Revista Brasileira de Ensino de Física, v. 33, n. 4, 4303 (2011)
www.sbfisica.org.br

Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte

(Quantum information theory: non-cloning, entanglement and teleportation)

José Roberto Castilho Piqueira[1]

Escola Politécnica, Universidade de São Paulo, São Paulo, SP, Brasil
Recebido em 28/10/2010; Aceito em 21/6/2011; Publicado em 21/11/2011

A idéia de desenvolver computadores cuja dinâmica obedeça às leis da Mecânica Quântica data do último quarto do século XX e assume, nos dias de hoje, importância tecnológica e científica notável, uma vez que o uso de algoritmos quânticos se disseminou na implementação de sistemas de criptografia e, além disso, relatos de experimentos de comunicação sobre canais quânticos são cada vez mais presentes na literatura. Há, até, conjecturas sobre comportamentos quânticos em sinapses e em outros fenômenos naturais tidos como macroscópicos. Todos esses desenvolvimentos têm como base a teoria quântica da informação que, de maneira geral, pode ser considerada como uma extensão da teoria clássica devida a Shannon, considerando-se dois aspectos peculiares dos fenômenos quânticos: a incapacidade de se obter uma cópia de um estado quântico e o fato de estados quânticos apresentarem uma dependência mútua, originada na sua preparação. É desses dois tópicos que este trabalho se ocupa: sem a menor pretensão de originalidade, procura conceituar entrelaçamento (*entanglement*) e demonstrar o teorema da impossibilidade de cópia (*non-cloning theorem*). Algumas aplicações são apresentadas entremeadas com relatos de ficção, cuja eventual semelhança com fatos reais será mera coincidência.
Palavras-chave: desigualdades de Bell, espaços de Hilbert, produto tensorial, qubit.

The idea of developing computers with dynamics obeying Quantum Mechanics laws comes from the last quarter of 20th century assuming, nowadays, a remarkable technological and scientific importance, as the use of quantum algorithms has been disseminated on implementing cryptography systems and, besides, quantum channel experiments start to become present in the literature. There are, even, conjectures about quantum behaviors in synapses and in other natural phenomena considered to be macroscopic. All these developments are based on Quantum Information Theory that, generally speaking, could be considered an extension of Classical Information Theory, due to Shannon, taking into account two peculiar aspects of quantum phenomena: the impossibility of copying a quantum state and the mutual dependence shown by two states originated in their preparation. This work is about these two points without originality intentions, presents the concept of entanglement and the proof of the non-conning theorem. Some applications, mixed with fiction, are presented and possible similarity with real facts is a mere coincidence.
Keywords: Bell inequalities, Hilbert spaces, tensor product, qubit.

1. Introdução

Embora a mecânica quântica tenha seus principais fundamentos teóricos desenvolvidos na primeira metade do século XX, a idéia de relacioná-la à ciência da computação data de 1981 quando, no Caltech, Richard Feynman, John Hopfield e Carver Mead ministraram um curso interdisciplinar denominado *The Physics of Computation*. Esse curso foi ministrado várias vezes, até o agravamento do estado de saúde de Richard Feynman, por volta de 1986 [1].

Sempre na forma de seminários, o curso contou com palestras de grandes especialistas como Marvin Minsky, Charles Bennet, John Cocke, Gerry Sussman, além dos organizadores. Os assuntos tratados versavam sobre os limites e potencialidades da computação no mundo físico. A publicação datada de setembro de 1996 [2], das notas dos seminários, constitui importante marco nos estudos de computação quântica que, atualmente, atingem um estado de amplo desenvolvimento, apresentando várias vertentes: a computação quântica propriemente dita, com computadores de alguns qubits já construídos experimentalmente; os algoritmos quânticos para fatoração utilizados para processos de criptografia; a comunicação sobre canais quânticos, já implementada para enlaces ópticos de al-

[1]E-mail: piqueira@lac.usp.br.

guns quilômetros [3, 4].

Esse progresso nas aplicações da mecânica quântica tomou como base a teoria da informação de Shannon [5], hoje dita clássica, que foi generalizada para o caso quântico levando em conta duas peculiaridades: a impossibilidade de copiar uma estado quântico (*non-cloning theorem*) e o entrelaçamento entre estados quânticos (*entanglement*).

Essas duas peculiaridades serão aqui explicadas, iniciando-se com uma sessão sobre os postulados da mecânica quântica e a representação de estados em um espaço de Hilbert [4]. Em seguida, o comportamento dinâmico de um sistema quântico será discutido, a partir do conceito de porta quântica. Nesse ponto, enuncia-se e demonstra-se o teorema da impossibilidade de cópia discutindo-se suas implicações do ponto de vista informacional.

Finaliza-se com a discussão do conceito de entrelaçamento e de não localidade, partindo de idéias qualitativas e discutindo o paradoxo EPR (Einstein-Podolski-Rosen) e as desigualdades de Bell [6], seguindo-se a breve descrição de algumas aplicações.

2. Formulação de Dirac da mecânica quântica

Os principais conceitos relativos à teoria quântica da informação são desenvolvidos partindo da formulação de Dirac que considera que o estado de um sistema pode ser representado por um vetor de um espaço complexo n-dimensional, H^n, com estrutura de espaço de Hilbert, isto é, de um espaço vetorial normado completo, equipado com a definição de produto interno [7].

