Trabalho de Conclusão de Curso do Bacharelado em Física

Estudos sobre comunicação quântica: distribuição de chaves quânticas e código de acesso aleatório

Aluno: Giovani Pinheiro da Silva
Orientador: Breno Marques Gonçalves Teixeira

Universidade Federal do ABC
Brasil
Maio, 2023

Resumo

Há vários aspectos que diferenciam um sistema clássico e quântico. Essas diferenças podem ser usadas para melhorias em protocolos de comunicação. Nesse trabalho de revisão, estudamos sobre medições em uma parte de um sistema, o paradoxo EPR e desigualdades de Bell e então, estudamos o protocolo BB84, protocolo E91 e por fim o código de acesso aleatório, onde analisamos a codificação clássica, quântica (QRAC) e a quântica assistida por emaranhamento (EARAC).

Abstract

There are several aspects that differentiate a classical and quantum system. These differences can be used for improvements in communication protocols. In this review work, we studied about measurements in a part of a system, the EPR paradox and Bell's inequalities and then, we studied the BB84 protocol, E91 protocol and finally the random access code, where we analyzed the classical, quantum coding (QRAC) and the entanglement-assisted quantum physics (EARAC).

Conteúdo

1 Introdução

Os aspectos que diferenciam sistemas clássicos e sistemas quânticos nos permitem pensar em diferentes aplicações nas últimas décadas. A informação quântica e a comunicação quântica [5] estudam como pode-se usar sistemas quânticos para implementações de processos informacionais. Essa tecnologia não vem para substituir a tecnologia de informação clássica, nossos computadores e internet, mas para abrir novas possibilidades de como manipular a informação. Vários protocolos foram propostos nas últimas décadas, por exemplo: criptografia quântica [2] [3], algoritmo de busca (Gloover) [6], algoritmo de fatoração (Shor) [7] e teleportação [8]. Porém para conseguirmos aplicar uma nova tecnologia é necessário saber quais são os conceitos que fundamentam e explicam o que vemos nos laboratórios. Esses conceitos podem ser fonte de tecnologias ou de limitações que inviabilizem suas aplicações. Nesse contexto, nós estudamos protocolos de comunicação quântica que podem posteriormente serem utilizados como passe para processos mais complexos.

Num primeiro momento focamos nas bases teóricas que seriam necessárias para compreender certos protocolos. Abordamos o emaranhamento quântico e, então, analisei o paradoxo EPR, que colocava em cheque a completeza da Mecânica Quântica e levou a hipótese da existência de variáveis ocultas, algo que poderia ser testado posteriormente devido as desigualdades de Bell, também analisadas neste trabalho.

Por fim, estudamos diferentes protocolos de criptografia quântica. Iniciamos com o BB84, o primeiro protocolo de distribuição de chaves quânticas [2] [3], que assim como outros permite que mensagens sejam encriptografadas em sistemas quânticos.Então abordamos o protocolo E91, que, diferentemente do BB84, usa emaranhamento quântico e uma comunicação clássica entre as partes.

No final do trabalho está contido os nossos estudos sobre o código de acesso aleatório [9] [10], onde uma mensagem de tamanho m é codificada em outra de tamanho n, onde um receptor da mensagem codificada é capaz de adivinhar qualquer um dos bits da mensagem original com probabilidade p. Abordamos a codificação clássica, que não envolve Física Quântica, a quântica e também a quântica assistida por emaranhamento, mostrando que a clássica é a codificação com a menor probabilidade de acerto.

2 Medidas em uma parte do sistema

2.1 Predições físicas

Considere um sistema composto por duas partes, (1) e (2). Sendo $\mathscr{E}_1$ e $\mathscr{E}_2$ os espaços de estados de tais partes do sistema, o espaço de estados do sistema composto por ambas as partes será $\mathscr{E} = \mathscr{E}_1 \otimes \mathscr{E}_2$. Sendo A_1 um observável que age em (1), $\tilde{A}_1$ é a sua extensão que age no sistema composto, correspondendo então a medidas referentes somente a uma das partes do mesmo, ou seja:

$$\tilde{A}_1 = A_1 \otimes \mathbb{1}_2 \tag{1}$$

onde $\mathbb{1}_2$ é o operador identidade em $\mathscr{E}_2$. Peguemos agora um autovalor a_n de A_1, com grau de degenerescência g_n. O conjunto de g_n kets ortonormais $\{|u_n^i\rangle_1\}$, forma o autoespaço associado a a_n. Logo, o projetor P_{n1} para tal espaço é:

$$P_{n1} = \sum_{i=1}^{g_n} |u_n^i\rangle_1 \langle u_n^i|_1 \tag{2}$$

A extensão $\tilde{P}_{n1}$, que age em $\mathscr{E}_1 \otimes \mathscr{E}_2$, será, assim como foi no caso de $\tilde{A}_1$, o produto tensorial de P_{n1} pelo operador identidade de $\mathbb{1}_2$:

$$\tilde{P}_{n1} = P_{n1} \otimes \mathbb{1}_2 \tag{3}$$

Com tais operadores é possível, ao se possuir um estado normalizado $|\Psi\rangle$, calcular a probabilidade $\mathscr{P}^{(1)}(a_n)$ de encontrar o autovalor a_n ao se medir A_1. Para isso basta calcular o valor esperado de $\tilde{P}_{n1}$:

$$\mathscr{P}^{(1)}(a_n) = \langle\Psi| \tilde{P}_{n1} |\Psi\rangle \tag{4}$$

Com a relação de fechamento, é possível escrever o operador identidade da segunda parte do sistema da seguinte maneira:

$$\mathbb{1}_2 = \sum_k |v_k^i\rangle_2 \langle v_k^i|_2 \tag{5}$$

onde $\{|v_k\rangle_2\}$ é uma base ortonormal de $\mathscr{E}_2$.

Após a medição de $\tilde{A}_1$ e da obtenção de um autovalor a_n no sistema em um estado arbitrário $|\Psi\rangle$, o estado imediatamente após a medida, $|\Psi'\rangle$, será a projeção normalizada de $|\Psi\rangle$ no autoespaço associado a a_n, ou seja:

$$|\Psi'\rangle = \frac{\tilde{P}_{n1}\,|\Psi\rangle}{\sqrt{\langle\Psi|\,\tilde{P}_{n1}\,|\Psi\rangle}}$$

$$|\Psi'\rangle = \frac{(P_{n1}\otimes \mathbb{1}_2)\,|\Psi\rangle}{\sqrt{\langle\Psi|\,(P_{n1}\otimes \mathbb{1}_2)\,|\Psi\rangle}} \tag{6}$$

Na equação anterior e na eq. (4), a única relação delas com a base escolhida para $\mathscr{E}_2$ é obtida ao se utilizar a relação de fechamento na eq. (5). Com isso é possível notar que tanto as predições probabilísticas da medição de A_1 da parte (1) do sistema quanto o estado imediatamente após tal medida, independem da base $\{|v_k\rangle_2\}$ escolhida. Por fim, utilizando a eq. (5) e a eq. (2), é possível expressar o estado imediatamente após a medida de uma maneira mais geral, da seguinte forma:

$$|\Psi'\rangle = \frac{\sum_{i=1}^{g_n}\sum_k |u_n^i\rangle_1\,|v_k\rangle_2\,\langle u_n^i|_1\,\langle v_k|_2\,|\Psi\rangle}{\sqrt{\langle\Psi|\sum_{i=1}^{g_n}\sum_k |u_n^i\rangle_1\,|v_k\rangle_2\,\langle u_n^i|_1\,\langle v_k|_2\,|\Psi\rangle}}$$

$$|\Psi'\rangle = \frac{\sum_{i=1}^{g_n}\sum_k |u_n^i\rangle_1\,|v_k\rangle_2\,\langle u_n^i|_1\,\langle v_k|_2\,|\Psi\rangle}{\sqrt{\sum_{i=1}^{g_n}\sum_k |\,\langle u_n^i|_1\,\langle v_k|_2\,|\Psi\rangle\,|^2}} \tag{7}$$

2.1.1 Estados separáveis e estados emaranhados

Agora suponhamos que o estado $|\Psi\rangle$ da eq. (4) é o produto tensorial entre dois kets normalizados e pertencentes, cada um, a (1) e (2):

$$|\Psi\rangle = |\phi\rangle_1 \otimes |\chi\rangle_2 \equiv |\phi\rangle_1\,|\chi\rangle_2 \tag{8}$$

Dessa forma, com as eq. (4) e a eq. (3) temos:

$$\mathscr{P}^{(1)}(a_n) = \langle\phi|_1\,\langle\chi|_2\,(\tilde{P}_{n1})\,|\phi\rangle_1\,|\chi\rangle_2$$
$$\mathscr{P}^{(1)}(a_n) = \langle\phi|_1\,\langle\chi|_2\,(P_{n1}\otimes \mathbb{1}(2))\,|\phi\rangle_1\,|\chi\rangle_2$$
$$\mathscr{P}^{(1)}(a_n) = \langle\phi|_1\,P_{n1}\,|\phi\rangle_1\,\langle\chi|_2\,|\chi\rangle_2$$

Como $|\chi\rangle_2$ é normalizado, encontramos que:

$$\mathscr{P}^{(1)}(a_n) = \langle\phi|_1\,P_{n1}\,|\phi\rangle_1 \tag{9}$$

Note que a eq. (9) não contém nada referente a parte (2) do sistema. Sendo assim, quando o estado do sistema global pode ser representado como na eq. (8), as predições físicas referentes a somente uma das partes, não terá nenhuma influência da outra parte do sistema. No exemplo acima, o cálculo de probabilidade de se obter um autovalor referente a parte (1) do sistema não dependeu em nada de $|\chi\rangle_2$. Em casos assim, o estado pode ser considerado meramente como uma justaposição entre os estados pertencentes cada qual a uma das partes, sendo chamados de estados separáveis.

No entanto, nem sempre o estado do sistema global pode ser expresso como na eq. (8). Tais estados que não podem ser expressos como o produto tensorial entre um estado pertencente à uma das partes por outro pertencente à outra parte, são chamados de estados emaranhados.

3 Paradoxo EPR

Einstein, Podolsky e Rosen, em 1935 publicaram um trabalho onde concluíam que a Mecânica Quântica era um teoria incompleta [11]. A ideia de EPR foi considerar duas partículas correlacionadas, de tal forma que a medida direta de uma delas acarretaria numa medida indireta da outra, devido ao postulado da projeção contido no formalismo da mecânica quântica. No entanto isso entrava em contradição com o princípio da localidade, que era aceito intuitivamente na época. A seguir as hipóteses foram analisadas mais detalhadamente.

3.1 Completeza, elementos de realidade e localidade

No artigo de EPR, uma condição necessária para que uma teoria seja considerada completa, a chamada condição de completeza, diz que "todo elemento da realidade física, deve ter uma contrapartida na teoria física" [11]. Para demonstrar que a Mecânica Quântica é incompleta, EPR busca mostrar um elemento de realidade que não tem contrapartida na teoria [1].

