# Capítulo 17

# Informação quântica

A teoria matemática da informação estuda o armazenamento, processamento e transmissão de informação [59]. A informação quântica é um campo que trata do armazenamento e processamento da informação por bits quânticos, os chamados *qubits*. No limite em que os qubits só apresentam dois estados permitidos (0 ou 1), temos a informação clássica fundamentada nos *bits*.

Um aspecto fundamental para o desenvolvimento da teoria matemática da informação foi a introdução de um conceito para quantificar a informação, propostos originalmente por Claude E. Shannon em 1948 [59], que deu o nome de entropia. Determinar a entropia do sistema representa um processo que quantifica a quantidade de incerteza envolvida no valor de uma variável aleatória ou na saída de um processo aleatório. Ou seja, passamos a tratar do armazenamento, do processamento e da comunicação da informação considerando a possibilidade de resultados probabilísticos. Assim sendo, os estados quânticos, que fundamentalmente representam probabilidades, passam a ser carregadores desta informação que pode ser armazenada, processada, comunicada.

A teoria de informação quântica é uma área de pesquisa relativamente recente e está muito atrelada ao conhecimento dos fundamentos da mecânica quântica. Não é possível cobrir adequadamente toda essa área que cresce rapidamente em um único capítulo, mas podemos apresentar o tema, introduzindo os princípios básicos e suas relações com os fundamentos da mecânica quântica. Ao longo do capítulo, outras referências serão fornecidas para estudos mais aprofundados.

## 17.1 Estados quânticos como carregadores de informação

### 17.1.1 A entropia de Shannon

Um dispositivo que armazene informação composto de $N$ bits[1] pode armazenar $W = 2^N$ distintos estados. Equivalentemente, o conteúdo máximo de informação do dispositivo (no caso, número de bits) é dado por $\log_2(W)$.

$W$ atinge seu valor máximo se todos os estados são igualmente prováveis, o que não é necessariamente verdade (um dado "viciado" terá probabilidades distintas, e com isso menos aleatoriedade, menos informação). A teoria que quantifica a informação foi introduzida por Shannon [59, 60] e define a chamada **entropia de Shannon** como um quantificador da informação num sistema, dada por:

$$H = -\sum_{i=1}^{W} p_i \log_2(p_i), \tag{17.1}$$

onde $p_i$ é a probabilidade de ocorrência do estado $i$.

Considere uma medida do sistema que resulte numa modificação das probabilidades de alguns estados, de tal forma que a entropia de Shannon seja reduzida no estado final. A diferença

$$I = H_{\text{inicial}} - H_{\text{final}}, \tag{17.2}$$

é a quantidade de informação dada pela medida. Se a medida revela um estado de mensagem final único, então as probabilidades finais serão 1 para o estado único e todos os demais $p_i$ serão nulos, gerando $H_{\text{final}} = 0$. Neste caso a quantidade de informação dada pela medida será:

$$I = -\sum_{i=1}^{W} p_i \log_2(p_i), \tag{17.3}$$

que deve ser interpretada como a informação *média*, resultado de se tomar a média de todas as possíveis mensagens transmitidas pelo sistema. A chegada de uma mensagem improvável ($p_i$ pequeno) carrega uma grande quantidade de informação ($\log_2(1/p_i)$ bits), mas a probabilidade disso acontecer é pequena. Enquanto a chegada de uma informação muito provável ($p_i \approx 1$) praticamente não carrega informação.

[1] A palavra "bit" é utilizada comumente para referir-se tanto ao dispositivo que armazena a informação, quando à informação em si.

### 17.1.2 Bits e qubits

Um bit de informação pode ser armazenado em um sistema quântico de dois níveis. Os estados da base podem ser descritos em um espaço de Hilbert como sendo $|0\rangle$ e $|1\rangle$, por exemplo. Consideremos, entretanto, que existe a possibilidade de superposição de um contínuo de estados puros:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle, \quad |c_0|^2 + |c_1|^2 = 1. \tag{17.4}$$

Como todos os espaços de Hilbert de dimensão 2 são isomórficos entre si, é possível pensar a equação (17.4) como sendo o estado de um sistema de spin-1/2. O estado de spin-1/2 mais geral possível é dado pelo operador de estado (ver §7.4, caso 1):

$$\rho = \frac{1}{2}(\mathbf{1} + \mathbf{a}\cdot\boldsymbol{\sigma})\,. \tag{17.5}$$

Os estados puros da equação (17.4) são aqueles para os quais **a** tem comprimento unitário. Essa classe de estados admite uma representação chamada **esfera de Bloch**, que apresentamos na Fig.17.1, onde foi escolhida a base $|0\rangle$ e $|1\rangle$ como os auto-estado de spin para cima e spin para baixo do operador $\sigma_z$.

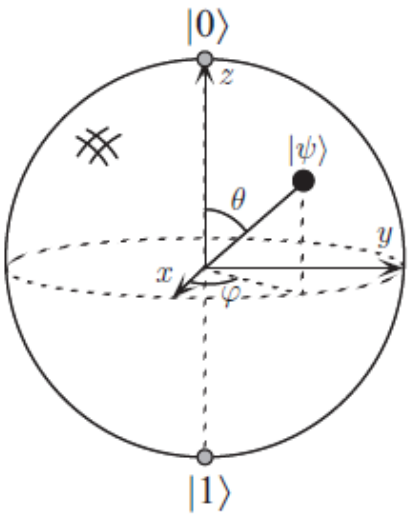


Figura 17.1: Esfera de Bloch: uma representação de um qubit. Extraído de [5].

Note que variando $\theta$ e $\varphi$ temos diversos estados distintos, todos eles representando estados puros de dois níveis. Nesta base, os autovetores sob

o eixo x e y são denotados por $(|0\rangle \pm |1\rangle)/\sqrt{2}$ e $(|0\rangle \pm i|1\rangle)/\sqrt{2}$, que são os autoestados de $\sigma_x$ e $\sigma_y$, respectivamente, na base $\{|0\rangle, |1\rangle\}$.

Define-se que o espaço de Hilbert bidimensional gerado pelos kets da base $|0\rangle$ e $|1\rangle$ é a menor unidade quântica de informação, um bit quântico, batizado de **qubit**. A esfera de Bloch é a representação de um qubit. O termo qubit pode significar tanto o estado (o que acabamos de apresentar) como também a menor quantidade de informação quântica possível de ser armazenada em um sistema. O contexto servirá para distinguir entre os dois significados.

Assim como o caso dos bits, há diversas formas de realizar um qubit fisicamente. Uma primeira possibilidade são spins de átomos em uma armadilha. Outra possibilidade os estados de polarização dos fótons. Neste segundo caso, a esfera de Bloch representará os estados de polarização linear horizontal/vertical (ao invés de spin para cima/para baixo), $+45/-45$ (no lugar dos autoestados no eixo $x$) e luz circularmente polarizada para a direita/esquerda (no lugar dos autoestados no eixo $y$), como discutido em §8.2.

O problema principal na realização de qubits experimentalmente é o controle, não só da amplitude dos coeficientes da equação (17.4), mas também de sua fase relativa. A fase relativa entre qubits é bastante sensível a perturbações externas, e a perda da estabilidade na diferença de fase é chamada de **decoerência**. Na prática, a escolha de como realizar um qubit será determinada pela facilidade de se minimizar a decoerência.

Finalizando, quando estamos tratando de estados de superposição como na equação (17.4), dizemos que estamos lidando com informação quântica. Quando estamos tratando de quaisquer estados ortogonais $|0\rangle$ e $|1\rangle$ para armazenar e transportar informação, podemos dizer que estamos lidando com informação clássica, que é um caso limite. Seja a informação manipulada por bits ou por qubits, trata-se de **teoria da informação**.

## 17.2 Alguns teoremas em informação quântica

A sub-área da informação quântica está para a mecânica quântica assim como a termodinâmica está para a mecânica clássica. Os resultados da termodinâmica podem, em princípio, ser obtidos a partir de premissas básicas da mecânica clássica. Porém, devido à construção da própria termodinâmica, há muitos resultados que ampliam a compreensão de sistemas clássicos, em especial a segunda lei da termodinâmica. Lembremos que a segunda lei da termodinâmica proíbe a ocorrência de alguns fenômenos.

Na informação quântica a situação é similar. Os teoremas que serão

apresentados aqui são derivados de conceitos fundamentais de mecânica quântica mas, uma vez estabelecidos, ampliam a sua compreensão, em especial no sentido de proibir a existência de alguns dispositivos e/ou processos.

**Teorema 14 (Teorema da não-clonagem)** *É impossível para qualquer dispositivo receber um estado quântico desconhecido e arbitrário como entrada e reproduzir exatamente o mesmo estado e uma cópia dele como saída. Ou seja, é impossível clonar um estado quântico.*

Este teorema foi demonstrado na seção 8.1, e o leitor deve rever a prova para relembrar os conceitos.

