CÓDIGOS QUÂNTICOS

Versão preliminar (sob revisão) das notas de aula do minicurso
do 1º Encontro de Teoria dos Códigos e Criptografia, UFABC,
10 a 12/11/2010

Renato Portugal
portugal@lncc.br

Coordenação de Ciência da Computação
Laboratório Nacional de Computação Científica
Ministério da Ciência e Tecnologia

Petrópolis, RJ, Brasil
2010

Portugal, Renato
Códigos Quânticos - Petrópolis, RJ :
LNCC, 2010, xxx p., 20.5 cm - ( )
( )

ISBN

1. Computação Quântica 2. Códigos Quânticos 3. Formalismo Estabilizador 4. Códigos Estabilizadores IV. Título. V. Série

CDD - 51

Conteúdo

Capítulo 1

Mecânica Quântica

É impossível fazer um resumo da Mecânica Quântica em poucas páginas. Como o objetivo deste trabalho é descrever códigos quânticos para correção de erros, limitaremos aos princípios da Mecânica Quântica e a descrevê-los como "regras do jogo". Suponha que você jogue Damas há muitos anos e domine diversas estratégias, mas você não conhece Xadrez. Suponha agora que alguém lhe descreva as regras do Xadrez. Em pouco tempo, você estará jogando um novo jogo. Certamente não estará dominando diversas estratégias do Xadrez, porém terá condições de jogar. Este capítulo tem um objetivo similar. Os postulados de uma teoria são como as regras do jogo. Se desrespeitarmos as regras, estaremos fora do jogo.

Na melhor das hipóteses, podemos nos concentrar em quatro postulados. O primeiro descreve a arena onde o jogo se passa. O segundo descreve a dinâmica do processo. O terceiro descreve como devemos fazer a composição de vários sistemas. O quarto descreve o processo da medição física. Todos esses postulados são descritos em termos da Álgebra Linear. É fundamental ter um conhecimento sólido dos resultados básicos dessa área. Além disso, o postulado dos sistemas compostos usa o conceito de produto tensorial, que é uma forma de combinar dois espaços vetoriais para construir um espaço vetorial maior. Também é importante estar familiarizado com esse conceito.

1.1 Espaço de Estados

O *estado* de um sistema físico descreve suas características físicas em um determinado instante. Usualmente descrevemos uma parte das possíveis características, que o sistema pode ter, pois, do contrário, os problemas físicos ficariam muito complexos. Por exemplo, o estado de rotação de uma bola de bilhar pode ser caracterizado por um

vetor no espaço $\mathbb{R}^3$. Nesse exemplo, não levaremos em consideração a velocidade linear da bola de bilhar, sua cor ou qualquer outra característica, que não esteja diretamente relacionada a sua rotação. O estado de rotação é totalmente caracterizado pelo eixo, pelo sentido e pela intensidade. Com três números reais caracterizamos o estado de rotação. Basta dar as componentes de um vetor, cuja direção caracteriza o eixo de rotação, cujo sentido caracteriza para qual lado a bola de bilhar está girando e cujo comprimento caracteriza a velocidade de rotação. Na Física Clássica, a direção do eixo de rotação pode variar continuamente assim como a intensidade de rotação.

Será que um *elétron*, considerado uma partícula elementar, isto é, não constituído de outras partículas menores, gira como uma bola de bilhar? A melhor maneira de responder a isto é fazendo experiências concretas para verificar se o elétron, de fato, gira e se obedece às leis da Física Clássica. Como o elétron tem carga, sua rotação produziria campos magnéticos, que poderiam ser medidos. Experiências desse tipo foram feitas, no início da Mecânica Quântica, com feixes de átomos de prata, depois com feixes de átomos de hidrogênio e, hoje em dia, elas são feitas com partículas individuais, sejam elétrons, sejam fótons. Tais resultados são efetivamente diferentes do que é previsto pelas leis da Física Clássica.

No caso do elétron, podemos enviá-lo através de um campo magnético na direção vertical (direção z), conforme o esquema da Fig. 1.1. Os possíveis resultados estão mostrados na figura. Ou o elétron bate no anteparo no ponto A ou no ponto B. Jamais encontramos o elétron no ponto O, que indica ausência de rotação. Essa experiência mostra que o *spin* do elétron só admite dois valores: *spin para cima* e *spin para baixo*, ambos com a mesma intensidade de "rotação". Esse resultado é bem diferente do clássico, já que a direção do eixo de rotação é quantizada, admitindo somente dois valores. A intensidade de rotação também é quantizada.

A Mecânica Quântica descreve o spin do elétron como um vetor unitário no espaço de Hilbert $\mathbb{C}^2$. O "spin para cima" é descrito pelo vetor

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

e "spin para baixo" pelo vetor

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

Isso parece um paradoxo, pois os vetores $|0\rangle$ e $|1\rangle$ são ortogonais. Por que associar vetores ortogonais a "spin para cima" e "spin para

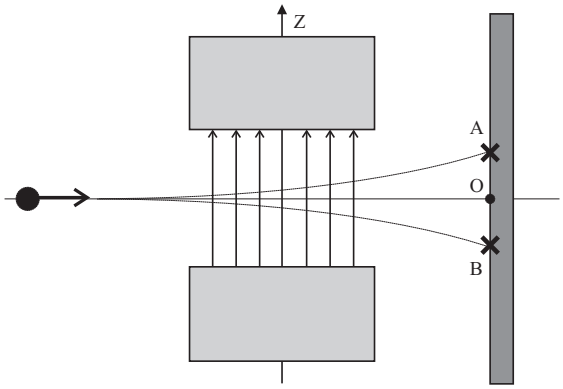

Figura 1.1: Desenho esquemático de um dispositivo experimental para medir o estado de rotação de um elétron. O elétron é enviado a uma velocidade fixa por um campo magnético na direção vertical. Ele bate em A ou B dependendo do sentido da rotação (*spin*). A distância dos pontos A e B ao ponto O depende da velocidade de rotação do elétron. Os resultados destas experiências são bem diferentes do que esperamos classicamente.

baixo"? No espaço $\mathbb{R}^3$, se somarmos "spin para cima" com "spin para baixo" obtemos uma partícula parada sem rotação, pois a soma de dois vetores opostos de comprimentos iguais dá o vetor nulo, que descreve ausência de rotação. No mundo clássico, não é possível uma bola de bilhar girar tanto para um lado como para o outro ao mesmo tempo. Temos duas situações excludentes. Vale a *lógica do terceiro excluído*. A noção de "spin para cima" ou "spin para baixo" se refere ao $\mathbb{R}^3$, porém a Mecânica Quântica também descreve o comportamento do elétron antes da observação, isto é, antes de entrar no campo magnético, que visa a determinar seu estado de rotação.

Se o elétron não entrou no campo magnético e se ele está isolado do meio macroscópico ao redor, seu estado de spin é descrito por um combinação linear dos vetores $|0\rangle$ e $|1\rangle$, da seguinte forma

$$|\psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle\,, \tag{1.1.1}$$

onde os coeficientes a_0 e a_1 são números complexos, que satisfazem ao vínculo

$$|a_0|^2 + |a_1|^2 = 1. \tag{1.1.2}$$

Como os vetores $|0\rangle$ e $|1\rangle$ são ortogonais, a soma não dá o vetor nulo. As possibilidades excludentes classicamente coexistem quanticamente. Essa coexistência é destruída quando tentamos observá-la usando o dispositivo da Fig. 1.1.

1.1.1 Postulado do Espaço de Estados

Um *sistema físico isolado* tem associado um espaço de Hilbert, chamado de *espaço de estados*. O estado do sistema é totalmente descrito por um vetor unitário, chamado de *vetor de estado*, nesse espaço de Hilbert.

Observações

1. O postulado do espaço de estados não nos diz qual é o espaço de Hilbert, que devemos usar para um dado sistema físico. Em geral, não é simples determinar a dimensão do espaço de Hilbert do sistema. No exemplo do spin do elétron, vimos que devemos usar o espaço de Hilbert de dimensão 2, porque só há duas possibilidades resultantes de um experimento para determinar o spin vertical do elétron. Sistemas físicos mais complexos admitem mais possibilidades, que podem ser um número infinito.

2. Um sistema está isolado se ele não influencia e não sofre influência da parte externa a ele. Em princípio, o sistema não precisa ser diminuto, porém é mais fácil isolar os sistemas pequenos com poucos átomos. Na prática, só conseguimos sistemas aproximadamente isolados, logo, o postulado do espaço de estados é uma idealização.

1.2 Evolução Unitária

O objetivo da Física não é simplesmente descrever o estado de um sistema físico em um determinado instante. O objetivo principal é determinar qual é o estado desse sistema no futuro. A teoria permite fazer previsões que podem ser confirmadas ou falseadas por experimentos físicos. Isso é equivalente a determinar quais são as leis dinâmicas a que o sistema obedece. Usualmente, tais leis são descritas por equações diferenciais. Elas governam a evolução temporal do sistema.

1.2.1 Postulado da Evolução

A evolução temporal de um sistema quântico fechado é descrita por uma transformação unitária. Se o estado do sistema quântico no instante t_1 é descrito pelo vetor $|\psi_1\rangle$, o estado do sistema $|\psi_2\rangle$ no instante t_2 está relacionado a $|\psi_1\rangle$ por um operador unitário U, que depende apenas de t_1 e t_2, da seguinte forma:

$$|\psi_2\rangle = U\,|\psi_1\rangle\,. \tag{1.2.3}$$

Observações

1. A ação de um operador unitário sobre um vetor preserva sua norma. Portanto se $|\psi\rangle$ é um vetor unitário, $U|\psi\rangle$ também o será.

2. Um *algoritmo quântico* consiste em uma prescrição de uma sequência de operadores unitários aplicados a uma condição inicial da forma

$$|\psi_n\rangle = U_n \cdots U_1 |\psi_1\rangle .$$

O estado $|\psi_n\rangle$ é medido retornando o resultado do algoritmo.

3. O postulado da evolução pode ser colocado sob a forma de uma equação diferencial, chamada *equação de Schrödinger*. Essa equação fornece um método para se obter o operador U uma vez dado o contexto físico em questão. O objetivo da Física é descrever a dinâmica de sistemas físicos, por isso, a equação de Schrödinger tem um papel fundamental. O objetivo da Ciência da Computação é analisar e implementar algoritmos, logo, o cientista da computação quer saber se é possível implementar de alguma forma um operador unitário previamente escolhido. A forma da Eq. (1.2.3) é conveniente para a área de algoritmos quânticos.

1.3 Sistemas Compostos

O espaço de estados de um *sistema composto* é o *produto tensorial* dos espaços de estados dos componentes. Se $|\psi_1\rangle, \cdots, |\psi_n\rangle$ descrevem os estados de n sistemas quânticos isoladamente, o estado do sistema composto é $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Um exemplo de sistema composto é a memória de um computador quântico de n *qubits*. Usualmente, a memória é dividida em conjunto de qubits, chamado de *registradores*. O espaço de estados da memória do computador é o produto tensorial dos espaços de estados dos registradores que, por sua vez, são obtidos pelo produto tensorial repetido do espaço de Hilbert $\mathbb{C}^2$ de cada *qubit*.

O espaço de estados da memória de um computador quântico de 2 qubits é $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$. Portanto, qualquer vetor unitário de $\mathbb{C}^4$ representa o estado quântico de 2 qubits. Por exemplo, o vetor

$$|0,0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{1.3.4}$$

que pode ser escrito como $|0\rangle \otimes |0\rangle$, representa o estado de 2 elétrons ambos com spin para cima. Interpretação análoga se aplica a $|0,1\rangle$, $|1,0\rangle$ e $|1,1\rangle$. Considere agora o vetor unitário de $\mathbb{C}^4$ dado por

$$|\psi\rangle = \frac{|0,0\rangle + |1,1\rangle}{\sqrt{2}}. \tag{1.3.5}$$

Qual é o estado de spin de cada elétron nesse caso? Para responder a essa pergunta, temos que fatorar $|\psi\rangle$ da seguinte forma:

$$\frac{|0,0\rangle + |1,1\rangle}{\sqrt{2}} = \big(a\,|0\rangle + b\,|1\rangle\,\big) \otimes \big(c\,|0\rangle + d\,|1\rangle\,\big). \tag{1.3.6}$$

Podemos expandir o lado direito e igualar os coeficientes montando um sistema de equações para achar a, b, c e d. O estado do primeiro qubit será $a\,|0\rangle + b\,|1\rangle$ e do segundo $c\,|0\rangle + d\,|1\rangle$. Porém, há um problema: o sistema de equações não tem solução, ou seja, não existem coeficientes a, b, c e d, que satisfaçam à Eq. (1.3.6). Todo estado de um sistema composto que não pode ser fatorado é chamado de *emaranhado*. Esses estados são bem definidos quando olhamos o sistema composto como um todo, porém não podemos atribuir estados para as partes.

1.4 Processo de Medida

Em geral, medir um sistema quântico que se encontra no estado $|\psi\rangle$ visa a obter informações clássicas a respeito desse estado. Na prática, a medida é feita no laboratório usando instrumentos como lasers, magnetos, escalas e cronômetros. Na teoria, descrevemos o processo matematicamente de modo que haja correspondência com o que ocorre na prática. Medir um sistema físico que se encontra em um estado desconhecido, em geral, perturba esse estado de forma irreversível. Não tem como recuperar ou conhecer o estado antes da execução da medida. Se o estado não foi perturbado, então não foi possível obter qualquer informação sobre ele. Matematicamente, a perturbação é descrita por um *projetor*. Se esse projetor for sobre um espaço unidimensional, então diz-se que o estado quântico *projetor* e passa a ser descrito pelo vetor unitário pertencente ao espaço unidimensional. No caso geral, a projeção é sobre um espaço vetorial de dimensão maior que 1, e assim, diz-se que o colapso é parcial ou, no caso extremo, não há alteração no estado quântico do sistema.

1.4.1 Postulado da Medida

Uma *medida projetiva* é descrita por um operador hermitiano O, chamado de *observável*, no espaço de estados do sistema, que está sendo

medido. O observável O tem uma *representação diagonal*

$$O = \sum_{\lambda} \lambda P_{\lambda}, \tag{1.4.7}$$

onde P_λ é o projetor no auto-espaço de O associado ao autovalor λ. Os possíveis resultados da medida correspondem aos autovalores λ do observável. Se o estado do sistema no momento da medida for $|\psi\rangle$, a probabilidade de se obter o resultado λ será

$$p_\lambda = \langle\psi| P_\lambda |\psi\rangle . \tag{1.4.8}$$

Se o resultado da medida for λ, o estado do sistema quântico imediatamente após a medida será

$$\frac{1}{\sqrt{p_\lambda}} P_\lambda |\psi\rangle . \tag{1.4.9}$$

Observações

1. Existe uma correspondência entre a disposição física do aparato de medida em um laboratório de Física e o observável O. Quando um físico experimental faz a medição de um sistema quântico, ele obtém números reais como resultado. Esses números correspondem aos autovalores λ do operador hermitiano O.

2. Os estados $|\psi\rangle$ e $\mathrm{e}^{i\phi}|\psi\rangle$ têm a mesma *estatística de medida*, isto é, a mesma *distribuição de probabilidades* p_λ quando medidos pelo mesmo observável O. O termo $\mathrm{e}^{i\phi}$ multiplicando um estado quântico é chamado de *fase global*.