Um elemento de realidade por sua vez, existe quando é possível predizer com probabilidade um o resultado de uma medição de uma quantidade física, sendo que o elemento será correspondente a tal quantidade. Sendo assim, se um determinado sistema está num autoestado de um observável, tal estado corresponde a um elemento de realidade [12], visto que uma medição resultara com probabilidade um no autovalor correspondente.

A condição descrita para a existência de um elemento de realidade é suficiente, e não necessária, para a existência de um elemento de realidade, não significando portanto que todos os elementos de realidade possuam valores que possam ser previstos.

Uma terceira definição importante é a de localidade, um princípio que diz que elementos de realidade de um sistema não podem ser afetados por medições realizadas à distância, em um outro sistema. Para Einstein, "à distância" significa que se um raio de luz é emitido por um dos eventos, não atingirá o outro sistema antes do outro evento acontecer [12].

3.2 O estado emaranhado

O estado das partículas utilizadas por EPR é um estado emaranhado, de tal forma que a soma dos momentos p_{x1} e p_{x2} é zero e que estejam distanciadas num valor l, ou seja, $x_1 - x_2 = l$. Uma proposta de como criar tal estado é a seguinte (mostrado na fig. 1): duas partículas, se deslocando na direção x, são incididas perpendicularmente a um diafragma que possui duas fendas paralelas, na direção y. O diafragma fica suspenso por uma mola e um medidor M verifica qual é o momento transferido para ele pelas partículas, sendo que o estado desejado sera adquirido quando esse momento for zero.

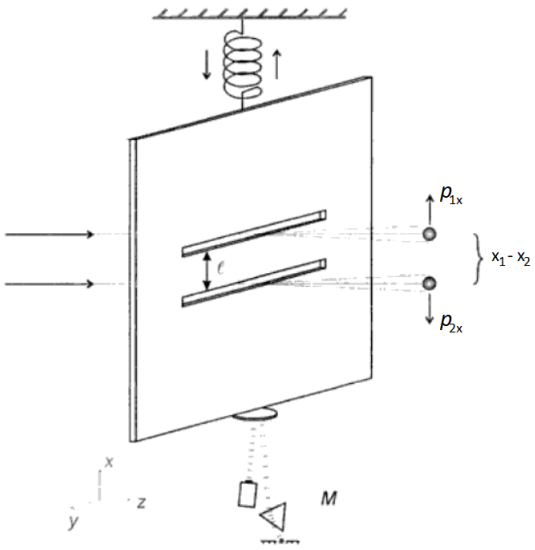

Figura 1: Preparação do estado emaranhado de EPR [12].

Em tal estado, não se sabe com precisão nem a posição nem o momento de nenhuma das partículas, mas caso se meça por exemplo a posição da primeira partícula, obtendo-se um valor x', o estado se reduzirá e a posição da segunda partícula será $x' - l$. Por outro lado caso se meça o momento da primeira partícula, obtendo-se p', o estado se reduzirá de tal forma que o momento da segunda será $-p'$.

Segundo o princípio de localidade anteriormente descrito, o ato de medir tanto a posição ou o momento de uma das partículas não pode alterar nenhum elemento de realidade na outra partícula num tempo menor do que l/c contado a partir do instante da medição. No caso em que se mede a posição da primeira, é possível, como foi descrito para este caso, predizer com probabilidade 1 qual será a posição da segunda partícula caso eu a meça, inclusive caso eu faça essa segunda medição num tempo menor do que l/c (contado a partir do instante em que a primeira foi realizada), sendo assim, existe um elemento de realidade correspondendo a posição da segunda partícula no momento da medição da sua posição. Além disso também é possível predizer com probabilidade 1 o momento da segunda partícula após o da

primeira ter sido medido, também num tempo menor do que l/c, o que novamente leva à conclusão de que existe um elemento de realidade, dessa vez correspondendo ao momento da segunda partícula, no momento da sua medição.

Com a descrição dada acima é possível notar que aparentemente a segunda partícula tem tanto um elemento de realidade que corresponde ao momento quanto um que corresponde à posição, simultaneamente, porém, isso não tem contrapartida na Mecânica Quântica, visto que R e P não comutam. Sendo assim, segundo EPR, a Mecânica Quântica é uma teoria incompleta, já que viola a condição de completeza.

3.3 Argumento da incompleteza com Spins

Outra forma de expor a ideia de EPR é utilizando o estado de singleto:

$$|\Psi_S\rangle = \frac{1}{\sqrt{2}}[\ |1\rangle_1 |0\rangle_2 - |0\rangle_1 |1\rangle_2\ ] \tag{10}$$

Em tal estado, que é não separável, caso se meça σ_{z1}, utilizando por exemplo um aparelho de Stern-Gerlach, e se obtenha o autovalor -1, o estado da eq. (10) se reduzirá para:

$$|\Psi_F\rangle = |1\rangle_1 |0\rangle_2$$

Em tal estado, caso se meça σ_{z2}, se obterá com certeza o autovalor 1. Da mesma forma, caso, ao medir σ_{z1} quando o sistema está no estado da eq. (10) se obtenha o autovalor 1, uma medição de σ_{z2} resultará certamente em -1.

Uma propriedade interessante do estado de singleto é a invariância rotacional. Caso se queira saber as probabilidades de obtenção dos autovalores de σ_x por exemplo, devemos expandir o estado da eq. (10) na base $\{|0_x\rangle\,;|1_x\rangle\}$. Fazendo isso obtemos o seguinte estado:

$$|\Psi_S\rangle = \frac{1}{\sqrt{2}}(\ |1_x\rangle_1 |0_x\rangle_2 - |0_x\rangle_1 |1_x\rangle_2\ ) \tag{11}$$

que possui a mesma forma que a eq. (10).

Supondo que o estado da eq. (10) seja gerado e que ambas as partículas se afastem, o argumento segue de maneira similar a descrita anteriormente. Caso se meça σ_{z1}, o resultado de uma medição de σ_{z2} só poderia resultar no valor oposto ao que foi obtido na medição da primeira, possuindo portanto um elemento de realidade que corresponde ao autovalor de σ_{z2}. Da mesma maneira, se σ_{x1} seja medido, a segunda partícula possuirá um elemento de realidade correspondendo ao autovalor de σ_{x2}. No entanto, segundo o princípio da localidade, uma medição em uma dessas partículas não poderia alterar nenhum elemento de realidade da outra instantaneamente ou numa velocidade mais rápida do que a da luz, o que leva a conclusão de que a segunda partícula possuía simultaneamente elementos de realidade correspondentes a dois operadores que não comutam (σ_z e σ_x), algo que não possui contrapartida na teoria, violando assim a condição de completeza.

3.4 Versão de Redhead para a incompleteza [1]

Supondo que ambas as partículas estão no estado de singleto da eq. (10) e que cada uma delas esteja separada uma da outra numa distância l. Em tal situação, é realizada uma medida de σ_{z1} no instante t_1. Com isso, da mesma maneira como foi descrito anteriormente, a segunda partícula possuirá um elemento de realidade correspondente ao autovalor de σ_{z2} (que terá o valor oposto ao que se obteve na medida de σ_{z1}) para tempos $t_2 \geq t_1$.

No entanto, utilizando o princípio de localidade, pode-se concluir que não foi a medida de de σ_{z1} que fez com que a segunda partícula viesse a ter tal elemento de realidade, sendo assim, ela já o possuía em um tempo $t < t_1$, por exemplo, imediatamente antes da medida de σ_{z1}.

O suposto paradoxo, nesse cenário, vem do fato que imediatamente antes da medição de σ_{z1} o sistema estava no estado de singleto, o que faz com que a segunda partícula não possa estar num autoestado de σ_{z2}, algo que entra em conflito com a existência de um elemento de realidade para um tempo $t < t_1$.

3.5 Contradição com a Mecânica Quântica

Até o momento expusemos a argumentação de EPR para a incompleteza da MQ, agora analisaremos os pontos nos quais eles estavam errados.

Seguindo a lógica de EPR, foi dito que após Alice medir o singleto, o estado passava a ser $|1\rangle_1 |0\rangle_2$, no caso do resultado obtido ser -1, porém, esse é o estado somente para Alice. Este seria o estado para Bob, antes de ele realizar alguma medida, no caso da Alice informar o Bob sobre a medida dela. O máximo que pode ser dito é que tendo a Alice

medido a sua parte do sistema, ela sabe qual será o resultado da medida de Bob, caso ele venha a realizar a medição na mesma direção que ela, no entanto, ela só poderá saber o que Bob fez depois que ele a informar.

Outro detalhe importante na dedução de EPR é que, segundo eles, o fato de a Alice poder saber qual será o resultado da medida de Bob numa situação específica, implicaria que a parte de Bob já teria um valor predefinido de spin, mas, medidas não realizadas não possuem resultado, ou seja, as partículas não tem valores específicos de spin até que sejam feitas medidas.

Com o que foi mostrado aqui é possível entender porque, ao contrário do que pode parecer num primeiro contato com o paradoxo EPR, o emaranhamento quântico não possibilita uma comunicação superluminal. Apesar de Alice poder saber qual virá a ser o resultado de Bob, ela não sabia qual seria o seu próprio resultado antes de realizar a medida, não podendo assim "forçar"algum resultado desejado na medição de Bob.

4 Desigualdade de Bell

Para uma Teoria de Variável oculta (TVO), o estado $|\Psi\rangle$ de uma partícula é uma descrição incompleta, existindo variáveis λ que são necessárias para torná-la completa. Segundo uma TVO, ao se especificar o estado $|\Psi\rangle$ e as variáveis λ, a medição de um observável A teria um único resultado predizível (não probabilístico). O valor que é obtido ao se medir A será denotado por a $a^{|\Psi\rangle}(\lambda)$. Neste cenário o valor esperado $\langle A\rangle$ é uma média ponderada dos valores de $a^{|\Psi\rangle}(\lambda)$ sobre uma distribuição $\rho_\Psi(\lambda)$ das variáveis ocultas.

$$\langle\Psi|A|\Psi\rangle = \int a^{|\Psi\rangle}(\lambda)\rho_\Psi(\lambda)d\lambda \tag{12}$$

Uma maneira de testar uma TVO é comparando suas previsões médias com as da MQ. As desigualdades de Bell impõem restrições aos valores médios previstos por TVO's.

4.1 Probabilidades e Correlações

Suponha que um estado de singleto, mostrado na eq. (10), onde a partícula 1 passará por um analisador de Stern-Gerlach orientado na direção $\vec{a}$ e a 2 por um orientado na direção $\vec{b}$. Neste cenário, segundo uma TVO, caso fosse possível saber os valores λ das variáveis ocultas, seríamos capazes de saber o resultado antes de realizar o experimento.

