

Sistemas múltiplos



[Baixe os slides](#) para esta lição.

Introdução

O foco desta lição está nos fundamentos da informação quântica quando há *múltiplos* sistemas sendo considerados. Tais situações surgem naturalmente no contexto do processamento de informações, tanto clássico quanto quântico. Grandes sistemas de transporte de informações são frequentemente mais facilmente construídos usando coleções de sistemas menores, como bits ou qubits.

Uma ideia simples, mas criticamente importante, para se ter em mente ao entrar nesta lição é que sempre podemos escolher visualizar múltiplos

sistemas *juntos* como se eles formassem um único sistema composto — ao qual a discussão na lição anterior se aplica. De fato, essa ideia leva muito diretamente a uma descrição de como estados quânticos, medições e operações funcionam para múltiplos sistemas.

Há mais para entender múltiplos sistemas quânticos, no entanto, do que simplesmente reconhecer que eles podem ser vistos coletivamente como sistemas únicos. Por exemplo, podemos ter múltiplos sistemas quânticos que estão coletivamente em um estado quântico particular e, então, escolher medir apenas um (ou um subconjunto apropriado) dos sistemas individuais. Em geral, isso afetará o estado dos sistemas restantes, e é importante entender exatamente como ao analisar algoritmos e protocolos quânticos. Uma compreensão dos tipos de *correlações* entre múltiplos sistemas — e particularmente um tipo de correlação conhecido como *emaranhamento* — também é importante em informações e computação quânticas.

Informação clássica

Como na lição anterior, começaremos com uma discussão sobre informação clássica. Mais uma vez, as descrições probabilísticas e quânticas são matematicamente semelhantes, e reconhecer como a matemática funciona no ambiente familiar da informação clássica é útil para entender por que a informação quântica é descrita da maneira que é.

Estados clássicos via produto cartesiano

Começaremos em um nível muito básico, com estados clássicos de sistemas múltiplos. Para simplificar, começaremos discutindo apenas dois sistemas e, então, generalizaremos para mais de dois sistemas.

Para sermos precisos, suponhamos que X é um sistema cujo conjunto de estados clássico é Σ , e E é um segundo sistema com conjunto de estados clássico Γ . Como na lição anterior, como nos referimos a esses conjuntos como *conjuntos de estados clássicos*, nossa suposição é que Σ e Γ são finitos e não vazios. Pode ser que $\Sigma = \Gamma$, mas isso não é necessariamente verdade — e, independentemente disso, é útil usar nomes diferentes para se referir a esses conjuntos, por uma questão de clareza.

Agora imagine que os dois sistemas, X e E , são colocados lado a lado, com X à esquerda e E à direita. Se assim o escolhermos, podemos ver esses dois sistemas como se formassem um único sistema, que podemos denotar por (X, E) ou XY dependendo da nossa preferência.

Uma pergunta natural a ser feita sobre este sistema composto (X, E) é: "Quais são seus estados clássicos?"

A resposta é que o conjunto de estados clássicos de (X, E) é o *produto cartesiano* de Σ e Γ , que é o conjunto definido como

$$\Sigma \times \Gamma = \{ (u, b) : u \in \Sigma \text{ e } b \in \Gamma \}.$$

Em termos simples, o produto cartesiano é precisamente a noção matemática que captura a ideia de visualizar um elemento de um conjunto e um elemento de um segundo conjunto juntos, como se eles formassem um único elemento de um único conjunto.

No caso em questão, dizer que (X, E) está no estado clássico $(u, b) \in \Sigma \times \Gamma$ significa que X está no estado clássico $u \in \Sigma$ e E está no estado clássico $b \in \Gamma$; e se o estado clássico de X é $u \in \Sigma$ e o estado clássico de E é $b \in \Gamma$, então o estado clássico do sistema conjunto (X, E) é (u, b) .

Para mais de dois sistemas, a situação se generaliza de forma natural. Se supusermos que X_1, \dots, X_n são sistemas que possuem conjuntos de estados clássicos $\Sigma_1, \dots, \Sigma_n$, respectivamente, para qualquer inteiro positivo n , o conjunto de estados clássico n -tupla (X_1, \dots, X_n) , visto como um único sistema de junta, é o produto cartesiano

$$\Sigma_1 \times \dots \times \Sigma_n = \{ (u_1, \dots, u_n) : u_1 \in \Sigma_1, \dots, u_n \in \Sigma_n \}$$

Note que somos livres para usar quaisquer nomes que desejarmos para os sistemas, e somos livres para ordená-los como escolhermos. Em particular, se tivermos n sistemas como o acima, podemos escolher nomeá-los X_{n-1}, \dots, X_0 e ordená-los desta forma, ou seja, como (X_{n-1}, \dots, X_0) . Imitando o mesmo padrão para nomear os estados clássicos associados e conjuntos de estados clássicos, poderíamos então nos referir a um estado clássico $(u_{n-1}, \dots, u_0) \in \Sigma_{n-1} \times \dots \times \Sigma_0$ deste sistema composto. De fato, esta é a convenção de ordenação padrão usada pelo Qiskit para nomear qubits, e voltaremos a isso na próxima lição, quando voltarmos nosso foco para circuitos quânticos.

Representando estados como strings

Muitas vezes é conveniente escrever um estado clássico $(um_1, \dots, um_{n\tilde{a}o})$ como um corda $um_1 \cdots um_{n\tilde{a}o}$ por uma questão de brevidade, particularmente na situação (muito típica) que o estado clássico estabelece $\Sigma_1, \dots, \Sigma_{n\tilde{a}o}$ estão associados a conjuntos de *símbolos* ou *caracteres*.

De fato, a noção de uma string, que é um conceito fundamentalmente importante na ciência da computação, é formalizada em termos matemáticos por meio de produtos cartesianos. O termo *alfabeto* é comumente usado para se referir a conjuntos de símbolos usados para formar strings, mas a definição matemática de um alfabeto é precisamente a mesma que a definição de um conjunto de estados clássico: é um conjunto finito e não vazio.

Por exemplo, suponha que X_1, \dots, X_{10} são bits, de modo que os conjuntos de estados clássicos desses sistemas são todos iguais.

$$\Sigma_1 = \Sigma_2 = \cdots = \Sigma_{10} = \{0, 1\}$$

(O conjunto $\{0, 1\}$ é comumente chamado de *alfabeto binário*.)
Existem então $2^{10} = 1024$ estados clássicos do sistema articular (X_1, \dots, X_{10}) , quais são os elementos do conjunto

$$\Sigma_1 \times \Sigma_2 \times \cdots \times \Sigma_{10} = \{0, 1\}^{10}.$$

Escritos como strings, esses estados clássicos se parecem com isto:

```
0000000000
0000000001
0000000010
0000000011
0000000100
:
1111111111
```

Para o estado clássico 0001010000, por exemplo, vemos que X_4 e X_6 estão no estado 1, enquanto todos os outros sistemas estão no estado 0.

Estados probabilísticos

Lembre-se da lição anterior que um *estado probabilístico* associa uma probabilidade a cada estado clássico de um sistema. Assim, um estado probabilístico de múltiplos sistemas — vistos coletivamente como se formassem um único sistema — associa uma probabilidade a cada

elemento do produto cartesiano dos conjuntos de estados clássicos dos sistemas individuais.

Por exemplo, suponha que X e E são ambos bits, de modo que seus conjuntos de estados clássicos correspondentes são $\Sigma = \{0, 1\}$ e $\Gamma = \{0, 1\}$, respectivamente. Aqui está um estado probabilístico do par (X, E) :

$$\Pr((X, E) = (0, 0)) = 1/2$$

$$\Pr((X, E) = (0, 1)) = 0$$

$$\Pr((X, E) = (1, 0)) = 0$$

$$\Pr((X, E) = (1, 1)) = 1/2$$

Este estado probabilístico é aquele em que ambos X e E são bits aleatórios — cada um é 0 com probabilidade $1/2$ e 1 com probabilidade $1/2$ — mas os estados clássicos dos dois bits sempre concordam. Este é um exemplo de *correlação* entre esses sistemas.

Ordenando conjuntos de estados de produtos cartesianos

Os estados probabilísticos dos sistemas são representados por vetores de probabilidade, que são vetores de coluna com índices que foram colocados em correspondência com o conjunto de estados clássicos subjacente do sistema considerado.

A mesma situação surge para sistemas múltiplos. Para representar um estado probabilístico de sistemas múltiplos como um produto cartesiano, deve-se decidir sobre uma ordenação dos elementos do produto.

Assumindo que os conjuntos de estados clássicos individuais Σ , Γ de sistemas X , E já estão ordenados, há uma convenção simples para fazer isso: *ordenação alfabética*. Mais precisamente, as entradas em cada *n*-tupla (ou, equivalentemente, os símbolos em cada string) são vistos como ordenados por significância que *decrece da esquerda para a direita*.

Por exemplo, de acordo com esta convenção, o produto cartesiano $\{1, 2, 3\} \times \{0, 1\}$ é ordenado assim:

$$(1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1).$$

Quando *n* — as tuplas são escritas como strings e ordenadas dessa forma, observamos padrões familiares, como $\{0, 1\} \times \{0, 1\}$ sendo ordenado como 00, 01, 10, 11, e o conjunto $\{0, 1\}^{10}$ sendo ordenado

como foi sugerido acima. Também vemos $\{0, 1, \dots, 9\} \times \{0, 1, \dots, 9\}$ ordenados como os números 0 através 99. Você pode reconhecer que isso não é uma coincidência: o sistema numérico decimal de hoje usa a mesma ordem alfabética. Aqui, é claro, "alfabético" tem um significado mais amplo que pode incluir uma coleção de símbolos numéricos.

Voltando ao exemplo dos dois bits acima, o estado probabilístico é representado pelo seguinte vetor de probabilidade (onde as entradas são rotuladas explicitamente por uma questão de clareza).

$$\begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{pmatrix} \begin{matrix} \leftarrow \text{probabilidade associada ao estado } 00 \\ \leftarrow \text{probabilidade associada ao estado } 01 \\ \leftarrow \text{probabilidade associada ao estado } 10 \\ \leftarrow \text{probabilidade associada ao estado } 11 \end{matrix} \quad (1)$$

Independência de dois sistemas

Um tipo especial de estado probabilístico de dois sistemas é aquele em que os sistemas são *independentes*. Intuitivamente falando, dois sistemas são independentes se aprender o estado clássico de qualquer um dos sistemas não tem efeito nas probabilidades associadas ao outro. Ou seja, aprender em que estado clássico um dos sistemas está não fornece nenhuma informação sobre o estado clássico do outro.

Para definir esta noção com precisão, suponhamos mais uma vez que X e E são sistemas que possuem conjuntos de estados clássicos Σ e Γ , respectivamente. Em relação a um dado estado probabilístico desses sistemas, eles são considerados *independentes* se for o caso de

$$\Pr((X, E) = (u, b)) = \Pr(X = u) \Pr(E = b) \quad (2)$$

para cada escolha de $u \in \Sigma$ e $b \in \Gamma$.

Para expressar esta condição em termos de vetores de probabilidade, suponha que o estado probabilístico dado de (X, E) é descrito por um vetor de probabilidade, escrito na notação de Dirac como

$$\sum_{(a, b) \in \Sigma \times \Gamma} p_{\text{sobre}} |ab\rangle.$$

A condição (2) pois a independência é então equivalente à existência de dois vetores de probabilidade

$$|\phi\rangle = \sum_{u \in \Sigma} q_u |u\rangle \quad \text{e} \quad |\psi\rangle = \sum_{b \in \Gamma} r_b |b\rangle$$

$b \in \Gamma$ (3)

representando as probabilidades associadas aos estados clássicos de X e E , respectivamente, de modo que

$$p_{sobre} = q_{um} r_b \quad (4)$$

para todos $um \in \Sigma$ e $b \in \Gamma$.

