# 4
# Informação Quântica

A teoria da Informação Quântica foi basicamente desenvolvida na última década (3, 10, 16). Nosso objetivo neste capítulo é apresentar sua estrutura fundamental, o *bit quântico*, e justificar a enorme superioridade de computadores quânticos sobre computadores clássicos.

## 4.1
## O Qubit

Um espaço de Hilbert unidimensional possui, obviamente, apenas um vetor em sua base. Logo, ao considerarmos um sistema associado a tal espaço, este terá apenas um estado, não sendo, portanto, um sistema interessante para ser analisado.

Os sistemas relevantes mais simples são aqueles associados a espaços de Hilbert bidimensionais, ou seja, isomorfos a $\mathbb{C}^2$. Em computação quântica, sistemas deste tipo são conhecidos como bits quânticos (quantum bits) ou, abreviadamente, *qubits*. Assim como o bit é o conceito fundamental da computação clássica, o qubit é a unidade básica de construção de um computador quântico.

Analogamente ao bit clássico (o qual pode ser encontrado nos estados 0 ou 1), dois possíveis estados para um qubit são $|0\rangle$ e $|1\rangle$, os quais formam uma base ortonormal para o espaço bidimensional associado. A principal diferença entre o bit clássico e o bit quântico é que o qubit também pode ser encontrado em estados diferentes de $|0\rangle$ ou $|1\rangle$, já que, pelo Princípio da Superposição, é possível formar novos estados a partir de combinações lineares de estados ortogonais. Assim, qualquer estado de um qubit pode ser representado por:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \tag{4-1}$$

onde $\alpha$, $\beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$. Como nada é dito sobre o meio físico em que os vetores são construídos, estes podem representar, por exemplo, spin-up e spin-down de uma partícula, direção vertical e horizontal de polarização, etc.

Enquanto bits clássicos têm seus estados facilmente determinados, não é possível examinar um qubit e determinar seu estado quântico, isto é, os valores de $\alpha$ e $\beta$. Isto se deve ao seguinte: como vimos ao longo do capítulo

2, ao medirmos um observável deste estado que possui autovetores $|0\rangle$ e $|1\rangle$, obtemos o resultado $|0\rangle$ com probabilidade $|\alpha|^2$, e $|1\rangle$ com probabilidade $|\beta|^2$.

Agora, utilizando a igualdade $|\alpha|^2+|\beta|^2 = 1$, podemos reescrever a eq.(4-1) como:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right).$$

Sabemos que o fator $e^{i\gamma}$ não influencia a observação do sistema, logo pode ser ignorado:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle.$$

Os números $\theta$ e $\varphi$ definem um ponto na esfera unitária $S^2$, a qual é geralmente denominada esfera de Bloch. Ou seja, o espaço de estados de um qubit pode ser parametrizado pelos pontos desta esfera:

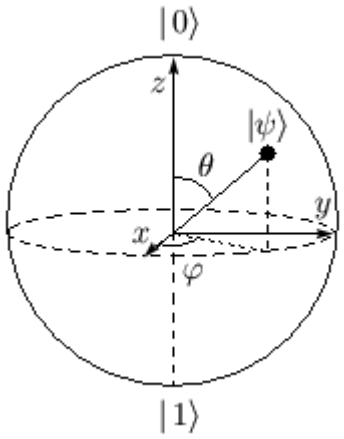


Figura 4.1

A partir desta representação podemos claramente afirmar que um qubit armazena infinita informação, já que a esfera unitária tem um número infinito de pontos. No entanto, não deve ser esquecido o fato de que ao observarmos um qubit obtemos apenas um bit de informação. Ou seja, somente com infinitas observações de qubits idênticos é que seríamos capazes de determinar os valores de $\alpha$ e $\beta$.