Uma maneira de calcular as desigualdades de Bell para este caso é utilizando o coeficiente de correlação $c_\Psi(\vec{a},\vec{b})$, sendo que tal coeficiente representa uma relação estatística entre duas variáveis, que varia de -1 até 1, como mostrarei a seguir. Caso o resultado esteja entre 0 e 1, o aumento de uma variável tende a significar um aumento da outra variável. Caso o coeficiente esteja entre -1 e 0, ao se aumentar uma das variáveis, a outra diminui. Neste caso as variáveis em questão serão os resultados das medições de σ_{a1} e σ_{b2}, ou seja, spins.

Sendo assim, neste caso, maior será o fator de correlação quanto mais vezes as medidas dos spins resultarem no mesmo valor, alcançando 1 caso sempre coincidam; e menor ele será quanto mais vezes eles sejam opostos, sendo -1 caso nunca coincidam.

Para fazer tal cálculo, comecemos pela expressão da correlação, onde A e B denotarão grandezas físicas a serem medidas, enquanto a e b denotarão os valores obtidos nas medições. Ela é definida como a covariância entre duas variáveis aleatórias, dividida pela multiplicação dos desvios padrões de cada uma dessas variáveis, ou seja:

$$c(a,b) = \frac{Cov(a,b)}{\sqrt{Var(a)Var(b)}} \tag{13}$$

A covariância por si só, quando positiva, indica que o aumento de uma variável implica numa maior probabilidade de aumento da outra. No caso dela ser negativa, é o contrário, porém, ela possui os inconvenientes de depender das unidades das variáveis e de o seu valor absoluto não informar facilmente o quão fortemente as variáveis estão correlacionadas. Ao dividir tal covariância pela multiplicação dos desvios padrões, o resultado estará entre -1 e 1. Para mostrar isso, comecemos pela seguinte expressão:

$$Var\left(\frac{a}{\Delta a} \pm \frac{b}{\Delta b}\right) \tag{14}$$

Tal expressão é maior ou igual a zero, já que a variância sempre é. Desenvolvendo a expressão:

$$Var\left(\frac{a}{\Delta a} \pm \frac{b}{\Delta b}\right) = \frac{Var(a)}{\Delta a^2} + \frac{Var(b)}{\Delta b^2} \pm \frac{2}{\Delta a \Delta b} Cov(a,b)$$
$$Var\left(\frac{a}{\Delta a} \pm \frac{b}{\Delta b}\right) = 1 + 1 \pm 2c(a,b)$$

Como dito anteriormente, a variância é maior ou igual a zero, então

$$0 \leq 2 \pm 2c(a,b) \Rightarrow -1 \leq c(a,b) \leq 1 \tag{15}$$

Tendo demonstrado o intervalo em que se encontra a correlação, desenvolvamos ela para uma forma que será mais útil para o problema que estamos abordando:

$$c(a,b) = \frac{\langle (a - \langle a \rangle)(b - \langle b \rangle) \rangle}{\Delta a \Delta b}$$
$$c(a,b) = \frac{\langle ab - a\langle b \rangle - b\langle a \rangle + \langle a \rangle \langle b \rangle \rangle}{\Delta a \Delta b}$$
$$c(a,b) = \frac{\langle ab \rangle - \langle a\langle b \rangle \rangle - \langle b\langle a \rangle \rangle + \langle a \rangle \langle b \rangle}{\Delta a \Delta b}$$

Agora, dado que $\langle a \rangle$ e $\langle b \rangle$ podem sair dos brakets por serem constantes, é possível chegar na expressão final:

$$c(a,b) = \frac{\langle ab \rangle - \langle a \rangle \langle b \rangle}{\Delta a \Delta b} \tag{16}$$

Como foi dito anteriormente, a grandeza física em questão será o spin, portanto $A \equiv \sigma_{a1}$ e $B \equiv \sigma_{b2}$. Para chegar na expressão final antes de se calcular a correlação, também é necessário notar que no estado da eq. (10) a probabilidade de se obter um spin para cima e para baixo (ao longo de seus respectivos eixos) são iguais, logo $\langle \sigma_{a1} \rangle = \langle \sigma_{b2} \rangle = 0$, o que por sua vez leva a $\Delta\sigma_{a1} = \Delta\sigma_{b2} = \sqrt{\langle {\sigma_{a1}}^2 \rangle - \langle \sigma_{a1} \rangle^2} = \sqrt{\langle \Delta{\sigma_{a1}}^2 \rangle} = 1$.

Por fim, utilizando tais informações se obtém que:

$$c(a,b) = \langle \Psi_S | \, \sigma_{a1}\sigma_{b2} \, | \Psi_S \rangle \tag{17}$$

É possível ver que a correlação é a média do operador $\sigma_{a1}\sigma_{b2}$. Existem 4 possibilidades a se considerar, ambos medem spin $+1$; ambos medem spin -1; Alice (parte 1 do sistema) mede $+1$ e Bob (parte 2 do sistema) mede -1; e por fim a possibilidade em que Alice mede -1 e Bob $+1$. O valor médio do observável será a soma dos autovalores multiplicados por suas respectivas probabilidades, ou seja:

$$c(a,b) = 1(\mathscr{P}_{++} + \mathscr{P}_{--}) - 1(\mathscr{P}_{+-} + \mathscr{P}_{-+}) \tag{18}$$

Onde o 1 e o -1 na frente dos parenteses são os autovalores do observável.

A primeira coisa que pode ser feita para simplificar o cálculo é observar que por simetria, $\mathscr{P}_{++} = \mathscr{P}_{--}$ e $\mathscr{P}_{+-} = \mathscr{P}_{-+}$, sendo assim:

$$c(a,b) = 2(\mathscr{P}_{--} - \mathscr{P}_{-+}) \tag{19}$$

Comecemos com o caso em que ambos medem o spin para baixo. A direção que escolherei para $\hat{a}$ para facilitar os cálculos será $\hat{z}$. A probabilidade será a probabilidade da Alice medir o spin para baixo e de Bob encontrar esse mesmo resultado dado que Alice já o obteve primeiro. Para o estado de singleto a probabilidade de Alice medir spin para baixo é $1/2$ e após tal medição o estado colapsa para:

$$|\Psi\rangle' = |0_a\rangle_1 \, |1_a\rangle_2 \tag{20}$$

Agora para encontrar a probabilidade condicional, devo expressar os autoestados de σ_a em termos do de σ_b. Como estou considerando que a direção $\hat{a}$ é $\hat{z}$, os autoestados de σ_b em função de σ_a tem a mesma forma que os autoestados de uma matriz de Pauli com direção arbitrária $\hat{n}$ (tal cálculo está feito no apêndice A), sendo assim:

$$|1_b\rangle = \cos\left(\frac{\theta}{2}\right) |1_a\rangle + e^{i\phi} sen\left(\frac{\theta}{2}\right) |0_a\rangle \tag{21}$$

$$|0_b\rangle = -e^{-i\phi} sen\left(\frac{\theta}{2}\right)|1_a\rangle + cos\left(\frac{\theta}{2}\right)|0_a\rangle \tag{22}$$

Disso se segue que:

$$|1_a\rangle = \cos\left(\frac{\theta}{2}\right)|1_b\rangle - e^{i\phi} sen\left(\frac{\theta}{2}\right)|0_b\rangle \tag{23}$$

$$|0_a\rangle = e^{-i\phi} sen\left(\frac{\theta}{2}\right)|1_b\rangle + cos\left(\frac{\theta}{2}\right)|0_b\rangle \tag{24}$$

Reescrevendo a eq. (20):

$$|\Psi\rangle' = |0_a\rangle_1 \left[\cos\left(\frac{\theta}{2}\right)|1_b\rangle_2 - e^{i\phi} sen\left(\frac{\theta}{2}\right)|0_b\rangle_2\right] \tag{25}$$

Pode-se por fim encontrar a probabilidade de ambos medirem spin para baixo:

$$\mathscr{P}_{--} = \frac{1}{2} sen^2\left(\frac{\theta}{2}\right) = \frac{1}{4}(1 - cos\ \theta) \tag{26}$$

Agora calculemos P_{-+}. Para Alice medir spin para baixo a probabilidade é 1/2, como foi dito anteriormente, então o singleto colapsa para o estado da eq. (25). Olhando para tal estado é possível notar que a probabilidade de Bob medir spin para cima ao longo do eixo $\hat{b}$ é, $cos^2(\theta/2)$, portanto:

$$\mathscr{P}_{-+} = \frac{1}{2} cos^2\left(\frac{\theta}{2}\right) = \frac{1}{4}(1 + cos\ \theta) \tag{27}$$

Substituindo na eq. (19) os resultados encontrados, obtemos que (considerando que θ é o ângulo entre $\hat{a}$ e $\hat{b}$):

$$c(a,b) = -cos(\theta) = -\hat{a}\cdot\hat{b} \tag{28}$$

Seria de se esperar que a correlação entre duas direções coincidentes (0 graus entre elas) fosse -1, pois os spins sempre são opostos; e de forma semelhante espera-se que a correlação entre direções diametralmente opostas seja 1. Olhando para a expressão final da correlação, é possível ver que ela é condizente com essas considerações.

4.2 Derivação de Bell

Mostrarei a seguir a derivação de Bell, mostrada em seu artigo, "*On The Einstein, Podolsky, Rosen Paradox*" [13], do que veio a ser conhecida como desigualdade de Bell.