Por exemplo, o estado probabilístico de um par de bits (X, E) representado pelo vetor

$$\frac{1}{6}|00\rangle + \frac{1}{12}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{4}|11\rangle$$

é aquele em que X e E são independentes. Especificamente, a condição necessária para a independência é verdadeira para os vetores de probabilidade

$$|\phi\rangle = \frac{1}{4}|0\rangle + \frac{3}{4}|1\rangle \quad \text{e} \quad |\psi\rangle = \frac{2}{3}|0\rangle + \frac{1}{3}|1\rangle.$$

Por exemplo, para combinar a entrada 00, precisamos $\frac{1}{6} = \frac{1}{4} \times \frac{2}{3}$, e de fato esse é o caso. Outras entradas podem ser verificadas de forma similar.

Por outro lado, o estado probabilístico (1) , que podemos escrever como

$$\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle, \quad (5)$$

não representa independência entre os sistemas X e E . Uma maneira simples de argumentar isso é a seguinte.

Suponha que existissem vetores de probabilidade $|\phi\rangle$ e $|\psi\rangle$, como na equação (3) acima, para o qual a condição (4) fica satisfeito com cada escolha de um e b . Seria então necessariamente que

$$q_0 r_1 = \Pr((X, E) = (0, 1)) = 0.$$

Isto implica que ou $q_0 = 0$ ou $r_1 = 0$, porque se ambos fossem diferentes de zero, o produto $q_0 r_1$ também não seria zero. Isso leva à conclusão de que $q_0 r_0 = 0$ (em caso $q_0 = 0$) ou $q_1 r_1 = 0$ (em caso $r_1 = 0$). Vemos, no entanto, que nenhuma dessas igualdades pode ser verdadeira porque devemos ter $q_0 r_0 = 1/2$ e $q_1 r_1 = 1/2$. Portanto, não existem vetores $|\phi\rangle$ e $|\psi\rangle$ satisfazendo a propriedade necessária para a independência.

Tendo definido a independência entre dois sistemas, podemos agora definir correlação precisamente como uma *falta de independência*. Por exemplo, porque os dois bits no estado probabilístico representados pelo

vetor(5) não são independentes, elas são, por definição, correlacionadas.

Produtos tensoriais de vetores

A condição de independência recém descrita pode ser expressa de forma mais sucinta por meio da noção de um *produto tensorial*. Embora esta seja uma noção muito geral que pode ser definida de forma bastante abstrata e aplicada a uma variedade de estruturas matemáticas, no caso em questão ela pode ser definida em termos simples e concretos. Dados dois vetores

$$|\phi\rangle = \sum_{u \in \Sigma} \alpha_u |u\rangle \quad \text{e} \quad |\psi\rangle = \sum_{b \in \Gamma} \beta_b |b\rangle,$$

o produto tensorial $|\phi\rangle \otimes |\psi\rangle$ é um novo vetor sobre o conjunto de estados conjuntos $\Sigma \times \Gamma$, definido como

$$|\phi\rangle \otimes |\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} \alpha_a \beta_b |ab\rangle.$$

Equivalentemente, o vetor $|\pi\rangle = |\phi\rangle \otimes |\psi\rangle$ é definido pela equação

$$\langle ab | \pi \rangle = \langle a | \phi \rangle \langle b | \psi \rangle$$

sendo verdade para todos $a \in \Sigma$ e $b \in \Gamma$.

Podemos agora reformular a condição de independência como exigindo o vetor de probabilidade $|\pi\rangle$ do sistema articular (X, E) ser representável como um produto tensorial

$$|\pi\rangle = |\phi\rangle \otimes |\psi\rangle$$

de vetores de probabilidade $|\phi\rangle$ e $|\psi\rangle$ em cada um dos subsistemas X e E . Nesta situação diz-se que $|\pi\rangle$ é um *estado de produto* ou *vetor de produto*.

Muitas vezes omitimos o símbolo \otimes ao tomar o produto tensorial de kets, como escrever $|\phi\rangle |\psi\rangle$ em vez de $|\phi\rangle \otimes |\psi\rangle$. Esta convenção captura a ideia de que o produto tensorial é, neste contexto, a maneira mais natural ou padrão de tomar o produto de dois vetores. Embora seja menos comum, a notação $|\phi \otimes \psi\rangle$ também é usada às vezes.

Quando usamos a convenção alfabética para ordenar elementos de produtos cartesianos, obtemos a seguinte especificação para o produto tensorial de dois vetores coluna.

$$\begin{pmatrix} um_1 \\ \vdots \\ um_{eu} \end{pmatrix} \otimes \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_o \end{pmatrix} = \begin{pmatrix} um_1\beta_1 \\ \vdots \\ um_1\beta_o \\ um_2\beta_1 \\ \vdots \\ um_2\beta_o \\ \vdots \\ um_{eu}\beta_1 \\ \vdots \\ um_{eu}\beta_o \end{pmatrix}$$

Como um aparte importante, observamos a seguinte expressão para produtos tensoriais de vetores de base padrão:

$$|um\rangle \otimes |b\rangle = |ab\rangle.$$

Alternativamente, escrevendo (um, b) como um par ordenado em vez de uma string, poderíamos escrever

$$|um\rangle \otimes |b\rangle = |(um, b)\rangle,$$

mas é mais comum escrever

$$|um\rangle \otimes |b\rangle = |um, b\rangle$$

seguindo uma prática matemática de remover parênteses que não acrescentam clareza nem removem ambiguidade.

O produto tensorial de dois vetores tem a importante propriedade de ser *bilinear*, o que significa que é linear em cada um dos dois argumentos separadamente, assumindo que o outro argumento é fixo. Essa propriedade pode ser expressa por meio dessas equações:

1. Linearidade no primeiro argumento:

$$\begin{aligned} (|\phi_1\rangle + |\phi_2\rangle) \otimes |\psi\rangle &= |\phi_1\rangle \otimes |\psi\rangle + |\phi_2\rangle \otimes |\psi\rangle \\ (\alpha|\phi\rangle) \otimes |\psi\rangle &= \alpha(|\phi\rangle \otimes |\psi\rangle) \end{aligned}$$

2. Linearidade no segundo argumento:

$$\begin{aligned} |\phi\rangle \otimes (|\psi_1\rangle + |\psi_2\rangle) &= |\phi\rangle \otimes |\psi_1\rangle + |\phi\rangle \otimes |\psi_2\rangle \\ |\phi\rangle \otimes (\alpha|\psi\rangle) &= \alpha(|\phi\rangle \otimes |\psi\rangle) \end{aligned}$$

Considerando a segunda equação em cada um desses pares de

equações, vemos que os escalares "flutuam livremente" dentro dos

produtos tensoriais:

$$(\alpha | \phi \rangle) \otimes | \psi \rangle = | \phi \rangle \otimes (\alpha | \psi \rangle) = \alpha (| \phi \rangle \otimes | \psi \rangle).$$

Não há, portanto, ambiguidade em simplesmente escrever $\alpha | \phi \rangle \otimes | \psi \rangle$, ou alternativamente $\alpha | \phi \rangle | \psi \rangle$ ou $\alpha | \phi \otimes \psi \rangle$, para se referir a este vetor.

Independência e produtos tensoriais para três ou mais sistemas

As noções de independência e produtos tensoriais generalizam-se diretamente para três ou mais sistemas. Se $X_1, \dots, X_{n\tilde{a}o}$ são sistemas que possuem conjuntos de estados clássicos $\Sigma_1, \dots, \Sigma_{n\tilde{a}o}$, respectivamente, então um estado probabilístico do sistema combinado $(X_1, \dots, X_{n\tilde{a}o})$ é um *estado de produto* se o vetor de probabilidade associado assume a forma

$$| \psi \rangle = | \phi_1 \rangle \otimes \dots \otimes | \phi_{n\tilde{a}o} \rangle$$

para vetores de probabilidade $| \phi_1 \rangle, \dots, | \phi_{n\tilde{a}o} \rangle$ descrevendo estados probabilísticos de $X_1, \dots, X_{n\tilde{a}o}$.

Aqui, a definição do produto tensorial generaliza-se de forma natural: o vetor

$$| \psi \rangle = | \phi_1 \rangle \otimes \dots \otimes | \phi_{n\tilde{a}o} \rangle$$

é definido pela equação

$$\langle um_1 \dots um_{n\tilde{a}o} | \psi \rangle = \langle um_1 | \phi_1 \rangle \dots \langle um_{n\tilde{a}o} | \phi_{n\tilde{a}o} \rangle$$

sendo verdade para todos $um_1 \in \Sigma_1, \dots, um_{n\tilde{a}o} \in \Sigma_{n\tilde{a}o}$. Uma maneira diferente, mas equivalente, de definir o produto tensorial de três ou mais vetores é recursivamente em termos de produtos tensoriais de dois vetores:

$$| \phi_1 \rangle \otimes \dots \otimes | \phi_{n\tilde{a}o} \rangle = (| \phi_1 \rangle \otimes \dots \otimes | \phi_{n-1} \rangle) \otimes | \phi_{n\tilde{a}o} \rangle,$$

assumindo $n\tilde{a}o \geq 3$.

Similar ao produto tensorial de apenas dois vetores, o produto tensorial de três ou mais vetores é linear em cada um dos argumentos individualmente, assumindo que todos os outros argumentos são fixos. Neste caso, dizemos que o produto tensorial de três ou mais vetores é *multilinear*.

Como fizemos no caso de dois sistemas, poderíamos dizer que os sistemas X_1, \dots, X_n são *independentes* quando estão em um estado de produto, mas o termo *mutuamente independente* é mais preciso. Acontece que há outras noções de independência para três ou mais sistemas, como *independência em pares*, com as quais não nos preocuparemos neste momento.

Generalizando a observação anterior sobre produtos tensoriais de vetores de base padrão, para qualquer inteiro positivo n e quaisquer estados clássicos u_1, \dots, u_n nós temos

$$|u_1\rangle \otimes \cdots \otimes |u_n\rangle = |u_1 \cdots u_n\rangle = |u_1, \dots, u_n\rangle$$

Medidas de estados probabilísticos

Agora, vamos prosseguir para medições de estados probabilísticos de múltiplos sistemas. Ao escolher visualizar múltiplos sistemas juntos como sistemas únicos, obtemos imediatamente uma especificação de como as medições devem funcionar para múltiplos sistemas — desde que *todos* os sistemas sejam medidos.

Por exemplo, se o estado probabilístico de dois bits (X, E) é descrito pelo vetor de probabilidade

$$\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle,$$

então o resultado 00 — significado 0 para a medição de X e 0 para a medição de E — é obtido com probabilidade $1/2$ e o resultado 11 também é obtido com probabilidade $1/2$. Em cada caso, atualizamos a descrição do vetor de probabilidade do nosso conhecimento de acordo, de modo que o estado probabilístico se torne $|00\rangle$ ou $|11\rangle$, respectivamente.

Medições parciais

Suponha, no entanto, que escolhemos não medir *todos* os sistemas, mas, em vez disso, apenas medimos algum *subconjunto apropriado* dos sistemas. Isso resultará em um resultado de medição para cada sistema que for medido e também afetará (em geral) nosso conhecimento dos sistemas restantes.

Vamos focar no caso de dois sistemas, um dos quais é medido. A situação mais geral — na qual algum subconjunto próprio de três ou mais sistemas é medido — reduz-se efetivamente ao caso de dois sistemas

quando vemos os sistemas que são medidos coletivamente como se formassem um sistema e os sistemas que não são medidos como se formassem um segundo sistema.

Para sermos precisos, vamos supor (como de costume) que X é um sistema com conjunto de estados clássico Σ , que E é um sistema com conjunto de estados clássico Γ , e os dois sistemas juntos estão em algum estado probabilístico. Vamos considerar o que acontece quando apenas medimos X e não fazer nada para E . A situação em que apenas E é medido e nada acontece com X é tratado simetricamente.