**Teorema 15** *É impossível determinar o estado quântico desconhecido de um sistema único e individual, mesmo considerando qualquer quantidade de medidas ou sequência de medições.*

Um operador de estados pode ter diversos termos na diagonal e fora dela. Na seção 8.2 descrevemos o número de medidas necessárias para determinar um estado quântico, sendo necessário obter informações a partir de medidas diversas em um ensemble de cópias do sistemas igualmente preparadas. É impossível, entretanto, obter todas as informações de um estado estatístico a partir de uma única cópia.

**Teorema 16** *É impossível, para qualquer dispositivo, distinguir de forma inequívoca, estados não-ortogonais.*

Para provar o teorema 16, considere que uma operação de medição leva o sistema $|\psi_1\rangle \otimes |\chi_0\rangle$ em $|\psi_1\rangle \otimes |\chi_1\rangle$, onde $|\psi_1\rangle$ representa o estado que está sendo medido, $|\chi_0\rangle$ o aparelho de medida antes da medição e $|\chi_1\rangle$ o aparelho após a medição. Equivalentemente, $|\psi_2\rangle \otimes |\chi_0\rangle \rightarrow |\psi_2\rangle \otimes |\chi_2\rangle$. Para que o dispositivo de medida seja capaz de distinguir os estados inequivocamente, temos que $\langle\chi_1|\chi_2\rangle = 0$. Mas se isto é verdade, e considerando que uma medida é um processo de transformação unitário, o produto interno dos estados antes da medida também deve ser nulo, e isto implica em $\langle\psi_1|\psi_2\rangle = 0$. Se $\langle\psi_1|\psi_2\rangle \neq 0$, necessariamente $\langle\chi_1|\chi_2\rangle \neq 0$, o que prova o teorema.

Esses três teoremas formam a base da teoria da informação quântica. Como todos os três são **impossibilidades** de se realizar algo, fica o questionamento da relevância prática dessa teoria. Nas próximas seções veremos que mesmo fundamentado em impossibilidades e incertezas, a informação quântica possui relevância prática extremamente poderosa, a ponto de tornar possível cálculos que são impraticáveis com computação clássica.

## 17.3 Transmissão quântica de informação

Qualquer processo de envio de informação entre aquele que envia a informação e o que recebe (com processamento de informação ou não) é chamado de um **canal**. Os conceitos básicos que definem os canais quânticos de informação são os conceitos familiares de preparação de estados (remetente) e medidas (destinatário).

Os teoremas que estabelecemos na seção anterior, em princípio, poderiam nos demonstrar que a comunicação quântica é inferior à atual comunicação clássica. Porém, devido justamente aos teoremas, é possível estabelecer resultados superiores aos clássicos, por exemplo em processos de proteção de informação, de criptografia de dados, numa subárea chamada de **criptografia quântica**, um dos primeiros e maiores triunfos da informação quântica. Antes de entrarmos nesse tópico, mais alguns aspectos elementares da teoria da informação quântica serão introduzidos.

### 17.3.1 Tipos relevantes de probabilidade

Um aspecto fundamental da M.Q. é a chamada **causalidade estatística**, que é uma forma de causalidade mais fraca que o determinismo. Isto é, um sistema quântico tem probabilidade (ou propensão) $p \leq 1$ de estar num determinado estado enquanto que um sistema clássico estará ou não em um determinado estado, com 100% de certeza.

Diante disso, a preparação de um estado tem influência causal nos resultados de medidas futuras, mas não determina os resultados individualmente. O estado determina apenas a probabilidade de obter tal resultado. Se o experimento pode ser repetido inúmeras vezes com igual preparação, então teremos um ensemble de resultados que pode ser significativo. A frequência em que vários desses resultados ocorrem podem ser estudados com um número vasto de técnicas estatísticas. Uma típica probabilidade quântica será:

$$P(D/\rho) = \mathrm{Tr}(E_\omega \rho), \tag{17.6}$$

em que $\rho$ é o operador de estado (matriz densidade) e $E_\omega$ é um projetor no subespaço $\omega$ do espectro de uma dada variável dinâmica que estamos interessados em medir. $P(D/\rho)$ mede a probabilidade do resultado $D \in \omega$, condicionado ao estado $\rho$ ocorrer. Note que a preparação do estado é extremamente relevante para a obtenção da probabilidade. Por causa disso, probabilidades quânticas são chamadas de **irredutíveis**: o operador $\rho$ carrega toda a informação necessária sobre probabilidade.

Vamos considerar agora um tipo diferente de problema. Suponha que comecemos com algum resultado $D$ de uma medida e queremos inferir qual

o estado desconhecido que a produziu. O teorema 15 da seção anterior estabelece que é impossível determinar o estado de um sistema completamente desconhecido através de qualquer tipo de medida. Porém, ainda é possível extrair **informação** do sistema, embora seja impossível determinar o seu estado de forma completa. Para fazer isso queremos calcular $P(\rho/D)$, ou seja, qual é a probabilidade de se ter um dado estado $\rho$ condicionado aos dados $D$. Pelo teorema de Bayes, equação (1.73), tem-se:

$$P(\rho/D\&C) = P(D/\rho\&C)\frac{P(\rho/D)}{P(D/C)}, \tag{17.7}$$

aqui o símbolo $C$ denota qualquer tipo de informação que possa ser relevante. Enquanto a equação (17.6) possui a interpretação de ensemble, na equação (17.7) pode-se considerar apenas um resultado que foi gerado por um estado desconhecido. Por isso chamamos a equação (17.6) de **indução** de probabilidade e a equação (17.7) de **inferência** de probabilidade. No segundo caso não é possível obter o estado com certeza, mas é possível inferir alguns candidatos que são melhores que outros. Nesse sentido, essa probabilidade é uma inferência, não uma determinação.

### 17.3.2 Transmissão de informação - alguns exemplos

Como um exemplo simples de transmissão de informação, considere um único qubit com vetores da base $|0\rangle$ e $|1\rangle$. Construímos, assim, dois pares de vetores ortogonais:

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \tag{17.8}$$

Para tornar o exemplo mais real, podemos pensar que são dois estados de polarização ortogonais da luz, onde $|0\rangle$ e $|1\rangle$ representam polarização linear horizontal e vertical, e $|+\rangle$ e $|-\rangle$ representam polarização linear em $+$ ou $-$ 45 graus. Considere agora que programamos uma máquina para emitir os estados $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ aleatoriamente, e vamos estudar as possibilidades de extração de informação.

**Exemplo 1** Como primeiro exemplo, a máquina envia aleatoriamente estados não-ortogonais $|1\rangle$ e $|+\rangle$, com mesma probabilidade de ocorrência. Entregamos essa máquina para um experimentador que sabe apenas que a máquina envia fótons, mas desconhece qualquer informação sobre seus estados possíveis de polarização, e lhe é pedido para descobrir qual estado é.

A matriz densidade desse problema é:

$$\rho = \frac{1}{2}(|1\rangle\langle 1| + |+\rangle\langle +|), \tag{17.9}$$

que na base $\{|1\rangle, |0\rangle\}$ fica:

$$\rho = \frac{1}{2}\Big[|1\rangle\langle 1| + \frac{1}{2}(|1\rangle\langle 1| + |1\rangle\langle 0| + |0\rangle\langle 1| + |0\rangle\langle 0|)\Big], \tag{17.10}$$

que pode ser escito na forma matricial

$$\rho = \begin{pmatrix} 1/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}. \tag{17.11}$$

Sem nenhuma informação sobre o sistema (símbolo $C$ no teorema de Bayes (17.7)) o experimentador não tem como extrair informação do sistema. Isto acontece porque existem infinitas possibilidades de se representar estados mistos a partir de estados puros, sendo impossível vislumbrar que o estado real é o da equação (17.9). Se a máquina estiver enviando uma mensagem codificada na base $|1\rangle$ e $|+\rangle$, o experimentador jamais será capaz de desvendá-la.

**Exemplo 2** Considere agora que a mesma máquina é entregue para um segundo experimentador, junto com a informação adicional de que as saídas possíveis da máquina são $|1\rangle$ ou $|+\rangle$. O segundo experimentador pode discernir em qual momento cada um dos estados foi preparado? Se isso for possível, então o experimentador será capaz de extrair informação que possa estar codificada neste canal.