Inicialmente, consideremos um estado de singleto, eq. (10), que terá os spins das partículas medidos. A função $I(a,\lambda)$ é o resultado da medição do spin da primeira partícula (medição de σ_{a1}), feito na direção $\vec{a}$, dadas as variáveis ocultas λ, enquanto a função $II(b,\lambda)$ se refere à segunda partícula (medição de σ_{b2}). Sendo assim, tais funções podem assumir os valores ± 1. Sendo o coeficiente de correlação do singleto, as médias dos produtos de $I(a,\lambda)$ e $II(b,\lambda)$, segundo uma TVO, de acordo com a eq. (12), a correlação ficaria sendo:

$$c(a,b) = \int \rho(\lambda) I(a,\lambda) II(b,\lambda) d\lambda \tag{29}$$

Sendo $\rho(\lambda)$ uma distribuição de probabilidade normalizada, temos que:

$$\int \rho(\lambda) d\lambda = 1 \tag{30}$$

Além disso, outra consideração que Bell fez em sua dedução é que, caso a primeira partícula tenha seu spin medido na mesma direção que a segunda, os valores obtidos serão opostos (anti-correlação perfeita):

$$II(b,\lambda) = -I(b,\lambda) \tag{31}$$

Utilizando a eq. (31) no cálculo da correlação da eq. (29), obtém-se que:

$$c(a,b) = -\int \rho(\lambda) I(a,\lambda) I(b,\lambda) d\lambda \tag{32}$$

Agora, sendo $\vec{c}$ uma terceira direção de medida do spin, é possível verificar que:

$$c(a,b) - c(a,c) = -\int \rho(\lambda) I(a,\lambda)[I(b,\lambda) - I(c,\lambda)]d\lambda \tag{33}$$

Para prosseguir com a derivação, utilizarei que $I^2(b,\lambda) = 1$. Multiplicarei a integral por um, utilizando tal informação.

$$c(a,b) - c(a,c) = -\int \rho(\lambda) I(a,\lambda) I^2(b,\lambda)[I(b,\lambda) - I(c,\lambda)]d\lambda$$

$$c(a,b) - c(a,c) = -\int \rho(\lambda) I(a,\lambda) I(b,\lambda)[I^2(b,\lambda) - I(b,\lambda)I(c,\lambda)]d\lambda$$

$$c(a,b) - c(a,c) = -\int \rho(\lambda) I(a,\lambda) I(b,\lambda)[1 - I(b,\lambda)I(c,\lambda)]d\lambda \tag{34}$$

Dentro dos colchetes da expressão anterior, ou o valor resultante da operação é 2 ou é 0, ou seja:

$$[1 - I(b,\lambda)I(c,\lambda)] \geq 0 \tag{35}$$

O módulo do lado direito da eq. (34) atinge um máximo caso, para todos os valores de λ, ou $I(a,\lambda)I(b,\lambda)$ seja sempre 1, ou seja sempre -1. Logo:

$$|c(a,b) - c(a,c)| \leq \int \rho(\lambda)[1 - I(b,\lambda)I(c,\lambda)]d\lambda$$

$$|c(a,b) - c(a,c)| \leq \int \rho(\lambda)d\lambda - \int \rho(\lambda) I(b,\lambda)I(c,\lambda)d\lambda$$

É possível notar que ambas a integrais acima são as mesmas que as da eq. (29) e eq. (30). Então, finalmente, a desigualdade de Bell é:

$$|c(a,b) - c(a,c)| \leq 1 + c(b,c) \tag{36}$$

Com a tal desigualdade em mãos, é possível verificar se ela pode ser violada utilizando o coeficiente de correlação definido pela MQ na eq. (28). Caso seja (mostrarei que esse é o caso), a MQ é incompatível com TVOs locais, ou seja, TVOs que respeitam o princípio de localidade, descrito na seção 3.1.

4.2.1 Violação da Desigualdade de Bell pela MQ

Com desigualdade de Bell, que foi obtida com pressupostos de uma TVO local, podemos verificar se ela pode ser violada para algum caso específico. Caso seja violada para algum caso, TVOs locais são incompatíveis com a MQ, pois a desigualdade foi derivada considerando-se que quaisquer direções de medidas podem ser usadas.

Consideremos que a direção $\hat{a}$ é perpendicular a $\hat{b}$ e que a direção $\hat{c}$ é da seguinte forma:

$$\hat{c} = \hat{a}\sin\phi + \hat{b}\cos\phi \tag{37}$$

Para calcular as correlações na eq. (36), utilizarei a eq. (28). Temos que:

$$|-\hat{a}\cdot\hat{b} + \hat{a}\cdot\hat{c}| \leq 1 + \hat{c}\cdot\hat{b}$$

$$|\sin\phi| \leq 1 - \cos\phi \tag{38}$$

Como é possível ver na fig. 2, a desigualdade de Bell, no intervalo mostrado, só não foi violada em 0 e em π (quando a direção $\hat{c}$ é coincidente ou com $\hat{a}$ ou com $\hat{b}$), portanto, a Mecânica Quântica e Teorias de Variáveis Ocultas locais, são incompatíveis.

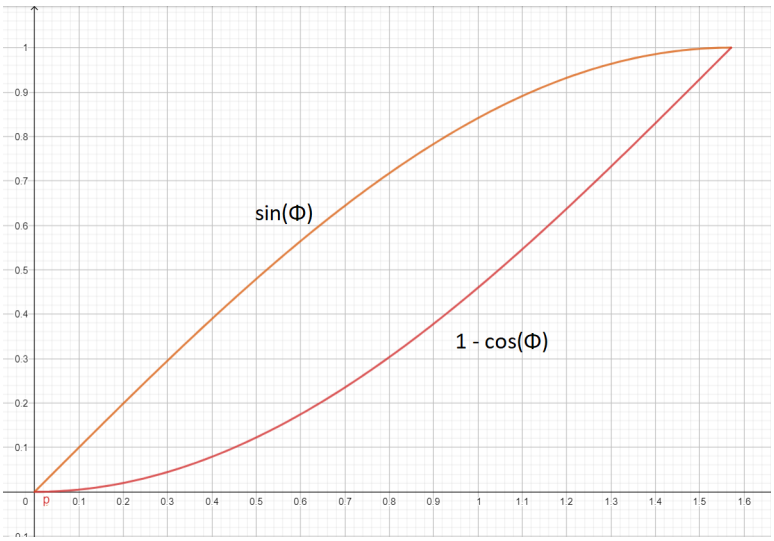

Figura 2: Gráfico contendo as funções de ambos os lados da desigualdade, no intervalo de 0 a $\pi/2$.

4.3 Desigualdade CHSH

Mostrarei a seguir uma versão diferente da desigualdade de Bell.

Consideremos um coletivo de singletos, com cada uma das partículas que os constituem incidindo em analisador de Stern-Gerlach. Tais analisadores podem, cada um, assumir duas direções diferentes, sendo elas $\vec{a}$, $\vec{a'}$ para o primeiro, e $\vec{b}$, $\vec{b'}$ para o segundo. Novamente usaremos funções para denotar o resultado das medições, mas dessa vez indexaremos elas para que indiquem qual par n está sendo medido, sendo assim, I_n é o resultado da medição da primeira partícula do enésimo singleto na direção $\vec{a}$, enquanto II'_n é o resultado da medição da segunda partícula do enésimo singleto na direção $\vec{b'}$, assim por diante. Em uma TVO, esses valores estão determinados antes de se realizar uma medição. Para cada par definiremos uma grandeza γ_n:

$$\gamma_n = I_n(a,b,\lambda)\cdot II_n(a,b,\lambda) + I_n(a,b',\lambda)\cdot II'_n(a,b',\lambda) + I'_n(a',b,\lambda)\cdot II_N(a',b,\lambda) - I'_n(a',b',\lambda)\cdot II'_n(a',b',\lambda) \quad (39)$$

Note que tal notação assume a possibilidade de que I_n seja afetado pela orientação do segundo analisador, ou seja, assume a possibilidade que $I_n(a,b,\lambda) \neq I_n(a,b',\lambda)$, o que estaria em desacordo com a localidade. Para introduzirmos tal principio, supondo a não interferência do segundo analisador, no primeiro, e vice e versa, façamos $I_n(a,b,\lambda) = I_n(a,b',\lambda) \equiv I_n$ e o mesmo para a segunda partícula.

Reescrevendo a equação anterior:

$$\gamma_n = I_n\cdot II_n + I_n\cdot II'_n + I'_n\cdot II_n - I'_n\cdot II'_n$$

$$\gamma_n = I_n(II_n + II'_n) + I'_n(II_n - II'_n) = \pm 2 \quad (40)$$

Nesta última equação é fácil de ver o motivo de γ_n ser sempre ± 2. Um dos parênteses sempre irá se anular, enquanto o outro resultará em ± 2 multiplicado pelo spin da primeira partícula (± 1).

O coeficiente de correlação $c(a,b)$ de N eventos, que se trata da média dos diferentes $I_n\cdot II_n$, é:

$$c(a,b) = \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} I_n\cdot II_n \quad (41)$$

Como cada γ_n é ± 2, uma média deles estaria entre -2 e +2, sendo assim:

$$|\frac{1}{N}\sum_{n=1}^{N}\gamma_n| \equiv |S| = |c(a,b) + c(a,b') + c(a',b) - c(a',b')| \leq 2 \quad (42)$$

A eq. (42) é uma das formas da desigualdade de Bell, chamada desigualdade CHSH [14], que possui esse nome devido aos sobrenomes dos pesquisadores que derivaram ela, Clauser, Horne, Shimony e Holt.

Esta desigualdade já foi violada experimentalmente [15] [16], corroborando com as predições da MQ.

4.3.1 Jogo CHSH

O jogo CHSH funciona da seguinte maneira. Alice e Bob, recebem, respectivamente, duas variáveis aleatórias, $x,\ y \in \{0;\ 1\}$, então, a partir de alguma estratégia previamente combinada entre ambos, sem saber que variável o outro recebeu, retornam as respostas $a,\ b \in \{0;\ 1\}$. Eles ganham caso

$$x \wedge y = a \oplus b \tag{43}$$

onde $\wedge$ denota a lógica AND e $\oplus$, XOR. A tabela 1 mostra as possibilidades dessas lógicas.

x	y	$x \wedge y$	$x \oplus y$
0	0	0	0
1	0	0	1
0	1	0	1
1	1	1	0

Tabela 1: Tabela verdade para as operações AND e XOR

Uma estratégia que não utiliza Física Quântica, pode ser Alice e Bob combinarem de ambos enviarem 0 independentemente da variável aleatória que receberam, já que $0 \oplus 0 = 0$ e $x \wedge y = 0$ em três das quatro possibilidades. Dessa forma obteriam 75% de sucesso, sendo esse o limite para uma estratégia clássica.

Analisemos agora uma estratégia que se utiliza da MQ. Como na situação descrita para a dedução da desigualdade CHSH, Alice e Bob possuem um analisador de Stern-Gerlach cada um, sendo que o analisador da Alice pode medir nas direções $\hat{a}$ e $\hat{a'}$, enquanto o de Bob em $\hat{b}$ e $\hat{b'}$. A direção $\hat{a}$ é $\hat{z}$, portanto possui autoestados $|0\rangle \equiv |0_a\rangle$ e $|1\rangle \equiv |1_a\rangle$ e as outras bases estão "giradas". Os vetores da base $\{|0_{a'}\rangle\,;\ |1_{a'}\rangle\}$ por exemplo, estão girados $\frac{\pi}{4}$ radianos em relação aos vetores correspondentes à direção $\hat{a}$, como mostrado na fig. 3. Já os autoestados de σ_b e $\sigma_{b'}$ estão girados, respectivamente, em $\frac{\pi}{8}$ e $\frac{-\pi}{8}$ em relação aos de σ_a.