Primeiro, sabemos que a probabilidade de observar um estado clássico particular $um \in \Sigma$ quando apenas X é medido deve ser consistente com as probabilidades que obteríamos sob a suposição de que E também foi medido. Ou seja, devemos ter

$$\Pr(X = uma) = \sum_{b \in \Gamma} \Pr((X, E) = (um, b)).$$

Esta é a fórmula para o chamado estado probabilístico *reduzido* (ou *marginal*) de X sozinho.

Esta fórmula faz todo o sentido em um nível intuitivo; algo muito estranho precisaria acontecer para que ela estivesse errada. Isso significaria que as probabilidades de X as medições são influenciadas simplesmente pelo fato de E também é medido, independentemente do resultado em E . Se E por acaso estivesse em um local distante, digamos, outra galáxia, isso permitiria uma sinalização mais rápida que a luz, que rejeitamos com base em nossa compreensão da física. Outra maneira de entender isso vem de uma interpretação da probabilidade como refletindo um grau de crença sobre o estado do sistema. Já que uma medição em E é tomado para simplesmente revelar um estado preexistente, um observador diferente olhando para X , desconhecendo o E medição, não devem ter suas probabilidades alteradas.

Dada a suposição de que apenas X é medido e E não é, pode ainda existir incerteza geral sobre o estado clássico de E . Por esta razão, em vez de actualizar a nossa descrição do estado probabilístico de (X, E) para $|ab\rangle$ para alguma seleção de $um \in \Sigma$ e $b \in \Gamma$, devemos atualizar nossa descrição para que essa incerteza sobre E é refletido corretamente.

A seguinte fórmula de probabilidade condicional reflete essa incerteza.

$$\Pr(E = b | X = uma) = \frac{\Pr((X, E) = (um, b))}{\Pr(X = uma)}$$

Aqui, a expressão $\Pr (E = b \mid X = uma)$ denota a probabilidade de que $E = b$ condicionado em (ou dado que) $X = uma$.

Deve-se notar que a expressão acima só é definida se $\Pr (X = uma)$ é diferente de zero, pois se

$$\Pr (X = uma) = 0 ,$$

então obtemos a forma indeterminada $\frac{0}{0}$. Isto não é um problema, no entanto, porque se a probabilidade associada a um é zero, então nunca observaremos um como resultado de uma medição de X , então não precisamos nos preocupar com essa possibilidade.

Para expressar essas fórmulas em termos de vetores de probabilidade, considere um vetor de probabilidade $|\psi\rangle$ descrevendo o estado conjunto de (X, E) .

$$|\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} p_{sobre} |ab\rangle$$

Medição X sozinho produz cada resultado possível com probabilidades

$$\Pr (X = uma) = \sum_{b \in \Gamma} p_{sobre}.$$

Assim, o vetor que representa o estado probabilístico de X sozinho (ou seja, o estado probabilístico reduzido de X) é dado por

$$\sum_{um \in \Sigma} \left(\sum_{c \in \Gamma} p_{umc} \right) |a\rangle.$$

Tendo obtido um resultado particular $um \in \Sigma$ da medição de X , o estado probabilístico de E é atualizado de acordo com a fórmula para probabilidades condicionais, de modo que é representado por este vetor de probabilidade:

$$|\pi_{um}\rangle = \frac{\sum_{b \in \Gamma} p_{sobre} |b\rangle}{\sum_{c \in \Gamma} p_{umc}}.$$

No caso de a medição de X resultou no estado clássico um , atualizamos, portanto, nossa descrição do estado probabilístico do sistema conjunto (X, E) para $|um\rangle \otimes |\pi_{um}\rangle$.

Uma maneira de pensar sobre esta definição de $|\pi_{um}\rangle$ é vê-lo como uma *normalização* do vetor $\sum_{b \in \Gamma} p_{sobre} |b\rangle$, onde dividimos pela soma das entradas neste vetor para obter um vetor de probabilidade. Esta

normalização efetivamente considera um condicionamento no evento de que a medição de X resultou no resultado uma .

Para um exemplo específico, suponha que o conjunto de estados clássico de X é $\Sigma = \{0, 1\}$, o conjunto de estados clássicos de E é $\Gamma = \{1, 2, 3\}$, e o estado probabilístico de (X, E) é

$$|\psi\rangle = \frac{1}{2}|0, 1\rangle + \frac{1}{12}|0, 3\rangle + \frac{1}{12}|1, 1\rangle + \frac{1}{6}|1, 2\rangle + \frac{1}{6}|1, 3\rangle.$$

Nosso objetivo será determinar as probabilidades dos dois resultados possíveis (0 e 1), e calcular qual seria o estado probabilístico resultante de E para os dois resultados, assumindo o sistema X é medido.

Usando a bilinearidade do produto tensorial, e especificamente o fato de que ele é linear no *segundo* argumento, podemos reescrever o vetor $|\psi\rangle$ do seguinte modo:

$$|\psi\rangle = |0\rangle \otimes \left(\frac{1}{2}|1\rangle + \frac{1}{12}|3\rangle\right) + |1\rangle \otimes \left(\frac{1}{12}|1\rangle + \frac{1}{6}|2\rangle + \frac{1}{6}|3\rangle\right)$$

Isolamos os distintos vetores de base padrão para o sistema que está sendo medido, reunindo todos os termos para o segundo sistema. Um momento de reflexão revela que isso é sempre possível, independentemente de qual vetor começamos.

Tendo reorganizado como tal, os resultados da medição tornam-se fáceis de analisar. As probabilidades dos dois resultados são dadas por

$$\begin{aligned}\Pr(X = 0) &= \frac{1}{2} + \frac{1}{12} = \frac{7}{12} \\ \Pr(X = 1) &= \frac{1}{12} + \frac{1}{6} + \frac{1}{6} = \frac{5}{12}.\end{aligned}$$

Observe que essas probabilidades somam um, como esperado, uma verificação útil em nossos cálculos.

Além disso, o estado probabilístico de E , condicionado a cada resultado possível, também pode ser rapidamente inferido pela normalização dos vetores entre parênteses (dividindo pela probabilidade associada recém-calculada), de modo que esses vetores se tornem vetores de probabilidade. Ou seja, condicionado a X ser 0, o estado probabilístico de E torna-se

$$\frac{\frac{1}{2}|1\rangle + \frac{1}{12}|3\rangle}{\frac{7}{12}} = \frac{6}{7}|1\rangle + \frac{1}{7}|3\rangle,$$

e condicionado à medição de X sendo 1, o estado probabilístico de E torna-se

$$\frac{\frac{1}{12} |1\rangle + \frac{1}{6} |2\rangle + \frac{1}{6} |3\rangle}{\frac{5}{12}} = \frac{1}{5} |1\rangle + \frac{2}{5} |2\rangle + \frac{2}{5} |3\rangle.$$

Operações em estados probabilísticos

Para concluir esta discussão de informação clássica para sistemas múltiplos, consideraremos *operações* em sistemas múltiplos em estados probabilísticos. Seguindo a mesma ideia que fizemos para estados probabilísticos e medições, podemos visualizar sistemas múltiplos coletivamente como formando sistemas únicos e compostos e olhar para a lição anterior para ver como isso funciona.

Voltando à configuração típica onde temos dois sistemas X e E , vamos considerar operações clássicas no sistema composto (X, E) . Com base na lição anterior e na discussão acima, concluímos que qualquer operação desse tipo é representada por uma matriz estocástica cujas linhas e colunas são indexadas pelo produto cartesiano $\Sigma \times \Gamma$.

Por exemplo, suponha que X e E são bits e considere uma operação com a seguinte descrição.

Se $X = 1$, então execute uma operação NOT em E .
Caso contrário, não faça nada.

Esta é uma operação determinística conhecida como operação *controlada-NÃO*, onde X é o bit *de controle* que determina se uma operação NOT deve ou não ser aplicada ao bit *de destino* E . Aqui está a representação matricial desta operação:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Sua ação em estados de base padrão é a seguinte.

$$|00\rangle \mapsto |00\rangle$$

$$|01\rangle \mapsto |01\rangle$$

$$|10\rangle \mapsto |11\rangle$$

$$|11\rangle \mapsto |10\rangle$$

Se trocássemos os papéis de X e E , tirando E para ser o bit de controle e X para ser o bit alvo, então a representação matricial da operação se tornaria

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

e sua ação em estados de base padrão seria assim:

$$|00\rangle \mapsto |00\rangle$$

$$|01\rangle \mapsto |11\rangle$$

$$|10\rangle \mapsto |10\rangle$$

$$|11\rangle \mapsto |01\rangle$$

Outro exemplo é a operação com esta descrição:

Execute uma das duas operações a seguir, cada uma com probabilidade $1/2$:

1. Definir E ser igual a X .
2. Definir X ser igual a E .

A representação matricial desta operação é a seguinte:

$$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} .$$

A ação desta operação em vetores de base padrão é a seguinte:

$$\begin{aligned}
 |00\rangle &\mapsto \frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle \\
 |01\rangle &\mapsto \frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle \\
 |10\rangle &\mapsto \frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle \\
 |11\rangle &\mapsto |11\rangle
 \end{aligned}$$

Nestes exemplos, estamos simplesmente visualizando dois sistemas juntos como um único sistema e procedendo como na lição anterior.

A mesma coisa pode ser feita para qualquer número de sistemas. Por exemplo, imagine que temos três bits, e incrementamos os três bits módulo 8— o que significa que pensamos nos três bits como codificando um número entre 0 e 7 usando notação binária, adicione 1, e então pegue o restante depois de dividir por 8. Podemos escrever esta operação assim:

$$\begin{aligned}
 &|001\rangle\langle 000| + |010\rangle\langle 001| + |011\rangle\langle 010| + |100\rangle\langle 011| \\
 &+ |101\rangle\langle 100| + |110\rangle\langle 101| + |111\rangle\langle 110| + |000\rangle\langle 111|.
 \end{aligned}$$

Também poderíamos escrever assim:

$$\sum_{k=0}^7 |(k+1) \bmod 8\rangle\langle k|,$$

assumindo que concordamos que um número $u \in \{0, 1, \dots, 7\}$ dentro de um ket refere-se à codificação binária de três bits daquele número. Uma terceira opção é expressar essa operação como uma matriz.

$$\begin{pmatrix}
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
 \end{pmatrix}.$$

Operações independentes

Agora suponha que temos vários sistemas e realizamos *operações separadas* nos sistemas *de forma independente*.

Por exemplo, tomando nossa configuração usual de dois sistemas X e E tendo conjuntos de estados clássicos Σ e Γ , respectivamente, suponhamos que realizamos uma operação em X , de forma totalmente independente, outra operação em E . Como sabemos da lição anterior, essas operações são representadas por matrizes estocásticas — e para sermos precisos, digamos que a operação em X é representado pela matriz M e a operação em E é representado pela matriz N . Assim, as linhas e colunas de M têm índices que são colocados em correspondência com os elementos de Σ , da mesma forma, as linhas e colunas de N correspondem aos elementos de Γ .

Uma pergunta natural a ser feita é esta: se vemos X e E juntos como um único sistema composto (X, E) , qual é a matriz que representa a ação combinada das duas operações neste sistema composto? Para responder a esta questão, precisamos primeiro introduzir o produto tensorial de matrizes — que é similar ao produto tensorial de vetores e é definido analogamente.

Produtos tensoriais de matrizes

O produto tensorial $M \otimes N$ das matrizes

$$M = \sum_{a, b \in \Sigma} m_{ab} |a\rangle \langle b|$$

e

$$N = \sum_{c, d \in \Gamma} n_{cd} |c\rangle \langle d|$$

é a matriz

$$M \otimes N = \sum_{a, b \in \Sigma} \sum_{c, d \in \Gamma} m_{ab} n_{cd} |a\rangle \langle b| \otimes |c\rangle \langle d|$$

Equivalentemente, $M \otimes N$ é definido pela equação

$$\langle a | M \otimes N | b \rangle = \langle a | M | b \rangle \langle c | N | d \rangle$$

sendo verdadeiro para cada seleção de $a, b \in \Sigma$ e $c, d \in \Gamma$.