Assim, um qubit de fato representa infinita informação, desde que não seja observado. Pode parecer estranho não termos como medir a quantidade de informação com que trabalhamos, mas o que devemos compreender é que quando um sistema quântico isolado evolui, sem realizarmos quaisquer medições, a Natureza mantém guardadas todas as variáveis que descrevem tal sistema, como $\alpha$ e $\beta$, o que chamamos de "informação escondida". Como veremos mais adiante, o mais interessante é que a quantidade deste tipo de informação cresce exponencialmente com o número de qubits que utilizamos para

compor nosso sistema. É justamente esta informação quântica escondida que faz da Mecânica Quântica uma ferramenta tão poderosa para o processamento de informação.

## 4.2 Coexistência de Sistemas Quânticos

Ao considerarmos sistemas quânticos compostos, a primeira pergunta que nos preocupamos em responder é a seguinte: como descrever os estados de um sistema deste tipo? A resposta é dada pelo próximo postulado.

**Postulado VI**: *O espaço de Hilbert associado a um sistema físico composto é o produto tensorial dos espaços de Hilbert associados aos sistemas físicos individuais. Além disso, se os sistemas forem numerados de* 1 *até* $n$*, e o* $i$*-ésimo sistema (associado ao espaço* $\mathcal{H}_i$*) for preparado no estado* $|\psi_i\rangle$*, então o estado do sistema composto (ou* $n$*-partido) é*

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n. \tag{4-2}$$

Note a importância de que cada um dos sistemas tenha sido preparado separadamente: somente assim somos capazes de afirmar que o estado do sistema $n$-partido pode ser fatorado como na eq.(4-2). Neste caso diremos que o estado é um *estado-produto*, ou *desemaranhado*. Sua principal característica é que ao aplicarmos alguma transformação a um dos estados, nenhum outro componente será alterado.

A equação (4-2) não apresenta a única configuração que estados compostos podem tomar. Na verdade, devemos ainda levar em conta a existência de um dos fenômenos mais intrigantes da Mecânica Quântica, que não possui análogo em toda a teoria clássica: o *emaranhamento*.

Por definição, um estado composto é dito ser emaranhado se ele não puder ser decomposto em produtos tensoriais de estados dos sistemas individuais, como sugerido pela eq.(4-2). Como exemplo, apresentaremos um dos estados de Bell, clássicos na literatura:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{4-3}$$

Esse é de fato um estado emaranhado, pois não pode ser escrito como o produto tensorial dos estados $|a\rangle$ e $|b\rangle$ de um qubit qualquer.

Para provar isto, considere

$$|a\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \quad \text{e} \quad |b\rangle = \alpha_2|0\rangle + \beta_2|1\rangle,$$

onde $\alpha_1$, $\beta_1$, $\alpha_2$, $\beta_2 \in \mathbb{C}$ e $|\alpha_1|^2 + |\beta_1|^2 = 1$, $|\alpha_2|^2 + |\beta_2|^2 = 1$. Logo,

$$\begin{aligned} |a\rangle \otimes |b\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\ &= \alpha_1\alpha_2|00\rangle + \beta_1\beta_2|11\rangle + \alpha_1\beta_2|01\rangle + \alpha_2\beta_1|10\rangle \end{aligned}$$

Tomar $\alpha_1\beta_2 = 0$ implica que $\alpha_1\alpha_2 = 0$ ou $\beta_1\beta_2 = 0$, ou seja, é impossível achar coeficientes complexos tais que $|\psi\rangle = |a\rangle \otimes |b\rangle$.

## 4.3 Estados Produto e Emaranhado e Universalidade

A universalidade será a nossa principal ferramenta para simplificar a demonstração do teorema de composicionalidade de Coecke, devido ao seguinte: qualquer aplicação linear ou antilinear que atue em estados emaranhados é unicamente determinada por sua atuação em estados produto.