O teorema 16 da seção anterior garante que é impossível distinguir entre dois estados não-ortogonais de forma inequívoca mas, ainda assim, é possível extrair informação dos estados. A probabilidade de medir cada estado individual, pelo teorema de Bayes, (17.7) pode ser reescrita como:

$$P(S_i/D\&C) = P(D/S_i\&C)\frac{P(S_i/C)}{P(D/C)}, \tag{17.12}$$

onde denotamos $S_1 = |1\rangle$ e $S_2 = |+\rangle$, e $C$ representa a nova informação disponível para o segundo experimentador. O fator $P(S_i/C)$ define a chamada probabilidade a priori de que o estado seja $S_1$. O termo a priori significa aqui que é antes da medida que gera o resultado $D$. Como os estados são gerados aleatoriamente e igualmente distribuídos:

$$P(S_1/C) = P(S_2/C) = 1/2. \tag{17.13}$$

Já para o termo do denominador, podemos usar a matriz densidade (17.11) para obter:

$$P(D = 0/C) = 1/4; \qquad P(D = 1/C) = 3/4. \tag{17.14}$$

O termo que sobra da equação que precisamos determinar são possíveis resultados das medidas realizadas em um dado estado $S_i$, $P(D/S_i\&C)$. Isso

se simplifica para $P(D/S_i\&C) = P(D/S_i)$ porque $S_i$ definido, a informação $C$ torna-se redundante. Os valores possíveis são:

$$P(D=0/S_1)=0; \quad P(D=1/S_1)=1; \qquad (17.15)$$
$$P(D=0/S_2)=1/2; \quad P(D=1/S_2)=1/2.$$

Finalmente, as probabilidades $P(S_i/D\&C)$ dos estados preparados para $|1\rangle$ ou $|+\rangle$, condicionadas às medidas $D=0$ e $D=1$ são:

| | $S_1 = \|1\rangle$ | $S_2 = \|+\rangle$ |
|---|---|---|
| $D=0$ | 0 | 1 |
| $D=1$ | 2/3 | 1/3 |

Usando esses resultados, vê-se que o experimentador é capaz de decidir, com 100% de certeza, que o estado preparado foi o $|+\rangle$ quando ele mede $D=0$. Estatisticamente, este resultado é observado em 25% das medidas (17.14), ou seja, em 25% das vezes ele estará seguro do resultado. Quando o resultado observado for $D=1$, existe 2/3 de chance do estado ser $|1\rangle$ e 1/3 de ser $|+\rangle$. Se o experimentador optar por assumir, sempre que medir $D=1$, que o estado é o estado $|1\rangle$, por uma simples opção pelo mais provável, estatisticamente ele estará certo em 2/3 dos casos, e isto acontecerá em 75% das medidas (17.14). No total, o número de vezes que o experimentador irá acertar o estado preparado será dado por $[(1\times 1/4)+(2/3\times 3/4)]$, que equivale a 75% das vezes. O teorema 15 proíbe uma taxa de sucesso de 100%.

Vamos calcular agora a entropia e a quantidade de informação contida neste caso. A entropia inicial é dada por (17.1)

$$H_{\text{inicial}} = -\frac{1}{2}log_2(\frac{1}{2}) - \frac{1}{2}log_2(\frac{1}{2}) = 1\,, \qquad (17.16)$$

Quando $D=0$ é medido, tem-se certeza do resultado, de forma que a entropia $H_{D=0}=0$. A quantidade de informação obtida nesta medida é (17.2) $H_{\text{inicial}} - H_{D=0} = 1$, ou seja, 1 bit de informação. Quando $D=1$ é medido, $H_{D=1} = -(2/3)log_2(2/3) - (1/3)log_2(1/3) = 0,91830$ bit. A quantidade de informação obtida nesta medida é $H_{\text{inicial}} - H_{D=1} = 0,08170$. Por fim, a informação média obtida neste caso é dada por $I_{\text{médio}} = (1/4)\times 1 + (3/4\times 0,0817) = 0,31128$ bit. Note que o valor é menor do que 1 bit, mas é melhor do que uma simples adivinhação.

## 17.4 Criptografia

A proteção da informação para sua transferência segura é realizada com métodos de criptografia, que são fundamentados em um procedimento de

encriptação da mensagem, usualmente chamado de chave. Uma vez conhecida a chave, a mensagem pode ser revelada. Por exemplo, substitua as letras do alfabeto por números, de forma ordenada ($a = 1, b = 2, c = 3...$)[2], qual a palavra formada pela sequência de números: 1 21 12 1? Este é um exemplo de mensagem (palavra) encriptada.

A segurança está então atrelada à dificuldade de se descobrir a chave. Um exemplo emblemático de quebra de chave em um processo criptográfico aconteceu na Segunda Guerra Mundial. O transmissor de rádio germânico era encriptado de tal forma que qualquer caractere era representado por um caractere diferente. A chave de encriptação era trocada aleatoriamente de forma frequente pelos nazistas.

A criptografia usada pelos nazistas não era completamente aleatória, possuía a restrição de que um caractere não era utilizado para representar ele próprio. Esta particularidade, junto com a consideração, pelos ingleses, de que o termo "Hiel Hitler" sempre aparecia no início ou no final da mensagem diminuiu significativamente a aleatoriedade estatística da chave utilizada pelos nazistas e fez com que, usando técnicas probabilísticas e a comparação das mensagens interceptadas, os britânicos (graças, principalmente, ao matemático Alan Turing) fossem capazes de desvendar a chave de encriptação e decodificar a mensagem.

A chave nazista apresentada é um exemplo de chave estática, pois é a mesma para uma dada mensagem. A mensagem se torna mais difícil de decodificar se a chave muda à medida que a mensagem é transmitida. Isso pode ser eficientemente implementado em binário. Primeiramente, gera-se uma chave aleatória de mesmo tamanho da mensagem e forma-se o criptograma ao adicionar a chave à mensagem. O efeito disso é que um bit da mensagem ficará inalterado, caso ele seja 0, e será trocado se ele for 1. Nesse esquema, dois caracteres iguais serão encriptados de forma ligeiramente diferente (o que não acontece na chave estática). É possível demonstrar que se a chave foi usada uma única vez e é totalmente aleatória, o criptograma é inquebrável. Porém, essa impossibilidade de quebra é teórica; na prática os comunicadores da mensagem terão que compartilhar algum tipo de chave prévia para compartilharem a chave criptográfica, o que insere algum tipo de padrão não-aleatório no criptograma. Não existe, portanto, um protocolo clássico de criptografia que seja 100% seguro.

[2] Considere as letras $k, y, w$!

### 17.4.1 Criptografia quântica

As características especiais da informação quântica podem ser usadas para realizar um processo de transferência de informação que não pode ser descoberto por um terceiro, sem que as pessoas envolvidas na transferência da mensagem descubram a espionagem. O método para isso é devido a Bennet e Brassard [61].

Os dois comunicadores são usualmente chamados de Alice e Bob, segundo o jargão da área de informação quântica. Suponha que Alice queira enviar uma mensagem para Bob de forma segura, usando a polarização de fótons como meio de comunicação. As polarizações lineares vertical/horizontal dos estados de fótons representam os valores binários 0 e 1. Alternativamente, Alice pode utilizar também as polarizações lineares a $\pm 45°$, e estes novos estados de polarização representarão os valores 0 e 1.

Alice pode encriptar sua mensagem criando uma chave que é a mudança aleatória de base, ou seja, ela escreve a mensagem utilizando a linguagem binária de 0's e 1's, mas mudando randomicamente entre as duas bases $\{|1\rangle,|0\rangle\}$ (horizontal/vertical) e $\{|+\rangle,|-\rangle\}$ $(+45°/-45°)$. Bob, para fazer a leitura binária, utiliza um polarizador, e ele também muda, de forma randômica, a orientação do seu filtro de polarização entre as duas bases, anotando a sequência de passagem ou não dos fótons pelo polarizador. Após uma sequência de fótons ter sido enviada, Alice revela, através de um canal público, a sequência de orientações da base que ela utilizou. Estatisticamente, na metade das tentativas, as bases de Bob coincidirão com as de Alice e, nesses caso, ele saberá com certeza qual valor ela enviou. Ou seja, ele terá a metade da informação obtida corretamente.

A desvantagem do método é que a metade da informação é perdida. A grande vantagem é que não é possível interceptar a mensagem sem que Bob descubra. Suponha que uma espiã, chamada Eva (outro jargão da área), tente interceptar a mensagem para decodificá-la. Eva mede a polarização de cada fóton da mesma forma que Bob faz, e Eva envia um outro fóton substituto do original para Bob, esperando permanecer como um intruso desconhecido. Como Eva desconhece a base utilizada por Alice, ela enviará bits com base aleatórias para Bob, que não são fidedignos à base original utilizada por Alice. Quando Alice publicar sua base e Bob usar a chave para decifrar a mensagem de Alice, ele obterá um resultado sem sentido. Com isso, Bob poderá alertar Alice sobre um intruso na comunicação entre eles, descobrindo a espionagem de Eva. Embora aquela mensagem tenha sido descoberta, o que aconteceu com os alemães na segunda guerra, que foi a decodificação de diversas mensagens após a descoberta do método nazista, não seria possível.

No mundo real, existe ainda a possibilidade de ruído entre os canais de

comunicação entre Alice e Bob, que podem causar decoerência da mensagem. É possível estender a teoria aqui desenvolvida para incluir esses casos e os resultados e características principais continuam valendo. Segue valendo, inclusive, o resultado mais forte da criptografia usando estados quânticos, que é o fato de um espião sempre ser detectado.

## 17.5 Emaranhamento

Um dos princípios fundamentais da M.Q., o princípio de superposição, produz resultados inesperados em informação quântica, como os exemplos já vistos da transmissão de informação §17.3 e da criptografia usando estados quânticos §17.4. Outros fenômenos ainda mais interessantes podem surgir quando consideramos o chamado **emaranhamento**, que consiste na aplicação do princípio de superposição para sistemas com dois ou mais componentes.