Uma maneira alternativa, mas equivalente, de descrever $M \otimes N$ é que é a única matriz que satisfaz a equação

$$(M \otimes N)(|\phi\rangle \otimes |\psi\rangle) = (M|\phi\rangle) \otimes (N|\psi\rangle)$$

para cada escolha possível de vetores $|\phi\rangle$ e $|\psi\rangle$. Aqui estamos assumindo que os índices de $|\phi\rangle$ correspondem aos elementos de Σ e os índices de $|\psi\rangle$ corresponde a Γ .

Seguindo a convenção descrita anteriormente para ordenar os elementos dos produtos cartesianos, também podemos escrever o produto tensorial de duas matrizes explicitamente como segue:

$$\begin{pmatrix} u_{m11} & \cdots & u_{m1\text{metro}} \\ \vdots & \ddots & \vdots \\ u_{m\text{milímetros}1} & \cdots & u_{m\text{milímetros}k} \end{pmatrix} \otimes \begin{pmatrix} \beta_{11} & \cdots & \beta_{1\text{mil}} \\ \vdots & \ddots & \vdots \\ \beta_{k1} & \cdots & \beta_{kk} \end{pmatrix}$$

$$= \begin{pmatrix} u_{m11}\beta_{11} & \cdots & u_{m11}\beta_{1\text{mil}} & \cdots & u_{m1\text{metro}}\beta_{11} \\ \vdots & \ddots & \vdots & \cdots & \vdots \\ u_{m11}\beta_{k1} & \cdots & u_{m11}\beta_{kk} & \cdots & u_{m1\text{metro}}\beta_{k1} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ u_{m\text{milímetros}1}\beta_{11} & \cdots & u_{m\text{milímetros}1}\beta_{1\text{mil}} & \cdots & u_{m\text{milímetros}1}\beta_{k1} \\ \vdots & \ddots & \vdots & \cdots & \vdots \\ u_{m\text{milímetros}k}\beta_{11} & \cdots & u_{m\text{milímetros}k}\beta_{1\text{mil}} & \cdots & u_{m\text{milímetros}k}\beta_{k1} \end{pmatrix}$$

Os produtos tensores de três ou mais matrizes são definidos de forma análoga. Se $M_1, \dots, M_{n_{\text{ão}}}$ são matrizes cujos índices correspondem a conjuntos de estados clássicos $\Sigma_1, \dots, \Sigma_{n_{\text{ão}}}$, então o produto tensorial $M_1 \otimes \dots \otimes M_{n_{\text{ão}}}$ é definido pela condição de que

$$\langle u_{m1} \cdots u_{m_{n_{\text{ão}}}} | M_1 \otimes \dots \otimes M_{n_{\text{ão}}} | b_1 \cdots b_{n_{\text{ão}}} \rangle = \langle u_{m1} | M_1 | b_1 \rangle$$

para cada escolha de estados clássicos $u_{m1}, b_1 \in \Sigma_1, \dots, u_{m_{n_{\text{ão}}}}, b_{n_{\text{ão}}} \in \Sigma_{n_{\text{ão}}}$.

Alternativamente, também poderíamos definir o produto tensorial de três ou mais matrizes recursivamente, em termos de produtos tensoriais de duas matrizes, semelhante ao que observamos para vetores.

O produto tensorial de matrizes é algumas vezes considerado *multiplicativo* porque a equação

$$(M_1 \otimes \dots \otimes M_{n_{\text{ão}}}) (N_1 \otimes \dots \otimes N_{n_{\text{ão}}}) = (M_1 N_{1\text{ão}}) \otimes \dots \otimes (M_{n_{\text{ão}}} N_{n_{\text{ão}}})$$

é sempre verdadeiro, para qualquer escolha de matrizes $M_1, \dots, M_{n_{\tilde{a}o}}$ e $N_{\tilde{a}o_1}, \dots, N_{\tilde{a}o_{n_{\tilde{a}o}}}$, desde que os produtos $M_1 N_{\tilde{a}o_1}, \dots, M_{n_{\tilde{a}o}} N_{\tilde{a}o_{n_{\tilde{a}o}}}$

faz sentido.

Operações independentes (continuação)

Para resumir a discussão acima, descobrimos que se M é uma operação probabilística em X , N é uma operação probabilística em E , e as duas operações são realizadas de forma independente, então a operação resultante no sistema composto (X, E) é o produto tensorial $M \otimes N$.

O que vemos, tanto aqui como para estados probabilísticos, é que os *produtos tensoriais representam independência*: se tivermos dois sistemas X e E que estão independentemente nos estados probabilísticos $|\phi\rangle$ e $|\pi\rangle$, então o sistema composto (X, E) está no estado probabilístico $|\phi\rangle \otimes |\pi\rangle$; e se aplicarmos operações probabilísticas de forma independente M e N para os dois sistemas de forma independente, então a ação resultante no sistema composto (X, E) é descrito pela operação $M \otimes N$.

Vejamos um exemplo que nos lembra de uma operação probabilística sobre um único bit da lição anterior: se o estado clássico do bit é 0, ele é deixado sozinho; e se o estado clássico do bit for 1, é invertido para 0 com probabilidade $1/2$. Como observamos, esta operação é representada pela matriz

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}.$$

Se esta operação for realizada em um bit X , e uma operação NOT é (independentemente) executada em um segundo bit E , então a operação conjunta no sistema composto (X, E) tem a representação matricial

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \frac{1}{2} \\ 1 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

Pela inspeção, vemos que esta é uma matriz estocástica.

Este será sempre o caso: o produto tensorial de duas ou mais matrizes estocásticas é sempre estocástico.

Uma situação comum que encontramos é aquela em que uma operação é realizada em um sistema e *nada* é feito em outro. Em tal caso, exatamente a mesma prescrição é seguida, notando que *não fazer nada*

é representado pela matriz identidade. Por exemplo, redefinir o bitXpara

o estado e não fazer nada para ele produz a operação probabilística (e de fato determinística) em (X, E) representado pela matriz

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Informação quântica

Agora estamos preparados para passar para a informação quântica no cenário de sistemas múltiplos. Assim como na lição anterior sobre sistemas únicos, a descrição matemática da informação quântica para sistemas múltiplos é bem similar ao caso probabilístico e faz uso de conceitos e técnicas similares.

Estados quânticos

Sistemas múltiplos podem ser vistos coletivamente como sistemas compostos e únicos. Já observamos isso no cenário probabilístico, e o cenário quântico é análogo.

Ou seja, estados quânticos de sistemas múltiplos são representados por vetores de coluna com entradas de números complexos e norma euclidiana igual a 1 — assim como estados quânticos de sistemas únicos. No caso de sistemas múltiplos, os índices desses vetores são colocados em correspondência com o *produto cartesiano* dos conjuntos de estados clássicos associados a cada um dos sistemas individuais (porque esse é o conjunto de estados clássicos do sistema composto).

Por exemplo, se X e E são qubits, então o conjunto de estados clássico do par de qubits (X, E) , visto coletivamente como um único sistema, é o produto cartesiano $\{0, 1\} \times \{0, 1\}$. Ao representar pares de valores binários como cadeias binárias de comprimento dois, associamos este conjunto de produtos cartesianos ao conjunto $\{00, 01, 10, 11\}$. Os vetores a seguir são, portanto, todos exemplos de vetores de estado quântico do par (X, E) :

$$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{6}}|01\rangle + \frac{e}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{6}}|11\rangle, \quad \frac{3}{5}|00\rangle - \frac{4}{5}|11\rangle,$$

Há variações sobre como vetores de estado quântico de múltiplos sistemas são expressos, e podemos escolher qualquer variação que se adapte às nossas preferências. Aqui estão alguns exemplos, que são para o primeiro vetor de estado quântico acima.

- Podemos usar o fato de que $|ab\rangle = |u\rangle |v\rangle$ (para quaisquer estados clássicos u, v) para escrever em vez disso

$$\frac{1}{\sqrt{2}}|0\rangle |0\rangle - \frac{1}{\sqrt{6}}|0\rangle |1\rangle + \frac{eu}{\sqrt{6}}|1\rangle |0\rangle + \frac{1}{\sqrt{6}}|1\rangle |1\rangle.$$

- Podemos escolher escrever o símbolo do produto tensorial explicitamente assim:

$$\frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle - \frac{1}{\sqrt{6}}|0\rangle \otimes |1\rangle + \frac{eu}{\sqrt{6}}|1\rangle \otimes |0\rangle + \frac{1}{\sqrt{6}}|1\rangle \otimes$$

- Podemos subscrever os kets para indicar como eles correspondem aos sistemas considerados, assim:

$$\frac{1}{\sqrt{2}}|0\rangle_x |0\rangle_E - \frac{1}{\sqrt{6}}|0\rangle_x |1\rangle_E + \frac{eu}{\sqrt{6}}|1\rangle_x |0\rangle_E + \frac{1}{\sqrt{6}}|1\rangle_x |1\rangle_E.$$

Claro, também podemos escrever vetores de estado quântico explicitamente como vetores de coluna:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{6}} \\ \frac{eu}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} \end{pmatrix}.$$

Dependendo do contexto em que aparece, uma dessas variações pode ser preferida — mas todas são equivalentes no sentido de que descrevem o mesmo vetor.

Produtos tensores de vetores de estado quântico

Semelhante ao que temos para vetores de probabilidade, produtos tensoriais de vetores de estado quântico também são vetores de estado quântico — e novamente eles representam *independência* entre sistemas.

Em maior detalhe, e começando com o caso de dois sistemas, suponha que $|\phi\rangle$ é um vetor de estado quântico de um sistema X e $|\psi\rangle$ é um vetor

de estado quântico de um sistema E . O produto tensorial $|\phi\rangle \otimes |\psi\rangle$,

que pode ser escrito alternativamente como $|\phi\rangle \otimes |\psi\rangle$ ou como $|\phi \otimes \psi\rangle$, é então um vetor de estado quântico do sistema conjunto (X, E) . Nós nos referimos a um estado dessa forma como um *estado de produto*.

Intuitivamente falando, quando um par de sistemas (X, E) está em um estado de produto $|\phi\rangle \otimes |\psi\rangle$, podemos interpretar isso como significando que X está no estado quântico $|\phi\rangle$, E está no estado quântico $|\psi\rangle$, e os estados dos dois sistemas não têm nada a ver um com o outro.

O fato de que o vetor produto tensorial $|\phi\rangle \otimes |\psi\rangle$ é de fato um vetor de estado quântico é consistente com a norma euclidiana sendo *multiplicativa* em relação aos produtos tensoriais:

$$\begin{aligned} \| |\phi\rangle \otimes |\psi\rangle \| &= \sqrt{\sum_{(a,b) \in \Sigma \times \Gamma} |\langle ab | \phi \otimes \psi \rangle|^2} \\ &= \sqrt{\sum_{a \in \Sigma} \sum_{b \in \Gamma} |\langle a | \phi \rangle \langle b | \psi \rangle|^2} \\ &= \sqrt{\left(\sum_{a \in \Sigma} |\langle a | \phi \rangle|^2 \right) \left(\sum_{b \in \Gamma} |\langle b | \psi \rangle|^2 \right)} \\ &= \| |\phi\rangle \| \| |\psi\rangle \|. \end{aligned}$$

Assim, porque $|\phi\rangle$ e $|\psi\rangle$ são vetores de estado quântico, temos $\| |\phi\rangle \| = 1$ e $\| |\psi\rangle \| = 1$, e portanto $\| |\phi\rangle \otimes |\psi\rangle \| = 1$, então $|\phi\rangle \otimes |\psi\rangle$ também é um vetor de estado quântico.