De maneira simplificada, o estado de um sistema pode ser representado por um vetor coluna com n componentes complexas, denominado "ket" e representado por $|. >$. A cada "ket" corresponde um vetor linha de mesma dimensão n, chamado "bra" e representado por $< .|$, cujas componentes são dadas pelo conjugado da componente correspondente do "ket".

Assim, caso o "ket" $|x>$ seja representado por

$$|x>= \begin{bmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{bmatrix},$$

o "bra" $< x|$ será representado por

$$< x| = \begin{bmatrix} x_1^* & x_2^* & ... & x_n^* \end{bmatrix},$$

com (*) indicando o complexo conjugado.

Compactamente, $< x| = (|x>)^{*T}$, isto é, o "bra" é o conjugado transposto do "ket" [8]. Os termos "bra" e "ket" foram escolhidos pois originam-se da divisão da palavra *braket* que, no idioma Inglês, significa colchete, em dois pedaços. Como se o símbolo matemático representativo do colchete ($< . >$) resultasse da justaposição de um "bra" e um "ket".

Para que o espaço vetorial H^n de "kets" seja um espaço de Hilbert é necessário definir produto interno como uma aplicação do produto cartesiano $H^n X H^n$ no conjunto dos números complexos, que deve, para todo $|x>, |y>$ e $|z> \in H^n$ e todo c_1 e $c_2 \in C$ satisfazer

- $i) < x|y> = < y|x>^*$;
- $ii) < x|x> \geq 0, < x|x> = 0 \Longleftrightarrow |x> = 0$;
- $iii) < x|c_1 y + c_2 z> = c_1 < x|y> + c_2 < x|z>$.

Uma vez definido produto interno, a norma de um vetor em H^n é dada por: $||x|| = \sqrt{< x|x>}$.

Considerando que H^n tem dimensão finita, é possível considerar um conjunto $E = \{|e_1>, |e_2>, ...|e_n>\}$ de "kets" ortonormais, isto é, $< e_i|e_j> = \delta_{i,j}$, de tal maneira que todo $|x> \in H^n$: $|x> = x_1|e_1> + x_2|e_2> + ... + x_n|e_n>$ e as representações de "kets" por vetores coluna e "bras" por vetores linha fica evidente. Nessas condições, o produto interno de dois vetores $< x|y>$ pode ser escrito como: $< x|y> = x_1^* y_1 + x_2^* y_2 + ... + x_n^* y_n$.

Essas idéias permitem estabelecer o que se costuma chamar de "primeiro postulado da mecânica quântica" [8] que formalmente se enuncia como:

> O estado $|\Psi>$ de um sistema quântico pode ser representado em um espaço de Hilbert por uma combinação linear de elementos de uma base ortonormal $E = \{|\phi_1>, |\phi_2>, ...|\phi_n>\}$, dada por:
>
> $$|\Psi> = \alpha_1|\phi_1> + \alpha_2|\phi_2> + ... + \alpha_n|\phi_n>, \quad (1)$$
>
> com $\alpha_1\alpha_1^* + \alpha_2\alpha_2^* + ... + \alpha_n\alpha_n^* = 1$.

A interpretação desse postulado é que, do ponto de vista da mecânica quântica, os valores possíveis para as diversas grandezas de um sistema físico, pertencem a um conjunto enumerável que pode ser finito ou infinito. Para evitar complicações matemáticas, somente os conjuntos finitos são considerados nesta pequena resenha.

Sendo um pouco mais específico, caso a expressão (1) seja relativa à posição de uma partícula, se nenhuma medição for executada ela se encontra, simultaneamente, em todas as posições $|\phi_i>$ possíveis. Quando a medição é feita, um dos estados $|\phi_i>$ é obtido, com probabilidade $\alpha_i\alpha_i^*$.

Tendo como base esse conceito de superposição de estados pode-se estabelecer a unidade fundamental de informação quântica, o *quantum bit* (qubit) considerando um sistema quântico cujo espaço de estados seja bi-dimensional equipado com a base $E = \{|0>, |1>\}$, seus estados são expressos por qubits na forma

$$|\Psi> = \alpha_1|0> + \alpha_2|1>, \quad (2)$$

com $\alpha_1\alpha_1^* + \alpha_2\alpha_2^* = 1$.

Intuitivamente, tudo se passa como se fosse uma extensão do conceito clássico de *bit*, isto é, caso uma moeda *clássica* esteja no interior de uma caixa fechada, seu estado pode ser cara (h) ou coroa (t), sendo representado pelo *bit* 0 ou 1. Entretanto, se a moeda do interior da caixa fechada for *quântica*, seu estado será uma superposição de cara (h) e coroa (t) podendo, por exemplo, ser representado pelo *qubit*: $\frac{1}{\sqrt{2}}(|0> + |1>)$ [9].

3. Evolução temporal de um sistema quântico

A pergunta seguinte a ser respondida é: como o estado de um sistema quântico evolui ao longo do tempo? Em outras palavras: dado o estado inicial $|\Psi_0>$, no instante t_0, como ele se relaciona com o estado $|\Psi_t>$, no instante $t > t_0$?