De fato, vimos que vetores da forma $v \otimes w$ são vetores-produto. Todos os outros são somas do tipo

$$\sum_{i=1}^{n} \alpha_i v_i \otimes w_i,$$

e que nunca poderão ser escritos como um produto $v \otimes w$. Assim, suponha que queremos definir uma aplicação linear $F : \mathcal{H}_1 \otimes \mathcal{H}_2 \to \mathcal{H}_3$. Obviamente devemos ter:

$$F\left(\sum_{i=1}^{n} \alpha_i v_i \otimes w_i\right) = \sum_{i=1}^{n} \alpha_i F(v_i \otimes w_i).$$

Ou seja, é suficiente definir $F$ apenas em vetores produto $v \otimes w$ (desde que estes sejam linearmente independentes). No caso de $F$ antilinear a mesma equação vale com o coeficiente $\bar{\alpha}_i$ do lado direito. Entretanto, pela propriedade da universalidade, para que $F$ seja definida basta que a aplicação $(v, w) \mapsto F(v \otimes w)$ seja bilinear. Quando tal argumento é usado, dizemos que $F$ é *definida por universalidade*.

Logo, qualquer teorema que utilize apenas a linearidade e/ou a antilinearidade em estados emaranhados (como a nossa versão do teorema de Coecke) é verdadeiro se conseguirmos demonstrá-lo para estados desemaranhados. Isto em geral torna a prova muito mais fácil.

## 4.4 Múltiplos Qubits

Se considerarmos um sistema com dois bits, sabemos que podemos encontrá-lo nos seguintes estados: 00, 01, 10 e 11. Analogamente, um sistema

composto por dois qubits possui quatro estados-base: $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$. No entanto, como combinações lineares destes vetores formam ainda outros estados possíveis para os qubits, vamos escrevê-los de forma geral como:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{4-4}$$

onde todos os coeficientes são números complexos e $|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2 = 1$.

Um sistema de $n$ qubits está associado a um espaço de Hilbert isomorfo a $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$. A base de vetores natural para este espaço é $\{|0\ldots0\rangle, |0\ldots1\rangle, \ldots, |1\ldots1\rangle\}$, e então a combinação linear que representa um estado geral terá $2^n$ coeficientes complexos. O interessante é que para $n = 500$, este número já é maior que o número estimado de átomos do Universo! (16) Obviamente, nenhum computador clássico conseguiria armazenar tantos coeficientes.

É importante perceber que, enquanto um sistema clássico de $n$ bits armazena apenas um destes $2^n$ números, um sistema de $n$ qubits pode armazenar todos eles simultaneamente. Sabemos no entanto que se o observarmos, veremos apenas um destes números, mas consideremos o seguinte: ao prepararmos um estado que é a superposição de $n$ números diferentes, podemos aplicar operações matemáticas a todos eles de uma só vez. Ou seja, um computador quântico utiliza apenas um passo computacional para operar sobre $2^n$ entradas distintas, sendo o resultado uma superposição de todas as saídas correspondentes. Para fazer o mesmo, um computador clássico deve repetir a computação $2^n$ vezes, ou usar $2^n$ processadores trabalhando em paralelo. Desta forma, constatamos o ganho enorme de tempo e memória computacional que a teoria quântica pode nos proporcionar.



## 4.5 Medições de Sistemas Compostos

Ao observarmos uma grandeza na base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ de um sistema quântico composto por dois qubits, obteremos como resultado, de acordo com a eq.(4-4), um destes quatro estados-base, associados às probabilidades $|\alpha|^2$, $|\beta|^2$, $|\gamma|^2$ e $|\delta|^2$, respectivamente. Após a medição, o estado do sistema é exatamente igual ao que foi observado.

Consideremos agora que a medição na base $\{|0\rangle, |1\rangle\}$ será feita somente sobre um dos qubits, digamos o primeiro. O resultado seria o seguinte: $|0\rangle$ com probabilidade $|\alpha|^2 + |\beta|^2$ e $|1\rangle$ com probabilidade $|\gamma|^2 + |\delta|^2$. No primeiro caso, o estado do sistema composto pós-medição é

$$|\psi'\rangle = \frac{\alpha|00\rangle + \beta|01\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}},$$

e para o segundo,

$$|\psi'\rangle = \frac{\gamma|10\rangle + \delta|11\rangle}{\sqrt{|\gamma|^2 + |\delta|^2}},$$

onde os estados são representados por vetores normalizados.