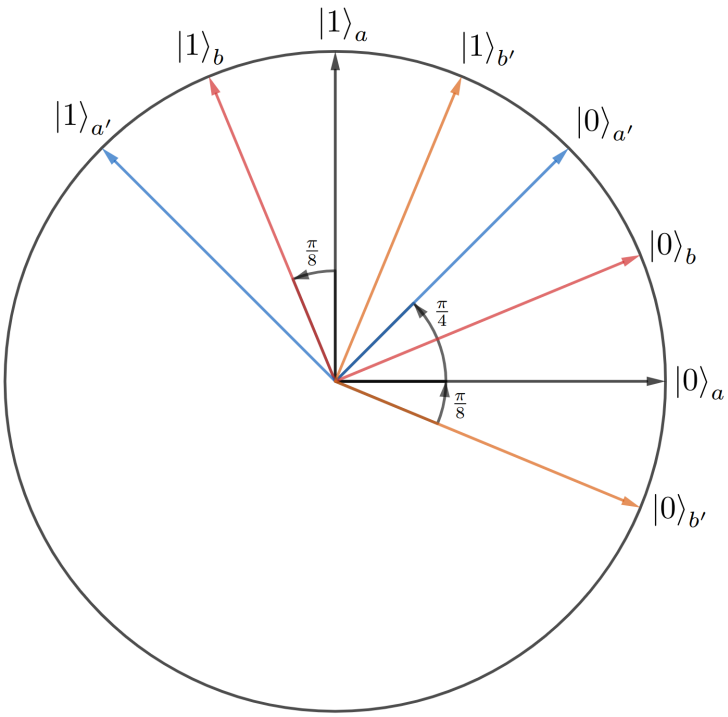

Figura 3: Autoestados de σ_a, $\sigma_{a'}$, σ_b e $\sigma_{b'}$, que correspondem às direções em que Alice e Bob realizarão as medidas.

Alice e Bob compartilharão o estado de Bell

$$|\Phi\rangle = \frac{1}{\sqrt{2}}[\ |0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2\ ] \tag{44}$$

onde a parte (1) se refere à partícula que está com Alice e a parte (2), á que está com Bob.

A estratégia será a seguinte: Após Alice receber o bit x, caso ele seja 0, ela medirá o spin da sua partícula na direção $\hat{a}$ e, caso seja 1, medirá na direção $\hat{a'}$; e de forma semelhante caso o bit y de Bob seja 0 ele medirá na direção $\hat{b}$ e na $\hat{b'}$ caso seja 1. Se o valor aferido for 1, envia-se 0 como resposta; caso seja -1, envia-se 1.

Note que as bases foram escolhidas te tal forma que, quando for necessário que Alice e Bob deem uma resposta igual (a=b), os estados que correspondem a um mesmo autovalor estarão em direções mais próximas. Por exemplo, se $x = y = 0$, ambos devem dar respostas iguais. Olhando para a fig. 3, note que $|0_a\rangle$ está numa direção mais próxima de $|0_b\rangle$ ($\frac{\pi}{8}$), do que de $|1_b\rangle$ ($\frac{3\pi}{8}$). Além disso, quando for necessário que ambos deem respostas diferentes, os estados que correspondem a autovalores distintos que estarão mais próximos.

Analisemos o caso em que $x = y = 0$ (Os outros casos estarão no apêndice B). A base em que Alice medirá será $\{|0_a\rangle\,;\ |1_a\rangle\}$ e a de Bob será $\{|0_b\rangle\,;\ |1_b\rangle\}$. Como $x \wedge y = 0$, para que ganhem o bit de resposta a terá que ser igual ao b. Calculemos a probabilidade de vitória.

$$p(a = b) = p(a = 1 \cap b = 1) + p(a = -1 \cap b = -1)$$

Pela simetria da questão a probabilidade de ambos serem 1 é igual a de ambos serem -1, então

$$p(a = b) = 2p(a = 1 \cap b = 1)$$

$$p(a = b) = 2p(a = 1)p(b = 1 \mid a = 1) \tag{45}$$

Como é possível ver pelo estado na eq. (44), a probabilidade de Alice medir 1 é de 1/2. Após a medição e estado passa a ser

$$|\Phi'\rangle = |0_a\rangle_1 |0_a\rangle_2$$

Ou então, expandindo a parte de Bob na base em que ele medirá:

$$|\Phi'\rangle = |0_a\rangle_1 \left[\cos\left(\frac{\pi}{8}\right)|0_b\rangle_2 - \sin\left(\frac{\pi}{8}\right)|1_b\rangle_2\right] \tag{46}$$

Olhando para este último estado é possível concluir que a probabilidade de Bob medir 1 é de $\cos^2\left(\frac{\pi}{8}\right)$.

Substituindo as informações obtidas no cálculo de probabilidade, encontra-se que

$$p(a = b) = \cos^2\left(\frac{\pi}{8}\right) \approx 0,85 \tag{47}$$

Que é o mesmo valor obtido para todos os casos de bits x e y (mostrarei os demais casos no apêndice).

Além disso, como havia dito, tal jogo se da de maneira semelhante a que foi descrita na dedução da desigualdade CHSH, portanto calculemos o valor de $|S|$, a partir da eq. (42), imaginando que Alice e Bob repetirão o jogo inúmeras vezes. No caso de $c(a, b)$ por exemplo, que é correlação para as direções $\hat{a}$ e $\hat{b}$, basta encontrar o valor médio da multiplicação dos spins medidos, ou seja

$$c(a, b) = p(a = b)(1) + p(a \neq b)(-1)$$

$$c(a, b) = \cos^2\left(\frac{\pi}{8}\right)(1) + \left[1 - \cos^2\left(\frac{\pi}{8}\right)\right](-1)$$

$$c(a, b) = 2\cos^2\left(\frac{\pi}{8}\right) - 1 \tag{48}$$

Os outros casos serão iguais, visto que possuem as mesmas probabilidades, a menos de $c(a', b')$, que será

$$c(a', b') = \left[1 - \cos^2\left(\frac{\pi}{8}\right)\right](1) + \cos^2\left(\frac{\pi}{8}\right)(-1) = 1 - 2\cos^2\left(\frac{\pi}{8}\right) \tag{49}$$

Substituindo tudo na eq. (42), obtém-se

$$|S| = 4\left[2cos^2\left(\frac{\pi}{8}\right) - 1\right] = 2\sqrt{2} \tag{50}$$

Ou seja, a desigualdade CHSH é violada. Além disso, o valor de $2\sqrt{2}$ é o máximo que pode ser alcançado [17].

5 Criptografia Quântica

No nosso cotidiano nós usamos criptografia praticamente em todas as nossa comunicação digital. Em sua maioria é usado algum tipo de criptografia para somente o remetente e o receptor tenham acesso a uma mensagem comunicada. Um dos tipos de criptografia usam chaves criptográficas simétricas, onde encriptar e decriptar usam a mesma chave. Porém, é necessário uma forma segura de assegurar que somente as duas partes interessadas tenham a chave. E aqui podemos usar propriedades quânticas para nos auxiliar nessa tarefa, conhecida como distribuição de chaves quânticas (QKD - quantum key distribution).

5.1 Protocolo BB84 [2]

O protocolo BB84 foi o primeiro protocolo de distribuição de chaves quânticas. Seu nome é devido aos sobrenomes dos pesquisadores que criaram ele, Bennet e Brassard, e também por ter sido criado em 1984. O protocolo utiliza-se de sistemas quânticos de dois níveis. Neste caso utilizarei fótons linearmente polarizados.

Em tal protocolo, Alice e Bob devem combinar, publicamente, as bases que utilizarão para codificar os fótons em bits (codificação essa que será feita pela Alice) e também receptarão eles (tarefa que será realizada pelo Bob). Aqui utilizarei para uma das bases, a base A, a polarização horizontal e vertical, sendo que a direção horizontal ($|0_A\rangle$) corresponderá ao bit 0 e a vertical ($|1_A\rangle$) ao bit 1. A outra base, B, será uma girada em 45° em relação a primeira, onde a direção que está em 45° em relação à horizontal ($|0_B\rangle$) corresponderá ao bit 0, enquanto a que está 135°em relação à horizontal ($|0_B\rangle$) ao bit 1. Vide fig. 4.

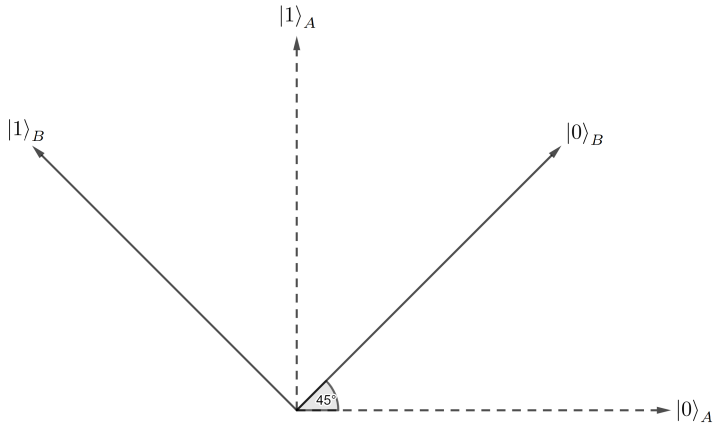

Figura 4: Autoestados de σ_a e σ_b, que correspondem às direções em que Alice e Bob realizarão as medidas.

A seguir, Alice escolhe uma sequência de bits aleatórios para enviar para Bob, usarei o exemplo 01001. Além disso, ela deve escolher aleatoriamente com qual das bases cada um dos bits será codificado. Nesta sequência de cinco bits por exemplo, ela pode usar a base A para os três primeiros e a B para os dois últimos, então ela enviaria os estados $|0_A\rangle$, $|1_A\rangle$, $|0_A\rangle$, $|0_B\rangle$, $|1_B\rangle$. Então quando tais fótons chegassem em Bob, ele deveria escolher aleatoriamente com quais bases irá medir cada um deles. Todas as vezes que Bob escolher, por coincidência, medir com a mesma base, um dado fóton, ele obterá o mesmo estado que foi enviado por Alice. Caso ela tenha por exemplo enviado um fóton polarizado verticalmente, o que corresponde ao bit 1 na base A, e Bob meça esse bit, coincidentemente, na mesma base, ele obterá também um fóton polarizado verticalmente. No entanto, caso ele meça na base B, ele terá 50% de chance de obter os autoestados de tal base, já que

$$|1\rangle_A = \frac{1}{\sqrt{2}}(|0_B\rangle + |1_B\rangle) \tag{51}$$

Um detalhe do protocolo BB84 é inclusive que, mesmo em casos de alfabetos maiores que o binário, ao se medir um estado na base errada, a probabilidade de obter, após a medida, qualquer um dos autoestados de tal base errada, deve ser a mesma. No atual caso, binário, isso significa que ao errar a base Bob terá 50% de chance de obter qualquer um dos autoestados.

Após Bob ter medido todos os fótons, ele se comunica com Alice e publicamente verificam quais bases foram coincidentes na codificação e na recepção. Todos os fótons que foram medidos em um base diferente, são descartados. Quando Bob no enésimo fóton, acerta a base, como medindo na base A um estado que foi gerado por ela, obtendo um fóton na vertical, ele sabe que o enésimo bit enviado por Alice é 1. O próximo passo é ambos selecionarem alguns dos

bits para verificar se o que Bob recebeu foi realmente o que Alice enviou (caso não coincidam, existe a possibilidade de que um terceiro tentou monitorar a transmissão). Tais bits também são descartados. Então, os bits restantes serão uma chave criptográfica, que é conhecida por ambos, mesmo que Alice não tenha utilizado nenhum canal de comunicação clássico para informá-la diretamente.