Esta discussão pode ser generalizada para mais de dois sistemas. Se $|\psi_1\rangle, \dots, |\psi_{n\tilde{a}o}\rangle$ são vetores de estado quânticos de sistemas $X_1, \dots, X_{n\tilde{a}o}$, então $|\psi_1\rangle \otimes \dots \otimes |\psi_{n\tilde{a}o}\rangle$ é um vetor de estado quântico que representa um *estado de produto* do sistema conjunto $(X_1, \dots, X_{n\tilde{a}o})$. Novamente, sabemos que este é um vetor de estado quântico porque

$$\| |\psi_1\rangle \otimes \dots \otimes |\psi_{n\tilde{a}o}\rangle \| = \| |\psi_1\rangle \| \dots \| |\psi_{n\tilde{a}o}\rangle \| = 1^{n\tilde{a}o} = 1.$$

Estados emaranhados

Nem todos os vetores de estado quântico de sistemas múltiplos são estados de produto. Por exemplo, o vetor de estado quântico

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \quad (6)$$

de dois qubits não é um estado de produto. Para raciocinar isso, podemos seguir exatamente o mesmo argumento que usamos para provar que o estado probabilístico representado pelo vetor (5) não é um estado do produto.

Isto é, se (6) fosse um estado de produto, existiriam vetores de estado quântico $|\phi\rangle$ e $|\psi\rangle$ para qual

$$|\phi\rangle \otimes |\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Mas então seria necessariamente o caso de que

$$\langle 0|\phi\rangle \langle 1|\psi\rangle = \langle 01|\phi \otimes \psi\rangle = 0$$

implicando que $\langle 0|\phi\rangle = 0$ ou $\langle 1|\psi\rangle = 0$ (ou ambos). Isso contradiz o fato de que

$$\langle 0|\phi\rangle \langle 0|\psi\rangle = \langle 00|\phi \otimes \psi\rangle = \frac{1}{\sqrt{2}}$$

e

$$\langle 1|\phi\rangle \langle 1|\psi\rangle = \langle 11|\phi \otimes \psi\rangle = \frac{1}{\sqrt{2}}$$

são ambos diferentes de zero.

Observe que o valor específico $1/\sqrt{2}$ não é importante para este argumento — o que é importante é que este valor seja diferente de zero. Assim, por exemplo, o estado quântico

$$\frac{3}{5}|00\rangle + \frac{4}{5}|11\rangle$$

também não é um estado de produto, pelo mesmo argumento.

Segue-se que o vetor de estado quântico (6) representa uma *correlação* entre dois sistemas e, especificamente, dizemos que os sistemas estão *emaranhados*.

O emaranhamento é uma característica quintessencial da informação quântica que será discutida com muito mais detalhes em lições posteriores. O emaranhamento pode ser complicado, particularmente para os tipos de estados quânticos ruidosos que podem ser descritos na formulação geral da matriz de densidade da informação quântica que foi mencionada na Lição 1 — mas para vetores de estado quântico na formulação simplificada em que estamos nos concentrando nesta unidade, o emaranhamento é equivalente à correlação. Ou seja, qualquer

vetor de estado quântico que não seja um vetor de produto representa um estado emaranhado.

Em contraste, o vetor de estado quântico

$$\frac{1}{2}|00\rangle + \frac{eu}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{eu}{2}|11\rangle$$

é um exemplo de um estado de produto:

$$\frac{1}{2}|00\rangle + \frac{eu}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{eu}{2}|11\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right) \otimes \left(\frac{1}{2}|0\rangle + \frac{eu}{2}|1\rangle \right)$$

Portanto, esse estado não está emaranhado.

Bell afirma

Agora daremos uma olhada em alguns exemplos importantes de estados quânticos de múltiplos qubits, começando com os *estados de Bell*. Estes são os quatro estados de dois qubits a seguir:

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle \end{aligned}$$

Os estados de Bell são assim chamados em homenagem a João Sino.

Observe que o mesmo argumento que estabelece que $|\phi^+\rangle$ não é um estado de produto revela que nenhum dos outros estados de Bell também é um estado de produto — todos os quatro estados de Bell representam o emaranhamento entre dois qubits.

A coleção de todos os quatro estados de Bell

$$\{ |\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle \}$$

é conhecido como a *base de Bell*; qualquer vetor de estado quântico de dois qubits, ou mesmo qualquer vetor complexo que tenha entradas correspondentes aos quatro estados clássicos de dois bits, pode ser expresso como uma combinação linear dos quatro estados de Bell. Por exemplo,

$$|00\rangle = \frac{1}{\sqrt{2}}|\phi^+\rangle + \frac{1}{\sqrt{2}}|\phi^-\rangle.$$

Estados GHZ e W

A seguir, consideraremos dois exemplos interessantes de estados de três qubits.

O primeiro exemplo que consideraremos representa um quantum de três qubits (X, E, Z), é o *estado GHZ* (assim chamado em homenagem a Daniel Greenberger, Michael Horne e Anton Zeilinger, que primeiro estudaram algumas de suas propriedades):

$$\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle.$$

O segundo exemplo é o chamado estado W:

$$\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle.$$

Nenhum desses estados é um estado produto, o que significa que eles não podem ser escritos como um produto tensorial de três vetores de estado quântico de qubits.

Examinaremos esses dois estados mais detalhadamente quando discutirmos medições parciais de estados quânticos de múltiplos sistemas.

Exemplos adicionais

Os exemplos de estados quânticos de múltiplos sistemas que vimos até agora são estados de dois ou três qubits, mas também podemos ter estados quânticos de múltiplos sistemas com diferentes conjuntos de estados clássicos.

Por exemplo, aqui está um estado quântico de três sistemas, X, E, Z, onde o conjunto de estados clássicos de X é o alfabeto binário (então X é um qubit) e o conjunto de estados clássico de E e Z é $\{\clubsuit, \diamond, \heartsuit, \spadesuit\}$:

$$\frac{1}{2}|0\rangle|\heartsuit\rangle|\heartsuit\rangle + \frac{1}{2}|1\rangle|\spadesuit\rangle|\heartsuit\rangle - \frac{1}{\sqrt{2}}|0\rangle|\heartsuit\rangle|\diamond\rangle.$$

E aqui está um exemplo de um estado quântico de três sistemas (X, E, Z), onde X, E, Z todos compartilham o mesmo conjunto de estados clássico $\{0, 1, 2\}$:

$$\frac{|012\rangle - |021\rangle + |120\rangle - |102\rangle + |201\rangle - |210\rangle}{\sqrt{6}}.$$

Sistemas que possuem o conjunto de estados clássico $\{0, 1, 2\}$ são frequentemente chamados de *trits* ou, assumindo que consideramos a possibilidade de que estejam em estados quânticos, *qutrits*. O termo *qudit* se refere a um sistema com conjunto de estados clássico $\{0, \dots, e-1\}$ para uma escolha arbitrária de e .

Medições de estados quânticos

As medições de base padrão de estados quânticos de sistemas individuais foram discutidas na lição anterior: se um sistema com conjunto de estados clássico Σ está em um estado quântico representado pelo vetor $|\psi\rangle$, e esse sistema é medido (com relação a uma medição de base padrão), então cada estado clássico $u \in \Sigma$ aparece com probabilidade $|\langle u | \psi \rangle|^2$.

Isso nos diz o que acontece quando temos um estado quântico de múltiplos sistemas e escolhemos medir todo o sistema composto (o que é equivalente a medir *todos* os sistemas). Para afirmar isso precisamente, vamos supor que $X_1, \dots, X_{n\tilde{o}}$ são sistemas que possuem conjuntos de estados clássicos $\Sigma_1, \dots, \Sigma_{n\tilde{o}}$, respectivamente. Podemos então visualizar $(X_1, \dots, X_{n\tilde{o}})$ coletivamente como um único sistema cujo conjunto de estados clássico é o produto cartesiano $\Sigma_1 \times \dots \times \Sigma_{n\tilde{o}}$. Se um estado quântico deste sistema for representado pelo vetor de estado quântico $|\psi\rangle$, e todos os sistemas são medidos, então cada resultado possível $(u_1, \dots, u_{n\tilde{o}}) \in \Sigma_1 \times \dots \times \Sigma_{n\tilde{o}}$ aparece com probabilidade $|\langle u_1 \dots u_{n\tilde{o}} | \psi \rangle|^2$.

Por exemplo, se os sistemas X e E estão conjuntamente no estado quântico

$$\frac{3}{5}|0\rangle|\heartsuit\rangle - \frac{4}{5}|1\rangle|\spadesuit\rangle,$$

então medir ambos os sistemas com relação a uma medição de base padrão produz o resultado $(0, \heartsuit)$ com probabilidade $9/25$ e o resultado $(1, \spadesuit)$ com probabilidade $16/25$.

Medições parciais para dois sistemas

Agora vamos considerar a situação em que temos múltiplos sistemas em

algum estado quântico, e medimos um subconjunto próprio dos

sistemas. Como antes, começaremos com dois sistemas X e E tendo conjuntos de estados clássicos Σ e Γ , respectivamente.

Em geral, um vetor de estado quântico de (X, E) assume a forma

$$|\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} \alpha_{a,b} |ab\rangle,$$

onde $\{\alpha_{a,b} : (a,b) \in \Sigma \times \Gamma\}$ é uma coleção de números complexos que satisfazem

$$\sum_{(a,b) \in \Sigma \times \Gamma} |\alpha_{a,b}|^2 = 1$$

(que é equivalente a $|\psi\rangle$ sendo um vetor unitário).

Já sabemos, pela discussão acima, que se ambos X e E foram medidos, então cada resultado possível $(a,b) \in \Sigma \times \Gamma$ apareceria com probabilidade

$$|\langle ab | \psi \rangle|^2 = |\alpha_{a,b}|^2.$$

Supondo que apenas o primeiro sistema X é medido, a probabilidade para cada resultado $a \in \Sigma$ aparecer deve, portanto, ser igual a

$$\sum_{b \in \Gamma} |\langle ab | \psi \rangle|^2 = \sum_{b \in \Gamma} |\alpha_{a,b}|^2.$$

Isto é consistente com o que já vimos no cenário probabilístico, e é mais uma vez consistente com nossa compreensão da física. Isto é, a probabilidade de cada resultado particular aparecer quando X é medido não pode depender de se ou não E também foi medido, pois isso permitiria uma comunicação mais rápida que a luz.

Tendo obtido um resultado particular $a \in \Sigma$ desta medição de X , esperamos que o estado quântico de X muda para que seja igual a $|a\rangle$, como tínhamos para sistemas individuais. Mas o que acontece com o estado quântico de E ?

Para responder a esta questão, vamos descrever o estado quântico conjunto de (X, E) sob a suposição de que X foi medido (com relação a uma medição de base padrão) e o resultado foi o estado clássico a .

Primeiro expressamos o vetor $|\psi\rangle$ como

$$|\psi\rangle = \sum_{um \in \Sigma} |um\rangle \otimes |\phi_{um}\rangle,$$

onde

$$|\phi_{um}\rangle = \sum_{b \in \Gamma} \alpha_{b,um} |b\rangle$$

para cada $um \in \Sigma$. Observe que a probabilidade de que a medição da base padrão de X resulte em cada resultado um pode ser escrita da seguinte forma:

$$\sum_{b \in \Gamma} |\alpha_{b,um}|^2 = \langle \phi_{um} | \phi_{um} \rangle.$$

Agora, como resultado da medição da base padrão de X resultando no resultado um , temos que o estado quântico do par (X, E) juntos se tornam

$$|um\rangle \otimes \frac{|\phi_{um}\rangle}{\|\phi_{um}\rangle\|}$$

Ou seja, o estado “entra em colapso” como no caso do sistema único, mas apenas na medida em que é necessário para que o estado seja consistente com a medição de X tendo produzido o resultado um .