A resposta a essa questão é dada no chamado "segundo postulado da mecânica quântica" [8], enunciado como

> O estado $|\Psi_t>$ relaciona-se com o estado $|\Psi_0>$ pelo operador dependente do tempo $U_t : H^n \to H^n$, isto é
>
> $$|\Psi_t> = U_t(|\Psi_0>), \qquad (3)$$
>
> com o operador U_t satisfazendo as seguintes propriedades
>
> - Preservação da norma: $||U_t(|\Psi>)|| = |||\Psi>||, \forall t \in R,\ \forall |\Psi> \in H^2$;
> - Linearidade: $U_t(\alpha_1|\phi_1> + \alpha_2|\phi_2> + ... + \alpha_n|\phi_n>) = \alpha_1 U_t(|\phi_1>) + \alpha_2 U_t(|\phi_2>) + ... + \alpha_n U_t(|\phi_n>), \forall t \in R, \forall \alpha_i \in C, \forall\ |\phi_i> \in H^n$;
> - $U_{t_1+t_2}(|\Psi>) = U_{t_1}U_{t_2}(|\Psi>)$, $\forall\ t_1, t_2 \in R, \forall |\Psi> \in H^n$;
> - $\lim_{t\to t_0} U_t(|\Psi(t)>) = |\Psi(t_0)>, \forall\, t_0 \in R, \forall\, |\Psi> \in H^n$.

O fato do operador U_t satisfazer às restrições supradescritas implica duas propriedades adicionais

- O operador U_t é unitário, isto é, $U_t^* = U_t$;
- A cada U_t corresponde um único operador auto-adjunto H, isto é, tal que $H = (H^*)^T$, que satisfaz $U_t = e^{-2\pi i t H/h}$, sendo $i = \sqrt{(-1)}$ e h, a constante de Planck.

Usando essas propriedades, é possível demostrar que a Eq. (3) implica a equaçãode Schrödinger unidimensional

$$\frac{ih}{2\pi}\frac{d|\Psi>}{dt} = H|\Psi(t)>\,. \qquad (4)$$

A título de exemplo, a seguir são apresentados dois casos interessantes de evolução temporal de sistemas quânticos: o jogo de cara-coroa quântico e a porta "negação" (not).

3.1. A moeda quântica

O experimento clássico quando se desenvolve teoria de probabilidades é o de jogar uma moeda e discutir quão provável é sair cara (h) ou coroa (t). Lá, uma moeda é considerada honesta se, em um grande número de jogadas, metade delas resultam (h) e metade, (t).

Uma versão quântica do mesmo experimento pode ser vista partindo da representaçãodos estados $|h>$ e $|t>$ em H^2 como

$$|h> = \begin{bmatrix} 1 \\ 0 \end{bmatrix};$$

$$|t> = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Aplicando o conceito de lançamento honesto de uma moeda ao caso quântico, a transformação U_t que leva os estados puros $|h>$ e $|t>$ a um estado constituído pela superposição em que ambos são equiprováveis é a chamada transformação Hadamard-Walsh [4], que pode ser representada matricialmente por

$$M = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

Assim, o produto $M|h>$ resulta

$$|x> = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix};$$

e o produto $M|t>$ resulta

$$|y> = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

Entretanto, a aplicação de M sobre $|x>(|y>)$ reproduz $|h>(|t>)$, o que mostra que a interpretação probabilística da mecânica quântica não está ligada ao desconhecimento dos fenômenos, mas à superposição de estados.

3.2. A porta "not" quântica

Como mais uma ilustração da idéia de evolução temporal em sistemas quânticos, seja a transformação representada por

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

Considerando as representações dos estados $|0>$ e $|1>$ como:

$$|0> = \begin{bmatrix} 1 \\ 0 \end{bmatrix};$$

$$|1> = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

$N|0> = |1>$ e $N|1> = |0>$ e, portanto, o operador N representa uma porta "not" quântica.

4. Teorema da impossibilidade de cópia

Deixando de lado aspectos culturais, não há dúvida que a informação clássica pode ser copiada. Livros, jornais, revistas, apostilas, *blogs* e *sites* contêm infinidades de reproduções dos mais diversos tipos de documentos gerados pela espécie humana.

Entretanto, a informação quântica não é reprodutível. Em outras palavras, é impossível copiar um estado quântico. Esse fato é conhecido como teorema da impossibilidade de cópia, havendo na literatura vários enunciados e demonstrações diferentes [3, 4, 8, 9]. O enunciado e a demonstação presentes em [8], por sua simplicidade e clareza, serão apresentados.

Para tanto, seja um espaço de Hilbert H^n, equipado com uma base ortonormal $E = \{|e_1>, |e_2>, ...|e_n>\}$, isto é, $< e_i|e_j >= \delta_{i,j}$. Seja $|e_1>$ o estado escolhido como *folha branca* e $|x> \in H^n$ um estado a ser copiado sobre a *folha branca*.

Caso a cópia seja possível, deve existir um mapa unitário $U : H^2 \rightarrow H^2$, chamado *máquina copiadora*, tal que

$$U(|x>|e_1>) = |x>|x> . \tag{5}$$

Teorema 1 *Para $n > 1$ não há máquina copiadora quântica.*

Prova:

A prova será feita pelo chamado método indireto, considerando que existe uma máquina copiadora quântica para $n > 1$.

Como $n > 1$ há, pelo menos, dois estados ortogonais $|e_1>$ e $|e_2>$ e na hipótese da existência da copiadora quântica: $U(|e_1>|e_1>) = |e_1>|e_1>$ e, também, $U(|e_2>|e_1>) = |e_2>|e_2>$.