### 17.5.1 Definição de emaranhamento

Considere uma partícula que pode estar em dois estados, digamos $|u_1\rangle$ ou $|u_2\rangle$, e outra partícula que possa estar também em dois estados, digamos $|v_1\rangle$ ou $|v_2\rangle$. O seguinte estado de duas partículas:

$$\alpha_1\beta_1|u_1\rangle \otimes |v_1\rangle + \alpha_1\beta_2|u_1\rangle \otimes |v_2\rangle + \alpha_2\beta_1|u_2\rangle \otimes |v_1\rangle + \alpha_2\beta_2|u_2\rangle \otimes |v_2\rangle \quad (17.17)$$

é um estado separável, fatorável, pois pode ser escrito como um termo que separadamente descreve a partícula 1, e outro que descreve a partícula 2, da seguinte forma:

$$(\alpha_1|u_1\rangle + \alpha_2|u_2\rangle) \otimes (\beta_1|v_1\rangle + \beta_2|v_2\rangle) \quad (17.18)$$

Por outro lado, o estado

$$|u_1\rangle \otimes |v_1\rangle + |u_2\rangle \otimes |v_2\rangle \quad (17.19)$$

não é fatorável. Comparando (17.17) com (17.19), os dois estados seriam iguais se $\alpha_1\beta_1 = \alpha_2\beta_2 = 1$ e $\alpha_1\beta_2 = \alpha_2\beta_1 = 0$, o que é impossível.

Estados emaranhados são estados que **não** são separáveis. Ou seja, o emaranhamento é definido por uma negação, conforme comentamos brevemente em §8.3. O estado separável mais geral possível pode ser escrito como um produto tensorial de suas partes $a$ e $b$:

$$\rho^{ab} = \sum_i c_i \rho_i^a \otimes \rho_i^b, \quad (17.20)$$

onde $\sum_i |c_i|^2 = 1$. O estado será dito emaranhado se não puder ser escrito dessa forma, se ele não for separável. Caso o estado seja separável, ele é dito não-emaranhado.

### 17.5.2 Identificação de emaranhamento

Por ser uma negação, a definição de emaranhamento leva a muitos problemas práticos. Por exemplo, um estado misto possui uma infinidade de maneiras de ser escrito como superposição de outros estados, o que dificulta a identificação de se o estado em estudo pode ser descrito na forma da equação (17.20) ou não. Por isso, é necessário encontrar critérios para identificar emaranhamento, e estes critérios dependem se os estados são **puros** ou **mistos**.

**Estados puros:** Considere um estado puro $\rho^{ab} = \left|\psi^{ab}\right\rangle\left\langle\psi^{ab}\right|$ em que as componentes dele são escritas como traços parciais $\rho^a = \mathrm{Tr}^b\left(\rho^{ab}\right)$ e $\rho^b = \mathrm{Tr}^a\left(\rho^{ab}\right)$. De acordo com a tabela 8.2 de §8.3, um estado composto por duas partes só pode ser puro se as duas partes são puras, ou se as duas são não puras. Sendo assim, pelo teorema 10 temos duas possibilidades:

1. Ambos estados $\rho^a$ e $\rho^b$ são puros e o estado total é separável, ou seja, não é emaranhado.

2. Ambos estados $\rho^a$ e $\rho^b$ são não puros e o estado total não é separável, ou seja, é emaranhado.

Note que o primeiro caso corresponde a um estado não-correlacionado e que o segundo caso corresponde a um estado correlacionado (pela tabela 8.2). Ou seja, para estados puros, a definição de emaranhamento é exatamente a mesma de correlação e, portanto, para esse tipo de estados, as definições são equivalentes. Para um estado puro composto de duas partes, é condição necessária e suficiente que, se os estados parciais forem puros ($\mathrm{Tr}\left(\rho^{a,b}\right) = 1$), o estado total é não-emaranhado. Se os estados parciais são mistos ($\mathrm{Tr}\left(\rho^{a,b}\right) < 1$), então o estado total é emaranhado.

É importante frisar que um estado é emaranhado em relação a uma dada escolha de separação de componentes. Por exemplo, o estado fundamental do átomo de hidrogênio, quando escrito em termos de posição relativa ao centro de massa, não tem as posições do elétron e do próton emaranhadas, e a equação de Schrödinger é fatorizável, $\Psi(x_1, x_2) = \psi(x_1)\phi(x_2)$[3]. Se, por outro lado, escrevermos o sistema na base de coordenadas de elétron e próton, com $V(|\vec{r}_{e^-} - \vec{r}_{p^+}|)$ a posição das duas partículas será emaranhada, $\Psi(x_1, x_2) \neq \psi(x_1)\phi(x_2)$.

[3]Se $\Psi(x_1, x_2) = \psi(x_1)\phi(x_2)$, então $|\Psi\rangle = \int dx_1 dx_2 \Psi(x_1, x_2)|x_1, x_2\rangle =$
$= \left(\int dx_1 \psi(x_1)|x_1\rangle_I\right) \otimes \left(\int dx_2 \phi(x_2)|x_2\rangle_{II}\right) = |\psi\rangle_I \otimes |\phi\rangle_{II}$.

**Estados mistos:** Para estados mistos, os conceitos de correlação e emaranhamento são diferentes. Um importante critério para identificar emaranhamento em sistemas de dois componentes (usualmente chamados de **sistemas bipartite**) é o chamado critério de Peres [62].

Escolha um conjunto ortonormal de vetores de base na forma de um produto, $\left\{|m\rangle^a \otimes |\mu\rangle^b\right\}$. Os elementos da matriz densidade terão a forma $\rho_{m\mu,n\nu}$. A transposição *parcial* com respeito à primeira componente será:

$$\sigma_{m\mu,n\nu} = \rho_{n\mu,m\nu}, \tag{17.21}$$

onde somente os índices latinos foram trocados. Peres, então, pensou se a nova matriz, $\sigma_{m\mu,n\nu}$, possui as mesmas características de uma matriz densidade. Ela é hermitiana e possui traço unitário, mas não é claro que seja não negativa. Para ver o efeito da transposição parcial em matrizes separáveis, escrevemos:

$$\rho^{ab}_{m\mu,n\nu} = \sum_i c_i (\rho^a_i)_{mn} \otimes \left(\rho^b_i\right)_{\mu\nu}. \tag{17.22}$$

A operação consiste em substituir as matrizes $(\rho^a_i)_{mn}$ pela sua transposição parcial, que possui os mesmos autovalores não-negativos da matriz original. Com isso, a soma de matrizes não-negativas será também não-negativa. Concluímos que um critério necessário para a separabilidade é a transposição parcial ser não-negativa.

Horodecki, depois, provou que a condição de Peres é uma condição necessária e suficiente se a dimensão do espaço de Hilbert for $2 \otimes 2$ ou $2 \otimes 3$ [63]. Na literatura moderna, o critério necessário e suficiente para que um estado seja separável ser identificado com a sua transposição parcial ser não-negativa passou a ser chamado de critério de Peres-Horodecki. Em alguns textos é comum encontrar a terminologia **PPT**, que vem do inglês **Positive Partial Transposition**. Essa terminologia simplesmente indica estados cuja transposição parcial é não-negativa.

### 17.5.3 O significado físico do emaranhamento

Fisicamente, um estado emaranhado significa que a determinação (medição) da propriedade emaranhada de uma das partes define, de forma instantânea e violando a localidade clássica (ou relativística), a respectiva propriedade da outra parte. O protótipo de sistema emaranhado é o estado de singleto de duas partículas de spin-1/2 (ou dois qubits):

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). \tag{17.23}$$

Esse estado não tem definido a orientação de um único spin mas, sim, que a orientação dos dois spins é oposta. Se medirmos um dos spins, teremos certeza que o outro está na orientação oposta. Essa é uma característica dos estados emaranhados.

O estado acima descrito também é comumente chamado, na literatura de informação quântica, de **estado de Bell**. Isto porque é o estado mais simples que viola a desigualdade de Bell maximalmente, ou seja, esse estado é a violação da desigualdade de Bell com maior valor possível. Além disso, também é possível mostrar que a correlação quântica mais fraca é ainda assim mais forte do que qualquer tipo de correlação clássica [5]. O emaranhamento é um exemplo de correlação quântica.

Como a definição de emaranhamento é pela negação da separabilidade da matriz densidade, definir todos os atributos físicos ou fenômenos que constituem a natureza qualitativa do emaranhamento não é trivial. Como contra-exemplos, considerando uma classe de estados tais que $\mathrm{Tr}(A\rho) = \langle A \rangle > 0$, todas as misturas desses estados terão essa propriedade; alternativamente, uma mistura de estados separáveis também é separável. Uma mistura de dois estados emaranhados, entretanto, pode não ser um estado não-emaranhado, como veremos a seguir.

Considere os dois estados emaranhados:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\uparrow\rangle + |\downarrow\rangle \otimes |\downarrow\rangle), \tag{17.24}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\uparrow\rangle - |\downarrow\rangle \otimes |\downarrow\rangle). \tag{17.25}$$

As matrizes densidade para os estados puros $\rho_i = |\psi_i\rangle\langle\psi_i|$ são dadas por:

$$\rho_1 = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix}, \qquad \rho_2 = \begin{pmatrix} 1/2 & 0 & 0 & -1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1/2 & 0 & 0 & 1/2 \end{pmatrix}. \tag{17.26}$$

A mistura $\rho = \rho_1 + \rho_2$ normalizada será:

$$\rho = diag(1/2, 0, 0, 1/2), \tag{17.27}$$

que é um estado separável. A mistura de dois estados fortemente emaranhados gerou um estado que é separável. Essa característica do emaranhamento mostra que esse fenômenos é bem diferente do que qualquer outro observável físico conhecido.