Como os possíveis resultados de uma medida do estado $|\psi\rangle$ com o observável O obedecem a uma distribuição de probabilidades, podemos definir o valor esperado da medida como

$$\langle O\rangle = \sum_{\lambda} p_\lambda \lambda, \tag{1.4.10}$$

e o desvio padrão como

$$\Delta O = \sqrt{\langle O^2\rangle - \langle O\rangle^2}. \tag{1.4.11}$$

É importante lembrar que a média e o desvio padrão de um observável depende do estado que o sistema físico estava no instante imediatamente anterior a medida.

Exercício 1.1. *Mostre que* $\langle O \rangle = \langle \psi | O | \psi \rangle$.

Exercício 1.2. *Mostre que se o sistema físico está em um estado* $|\psi\rangle$ *que é autovetor de* O*, então* $\Delta O = 0$*, isto é, não há nenhuma incerteza com relação ao resultado da medida com o observável* O*. Qual é o resultado da medida?*

Exercício 1.3. *Mostre que* $\sum_\lambda p_\lambda = 1$ *para qualquer observável* O *e qualquer estado* $|\psi\rangle$*.*

Exercício 1.4. *Suponha que o sistema físico está em um estado* $|\psi\rangle$ *genérico. Mostre que* $\sum_\lambda p_\lambda^2 = 1$ *para um observável* O *se, e somente se* $\Delta O = 0$*.*

1.4.2 Medida na Base Computacional

A *base computacional* do espaço $\mathbb{C}^2$ é o conjunto $\{ |0\rangle, |1\rangle \}$. No caso particular de um qubit, o observável da *medida na base computacional* é a matriz de Pauli Z, cuja decomposição espectral é

$$Z = (+1)P_{+1} + (-1)P_{-1}, \tag{1.4.12}$$

onde $P_{+1} = |0\rangle\langle 0|$ e $P_{-1} = |1\rangle\langle 1|$. Os possíveis resultados da medida são ± 1. Se o estado do qubit é dado pela Eq. (1.1.1), as probabilidades associadas aos possíveis resultados são

$$p_{+1} = |a_0|^2, \tag{1.4.13}$$
$$p_{-1} = |a_1|^2 \tag{1.4.14}$$

e os estados associados logo após a medida serão $|0\rangle$ e $|1\rangle$, respectivamente. A rigor, cada um desses estados têm uma fase global que pode ser descartada. Note que

$$p_{+1} + p_{-1} = 1,$$

pois o estado $|\psi\rangle$ é unitário.

Antes de generalizar para n qubits, é interessante re-analisar o processo de medida de 1 qubit com outro observável dado por

$$O = \sum_{k=0}^{1} k\,|k\rangle\langle k|. \tag{1.4.15}$$

Como os autovalores de O são 0 e 1, toda a análise anterior se mantém se substituirmos $+1$ por 0 e -1 por 1. Com esse observável, existe uma correlação direta entre o resultado da medida e o estado final

do qubit. Se o resultado for 0, o estado após a medida será $|0\rangle$. Se o resultado for 1, o estado após a medida será $|1\rangle$.

A *base computacional* de n qubits na notação decimal é o conjunto $\{\,|0\rangle\,,\cdots,\,|2^n-1\rangle\,\}$. A *medida na base computacional* é feita com o observável

$$O=\sum_{k=0}^{2^n-1} k\,P_k. \tag{1.4.16}$$

onde $P_k=|k\rangle\,\langle k|$. Um estado genérico de n qubits é dado por

$$|\psi\rangle=\sum_{k=0}^{2^n-1} a_k\,|k\rangle\,, \tag{1.4.17}$$

onde as amplitudes a_k satisfazem ao vínculo

$$\sum_k |a_k|^2 \;=\; 1. \tag{1.4.18}$$

A medida tem como resultado um valor inteiro k no intervalo $0\leq k\leq 2^n-1$ com a distribuição de probabilidades dada por

$$\begin{aligned} p_k &= \langle\psi|P_k|\psi\rangle \\ &= \big|\,\langle k|\psi\rangle\,\big|^2 \\ &= |a_k|^2. \end{aligned} \tag{1.4.19}$$

A Eq. (1.4.18) garante que a soma das probabilidades dê 1. O estado dos n qubits imediatamente após a medida é

$$\frac{P_k\,|\psi\rangle}{\sqrt{p_k}}\simeq|k\rangle\,. \tag{1.4.20}$$

O resultado da medida especifica em qual vetor da base computacional o estado $|\psi\rangle$ foi projetado. O resultado não fornece o valor do coeficiente a_k, isto é, de nenhuma das 2^n amplitudes a_k, que descrevem o estado $|\psi\rangle$. Suponha que queiramos encontrar o número k como resultado de um algoritmo. Esse resultado deverá estar codificado como um dos vetores da base computacional, gerador do espaço vetorial, a que o estado $|\psi\rangle$ pertence. Não é conveniente, em princípio, que o resultado em si esteja associado a uma das amplitudes. Se o resultado desejado for um número real não inteiro, então os k dígitos mais significativos deverão ser codificados como um vetor da base computacional. Após uma medida, temos chance de obter uma aproximação para k. Repetindo, as amplitudes do estado quântico em um algoritmo estão associadas às probabilidades de se obter um

resultado e o número que especifica um *ket*, por exemplo o número k de $|k\rangle$, é um possível resultado do algoritmo.

A descrição do processo de medida usando o observável (1.4.16) é equivalente a medidas simultâneas ou em cascata dos qubits com o observável Z. Os possíveis resultados da medida com Z são ± 1. Medidas simultâneas ou em cascata de n qubits resultam numa sequência de n componentes ± 1. Por exemplo, para $n = 3$ qubits podemos ter $(-1, +1, +1)$. A relação de um resultado da medida desse tipo, como o que foi descrito anteriormente, é obtida substituindo-se cada resultado $+1$ por 0 e -1 por 1. Teremos, então, um número binário que pode ser convertido para base decimal fornecendo um dos valores k. No caso do exemplo com o resultado $(-1, +1, +1)$, obtemos 100, que corresponde ao número 4. O estado, logo após a medida, será dado pela aplicação do projetor

$$\begin{aligned} P_{-1,+1,+1} &= |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\ &= |1,0,0\rangle\langle 1,0,0| \end{aligned} \tag{1.4.21}$$

no estado do sistema de 3 qubits seguido da *renormalização*. A renormalização, nesse caso, equivale a substituir o coeficiente por 1. O estado após a medida será $|1,0,0\rangle$. Portanto, numa medida usando a base computacional, seja com o observável (1.4.16), seja como operadores Z, podemos falar que o resultado foi $|1,0,0\rangle$, pois automaticamente sabemos que os autovalores de Z em questão são $(-1, +1, +1)$.

Uma medida simultânea com n observáveis Z não é equivalente a uma medida com o observável $Z \otimes \cdots \otimes Z$. A medida com esse último observável retorna um único valor, que pode ser $+1$ ou -1, enquanto que com n observáveis Z, simultaneamente ou não, temos n valores ± 1. A medida em cascata é feita com os observáveis $Z \otimes I \otimes \cdots I$, $I \otimes Z \otimes \cdots I$, e assim por diante. Usualmente, empregamos uma notação mais compacta, Z_1, Z_2, sucessivamente, onde Z_1 quer dizer que o observável Z foi usado para o qubit 1 e o operador identidade para os qubits restantes.

Exercício 1.5. *Suponha que o estado de um qubit seja* $|1\rangle$.

1. *Se uma medida é feita com o observável* X*, qual é o valor médio de* X *e qual é o desvio padrão?*

2. *Se uma medida é feita com o observável* Z*, qual é o valor médio de* X *e qual é o desvio padrão?*

1.4.3 Medida Parcial na Base Computacional

Suponha que o estado de 2 qubits é dado por

$$|\psi\rangle = \frac{3}{5\sqrt{2}}\,|0,0\rangle - \frac{3\,i}{5\sqrt{2}}\,|0,1\rangle + \frac{2\sqrt{2}}{5}\,|1,0\rangle - \frac{2\sqrt{2}\,i}{5}\,|1,1\rangle\,. \quad (1.4.22)$$

Pelo método descrito na seção anterior, concluímos que a probabilidade de obtermos o resultado $|0,0\rangle$ após uma medida do estado $|\psi\rangle$ na base computacional é 9/50.

O termo *medida na base computacional* de n qubits subentende uma medida de todos os qubits. No entanto, existe a possibilidade de uma *medida parcial*, ou seja, medir uma parte dos qubits, cada um com o observável Z em cascata ou simultaneamente. O resultado, nesse caso, não é necessariamente um estado da base computacional. Por exemplo, medindo apenas o segundo qubit do estado $|\psi\rangle$ da Eq. (1.4.22) podemos obter o resultado 0 com probabilidade 1/2 ou 1 também com probabilidade 1/2. No primeiro caso, o estado logo após a medida será

$$\left(\frac{3}{5}\,|0\rangle + \frac{4}{5}\,|1\rangle\right) \otimes |0\rangle$$

e no segundo caso, o estado será

$$\left(\frac{3}{5}\,|0\rangle + \frac{4}{5}\,|1\rangle\right) \otimes |1\rangle\,.$$

Somente os qubits que sofreram a medição são projetados na base computacional.

Se tivermos um sistema composto dos subsistemas A e B, uma medida parcial será feita com um observável da forma $I_A \otimes O_B$, onde I_A é o operador identidade do sistema A e O_B é um observável do sistema B. Fisicamente, isso quer dizer que o aparato de medida interagiu apenas com o subsistema B. Equivalentemente, o observável $O_A \otimes I_B$ também faz uma medida parcial interagindo apenas com o subsistema A.

Se tivermos um registrador de m qubits junto com um registrador de n qubits, poderemos representar a base computacional na forma compacta $\big\{\,|i,j\rangle : 0 \le i \le 2^m - 1,\ 0 \le j \le 2^n - 1\big\}$, onde tanto i como j estarão representados na base decimal. Um estado genérico será representado por

$$|\psi\rangle = \sum_{i=0}^{2^m-1} \sum_{j=0}^{2^n-1} a_{ij}\,|i,j\rangle\,. \quad (1.4.23)$$

Suponha que meçamos todos os qubits do segundo registrador, a probabilidade de se obter o valor $0 \leq k \leq 2^n - 1$ é

$$\begin{aligned} p_k &= \langle\psi| \left(I \otimes P_k\right) |\psi\rangle \\ &= \sum_{i=0}^{2^m-1} |a_{ik}|^2 . \end{aligned} \tag{1.4.24}$$

O conjunto $\left\{p_1, \cdots, p_{2^n-1}\right\}$ é uma distribuição de probabilidades, que satisfaz a

$$\sum_{k=0}^{2^n-1} p_k = 1. \tag{1.4.25}$$

Se o resultado da medida for k, o estado logo após será

$$\frac{1}{\sqrt{p_k}} \left(I \otimes P_k\right) |\psi\rangle = \frac{1}{\sqrt{p_k}} \left(\sum_{i=0}^{2^m-1} a_{ik} |i\rangle \right) |k\rangle . \tag{1.4.26}$$

Sugestões para Leitura

A quantidade de bons livros de Mecânica Quântica é muito grande. Para um contato inicial, sugerimos as Refs. [8, 16, 18]; para uma abordagem mais completa sugerimos a Ref. [5]; para quem está interessado apenas na aplicação da Mecânica Quântica na Computação Quântica, sugerimos as Refs. [14, 17, 13]; para uma abordagem mais conceitual, sugerimos as Refs. [15, 6].

Capítulo 2

Correção Quântica de Erros

A teoria dos *códigos quânticos* de correção de erros estende as noções básicas do *códigos clássicos* de correção de erros. Uma diferença marcante reside no fato do que os erros quânticos estão muito mais presentes do que no caso clássico. Não é possível implementar um hardware quântico sem lidar com correções de erros. Os *estados quânticos* facilmente entram em *descoerência* devido a influências do *sistema macroscópico* sobre o sistema quântico. A correção de erros é possível quando armazenamos a informação quântica de forma redundante. Os métodos quânticos servem tanto para garantir o funcionamento correto dos algoritmos quânticos como para enviar mensagens codificadas por um canal quântico de forma mais resistentes a erros.

2.1 Modelo Padrão

Vamos supor que Alice quer enviar uma mensagem para Beto através de um canal, que não é perfeito. No caso clássico, Alice teria uma mensagem composta de um string de caracteres binários. O modelo mais simples de canal clássico, que é chamado de simétrico, admite um probabilidade de erro p do bit 0 ser convertido para o bit 1 e vice-versa. Alice codifica a mensagem usando redundância e envia pelo canal, um bit de cada vez. Beto recebe um string que pode ter sido adulterado, ele faz a *análise de síndrome* para determinar se houve erro e tenta recuperar a mensagem original. Se a probabilidade p for suficientemente pequena ou se a redundância usada na codificação for suficientemente grande, Beto pode ter sucesso em recuperar a mensagem completamente. Os bons códigos maximizam a chance de sucesso sem usar um excesso de redundância.

A *codificação* mais simples replica os bits originais da seguinte forma: $0 \to 0_L$ onde $0_L = 000$ e $1 \to 1_L$ onde $1 = 111$. A mensagem triplica de tamanho. Beto recebe a mensagem codificada, verifica quais blocos de 3 bits não tem o formato 000 ou 111 e usa o método de "voto de maioria" para corrigir os bits "errados". Após a codificação, a probabilidade de ocorrer um erro nos bits lógicos 0_L ou 1_L é quadraticamente menor.

No caso quântico, Alice vai usar *bits quânticos* (qubits) para escrever a mensagem. Ela pode usar tanto os estados $|0\rangle$ e $|1\rangle$ como estados em superposição $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. A mensagem é enviada pelo canal quântico, um qubit de cada vez. Um possível erro que pode acontecer no canal é *inversão de qubit*: $|0\rangle \to |1\rangle$ e vice-versa. Mas esse não é o único tipo de erro. A *inversão de fase*, $|0\rangle \to |0\rangle$ e $|1\rangle \to -|1\rangle$, é tão problemática quanto a inversão de qubit. Por exemplo, se o qubit da mensagem for $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, após a inversão de fase, o qubit é transformado no estado $|\psi'\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, que é ortogonal ao primeiro.

No caso geral (simétrico), o erro é da forma

$$|0\rangle \to E\,|0\rangle\,,$$
$$|1\rangle \to E\,|1\rangle\,,$$

onde E é um operador genérico de 1 qubit. Note que há um continuum de possibilidades. Alice deve codificar a mensagem e enviar pelo canal quântico. Beto deve medir cada qubit que for recebendo, ou esperar e formar blocos antes de medir. Essas medições devem ter o intuito de detectar os erros para corrigí-los e reproduzir a mensagem original. A mensagem original não deve ser destruída no processo de medição. Isso tem que ser feito criteriosamente, pois sabemos que, no caso geral, medidas perturbam o estado quântico. Temos que obter informações apenas sobre os erros e não sobre a mensagem original. Após ter em mãos a mensagem original, Beto pode dar o destino que quiser à mensagem.

2.2 Código de 3 Qubits

O exemplo mais simples de um código quântico é o *código de 3 qubits* para corrigir inversão de 1 qubit. Suponha que um qubit da mensagem seja $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. A codificação visa substituir os qubits $|0\rangle$ e $|1\rangle$ por

$$\begin{aligned} |0\rangle &\to |0_L\rangle = |000\rangle \\ |1\rangle &\to |1_L\rangle = |111\rangle\,. \end{aligned}$$

Esse código corrige no máximo um erro de inversão de qubit nos estados lógicos $|0_L\rangle$ e $|1_L\rangle$.