Além disso,

$$\begin{aligned} &U[\frac{1}{\sqrt{2}}(|e_1> + |e_2>)|e_1>] = \\ &\frac{1}{\sqrt{2}}(|e_1> + |e_2>)\frac{1}{\sqrt{2}}(|e_1> + |e_2>) = \\ &\frac{1}{2}(|e_1>|e_1> + |e_1>|e_2> + |e_2>|e_1> + \\ &|e_2>|e_2> . \end{aligned} \tag{6}$$

Como, de acordo com o postulado apresentado no item 3, U deve ser linear:

$$\begin{aligned} &U[\frac{1}{\sqrt{2}}(|e_1> + |e_2>)|e_1>] = \\ &\frac{1}{\sqrt{2}}U(|e_1>|e_1>) + \frac{1}{\sqrt{2}}U(|e_2>|e_1>) = \\ &\frac{1}{\sqrt{2}}(|e_1>|e_1>) + \frac{1}{\sqrt{2}}(|e_2>|e_2>). \end{aligned} \tag{7}$$

Os resultados das Eqs. (8) e (9) são diferentes e, portanto, a hipótese de que há copiadora quântica para $n > 1$ é incorreta. Logo, não há copiadora quântica para $n > 1$ e o teorema está demonstrado.

5. Não localidade e entrelaçamento: explicação informal

Nesta sessão, os conceitos de não localidade e de entrelaçamento serão apresentados tendo como base uma analogia desenvolvida na Ref. [10]. Será feita, apenas, uma interpretação do que já está apresentado na Ref. [10], trazendo de original, apenas, a escolha dos nomes dos detetives e os lugares para onde foram viajar. Os nomes escolhidos são Jocelyn Bennaton e Henrique Del Nero, em homenagem a dois grandes amigos, e as cidades, Florianópolis e Campos de Jordão, bem a gosto de cada um.

Então, que se inicie a narrativa ficcional. Jocelyn e Henrique são dois astutos detetives dos quadros policiais brasileiros, acostumados a desvendar intrigantes mistérios como o aparecimento de ETs em Varginha e do *chupa-cabras* no interior do estado de São Paulo. Entretanto, até eles têm períodos de férias e, em um deles, Jocelyn foi a Florianópolis surfar e Henrique, a Campos de Jordão, relaxar no ambiente montanhoso.

Decorridos alguns dias, cada um deles recebeu, no endereço em que estava hospedado, uma estranha encomenda: 1000 caixas de titânio, numeradas de 1 a 1000. Henrique, assustado com a encomenda, telefonou para Jocelyn e, ambos, ao abrirem as diversas caixas e observarem os resultados, perceberam que as caixas, aparentemente, faziam uma espécie de trabalho conjunto: se a caixa de número n de Henrique, quando aberta, emitia luz azul (vermelha), a de Jocelyn também emitia. Henrique, sempre pragmático, concluiu que nada de excepcional havia nisso: apenas que as caixas haviam sido previamente programadas dessa forma.

Jocelyn, um pouco mais desconfiado e curioso ficou com a dúvida: será que não há algum tipo de ação imediata, à distância? Isto é, será que a abertura de uma caixa em Campos de Jordão e a consequente emissão de luz, não determina a luz a ser emitida pela caixa correspondente em Florianópolis?

Esse pequeno relato ilustra a controvérsia a respeito da mecânica quântica, que durou até os anos 1980. Duas partículas, elétrons, por exemplo, geradas simultaneamente e em seguida separadas têm spin não definido em torno de qualquer eixo enquanto nenhuma medida for efetuada. Entretanto, quando o spin de uma delas é medido, assume um certo valor (horário ou anti-horário) e, então, o spin da outra também se torna conhecido, mesmo que não se tenha acesso a ela.

Era à essa idéia que Einstein se opunha pois acreditava que, caso a interpretação da não localidade fosse verdadeira, haveria uma ação à distância de propagação instantânea, ou seja, com velocidade maior do que a velocidade da luz. Essas idéias levaram à publicação do artigo clássico sobre o hoje denominado paradoxo EPR (Einstein, Podolsky e Rosen), que considera a mecânica quântica como uma descrição incompleta da realidade [11].

Essa discussão permeou o desenvolvimento da física teórica entre os anos 30 e 60 do século XX, embora muitos a considerassem irrelevante, uma vez que os cálculos feitos tomando a mecânica quântica como base produziam resultados compatíveis com os fatos experimentais.

Em [11], Einstein, Podolsky e Rosen argumentavam que a idéia de não localidade era incorreta e poderia ser explicada de maneira semelhante à conservação de momento na Mecânica Clássica: ao medir a velocidade de uma partícula após um choque, sabe-se a velocidade da outra sem efetuar medidas, pois o conhecimento de suas massas e a conservação do momento proporcionam o seu valor.

David Bohm, na década de 1950, explorou bastante esse modo de pensar, formulando a teoria das "Variáveis Escondidas" [12, 13]. Essas variáveis seriam responsáveis pela determinação dos valores das grandezas relativas às duas partículas. Inacessíveis antes das medições mas, uma vez realizada a medição em uma partícula, o valor relativo à outra está determinado por algum teorema de conservação.