O exemplo que usamos são estados que violam maximalmente a desigualdade de Bell. Por isso, pode-se pensar que emaranhamento é um exemplo

de correlação quântica mais forte que qualquer correlação clássica. Embora essa ideia seja verdadeira, ou seja, o emaranhamento realmente é mais forte que correlações clássicas, não é sempre verdade que sistemas emaranhados violarão a desigualdade de Bell.

Como exemplo, vejamos o estado de Werner. Ele é construído como a mistura de um estado de singleto com um estado totalmente despolarizado:

$$\rho_W = x|\psi_S\rangle\langle\psi_S| + \frac{1-x}{4}\mathbf{1}. \tag{17.28}$$

Pelo critério de Peres-Horodecki, o estado é emaranhado no intervalo $1/3 < x < 1$. Por outro lado, a desigualdade de Bell é válida para $x < 1/\sqrt{2}$. Isso significa que se $x$ estiver no intervalo $1/3 < x < 1/\sqrt{2}$, o sistema será emaranhado e não violará a desigualdade de Bell.

Há muito ainda a ser explorado nesse campo mas, em linhas gerais, a definição de emaranhamento como a negação da separabilidade é demasiado abrangente e pode incluir diversos "tipos" de emaranhamento sobre um mesmo nome ou estrutura. Essas distinções entre diferentes classes de emaranhamento são difíceis de perceber em baixa dimensão, como $2 \otimes 2$, mas são mais fáceis de ser investigadas em dimensões mais altas. A relação entre o uso do estado de Werner e sua eficiência para realizar o teleporte quântico (veremos melhor na seção seguinte) pode ser encontrada em [64].

Para mais detalhes sobre os diferentes tipos de emaranhamento, e a presença de classes de emaranhamento em altas dimensões, sugerimos as referências [65, 66, 67]

## 17.6 Teletransporte de estados quânticos

Considere que você queira enviar uma fotografia para alguém que vive em outro lugar. Você pode enviar essa fotografia pelo serviço de correios, e neste caso a fotografia terá sido **transportada**. Alternativamente, em vez de enviar a própria fotografia, você pode enviar um arquivo digital que contém informação sobre a fotografia, de tal forma o signatário possa recriá-la. Neste caso, a fotografia foi **teletransportada**.

Por teletransporte de estados quânticos entendemos algum tipo de operação que produz uma descrição completa de um estado existente em outro local. Como no caso clássico, a informação sobre o estado deve ser enviada a alguém que poderá recriar o estado completamente. Entretanto, o teorema da não clonagem, teorema 14, e o da impossibilidade de se determinar um estado com medidas em apenas um objeto, teorema 15, impedem que o teleporte de um estado quântico arbitrário através de métodos usuais de informação seja

possível. Porém, Bennett *et al.* [68] mostraram ser possível implementar o teleporte usando um canal de informação clássico utilizando pares de partículas em estados quânticos emaranhados.

O método de teletransporte de estados quânticos deve seguir alguns passos, como exemplificado a seguir:

1. Consideremos que Alice tem uma partícula (índice $c$) cujo estado desconhecido é:
$$|\psi^c\rangle = u|0^c\rangle + v|1^c\rangle, \quad |u|^2 + |v|^2 = 1, \tag{17.29}$$
que ela quer teletransportar para Bob.

2. Defini-se uma base emaranhada para o sistema de dois qubits (também conhecida como estados de Bell):
$$\begin{aligned}
\left|\psi_+^{ab}\right\rangle &= \frac{1}{\sqrt{2}}\Big(|0^a\rangle\left|1^b\right\rangle + |1^a\rangle\left|0^b\right\rangle\Big) \\
\left|\psi_-^{ab}\right\rangle &= \frac{1}{\sqrt{2}}\Big(|0^a\rangle\left|1^b\right\rangle - |1^a\rangle\left|0^b\right\rangle\Big) \\
\left|\phi_+^{ab}\right\rangle &= \frac{1}{\sqrt{2}}\Big(|0^a\rangle\left|0^b\right\rangle + |1^a\rangle\left|1^b\right\rangle\Big) \\
\left|\phi_-^{ab}\right\rangle &= \frac{1}{\sqrt{2}}\Big(|0^a\rangle\left|0^b\right\rangle - |1^a\rangle\left|1^b\right\rangle\Big),
\end{aligned} \tag{17.30}$$
que serão utilizados por Alice e Bob para o teletransporte da informação. Esses estados são ortonormais. Assim como o estado singleto (o segundo da sequência) todos eles violam maximalmente a desigualdade de Bell e, além disso, um pode ser transformado no outro através de uma única transformação unitária.

   Para preparar a comunicação, Alice e Bob precisam compartilhar um estado emaranhado, por exemplo o estado $\left|\psi_-^{ab}\right\rangle$. Alice fica com a partícula $a$ e Bob com a $b$. O estado de três partículas será dado por:
$$\begin{aligned}
\left|\psi^{abc}\right\rangle &= |\psi^c\rangle\left|\psi_-^{ab}\right\rangle = \\
&\frac{1}{\sqrt{2}}\Big(u|0^c\rangle|0^a\rangle\left|1^b\right\rangle - u|0^c\rangle|1^a\rangle\left|0^b\right\rangle + v|1^c\rangle|0^a\rangle\left|1^b\right\rangle - v|1^c\rangle|1^a\rangle\left|0^b\right\rangle\Big).
\end{aligned} \tag{17.31}$$

   Note que $\left|\psi^{abc}\right\rangle$ contém todos os estados de $a$ e $c$ necessários para reescrever a equação (17.31) na base de Bell para estas duas partículas

$\{|0^c\rangle|0^a\rangle, |1^c\rangle|0^a\rangle, |0^c\rangle|1^a\rangle, |1^c\rangle|1^a\rangle\}$. E equação (17.31) pode ser então reescrita como:

$$\begin{aligned}\left|\psi^{abc}\right\rangle = \frac{1}{2}\Big[&\left|\psi_+^{ca}\right\rangle\left(-u\left|0^b\right\rangle + v\left|1^b\right\rangle\right) + \left|\psi_-^{ca}\right\rangle\left(-u\left|0^b\right\rangle - v\left|1^b\right\rangle\right) \\ &+ \left|\phi_+^{ca}\right\rangle\left(-v\left|0^b\right\rangle + u\left|1^b\right\rangle\right) + \left|\phi_-^{ca}\right\rangle\left(v\left|0^b\right\rangle + u\left|1^b\right\rangle\right)\Big]. \end{aligned} \tag{17.32}$$

É importante notar que $c$ não está emaranhado com $a$ ou $b$ mas o estado $ca$ está emaranhado com $b$.

3. O próximo passo consiste em Alice realizar medidas conjuntas das partículas $a$ e $c$ para definir um estado de Bell. Se ela medir, por exemplo, $\left|\psi_+^{ca}\right\rangle$, como há emaranhamento com a partícula de Bob, ele saberá que seu estado é o $\left(-u\left|0^b\right\rangle + v\left|1^b\right\rangle\right)$ (ver 17.32).

4. Por fim, Alice conta a Bob qual foi seu estado de Bell encontrado, e a partir dessa informação, Bob saberá qual transformação unitária ele terá que realizar para recuperar o estado inicial original. No caso do nosso exemplo, como Bob conclui que seu estado é o $\left(-u\left|0^b\right\rangle + v\left|1^b\right\rangle\right)$, ele realiza a operação:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -u \\ v \end{pmatrix}^b = \begin{pmatrix} u \\ v \end{pmatrix}^b = |\psi^c\rangle. \tag{17.33}$$

Cada um dos possíveis estados de Bell de $ac$ que Alice pode encontrar indicará que Bob está com uma combinação linear específica de $\left|0^b\right\rangle$ e $\left|1^b\right\rangle$, e para cada combinação haverá uma operação unitária específica para reconstruir $|\psi^c\rangle$. Alice só precisa dizer qual estado de Bell $ac$ ela mediu.

Note que nenhuma das operações descritas depende de $u$ e $v$ que definem o estado $|\psi^c\rangle$. O procedimento não viola o teorema da não-clonagem, pois permanece existindo uma única cópia do estado $|\psi^c\rangle$ no final. O estado inicial foi alterado pela medida de Alice e recuperado pela transformação de Bob. Efetivamente, podemos dizer que o estado $c$ de Alice foi teletransportado para a partícula $b$ de Bob.

### 17.6.1 Realização experimental do teletransporte

Para a realização experimental do teletransporte, de acordo com o protocolo estabelecido, é necessário realizar três tarefas:

- (i) produzir estados emaranhados (estado de Bell) $ab$;
- (ii) Alice deve ser capaz de medir qual estado de Bell $ac$ ela possui;
- (iii) Bob deve ser capaz de realizar as transformações unitárias para obtenção do estado $c$ a partir do estado $b$.