Analisemos o que acontece caso alguém, Eve, tente monitorar os fótons enviados para também saber qual é a chave criptográfica. Como foi dito anteriormente, existe uma etapa onde Alice e Bob, após selecionarem as bases coincidentes, verificam se alguns dos bits que ambos possuem são realmente iguais. A cada um desses bits, Eve pode ter escolhido a base errada para medi-los, algo que acontecerá em 50% das vezes. Nessas vezes o estado colapsou para um dos autoestados da base em que Eve mediu, de tal forma quando Bob mediu o fóton na mesma base em que ele avia sido originalmente enviado por Alice, ele terá 50% de obter um estado diferente do que seria esperado caso Eve não tivesse medido. Sendo assim, sendo N o número de vezes que Eve escolhe a base errada, a probabilidade de Bob encontrar os mesmos estados enviados por Alice (dentre aqueles em que ambos escolheram a mesma base), é de $(0,5)^N$, fazendo com que seja difícil que na fase de verificação a ação Eve não seja descoberta.

5.2 Protocolo E91 [3]

O protocolo E91, seguindo a mesa lógica do BB84, possui tal nome porque o seu criador tem o sobrenome Ekert e porque foi criado em 1991. No E91, são usados pares de fótons emaranhados, singletos (eq.(10)), gerados em um terceiro lugar, que não é onde Alice e Bob estão. Diferentemente do protocolo BB84 (seção 5.1), a comunicação direta entre ambos se dará de maneira exclusivamente clássica.

Cada um disporá de três direções para realizar as medidas de polarização, que denotarei por $\hat{a}_i$ e $\hat{b}_j$ $(i,j=1,2,3)$, todas contidas no plano xy. Os ângulos das direções de medição de Alice são respectivamente 0, $\pi/4$ e $\pi/2$, enquanto os de Bob são $\pi/4$, $\pi/2$ e $3\pi/4$. Ambos também devem combinar, como no BB84, a que bit (0 e 1) corresponderá cada um dos autovalores (1 e -1). Note que $\hat{a}_2 = \hat{b}_1$ e $\hat{a}_3 = \hat{b}_2$.

A fonte de fótons emaranhados envia-os para Alice e Bob, que por sua vez realizam as medidas escolhendo aleatoriamente as três bases que cada um tem à disposição. Após feito isso, eles se comunicam de maneira clássica e anunciam quais bases usaram para cada fóton. A seguir eles separam as medidas em dois grupos diferentes, um com todos os resultados obtidos de quando usaram bases coincidentes e, o outro, o restante. Com o primeiro grupo, da mesma forma como foi feito no BB84 (seção 5.1), eles cunham uma chave criptográfica, se atentando ao fato de que se tratando de singletos, todas as vezes que Alice obteve 1 como resultado da medida, Bob obteve -1 e vice e versa. O segundo grupo, das bases não coincidentes, é usado para verificar a segurança do canal, da maneira como descreverei a seguir.

Com os resultados de medições do segundo grupo, Alice e Bob devem calcular a desigualdade CHSH

$$|S| = |c(a_1,b_1) + c(a_3,b_3) + c(a_3,b_1) - c(a_1,b_3)| \tag{52}$$

usando, por exemplo, a eq. (19). Pode-se encontrar qual é o valor de $|S|$ previsto pela MQ e então compará-lo com o encontrado no experimento. Usando a eq. (28):

$$\begin{aligned} |S| &= |-\hat{a}_1\cdot\hat{b}_1 - \hat{a}_3\cdot\hat{b}_3 - \hat{a}_3\cdot\hat{b}_1 + \hat{a}_1\cdot\hat{b}_3| \\ |S| &= \left|-3\cos\left(\frac{\pi}{4}\right) + \cos\left(\frac{3\pi}{4}\right)\right| \\ |S| &= 2\sqrt{2} \end{aligned} \tag{53}$$

Caso Alice e Bob não encontrem tal valor com os seus resultados, eles devem descartar tudo e começar novamente. Eles podem por exemplo obter o valor máximo não quântico, que seria 2, como foi obtido na eq. (42), significando que os pares de fótons que eles mediram não estavam emaranhados, ou por algum problema no canal ou pelo fato de que alguém interceptou os fótons numa tentativa de obter informações, desemaranhando os fótons no ato.

6 Código de acesso aleatório (RAC, na sigla em inglês)

Alice tem uma palavra aleatória $x = x_1x_2...x_n$, de comprimento n, escrita em um alfabeto $X = \{1,2,...,d\}$ de dimensão d. Bob, separado espacialmente de Alice, recebe um índice aleatório $j \in \{1,2,...,n\}$, sendo que o objetivo de Bob é adivinhar a j-ésima letra (x_j) da palavra de Alice. A comunicação entre ambos é restrita ao envio de uma mensagem codificada m, sendo $m < n$. Diferentes estratégias podem ser utilizadas e uma maneira de representar o quão boa é uma dada estratégia é com a probabilidade média p de Bob acertar a letra. Uma notação compacta que expressa os parâmetros previamente descritos de um RAC é: $n^{(d)} \xrightarrow{p} m$

6.1 Codificação clássica

O RAC mais simples é $2^2 \to 1$. Uma estratégia que eles podem adotar é Alice sempre enviar para Bob o valor da primeira letra da sua palavra. Um índice j (1 ou 2 nesse caso) será aleatoriamente gerado para que Bob tente acertar a letra x_j. Caso o j seja 1, devido a estratégia adotada ele com certeza acertará, pois Alice já enviou para ele a letra x_1. Caso j seja 2, Bob terá que chutar qual é a letra, tendo portanto 50% de probabilidade de acerto. Sendo assim, a probabilidade média de sucesso para tal estratégia é $p = \frac{1}{2}(1 + \frac{1}{2}) = \frac{3}{4}$.

Já em um RAC mais geral $2^{(d)} \to 1$, caso a mesma estratégia seja adotada, se j for 1, novamente Bob com certeza acertará, mas, caso $j \neq 1$, a probabilidade dele acertar no chute será de $\frac{1}{d}$. Sendo assim, a probabilidade de sucesso será de $p = \frac{1}{2}(1 + \frac{1}{d})$. Então quanto maior for a dimensão do alfabeto, menor será a probabilidade de sucesso para essa estratégia, tendendo a um limite de $\frac{1}{2}$.

6.2 Codificação quântica $2^{(2)} \to 1$

No RAC quântico (QRAC, na sigla em inglês) $2^{(2)} \to 1$, Alice codificará a sua mensagem x_0x_1 em um qubit, se utilizando da representação da fig. 5.

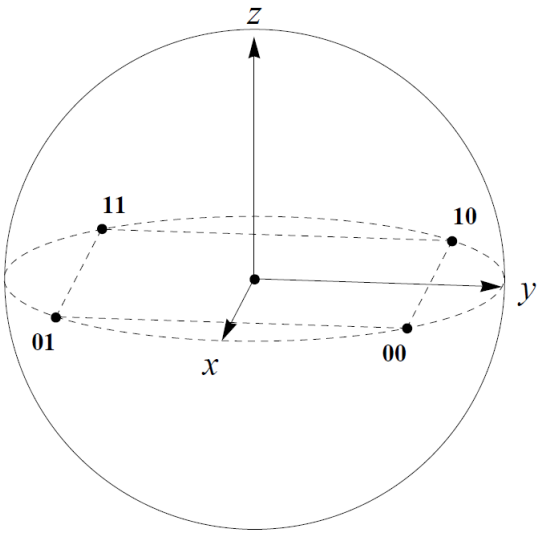

Figura 5: Representação na esfera de Bloch da codificação para o QRAC $2^{(2)} \to 1$ [18].

Um qubit arbitrário é dado por:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{54}$$

Olhando para a a fig. 5, é possível notar que em todos os casos $\theta = \frac{\pi}{2}$ e com os diferentes ϕ de cada ponto na esfera de Bloch, os diferentes estados $|\Psi_{x_0x_1}\rangle$ ficam sendo:

$$|\Psi_{00}\rangle = \cos\left(\frac{\pi}{4}\right)|0\rangle + \left[\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)\right]\left[\sin\left(\frac{\pi}{4}\right)\right]|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle$$

$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{-1+i}{2}|1\rangle$$

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{-1-i}{2}|1\rangle$$

$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1-i}{2}|1\rangle$$

Ou então, de uma maneira mais concisa:

$$|\Psi_{x_0x_1}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{x_0} + i(-1)^{x_1}}{2}|1\rangle \tag{55}$$

Após Alice enviar o qubit, como no caso clássico, Bob recebe um índice j aleatório, tendo que adivinhar a letra x_j. Agora a estratégia de Bob será medir o qubit na base σ_x, $\left\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\right\} \equiv \{|0_x\rangle\,;\ |1_x\rangle\}$, caso j seja 0 e medir na base σ_y, $\left\{\frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)\right\} \equiv \{|0_y\rangle\,;\ |1_t\rangle\}$, caso j seja 1.

Caso j seja 0 por exemplo e Bob realize uma medida na base σ_x, se ele obter o autovalor 1, correspondente ao autoestado $|0_x\rangle$, Bob dirá que a letra x_0 é 0, mas caso obtenha o autovalor -1, correspondente ao autoestado $|1_x\rangle$, dirá que a letra x_0 é 1. Para encontrar as probabilidades de sucesso nesses dois casos basta calcular $|\langle 0_x|\Psi_{x_0x_1}\rangle|^2$ e $|\langle 1_x|\Psi_{x_0x_1}\rangle|^2$, respectivamente. Com a mensagem sendo por exemplo 00 e j sendo 0, a probabilidade de Bob acertar a primeira letra utilizando a estratégia descrita é:

$$
\begin{aligned}
p &= |\langle 0_x|\Psi_{x_0x_1}\rangle|^2 \\
p &= \left|\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle\right)\right|^2 \\
p &= \left|\frac{2 + 2\sqrt{2} + 2i}{4\sqrt{2}}\right|^2 \\
p &= \frac{1}{2}\left(1 + \frac{\sqrt{2}}{2}\right) \approx 0,854
\end{aligned}
\tag{56}
$$

Ao se repetir esse mesmo processo para outras mensagens e outros índices j, a probabilidade de sucesso encontrada sempre será igual a que foi obtida na eq. (56), devido a distribuição simétrica dos estados no equador da esfera.

6.3 Codificação quântica $3^{(2)} \to 1$

No código de acesso aleatório quântico (QRAC, na sigla em inglês) $3^{(2)} \to 1$, Alice codificará sua mensagem $x_0x_1x_2$ em um qubit, se utilizando da representação da fig. 6, onde o estado de cada mensagem será o vértice de um cubo inscrito na esfera de Bloch.