O raciocínio EPR e de variáveis escondidas para o caso dos spins é análogo ao do agente Henrique no caso das caixas de titânio. Há, embora não visível, uma relação programada entre as cores emitidas quando da abertura das caixas.

Felizmente, o trabalho dos agentes Henrique e Jocelyn não para por aí. Decorridos mais alguns dias, cada um deles recebe uma nova remessa de caixas de titânio, agora com três tampas (frente, cima, lateral), também numeradas sequencialmente. Caso uma das tampas de uma das caixas seja aberta, haverá, ao acaso, a emissão de luz vermelha ou azul.

Quando Henrique e Jocelyn abrem a mesma tampa de duas caixas correspondentes, a mesma luz é emitida. Mais uma vez, Henrique opina, como Einstein e Bohm, que isso está previamente programado, embora escondido, uma vez que as tampas estão, inicialmente, fechadas.

Passa, então, pela cabeça de Jocelyn a seguinte idéia: até agora só foi verificado o que acontece quando os dois, após escolher a caixa, abrem a mesma tampa. Que tal fazer um experimento escolhendo aleatoriamente a tampa de cada caixa?

Com seu brilhante raciocínio sobre combinatória e probabilidades, o agente Jocelyn propôs: para cada caixa, escolher a tampa de maneira aleatória em Florianópolis e Campos de Jordão, abrir e anotar o resultado. Caso o agente Henrique esteja certo, a mesma cor será obtida em mais de 50% das vezes. Caso contrário, Henrique está errado.

O argumento não é complicado: seja uma caixa com as cores azul, azul, vermelho nas tampas de cima (1), lateral (2) e de frente (3). Supondo que os agentes abram as tampas aleatoriamente, as combinações da Tabela 1 podem ocorrer.

Tabela 1 - Escolhas possíveis de abertura das tampas.

	Jocelyn	Henrique
Tampa	1	1
Tampa	1	2
Tampa	1	3
Tampa	2	1
Tampa	2	2
Tampa	2	3
Tampa	3	1
Tampa	3	2
Tampa	3	3

Pode-se observar da tabela 1 que o resultado indicará a mesma cor nos casos das tampas (1,1); (1,2); (2,1); (2,2) e (3,3), isto é, em mais de 50% dos casos.

Esse tipo de raciocínio permitiu a John Bell [6] propor, em 1964 [14], um experimento, acompanhado de uma desigualdade. Caso o resultado do experimento fosse de acordo com a desigualdade, a mecânica quântica seria incompleta para descrever a realidade física. Caso contrário, descreveria de maneira completa e satisfatória os fenômenos de natureza microscópica.

O experimento, entretanto, é de difícil implementação, tendo sido realizado pela primeira vez por Alain Aspect, em 1982 [15], contradizendo Einstein e validando a mecânica quântica, confirmando a não localidade e o entrelaçamento (*entanglement*) entre os estados de diferentes partículas.

6. Produto tensorial e entrelaçamento

Um conceito necessário para a formulação do conceito de entrelaçamento é o de produto tensorial. De maneira simplificada, ao se considerar duas matrizes $A : m\,x\,n$ e $B : p\,x\,q$, o produto tensorial $A \otimes B$ é expresso pela matriz

$$A \bigotimes B = \begin{bmatrix} a_{11}B & a_{12}B & ... & a_{1n}B \\ a_{21}B & a_{22}B & ... & a_{2n}B \\ ... & ... & ... & ... \\ a_{m1}B & a_{m2}B & ... & a_{mn}B \end{bmatrix},$$

de dimensões $mp\,x\,nq$.

Assim, sejam o espaço de Hilbert H_1^n, em que $E_1 = \{|\phi_1^1>, |\phi_2^1>, ...|\phi_n^1>\}$ é uma base e H_2^n, em que $E_2 = \{|\phi_1^2>, |\phi_2^2>, ...|\phi_n^2>\}$ é uma base. Os produtos tensoriais ordenados dos vetores $|\phi_i^1> \otimes |\phi_i^2>$ têm dimensão n^2 e geram o espaço de Hilbert $H_1^n \otimes H_2^n$, de dimensão n^2.

Isto é, considerando $|\Phi>= \sum_1^n \alpha_i|i>$ e $|\Psi>= \sum_1^n \beta_j|j>$, o produto tensorial entre eles é dado por

$$|\Phi> \bigotimes |\Psi>= \sum_{i,j} \alpha_i\beta_j|i> \bigotimes |j>. \qquad (8)$$

De maneira simplificada, os produtos tensoriais serão aqui representados por: $|\Phi> \otimes |\Psi>= |\Phi> |\Psi>= |\Phi\Psi>$.

A definição de produto tensorial permite conceituar *entanglement* da seguinte maneira: um estado $|\Psi> \in$

$H_1^n \otimes H_2^n$ é decomponível se existirem $|\Psi_1 > \in H_1^n$ e $|\Psi_2 > \in H_2^n$ tais que: $|\Psi >= |\Psi_1 > \otimes |\Psi_2 >$, caso contrário, trata-se de um estado entrelaçado.

Por exemplo, com uma verifição algébrica simples, nota-se que é impossível representar o chamado estado de Bell, $|\Phi^+ >= \frac{1}{\sqrt{2}}(|00 > +|11 >)$ que pertence a H^{2x2} como produto tensorial de $|\Phi >= \alpha|0 > +\beta|1 > \in H^2$ por $|\Psi >= \gamma|0 > +\delta|1 > \in H^2$. Isto é, que o estado de Bell é entrelaçado.

