^2 \ .$$

O estado do sistema após a medição é:

$$\frac{\Pi_i \, |\psi\rangle}{\sqrt{\langle\psi| \, \Pi_i \, |\psi\rangle}} = \frac{|\varphi_i\rangle \, \langle\varphi_i|\psi\rangle}{\sqrt{|\alpha_i|^2}} = \frac{\alpha_i \, |\varphi_i\rangle}{\alpha_i} = |\varphi_i\rangle \ .$$

Uma outra maneira de se enunciar o Postulado 4, portanto, é a seguinte:

Postulado 4'. *Dados uma base ortonormal $B = \{|\psi_i\rangle\}$ de um espaço de estado $\mathcal{H}_A$ e um estado $|\psi\rangle = \sum_i \alpha_i \, |\psi_i\rangle$, ao fazermos uma **medição de Von Neumann** de $|\psi\rangle$ com respeito à base B, obtemos o estado $|\psi_i\rangle$ com probabilidade $|\alpha_i|^2$ e perdemos todas as demais informações do estado original. Em outras palavras, ao medirmos $|\psi\rangle$, o estado **colapsa** em $|\psi_i\rangle$ com probabilidade $|\alpha_i|^2$.*

Considere um estado $|\psi\rangle = \sum_i \alpha_i \, |\varphi_i\rangle \, |\gamma_i\rangle$ de um espaço de estado $\mathcal{H}_A \otimes \mathcal{H}_B$ em que $|\varphi_i\rangle$ são ortonormais e $|\gamma_i\rangle$ são vetores unitários, a medição no sistema A colapsa o estado $|\psi\rangle$ em $|\varphi_i\rangle \, |\gamma_i\rangle$ com probabilidade $|\alpha_i|^2$.

Há casos em que o sistema é descrito por um conjunto de estados puros $\{|\psi_i\rangle\}$, associado cada um a uma probabilidade p_i, de modo que $\sum_i p_i = 1$:

$$\{(|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \cdots, (|\psi_k\rangle, p_k)\} .$$

Esse conjunto é chamado de *estado misto*. O *operador densidade*, também conhecido como matriz densidade, associado a esse estado misto é definido como

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| .$$

Em particular, para um estado puro ψ,

$$\rho = |\psi\rangle \langle\psi| .$$

Denotamos $\mathbf{D}(\mathcal{H})$ como o conjunto de operadores densidade no espaço de Hilbert $\mathcal{H}$.

Por exemplo, o operador densidade para o estado puro $|\psi\rangle = a|0\rangle + b|1\rangle$ é

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| = 1 \cdot |\psi\rangle \langle\psi| = (a|0\rangle + b|1\rangle)(a^* \langle 0| + b^* \langle 1|)$$
$$\rho = aa^* |0\rangle \langle 0| + ab^* |0\rangle \langle 1| + ba^* |1\rangle \langle 0| + bb^* |1\rangle \langle 1| .$$

A representação matricial de ρ é

$$\rho = \begin{bmatrix} aa^* & ab^* \\ ba^* & bb^* \end{bmatrix} .$$

O operador densidade para o estado misto em que há a probabilidade p de se ter o estado $|0\rangle$ e $1 - p$ de se ter o estado $|1\rangle$ é

$$\rho = p|0\rangle \langle 0| + (1-p)|1\rangle \langle 1|$$
$$\rho = \begin{bmatrix} p & 0 \\ 0 & 1-p \end{bmatrix} .$$

Teorema 2. *Um operador ρ é o operador densidade associado a um conjunto $\{|\psi_i\rangle, p_i\}$ se e somente se satisfaz:*

1. $\mathrm{tr}(\rho) = 1$;
2. $\rho \in \mathbf{Pos}(\mathcal{H})$.

Observe que, se o estado ao qual um operador densidade ρ está associado é puro, então

$$\mathrm{tr}(\rho^2) = 1 ,$$

caso contrário

$$\mathrm{tr}(\rho^2) < 1 .$$

Podemos agora reescrever os postulados para os operadores de densidade.