Falando informalmente, $|um\rangle \otimes \frac{|\phi_{um}\rangle}{\|\phi_{um}\rangle\|}$ representa o componente de $|\psi\rangle$ que é consistente com a medição de X resultando no resultado um . Normalizamos este vetor — dividindo-o pela sua norma euclidiana, que é igual a $\|\phi_{um}\rangle\|$ — para produzir um vetor de estado quântico válido com norma euclidiana igual a 1. Esta etapa de normalização é análoga ao que fizemos no cenário probabilístico quando dividimos vetores pela soma de suas entradas para obter um vetor de probabilidade.

Como exemplo, consideremos o estado de dois qubits (X, E) do início da seção:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{6}}|01\rangle + \frac{eu}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{6}}|11\rangle.$$

Para entender o que acontece quando o primeiro sistema X é medido, começamos escrevendo

$$|\psi\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{6}}|1\rangle\right) + |1\rangle \otimes \left(\frac{eu}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle\right)$$

Agora vemos, com base na descrição acima, que a probabilidade de a medição resultar no resultado 0 é

$$\left\| \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{6}}|1\rangle \right\|^2 = \frac{1}{2} + \frac{1}{6} = \frac{2}{3}$$

nesse caso o estado de (X, E) torna-se

$$|0\rangle \otimes \frac{\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{6}}|1\rangle}{\sqrt{\frac{2}{3}}} = |0\rangle \otimes \left(\sqrt{\frac{3}{4}}|0\rangle - \frac{1}{2}|1\rangle \right);$$

e a probabilidade de a medição resultar no resultado 1 é

$$\left\| \frac{eu}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle \right\|^2 = \frac{1}{6} + \frac{1}{6} = \frac{1}{3}$$

nesse caso o estado de (X, E) torna-se

$$|1\rangle \otimes \frac{\frac{eu}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle}{\sqrt{\frac{1}{3}}} = |1\rangle \otimes \left(\frac{eu}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right).$$

A mesma técnica, usada de forma simétrica, descreve o que acontece se o segundo sistema E é medido em vez do primeiro. Reescrevemos o vetor $|\psi\rangle$ como

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{eu}{\sqrt{6}}|1\rangle \right) \otimes |0\rangle + \left(-\frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle \right) \otimes |1\rangle$$

A probabilidade de que a medição de E produza o resultado 0 é

$$\left\| \frac{1}{\sqrt{2}}|0\rangle + \frac{eu}{\sqrt{6}}|1\rangle \right\|^2 = \frac{1}{2} + \frac{1}{6} = \frac{2}{3}$$

nesse caso o estado de (X, E) torna-se

$$\frac{\frac{1}{\sqrt{2}}|0\rangle + \frac{eu}{\sqrt{6}}|1\rangle}{\sqrt{\frac{2}{3}}} \otimes |0\rangle = \left(\sqrt{\frac{3}{4}}|0\rangle + \frac{eu}{2}|1\rangle \right) \otimes |0\rangle;$$

e a probabilidade de que o resultado da medição seja 1 é

$$\left\| -\frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle \right\|^2 = \frac{1}{6} + \frac{1}{6} = \frac{1}{3}$$

nesse caso o estado de (X, E) torna-se

$$-\frac{\frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle}{\frac{1}{\sqrt{3}}} \otimes |1\rangle = \left(-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes |1\rangle.$$

Observação sobre estados quânticos reduzidos

Este exemplo mostra uma limitação da descrição simplificada da informação quântica: ela não nos oferece nenhuma maneira de descrever o estado quântico reduzido (ou marginal) de apenas um dos dois sistemas (ou um subconjunto adequado de qualquer número de sistemas), como fizemos no caso probabilístico.

Especificamente, dissemos que para um estado probabilístico de dois sistemas (X, E) descrito por um vetor de probabilidade

$$|\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} p_{\text{sobre}} |ab\rangle,$$

o estado *reduzido* (ou *marginal*) de X sozinho é descrito pelo vetor de probabilidade

$$\sum_{(a,b) \in \Sigma \times \Gamma} p_{\text{sobre}} |um\rangle.$$

Para vetores de estado quântico, não há análogo — para um vetor de estado quântico

$$|\phi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} um_{\text{sobre}} |ab\rangle,$$

o vetor

$$|\phi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} um_{\text{sobre}} |um\rangle$$

não é um vetor de estado quântico em geral, e não representa adequadamente o conceito de um estado reduzido ou marginal. Pode ser, de fato, que esse vetor seja o vetor zero.

Então, o que devemos fazer em vez disso é nos voltar para a descrição geral da informação quântica. Como descreveremos na Unidade 3, a descrição geral da informação quântica fornece uma maneira significativa de definir estados quânticos reduzidos que é análoga à configuração probabilística.

Medições parciais para três ou mais sistemas

Medições parciais para três ou mais sistemas, onde algum subconjunto apropriado dos sistemas é medido, podem ser reduzidas ao caso de dois

sistemas, dividindo os sistemas em duas coleções: aqueles que são medidos e aqueles que não são.

Aqui está um exemplo específico que ilustra como isso pode ser feito. Ele demonstra como subscriver kets pelos nomes dos sistemas que eles representam pode ser útil — neste caso porque nos dá uma maneira simples de descrever permutações dos sistemas.

Por exemplo, temos um estado quântico de 5 sistemas X_1, \dots, X_5 , todos compartilhando o mesmo conjunto de estados clássico

$\{\clubsuit, \diamond, \heartsuit, \spadesuit\}$:

$$\begin{aligned} & \sqrt{\frac{1}{7}} |\heartsuit\rangle |\clubsuit\rangle |\diamond\rangle |\spadesuit\rangle |\spadesuit\rangle + \sqrt{\frac{2}{7}} |\diamond\rangle |\clubsuit\rangle |\diamond\rangle |\spadesuit\rangle |\clubsuit\rangle + \sqrt{\frac{1}{7}} |\spadesuit\rangle |\heartsuit\rangle |\heartsuit\rangle |\heartsuit\rangle |\heartsuit\rangle \\ & - eu \sqrt{\frac{2}{7}} |\heartsuit\rangle |\clubsuit\rangle |\diamond\rangle |\heartsuit\rangle |\heartsuit\rangle - \sqrt{\frac{1}{7}} |\spadesuit\rangle |\heartsuit\rangle |\clubsuit\rangle |\spadesuit\rangle |\spadesuit\rangle \end{aligned}$$

Consideraremos a situação em que o primeiro e o terceiro sistemas são medidos, e os sistemas restantes são deixados sozinhos.

Conceitualmente falando, não há diferença fundamental entre esta situação e uma em que um dos dois sistemas é medido — mas infelizmente, como os sistemas medidos são intercalados com os sistemas não medidos, enfrentamos um obstáculo ao escrever as expressões necessárias para executar esses cálculos. Uma maneira de proceder é, como mencionado acima, subscriver os kets para indicar a quais sistemas eles se referem. Isso nos dá a liberdade de alterar sua ordem, como descreveremos agora.

Primeiro, o vetor de estado quântico acima pode ser escrito alternativamente como

$$\begin{aligned} & \sqrt{\frac{1}{7}} |\heartsuit\rangle_1 |\clubsuit\rangle_2 |\diamond\rangle_3 |\spadesuit\rangle_4 |\spadesuit\rangle_5 + \sqrt{\frac{2}{7}} |\diamond\rangle_1 |\clubsuit\rangle_2 |\diamond\rangle_3 |\spadesuit\rangle_4 |\clubsuit\rangle_5 \\ & + \sqrt{\frac{1}{7}} |\spadesuit\rangle_1 |\spadesuit\rangle_2 |\clubsuit\rangle_3 |\diamond\rangle_4 |\clubsuit\rangle_5 - eu \sqrt{\frac{2}{7}} |\heartsuit\rangle_1 |\clubsuit\rangle_2 |\diamond\rangle_3 |\heartsuit\rangle_4 |\heartsuit\rangle_5 \\ & - \sqrt{\frac{1}{7}} |\spadesuit\rangle_1 |\heartsuit\rangle_2 |\clubsuit\rangle_3 |\spadesuit\rangle_4 |\spadesuit\rangle_5. \end{aligned}$$

Nada aqui mudou, exceto que cada ket agora tem um subscrito indicando a qual sistema ele corresponde. Aqui usamos os subscritos $1, \dots, 5$, mas os nomes dos próprios sistemas também podem ser usados (numa situação em que temos nomes de sistemas como X, E, eZ , por exemplo).

Podemos então reordenar os kets e coletar os termos da seguinte forma:

$$\begin{aligned}
 & \sqrt{\frac{1}{7}} |\heartsuit\rangle_1 |\diamond\rangle_3 |\clubsuit\rangle_2 |\spadesuit\rangle_4 |\spadesuit\rangle_5 + \sqrt{\frac{2}{7}} |\diamond\rangle_1 |\diamond\rangle_3 |\clubsuit\rangle_2 |\spadesuit\rangle_4 |\clubsuit\rangle_5 \\
 & + \sqrt{\frac{1}{7}} |\spadesuit\rangle_1 |\clubsuit\rangle_3 |\spadesuit\rangle_2 |\diamond\rangle_4 |\clubsuit\rangle_5 - eu \sqrt{\frac{2}{7}} |\heartsuit\rangle_1 |\diamond\rangle_3 |\clubsuit\rangle_2 |\heartsuit\rangle_4 |\spadesuit\rangle_5 \\
 & - \sqrt{\frac{1}{7}} |\spadesuit\rangle_1 |\clubsuit\rangle_3 |\heartsuit\rangle_2 |\spadesuit\rangle_4 |\clubsuit\rangle_5 \\
 & = |\heartsuit\rangle_1 |\diamond\rangle_3 \left(\sqrt{\frac{1}{7}} |\clubsuit\rangle_2 |\spadesuit\rangle_4 |\spadesuit\rangle_5 - eu \sqrt{\frac{2}{7}} |\clubsuit\rangle_2 |\heartsuit\rangle_4 |\spadesuit\rangle_5 \right) \\
 & + |\diamond\rangle_1 |\diamond\rangle_3 \left(\sqrt{\frac{2}{7}} |\clubsuit\rangle_2 |\spadesuit\rangle_4 |\clubsuit\rangle_5 \right) \\
 & + |\spadesuit\rangle_1 |\clubsuit\rangle_3 \left(\sqrt{\frac{1}{7}} |\spadesuit\rangle_2 |\diamond\rangle_4 |\clubsuit\rangle_5 - \sqrt{\frac{1}{7}} |\heartsuit\rangle_2 |\spadesuit\rangle_4 |\clubsuit\rangle_5 \right)
 \end{aligned}$$

(Os produtos tensoriais ainda são implícitos, mesmo quando parênteses são usados, como neste exemplo.)