Para ilustrar as aplicações dos conceitos até aqui apresentados, isto é: representação de estados em espaços de Hilbert, teorema da impossibilidade de cópia e entrelaçamento, três casos práticos serão discutidos na sessão seguinte: criptografia quântica, codificação densa e teletransporte.

7. Aplicações

Antes de apresentar as aplicações algumas idéias precisam ser completadas e alguma notação deve ser estabelecida. Iniciando pela representação de estados em H^2 (qubits) que podem ser representados como combinações lineares da base canônica, $\{H_1 : |0 >; |1 >\}$ ou como combinação linear de quaisquer dois vetores linearmente independentes, como, por exemplo, a chamada base de Hadamard [8], constituída pelos vetores $\{H_2 : |+ >= \frac{1}{\sqrt{2}}(|0 > +|1 >); |- >= \frac{1}{\sqrt{2}}(|0 > -|1 >)\}$.

Também será necessário definir os estados de Bell [4], que servem como bons exemplos de estados entrelaçados

- $|\Phi^+ >= \frac{1}{\sqrt{2}}(|00 > +|11 >)$; $|\Phi^- >= \frac{1}{\sqrt{2}}(|00 > -|11 >)$;
- $|\Psi^+ >= \frac{1}{\sqrt{2}}(|01 > +|10 >)$; $|\Psi^- >= \frac{1}{\sqrt{2}}(|01 > -|10 >)$.

Há, em complemento, as matrizes de Pauli, que podem ser definidas em termos de "kets" e "bras" como

- $\sigma_1 = |1 >< 0| + |0 >< 1|$;
- $\sigma_2 = i|1 >< 0| - i|0 >< 1|$;
- $\sigma_3 = |0 >< 0| - |1 >< 1|$,

sendo possível demostrar a validade das igualdades expressas pelas operaçõesunitárias:

- $(\sigma_1 \otimes I)(|\Phi^+) = |\Psi^+ >$; $(\sigma_1 \otimes I)(|\Phi^-) = |\Psi^- >$;
- $(\sigma_1 \otimes I)(|\Psi^+) = |\Phi^+ >$; $(\sigma_1 \otimes I)(|\Psi^-) = |\Phi^- >$;
- $(\sigma_3 \otimes I)(|\Phi^+) = |\Phi^- >$; $(\sigma_1 \otimes I)(|\Phi^-) = |\Phi^+ >$;
- $(\sigma_3 \otimes I)(|\Psi^+) = |\Psi^- >$; $(\sigma_1 \otimes I)(|\Psi^-) = |\Psi^+ >$,

sendo o efeito de σ_2 igual ao efeito do produto de σ_1 por σ_3.

7.1. Criptografia quântica

Como se espera, nossos detetives Jocelyn e Henrique conhecem a teoria de codificação, sendo habituados com os modelos clássicos de detecção e prevenção de intrusões em mecanismos usuais de comunicação. Esses procedimentos de segurança são fundamentados na existência de duas chaves: uma pública, distribuída para todos os usuários de um certo sistema, e uma privada, compartilhada, apenas com um usuário específico. Assim, quando Jocelyn manda de Florianópolis uma mensagem para Henrique, em Campos de Jordão, o sistema de criptografia executa um algoritmo de modificação da chave pública pela chave privada, identificável apenas por Henrique.

Hilda Friday, uma menina mimada acostumada a ter todas suas vontades satisfeitas, interessada nas investigações sobre o mafioso Sobrino Fredo, contratou um matemático do mal, chamado Half Romeo que desenvolveu algoritmos bastante trabalhosos, mas capazes de violar as chaves privadas, embora a um altíssimo custo computacional. Entretanto, dinheiro não é problema para Hilda, herdeira de um império de produção de papéis. Jocelyn, sempre perspicaz e com trânsito no mundo da matemática, percebeu, então, que suas informações secretas sobre Fredo, vitais para a segurança nacional, poderiam ser violadas por uma criança com dinheiro e um cientista mal intencionado.

Saindo da ficção, está demonstrado que os algoritmos clássicos de criptografia, embora bastante seguros, apresentam uma certa possibilidade de serem violados. A troca de dados usando estados quânticos, considerando-se as condições impostas pelo teorema da impossibilidade de cópia, são mais seguras, pois as intrusões podem ser detectadas de maneira mais eficiente.

O primeiro protocolo de criptografia quântica foi desenvolvido por Bennet e Brassard, em 1984, sendo denominado *BB84 protocol* [4] que se fundamenta na representação do bit x_i, a ser enviado de Jocelyn para Henrique, pelo qubit $|\Psi_i >$ na base canônica H_1 ou na base de Hadamard H_2, escolhida com distribuição de probabilidade uniforme. Hilda, ao violar a comunicação e escolher uma base para a leitura dos dados, faz com que o estado $|\Psi_i >$ colapse para o estado errado em 50% dos casos, proporcionando a detecçãoda intrusão.

A primeira ação do protocolo *BB84* é a escolha, por Jocelyn, de uma sequência aleatória de dados, $x_1, x_2, ..., x_n$, a ser enviada para Henrique. A título de exemplo, a sequência da Tabela 2 pode ser considerada.

Tabela 2 - Exemplo de sequência para o algoritmo BB84.