O primeiro é bem conhecido, conforme comentamos na seção 16.5, usando, por exemplo, o decaimento do positrônio ou a conversão paramétrica descendente.

O terceiro também é bem conhecido. Se ignorarmos alguma fase relativa que não afete o estado final e usando o mesmo exemplo de fótons como qubits, as transformações unitárias são rotações que podem ser feitas utilizando elementos ópticos bem conhecidos, com as placas de meia onda.

O procedimento menos trivial neste caso é o segundo, o de distinguir os estados de Bell. Já foi demonstrado que esta tarefa é impossível de ser realizada via óptica linear, com o uso de divisores de feixe, polarizadores e reguladores de fase [69]. Porém, mesmo assim, essa medida ainda é possível.

Usando a interpretação usual de spin para qubits, os quatro estados de Bell são os autovetores dos três operadores que comutam: $\sigma_x \otimes \sigma_x$, $\sigma_y \otimes \sigma_y$ e $\sigma_z \otimes \sigma_z$. Os autovalores para esses operadores estão mostrados na tabela abaixo:

| | $\sigma_x \otimes \sigma_x$ | $\sigma_y \otimes \sigma_y$ | $\sigma_z \otimes \sigma_z$ |
|---|---|---|---|
| $\psi_+$ | $+1$ | $+1$ | $-1$ |
| $\psi_-$ | $-1$ | $-1$ | $-1$ |
| $\phi_+$ | $+1$ | $-1$ | $+1$ |
| $\phi_-$ | $-1$ | $+1$ | $+1$ |

É suficiente medir quaisquer dois dos três operadores, pois eles satisfazem a identidade $(\sigma_x \otimes \sigma_x)(\sigma_y \otimes \sigma_y)(\sigma_z \otimes \sigma_z) = -1$.

Suponha que Alice escolha medir $\sigma_z \otimes \sigma_z$ e depois $\sigma_x \otimes \sigma_x$. A primeira medida determina se a componente $z$ dos spins são paralelas ou anti-paralelas (isto é, distingue entre $\psi$ ou $\phi$). É essencial que esse procedimento seja feito sem determinar os estados de $\sigma_z$ pra ambas partículas. Isso ocorre porque $\sigma_x \otimes \mathbf{1}$ e $\mathbf{1} \otimes \sigma_z$ não comutam com $\sigma_x \otimes \sigma_x$.

O método anterior, obviamente, irá destruir o estado de Bell, mas isso não é tão importante. O que importa é que o teleporte ocorra. Outras técnicas mais sofisticadas foram produzidas para distinguir estados de Bell e realizar teleporte. Recentemente [70] foi usado um par de estados atômicos de dois átomos únicos de rubídio como um par emaranhado em uma cavidade ótica

e, com isso, os autores foram capazes de distinguir os quatro estados de Bell e conseguir o teleporte em uma distância de 21 metros.

## 17.7 Informação quântica de pares independentes

Em vez de preparar ensembles de partículas (ou de sistemas) separados, poderíamos preparar ensembles de pares ($\rho \otimes \rho$) ou de tripletos ($\rho \otimes \rho \otimes \rho$). Como não há correlação, é de se esperar que nenhuma informação nova possa ser tirada dessa preparação.

Porém, foi demonstrado por Peres e Wootters [71] que medidas de probabilidade conjunta de duas partículas fornece mais informação do que medidas individuais em cada uma das duas partículas.

A título de curiosidade, realizando medidas individuais nos spins, Peres e Wootters conseguiram uma informação média de $1,05228$ bits. Usando distribuição conjunta de probabilidade e medindo em ambos spins de um tripleto simultaneamente, eles conseguiram uma informação média de $1,36907$ bits, um valor bem mais alto que o anterior.

A possibilidade de se obter mais informação a partir de medidas conjuntas em pares de partículas não seria surpreendente se estivéssemos tratando de um sistema emaranhado mas, aqui, estamos sempre tratanto de sistemas separáveis. Peres e Wootters, inteligentemente, sugeriram que esse caso é o inverso do teorema de Bell: no teorema de Bell, as medidas são individuais em um sistema correlacionado. Aqui o sistema é descorrelacionado, porém as medidas se relacionam a um observável não fatorizável.

## 17.8 Mensuráveis

O postulado básico da M.Q. afirma que observáveis são representados por operadores hermitianos e estados puros são vetores no espaço de Hilbert. Porém, a afirmação inversa, que todos os operadores hermitianos representam quantidades mensuráveis e que todos os vetores representam estados não é imediatamente demonstrável dos postulados.

A comunidade científica de informação quântica segue uma visão bastante otimista sobre esse tema: ela acredita que se uma operação é baseada em transformações unitárias e projetores ela pode, em princípio, ser implementada experimentalmente. Veremos essas questões mais de perto nessa seção.

### 17.8.1 Observáveis locais

Nesse texto consideraremos observáveis locais como variáveis dinâmicas de uma única partícula, como sua posição, momento ou spin. Por simplicidade consideraremos espaços de Hilbert de dimensão finita para dar dois exemplos.

De forma geral, para observáveis locais, existe a correlação entre operadores Hermitianos de dimensão $(2s+1)$ e variáveis dinâmicas de spins de momento angular de spin $s$.

Já comentamos no capítulo 9 que é possível medir todas as componentes de spin para um sistema de uma partícula de spin $s = 1/2$. Nesse caso, sim, todos os operadores hermitianos descrevem quantidades mensuráveis.

Para spin $s = 1$, por exemplo, a situação é diferente. O estado possui um conjunto de 9 componentes, enquanto as combinações lineares da identidade e das matrizes de Pauli formam um conjunto de 4 componentes apenas. Nesse caso, seguindo [72], é possível realizar medidas que são combinações tensoriais de dipolos, quadrupolos etc. de spin. Então, de forma geral, todas as matrizes hermitianas de sistemas de spin de dimensão $(2s + 1)$ são, em princípio, mensuráveis.

### 17.8.2 Observáveis não-locais de dois objetos

Consideramos como observável não-local um conjunto de variáveis pertencendo conjuntamente a um par de objetos que não estão conectados de nenhuma forma.

No caso de observáveis não-locais é mais difícil estabelecer se é possível ou não mensurá-los. Num sistema de duas partículas de spin-1/2, por exemplo, não podemos medir o spin total, apenas uma componente dele.

Para uma medida coletiva, por exemplo $(J_x J_z + J_z J_x)$, há uma estrutura quadrupolar, que é impossível de ser obtida a partir de partículas individuais de combinações de dipolos. Essa estrutura quadrupolar é dependente do estado orbital do sistema, que pode ser medido. Porém, medir o estado orbital nada diz a respeito de $(J_x J_z + J_z J_x)$. Portanto, em um caso como esse, não há um procedimento de Stern-Gerlach generalizado, como aquele estabelecido em [72], que nos permita decidir se uma medida coletiva de observável não-local é mensurável.

## 17.9 Computação quântica

A aplicação mais ambiciosa da informação quântica é a construção e desenvolvimento de um computador quântico. Essa é uma área muito ativa e frutífera de pesquisa, surgindo artigos com novas ideias todos os dias, e os

primeiros computadores quânticos começam a aparecer, sendo construídos por grandes companhias como IBM e Google. O que será apresentado aqui são apenas os conceitos fundamentais, sendo esta uma área já extremamente complexa do ponto de vista teórico e de implementação experimental, fora do escopo deste curso.

### 17.9.1 Operações quânticas (portas quânticas)

Os conceitos básicos da computação clássica digital é a manipulação de informação armazenada em bits discretos e manipulados pelas operações lógicas AND, OR ou NOT. Um computador quântico armazenaria informação em qubits.

Conforme já comentamos, um qubit é uma combinação linear dos estados $|0\rangle$ e $|1\rangle$ formando um espaço de Hilbert de dimensão 2. Um conjunto de $N$ qubits será descrito por um espaço de Hilbert de dimensão $2^N$. A transformação mais geral possível nesse espaço são transformações unitárias que, em particular, podem transformar um estado não-emaranhado em um estado emaranhado e vice-versa. Um teorema devido a Barenco *et al.* [73] demonstra que uma transformação geral unitária pode ser obtida pelo produto de operações unitárias locais (em um único qubit) e portas NOT controladas (CNOT *gates*), as quais agem em pares de qubits, um chamado controle e o outro alvo. A porta CNOT atua da seguinte forma:

$$\begin{aligned} &|0\rangle \otimes |0\rangle \to |0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle \to |0\rangle \otimes |1\rangle, \\ &|1\rangle \otimes |0\rangle \to |1\rangle \otimes |1\rangle, \quad |1\rangle \otimes |1\rangle \to |1\rangle \otimes |0\rangle, \end{aligned} \tag{17.34}$$

o primeiro bit é o controle e o segundo é o alvo. Quando o primeiro é zero, o segundo não é alterado. Quando o primeiro é um, o segundo é alterado. Na base de estados de bits a operação CNOT assume a forma matricial:

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{17.35}$$

escrita na base $\{00, 01, 10, 11\}$. Apesar de ser uma porta clássica (uma operação clássica) ela é muito importante. Por exemplo, considere a porta CNOT atuando no estado:

$$U_{CNOT}|+\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle), \tag{17.36}$$

onde $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, e a operação CNOT transformou um estado inicial separável em um dos estados de Bell maximalmente emaranhados. Como essa

porta permite transformar estados separáveis em estados emaranhados, ela é muito útil em computação quântica.