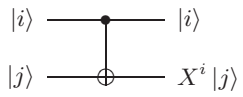

Figura 2.1: Circuito da porta CNOT. As variáveis i e j assumem os valores 0 ou 1. X é a matriz de Pauli que inverte qubits.

A porta CNOT é a porta adequada para replicar os qubits $|0\rangle$ e $|1\rangle$. O funcionamento do CNOT está descrito na Fig. 2.1. O primeiro qubit (inicialmente no estado $|i\rangle$) é o controle e o segundo qubit (inicialmente no estado $|j\rangle$) é o alvo. Se o valor de i for 0, a saída será igual a entrada. Se o valor de i for 1, o controle é ativado e a saída do qubit alvo será modificada pela *matriz de Pauli* X. O funcionamento da porta foi descrito para a *base computacional*. A linearidade deve ser usada para se obter a saída quando a entrada são estados em superposição. A porta CNOT é um operador unitário cuja representação matricial é

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.2.1}$$

Pela Fig. 2.1, vemos que se $j = 0$, a saída será $|i\rangle\,|i\rangle$. Portanto, a porta CNOT faz uma cópia do estado do primeiro registrador, quando ele é um estado da base computacional. Se colocarmos o estado $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ como entrada para o qubit de controle e o estado $|0\rangle$ como entrada para o qubit alvo, obtemos a saída $a\,|00\rangle + b\,|11\rangle$ por linearidade.

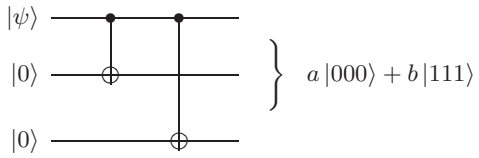

Figura 2.2: Circuito para a codificação de 3 qubits.

Para fazer a codificação de 3 qubits, usamos duas portas CNOTs como no circuito da Fig. 2.2. Esse circuito faz a substituição dos

estados $|0\rangle$ e $|1\rangle$ do estado original para os estados $|0_L\rangle$ e $|1_L\rangle$. A *decodificação* é feita com o circuito transposto conjugado, que nesse caso coincide com o circuito original.

Após o estado $|\psi\rangle$ ser codificado, Alice envia os 3 qubits pelo canal quântico para Beto. Esse qubits podem ser enviados um por vez. Note que $|\psi\rangle$ está *emaranhado* no caso geral. Não há problemas em enviar os qubits separadamente, pois o *emaranhamento* é preservado mesmo quando os qubits estão afastados uns dos outros. Em geral, os canais têm todo tipo de imperfeição, porém vamos supor que ocorre apenas inversão de qubit no máximo em um dos qubits.

Beto recebe os qubits e faz a análise de síndrome fazendo medidas em cascata com os *observáveis* Z_1Z_2 e Z_2Z_3. A decomposição de Z_1Z_2 em projetores é

$$Z_1Z_2 = P_+ - P_-, \tag{2.2.2}$$

onde

$$P_+ = |00\rangle\langle 00| + |11\rangle\langle 11| \tag{2.2.3}$$
$$P_- = |01\rangle\langle 01| + |10\rangle\langle 10|. \tag{2.2.4}$$

A probabilidade de medida retornar os valores ± 1 são $p_\pm = \langle\psi|P_\pm|\psi\rangle$, respectivamente. O observável Z_1Z_2 retorna $+1$ se os valores dos 2 primeiros qubits forem iguais e -1 se forem diferentes, análogo para Z_2Z_3 com relação aos 2 últimos qubits. Se não houve nenhuma inversão de qubits, ambas medidas retornam $+1$. Se houve inversão do primeiro qubit, a primeira medida retorna -1 e a segunda $+1$. Se houve inversão do segundo qubit, ambas medidas retornam -1. Finalmente, se houve inversão do terceito qubit, a primeira medida retorna $+1$ e a segunda -1.

A correção é feita aplicando-se a matriz de Pauli X no qubit invertido. A etapa final é a decodificação, que é feita com o mesmo circuito da codificação. Beto deve descartar os dois qubits auxiliares. O qubit restante estará no estado $|\psi\rangle$, como preparado por Alice.

2.3 Códigos Lineares Clássicos

Um código $\mathcal{C}$ linear binário (n, k) é obtido como imagem de uma *transformação linear injetiva* $\Phi : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^n$ tal que

$$\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} \mapsto G_{n\times k} \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}.$$

$G_{n\times k}$ é a *matriz geradora* do código $\mathcal{C}$, que tem posto k. As colunas de G são linearmente independentes e geram o subespaço $\mathcal{C}$ de dimensão 2^k em $\mathbb{Z}_2^n$. Isto é, o código tem 2^k *palavras binárias* de comprimento n, que codificam as palavras originais que tinham k bits.

A matriz geradora não é única, pois podemos fazer uma mudança de base no subespaço $\mathcal{C}$. A apresentação canônica de G é da forma

$$G = \begin{bmatrix} I_{k\times k} \\ B_{(n-k)\times k} \end{bmatrix}. \tag{2.3.5}$$

Nesse caso, a codificação de uma palavra $(a_1, \cdots, a_k)$ é da forma

$$G_{n\times k} \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_k \\ h_1 \\ \vdots \\ h_{n-k} \end{pmatrix},$$

onde $h_1, \cdots, h_{n-k}$ são combinações lineares das primeiras coordenadas. Em particular, a codificação da palavra $\mathbf{e}_j = (0, \cdots, 1, \cdots, 0)$ com um único 1 na j-ésima posição é a j-ésima coluna de G.

A *matriz verificadora* é da forma

$$H_{(n-k)\times n} = \begin{bmatrix} B_{(n-k)\times k} & I_{(n-k)\times(n-k)} \end{bmatrix}. \tag{2.3.6}$$

$H_{(n-k)\times n}$ é uma matriz capaz de detectar se um vetor $\mathbf{v} \in \mathbb{Z}_2^n$ é uma palavra do código ou não, pois

$$H\mathbf{v}^T = 0,$$

se, e somente se, $\mathbf{v}$ está no código. Isso se deve ao fato de que as colunas de G geram os vetores de $\mathcal{C}$ enquanto que as linhas de H geram os vetores do espaço ortogonal $\mathcal{C}^\perp$. Usando as Eqs. (2.3.5) e (2.3.6), podemos verificar que $H\,G = 0$. A matriz H serve também como análise de síndrome, como veremos na próxima seção em um caso particular.

2.3.1 Códigos de Hamming

Os *códigos de Hamming* $\mathcal{H}_r$ são *códigos lineares clássicos* do tipo $(2^r-1, 2^r-r-1, 3)$ para inteiros r positivos, portanto são subespaços de $\mathbb{Z}_2^{2^r-1}$. A *matriz de paridade* tem como colunas os elementos não nulos de $\mathbb{Z}_2^r$. Por exemplo, para $r = 3$

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Escolhemos a ordem dos números de forma que H ficasse na forma canônica descrita na Eq. (2.3.6). Usando a Eq. (2.3.5) obtemos a seguinte matriz geradora:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Como G tem 4 colunas, o número total de palavras é 16. Fazendo todas as combinações lineares possíveis, obtemos

0000000	0001111	0010110	0011001
0100101	0101010	0110011	0111100
1000011	1001100	1010101	1011010
1100110	1101001	1110000	1111111

Tirando a palavra 0000000, todas as outras tem peso maior ou igual a 3, portanto a distância do código é 3.

Esse código é do tipo $(7, 4, 3)$. Como a distância é 3, ele consegue detectar erros em até duas letras e corrigir erros em até uma letra da palavra. Suponha que o erro tenha ocorrido no j-ésimo bit da palavra. Se a palavra do código era $\mathbf{v}$, ela passou a ser $\mathbf{v} + \mathbf{e}_j$. Aplicando H na palavra modificada e usando que $H\mathbf{v} = 0$, obtemos $H\mathbf{e}_j$. Como $H\mathbf{e}_j$ é a j-ésima coluna de H, por inspeção da matriz H, podemos determinar qual é a posição da coluna em questão e, portanto, determinar qual bit foi modificado.

Esse código tem uma propriedade interessante: para cada palavra do código, existem 7 strings de 7 bits que têm distância 1 da palavra selecionada. Todos esses strings não pertencem ao código. Esses 7 strings junto com a palavra do código formam uma bola de 8 elementos. Existem 16 bolas com interseção vazia 2-a-2 e que cuja união cobre todos os 2^7 strings possíveis. Um código com esta propriedade se chama *perfeito*.

Para qualquer código linear $\mathcal{C}$ com matriz geradora G, podemos definir um *código dual* $\mathcal{C}^\perp$, cuja matriz de paridade é $H^\perp = G^T$. As palavras do código dual são ortogonais a todas palavras do código original. Apesar dessa disso, pode acontecer que $C^\perp \subseteq C$. Nesse caso, o código é chamado de *auto-dual*. Os duais dos códigos de Hamming são códigos auto-duais. Vamos definir $H' = G^T$ e $G' = H^T$. Como $HG = 0$, segue que $H'G' = 0$. Portanto, a matriz geradora

do código dual é H^T. Fazendo todas as combinações lineares das colunas, obtemos

$$\begin{array}{cccc} 0000000 & 0001111 & 0110011 & 0111100 \\ 1010101 & 1011010 & 1100110 & 1101001 \end{array}$$

O novo código é do tipo (7,3,4). Ele não é um *código perfeito*. Podemos verificar que todas as palavras de $\mathcal{C}^{\perp}$ estão em $\mathcal{C}$. Portanto, $C^{\perp} \subseteq C$, confirmando que o código dual ao código de Hamming é auto-dual.

2.4 Códigos Quânticos CSS

Os *códigos de Calderbank-Shor-Steane* (CSS) formam uma ampla classe de códigos quânticos que são construídos a partir dos *códigos lineares clássicos*. Eles pertencem a uma classe mais geral dos *códigos quânticos estabilizadores*. A estrutura desses códigos pode ser entendida através de um caso particular. Vamos tomar como base o código de Hamming (7,4,3) descrito na seção anterior. Os códigos CSS são construídos usando dois códigos lineares clássicos, $\mathcal{C}_1$ e $\mathcal{C}_2$, tal que $\mathcal{C}_2 \subseteq \mathcal{C}_1$. Vamos tomar $\mathcal{C}_1$ como o código de Hamming $(7, 4, 3)$ e $\mathcal{C}_2$ como o código dual $(7, 3, 4)$. O código quântico resultante será do tipo $[7, 1, 3]$.

Os códigos lineares clássicos têm a estrutura do espaço vetorial $\mathbb{Z}_2^n$. No contexto quântico, esse códigos são imersos em um espaço de Hilbert e passam a ser um espaço vetorial $\mathbb{C}_2^n$. As palavras do código podem ser colocadas em superposição formando um estado quântico, que não poderia ser implementado diretamente em um computador clássico, porém é tratado eficientemente em um computador quântico. Em particular, vamos definir o estado quântico $|\mathcal{C}_2\rangle$ da seguinte forma:

$$|\mathcal{C}_2\rangle = \frac{1}{\sqrt{\mid \mathcal{C}_2 \mid}} \sum_{x \in \mathcal{C}_2} |x\rangle \,, \tag{2.4.7}$$

isto é, $|\mathcal{C}_2\rangle$ é a superposição quântica normalizada de todas as palavras do código $\mathcal{C}_2$.

Um código linear $\mathcal{C}$, além de ter a estrutura do espaço de Hilbert $\mathbb{C}_2^n$, tem também uma estrutura de grupo. A palavras do código $\mathcal{C}$ formam um *grupo Abeliano* com a operação de soma binária bit-a-bit (XOR). O código $\mathcal{C}_2$ é portanto um subgrupo do código $\mathcal{C}_1$. O estado $|\mathcal{C}_2\rangle$ é a superposição de todos os elementos do subgrupo $\mathcal{C}_2$. Podemos agora definir a superposição de todos elementos de uma *classe lateral*

de $\mathcal{C}_2$ em $\mathcal{C}_1$. Seja $y \in \mathcal{C}_1$. Vamos definir

$$|\mathcal{C}_2 + y\rangle = \frac{1}{\sqrt{|\ \mathcal{C}_2\ |}} \sum_{x \in \mathcal{C}_2} |x + y\rangle\,, \tag{2.4.8}$$

onde $C_2 + y$ é a classe lateral de $\mathcal{C}_2$ em $\mathcal{C}_1$ que contém y. Como todas as classes laterais tem a mesma cardinalidade, devemos usar a mesma normalização.

Os códigos CSS($\mathcal{C}_1$, $\mathcal{C}_2$) sobre os códigos lineares clássicos $\mathcal{C}_1$ e $\mathcal{C}_2$, (n, k_1) e (n, k_2) respectivamente, são códigos quânticos do tipo $[n, k1 - k2]$ gerados pelos estados quânticos das classes laterais de $\mathcal{C}_2$ em $\mathcal{C}_1$. O *índice* (número de classes laterais) de $\mathcal{C}_2$ em $\mathcal{C}_1$ é $|\mathcal{C}_1|/|\mathcal{C}_2|$, isto é, $2^{k_1 - k_2}$.

2.4.1 Código de Steane

No exemplo onde $\mathcal{C}_1$ é o código de Hamming $(7, 4, 3)$ e $\mathcal{C}_2$ é o código dual $(7, 3, 4)$, o código quântico CSS é do tipo $[7, 1, 3]$, tem dimensão 2 e os estados lógicos são

$$\begin{aligned} |0_L\rangle &= \frac{1}{2\sqrt{2}}\big(\,|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle + \\ &\quad |1010101\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle\,\big) \end{aligned}$$

e

$$\begin{aligned} |1_L\rangle &= \frac{1}{2\sqrt{2}}\big(\,|1111111\rangle + |1110000\rangle + |1001100\rangle + |1000011\rangle + \\ &\quad |0101010\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle\,\big). \end{aligned}$$

Esse código é conhecido como *código de Steane*. Ele detecta e corrige um erro genérico em 1 qubit. A análise de síndrome é feita através de uma medição em cascata com os seguintes 6 observáveis: $X_4X_5X_6X_7$, $X_2X_3X_6X_7$, $X_1X_3X_5X_7$, $Z_4Z_5Z_6Z_7$, $Z_2Z_3Z_6Z_7$, $Z_1Z_3Z_5Z_7$. A explicação do porquê esses observáveis fazem a análise de síndrome vem do uso do formalismo estabilizador, que será tratado na próxima seção. Sem o formalismo estabilizador, a análise do processo é extremamente trabalhosa e particular para esse código em questão. Para dar pelo menos uma intuição do porquê o processo funciona, vamos considerar um caso particular de erro: inversão de 1 qubit.

Uma palavra genérica enviada por Alice para Beto no canal quântico é da forma $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. A codificação é feita com um operador unitário que obedece

$$\begin{aligned} U_{\text{cod}}\,|0000000\rangle &= |0_L\rangle\,, \\ U_{\text{cod}}\,|1000000\rangle &= |1_L\rangle\,. \end{aligned}$$

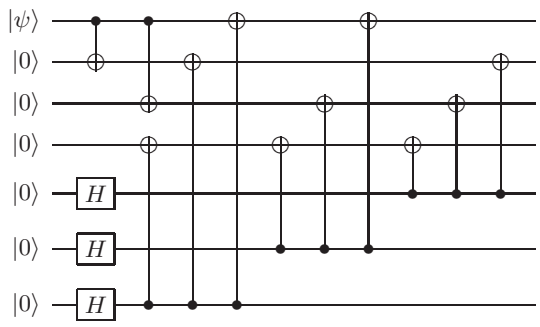

Figura 2.3: Circuito de codificação do código de Steane.