Agora vemos que se os sistemas X_1 e X_3 são medidas, as probabilidades (diferentes de zero) dos diferentes resultados são as seguintes:

- O resultado da medição (\heartsuit, \diamond) ocorre com probabilidade

$$\left\| \sqrt{\frac{1}{7}} |\clubsuit\rangle_2 |\spadesuit\rangle_4 |\spadesuit\rangle_5 - eu \sqrt{\frac{2}{7}} |\clubsuit\rangle_2 |\heartsuit\rangle_4 |\heartsuit\rangle_5 \right\|^2 = \frac{1}{7} + \frac{2}{7} = \frac{3}{7}$$

- O resultado da medição (\diamond, \diamond) ocorre com probabilidade

$$\left\| \sqrt{\frac{2}{7}} |\clubsuit\rangle_2 |\spadesuit\rangle_4 |\clubsuit\rangle_5 \right\|^2 = \frac{2}{7}$$

- O resultado da medição (\spadesuit, \clubsuit) ocorre com probabilidade

$$\left\| \sqrt{\frac{1}{7}} |\spadesuit\rangle_2 |\diamond\rangle_4 |\clubsuit\rangle_5 - \sqrt{\frac{1}{7}} |\heartsuit\rangle_2 |\spadesuit\rangle_4 |\clubsuit\rangle_5 \right\|^2 = \frac{1}{7} + \frac{1}{7} = \frac{2}{7}$$

Se o resultado da medição for (\heartsuit, \diamond) , por exemplo, temos que o estado de (X_1, \dots, X_5) torna-se

$$|\heartsuit\rangle_1|\diamond\rangle_3 \otimes \frac{\sqrt{\frac{1}{7}}|\clubsuit\rangle_2|\spadesuit\rangle_4|\spadesuit\rangle_5 - eu \sqrt{\frac{2}{7}}|\clubsuit\rangle_2|\heartsuit\rangle_4|\heartsuit\rangle_5}{\sqrt{\frac{3}{7}}} \\ = \sqrt{\frac{1}{3}}|\heartsuit\rangle_1|\clubsuit\rangle_2|\diamond\rangle_3|\spadesuit\rangle_4|\spadesuit\rangle_5 - eu \sqrt{\frac{2}{3}}|\heartsuit\rangle_1|\clubsuit\rangle_2|\diamond\rangle_3|\heartsuit\rangle_4$$

Para outros resultados de medição, o estado pode ser determinado de maneira semelhante.

Agora, deve-se entender que o produto tensorial não é comutativo: se $|\phi\rangle$ e $|\pi\rangle$ são vetores, então, em geral, $|\phi\rangle \otimes |\pi\rangle$ é diferente de $|\pi\rangle \otimes |\phi\rangle$, e da mesma forma para produtos tensoriais de três ou mais vetores. Por exemplo, $|\heartsuit\rangle|\clubsuit\rangle|\diamond\rangle|\spadesuit\rangle|\spadesuit\rangle$ é um vetor diferente de $|\heartsuit\rangle|\diamond\rangle|\clubsuit\rangle|\spadesuit\rangle|\spadesuit\rangle$. A técnica recém descrita de reordenar kets não deve ser interpretada como sugerindo o contrário. Em vez disso, para fins de execução de cálculos e expressão dos resultados, estamos simplesmente tomando uma decisão de que é mais conveniente coletar os sistemas X_1, \dots, X_5 juntos como $(X_1, X_3, X_2, X_4, X_5)$ em vez de $(X_1, X_2, X_3, X_4, X_5)$. Os subscritos nos kets servem para manter tudo isso em ordem.

Analogamente, no contexto estreitamente relacionado, mas mais simples, dos produtos cartesianos e dos pares ordenados, se u e b são estados clássicos diferentes, então (u, b) e (b, u) também são diferentes. No entanto, dizer que o estado clássico de dois bits (X, E) é $(1, 0)$ é equivalente a dizer que o estado clássico de (E, X) é $(0, 1)$; quando cada sistema tem seu próprio nome exclusivo, não importa realmente a ordem que escolhemos para listá-los, desde que a ordem fique clara.

Finalmente, aqui estão dois exemplos envolvendo os estados GHZ e W, como prometido anteriormente. Primeiro, vamos considerar o estado GHZ

$$\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle.$$

Se apenas o primeiro sistema for medido, obtemos o resultado 0 com probabilidade $1/2$, nesse caso o estado dos três qubits se torna $|000\rangle$; e também obtemos o resultado 1 com probabilidade $1/2$, nesse caso o estado dos três qubits se torna $|111\rangle$.

Em seguida, vamos considerar um estado W, que pode ser escrito assim:

$$\begin{aligned} & \frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle \\ &= |0\rangle \left(\frac{1}{\sqrt{3}}|01\rangle + \frac{1}{\sqrt{3}}|10\rangle \right) + |1\rangle \left(\frac{1}{\sqrt{3}}|00\rangle \right). \end{aligned}$$

A probabilidade de que uma medição do primeiro qubit resulte no resultado 0 é, portanto, igual a

$$\left\| \frac{1}{\sqrt{3}}|01\rangle + \frac{1}{\sqrt{3}}|10\rangle \right\|^2 = \frac{2}{3},$$

e condicionado à medição que produz este resultado, o estado quântico dos três qubits torna-se

$$|0\rangle \otimes \frac{\frac{1}{\sqrt{3}}|01\rangle + \frac{1}{\sqrt{3}}|10\rangle}{\sqrt{\frac{2}{3}}} = |0\rangle \left(\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \right) = |0\rangle |\psi\rangle$$

A probabilidade de que o resultado da medição seja 1 é $1/3$, nesse caso o estado dos três qubits se torna $|100\rangle$.

Operações unitárias

Em seções anteriores desta lição, usamos o produto cartesiano para tratar sistemas individuais como um sistema único e maior. Seguindo a mesma linha de pensamento, podemos representar operações em múltiplos sistemas como matrizes unitárias agindo no vetor de estado deste sistema maior.

Em princípio, qualquer matriz unitária cujas linhas e colunas correspondem aos estados clássicos de qualquer sistema que estejamos pensando representa uma operação quântica válida — e isso vale para sistemas compostos cujos conjuntos de estados clássicos são produtos cartesianos dos conjuntos de estados clássicos dos sistemas individuais.

Concentrando-se em dois sistemas, se X é um sistema com conjunto de estados clássico Σ e E é um sistema com conjunto de estados clássico Γ , então o conjunto de estados clássico do sistema conjunto (X, E) é $\Sigma \times \Gamma$ — e, portanto, o conjunto de operações que podem ser realizadas neste sistema conjunto são representadas por matrizes unitárias cujas linhas e colunas são colocadas em correspondência com o conjunto $\Sigma \times \Gamma$. A ordenação das linhas e colunas dessas matrizes é a mesma que a ordenação usada para vetores de estado quântico do sistema (X, E) .

Por exemplo, suponhamos que $\Sigma = \{1, 2, 3\}$ e $\Gamma = \{0, 1\}$, e lembre-se de que a convenção padrão para ordenar os elementos do produto cartesiano $\{1, 2, 3\} \times \{0, 1\}$ é $(1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)$. Aqui está um exemplo de uma matriz unitária que representa uma operação em (X, E) :

$$U = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{eu}{2} & -\frac{1}{2} & 0 & 0 & -\frac{eu}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{2} & -\frac{eu}{2} & -\frac{1}{2} & 0 & 0 & \frac{eu}{2} \\ 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix}.$$

Esta operação unitária não é importante, é apenas um exemplo. Para verificar se U é unitário, basta calcular: $U^\dagger U = I$.

A ação de U na base padrão do vetor $|11\rangle$, por exemplo, é

$$U |11\rangle = \frac{1}{2} |10\rangle + \frac{eu}{2} |11\rangle - \frac{1}{2} |20\rangle - \frac{eu}{2} |30\rangle,$$

o que podemos ver examinando a segunda coluna de U , considerando nossa ordenação do conjunto $\{1, 2, 3\} \times \{0, 1\}$.

Como em qualquer matriz, é possível expressar U usando a notação de Dirac usando 20 termos para as 20 entradas diferentes de zero de U . No entanto, se escrevêssemos todos esses termos em vez de escrever uma 6×6 matrix, podemos perder certos padrões que são evidentes da expressão matrix. Simplificando, a notação de Dirac nem sempre é a melhor escolha para como representar matrizes.

Operações unitárias em três ou mais sistemas funcionam de maneira semelhante, com as matrizes unitárias tendo linhas e colunas correspondentes ao produto cartesiano dos conjuntos de estados clássicos dos sistemas.

Já vimos um exemplo nesta lição: a operação de três qubits

$$\sum_{k=0}^7 |(k+1) \bmod 8\rangle \langle k|$$

de antes, onde $|j\rangle$ significa a codificação binária de três bits do número j , U é unitária. Operações que são unitárias e representam operações

determinísticas são chamadas de operações *reversíveis*. A transposta conjugada desta matriz pode ser escrita assim:

$$\sum_{k=0}^7 |k\rangle \langle (k+1) \bmod 8| = \sum_{k=0}^7 |(k-1) \bmod 8\rangle \langle k|.$$

Esta matriz representa o *reverso*, ou em termos matemáticos o *inverso*, da operação original — que é o que esperamos da transposta conjugada de uma matriz unitária.

Veremos outros exemplos de operações unitárias em múltiplos sistemas à medida que a lição avança.

Operações unitárias realizadas independentemente em sistemas individuais

Quando operações unitárias são realizadas independentemente em uma coleção de sistemas individuais, a ação combinada dessas operações independentes é descrita pelo produto tensorial das matrizes unitárias que as representam. Ou seja, se $X_1, \dots, X_{n\tilde{a}o}$ são sistemas quânticos, $\hat{v}oc\hat{e}_1, \dots, \hat{v}oc\hat{e}_{n\tilde{a}o}$ são matrizes unitárias que representam operações nesses sistemas, e as operações são realizadas independentemente nos sistemas, a ação combinada em $(X_1, \dots, X_{n\tilde{a}o})$ é representado pela matriz $\hat{v}oc\hat{e}_1 \otimes \dots \otimes \hat{v}oc\hat{e}_{n\tilde{a}o}$. Mais uma vez, descobrimos que as configurações probabilísticas e quânticas são análogas nesse aspecto.

Seria de se esperar naturalmente, a partir da leitura do parágrafo anterior, que o produto tensorial de qualquer coleção de matrizes unitárias fosse unitário. De fato, isso é verdade, e podemos verificar isso da seguinte forma.

Observe primeiro que a operação de transposição conjugada satisfaz

$$(M_1 \otimes \dots \otimes M_{n\tilde{a}o})^\dagger = M_1^\dagger \otimes \dots \otimes M_{n\tilde{a}o}^\dagger$$

para qualquer coleção de matrizes $M_1, \dots, M_{n\tilde{a}o}$. Isso pode ser verificado voltando à definição do produto tensorial e da transposta conjugada, e verificando se cada entrada dos dois lados da equação está de acordo. Isso significa que

$$(\hat{v}oc\hat{e}_1 \otimes \dots \otimes \hat{v}oc\hat{e}_{n\tilde{a}o})^\dagger (\hat{v}oc\hat{e}_1 \otimes \dots \otimes \hat{v}oc\hat{e}_{n\tilde{a}o}) = (\hat{v}oc\hat{e}_1^\dagger \otimes \dots \otimes \hat{v}oc\hat{e}_{n\tilde{a}o}^\dagger) (\hat{v}oc\hat{e}_1 \otimes \dots \otimes \hat{v}oc\hat{e}_{n\tilde{a}o})$$

Como o produto tensorial das matrizes é multiplicativo, descobrimos que

$$(\underbrace{você_1^\dagger}_{1} \otimes \cdots \otimes \underbrace{você_{n\tilde{o}}^\dagger}_{n\tilde{o}}) (\underbrace{você_1}_{1} \otimes \cdots \otimes \underbrace{você_{n\tilde{o}}}_{n\tilde{o}}) = (\underbrace{você_1^\dagger}_{1} \underbrace{você_1}_{1})$$

Aqui escrevemos $EU_1, \dots, EU_{n\tilde{o}}$ para se referir às matrizes que representam a operação de identidade nos sistemas $X_1, \dots, X_{n\tilde{o}}$ — o que quer dizer que estas são matrizes identidade cujos tamanhos concordam com o número de estados clássicos de $X_1, \dots, X_{n\tilde{o}}$.

Finalmente, o produto tensorial $EU_1 \otimes \cdots \otimes EU_{n\tilde{o}}$ é igual à matriz identidade, onde temos um número de linhas e colunas que concorda com o produto do número de linhas e colunas das matrizes $EU_1, \dots, EU_{n\tilde{o}}$. Podemos ver esta matriz de identidade maior como representando a operação de identidade no sistema conjunto $(X_1, \dots, X_{n\tilde{o}})$.