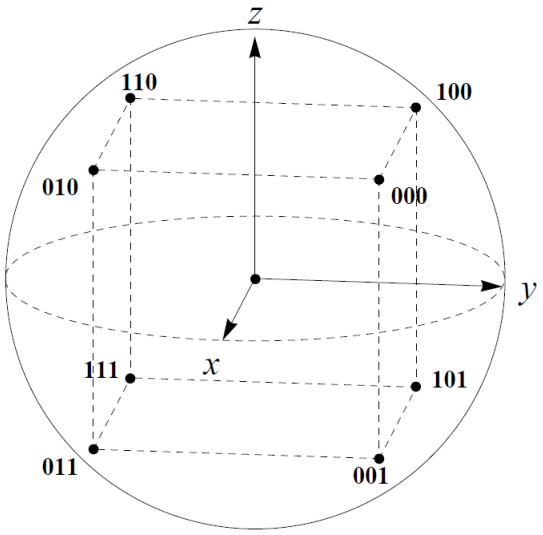

Figura 6: Representação na esfera de Bloch da codificação para o QRAC $3^{(2)} \to 1$ [18].

Diferentemente do QRAC $2^{(2)} \to 1$, onde todos os estados possuíam o mesmo valor para θ na eq. (54), agora existem duas possibilidades, uma para os estados que codificam as mensagens que terminam com 0 e outro para as que terminam com 1. Se utilizando da informação de que a esfera de Bloch tem raio unitário, é possível concluir que a diagonal do cubo é 2. Como a diagonal d de um cubo é $a\sqrt{3}$ (sendo a a aresta), ao igualar os dois valores para a diagonal obtém-se que a aresta é $\frac{2}{\sqrt{3}}$, o que nos leva a concluir que a coordenada z para os estados que codificam mensagens terminadas em 0, é $\frac{1}{\sqrt{3}}$, logo possuem um θ tal que $\cos\theta = \frac{1}{\sqrt{3}}$. Seguindo o mesmo raciocínio, os que codificam mensagens terminadas em 1, $\cos\theta = -\frac{1}{\sqrt{3}}$. Sendo assim, para ambos os casos, $\cos^2\left(\frac{\theta}{2}\right) = \frac{1}{2} + \frac{\cos\theta}{2} = \frac{1}{2} + \frac{1}{2\sqrt{3}}$

Neste caso o j sorteado também determinará a base em que será medido o qubit, com a diferença de que com o bit a mais na mensagem, se comparado com o QRAC anterior, caso j seja 2, a base utilizada para medir será σ_z. Exemplificando, caso a mensagem seja 000, e o j seja 2, como o estado já está na base σ_z, a probabilidade de se obter o autovalor 1 será simplesmente:

$$\left|\cos\left(\frac{\theta}{2}\right)\right|^2 = \frac{1}{2} + \frac{1}{2\sqrt{3}} \approx 0,78868. \tag{57}$$

Novamente, devido a distribuição simétrica dos estados na esfera de Bloch, a probabilidade de acerto para os outros casos é mesma .

6.4 RAC assistido por emaranhamento $2^{(2)} \to 1$ [4]

No código de acesso aleatório assistido por emaranhamento (EARAC, na sigla em inglês), Alice e Bob compartilharão um estado de singleto, eq.(10), sendo a parte (1) referente à Alice e a (2), ao Bob. Diferentemente do QRAC (seção 6.2), ao invés de enviar qubits para Bob, Alice enviará uma mensagem M que contém um bit clássico.

No EARAC em questão, dada uma mensagem $x = x_0x_1$, Alice realizará uma medida na parte (1) do sistema, dependendo do valor de $x_0 \oplus x_1$. Ela realizará uma medida na direção $\hat{a}$, que corresponde à base que denotaremos por A_0, ou na $\hat{a}'$, que corresponde a base que denotarei por A_1. Os vetores das bases de tais são:

$$A_0 = \{|0_a\rangle ; |1_a\rangle\} = \left\{ \frac{1}{\sqrt{2}} |0\rangle + \frac{1+i}{2} |1\rangle ; \frac{1}{\sqrt{2}} |0\rangle - \frac{-1+i}{2} |1\rangle \right\} \tag{58}$$

$$A_1 = \{|0_{a'}\rangle ; |1_{a'}\rangle\} = \left\{ \frac{1}{\sqrt{2}} |0\rangle + \frac{1-i}{2} |1\rangle ; \frac{1}{\sqrt{2}} |0\rangle + \frac{-1+i}{2} |1\rangle \right\} \tag{59}$$

A base A_0 será utilizada caso $x_0 \oplus x_1 = 0$, e A_1 caso $x_0 \oplus x_1 = 1$. Já Bob, como no caso do QRAC, medirá na base σ_x caso tenha que adivinhar x_0 e na base σ_y caso tenha que adivinhar x_1. Lembrando que a letra da mensagem que ele terá que adivinhar é determinado por um índice j gerado aleatoriamente e dado a ele.

Por fim, resta a questão de como Bob dará seu palpite. Quando Alice realiza a medida, ela obtém $+1$ ou -1, autovalores correspondentes respectivamente aos kets 0 e kets 1. O parâmetro que chamarei de A, será 0 quando a medida de Alice resultar em $+1$, e será 1 quando a medida de Alice resultar em -1. Em posse de tal parâmetro A, ela envia para Bob a mensagem $M = x_0 \oplus A$. Então, Bob, após medir σ_x ou σ_y (dependendo de qual letra da mensagem ele deve tentar adivinhar), e obtendo $+1$ ou -1, dará o palpite que a letra x_j que ele deve adivinhar é $x_j = M \oplus B$, onde B é 1 caso a medida de Bob resulte em 1, e 0 caso a medida de Bob resulta em -1.

Analisaremos a seguir, os casos envolvendo duas palavras, encontrando qual é a probabilidade de Bob acertar.

6.4.1 Análise dos casos no EARAC onde a mensagem é 00

Ao realizar a medida, Alice obterá $+1$ ou -1. Primeiramente suponhamos que a medida resulte em -1. Neste caso, $A = 1$. Além disso, se tratando de um singleto, antes da medida possuía a mesma forma que na eq. (10), logo, após a medida o estado é, utilizando a eq. (58):

$$|\Psi'\rangle = |1_a\rangle_1 |0_a\rangle_2 = |1_a\rangle_1 \left(\frac{1}{\sqrt{2}} |0\rangle_2 + \frac{1+i}{2} |1\rangle_2 \right) \tag{60}$$

Como dito anteriormente, a base em que Bob realizará a medida em sua parte é determinada pela letra que terá que adivinhar. Expandindo a parte (2) em σ_x e σ_y respectivamente, obtemos (omitirei que se trata exclusivamente da parte (2) nas equações a seguir):

$$\frac{1}{\sqrt{2}} |0\rangle_2 + \frac{1+i}{2} |1\rangle_2 = \left(\frac{\sqrt{2}+1}{2\sqrt{2}} + \frac{i}{2\sqrt{2}} \right) |0_x\rangle_2 + \left(\frac{\sqrt{2}-1}{2\sqrt{2}} - \frac{i}{2\sqrt{2}} \right) |1_x\rangle_2 \tag{61}$$

$$\frac{1}{\sqrt{2}} |0\rangle_2 + \frac{1+i}{2} |1\rangle_2 = \left(\frac{\sqrt{2}+1}{2\sqrt{2}} - \frac{i}{2\sqrt{2}} \right) |0_y\rangle_2 + \left(\frac{\sqrt{2}-1}{2\sqrt{2}} + \frac{i}{2\sqrt{2}} \right) |1_y\rangle_2 \tag{62}$$

É possível ver na eq. (61) que, no caso em que Bob deve adivinhar a primeira letra, e portanto tem que realizar a medida de σ_x, o mais provável é que a medida resulte em $+1$. Vejamos qual é a probabilidade de tal resultado:

$$p(1) = \left| \frac{\sqrt{2}+1}{2\sqrt{2}} + \frac{i}{2\sqrt{2}} \right|^2 = \frac{2+\sqrt{2}}{4} \approx 0,854 \tag{63}$$

Caso seja esse o resultado que Bob obtenha ao medir σ_x, $B = 1$ e, sendo assim, o palpite de Bob para a primeira letra seria $M \oplus B = 1 \oplus 1 = 0$, o que estaria correto. Portanto, a probabilidade de Bob acertar neste caso (assim como será em todos os outros) é de aproximadamente $0,854$, a mesma que para o QRAC mostrado nesse trabalho.

Por outro lado, como se nota na eq. (62), caso Bob tenha que adivinhar a segunda letra, tendo portanto que medir σ_y, também será mais provável que a medida resulte em $+1$, fazendo com que seu palpite seja $M \oplus B = 1 \oplus 1 = 0$, fazendo novamente com que acerte seu palpite. A probabilidade de que isso aconteça é novamente aproximadamente $0,854$.

Tendo analisado o cenário em que a medida de Alice resulta em -1, vejamos o que acontece no caso em que ela resulte em $+1$. Neste caso, após a medida o estado passa a ser

$$|\Psi'\rangle = |0_a\rangle_1 |1_a\rangle_1 = |0_a\rangle_1 \left(\frac{1}{\sqrt{2}} |0\rangle_2 - \frac{1+i}{2} |1\rangle_2 \right) \tag{64}$$

Expandindo o estado anterior nas bases σ_x e σ_y, obtém-se

$$\frac{1}{\sqrt{2}} |0\rangle_2 - \frac{1+i}{2} |1\rangle_2 = \left(\frac{\sqrt{2}-1}{2\sqrt{2}} - \frac{i}{2\sqrt{2}} \right) |0_x\rangle_2 + \left(\frac{\sqrt{2}+1}{2\sqrt{2}} + \frac{i}{2\sqrt{2}} \right) |1_x\rangle_2 \tag{65}$$

$$\frac{1}{\sqrt{2}} |0\rangle_2 - \frac{1+i}{2} |1\rangle_2 = \left(\frac{\sqrt{2}-1}{2\sqrt{2}} + \frac{i}{2\sqrt{2}} \right) |0_y\rangle_2 + \left(\frac{\sqrt{2}+1}{2\sqrt{2}} - \frac{i}{2\sqrt{2}} \right) |1_y\rangle_2 \tag{66}$$

Iniciando pelo caso em que o índice aleatório j é tal que Bob tenha que adivinhar a primeira letra, tendo portanto que medir σ_x, é mais provável que ele obtenha -1, o que, por consequência, faria com que o parâmetro B fosse 0 e seu palpite para a primeira letra fosse $M \oplus B = 0 \oplus 0 = 0$, acertando assim a letra. A probabilidade para que isso aconteça é a mesma que nos casos anteriores, já que o módulo da parte real e imaginária do coeficiente de $|1(2)\rangle_x$ são os mesmos que dos casos anteriormente discutidos.

