2
Distinção de Estados Quânticos

2.1
Fundamentos

Conhecer o *estado* de um sistema físico é ter toda a informação necessária para prever sua evolução temporal, assim como os efeitos de uma possível interação com outros sistemas. Por exemplo, no caso mais simples de todos — um sistema composto por uma partícula clássica, as variáveis dinâmicas que descrevem o estado do sistema são sua posição p e momento q. Em sistemas clássicos em geral, estas variáveis são *observáveis*, e então a quantidade de informação que podemos obter sobre elas (ou seja, a quantidade de informação *acessível* sobre o estado) depende apenas do quão precisas são as nossas medições. Obviamente, dizermos que tal precisão é arbitrariamente grande não corresponde à realidade, já que nossos aparelhos de medição sempre provocam alguma perturbação ao sistema observado e possuem precisão finita. É então aceito, em geral, que os estados sejam descritos de forma *aproximada*. No exemplo que citamos, uma maneira adequada de descrever o estado do sistema é através da função de densidade de probabilidade conjunta $\mathcal{P}(p, q)$.

Entretanto, se esta descrição aproximada do mundo que nos é fornecida pela Física Clássica não for suficiente para nossos propósitos, uma visão mais precisa pode ser obtida ao considerarmos a teoria quântica, onde os conceitos de *estados* e *observáveis* são, ao contrário do que vimos anteriormente, completamente distintos. O estado de um sistema quântico é representado por um vetor normalizado $|\psi\rangle$ em um espaço de Hilbert, e suas propriedades observáveis são, assim como na teoria clássica, posição, momento, etc. Entretanto, na teoria quântica, tais observáveis não são representados por variáveis dinâmicas que assumem valores determinados em cada instante de tempo, e sim por operadores auto-adjuntos no espaço de Hilbert em questão. Por um abuso de notação, costuma-se denotar tanto o observável quanto seu operador correspondente por A. Vale a pena ressaltar que esta distinção entre estados e observáveis não é apenas uma questão matemática. De fato, medir a posição e o momento de uma partícula quântica não é algo trivial como no caso clássico, pois não é possível realizar duas medições simultâneas e, mesmo que uma medição fosse feita imediatamente após a outra, ainda assim não obteríamos o resultado desejado: uma das propriedades fundamentais de Mecânica Quântica é que medições alteram o estado do sistema, ou seja, a primeira medição perturbaria o estado, e então uma segunda medição não seria feita sobre o mesmo estado.

A medição de certa grandeza A é geralmente um processo probabilístico: seja $A = \sum a_i|a_i\rangle\langle a_i|$ a decomposição espectral do operador correspondente. Uma medição *projetiva* de A é aquela expressada em termos dos projetores espectrais de A, e cujos resultados podem ser qualquer um dos valores a_i, cada um com certa probabilidade associada. Para calcular tais probabilidades, suponha que temos um conjunto de sistemas quânticos, todos preparados em um mesmo estado $|\psi\rangle$. Então o valor esperado de A é $\langle A\rangle = \langle\psi|A|\psi\rangle = \sum a_i|\langle\psi|a_i\rangle|^2$, e assim podemos afirmar que a probabilidade de que a medida de uma grandeza A produza o resultado a_i é $P(a_i|\psi) = |\langle\psi|a_i\rangle|^2$. Além disso, o estado pós-medição é $P_i|\psi\rangle$, onde P_i é o projetor espectral de A associado ao autovalor a_i que foi observado.

Quando um sistema quântico sabidamente está em um certo estado, dizemos que este é um estado *puro*. Mas, assim como na teoria clássica, os estados quânticos também não podem, em geral, ser descritos perfeitamente. Em analogia à função de densidade de probabilidade que mencionamos anteriormente, $\mathcal{P}(p, q)$, representaremos o vetor de estado do sistema por um *operador densidade*, $\rho = \sum p_k|\psi_k\rangle\langle\psi_k|$, onde p_k é a probabilidade de que o estado seja $|\psi_k\rangle$ e $\sum p_k = 1$ (ou seja, $\{|\psi_k\rangle\}_k$ é uma base para o espaço associado ao sistema). Neste caso, dizemos que o estado do sistema é *misto*. É imediato verificar que um operador densidade tem traço igual a 1 e é um operador positivo. Quanto à probabilidade de obtermos o resultado a_i quando medimos uma grandeza A de um sistema que está em um estado misto, podemos afirmar que $P(a_i|\rho) = \langle a_i|\rho|a_i\rangle = \mathrm{Tr}\rho|a_i\rangle\langle a_i|$.