Outro exemplo de porta quântica é a porta controle unitário (CU *gate*), definida por:

$$|0\rangle \otimes |0\rangle \to |0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle \to |0\rangle \otimes |1\rangle, \tag{17.37}$$
$$|1\rangle \otimes |0\rangle \to |1\rangle \otimes U|0\rangle, \quad |1\rangle \otimes |1\rangle \to |1\rangle \otimes U|1\rangle, \tag{17.38}$$

que aplica uma operação unitária $U$ no bit alvo se o bit controle for $|1\rangle$. Outro exemplo importante é a porta de troca (swap gate), que troca os estados de controle e alvo da seguinte forma:

$$U_{swap}|\phi\rangle \otimes |\psi\rangle = |\psi\rangle \otimes |\phi\rangle. \tag{17.39}$$

Esta operação pode ser escrita como $U_{swap} = |0\rangle\langle 0| \otimes \mathbf{1} + |1\rangle\langle 1| \otimes \sigma_x$, que na base matricial usual é representada por:

$$U_{swap} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{17.40}$$

Superposição de estados também costuma ser necessário, e isso pode ser obtido com a porta Hadamard, que opera da seguinte forma:

$$U_H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \tag{17.41}$$
$$U_H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle, \tag{17.42}$$

que na base usual pode ser representada pela seguinte matriz:

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{17.43}$$

Quando se está construindo um computador quântico com várias operações quânticas é comum representar essas operações em um diagrama conhecido como **circuito quântico**. É uma forma bastante útil de se representar algoritmos para o computador quântico que estamos interessados em implementar. Para mais detalhes sobre o tema sugerimos [74].

### 17.9.2 Algumas portas quânticas impossíveis

Algumas operações quânticas, em consequência dos teoremas da seção 17.2, são proibidas. A estrutura geral de operações quânticas proibidas pode ser encontrada em [75].

Um exemplo de porta quântica impossível é a porta NOT universal (u-NOT). Em computação digital clássica essa porta troca o bit 0 pelo bit 1 e vice-versa. Quanticamente é possível fazê-lo para os kets $|0\rangle$ e $|1\rangle$ mas não é possível fazê-lo de modo geral. Essa impossibilidade pode ser vista em sistemas de spin-1/2. A operação u-NOT seria tal que trocasse todas as componentes de um eixo para o outro, como numa rotação de $\pi$ na esfera de Bloch. O problema é que uma rotação não altera os elementos que estão no eixo de rotação, logo ela não é suficiente para alterar todos os elementos da esfera de Bloch. Isso significa que não existirá uma operação unitária que conduzirá essa porta u-NO,T e portanto ela é impossível.

Outra impossibilidade é obter um qubit complementar. Essa operação seria transformar $|\psi\rangle \otimes |\omega\rangle \rightarrow |\psi\rangle \otimes \left|\psi^{\perp}\right\rangle$, que produz um qubit arbitrário e o seu complementar. Essa operação é impossível pois não é possível clonar estados, uma consequência do teorema (14), teorema de não clonagem,.

Outra impossibilidade é uma porta para superposição universal. Essa porta hipotética, u-SUP, receberia como input um estado arbitrário e produziria uma superposição de igual peso entre o estado e o seu complemento ortogonal. Essa seria uma versão da porta de Hadamard que é independente da escolha da base. Para que uma porta dessa possa ser implementada, ela deve preservar valores esperados entre dois vetores de estado arbitrários. Isso é verdade para larga classe de estados para os quais:

$$|\psi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle, \tag{17.44}$$

onde $\alpha$ e $\beta$ são reais. Porém, no caso geral, não podemos exigir que tais coeficientes sejam reais e assim o valor esperado não é preservado, implicando que uma porta de superposição universal não pode existir no caso geral. Para os casos onde os coeficientes são reais ela pode, sim, ser implementada.

### 17.9.3 Vantagens e aplicações da computação quântica

É possível resolver a equação de Schrödinger numericamente em um computador clássico usual. Como o computador quântico nada mais é que uma realização física da equação de Schrödinger para qubits é possível, em princípio, simular um computador quântico em um computador clássico.

Diante disso, fica o questionamento: então qual a vantagem de se investir tantos esforços em um computador quântico? A resposta reside, basicamente,

no fato de que em um computador quântico é possível realizar inúmeras outras tarefas que são praticamente impossíveis em um computador clássico devido ao custo de memória e computacional. Veremos alguns exemplos específicos.

### Simulações quânticas

Considere um sistema de spins numa rede como, por exemplo, um sistema magnético. Se a rede possuir $N$ spins a dimensão do espaço de Hilbert será $n_d = 2^N$ e a dimensão da matriz densidade será $n_d \times n_d$. Para resolver o sistema teríamos que resolver um conjunto de $N$ equações diferenciais acopladas cujo custo computacional será algum polinômio de $n_d$ que, por sua vez, cresce exponencialmente com $N$. Esse pequeno exemplo é suficiente para mostrar que a partir de um dado valor de $N$ é praticamente impossível resolver um sistema dessa forma em um computador clássico. O custo computacional e o consumo de memória cresce exponencialmente com o tamanho do sistema.

Por outro lado, em um computador quântico, seria necessário apenas $N$ qubits para representar um sistema de $N$ spins, resultando em um custo computacional que é polinomial em $N$ (e não mais exponencial). Essa diferença ressalta o poder computacional superior da computação quântica. Para $N > 20$, a computação quântica supera a clássica.

Recentemente a empresa Google publicou na revista Nature uma demonstração da supermacia quântica utilizando um computador quântico com 53 qubits [**?**]. Entretanto, ainda há muita incerteza na área sobre a execução dos computadores quânticos e até mesmo competição comercial. Portanto, a comunidade aguarda o desenvolvimento desta área que promete revolucionar a tecnologia da informação.

### Computação quântica numérica

Outra importante característica da computação quântica é a chamada **correção de erros**. Mesmo em um sistema digital clássico, de bits 0 e 1, existe a possibilidade de termos pequenos erros nos resultados dos bits. Porém, um sistema clássico possui mais tolerância ao erro e maior facilidade em corrigi-lo.

Por outro lado, qubits formam um contínuo, ao contrário dos bits discretos, o que dificulta a correção de erros. Existem diversos protocolos que foram desenvolvidos para implementar a correção de erros.

Uma forma de fazer isso é implementar sistemas de 3-qubits para representar os valores lógicos 0 e 1 de tal modo que um estado geral será dado por:

$$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle. \tag{17.45}$$

Nesse caso é possível corrigir erros através de medidas que são realizadas em dois qubits simultaneamente, uma vez que o erro aleatório não irá atingir os dois de forma sistemática. Isso é muito mais vantajoso do que se admitir que os valores lógicos são representados por qubits únicos.

Há, ainda, outras possibilidades como um protocolo de correção de erros usando estados emaranhados de sete qubits. Esse protocolo é superior ao que apresentamos por permitir a detecção e correção de erros em amplitude (os coeficientes $\alpha$ e $\beta$) e também em fases relativas. Sem os protocolos de correção de erros é extremamente questionável se a computação numérica quântica pode ser feita na prática.

### Transformadas de Fourier quânticas

Em muitas aplicações práticas e também na matemática pura existe a necessidade de se calcular a chamada transformada de Fourier discreta (DFT):

$$f_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N_1} e^{i2\pi jk/N} g_k. \tag{17.46}$$

O cálculo da DFT geralmente escala com $O(N^2)$. Para sistemas $N = 2^n$ é possível construir a transformada de Fourier rápida (FFT) e, usando um truque de se quebrar o sistema em grupos menores de $N/2$, $N/4$ partes e assim sucessivamente, é possível obter uma eficiência computacional da ordem de $O(N \log_2 N) = O(n2^n)$.

Podemos pensar numa transformada de Fourier quântica (QFT) que consiste em generalizar a equação (17.46) para vetores, que consiste em escrever $f = Mg$ com os elementos da matriz $M$ dados por:

$$M_{jk} = \frac{1}{\sqrt{N}} e^{i2\pi jk/N}. \tag{17.47}$$

A QFT consiste em atuar a transformada de Fourier nos estados da base da mesma forma que é feita por um computador quântico. A eficiência da QFT depende de como é possível escrevê-la em termos de portas quânticas e CNOT's. O problema tem uma solução elegante e bastante complicada que garante uma eficiência da ordem de $O(n^2)$, que é bem menor que a eficiência de $O(n2^n)$ da FFT. A QFT portanto é um importante recurso computacional quântico.