Postulado 1. *A todo sistema físico isolado está associado um espaço de Hilbert, conhecido por **espaço de estado** do sistema. O sistema é descrito por seu **operador densidade**, que é um operador ρ positivo com traço igual a um agindo sobre o espaço de estado do sistema. Se um sistema quântico está no estado ρ_i com probabilidade p_i, então o operador densidade para o sistema é $\sum_i p_i \rho_i$.*

Postulado 2. *A evolução de um sistema **isolado** é descrita por uma **transformação unitária**. O estado ρ do sistema no tempo t_1 está relacionado com o estado ρ' do sistema no tempo t_2 por meio de um operador unitário U que depende apenas dos tempos t_1 e t_2:*

$$\rho' = U\rho U^\dagger \, .$$

Postulado 3. *O espaço de estado de um sistema físico composto é o produto tensorial dos espaços de estados dos subsistemas. Se os sistemas forem numerados de 1 a n, o estado composto do sistema total é $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$.*

Um estado $\rho \in \mathbf{D}(\mathcal{V} \otimes \mathcal{W})$ é *separável* se pode ser escrito como uma combinação linear de produtos estados,

$$\rho = \sum_i p_i \rho_V^i \otimes \rho_W^i \, ,$$

sendo $0 \leq p_i \leq 1$, $\sum_i p_i = 1$, $\rho_V^i \in \mathbf{D}(\mathcal{V})$ e $\rho_W^i \in \mathbf{D}(\mathcal{W})$. Caso não seja possível, ele é *emaranhado*.

Postulado 4. *As medições quânticas são descritas por uma coleção $\{M_i\}$ de **operadores de medição**. Esses são os operadores lineares agindo sobre o espaço de estado do sistema. O índice i se refere aos possíveis resultados da medição. Se o estado do sistema for ρ imediatamente antes da medição, então a probabilidade de ocorrer o resultado i é dada por*

$$p(i) = \mathrm{tr}(M_i^\dagger M_i \rho) \, ,$$

e o estado do sistema após a medição é

$$\frac{M_i \rho M_i^\dagger}{\mathrm{tr}(M_i^\dagger M_i \rho)} \, .$$

Os operadores de medição satisfazem a equação de completude

$$\sum_i M_i^\dagger M_i = \mathbb{1} \ .$$

A seguir, uma maneira alternativa de enunciar o Postulado 4 é enunciada a seguir.

Postulado 4'. *Dada uma coleção $\{(|\psi_i\rangle \, , p_i)\}_{i=1}^N$ onde $\psi_i \in \mathcal{H}$ e p_i é a probabilidade de se obter $|\psi_i\rangle$, temos:*

$$\begin{aligned}
\Pr[\textit{obter } |\phi\rangle] &= \sum_{i=1}^N p_i |\langle\psi_i|\phi\rangle|^2 \\
&= \sum_{i=1}^N p_i \, \langle\phi|\psi_i\rangle \, \langle\psi_i|\phi\rangle \\
&= \langle\phi| \left(\sum_{i=1}^N p_i \, |\psi_i\rangle \, \langle\psi_i| \right) |\phi\rangle \\
&= \langle\phi| \, \rho \, |\phi\rangle \ .
\end{aligned}$$

Dados os sistemas quânticos $A = |a_1\rangle \langle a_2|$ e $B = |b_1\rangle \langle b_2|$, cujos estados são descritos por um operador densidade ρ^{AB}, o *operador de densidade reduzido* para o sistema A é definido como

$$\rho^A = \mathrm{tr}_B(\rho^{AB}) ,$$

onde tr_B é o *traço parcial* sobre o sistema B, definido como

$$\mathrm{tr}_B \left(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|\right) = |a_1\rangle \langle a_2| \, \mathrm{tr}(|b_1\rangle \langle b_2|) .$$

Como

$$\mathrm{tr}(|b_1\rangle \langle b_2|) = \mathrm{tr}(\langle b_2|b_1\rangle) = \langle b_2|b_1\rangle ,$$

obtemos

$$\mathrm{tr}_B \left(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|\right) = |a_1\rangle \langle a_2| \langle b_2|b_1\rangle .$$

Uma definição alternativa para o traço parcial é: dados dois espaços de Hilbert A e B e uma base ortonormal $\{|b_1\rangle, \cdots, |b_n\rangle\}$ para B, definimos um mapeamento $\mathrm{tr}_B : \mathbf{L}(A \otimes B) \to \mathbf{L}(A)$ tal que

$$\mathrm{tr}_B \, \rho^{AB} = \sum_{j=1}^{n} (I \otimes \langle b_j|) \rho^{AB} (I \otimes |b_j\rangle) .$$

O traço parcial sobre B intuitivamente significa que descartamos ou ignoramos a parte B do sistema. Ao dizermos que uma parte do sistema quântico foi *traced out*, significa que foi executado o traço parcial ignorando essa parte do sistema.