O operador U_{cod} está especificado na Fig. 2.3 em termos das portas elementares universais H e CNOT. Após a codificação, o estado $|\psi_{\text{cod}}\rangle = a\,|0_L\rangle + b\,|1_L\rangle$ é enviado pelo canal quântico. Se ocorrer a inversão de qubit no primeiro qubit, Beto vai receber o estado $|\psi'\rangle = aX_1\,|0_L\rangle + bX_1\,|1_L\rangle$, onde

$$\begin{aligned} X_1\,|0_L\rangle &= \frac{1}{2\sqrt{2}}\big(\,|1000000\rangle + |1001111\rangle + |1110011\rangle + |1111100\rangle + \\ &\quad |0010101\rangle + |0011010\rangle + |0100110\rangle + |0101001\rangle\,\big) \end{aligned}$$

e

$$\begin{aligned} X_1\,|1_L\rangle &= \frac{1}{2\sqrt{2}}\big(\,|0111111\rangle + |0110000\rangle + |0001100\rangle + |0000011\rangle + \\ &\quad |1101010\rangle + |1100101\rangle + |1011001\rangle + |1010110\rangle\,\big). \end{aligned}$$

O estado $|\psi'\rangle$ é ortogonal ao código quântico, pois ele é ortogonal tanto a $|0_L\rangle$ como a $|1_L\rangle$. Além disso, dois erros em qubits distintos, por exemplo $X_1\,|\psi_{\text{cod}}\rangle$ e $X_2\,|\psi_{\text{cod}}\rangle$, também estão associados a espaços ortogonais entre si. Quando erros distintos são levados em espaços ortogonais, se diz que os erros são distinguíveis. O que temos que fazer é o seguinte: escolhemos um observável cuja decomposição em projetores coincide exatamente com os projetores nesses espaços ortogonais. Uma medida com esse observável vai permitir Beto identificar se o estado recebido está com problemas, isto é, se é ortogonal ao código e mais que isso, vai permitir identificar para qual dos espaços ortogonais ao código a mensagem corrompida foi enviada. A partir dessa informação, Beto pode aplicar a correção no qubit correto. Note que há espaço de sobra ortogonal ao código quântico para todos possíveis erros de inversão em 1 qubit. A análise completa de todas as possibilidades será feita na próxima seção usando um formalismo bem mais poderoso, chamado formalismo estabilizador.

Sugestões para Leitura

Um excelente referência para uma introdução aos códigos clássicos é [12]. Para uma rápida introdução aos códigos quânticos, sugerimos a Ref. [11]. A Ref. [14] também é muito útil. Os primeiros trabalhos que apareceram na literatura sobre códigos quânticos foram [19] e [20]. Os códigos CSS foram introduzidos nas Refs. [4] e [21].

Capítulo 3

Códigos Baseados no Formalismo Estabilizador

O *formalismo estabilizador* é um método de expressar estados quânticos por um conjunto de operadores do *grupo de Pauli*. Tanto a descrição da *evolução quântica* como da *medida quântica* devem ser adaptadas a esse formalismo. No entanto, o método não é totalmente geral, pois nem todos os *estados quânticos* podem ser expressos em termos do formalismo estabilizador. Os *códigos aditivos quânticos*, generalização dos *códigos lineares clássicos*, podem ser totalmente expressos em termos do formalismo estabilizador.

Vamos destacar alguns fatos que serão importantes para a aplicação do formalismo estabilizador para a descrição dos códigos estabilizadores. As provas para esses fatos podem ser encontradas nas referências.

3.1 Formalismo Estabilizador

Vamos começar descrevendo o formalismo estabilizador com um exemplo. Considere o seguinte estado da *base de Bell*:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Esse estado satisfaz

$$\begin{aligned} X_1 X_2 |\psi\rangle &= |\psi\rangle\,, \\ Z_1 Z_2 |\psi\rangle &= |\psi\rangle\,. \end{aligned}$$

Nesse caso, diz-se que o estado $|\psi\rangle$ é *estabilizado* tanto pelo operador $X_1X_2 = X \otimes X$ como por $Z_1Z_2 = Z \otimes Z$. A menos de uma fase global, o estado $|\psi\rangle$ é o único *estado estabilizado* pelos operadores X_1X_2 e

Z_1Z_2. A ideia do formalismo é descrever o estado $|\psi\rangle$ pelo conjunto $\{X_1X_2,\ Z_1Z_2\}$. Esta opção pode parecer estranha a primeira vista, porém veremos que há uma enorme economia na descrição do sistema físico e da sua evolução.

O poder do formalismo estabilizador reside em alguns fatos básicos da Teoria de Grupos. Em particular, se um grupo G tem $|G|$ elementos, então é possível achar um *conjunto gerador* com no máximo $\lceil \log_2 |G| \rceil$ elementos. No caso do formalismo estabilizador, o grupo é questão é o *grupo de Pauli* G_n, onde n é o número de qubits. Para um qubit, o grupo de Pauli é

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}. \tag{3.1.1}$$

É fácil de verificar que este conjunto satisfaz as propriedades de fechamento, existência de elemento neutro ($I_{2\times 2}$), associatividade e existência de elemento inverso (próprio elemento ou o negativo do elemento) com relação ao produto usual de matrizes. Quando passamos para 2 qubits, o grupo G_2 é obtido tomando o produto tensorial dos elementos de G_1, isto é

$$G_2 = \{\pm I\otimes I, \pm iI\otimes I, \pm I\otimes X, \pm iI\otimes X, \pm I\otimes Y, \cdots, \pm iZ\otimes Z\}. \tag{3.1.2}$$

No caso geral de n qubits, os elementos do grupo G_n são produtos tensoriais de n matrizes de Pauli com fatores multiplicativos ± 1 e $\pm i$. Daqui para frente vamos tomar n como o número de qubits em questão.

Um conjunto estabilizador, que vamos denotar por S, é um subgrupo comutativo do grupo de Pauli G_n que não contenha $-I$. O conjunto S tem um espaço vetorial associado, denotado por V_S. V_S consiste dos vetores do espaço de Hilbert $\mathcal{H}$ de n qubits que são estabilizados por todos elementos de S. V_S é um subespaço de $\mathcal{H}$. Esta definição é coerente pois se $|\psi_1\rangle$ e $|\psi_2\rangle$ são estabilizados por S, então uma combinação linear de $|\psi_1\rangle$ e $|\psi_2\rangle$ também é estabilizada por S.

Fato 1

Se $-I \in S$, então V_S é o espaço vetorial trivial gerado pelo vetor nulo.

O Fato 1 é verdadeiro porque o único vetor estabilizado por $-I$ (um vetor $|\psi\rangle$ tal que $|\psi\rangle = -|\psi\rangle$) é o vetor nulo. Por isso assumimos que $-I \notin S$. Segue como consequência que $\pm iI \notin S$.

Fato 2

Seja S um subgrupo não-comutativo de G_n. Então, V_S é o espaço vetorial trivial gerado pelo vetor nulo.

Uma segunda exigência para que V_S não ser o espaço vetorial nulo é que S seja um subgrupo comutativo. As matrizes de Pauli obedecem às seguintes propriedades: duas matrizes de Pauli comutam ou anti-comutam. Não existe outra opção. Se S não for um grupo comutativo, deve existir g_1 e g_2 tal que $g_1 g_2 = -g_2 g_1$. Usando este fato podemos mostrar que se $g_1, g_2 \in S$ e $g_1 g_2 = -g_2 g_1$ então $g_1 g_2 |\psi\rangle = -g_2 g_1 |\psi\rangle$ e, portanto, $|\psi\rangle = -|\psi\rangle$. Por isso assumimos que S seja comutativo.

Fato 3

Seja $S = \langle g_1, \cdots, g_{n-k} \rangle$, para algum $0 \leq k < n$, isto é, S é gerado por $n-k$ elementos do grupo de Pauli G_n. Então, V_S é um espaço vetorial de dimensão 2^k.

A demonstração do Fato 3 é trabalhosa. Ela pode ser encontrada nas referências. A compreensão desse fato é fundamental para verificarmos a consistência do que se segue. Note que, quanto menos elementos tiver o conjunto gerador de S, maior será a dimensão do espaço vetorial V_S. Para representar um estado por S, o espaço vetorial V_S deve ter dimensão 1. Portanto, o conjunto gerador de S deve ter n elementos.

Uma outra maneira de visualizar V_S é pela interseção dos espaços vetoriais associados a cada elemento do conjunto gerador de S. Isto é, tome o primeiro elemento g_1 e descubra qual é o espaço estabilizado por este elemento. A dimensão do espaço vetorial V_{g_1} é 2^{n-1}. Faça isso para os outros elementos, e tome a interseção:

$$V_S = V_{g_1} \cap \cdots \cap V_{g_{n-k}}. \tag{3.1.3}$$

Por exemplo, para $n = 3$, tome $S = \langle g_1, g_2 \rangle$ onde $g_1 = Z_1 Z_2$, $g_2 = Z_2 Z_3$. Portanto, $S = \{I_{8\times 8}, Z_1 Z_2, Z_2 Z_3, Z_1 Z_3\}$. Vamos determinar V_{g_1}. Por inspeção, descobrimos que $|000\rangle$, $|001\rangle$, $|110\rangle$ e $|111\rangle$ são estabilizados por g_1. Pelo Fato 2, V_{g_1} tem dimensão 4, portanto acabamos de determinar uma base para esse espaço vetorial. Analogamente, os vetores $|000\rangle$, $|011\rangle$, $|100\rangle$ e $|111\rangle$ formam uma base para V_{g_2}. Tomando a interseção, obtemos que $|000\rangle$ e $|111\rangle$ formam uma base para V_S.

3.2 Portas Unitárias no Formalismo Estabilizador

Quando descrevemos espaços vetoriais usando o formalismo estabilizador, estamos lidando com o postulado do espaço de estados da Mecânica Quântica. O próximo passo é descrever as operações dinâmicas. O postulado da evolução dinâmica afirma que se no instante inicial o sistema físico é descrito pelo estado $|\psi\rangle$, então, após a evolução, o estado será descrito por $U|\psi\rangle$, para algum operador unitário U, que depende dos processos físicos em questão. No formalismo estabilizador, representamos os *estados quânticos* por subgrupos S do *grupo de Pauli* G_n. Após a evolução, temos que descrever o sistema físico por um novo subgrupo do grupo de Pauli. A questão é como determinar esse novo subgrupo conhecendo-se S e U.

Suponha que aplicamos um operador unitário U sobre um espaço vetorial V_S que é estabilizado pelo grupo S. Seja $|\psi\rangle$ um estado de V_S. Então para qualquer elemento $g \in S$

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle\,. \tag{3.2.4}$$

Isso mostra que $U|\psi\rangle$ é estabilizado por $UgU^\dagger$. Portanto, se $|\psi\rangle$ é estabilizado por S, $U|\psi\rangle$ é estabilizado por $USU^\dagger := \{UgU^\dagger,\ g \in S\}$. Além disso, se $g_1, \cdots, g_k$ gera S, então $Ug_1U^\dagger, \cdots, Ug_kU^\dagger$ gera $USU^\dagger$. Estas observações mostram completamente como caracterizar a evolução unitária no formalismo estabilizador. Se no instante inicial, o estado quântico é descrito por S, então no instante posterior, após a evolução, o estado será descrito por $USU^\dagger$, que é uma *operação de conjugação* de cada elemento de S.

Dado um *grupo estabilizador* no instante inicial, sabemos como calcular o grupo estabilizador após a evolução descrita por um operador unitário genérico U. Porém, pode ocorrer um problema nesse ponto. O formalismo estabilizador não é totalmente genérico. Ele não pode substituir completamente o formalismo usual baseado em vetores do espaço de Hilbert, pois existem estados que não são estabilizados por nenhum elemento do grupo de Pauli, a não ser pela identidade. Por exemplo,

$$|\psi\rangle = \frac{|0\rangle + \mathrm{e}^{i\frac{\pi}{4}}|1\rangle}{\sqrt{2}} \tag{3.2.5}$$

não é estabilizado por nenhuma das matrizes da Eq. (3.1.1), exceto pela identidade. Portanto, para usar o formalismo estabilizador, temos que iniciar o processo com um estado que pode ser estabilizado por algum subgrupo S. A princípio isso não é uma restrição séria,

pois podemos iniciar o processo com um estado da base computacional e depois gerar estados mais complexos através de operadores unitários. No entanto, se o operador U gerar um estado que não pode ser estabilizado por nenhum elemento do grupo de Pauli, o formalismo estabilizador não pode ser aplicado. Quais operadores U podem ser usados no formalismo estabilizador? Uma boa forma de responder isso e verificar quais operadores universais podem ser usados. O *conjunto universal* mais usado é formado pelo operador CNOT de 2 qubits e pelos operadores de 1 qubit

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad \text{e} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\frac{\pi}{4}} \end{bmatrix},$$

conhecidos como *Hadamard*, *fase* e *porta* T, respectivamente.

Vamos começar com o operador H. Um cálculo direto mostra que

$$HXH^\dagger = Z, \quad HYH^\dagger = -Y, \quad HZH^\dagger = X.$$

Isso é uma excelente notícia. Se o estado inicial é estabilizado por elementos do grupo de Pauli, as relações acima mostram que, após a aplicação do operador Hadamard, o novo estado vai continuar sendo estabilizado por elementos do grupo de Pauli. A regra é trocar X por Z, vice-versa e trocar Y por $-Y$ para cada qubit que tenha sido transformado pelo operador H.

Agora vamos analisar o operador S. Um cálculo direto mostra que

$$SXS^\dagger = Y, \quad SZS^\dagger = Z.$$

Multiplicando as relações acima e usando que $XZ = -iY$ obtemos

$$SYS^\dagger = -X.$$

Essas relações mostram que não há problema algum com a evolução governada pelo operador S.

O operador CNOT admite diversas possibilidades. Todas elas podem ser obtidas das seguinte relações:

$$UX_1U^\dagger = X_1X_2, \quad UX_2U^\dagger = X_2, \quad UZ_1U^\dagger = Z_1, \quad UZ_2U^\dagger = Z_1Z_2$$

onde $U = \text{CNOT}$. Também não há problemas com relação ao CNOT.

A última porta universal gera um problema incontornável, pois

$$TXT^\dagger = \frac{X+Y}{\sqrt{2}}.$$

Portanto, a evolução produzida pela porta T gera estados que não são estabilizados pelos elementos do grupo de Pauli. Eles são estabilizados por um operador que é a soma de matrizes de Pauli. Não pode.

Concluímos que qualquer operador obtido por multiplicação das portas CNOT, H e S e produto tensorial entre elas está incorporado ao formalismo estabilizador. Isso quer dizer que se o estado inicial é estabilizado por um conjunto de elementos do grupo de Pauli, após a evolução produzida por esse subconjunto de portas universais, o estado será estabilizado por um outro conjunto de elementos do grupo de Pauli.