Por fim, a última possibilidade para a mensagem 00 é que, tendo Alice medido -1, Bob tenha que adivinhar a segunda letra. Ao medir σ_y ele obterá -1 com probabilidade de aproximadamente $0,854$, cenário no qual ele acertaria o palpite ($M \oplus B = 0 \oplus 0 = 0$), fazendo novamente com que seja mais provável que ele acerte qual é a letra.

Em todos os outros 12 casos, para as mensagens 01, 10 e 11, utilizando a mesma lógica que foi aqui mostrada para 00, a probabilidade de acerto de Bob também será de aproximadamente $0,854$.

7 Conclusão

Neste trabalho pudemos, como havíamos proposto, aprender sobre as bases por trás de certos protocolos de criptografia quântica (BB84, E91) e do código de acesso aleatório (QRAC e EARAC), percorrendo temas que também foram de suma importância para o desenvolvimento da Mecânica Quântica, como o paradoxo EPR.

Além disso, verificamos que codificações quânticas podem em teoria ter uma maior probabilidade de sucesso do que caso se tivesse utilizado a versão clássica, como nos protocolos de RAC, em que tanto o QRAC e o EARAC foram superiores a codificação clássica aqui mostrada. Tais detalhes, assim como a impossibilidade de copiar estados quânticos, corroboram para a utilização futura de codificações quânticas em tecnologias de comunicação.

Apêndices

A Autovetores de σ_n

Calcularemos aqui os autovetores da matriz de Pauli para uma direção arbitrária $\hat{n}$:

$$\sigma_n = \begin{bmatrix} \cos\theta & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & -\cos\theta \end{bmatrix} \tag{67}$$

Já partiremos do ponto em que sebemos que os autovalores da matriz são 1 e -1.

A.1 Autovalor 1

Para o autovalor 1 o problema a ser resolvido é:

$$\begin{bmatrix} \cos\theta - 1 & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & -\cos\theta - 1 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = 0 \tag{68}$$

Disso é possível ver que:

$$\frac{1-\cos\theta}{\sin\theta} e^{i\phi} C_1 = C_2$$
$$\frac{2\sin^2\left(\frac{\theta}{2}\right)}{2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)} e^{i\phi} C_1 = C_2$$
$$\frac{\sin\left(\frac{\theta}{2}\right)}{\cos\left(\frac{\theta}{2}\right)} e^{i\phi} C_1 = C_2$$

Para se obter um estado normalizado, utilizando o resultado anterior:

$$|C_1|^2 + |C_2|^2 = 1$$
$$|C_1|^2 \left[1 + \frac{\sin^2\left(\frac{\theta}{2}\right)}{\cos^2\left(\frac{\theta}{2}\right)}\right] = 1$$

Por fim, a despeito de uma fase que não muda o estado físico:

$$C_1 = \cos\left(\frac{\theta}{2}\right);\ C_2 = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$$
$$|1_n\rangle = \cos\left(\frac{\theta}{2}\right)|1\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|0\rangle \tag{69}$$

que possui a mesma forma que o estado de um qubit arbitrário, mostrado na eq. (54).

A.2 Autovalor -1

Para o autovalor 1 o problema a ser resolvido é:

$$\begin{bmatrix} \cos\theta + 1 & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & -\cos\theta + 1 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = 0 \tag{70}$$

Disso é possível ver que:

$$\frac{-(1+\cos\theta)}{\sin\theta} e^{i\phi} C_1 = C_2$$
$$\frac{-\left[1 + 2\cos^2\left(\frac{\theta}{2}\right) - 1\right]}{2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)} e^{i\phi} C_1 = C_2$$
$$\frac{-\cos\left(\frac{\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)} e^{i\phi} C_1 = C_2$$

Para se obter um estado normalizado, utilizando o resultado anterior:

$$|C_1|^2 + |C_2|^2 = 1$$
$$|C_1|^2 \left[1 + \frac{\cos^2\left(\frac{\theta}{2}\right)}{\sin^2\left(\frac{\theta}{2}\right)}\right] = 1$$

Por fim, a despeito de uma fase, e multiplicando o estado resultante por $(-e^{-i\phi})$, coisas que não mudam o estado físico, obtém-se que:

$$C_1 = -e^{-i\phi}\sin\left(\frac{\theta}{2}\right);\ C_2 = \cos\left(\frac{\theta}{2}\right)$$

$$|0_n\rangle = -e^{-i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle + \cos\left(\frac{\theta}{2}\right)|0\rangle \tag{71}$$

B Demais casos para o jogo CHSH

Anteriormente foi calculada a probabilidade de vitória no jogo CHSH, quando $x = y = 0$. Mostraremos aqui que nas demais possibilidades a probabilidade de vitória será a mesma.

B.1 x=0 e y=1

Neste caso, Alice mede na base $\{|0_a\rangle\,;\ |1_a\rangle\}$ e Bob na $\{|0_{b'}\rangle\,;\ |1_{b'}\rangle\}$ e eles vencem caso obtenham o mesmo autovalor ao medirem, sendo assim, a eq. (45) continua valendo.

A probabilidade de Alice obter o autovalor 1 é 1/2. Após a medida o estado passa a ser

$$|\Phi'\rangle = |0_a\rangle_1\,|0_a\rangle_2$$

$$|\Phi'\rangle = |0_a\rangle_1\left[\cos\left(\frac{\pi}{8}\right)|0_{b'}\rangle_2 + \sin\left(\frac{\pi}{8}\right)|1_{b'}\rangle_2\right] \tag{72}$$

Olhando para este estado podemos ver que a probabilidade de Bob medir o autovalor 1 é de $\cos^2\left(\frac{\pi}{8}\right)$. Substituindo tudo na eq. (45) obtém-se que

$$p(a=b) = \cos^2\left(\frac{\pi}{8}\right) \approx 0,854 \tag{73}$$

B.2 x=1 e y=0

Neste caso, Alice mede na base $\{|0_{a'}\rangle\,;\ |1_{a'}\rangle\}$ e Bob na $\{|0_b\rangle\,;\ |1_b\rangle\}$ e mais uma vez vencem caso obtenham o mesmo autovalor ao medirem, sendo assim, a eq. (45) continua valendo.

Para sabermos qual é a probabilidade de Alice obter 1 ao medir, é necessário expandir o estado de Bell em questão, na base $\{|0_{a'}\rangle\,;\ |1_{a'}\rangle\}$, mas como esse estado, assim como o singleto, possui invariância rotacional, ele será simplesmente

$$|\Phi\rangle = \frac{1}{\sqrt{2}}[\ |0_{a'}\rangle_1\,|0_{a'}\rangle_2 + |1_{a'}\rangle_1\,|1_{a'}\rangle_2\ ] \tag{74}$$

o que permite a conclusão de que a probabilidade de Alice obter 1 continuará sendo 1/2.

Após a medida o estado passa a ser

$$|\Phi'\rangle = |0_{a'}\rangle_1\,|0_{a'}\rangle_2$$

$$|\Phi'\rangle = |0_{a'}\rangle_1\left[\cos\left(\frac{\pi}{8}\right)|0_b\rangle_2 + \sin\left(\frac{\pi}{8}\right)|1_b\rangle_2\right] \tag{75}$$

então novamente Bob obterá 1 com uma probabilidade de $\cos^2\left(\frac{\pi}{8}\right)$. Pela eq. (45)

$$p(a=b) = \cos^2\left(\frac{\pi}{8}\right) \approx 0,854 \tag{76}$$

B.3 x=1 e y=1

Neste caso, Alice mede na base $\{|0_{a'}\rangle\,;\ |1_{a'}\rangle\}$ e Bob na $\{|0_{b'}\rangle\,;\ |1_{b'}\rangle\}$, porém agora eles vencem caso obtenham autovalores diferentes ao medirem. Calculemos a probabilidade de vitória.

$$p(a \neq b) = p(a = 1 \cap b = -1) + p(a = -1 \cap b = 1)$$

Mais uma vez por simetria

$$p(a \neq b) = 2p(a = 1 \cap b = -1)$$

$$p(a \neq b) = 2p(a = 1)p(b = -1 \mid a = 1) \tag{77}$$

Como em todos os outros casos, Alice mede 1 com probabilidade 1/2. O estado passa a ser

$$|\Phi'\rangle = |0_{a'}\rangle_1 \, |0_{a'}\rangle_2$$

$$|\Phi'\rangle = |0_{a'}\rangle_1 \left[\sin\left(\frac{\pi}{8}\right)|0_{b'}\rangle_2 + \cos\left(\frac{\pi}{8}\right)|1_{b'}\rangle_2\right] \tag{78}$$

Agora diferentemente dos outros casos, procura-se a probabilidade de Bob obter -1, porém devido à maneira como as bases foram escolhidas, mais uma vez tal probabilidade é $\cos^2\left(\frac{\pi}{8}\right)$. Substituindo o que foi encontrado na eq. (77)

$$p(a \neq b) = \cos^2\left(\frac{\pi}{8}\right) \approx 0,85 \tag{79}$$

Referências

[1] M. Redhead, "Completeness, nonlocality and realism: A prolegomenon to the philosophy of quantum mechanics. clarendon," 1987.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, (India), p. 175, 1984.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, Aug. 1991.

[4] M. Pawłowski and M. Ż ukowski, "Entanglement-assisted random access codes," *Physical Review A*, vol. 81, apr 2010.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[6] L. K. Grover, "From schrödinger's equation to the quantum search algorithm," *American Journal of Physics*, vol. 69, pp. 769–777, 2001.

[7] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, p. 1484–1509, 1997.

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, pp. 1895–1899, Mar. 1993.

[9] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, "Quantum random access codes using single d-level systems," *Physical Review Letters*, vol. 114, p. 170502, 2015.

[10] A. Tavakoli, B. Marques, M. Pawłowski, and M. Bourennane, "Spatial versus sequential correlations for random access coding," *Physical Review A*, vol. 93, p. 032336, 2016.

[11] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, p. 777, 1935.

[12] O. P. Junior, *Conceitos de Física Quântica 2*. Editora Livraria da Fisica, 2003.

[13] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics*, vol. 1, pp. 195–200, 1964.

[14] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical review letters*, vol. 23, no. 15, p. 880, 1969.

[15] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of bell's inequalities using time-varying analyzers," *Phys. Rev. Lett.*, vol. 49, pp. 1804–1807, Dec 1982.

[16] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. Twitchen, D. Elkouss, S. Wehner, T. Taminiau, and R. Hanson, "Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km," *arXiv arXiv:1508.05949*, 2016.

[17] B. S. Cirel'son, "Quantum generalizations of bell's inequality," *Letters in Mathematical Physics*, vol. 4, no. 2, p. 93–100, 1980.

[18] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness," *arXiv preprint arXiv:0810.2937*, 2008.