Em resumo, temos a seguinte sequência de igualdades:

$$\begin{aligned} & (\underbrace{você_1^\dagger}_{1} \otimes \cdots \otimes \underbrace{você_{n\tilde{o}}^\dagger}_{n\tilde{o}}) (\underbrace{você_1}_{1} \otimes \cdots \otimes \underbrace{você_{n\tilde{o}}}_{n\tilde{o}}) \\ &= (\underbrace{você_1^\dagger}_{1} \otimes \cdots \otimes \underbrace{você_1^\dagger}_{1}) (\underbrace{você_1}_{1} \otimes \cdots \otimes \underbrace{você_{n\tilde{o}}}_{n\tilde{o}}) \\ &= (\underbrace{você_1^\dagger}_{1} \underbrace{você_1}_{1}) \otimes \cdots \otimes (\underbrace{você_{n\tilde{o}}^\dagger}_{n\tilde{o}} \underbrace{você_{n\tilde{o}}}_{n\tilde{o}}) \\ &= EU_1 \otimes \cdots \otimes EU_{n\tilde{o}} \\ &= EU. \end{aligned}$$

Concluimos, portanto, que $\underbrace{você_1^\dagger}_{1} \otimes \cdots \otimes \underbrace{você_{n\tilde{o}}^\dagger}_{n\tilde{o}}$ é unitário.

Uma situação importante que frequentemente surge é aquela em que uma operação unitária é aplicada a apenas um sistema — ou um subconjunto apropriado de sistemas — dentro de um sistema conjunto maior. Por exemplo, suponha que X e E são sistemas que podemos ver juntos como formando um único sistema composto (X, E) , e realizamos uma operação apenas no sistema X . Para sermos precisos, suponhamos que $você$ é uma matriz unitária que representa uma operação em X , de modo que suas linhas e colunas foram colocadas em correspondência com os estados clássicos de X .

Dizer que realizamos a operação representada por $você$ apenas no sistema X implica que não fazemos nada para E , significando que realizamos de forma independente $você$ sobre X e a *operação de identidade* em E . Ou seja, “não fazer nada” para E é equivalente a realizar a operação de identidade em E , que é representado pela matriz identidade EU_E . (Aqui, a propósito, o subscrito E nos diz que EU_E refere-se à matriz identidade que possui um número de linhas e colunas de acordo com o conjunto de estados clássico de E .) A operação em

(X, E) que é obtido quando realizamos *você* sobre *X* e não fazer nada para *E*, portanto, representado pela matriz unitária

$$você \otimes EU_E.$$

Por exemplo, se *X* e *E* são qubits, realizando uma operação de Hadamard em *X* (e não fazer nada para *E*) é equivalente a realizar a operação

$$O \otimes EU_E = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

no sistema articular (X, E) .

Na mesma linha, podemos considerar que uma operação representada por uma matriz unitária *você* é aplicado a *E* e nada é feito para *X*, nesse caso a operação resultante em (X, E) é representado pela matriz unitária

$$EU_X \otimes você.$$

Por exemplo, se considerarmos novamente a situação em que ambos *X* e *E* são qubits e *você* é uma operação de Hadamard, a operação resultante em (X, E) é representado pela matriz

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

Nem toda operação unitária em uma coleção de sistemas $X_1, \dots, X_{n\tilde{a}o}$ pode ser escrito como um produto tensorial de operações unitárias $você_1 \otimes \dots \otimes você_{n\tilde{a}o}$, assim como nem todo vetor de estado quântico desses sistemas é um estado de produto. Por exemplo, nem a operação de troca nem a operação NOT controlada em dois qubits, que são descritas abaixo, podem ser expressas como um produto tensorial de operações unitárias.

A operação de troca

Para concluir a lição, vamos dar uma olhada em duas classes de exemplos de operações unitárias em múltiplos sistemas, começando com a *operação de troca*.

Suponha que X e E são sistemas que compartilham o mesmo conjunto de estados clássicos Σ . A operação *de swap* no par (X, E) é a operação que troca o conteúdo dos dois sistemas, mas, de outra forma, deixa os sistemas sozinhos (de modo que X permanece à esquerda e E permanece à direita).

Vamos denotar esta operação como $TROCAR$. Ele opera assim para cada escolha de estados clássicos $a, b \in \Sigma$:

$$TROCAR |a\rangle |b\rangle = |b\rangle |a\rangle.$$

Uma maneira de escrever a matriz associada a esta operação usando a notação de Dirac é a seguinte:

$$TROCAR = \sum_{c, d \in \Sigma} |c\rangle \langle d| \otimes |d\rangle \langle c|.$$

Pode não ficar imediatamente claro que esta matriz representa $TROCAR$, mas podemos verificar se satisfaz a condição $TROCAR |a\rangle |b\rangle = |b\rangle |a\rangle$ para cada escolha de estados clássicos $a, b \in \Sigma$.

Como um exemplo simples, quando X e E são qubits, descobrimos que

$$TROCAR = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Operações unitárias controladas

Agora vamos supor que P é um qubit e R é um sistema arbitrário, tendo qualquer conjunto de estados clássicos que desejamos.

Para cada operação unitária U agindo no sistema R , uma *controlada* U operação é uma operação unitária no par (P, R) definido como segue:

$$U_{\text{controlada}} = |0\rangle \langle 0| \otimes U_R + |1\rangle \langle 1| \otimes U.$$

Por exemplo, se R também é um qubit e pensamos no Pauli X operação em R , então um controlado- X operação é dada por

$$CX = |0\rangle\langle 0| \otimes EU_R + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Já encontramos essa operação no contexto de informações clássicas e operações probabilísticas anteriormente na lição.

Se em vez disso considerarmos o PauliZ operação em R no lugar do X operação, obtemos esta operação:

$$República Checa = |0\rangle\langle 0| \otimes EU_R + |1\rangle\langle 1| \otimes Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Se em vez disso tomarmos R para ser dois qubits, e tomamos *você* para ser a *operação de troca* entre esses dois qubits, obtemos esta operação:

$$CSWAP = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Esta operação também é conhecida como uma *operação de Fredkin* (ou, mais comumente, uma *porta de Fredkin*), nomeada em homenagem a Edward Fredkin. Sua ação em estados de base padrão pode ser descrita como segue:

$$CSWAP |0\ b\ c\rangle = |0\ b\ c\rangle$$

$$CSWAP |1\ b\ c\rangle = |1\ c\ b\rangle$$

Finalmente, a *operação controlada-controlada-NÃO*, que podemos denotar como *CCX*, é chamada de *operação de Toffoli* (ou *porta de Toffoli*), nomeada em homenagem a Tommaso Toffoli. Sua representação matricial se parece com isso:

$$CCX = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Podemos alternativamente expressá-lo usando a notação de Dirac da seguinte forma:

$$CCX = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes EU + |11\rangle\langle 11|$$

Exemplos de Qiskit

Na lição anterior, aprendemos sobre o Qiskit `Vetor de estado` e `Operador` classes, e as usamos para simular sistemas quânticos. Nesta seção, nós as usaremos para explorar o comportamento de múltiplos sistemas. Começaremos importando essas classes, assim como a função de raiz quadrada de `NumPy`.

```
1 from qiskit.quantum_info import Statevector, Operator
2 from numpy import sqrt
```

Nenhuma saída produzida

Produtos tensores

O `Vetor de estado` a classe tem uma `tensor` método que retorna o produto tensorial de si mesmo e de outro `Vetor de estado`.

Por exemplo, abaixo criamos dois vetores de estado representando $|0\rangle$ e $|1\rangle$, e usar o `tensor` método para criar um novo vetor, $|0\rangle \otimes |1\rangle$.

```
1 zero, one = Statevector.from_label("0"), Statevector.from_label("1")
2 zero.tensor(one).draw("latex")
```

Saída:

$|01\rangle$

Em outro exemplo abaixo, criamos vetores de estado que representam o $|+\rangle$ e $\frac{1}{\sqrt{2}}(|0\rangle + eu|1\rangle)$ estados e combiná-los para criar um novo vetor de estado. Atribuiremos esse novo vetor à variável `psi`.

```
1 plus = Statevector.from_label("+")
2 i_state = Statevector([1 / sqrt(2), 1j / sqrt(2)])
3 psi = plus.tensor(i_state)
4
5 psi.draw("latex")
```

Saída:

$\frac{1}{2}|00\rangle + \frac{eu}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{eu}{2}|11\rangle$

O `Operator` a classe também tem uma `tensor` método. No exemplo abaixo, criamos o `X` e `I` portas e exibir seu produto tensorial.

```
1 X = Operator([[0, 1], [1, 0]])
2 I = Operator([[1, 0], [0, 1]])
3
4 X.tensor(I)
```

Saída:

```
Operator([[0.+0.j, 0.+0.j, 1.+0.j, 0.+0.j],
          [0.+0.j, 0.+0.j, 0.+0.j, 1.+0.j],
          [1.+0.j, 0.+0.j, 0.+0.j, 0.+0.j],
          [0.+0.j, 1.+0.j, 0.+0.j, 0.+0.j]],
          input_dims=(2, 2), output_dims=(2, 2))
```

Podemos então tratar esses estados e operações compostos como fizemos com sistemas simples na lição anterior. Por exemplo, na célula abaixo calculamos

$$(EU \otimes X) |\psi\rangle$$

para o estado `psi` definimos acima. (O ^ operador tensores matrizes juntos.)

```
1 | psi.evolve(I ^ X).draw("latex")
```



Saída:

$$\frac{eu}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{eu}{2}|10\rangle + \frac{1}{2}|11\rangle$$

Abaixo, criamos um `CX` operador e calcular $CX |\psi\rangle$.

```
1 | CX = Operator(
2 |     [
3 |         [1, 0, 0, 0],
4 |         [0, 1, 0, 0],
5 |         [0, 0, 0, 1],
6 |         [0, 0, 1, 0],
7 |     ]
8 | )
9 |
10 | psi.evolve(CX).draw(" latex")
```



Saída:

$$\frac{1}{2}|00\rangle + \frac{eu}{2}|01\rangle + \frac{eu}{2}|10\rangle + \frac{1}{2}|11\rangle$$

Medições parciais

Na página anterior, usamos o `medir` método para simular uma medição do vetor de estado quântico. Este método retorna dois itens: o resultado da medição simulada e o novo `Vetor de estado` dada esta medição.

Por padrão, `medir` mede todos os qubits no vetor de estado, mas podemos fornecer uma lista de inteiros para medir apenas os qubits nesses índices. Para demonstrar, a célula abaixo cria o estado

$$C = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle).$$

(Observe que o Qiskit é projetado principalmente para uso com computadores quânticos baseados em qubit. Como tal, Vetor de estado tentará interpretar qualquer vetor com 2^n elementos como um sistema de n qubits. Você pode substituir isso passando um escalar argumento para o construtor. Por exemplo, `Statevector(4, 2)` diria ao Qiskit que o sistema tem um sistema de quatro níveis e um sistema de dois níveis (qubit).)

```
1 | W = Statevector([0, 1, 1, 0, 1, 0, 0, 0] / sqrt(3))
2 | W.draw("latex")
```



Copiar para a área de tr

Saída:

$$\frac{\sqrt{3}}{3}|001\rangle + \frac{\sqrt{3}}{3}|010\rangle + \frac{\sqrt{3}}{3}|100\rangle$$

A célula abaixo simula uma medição no qubit mais à direita (que tem índice 0). Os outros dois qubits não são medidos.

```
1 | result, new_sv = W.measure([0]) # measure qubit 0
2 | print(f"Measured: {result}\nState after measurement:")
3 | new_sv.draw("latex")
```



Saída:

```
Measured: 0
State after measurement:
```

$$\frac{\sqrt{2}}{2}|010\rangle + \frac{\sqrt{2}}{2}|100\rangle$$

Tente executar a célula algumas vezes para ver resultados diferentes. Observe que medir um `1` significa que sabemos que os outros dois qubits são $|0\rangle$, mas medindo um `0` significa que os dois qubits restantes estão no estado $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.