2.2 Distinção via Medições Projetivas

O cenário usual em que trabalhamos é o seguinte: *Alice* deve preparar um sistema quântico, e para isso escolhe, com certa probabilidade, um estado pertencente a um conjunto finito de estados quânticos. As probabilidades de que cada estado seja escolhido não são necessariamente iguais. Ela então envia o sistema para *Bob*, dizendo a ele em quais estados o sistema pode estar, e as probabilidades associadas a cada um deles. Bob traça então alguma estratégia para obter o máximo de informação possível sobre o estado em que o sistema foi preparado.

A pergunta natural agora é a seguinte: até que ponto podemos determinar o estado de um sistema quântico? Obviamente, se pudéssemos descrevê-lo com exatidão, seríamos capazes de explicitar as probabilidades associadas a todos os resultados possíveis de uma medição sobre o sistema. Em Mecânica Quântica, o estado em si não é um observável, portanto esta tarefa não é trivial. Entretanto, através de uma escolha conveniente de observáveis, podemos obter informação sobre o estado.

O caso trivial de distinção de dois estados quânticos ocorre quando estes são ortogonais entre si: sejam $|\psi_1\rangle$ e $|\psi_2\rangle$ tais que $\langle\psi_1|\psi_2\rangle = 0$. Se realizarmos uma medição projetiva da forma $M = a_1|\psi_1\rangle\langle\psi_1| + a_2|\psi_2\rangle\langle\psi_2|$, obteremos o resultado a_1 se o sistema tiver sido preparado em $|\psi_1\rangle$, e o resultado a_2 se o estado for $|\psi_2\rangle$. Claramente, esta medição sempre distingue estre dois estados ortogonais, ou seja, a probabilidade de erro é igual a zero. A partir de agora, vamos então considerar o caso verdadeiramente interessante: o de estados não-ortogonais entre si.

Uma primeira estratégia que Bob poderia usar para distinguir estados não-ortogonais é aquela conhecida como *teste de hipóteses quântico*: digamos que o estado do sistema foi escolhido em um conjunto de n estados quânticos (onde cada um deles é representado por um operador densidade ρ_j). Seja ν_j a probabilidade de que o sistema tenha sido preparado no estado ρ_j, $j = 1, \ldots, n$. Para tentar adivinhar o estado do sistema, Bob realiza uma certa medição, a qual possui n resultados possíveis, digamos a_k. Caso obtenha a_j como resultado da medição, Bob afirma que o estado que recebeu de Alice era ρ_j. Obviamente, $\sum_{k=1}^{n} P(a_k|\rho_j) = 1$, ou seja, qualquer que seja o estado ρ_j do sistema, Bob sempre obterá um dos valores a_k como resultado. A probabilidade de que a resposta de Bob esteja errada é $1 - \sum_{j=1}^{n} \nu_j P(a_j|\rho_j)$, e foi demonstrado em 1973, em (20) que sempre existe uma medição projetiva que minimiza tal probabilidade.

Uma outra estratégia possível (de fato, a que adotaremos como padrão nesta tese) é aquela em que não admitimos erros nas previsões, mas sim resultados inconclusivos. Por exemplo, suponhamos que o sistema tenha sido preparado em um de dois estados conhecidos, $|\psi_1\rangle$ ou $|\psi_2\rangle$ (com probabilidades iguais para cada uma das situações). Consideremos a medição projetiva $P_{\psi_1} = |\psi_1^\perp\rangle\langle\psi_1^\perp|$. Se recebermos o valor 1 como resultado da medição, podemos afirmar com certeza que o sistema tinha sido preparado no estado $|\psi_2\rangle$. Já se o valor recebido for 0, nada pode ser afirmado sobre o estado. Analogamente, considerando a medição $P_{\psi_2} = |\psi_2^\perp\rangle\langle\psi_2^\perp|$, concluimos que o estado do sistema é $|\psi_1\rangle$ quando o resultado obtido é 1, e nada se pode afirmar quando o resultado é 0. A probabilidade de acerto, ou seja, a probabilidade de termos um resultado conclusivo, é $P = \frac{1-|\langle\psi_1|\psi_2\rangle|^2}{2}$.