Por exemplo, o operador densidade do estado

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

é

$$\rho = \frac{1}{2} (|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11|) .$$

O operador de densidade reduzido do primeiro qubit sendo feito o traço parcial do segundo qubit é

$$\begin{aligned}
\rho^A &= \frac{1}{2} \mathrm{tr}_2(|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11|) \\
&= \frac{1}{2} \mathrm{tr}_2(|0\rangle \langle 0| \otimes |0\rangle \langle 0| + |0\rangle \langle 1| \otimes |0\rangle \langle 1| + |1\rangle \langle 0| \otimes |1\rangle \langle 0| + |1\rangle \langle 1| \otimes |1\rangle \langle 1|) \\
&= \frac{1}{2} (|0\rangle \langle 0| \, \mathrm{tr}_2(|0\rangle \langle 0|) + |0\rangle \langle 1| \, \mathrm{tr}_2(|0\rangle \langle 1|) + |1\rangle \langle 0| \, \mathrm{tr}_2(|1\rangle \langle 0|) + |1\rangle \langle 1| \, \mathrm{tr}_2(|1\rangle \langle 1|)) \\
&= \frac{1}{2} (|0\rangle \langle 0| \langle 0|0\rangle + |0\rangle \langle 1| \langle 1|0\rangle + |1\rangle \langle 0| \langle 0|1\rangle + |1\rangle \langle 1| \langle 1|1\rangle) \\
&= \frac{1}{2} (|0\rangle \langle 0| + |1\rangle \langle 1|) .
\end{aligned}$$

Um estado puro ρ^{AB} é um produto estado, se e somente se os operadores de densidade reduzidos ρ^A e ρ^B são estados puros. Caso contrário, o estado ρ^{AB} é emaranhado.

O *rank* de uma matriz é o número de linhas ou colunas independentes. No caso de um operador de densidade, o rank corresponde ao menor número de estados puros necessários para formar um estado misto

$$\rho = \sum_{i}^{\mathrm{rank}} p_i \, |\psi_i\rangle \langle \psi_i| .$$

A *purificação de um estado misto* $\rho \in \mathbf{D}(\mathcal{V})$ é qualquer estado puro $|\psi\rangle \in \mathcal{V} \otimes \mathcal{W}$ tal que $\mathrm{tr}_{\mathcal{W}} |\psi\rangle \langle\psi| = \rho$. Essa purificação sempre existe, desde que $\dim(\mathcal{W}) \geq \mathrm{rank}(\rho)$.

Dados dois operadores de densidade ρ e σ, definimos a *distância de traço* como

$$T(\rho, \sigma) = \|\rho - \sigma\|_{\mathrm{tr}} = \frac{1}{2} \mathrm{tr}\left[\sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)}\right] = \frac{1}{2} \sum_i |\lambda_i| \,,$$

onde λ_i são os autovalores da matriz $\rho - \sigma$.

A distância de traço tem as seguintes propriedades:

- $T(\rho, \sigma) = 0$ se e somente se $\rho = \sigma$;
- $0 \leq T(\rho, \sigma) \leq 1$ e $T(\rho, \sigma) = 1$ se e somente se ρ e σ têm suportes ortogonais;
- $T(\sum_i p_i \rho_i, \sigma) \leq \sum_i p_i T(\rho_i, \sigma)$.

Se ρ e σ comutam, então a distância de traço entre ρ e σ é igual à distância estatística, definida a seguir, entre as distribuições de probabilidade representadas pelos conjuntos de autovalores de ρ e σ. A *distância estatística* entre duas distribuições de probabilidade (ou variáveis aleatórias) X e Y definidas sobre o mesmo espaço amostral $\mathcal{U}$ é

$$\Delta(X, Y) = \|X - Y\|_1 = \max_{S \subseteq \mathcal{U}} \{|\Pr[X \in S] - \Pr[Y \in S]|\} = \frac{1}{2} \sum_{x \in \mathcal{U}} |\Pr[X = x] - \Pr[Y = x]| \,.$$

Teorema 3 (Montanaro e de Wolf, 2016, Sec. 4.2, p. 44)**.** *Seja $T(\rho, \sigma) \geq \epsilon$, sendo $\rho, \sigma \in \mathbf{D}(\mathcal{H})$ onde $\mathcal{H}$ tem dimensão N. Então, é possível distinguir ρ de σ com probabilidade maior que $2/3$ usando $O(N^2/\epsilon^2)$ cópias de ρ .*

3 Circuitos quânticos

Além das referências que já indicamos na abertura do capítulo, esta seção baseia-se também no trabalho de Aharonov (2003).

Um *qubit* é um estado quântico em um espaço de Hilbert com dimensão 2,

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

onde $\alpha, \beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$.

Podemos medir o qubit com relação a base $\{|0\rangle, |1\rangle\}$. A probabilidade de obtermos o estado $|0\rangle$ é

$$\begin{aligned} \Pr[0] &= |\langle 0|\psi\rangle|^2 = |\langle 0| \cdot (\alpha |0\rangle + \beta |1\rangle)|^2 \\ &= |\alpha \langle 0|0\rangle + \beta \langle 0|1\rangle|^2 = |\alpha \cdot 1 + \beta \cdot 0|^2 = |\alpha|^2 \,. \end{aligned}$$

Calcula-se de modo similar a probabilidade para o estado $|1\rangle$. Isso significa que, obtemos ou com probabilidade $|\alpha|^2$ o estado $|0\rangle$ ou com probabilidade $|\beta|^2$ o estado $|1\rangle$.