Bit	x_1	x_2	x_3	x_4
Valor	0	1	1	0

Para prevenir intrusões, Jocelyn representa o bit x_i, a ser enviado para Henrique, pelo qubit $|\Psi_i >$ na base canônica H_1 ou na base de Hadamard H_2, escolhida com distribuição de probabilidade uniforme, conforme mostra a Tabela 3.

Tabela 3 - Codificação quântica.

Bit	x_1	x_2	x_3	x_4
Valor clássico	0	1	1	0
Base(Jocelyn)	H_1	H_2	H_1	H_2
Codificação	$\|\Psi_1>=\|0>$	$\|\Psi_2>=\|->$	$\|\Psi_3>=\|1>$	$\|\Psi_4>=\|+>$

Ao receber a sequência, Henrique também escolhe uma base, entre H_1 e H_2, com distribuição uniforme de probabilidades, para medir cada qubit codificado $|\Psi_i>$. A Tabela 4 mostra um exemplo dessa escolha.

Tabela 4 - Bases escolhidas por Jocelyn e Henrique.

Bit	x_1	x_2	x_3	x_4
Valor clássico	0	1	1	0
Base(Jocelyn)	H_1	H_2	H_1	H_2
Base(Henrique)	H_2	H_2	H_1	H_1
Concordância	N	S	S	N

Em seguida, Henrique fala com Jocelyn em um canal público sobre os qubits medidos na mesma base, sem se importar que Hilda os ouça. Henrique usa os qubits medidos na mesma base e descarta os outros. No caso do exemplo, Henrique usa os estados $|\Psi_2>$ e $|\Psi_3>$.

Caso Hilda tenha interceptado a comunicação entre Jocelyn e Henrique, tendo feito medidas nos qubits $x_1, x_2, ..., x_n$, para cada qubit que as bases de Jocelyn e Henrique concordam, Hilda tem probabilidade 50% de ter escolhido a base errada. Assim, pela intervenção de Hilda, há uma probabilidade de 50% das medidas concordantes de Jocelyn e Henrique darem resultado errado, uma vez que o efeito da medida executada por Hilda é o colapso do estado.

Assim, Jocelyn e Henrique podem escolher, aleatoriamente, algumas de suas medições em bases concordantes. Se, para um número estatisticamente significativo de testes houver cerca de 50% de erros, a intrusão é detectada, havendo indícios da ação maligna de Hilda e Half.

7.2. Codificação quântica densa

Uma outra aplicação dos conceitos aqui desenvolvidos é a codificação quântica densa, isto é, a maneira de se enviar dois bits clássicos, fazendo uso de um qubit. Voltando aos nossos heróis, como Jocelyn pode mandar dois bits clássicos para Henrique fazendo uso de um qubit.

A idéia inicial é supor que Jocelyn e Henrique compartilhem um estado de Bell, por exemplo $|\Phi^+>$. Assim, o algoritmo pode ser feito em sequência: ao receber o primeiro bit clássico, caso se trate de um 0, Jocelyn não altera seu estado; caso seja um 1, executa sobre $|\Phi^+>$ a operação $(\sigma_1 \otimes I)(|\Phi^+)$ que resulta, conforme já explicado, em $|\Psi^+>$.

Ao final dessa primeira parte, Jocelyn está de posse de $|\Phi^+>$ ou $|\Psi^+>$, quando recebe seu segundo bit clássico. Caso ele seja 0, Jocelyn não altera seu estado; caso seja um 1, executa sobre $|\Phi^+>$ ou sobre $|\Psi^+>$ a operação $(\sigma_3 \otimes I)$ que resulta em $|\Phi^->$ ou $|\Psi^->$, respectivamente. A Tabela 5 resume o estado qubit enviado por Jocelyn a Henrique, a cada dois bits clássicos.

Tabela 5 - Código denso.

Bits clássicos	qubit
00	$\|\Phi^+>$
01	$\|\Phi^->$
10	$\|\Psi^+>$
11	$\|\Psi^->$

Ao comparar o estado que possui com o que recebe, Henrique recebe dois bits clássicos em um qubit.

7.3. Teletransporte

Chega-se, finalmente, ao teletransporte e a imagem do Doutor Spock é inevitável. Será que a realidade, finalmente, alcançou a ficção de maior sucesso no cinema? Ainda não, mas há coisas interessantes acontecendo.

Em teoria quântica da informação, entende-se por teletransporte a possibilidade de transferir de um lugar para o outro um estado quântico deconhecido, pelo envio de dois bits clássicos. Isto é, Jocelyn é capaz de transferir para Henrique um estado quântico $|\Psi>$, desconhecido, caso ambos compartilhem um estado de Bell.

Quando os bits clássicos são mandados sobre o canal, é possível para Jocelyn manter uma cópia do estado original. Entretanto, pelo teorema da impossibilidade de cópia é impossível para Jocelyn copiar o estado desconhecido $|\Psi>$. Ao mandar $|\Psi>$ para Henrique, não há como Jocelyn manter informação sobre o estado. Tudo se passa como se o estado $|\Psi>$ tivesse se transferido de Florianópolis para Campos de Jordão, daí a denominação: teletransporte.