O formalismo estabilizador produz uma enorme economia na notação de estados quânticos. Um estado genérico de n qubits é descrito na base computacional por 2^n coeficientes complexos. Se esse estado é estabilizado por um subgrupo S do grupo de Pauli G_n, então podemos caracterizá-lo usando um conjunto gerador para S, cujo número de elementos será $O(n)$. Também haverá economia de notação na descrição da evolução desse estado, pois temos que operar o operador de evolução por conjugação sobre $O(n)$ elementos. Falta ainda descrever a etapa final, que é a realização de uma *medida física*. Até o momento, estamos perto de mostrar que qualquer circuito que usa as portas CNOT, H e S pode ser simulado eficientemente por um computador clássico. Toda a riqueza da computação quântica, frente a computação clássica, fica a cargo da porta T. Esse impressionante resultado é conhecido como *teorema de Gottesman-Knill*.

3.3 Medida no Formalismo Estabilizador

Para completar o programa de descrever os postulados da Mecânica Quântica em termos do formalismo estabalizador para um conjunto particular de operadores unitários, temos que descrever o *processo da medida*. Em particular, vamos mostrar que medidas usando matrizes de Pauli ou produto tensorial de matrizes de Pauli como *observável* preservam o formalismo estabilizador e, portanto, a *medida na base computacional* também preserva. Suponha que o sistema físico é descrito pelo estado $|\psi\rangle$, que é estabilizado por $S = \langle g_1, \cdots, g_n \rangle$. Tome agora como observável g um produto tensorial de n matrizes de Pauli. Esse observável é um elemento do grupo de Pauli G_n. Queremos determinar como S se transforma após a medida com o observável g. Temos duas possibilidades:

1) g comuta como todos os geradores de S, ou

2) g anti-comuta com pelo menos um dos geradores de S.

Vamos analisar a possibilidade 1). Se g comuta com todos geradores de S, então $g_j g\,|\psi\rangle = g g_j\,|\psi\rangle = g\,|\psi\rangle$, para todos os geradores g_j, isto é, $g\,|\psi\rangle$ é estabilizado por S. Segue que $g\,|\psi\rangle$ pertence a V_S e $g\,|\psi\rangle$ tem que ser um múltiplo de $|\psi\rangle$, pois V_S tem dimensão 1. Uma vez que $g^2 = I$, temos duas possibilidades: $g\,|\psi\rangle = \pm\,|\psi\rangle$. Portanto, $g \in S$ ou $-g \in S$. Os autovalores das matrizes de Pauli são ± 1. Se $g \in S$, então a média dos possíveis resultados da medida com g é $\langle g\rangle = \langle\psi|g|\psi\rangle = 1$. Isso quer dizer que o resultado da medida nunca é -1, portanto será sempre igual a 1. Se $-g \in S$, então $\langle g\rangle = -1$ e o resultado da medida será sempre igual a -1. O estado após a medida pode ser obtido usando os seguintes fatos: $g = P_+ - P_-$ e $I = P_+ + P_-$, onde P_+ é o projetor no auto-espaço associado ao $+1$ e P_- é o projetor associado ao -1. Portanto,

$$P_+ = \frac{I+g}{2}, \tag{3.3.6}$$

$$P_- = \frac{I-g}{2}. \tag{3.3.7}$$

A partir destas expressões, podemos verificar que o estado $|\psi\rangle$ fica inalterado após a medida.

Vamos analisar a possibilidade 2). Se g não comuta com um dos geradores de S, basta considerar o seguinte caso: g não comuta apenas com g_1, pois se g também anti-comuta com g_2, podemos substituir g_2 por $g_1 g_2$ e assim sucessivamente com todos os geradores que anti-comutam com g. No final, teremos um novo conjunto gerador para S com a propriedade desejada. Os projetores associados à medida com o observável g estão descritos nas Eqs. (3.3.6) e (3.3.7). No entanto, o estado $|\psi\rangle$ não é estabilizado por S. As probabilidades associadas a cada autovalor são

$$p_\pm = \langle\psi|P_\pm|\psi\rangle\,. \tag{3.3.8}$$

Usando o fato $\langle\psi|g|\psi\rangle = \langle\psi|gg_1|\psi\rangle = -\langle\psi|g_1 g|\psi\rangle$ temos que $\langle\psi|g|\psi\rangle = 0$. Usando as Eqs. (3.3.6) e (3.3.7) na Eq. (3.3.8), obtemos $p_+ = p_-$. Como $p_+ + p_- = 1$, segue que $p_+ = p_- = 1/2$. Se o resultado da medida for $+1$, o estado do sistema logo após será

$$|\psi'\rangle = \frac{1}{\sqrt{2}}(I+g)\,|\psi\rangle\,,$$

que é estabilizado por $S' = \langle g, g_2, \cdots, g_n\rangle$. Se o resultado da medida for -1, o estado do sistema logo após será

$$|\psi'\rangle = \frac{1}{\sqrt{2}}(I-g)\,|\psi\rangle\,,$$

que é estabilizado por $S' = \langle -g, g_2, \cdots, g_n \rangle$.

A *medida na base computacional* é realizada com *medidas em cascata* usando o operador Z, um qubit de cada vez. Os resultados acima se aplicam nesse caso. Portanto, podemos acompanhar os resultados intermediários usando o formalismo estabilizador.

3.4 Código de Shor

O *código de Shor* é um código $[9, 1, 3]$, onde $S = \langle g_1, \cdots, g_8 \rangle$, de acordo com a Tabela 3.1. Pelo Fato 3, concluímos que V_S é um subespaço de dimensão 2, representando 1 *qubit lógico*, do espaço de Hilbert de dimensão 2^9. Nosso objetivo agora é achar uma base para V_S.

Gerador	Expressão
g_1	$Z_1 Z_2$
g_2	$Z_2 Z_3$
g_3	$Z_4 Z_5$
g_4	$Z_5 Z_6$
g_5	$Z_7 Z_8$
g_6	$Z_8 Z_9$
g_7	$X_1 X_2 X_3 X_4 X_5 X_6$
g_8	$X_4 X_5 X_6 X_7 X_8 X_9$
$\bar{X}$	$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$
$\bar{Z}$	$X\,X\,X\,X\,X\,X\,X\,X\,X$

Tabela 3.1: Geradores do código de Shor e os operadores lógicos $\bar{X}$ e $\bar{Z}$.

O exemplo no final da Sec. 3.1 mostra que qualquer produto tensorial dos vetores $|000\rangle$ e $|111\rangle$ entre si com 3 termos, de forma a representar uma estado de 9 qubits, por exemplo $|000\rangle\,|000\rangle\,|111\rangle$, é estabilizado por $g_1, \cdots, g_6$. Como há 8 possibilidades de vetores independentes, temos um espaço estabilizado de dimensão 8. Qualquer combinação linear destes vetores da base também são estabilizados. Falta tratar g_7 e g_8. Um operador do tipo $X_1 X_2 X_3$ converte $|000\rangle$ em $|111\rangle$ e vice-versa. Portanto, o estado de 3 qubits

$$|\psi_+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

é estabilizado por $X_1X_2X_3$. Note que o estado

$$|\psi_-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

é não estabilizado por $X_1X_2X_3$, pois há uma troca de sinal. No entanto, $|\psi_-\rangle\,|\psi_-\rangle$ é estabilizado por $X_1X_2X_3X_4X_5X_6$. Analisando todos os produtos tensoriais de $|\psi_+\rangle$ e $|\psi_-\rangle$ que formam um estado de 9 qubits, concluímos que, para ser estabilizado tanto por g_7 como por g_8, as únicas possibilidades são

$$|0_L\rangle = |\psi_+\rangle\,|\psi_+\rangle\,|\psi_+\rangle\,, \tag{3.4.9}$$
$$|1_L\rangle = |\psi_-\rangle\,|\psi_-\rangle\,|\psi_-\rangle\,. \tag{3.4.10}$$

Os estados $|0_L\rangle$ e $|1_L\rangle$ são estabilizados por S e, portanto, formam uma base ortonormal para V_S. Esses estados representam as *palavras lógicas* do código, isto é, os qubits $|0\rangle$ e $|1\rangle$ que eram usados antes da *codificação* para escrever uma mensagem devem ser substituídos por $|0_L\rangle$ e $|1_L\rangle$. Se a mensagem for um string de n qubits, a mensagem codificada terá $9n$ qubits. No espaço original, os operadores X e Z são muito úteis. X converte $|0\rangle$ em $|1\rangle$ e vice-versa. Z mantém $|0\rangle$ inalterado e inverte o sinal de $|1\rangle$. No espaço codificado, os operadores $\bar{X}$ e $\bar{Z}$, descritos na Tabela 3.1, fazem o papel dos operadores X e Z. Note que tanto $\bar{X}$ como $\bar{Z}$ comutam com todos os geradores de S. O estado $|0_L\rangle$ é estabilizado por $S_0 = \langle g_1, \cdots, g_8, \bar{Z}\rangle$ enquanto que $|1_L\rangle$ é estabilizado por $S_1 = \langle g_1, \cdots, g_8, -\bar{Z}\rangle$. Essa é uma maneira padrão de determinar os *estados lógicos*. No caso geral, quando V_S tem dimensão 2^k, teremos k *operadores lógicos* do tipo $\bar{Z}$ independentes, gerando um número maior (2^k) de estados lógicos.

Como o código de Shor tem distância 3, ele corrige um erro genérico em 1 qubit. Um erro genérico E sobre um qubit pode ser expresso como uma combinação linear de matrizes de Pauli

$$E = aI + bX + cY + dZ. \tag{3.4.11}$$

Nesse ponto precisamos do seguinte fato:

Fato 4

Um código que detecta e corrige erros produzidos por um conjunto de operadores, também detecta e corrige erros produzidos pela combinação linear desses operadores.

Esse fato é fundamental no que se segue, porém sua prova é trabalhosa e extensa, de forma que os detalhes podem ser obtidos nas

referências. Portanto, se formos capazes de detectar e corrigir erros provocados por matrizes de Pauli sobre um único qubit, seremos capazes de corrigir um erro genérico. Daqui para frente, vamos supor então que o erro foi produzido por uma das matrizes de Pauli em um único qubit.

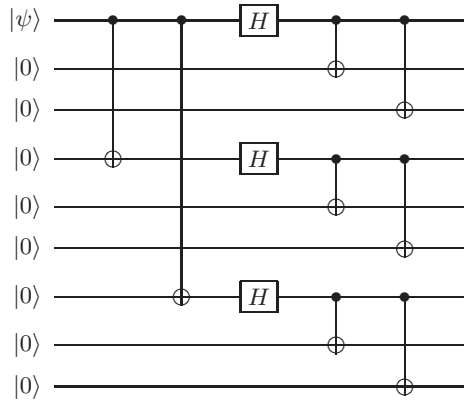

Figura 3.1: Circuito de codificação do código de Shor.

O primeiro passo é a *codificação*. Suponha que Alice vai enviar o estado $|\psi_0\rangle = a\,|0\rangle + b\,|1\rangle$ pelo canal quântico. A codificação deve transformar simultaneamente

$$\begin{aligned} |000000000\rangle &\rightarrow |0_L\rangle\,, \\ |100000000\rangle &\rightarrow |1_L\rangle\,. \end{aligned}$$

Essa codificação é feita com o circuito da Fig. 3.1. A apresentação do operador unitário de codificação na forma de circuito é muito interessante quando o circuito é descrito em termos das portas universais ou em termos de portas cuja decomposição em portas universais é conhecida. Dessa forma fica imediatamente evidente se o operador de codificação é unitário e fica fácil de verificar se ele é eficientemente implementável.

O segundo passo é a *análise de síndrome*. No formalismo estabilizador, isso é feito fazendo-se medidas em cascata tomando como observáveis os geradores de S. Se não tiver ocorrido erro, ou equivalentemente, se o erro foi produzido por I, a medida em cascata vai resultar na sequência $\{1, \cdots, 1\}$, com n uns, e o estado do sistema fica inalterado, pois todas as medidas recaem na possibilidade 1) analisada na Sec. 3.3.

Vamos supor que o erro ocorreu no primeiro qubit e foi produzido pela matriz X. Se estado original do sistema após a codificação era

$|\psi\rangle$, após a ocorrência do erro ele foi modificado para $X_1 |\psi\rangle$. Pela Tabela 3.1, podemos verificar que X_1 não pertence a S. De fato, X_1 anti-comuta com g_1 e como S é um grupo comutativo, segue que $X_1 \notin S$. Note que X_1 comuta com todo os outros geradores. Vamos mostrar agora que o resultado da medida será -1 para o observável g_1 e continuará sendo 1 quando a medida usar os outros geradores como observáveis. Observe que os projetores tem a forma descrita nas Eqs. (3.3.6) e (3.3.7), onde g é o observável em questão. Portanto, a probabilidade do resultado ser -1 é

$$\begin{aligned} p_- &= \langle\psi| X_1^\dagger P_- X_1 |\psi\rangle \\ &= \langle\psi| P_+ |\psi\rangle \\ &= 1. \end{aligned}$$

Para mostrar que $X_1^\dagger P_- X_1 = P_+$, usamos a Eq. (3.3.7) (substituindo g por g_1), $g_1 X = -X g_1$ e $X^\dagger X = I$. Para mostrar que $\langle\psi| P_+ |\psi\rangle = 1$, usamos a Eq. (3.3.6) e o fato que g_1 estabiliza $|\psi\rangle$. Como $p_- = 1$, segue que $p_+ = 0$. O cálculo análogo usando os outros geradores que comutam com X_1 mostra que $p_+ = 1$ em todos os casos. A medida em cascata vai resultar na sequência $\{-1, 1, 1, 1, 1, 1, 1, 1\}$ e o estado do sistema fica inalterado. A correção nesse caso deve ser a aplicação de $X_1^\dagger$.

Vamos supor que o erro ocorreu no primeiro qubit e foi produzido pela matriz Z. Se estado original do sistema era $|\psi\rangle$, após a ocorrência do erro ele foi modificado para $Z_1 |\psi\rangle$. Pela Tabela 3.1, podemos verificar que Z_1 não pertence a S. De fato, Z_1 anti-comuta com g_7 e comuta com todo os outros geradores. Portanto, o resultado da medida será -1 para o observável g_7 e continuará sendo 1 quando a medida usar os outros geradores como observáveis. A medida em cascata vai resultar na sequência $\{1, 1, 1, 1, 1, 1, -1, 1\}$ e o estado do sistema fica inalterado. A correção nesse caso deve ser a aplicação de $Z_1^\dagger$. Note que se o erro tivesse sido Z_2 ou Z_3, a análise de síndrome teria dado o mesmo resultado e a aplicação de Z_1 teria corrigido da mesma forma, pois o efeito dos operadores Z_1, Z_2 e Z_3 nos estados $|\psi_+\rangle$ e $|\psi_-\rangle$ é o mesmo.

Vamos supor que o erro ocorreu no primeiro qubit e foi produzido pela matriz Y. Se estado original do sistema era $|\psi\rangle$, após a ocorrência do erro ele foi modificado para $Y_1 |\psi\rangle$. Pela Tabela 3.1, podemos verificar que Y_1 não pertence a S. De fato, Y_1 anti-comuta com g_1 e com g_7 e comuta com todo os outros geradores. Portanto, o resultado da medida será -1 para os observáveis g_1 e g_7 e continuará sendo 1 quando a medida usar os outros geradores como observáveis. A medida em cascata vai resultar na sequência $\{-1, 1, 1, 1, 1, 1, -1, 1\}$ e

o estado do sistema fica inalterado. A correção nesse caso deve ser a aplicação de Y_1. Esse resultado também pode ser obtido a partir dos resultados com os observáveis X e Z.