### Algoritmo de fatorização de Shor

Um problema antigo em teoria dos números é achar a fatoração de um número $N$ muito grande. Já comentamos, na seção 17.4, sobre a possibilidade

de troca de chaves de encriptação privadas. A encriptação RSA, uma das mais usadas, consiste em escrever um número $N = pq$ em que $p$ e $q$ são dois números primos muito grandes. Por outro lado se um espião invadir o canal de comunicação e for capaz de fatorar números grandes de forma eficiente, então ele será capaz de quebrar a criptografia e ler a mensagem.

Um dos algoritmos mais simples de se realizar tal fatoração é se encontrar todos os divisores de $N$ até o maior inteiro não maior do que $\sqrt{N}$. O problema desse método é que ele possui custo computacional de $O\left(2^{n/2}\right)$, que é uma exponencial (em linguagem de computação, é um problema NP-difícil, ou seja, um problema difícil que só pode ser resolvido em tempo não-polinomial).

Existe um algoritmo de teoria dos números, chamado algoritmo de fatoração de Shor, que é muito utilizado para se fatorar um número $N$ grande. A parte mais computacionalmente difícil desse algoritmo consiste em calcular o período de uma função que está estreitamente relacionada com o número que queremos fatorar. A solução desse algoritmo utiliza a FFT. Se for possível construir um computador quântico que implemente a QFT em tempo polinomial (conforme comentamos acima) seria possível, em princípio, quebrar uma criptografia RSA.

## 17.10 Informação quântica e os fundamentos da M.Q. (CARO ESTUDANTE, ESTA SEÇÃO AINDA ESTÁ EM DESENVOLVIMENTO. PODE HAVER ALGUMA FRAGILIDADE DE CONCEITO.)

Conforme vimos ao longo desde capítulo a informação quântica fornece inúmeras novas ferramentas e insights sobre a própria mecânica quântica e seus fundamentos.

Um exemplo histórico é o artigo EPR [50], mencionado no capítulo 16. Esse artigo levanta uma questão, que foi respondida de forma negativa, que mais tarde foi entendida nos termos do emaranhamento. Hoje, os chamados estados EPR (ou estados do gato de Schrödinger) são estados maximalmente emaranhados separados espacialmente. Emaranhamento é muito importante em comunicação, teleporte e computação quânticos.

### 17.10.1 Interpretação de estados quânticos

O debate acerca da interpretação apropriada para a MQ recebeu novas ideias às luzes da informação quântica. Três dicotomias são usualmente consideradas:

- individual vs. ensemble,
- ôntico vs epistêmico,
- objetivo vs. subjetivo.

Essas dicotomias estão relacionadas, mas não são totalmente equivalentes entre si. Vejamos melhor.

#### Individual vs. ensemble

A ideia central da interpretação de ensemble é que a MQ não prevê eventos individuais, mas a probabilidade de vários eventos possíveis. Em particular, ela não prevê resultados de medidas individuais. Mas se esse procedimento de medida puder ser repetido nas mesmas condições um grande número de vezes, então as probabilidades preditas pela MQ podem ser comparadas com a estatística dos resultados das medidas dos ensembles.

A interpretação de ensemble é preferida, conforme comentamos no capítulo 9, em detrimento da interpretação de partículas individuais. Em MQ é irrelevante falar sobre o vetor de estado de uma partícula individualmente e, aqui na Informação Quântica, essa afirmativa é suportada pelo teorema (15).

#### Ôntico vs. epistêmico

Esses dois conceitos foram importados da filosofia para a física quântica e antes de discutir essa dicotomia é importante entender o que esses conceitos significam.

Ôntico se refere à realidade. Essa realidade não precisa necessariamente ser observável, ou mensurável. É, de certa forma, similar aos conceitos **elementos da realidade** do artigo EPR [50]. Ou, melhor ainda, poderíamos dizer que os elementos da realidade de EPR são um conceito ôntico.

Em oposição, epistêmico se refere ao conhecimento, que em MQ poderíamos chamar de **informação**. Em geral a interpretação de ensemble é assumida como sendo epistêmica (por fornecer informação acerca das probabilidades do sistema físico) enquanto que a interpretação de partículas individuais é assumida como ôntica (no sentido de fornecer o estado real do sistema).

Para uma descrição mais completa sobre essa dicotomia é necessário construir um modelo ontológico que, de certa forma, abarca os estados que são ônticos e os que são epistêmico, permitindo uma discussão num nível matemático e não apenas filosófico. Para mais detalhes dessa discussão sugerimos [76].

### Objetivo vs. subjetivo

Essas duas categorias geralmente são contrastadas com o par ôntico-epistêmico, mas aqui existem algumas diferenças importantes. O termo subjetivo está associado ao conhecimento ou crença de alguém sobre algo. Por outro lado, objetivo se refere as propriedades físicas reais que não dependem de nenhuma percepção particular. Um modelo ôntico necessariamente será objetivo, enquanto que um modelo epistêmico pode ou não ser subjetivo.

Considere que o procedimento de preparação de estados gere uma distribuição de probabilidade de estados ônticos $P(\lambda|Q_\rho)$. Essa distribuição é uma caracterização objetiva do procedimento de preparação. Por outro lado se o operador tiver conhecimento sobre o funcionamento do dispositivo, ele irá conhecer a distribuição que ele produz. Por isso $P(\lambda|Q_\rho)$ também será um conhecimento subjetivo. Isso mostra que o conhecimento subjetivo é menos relevante na discussão sobre estados quânticos.

### Estados quânticos não descrevem conhecimento ou crença

O exemplo abaixo ilustra as ideias de probabilidade objetiva e subjetiva. Ele consiste num jogo onde um operador prepara um fóton num estado de polarização linear mas mantém o procedimento de preparação em segredo. Ele fala para Alice que o estado é um dentre dois e fala para Bob que é um dentre quatro.

Os estados de polarização vertical e horizontal são representados por $|0\rangle$ e $|1\rangle$ enquanto que os estados de polarização a 45 graus são representados por $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Esses estados possuem as seguintes matrizes densidade (são os quatro estados de Bob):

$$\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \rho_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{17.48}$$

$$\rho_+ = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, \quad \rho_- = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}. \tag{17.49}$$

O estado atual do fóton que foi preparado é $\rho_0$ mas nem Alice e nem Bob sabem desse fato, então eles precisam usar seu conhecimento incompleto para fazer predições. Alice dispõe dos estados $\rho_0$ e $\rho_1$ de tal forma que ela

poderá combiná-los com igual probabilidade para obter a **matriz densidade subjetiva**:

$$\rho_s = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}. \tag{17.50}$$

Bob possui quatro estados e poderá combiná-los com igual probabilidade para obter a mesma matriz $\rho_s$. Apesar de ambos obterem a mesma matriz densidade subjetiva, suas predições futuras serão diferentes por conta dos diferentes estados que ambos possuem.

Para decidir qual é o estado original, Alice e Bob medirão a polarização do fóton. Alice, ao se fazer uma medida para distinguir qual das duas possibilidade, encontrará a resposta correta para o estado inicial $\rho_0$. Porém, Bob, deverá usar o teorema de Bayes (1.73):

$$P(\rho|D\&C) = P(D|\rho\&C)\frac{P(\rho|C)}{P(D|C)}, \tag{17.51}$$

em que $C$ é a informação anterior de Bob, $D$ são os dados a partir das medidas e $\rho$ é um dois estados que ele por obter informação.

Como o conjunto de possíveis estados é invariante por rotações então $P(\rho|C) = 0,25$. Similarmente as probabilidade iniciais para os possíveis resultados das medidas de polarização, $D = 0$ e $D = 1$, são $P(D|C) = 0,50$. E teremos também:

$$P(0|\rho_0) = 1, \quad P(0|\rho_1) = 0, \quad P(0|\rho_+) = 0,5, \quad P(0|\rho_-) = 0,5, \tag{17.52}$$

de tal forma que a matriz densidade subjetiva de Bob será:

$$\rho_B = \begin{pmatrix} 0,75 & 0 \\ 0 & 0,75 \end{pmatrix}. \tag{17.53}$$

Devemos tomar cuidado porque a matriz densidade subjetiva não é uma matriz densidade "verdadeira". As matrizes densidade reais (de traço unitário, não-negativas e hermitianas) são as que usamos para os cálculos de valores esperados, $\mathrm{Tr}(\rho E_x)$, em que $E_x$ é o projetor no subespaço de interesse. Nesse sentido, as matrizes densidade real são **objetivas**, não requerendo qualquer menção ao conhecimento que se tem sobre o estado.

Por outro lado, para as matrizes densidade subjetivas, como o próprio nome indica, há uma certa **subjetividade** pois se assume o conhecimento a priori sobre o estado do sistema em uma forma que se pareça com uma matriz densidade.

Com isso podemos afirmar que a matriz densidade subjetiva **não** representa nenhum conhecimento do observador sobre o sistema. Consequentemente a

afirmação de que a interpretação dos estados quânticos como representantes do conhecimento é insustentável. Um observador pode ter conhecimento sobre algum sistema físico, ou sobre sua preparação, mas o sistema em si não terá conhecimento sobre nada.

## 17.11 Exercícios

**Exercício 17.1** *Resolva os exercícios do livro do Ballentine, [2].*