No raciocínio a seguir, serão utilizados índices J e H, indicando o fato de um dado bit ou qubit estar relacionado a Jocelyn ou Henrique, respectivamente. Seja, então, o estado de Bell compartilhado por Jocelyn e Henrique dado por

$$|\Phi^+_{JH}>= \frac{1}{\sqrt{2}}(|0_J>|0_H>+|1_J>|1_H>), \quad (9)$$

e o estado desconhecido $|\Psi>$, de posse de Jocelyn, dado por

$$|\Psi>= \alpha|0>+\beta|1>. \quad (10)$$

Inicialmente, o estado de três qubits é dado por

$$|\Psi_J > |\Phi^+_{JH} >= (\alpha|0_J > +\beta|1_J >)$$

$$\frac{1}{\sqrt{2}}(|0_J > |0_H > +|1_J > |1_H >) =$$

$$\frac{1}{\sqrt{2}}(\alpha|0_J 0_J 0_H > +\alpha|0_J 1_J 1_H > +$$

$$\beta|1_J 0_J 0_H > +\beta|1_J 1_J 1_H >). \quad (11)$$

Um pouco de enfadonho trabalho algébrico permite demonstrar que a expressão (13) pode ser rescrita como

$$|\Psi_J > |\Phi^+_{JH} >= \frac{1}{2}[\,|\Phi^+_{JJ} > (\alpha|0_H > +\beta|1_H >) +$$
$$|\Phi^-_{JJ} > (\alpha|0_H > -\beta|1_H >) +$$
$$|\Psi^+_{JJ} > (\alpha|1_H > +\beta|0_H >) +$$
$$|\Psi^-_{JJ} > (\alpha|1_H > -\beta|0_H >). \quad (12)$$

Na Eq. (14) pode-se observar que o sistema de Jocelyn de dois qubits está expresso como uma combinação dos quatro estados de Bell. Ao medir sua parte do estado, Jocelyn obtém um dos estados de Bell e, usando dois bits clássicos, comunica o resultado para Henrique que pode, então, por uma operação unitária de Pauli, encontrar o estado $|\Psi >$ desejado, procedendo de acordo com a Tabela 6.

Tabela 6 - Teletransporte.

Estado de Bell(Jocelyn)	Estado(Henrique)	Operação de Pauli	Resultado
$\|\Phi^+ >$	$\alpha\|0 > +\beta\|1 >$	I	$\|\Psi >$
$\|\Phi^- >$	$\alpha\|0 > -\beta\|1 >$	σ_3	$\|\Psi >$
$\|\Psi^+ >$	$\alpha\|1 > +\beta\|0 >$	σ_1	$\|\Psi >$
$\|\Psi^- >$	$\alpha\|1 > -\beta\|0 >$	$\sigma_1\sigma_3$	$\|\Psi >$

O exemplo desenvolvido mostra que não houve transporte de informação com velocidade maior que a da luz (paradoxo EPR), uma vez que o teletransporte se deu às custas de dois bits clássicos.

8. Conversa final

Se você leu até aqui, percebeu que este texto pode ser lido e entendido por um estudante de primeiro ano de Engenharia ou de Ciências Exatas, com conhecimentos rudimentares de álgebra linear. Caso você esteja pensando: como implementar um qubit fisicamente? Como enviar um qubit? Como detectar um qubit?; então o objetivo está cumprido.

Já que começou, vá em frente. Há livros muito bons por aí de controle quântico, computação quântica e informação quântica. A engenharia do século XXI o espera.

As referências aqui utilizadas foram as clássicas, entretanto, há vários pesquisadores brasileiros envolvidos em trabalhos na área. A seguir, cito alguns nominalmente, desculpando-me por eventuais omissões:

- Carlile Campos Lavor - UNICAMP;
- Francisco Marcos de Assis - UFCG;
- Ivan dos Santos Oliveira Júnior - CBPF;
- Marcelo de Oliveira Terra Cunha - UFMG;
- Paulo Alberto Nussenzveig - IFUSP;
- Reginaldo Palazzo Junior - FEC-UNICAMP;
- Renato Portugal - LNCC.

Referências

[1] T. Hey, Contemporary Physics **40**, 257 (1999).

[2] R.P. Feynman, *The Feynman Lectures on Computation* (Addison Wesley, Reading, 1996).

[3] G. Jaeger, *Quantum Information: An Overview* (Springer, New York, 2007).

[4] V. Vedral, *Introduction to Quantum Information* (Oxford University Press, Oxford, 2006).

[5] C.E. Shannon and W. Weaver, *The Mathematical Theory of Communication* (Illini Books, Illinois, 1963).

[6] J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 2004), 2nd ed.

[7] E. Kreysig, *Introductory Functional Analysis with Applications* (Wiley, New York, 1978).

[8] M. Hirvensalo, *Quantum Computing* (Springer, Berlin, 2001).

[9] E. Desurvire, *Classical and Quantum Information Theory: An Introduction for the Telecom Scientist* (Cambridge University Press, Cambridge, 2009).

[10] B. Greene *O Tecido do Cosmos* (Companhia das Letras, São Paulo, 2008).

[11] A. Einstein, B.Podolsky and N. Rosen, Physical Review **47**, 777 (1935).

[12] D. Bohm, Physical Review **85**, 166 (1952).

[13] D. Bohm, Physical Review **85**, 180 (1952).

[14] J.S. Bell, Physics I **3**, 195 (1964).

[15] A. Aspect, J. Dalibard and G. Roger, Physical Review Letters **49**, 1804 (1982).