Para um sistema com n qubits, o estado quântico do sistema pode ser descrito como

$$|\psi\rangle = \sum_{i=0}^{2^n - 1} \alpha_i |i\rangle \ ,$$

onde $\alpha_0, \cdots, \alpha_{2^n - 1} \in \mathbb{C}$ e $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$. A base $\{|i\rangle\}$ é denominada de *base computacional*.

Uma *porta quântica* para n qubits é um operador que faz uma transformação unitária de n qubits. Um *circuito quântico* é uma rede acíclica de portas quânticas agindo sobre qubits. Como toda rede acíclica possui ordenação topológica, por vezes representamos circuitos quânticos por uma sequência de operadores. Observe que em um circuito quântico o número de qubits de entrada é sempre igual ao número de qubits da saída. No entanto, por vezes nos referimos a circuitos com m qubits de entrada e $n < m$ qubits de saída, presumindo uma operação *trace-out* dos $m - n$ qubits que não fazem parte da saída. Para todo circuito quântico em que medições ocorrem em estágios intermediários, é possível construir um circuito quântico equivalente com medições apenas no final. Portanto, supomos que as medições ocorrem apenas no final do circuito.

Um conjunto de portas quânticas S é *estritamente universal* se, para qualquer porta U para $n \geq 1$ qubits, podemos obter, por meio de um circuito quântico com n qubits formado apenas por portas em S, uma porta $\tilde{U}$ tal que, dada uma tolerância de erro ϵ, temos $\|\tilde{U} - U\| \leq \epsilon$.

O *Teorema de Solovay–Kitaev* implica que qualquer porta quântica para $O(1)$ qubits pode ser aproximada com uma precisão arbitrária ϵ usando $O(\log^c(1/\epsilon))$ portas de um conjunto estritamente universal.

Um conjunto de portas quânticas S é *computacionalmente universal* se, para todo circuito quântico C com n qubits e t portas de um conjunto estritamente universal, é possível construir um circuito para simular C dentro de um erro ϵ com um *overhead* apenas polilogarítmico em $(n, t, 1/\epsilon)$. A definição de conjunto *computacionalmente universal* é uma generalização da definição de conjunto *estritamente universal* em que se permite, por exemplo, o uso de qubits auxiliares.

Dado um circuito C formado com apenas portas de um conjunto (estrita ou computacionalmente) universal, o *tamanho* de C é definido como o número de portas quânticas mais o número de qubits de C.

Dentre os conjuntos de portas quânticas computacionalmente universais, citamos o conjunto com as portas Hadamard e Toffoli, definidas a seguir, assim como o conjunto com as portas Hadamard e Fredkin. Observamos que a porta Toffoli é universal para circuitos clássicos reversíveis.

- Porta Hadamard

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

- Porta Toffoli (CCNOT)

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

- Porta Fredkin (CSWAP)

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Se aplicarmos a porta Hadamard em n qubits, todos inicialmente iguais a 0, obtemos todas as 2^n possíveis strings binárias em sobreposição, todas com igual amplitude:

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \ .$$

É comum, em algoritmos quânticos, o uso de operações "caixa-preta". Sendo $f : \{0,1\}^n \to \{0,1\}^m$ uma função clássica, definimos U_f como a transformação unitária, para quaisquer $x \in \{0,1\}^n$ e $y \in \{0,1\}^m$,

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle \ ,$$

onde a operação $\oplus$ indica a adição módulo 2. Podemos aplicar a função $f(x)$ para diversos valores diferentes de x de modo simultâneo, o que é chamado de *paralelismo quântico*. Por exemplo, podemos colocar $f(x)$ em sobreposição para todos valores possíveis para x da seguinte forma:

$$U_f(H^{\otimes n} |0\rangle^{\otimes n}) |0\rangle^m = U_f \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle^m = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle \ .$$

Referências

Aharonov, D. (2003). A simple proof that Toffoli and Hadamard are quantum universal. *arXiv preprint quant-ph/0301040*.

Kaye, P., Laflamme, R. e Mosca, M. (2007). *An Introduction to Quantum Computing*. Oxford University Press.

Montanaro, A. e de Wolf, R. (2016). A survey of quantum property testing. *Theory of Computing*, (7):1–81.

Nielsen, M. A. e Chuang, I. L. (2011). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 10th edition.