Em seu artigo (18), Ivanovic mostrou que uma sequência de medições poderiam nos fornecer uma melhor probabilidade de acerto, em comparação com esta obtida através de uma única medição projetiva. Em (14), Diecks reescreveu tal sequência como uma *medição generalizada* (dita um *POVM — Positive Operator Valued Measure*). Por fim, Peres (26) mostrou que tal medição é de fato ótima, no sentido de que a probabilidade dos resultados inconclusivos é a menor possível. A probabilidade de acerto é conhecida como *limite de Ivanovic-Diecks-Peres*, dado por: $P = 1 - |\langle\psi_1|\psi_2\rangle|$. Vamos então agora descrever este POVM.

2.3 Distinção via POVMs

As medições projetivas que descrevemos anteriormente, P_{ψ_1} e P_{ψ_2}, têm cada uma dois resultados possíveis. Escolhendo uma delas, conseguimos identificar corretamente um dos estados, mas em contrapartida nunca identificamos o outro, além de perdemos o identificável algumas vezes também. Teríamos um melhor resultado (ou seja, uma maior probabilidade de acerto) se realizássemos uma medição com três resultados: $|\psi_1\rangle$, $|\psi_2\rangle$ e o inconclusivo, mas isto é impossível através de uma medição projetiva, já que seus elementos são ortogonais, e então o número máximo de resultados é igual à dimensão do espaço de Hilbert associado aos estados. É exatamente por isso que introduzimos o conceito de medição generalizada (POVM), onde o número de resultados é arbitrariamente grande, pois seus elementos não são necessariamente ortogonais. Um POVM (25) é basicamente um conjunto de operadores $\{\Pi_i\}$ auto-adjuntos e positivos semi-definidos tais que $\sum \Pi_i = I$. Para construir uma medição introduzimos um POVM de três operadores Π_1, Π_2 e Π_0, onde o último é associado aos resultados inconclusivos. Estes três operadores devem ser tais que $\langle\psi_1|\Pi_1|\psi_1\rangle = p_1$ é a probabilidade de identificarmos corretamente o estado $|\psi_1\rangle$, $\langle\psi_1|\Pi_0|\psi_1\rangle = q_1$ é a probabilidade de não conseguirmos identificar $|\psi_1\rangle$, e equações análogas para $|\psi_2\rangle$. Como não admitimos erros nas identificações, devemos ainda requerer $\langle\psi_1|\Pi_2|\psi_1\rangle = \langle\psi_2|\Pi_1|\psi_2\rangle = 0$. De modo geral, tal POVM pode ser expressado pelos seguintes operadores:

$$\begin{aligned}\Pi_1 &= \alpha|\psi_2^\perp\rangle\langle\psi_2^\perp| \\ \Pi_2 &= \beta|\psi_1^\perp\rangle\langle\psi_1^\perp| \\ \Pi_0 &= I - \Pi_1 - \Pi_2\,,\end{aligned}$$

onde α e β são determinados pela condição de não-negatividade dos três operadores.

A generalização destes operadores para o caso em que desejamos distinguir entre n estados linearmente independentes é facilmente obtida, e pode ser encontrada, por exemplo, em (10).

2.4 Probabilidade Ótima

Observe que até agora discutimos apenas o caso em que os dois estados tinham iguais probabilidades de terem sido escolhidos para a preparação do sistema. Como vimos, neste caso, a probabilidade ótima de distinção entre dois estados não-ortogonais é dada pelo limite de Ivanovic-Diecks-Peres, $P = 1-|\langle\psi_1|\psi_2\rangle|$. Para probabilidades arbitrárias, os resultados análogos foram deduzidos por Jaeger e Shimony em (19).

Sejam r e $1-r$ as probabilidades do sistema ter sido preparado em $|\psi_1\rangle$ e $|\psi_2\rangle$, respectivamente. Sem perda de generalidade, suponhamos $r \geq \frac{1}{2}$. Então, a probabilidade ótima de distinção dos estados $|\psi_1\rangle$ e $|\psi_2\rangle$ é dada por:

$$P = \begin{cases} 1 - 2\sqrt{r(1-r)}\,|\langle\psi_1|\psi_2\rangle| & \text{se } |\langle\psi_1|\psi_2\rangle|\sqrt{\frac{1-r}{r}} \geq |\langle\psi_1|\psi_2\rangle|^2 \\ r(1-|\langle\psi_1|\psi_2\rangle|^2) & \text{caso contrário.} \end{cases}$$

Para qubits, estas expressões para a probabilidade ótima podem ser facilmente deduzidas minimizando-se a probabilidade de obtermos resultados inconclusivos fornecidos pelo POVM da seção anterior, ou ainda impondo-se a condição de que tais medidas não podem ser usadas para transmitir sinais a velocidade maior que a da luz (3).