Erro	Resultado da medida	Correção
I	1, 1, 1, 1, 1, 1, 1, 1	I
X_1	-1, 1, 1, 1, 1, 1, 1, 1	X_1
X_2	-1,-1, 1, 1, 1, 1, 1, 1	X_2
X_3	1,-1, 1, 1, 1, 1, 1, 1	X_3
Z_1 ou Z_2 ou Z_3	1, 1, 1, 1, 1, 1,-1, 1	Z_1
X_4	1, 1,-1, 1, 1, 1, 1, 1	X_4
X_5	1, 1,-1,-1, 1, 1, 1, 1	X_5
X_6	1, 1, 1,-1, 1, 1, 1, 1	X_6
Z_4 ou Z_5 ou Z_6	1, 1, 1, 1, 1, 1,-1,-1	Z_4
X_7	1, 1, 1, 1,-1, 1, 1, 1	X_7
X_8	1, 1, 1, 1,-1,-1, 1, 1	X_8
X_9	1, 1, 1, 1, 1,-1, 1, 1	X_9
Z_7 ou Z_8 ou Z_9	1, 1, 1, 1, 1, 1, 1,-1	Z_7

Tabela 3.2: Possíveis erros de 1 qubit no código de Shor, análise de síndrome e os operadores de correção. Os erros produzidos pela matriz de Pauli Y podem ser analisados através do produto dos erros X por Z.

A Tabela 3.2 resume todos os possíveis erros de 1 qubit, mostra os resultados da análise de síndrome e os operadores de correção em cada caso. Os erros produzidos pela matriz de Pauli Y podem ser analisados através do produto dos erros X por Z.

Vamos dar um exemplo de um erro que não pode ser corrigido: $X_1X_2X_3$. Esse operador comuta com todos os geradores do código de Shor e a análise de síndrome retornará a sequência $\{1,1,1,1,1,1,1,1\}$ indicando que deveríamos corrigir com o operador I. Qualquer erro que seja um operador do grupo de Pauli G_n que não está em S, mas comuta com todos os geradores de S, não pode ser corrigido. Mostramos que nenhum operador de um qubit está nessa classe, portanto podem ser corrigidos. Como o código tem distância 3, os erros que são operadores de 2 qubits podem ser detectados, porém não podem ser corrigidos. Por exemplo, o erro X_1X_2 tem a análise de síndrome igual ao erro X_3. Portanto, verificamos que houve erro, porém a correção sugerida na Tabela 3.2 não funciona.

3.5 Código Quântico [5,1,3]

O código quântico $[5, 1, 3]$ é a menor *codificação* possível de um qubit com distância 3. Esse código satura o *limite quântico de Singleton*. Os geradores do grupo estabilizador estão descritos na Tabela 3.3.

Gerador	Expressão
g_1	$X_1Z_2Z_3X_4$
g_2	$X_2Z_3Z_4X_5$
g_3	$X_1X_3Z_4Z_5$
g_4	$Z_1X_2X_4Z_5$
$\bar{X}$	$XXXXX$
$\bar{Z}$	$ZZZZZ$

Tabela 3.3: Geradores do código de $[5, 1, 3]$ e os operadores lógicos $\bar{X}$ e $\bar{Z}$.

Dados os geradores, existe uma maneira alternativa de encontrar os *qubits lógicos* usando um processo iterativo. Tomamos como estado inicial $|\psi_1\rangle = |00000\rangle$ e selecionamos o primeiro gerador g_1. A aplicação $g_1 |\psi_1\rangle$ retorna $|10010\rangle$. O próximo estado será

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\big(|00000\rangle + |10010\rangle \big).$$

Note que $|\psi_2\rangle$ é estabilizado por g_1. Selecionamos o segundo gerador, e repetimos o processo. A aplicação $g_2 |\psi_2\rangle$ retorna $(|01001\rangle - |11011\rangle)/\sqrt{2}$. O próximo estado será

$$|\psi_2\rangle = \frac{1}{2}\big(|00000\rangle + |10010\rangle + |01001\rangle - |11011\rangle \big).$$

Continuamos o processo até encontrar um estado que será estabilizado por todos os geradores. O resultado final será

$$\begin{aligned} |0_L\rangle = \frac{1}{4}\big(& |00000\rangle + |10010\rangle + |01001\rangle - |11011\rangle + \\ & |10100\rangle - |00110\rangle - |11101\rangle - |01111\rangle + \\ & |01010\rangle - |11000\rangle - |00011\rangle - |10001\rangle - \\ & |11110\rangle - |01100\rangle - |10111\rangle + |00101\rangle \big). \end{aligned} \tag{3.5.12}$$

Agora aplicamos o operador $\bar{X}$ em $|0_L\rangle$

$$\begin{aligned} |1_L\rangle = \frac{1}{4}\big(& |11111\rangle + |01101\rangle + |10110\rangle - |00100\rangle + \\ & |01011\rangle - |11001\rangle - |00010\rangle - |10000\rangle + \\ & |10101\rangle - |00111\rangle - |11100\rangle - |01110\rangle - \\ & |00001\rangle - |10011\rangle - |01000\rangle + |11010\rangle \big). \end{aligned} \tag{3.5.13}$$

Note que $|0_L\rangle$ é estabilizado por $S_0 = \langle g_1, \cdots, g_4, \bar{Z}\rangle$, pois todos os *kets* de $|0_L\rangle$ têm um número par de 1s e $|1_L\rangle$ é estabilizado por $S_1 = \langle g_1, \cdots, g_4, -\bar{Z}\rangle$, pois todos os *kets* de $|1_L\rangle$ têm um número ímpar de 1s.

Erro	Resultado da medida	Correção
X_1	1, 1, 1,-1	X_1
X_2	-1, 1, 1, 1	X_2
X_3	-1,-1, 1, 1	X_3
X_4	1,-1,-1, 1	X_4
X_5	1, 1,-1,-1	X_5
Z_1	-1, 1,-1, 1	Z_1
Z_2	1,-1, 1,-1	Z_2
Z_3	1, 1,-1, 1	Z_3
Z_4	-1, 1, 1,-1	Z_4
Z_5	1,-1, 1, 1	Z_5

Tabela 3.4: Possíveis erros de 1 qubit no código $[5, 1, 3]$, análise de síndrome e os operadores de correção. Basta analisar os erros produzidos por X e Z nos diferentes qubits. Os resultados da medida correspondem a medida em cascata com os 4 geradores como observáveis.

A Tabela 3.4 resume todos os possíveis erros de 1 qubit independentes (X e Z), mostra os resultados da análise de síndrome e os operadores de correção em cada caso. Na análise de síndrome do código de Shor, mostramos que quando um erro comuta com um gerador, o resultado da medida com esse gerador é $+1$ e quando anti-comuta, o resultado é -1. Portanto, o resultado 1, 1, 1, -1 da síndrome do erro X_1 foi obtido da seguinte forma: X_1 comuta com g_1, g_2 e g_3 e anti-comuta com g_4. As outras síndromes foram obtidas de forma análoga. Os erros produzidos pela matriz de Pauli Y podem ser obtidos tomando o produto das linhas dos erros X por Z. Por exemplo, a linha correspondente a X_1 vezes a linha de Z_1 dá -1, 1, -1, -1 que corresponde ao erro produzido por Y_1. Note que há exatamente 16 possibilidades de resultados de medidas que correspondem exatamente ao erros produzidos pelas 16 matrizes de Pauli.

Sugestões para Leitura

Os códigos estabilizadores foram introduzidos por Daniel Gottesman na sua tese de doutoramento [7]. A Ref. [14] tem excelente material sobre o assunto. O código quântico $[5, 1, 3]$ foi introduzido na Ref. [3].

Apêndice A

Álgebra Linear

O objetivo deste apêndice é compilar as definições, notações e fatos da Álgebra Linear que são importantes neste trabalho. Este apêndice também serve de referência rápida para as propriedades das operações em espaços vetoriais como, por exemplo, o produto interno e o produto tensorial. A Computação Quântica herdou da Mecânica Quântica a Álgebra Linear como a linguagem para a descrição da área. Portanto, é fundamental um conhecimento sólido dos resultados básicos da Álgebra Linear para a compreensão da Computação Quântica e de algoritmos quânticos. Caso o leitor não tenha essa base, sugerimos a leitura de alguma das referências básicas do final deste apêndice.

A.1 Espaços Vetoriais

Um *espaço vetorial* V sobre o corpo dos números complexos $\mathbb{C}$ é um conjunto não-vazio de elementos chamados de vetores. Em V, estão definidas as operações de soma de vetores e multiplicação de um vetor por um escalar em $\mathbb{C}$. A operação de soma é associativa e comutativa. Além disso satisfaz às propriedades

- Há um elemento $\mathbf{0} \in V$, tal que, para cada $\mathbf{v} \in V$, $\mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v}$ (existência de elemento neutro)
- Para cada $\mathbf{v} \in V$, existe $\mathbf{u} = (-1)\mathbf{v}$ em V tal que $\mathbf{v} + \mathbf{u} = \mathbf{0}$ (existência de elemento oposto)

$\mathbf{0}$ é chamado de vetor nulo. A operação de multiplicação por escalar satisfaz às propriedades

- $a.(b.\mathbf{v}) = (a.b).\mathbf{v}$ (associatividade)
- $1.\mathbf{v} = \mathbf{v}$ (1 é o elemento neutro da multiplicação)

- $(a+b).\mathbf{v} = a.\mathbf{v} + b.\mathbf{v}$ (distributividade sobre soma de escalares)
- $a.(\mathbf{v}+\mathbf{w}) = a.\mathbf{v} + a.\mathbf{w}$ (distributividade em V)

onde $\mathbf{v}, \mathbf{w} \in V$ e $a, b \in \mathbb{C}$.

Um espaço vetorial pode ser infinito, porém na maior parte das aplicações em Computação Quântica, são usados espaços vetoriais finitos que são denotados por $\mathbb{C}^n$. Nesse caso os vetores têm n componentes complexas. Neste livro, raramente vamos usar espaços infinitos e, nesses poucos casos, estaremos interessados apenas em subespaços finitos. No contexto da Mecânica Quântica, os espaços vetoriais infinitos são usados com mais frequência do que os finitos.

Uma *base* de $\mathbb{C}^n$ é constituída por exatamente n vetores linearmente independentes. Se $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ é uma base de $\mathbb{C}^n$, então um vetor genérico $\mathbf{v}$ pode ser escrito como

$$\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{v}_i,$$

onde os coeficientes a_i são números complexos. A *dimensão* de um espaço vetorial é o número de vetores da base.

A.2 Produtos Internos

O *produto interno* é uma operação binária $(\cdot,\cdot) : V \times V \mapsto \mathbb{C}$ que satisfaz às seguintes propriedades

1. $(\cdot,\cdot)$ é linear no segundo argumento

$$\left(\mathbf{v}, \sum_{i=1}^{n} a_i \mathbf{v}_i\right) = \sum_{i=1}^{n} a_i \left(\mathbf{v}, \mathbf{v}_i\right).$$

2. $(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_2, \mathbf{v}_1)^*$.
3. $(\mathbf{v}, \mathbf{v}) \geq 0$ com a igualdade se, e somente se $\mathbf{v} = \mathbf{0}$.

Em geral, o produto interno não é linear no primeiro argumento, e sim conjugado-linear.

Existe mais de uma forma de definir um produto interno em um espaço vetorial. Em $\mathbb{C}^n$, o produto interno mais usado é definido da seguinte maneira: sejam

$$\mathbf{v} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

então

$$(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^{n} a_i^* b_i.$$

Essa expressão equivale ao produto matricial do vetor transposto-conjugado cuja notação usual é $\mathbf{v}^\dagger$, por $\mathbf{w}$.

Se um produto interno foi introduzido em um espaço vetorial, podemos definir a noção de ortogonalidade. Dois vetores são ortogonais se o produto interno for zero. Podemos também introduzir a noção de norma de vetores via o produto interno. A norma de $\mathbf{v}$, denotado por $\|\mathbf{v}\|$ é definida como

$$\|\mathbf{v}\| = \sqrt{(\mathbf{v}, \mathbf{v})}.$$

Um vetor é dito normalizado se sua norma é igual a 1. Uma base é dita ortonormal se todos os vetores da base são normalizados e ortogonais entre si.

Um espaço vetorial finito com um produto interno é dito um *espaço de Hilbert*. Para um espaço vetorial infinito ser um espaço de Hilbert, ele deve satisfazer a propriedades adicionais além de ter um produto interno. Como lidaremos basicamente com espaços vetoriais finitos, usaremos o termo espaço de Hilbert como sinônimo de espaço vetorial com um produto interno. Um *subespaço* W de um espaço de Hilbert V finito também é um espaço de Hilbert. O conjunto de vetores ortogonais a todos os vetores de W é o espaço de Hilbert $W^\perp$ chamado de *complemento ortogonal*. V é a soma direta de W e $W^\perp$, isto é $V = W \oplus W^\perp$.

A.3 Notação de Dirac

Nesta revisão dos principais conceitos de Álgebra Linear usados na Computação Quântica, vamos usar a notação de Dirac que foi introduzida pelo físico inglês Paul A.M. Dirac no início da Mecânica Quântica para facilitar a execução de cálculos aplicados. Essa notação é muito simples. Diversas notações são usada para vetores, como $\mathbf{v}$ e $\vec{v}$. Na notação de Dirac temos

$$\mathbf{v} \equiv |v\rangle .$$

Até esse ponto, em vez de usar negrito ou colocar uma seta sobre a letra, colocamos a letra entre a barra vertical e o sinal de maior. Se temos uma base indexada, como por exemplo $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$, na notação de Dirac usamos a forma $\{|v_1\rangle, \cdots, |v_n\rangle\}$ ou $\{|1\rangle, \cdots, |n\rangle\}$. Note que se usarmos uma única base, a letra $\mathbf{v}$, em princípio, será

desnecessária. Na área da computação, é muito comum começar a numeracão pelo zero, assim o primeiro vetor da base usualmente é chamado de $\mathbf{v}_0$. Na notação de Dirac temos

$$\mathbf{v}_0 \equiv |0\rangle .$$

O vetor $|0\rangle$ não é o vetor nulo, ele é apenas o primeiro vetor de uma coleção de vetores. Na notação de Dirac, o vetor nulo é uma exceção, cuja notação não é modificada. Aqui vamos usar a notação $\mathbf{0}$.

Suponha que o vetor $|v\rangle$ tenha as seguintes componentes em uma determinada base

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} .$$

O vetor dual é denotado por $\langle v|$ e é definido por

$$\langle v| = \begin{pmatrix} a_1^* & \cdots & a_n^* \end{pmatrix} .$$

Os vetores usuais e os duais podem ser vistos como matrizes colunas e matrizes linhas, respectivamente, para fins de cálculo. O produto matricial de $\langle v|$ por $|v\rangle$ é denotado por $\langle v|v\rangle$ e seu valor em termos das componentes é

$$\langle v|v\rangle = \sum_{i=1}^{n} a_i^* a_i.$$

Esse é um exemplo de um produto interno, implicitamente usado na notação de Dirac. Se $\{|v_1\rangle, \cdots, |v_n\rangle\}$ é uma base ortonormal então

$$\langle v_i|v_j\rangle = \delta_{ij},$$

onde δ_{ij} é o delta de Kronecker. A norma de um vetor nessa notação é

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

Usa-se a terminologia *ket* para o vetor $|v\rangle$ e *bra* para o vetor dual $\langle v|$. Mantendo a concistência, usa-se a terminologia *braket* para $\langle v|v\rangle$, pois *braket* é similar a palavra da língua inglesa *bracket*.