Vamos supor que obtivemos o estado $|0\rangle$ ao realizarmos esta primeira medição. Então, a probabilidade de medir o segundo qubit como $|0\rangle$ é

$$\frac{\alpha^2}{\alpha^2 + \beta^2},$$

e o estado pós-medição do sistema quântico composto pelos dois qubits é

$$|00\rangle.$$

Já a probabilidade de medi-lo como $|1\rangle$ é

$$\frac{\beta^2}{\alpha^2 + \beta^2},$$

onde o respectivo estado resultante é

$$|01\rangle.$$

Consideremos então um estado-produto bastante simples:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes (|0\rangle + |1\rangle)). \end{aligned}$$

Pelo que foi visto nesta seção, ao observarmos seu primeiro qubit na base $\{|0\rangle, |1\rangle\}$, este retorna $|0\rangle$ com probabilidade igual a 1. Já o segundo pode ser observado tanto como $|0\rangle$ ou $|1\rangle$, ambos com probabilidade 1/2. Notemos que as duas medições são completamente independentes, pois o resultado da primeira não influencia de maneira alguma a segunda.

Agora, suponhamos que a medição será feita sobre o estado emaranhado de Bell, dado pela eq. (4-3): ao observarmos o primeiro qubit na base $\{|0\rangle, |1\rangle\}$, obteremos os estados $|0\rangle$ ou $|1\rangle$ com probabilidade 1/2 cada um. Considere que o resultado foi $|0\rangle$. Então, ao observarmos o outro qubit, ainda na mesma base, este certamente será encontrado no estado $|0\rangle$, já que não há outra possibilidade de estado para o sistema composto que retorne $|0\rangle$ na medição do primeiro qubit. Analogamente, se considerarmos que a primeira medição retornou um autovalor associado a $|1\rangle$, a medição subseqüente nos dirá, com

certeza, que o segundo qubit será encontrado no estado $|1\rangle$. Assim, destaca-se agora a principal característica de estados emaranhados: ao contrário do que foi afirmado para o estado-produto analisado, a medição de uma grandeza observável de um dos sistemas individuais (no caso, um dos qubits), influencia a observação dos outros sistemas, ou seja, as medições não são independentes.

Diremos então que dois qubits encontram-se em um estado emaranhado quando cada uma das partes não possuir um estado próprio.

É justamente este o ponto da teoria quântica questionado pelo *paradoxo EPR*, assim denominado por ter sido proposto por Einstein, Podolsky e Rosen, em 1935 (9). Através da descrição de um experimento que utilizaria um par de partículas emaranhadas, os autores pretendiam afirmar que um resultado natural da teoria da relatividade, o princípio da localidade, estava sendo violado, pois ao separarmos tais partículas arbitrariamente, uma medição em uma delas faz com que a outra assuma instantaneamente o estado medido na primeira. Logo, poderíamos pensar que a informação é enviada a uma velocidade maior que a da luz, contrariando o princípio formulado por Einstein.

Somente na década de 80 foram realizados os experimentos EPR, sendo de fato comprovado que o emaranhamento é um fenômeno real. Embora esta pareça ser uma questão essencialmente filosófica, vale a pena citar a explicação que é dada ao paradoxo: medir uma das partículas do par emaranhado realmente faz com que tenhamos certeza de qual será o resultado de uma medição na segunda partícula. Entretanto, não há transporte imediato de informação, pois em Mecânica Quântica um estado não tem valor algum antes de ser observado. O que pode na verdade ser dito é que o emaranhamento apenas garante que os resultados de observações realizadas sobre as duas partículas possuem certas correlações.

A aplicação mais interessante deste fenômeno é a que será dada no próximo capítulo: a teleportação (17, 15, 19).