É muito comum também o produto matricial de $|v\rangle$ por $\langle v|$, denotado por $|v\rangle \langle v|$, conhecido como produto externo cujo resultado é uma matriz $n \times n$

$$\begin{aligned} |v\rangle \langle v| &= \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} a_1^* & \cdots & a_n^* \end{pmatrix} \\ &= \begin{pmatrix} a_1 a_1^* & \cdots & a_1 a_n^* \\ & \ddots & \\ a_n a_1^* & \cdots & a_n a_n^* \end{pmatrix} . \end{aligned}$$

A chave para a notação de Dirac é sempre visualizar o *ket* como uma matriz coluna, o *bra* como uma matriz linha e reconhecer que uma sequência de *bras* e *kets* é um produto matricial, portanto associativo, porém não-comutativo.

A.4 Base Computacional

A *base computacional* de $\mathbb{C}^n$, denotada por $\{|0\rangle, \cdots, |n-1\rangle\}$, é dada por

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots, \quad |n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Essa base também é conhecida por *base canônica*. Algumas poucas vezes vamos usar a numeração da base computacional começando por $|1\rangle$ e terminando com $|n\rangle$. Neste livro, quando usarmos uma letra latina minúscula dentro de um *ket* ou um *bra*, estaremos nos referindo à base computacional, portanto sempre será válida a relação

$$\langle i|j\rangle = \delta_{ij}.$$

A soma normalizada de todos os vetores da base computacional define o vetor

$$|\mathrm{D}\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle,$$

que chamaremos de *estado diagonal*. Quando $n = 2$, o estado diagonal é dado por $|\mathrm{D}\rangle = |+\rangle$ onde

$$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

A.5 Qubit e a Esfera de Bloch

O *qubit* é um vetor unitário no espaço vetorial $\mathbb{C}^2$. Um qubit genérico $|\psi\rangle$ é representado por

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

onde os coeficientes complexos α e β satisfazem ao vínculo

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

O conjunto $\{|0\rangle, |1\rangle\}$ é a base computacional de $\mathbb{C}^2$ e α, β são chamados de amplitudes do estado $|\psi\rangle$. O termo *estado* (ou *vetor de*

estado) é usado como sinônimo de vetor unitário em um espaço de Hilbert.

Em princípio, precisamos de quatro números reais para descrever um qubit, dois para especificar α e dois para β. O vínculo $|\alpha|^2 + |\beta|^2 = 1$ reduz para três números. Na Mecânica Quântica, dois vetores que diferem de um fator de fase global são considerados equivalentes. Uma fase global é um número complexo de módulo unitário multiplicado ao estado. Eliminando a fase global, um qubit pode ser descrito por dois números reais θ e ϕ da seguinte forma:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{i\phi}\sin\frac{\theta}{2}|1\rangle\,,$$

onde $0 \leq \theta \leq \pi/2$ e $0 \leq \phi < 2\pi$. Na notação acima, o estado $|\psi\rangle$ pode ser representado por um ponto na superfície de uma esfera de raio unitário, chamada *esfera de Bloch*. Colocando o estado $|0\rangle$ como o polo norte da esfera, os números θ e ϕ são os ângulos esféricos que situam o ponto que descreve $|\psi\rangle$, como na Fig. A.1. O vetor indicado na figura é dado por

$$\begin{pmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ \cos\theta \end{pmatrix}.$$

Existe uma correspondência bi-unívoca entre os estados quânticos de um qubit e os pontos na esfera de Bloch. Os estados

$$|\pm\rangle := \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

ficam nos pontos de encontro do eixo x com a esfera e os estados $(|0\rangle \pm i\,|1\rangle)/\sqrt{2}$ ficam nos pontos de encontro do eixo y com a esfera.

A.6 Operadores Lineares

Sejam V, W espaços vetoriais; $\{|v_1\rangle, \cdots, |v_n\rangle\}$ uma base para V; $\mathcal{A}$ uma função $\mathcal{A} : V \mapsto W$ que satisfaz à

$$\mathcal{A}\left(\sum_i a_i\,|v_i\rangle\right) = \sum_i a_i \mathcal{A}(|v_i\rangle),$$

para quaisquer números complexos a_i. $\mathcal{A}$ é dito um *operador linear* de V em W. O termo operador linear em V quer dizer que tanto

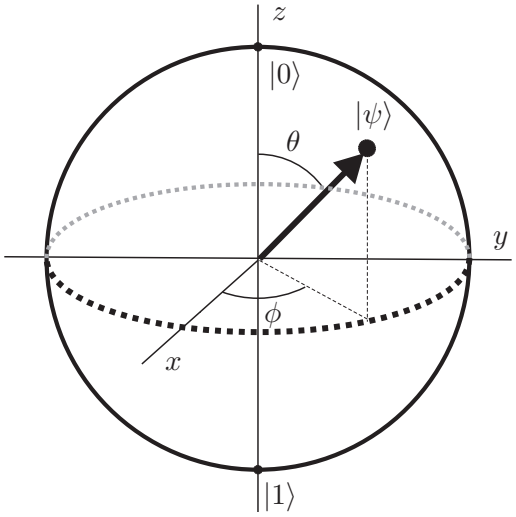

Figura A.1: Esfera de Bloch. O estado $|\psi\rangle$ de um qubit é representado por um ponto sobre a esfera.

o domínio como o contradomínio de $\mathcal{A}$ é V. A composição de operadores lineares $\mathcal{A} : V_1 \mapsto V_2$ e $\mathcal{B} : V_2 \mapsto V_3$ é também um operador linear $\mathcal{C} : V_1 \mapsto V_3$ obtido através da composição das respectivas funções: $\mathcal{C}(|v\rangle) = \mathcal{B}(\mathcal{A}(|v\rangle))$. A soma de dois operadores lineares, ambos de V em W, é naturalmente definida através da fórmula $(A + B)(|v\rangle) = A(|v\rangle) + B(|v\rangle)$.

O operador identidade I em V é um operador linear em V tal que $I(|v\rangle) = |v\rangle$ para todo $|v\rangle \in V$. O operador nulo O em V é um operador linear tal que $O(|v\rangle) = \mathbf{0}$ para todo $|v\rangle \in V$.

Fato

Se especificarmos a ação de um operador linear em uma base do espaço vetorial V, sua ação em qualquer vetor de V estará automaticamente determinada.

A.7 Representação Matricial

Os operadores lineares podem ser representados por matrizes. Sejam $\mathcal{A} : V \mapsto W$ um operador linear; $\{|v_1\rangle, \cdots, |v_n\rangle\}$ e $\{|w_1\rangle, \cdots, |w_m\rangle\}$ bases ortonormais para V e W, respectivamente. A *representação matricial* de $\mathcal{A}$ é obtida aplicando $\mathcal{A}$ a cada vetor da base de V e expressando o resultado como uma combinação linear de vetores da

base de W, da seguinte forma:

$$\mathcal{A}\left(|v_j\rangle\right) = \sum_{i=1}^{m} A_{ij} \left|w_i\right\rangle ,$$

onde o sub-índice j corre de 1 até n. Portanto, A_{ij} são componentes de uma matriz de dimensão $m \times n$ que chamaremos de A. Quando fixamos as bases dos espaços vetoriais envolvidos, um operador linear pode ser substituído pela sua representação matricial. Nesse caso, a expressão $\mathcal{A}\left(|v_j\rangle\right)$ que significa a função $\mathcal{A}$ aplicada ao argumento $|v_j\rangle$ é equivalente ao produto matricial $A\,|v_j\rangle$. Usando a notação de produto externo, temos

$$A = \sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij} \left|w_i\right\rangle \left\langle v_j\right| .$$

Usando a equação acima e a ortonormalidade da base de V, podemos verificar que o produto matricial de A por $|v_j\rangle$ é igual a $\mathcal{A}\left(|v_j\rangle\right)$. A chave para esse cálculo é usar a associatividade da multiplicação matricial, pois

$$\begin{aligned} \left(\left|w_i\right\rangle \left\langle v_j\right| \right) \left|v_k\right\rangle &= \left|w_i\right\rangle \left(\left\langle v_j | v_k \right\rangle \right) \\ &= \delta_{jk} \left|w_i\right\rangle . \end{aligned}$$

Se o operador linear $\mathcal{C}$ for a composição do operador linear $\mathcal{B}$ com $\mathcal{A}$, a representação matricial de $\mathcal{C}$ será obtida por multiplicação da representação matricial de $\mathcal{B}$ com a de $\mathcal{A}$, ou seja, $C = BA$.

Uma vez fixadas as bases ortonormais para os espaços vetoriais em questão, existe uma identificação entre operadores lineares e matrizes. Em $\mathbb{C}^n$, temos a base computacional como referência, portanto podemos usar os termos operadores lineares e matrizes como sinônimos. Vamos também usar o termo operador como sinônimo de operador linear.

A.8 Representação Diagonal

Seja $\mathcal{O}$ um operador em V. Se existir uma base $\{|v_1\rangle, \cdots, |v_n\rangle\}$ ortonormal de V tal que

$$O = \sum_{i=1}^{n} \lambda_i \left|v_i\right\rangle \left\langle v_i\right| ,$$

dizemos que $\mathcal{O}$ admite uma *representação diagonal* ou, equivalentemente, $\mathcal{O}$ é *diagonalizável*. Os números complexos λ_i são os *autovalores* de $\mathcal{O}$ e $|v_i\rangle$ os seus *autovetores* associados. Qualquer múltiplo de

um autovetor também é um autovetor. Se dois autovetores estão associados ao mesmo autovalor, então qualquer combinação linear desses autovetores é um autovetor. O número de autovetores linearmente independentes associados a um mesmo autovalor é a multiplicidade desse autovalor.

Quando há autovalores com multiplicidade maior que 1, a representação diagonal pode ser fatorada da seguinte forma

$$O = \sum_{\lambda} \lambda P_{\lambda},$$

onde o índice λ do somatório corre apenas nos autovalores distintos e P_{λ} é o projetor no auto-espaço de $\mathcal{O}$ associado ao autovalor λ. Se λ tiver multiplicidade 1, $P_{\lambda} = |v\rangle \langle v|$, onde $|v\rangle$ é o autovetor unitário associado a λ. Se λ tiver multiplicidade 2 e $|v_1\rangle, |v_2\rangle$ são os autovetores unitários associados linearmente independentes, $P_{\lambda} = |v_1\rangle \langle v_1| + |v_2\rangle \langle v_2|$ e assim por diante. Os projetores satisfazem

$$\sum_{\lambda} P_{\lambda} = I.$$

Uma definição alternativa de um operador diagonalizável é exigir que O é *similar* a uma matriz diagonal por uma transformação de similaridade com uma matriz unitária. Uma *transformação de similaridade* é do tipo $O \rightarrow M^{-1}OM$ onde M é uma matriz inversível. A definição do termo *diagonalizável* é mais restrita do que usualmente aparece na literatura, pois estamos exigindo que M seja uma matriz unitária.

A.9 Relação de Completeza

A *relação de completeza* é tão útil que merece destaque. Seja $\{|v_1\rangle, \cdots, |v_n\rangle\}$ uma base ortonormal de V, então

$$I = \sum_{i=1}^{n} |v_i\rangle \langle v_i| .$$

A relação de completeza é uma representação diagonal da matriz identidade.

A.10 Desigualdade de Cauchy-Schwarz

Seja V um espaço de Hilbert e $|v\rangle, |w\rangle \in V$, então

$$| \langle v|w\rangle | \leq \sqrt{\langle v|v\rangle \langle w|w\rangle}.$$

Uma forma mais explícita de apresentar a desigualdade de Cauchy-Schwarz é

$$\left|\sum_i v_i w_i\right|^2 \leq \left(\sum_i |v_i|^2\right)\left(\sum_i |w_i|^2\right),$$

que é obtida quando tomamos $|v\rangle = \sum_i v_i^* |i\rangle$ e $|w\rangle = \sum_i w_i |i\rangle$.

A.11 Operadores Especiais

Seja A um operador linear no espaço de Hilbert V, então existe um único operador linear $A^\dagger$ em V, chamado de *operador ajunto*, que satisfaz à

$$(|v\rangle, A|w\rangle) = \left(A^\dagger |v\rangle, |w\rangle\right),$$

para todos $|v\rangle, |w\rangle \in V$.

A representação matricial de $A^\dagger$ é a matriz transposta-conjugada de A. As principais propriedades da operação *adaga* ou *transposta-conjugada* são

1. $(AB)^\dagger = B^\dagger A^\dagger$
2. $|v\rangle^\dagger = \langle v|$
3. $A|v\rangle^\dagger = \langle v| A^\dagger$
4. $\left(|w\rangle\langle v|\right)^\dagger = |v\rangle\langle w|$
5. $\left(A^\dagger\right)^\dagger = A$
6. $(\sum_i a_i A_i)^\dagger = \sum_i a_i^* A_i^\dagger$

A última propriedade mostra que a operação adaga é conjugada-linear.

Operador Normal

Um operador A em V é *normal* se $A^\dagger A = AA^\dagger$.

Teorema Espectral

Um operador A em V é diagonalizável se, e somente se A for normal.

Operador Unitário

Um operador U em V é *unitário* se $U^\dagger U = UU^\dagger = I$.

Fatos sobre Operadores Unitários

Operadores unitários são normais, portanto são diagonalizáveis com relação a uma base ortonormal. Autovetores de um operador unitário associados a autovalores diferentes são ortogonais. Os autovalores têm módulo iguais a 1. A aplicação de um operador unitário sobre um vetor preserva a norma.

Operador Hermitiano

Um operador A em V é *hermitiano* ou *auto-adjunto* se $A^\dagger = A$.

Fatos sobre Operadores Hermitianos

Operadores hermitianos são normais, portanto são diagonalizáveis com relação a uma base ortonormal. Autovetores de um operador hermitiano associados a autovalores diferentes são ortogonais. Os autovalores de um operador hermitiano são reais. Uma matriz real simétrica é hermitiana.

Projetor

Um operador P em V é um *projetor* se $P^2 = P$.

Fatos sobre Projetores

Projetores são hermitianos. Os autovalores são iguais a 0 ou 1. Se P é um projetor, então o *complemento ortogonal* $I - P$ também é um projetor. A aplicação de um projetor sobre um vetor ou diminui a sua norma ou a mantém invariante.

Operador Positivo

Um operador A em V é dito *positivo* se $\langle v|A|v\rangle \geq 0$ para todo $|v\rangle \in V$. Se a desigualdade for estrita para todo vetor não-nulo de V, então o operador é dito *positivo definido*.

Fatos sobre Operadores Positivos

Os operadores positivos são hermitianos.

Exercício A.1. *Considere a matrix*

$$M = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

1. *Mostre que M não é normal.*
2. *Mostre que os autovetores de M geram um espaço unidimensional.*

Exercício A.2. *Considere a matrix*

$$M = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}.$$

1. *Mostre os autovalores de M são ± 1.*
2. *Mostre que M não é unitária e não é hermitiana.*
3. *Mostre que os autovetores de M associados a autovalores distintos não são ortogonais.*
4. *Mostre que M não tem uma representação diagonal.*

A.12 Matrizes de Pauli

As *matrizes de Pauli* são

$$\begin{aligned}
\sigma_0 &= I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\
\sigma_1 &= \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\
\sigma_2 &= \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \\
\sigma_3 &= \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.
\end{aligned}$$

Essas matrizes são unitárias e hermitianas, portanto seus autovalores são iguais a 1 ou -1. Dito de outra forma: $\sigma_j^2 = I$ e $\sigma_j^\dagger = \sigma_j$, para $j = 0, \cdots, 3$.

Os seguintes fatos são extensivamente usados: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, $Z|0\rangle = |0\rangle$ e $Z|1\rangle = -|1\rangle$. As matrizes de Pauli formam uma base para o espaço vetorial das matrizes de dimensão 2×2. Portanto, um operador genérico que atua em 1 qubit pode ser escrito como uma combinação linear de matrizes de Pauli.

A.13 Funções de Operadores

Se temos um operador A em V, podemos perguntar se é possível calcular $\sqrt{A}$, isto é, achar um operador cujo quadrado é A? De modo geral, podemos nos perguntar se faz sentido usar um operador como argumento de uma função, como a função exponencial ou logaritmo? Se o operador A é normal, ele tem uma representação diagonal, ou seja, pode ser escrito na forma

$$A = \sum_i a_i \left|v_i\right\rangle \left\langle v_i\right| ,$$

onde a_i são os autovalores e o conjunto $\{|v_i\rangle\}$ é uma base ortonormal de autovetores de A. Podemos estender a aplicação de uma função $f : \mathbb{C} \mapsto \mathbb{C}$ para A da seguinte forma

$$f(A) = \sum_i f(a_i) \left|v_i\right\rangle \left\langle v_i\right| .$$

O resultado é um operador definido no mesmo espaço vetorial V e é independente da escolha da base de V.

Se o objetivo é calcular $\sqrt{A}$, primeiramente diagonalizamos A, isto é, determinamos uma matriz unitária U tal que $A = U D U^\dagger$, onde D é uma matriz diagonal. Depois usamos o fato que $\sqrt{A} = U\sqrt{D}\,U^\dagger$, onde $\sqrt{D}$ é calculada tomando a raíz quadrada de cada elemento da diagonal.

Se U é o operador de evolução de um sistema quântico isolado que está inicialmente no estado $|\psi(0)\rangle$, o estado no instante t será dado por

$$\left|\psi(t)\right\rangle \;=\; U^t \left|\psi(0)\right\rangle .$$

A maneira mais eficiente de calcular o estado $|\psi(t)\rangle$ é obter a representação diagonal do operador unitário U

$$U \;=\; \sum_i \lambda_i \left|v_i\right\rangle \left\langle v_i\right| ,$$

e calcular a t-ésima potência de U, ou seja

$$U^t \;=\; \sum_i \lambda_i^t \left|v_i\right\rangle \left\langle v_i\right| .$$

O estado do sistema no instante t será

$$\left|\psi(t)\right\rangle \;=\; \sum_i \lambda_i^t \left\langle v_i|\psi(0)\right\rangle \;\left|v_i\right\rangle .$$

O traço de uma matriz é outro tipo de função de operadores. Nesse caso, o resultado da aplicação da função é um número complexo definido como

$$\mathrm{tr}(A) = \sum_i A_{ii},$$

onde A_{ii} são os elementos diagonais de A. A função traço satisfaz às seguintes propriedades

1. $\mathrm{tr}(aA + bB) = a\,\mathrm{tr}(A) + b\,\mathrm{tr}(B)$, (linearidade)
2. $\mathrm{tr}(AB) = \mathrm{tr}(BA)$,
3. $\mathrm{tr}(A\,B\,C) = \mathrm{tr}(C\,A\,B)$. (propriedade cíclica)

A propriedade 3 é consequência imediata da 2.

A função traço é invariante por transformações de similaridade, isto é, $\mathrm{tr}(M^{-1}AM)$=$\mathrm{tr}(A)$, onde M é uma matriz inversível. Isso implica que o traço não depende da base escolhida para obter a representação matricial do operador.

Uma fórmula bastante útil envolvendo o traço de operadores é

$$\mathrm{tr}(A\,|\psi\rangle\,\langle\psi|) = \langle\psi|A|\psi\rangle\,,$$

para qualquer $|\psi\rangle \in V$ e qualquer A em V.

Exercício A.3. *Usando o método de avaliação de funções sobre matrizes descrito nesta seção, encontre a matriz M tal que*

$$M^2 = \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix}.$$

A.14 Produto Tensorial

Sejam V e W espaços de Hilbert finitos com as base $\{|v_1\rangle, \cdots, |v_m\rangle\}$ e $\{|w_1\rangle, \cdots, |w_n\rangle\}$, respectivamente. O *produto tensorial* de V com W, denotado por $V \otimes W$, é um espaço de Hilbert de dimensão mn, que tem o conjunto $\{|v_1\rangle \otimes |w_1\rangle, |v_1\rangle \otimes |w_2\rangle, \cdots, |v_m\rangle \otimes |w_n\rangle\}$ como uma base. O produto tensorial de um vetor de V por um vetor de W, $|v\rangle \otimes |w\rangle$, também denotado por $|v\rangle\,|w\rangle$ ou $|v, w\rangle$ ou $|v\,w\rangle$, pode ser calculado explicitamente via o produto de Kronecker, definido logo adiante. Um vetor genérico de $V \otimes W$ é uma combinação linear de vetores do tipo $|v_i\rangle \otimes |w_j\rangle$, ou seja, se $|\psi\rangle \in V \otimes W$ então

$$|\psi\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\,|v_i\rangle \otimes |w_j\rangle\,.$$

O produto tensorial é *bilinear*, isto é, linear em cada argumento. Portanto

1. $|v\rangle \otimes \big(a\,|w_1\rangle + b\,|w_2\rangle\big) \;=\; a\,|v\rangle \otimes |w_1\rangle + b\,|v\rangle \otimes |w_2\rangle\,,$
2. $\big(a\,|v_1\rangle + b\,|v_2\rangle\big) \otimes |w\rangle \;=\; a\,|v_1\rangle \otimes |w\rangle + b\,|v_2\rangle \otimes |w\rangle\,.$

Um escalar pode sempre ser fatorado para o início da expressão, pois

$$a\big(\,|v\rangle \otimes |w\rangle\,\big) \;=\; \big(a\,|v\rangle\,\big) \otimes |w\rangle \;=\; |v\rangle \otimes \big(a\,|w\rangle\,\big).$$

O produto tensorial dos operadores lineares A em V e B em W, denotado por $A \otimes B$, é o operador linear em $V \otimes W$ definido por

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

Um operador linear genérico em $V \otimes W$ pode ser escrito como combinação linear de operadores da forma $A \otimes B$, porém um operador em $V \otimes W$ não precisa admitir a forma fatorada. Essa definição pode ser facilmente estendida para operadores do tipo $A : V \mapsto V'$ e $B : W \mapsto W'$. Nesse caso, o produto tensorial desses operadores é do tipo $(A \otimes B) : (V \otimes W) \mapsto (V' \otimes W')$.

Na Mecânica Quântica é muito comum usar operadores na forma de produto externo, por exemplo, $A = |v\rangle\langle v|$ e $B = |w\rangle\langle w|$. O produto tensorial de A por B pode ser representado das seguintes maneiras equivalentes entre si:

$$\begin{aligned} A \otimes B &= \big(\,|v\rangle\langle v|\,\big) \otimes \big(\,|w\rangle\langle w|\,\big) \\ &= |v\rangle\langle v| \otimes |w\rangle\langle w| \\ &= |v, w\rangle\langle v, w|\,. \end{aligned}$$

Se A_1, A_2 são operadores em V e B_1, B_2 são operadores em W então a composição ou o produto matricial das representações matriciais obedecem à propriedade

$$(A_1 \otimes B_1) \cdot (A_2 \otimes B_2) = (A_1 \cdot A_2) \otimes (B_1 \cdot B_2).$$

O produto interno de $|v_1\rangle \otimes |w_1\rangle$ por $|v_2\rangle \otimes |w_2\rangle$ é definido como

$$\big(\,|v_1\rangle \otimes |w_1\rangle\;,\; |v_2\rangle \otimes |w_2\rangle\,\big) \;=\; \big\langle v_1\big|v_2\big\rangle\,\big\langle w_1\big|w_2\big\rangle\,.$$

O produto interno entre vetores escritos como combinação lineares de vetores da base são calculados aplicando-se a propriedade de linearidade no segundo argumento do produto interno e a propriedade de conjugação-linear no primeiro argumento. Por exemplo,

$$\left(\left(\sum_{i=1}^{n} a_i\,|v_i\rangle\right) \otimes |w_1\rangle\;,\; |v\rangle \otimes |w_2\rangle\right) \;=\; \left(\sum_{i=1}^{n} a_i^*\,\big\langle v_i\big|v\big\rangle\right)\big\langle w_1\big|w_2\big\rangle\,.$$

A definição do produto interno implica que

$$\big\| \, |v\rangle \otimes |w\rangle \, \big\| \; = \; \big\| \, |v\rangle \, \big\| \cdot \big\| \, |w\rangle \, \big\|.$$

Em particular, a norma do produto tensorial de vetores de norma unitária é um vetor de norma unitária.

Quando usamos representações matriciais para os operadores, o produto tensorial pode ser calculado explicitamente via o *produto de Kronecker*. Seja A uma matriz de dimensão $m \times n$ e B uma matriz de dimensão $p \times q$, então

$$A \otimes B = \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ & \ddots & \\ A_{m1}B & \cdots & A_{mn}B \end{bmatrix}.$$

A matriz $A \otimes B$ tem dimensão $mp \times nq$. O produto de Kronecker pode ser usado para matrizes de qualquer dimensão, em particular para dois vetores,

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \; = \; \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ \\ b_2 \end{pmatrix} \\ \\ a_2 \begin{pmatrix} b_1 \\ \\ b_2 \end{pmatrix} \end{pmatrix} \; = \; \begin{pmatrix} a_1 b_1 \\ \\ a_1 b_2 \\ \\ a_2 b_1 \\ \\ a_2 b_2 \end{pmatrix}.$$

O produto tensorial é uma operação associativa e distributiva, porém não-comutativa, de modo que $|v\rangle \otimes |w\rangle \neq |w\rangle \otimes |v\rangle$. A maioria das operações sobre um produto tensorial de vários termos é feita termo a termo:

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$

Por sua vez, o traço de um produto de Kronecker de matrizes é

$$\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\,\mathrm{tr}(B).$$

Se ambos operadores A e B são operadores especiais do mesmo tipo, como definidos na Sec. A.11, então o produto tensorial $A \otimes B$ também é um operador especial desse tipo. Por exemplo, o produto tensorial de operadores hermitianos é um operador hermitiano.

A soma direta de um espaço vetorial V consigo mesmo n vezes é um caso particular de produto tensorial. De fato, $V \oplus \cdots \oplus V$ é igual a $I \otimes V$, onde I é a matriz identidade de dimensão $n \times n$. Isso mostra que, de certa forma, o produto tensorial é uma construção a

partir da soma direta de espaços vetoriais, assim como o produto de números é uma construção a partir da soma de números. No entanto, o produto tensorial é mais rico do que a simples repetição de soma direta de espaços vetoriais. É natural definir potenciação tensorial, de fato $V^{\otimes n}$ quer dizer $V \otimes \cdots \otimes V$ com n termos.

Se o estado diagonal do espaço vetorial V é $|\mathrm{D}\rangle_V$ e do espaço W é $|\mathrm{D}\rangle_W$, o estado diagonal do espaço $V \otimes W$ é $|\mathrm{D}\rangle_V \otimes |\mathrm{D}\rangle_W$. Portanto, o estado diagonal do espaço $V^{\otimes n}$ é $|\mathrm{D}\rangle^{\otimes n}$.

A.15 Registradores

Um *registrador* é um conjunto de qubits tratados como um sistema composto. Suponha que temos um registrador com 2 qubits. A base computacional é

$$|0,0\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |0,1\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |1,0\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |1,1\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Um estado genérico desse registrador é

$$|\psi\rangle = \sum_{i=0}^{1}\sum_{j=0}^{1} a_{ij}\,|i,j\rangle$$

onde os coeficientes a_{ij} são números complexos que satisfazem ao vínculo

$$\left|a_{00}\right|^2 + \left|a_{01}\right|^2 + \left|a_{10}\right|^2 + \left|a_{11}\right|^2 = 1.$$

Para facilitar a generalização para n qubits, é usual compactar a notação convertendo de base binária para base decimal. A base computacional para um registrador de 2 qubits na notação decimal é $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. Na base binária podemos determinar o número de qubits contando o número de dígitos dentro do *ket*, por exemplo, $|011\rangle$ ser refere a três qubits. Na base decimal não podemos determinar a princípio qual é o número de qubits. Essa informação deve estar implícita. Podemos sempre voltar atrás, escrever o número decimal na base binária e recuperar a notação explícita. Nessa notação compacta, um estado genérico de um registrador com n qubits é

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

onde os coeficientes a_i são números complexos que satisfazem ao vínculo

$$\sum_{i=0}^{2^n-1} \left|a_i\right|^2 = 1.$$

O estado diagonal de um registrador de n qubits é o produto tensorial dos estados diagonais de cada qubit, ou seja, $|\mathrm{D}\rangle = |+\rangle^{\otimes n}$.

Sugestões para Leitura

A quantidade de bons livros de Álgebra Linear é muito grande. Para um contato inicial, sugerimos as Refs. [22, 1, 2, 10]; para uma abordagem mais avançada sugerimos a Ref. [9]; para quem já domina os conceitos básicos e está interessado apenas na aplicação da Álgebra Linear na Computação Quântica, sugerimos a Ref. [14].

Bibliografia

[1] Tom M. Apostol. *Calculus, vol. 1: One-Variable Calculus with an Introduction to Linear Algebra*. Wiley, New York, 1967.

[2] Sheldon Axler. *Linear Algebra Done Right*. Springer, New York, 1997.

[3] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, Nov 1996.

[4] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098–1105, Aug 1996.

[5] Bernard Diu Claude Cohen-Tannoudji and Frank Laloe. *Quantum Mechanics*. Wiley-Interscience, 2006.

[6] Bernard d'Espagnat. *Conceptual foundations of quantum mechanics*. Westview Press, 1999.

[7] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, Ph.D. Thesis, Caltech, 1997, quant-ph/9705052.

[8] David Griffiths. *Introduction to Quantum Mechanics*. Benjamin Cummings, 2nd edition, 2005.

[9] Kenneth M. Hoffman and Ray Kunze. *Linear Algebra*. Prentice Hall, New York, 1971.

[10] Roger Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[11] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, Inc., New York, NY, USA, 2007.

[12] Carlile C. Lavor, M.M.S. Alves, R.M. Siqueira, and S.I.R. Costa. *Uma Introdução à Teoria de Códigos*, volume 21 of *Notas em*

Matemática Aplicada. Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC), São Carlos, 1st edition, 2006.

[13] N. David Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, New York, NY, USA, 2007.

[14] Michael A. Nielsen and Isaac L. Chuang. *Computação Quântica e Informação Quântica*. Editora Bookman, 2005.

[15] Roland Omnès. *Understanding Quantum Mechanics*. Princeton University Press, 1999.

[16] Asher Peres. *Quantum Theory: Concepts and Methods*. Springer, 1995.

[17] Jonh Preskill. *Lecture Notes on Quantum Computation*. `http://www.theory.caltech.edu/~preskill/ph229`, 1998.

[18] J. J. Sakurai. *Modern Quantum Mechanics*. Addison Wesley, 1993.

[19] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):R2493–R2496, Oct 1995.

[20] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5):793–797, Jul 1996.

[21] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. A*, 452:2551, 1996, quant-ph/9601029.

[22] Gilbert Strang. *Linear Algebra and Its Applications*. Brooks Cole, February 1988.

Índice