Alan Cavalcanti Duriez

Computação quântica com óptica linear e suas aplicações

Niterói-RJ

2019

Ficha catalográfica automática - SDC/BIF
Gerada com informações fornecidas pelo autor

D962c Duriez, Alan Cavalcanti
Computação quântica com óptica linear e suas aplicações / Alan Cavalcanti Duriez ; Daniel Brod, orientador. Niterói, 2019.
55 f. : il.

Trabalho de Conclusão de Curso (Graduação em Física)- Universidade Federal Fluminense, Instituto de Física, Niterói, 2019.

1. Computação quântica. 2. Óptica. 3. Produção intelectual. I. Brod, Daniel, orientador. II. Universidade Federal Fluminense. Instituto de Física. III. Título.

CDD -

Bibliotecário responsável: Mario Henrique de Oliveira Castro - CRB7/6155

Alan Cavalcanti Duriez

Computação quântica com óptica linear e suas aplicações

Monografia apresentada no programa de graduação em Física da UFF como requisito para obtenção do grau de Graduado em bacharel em Física.

Universidade Federal Fluminense – UFF

Orientador: Daniel Jost Brod

Niterói-RJ

2019

ALAN CAVALCANTI DURIEZ

COMPUTAÇÃO QUÂNTICA COM ÓPTICA LINEAR E SUAS APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Física da Universidade Federal Fluminense como requisito parcial para obtenção do título de Bacharel em Física.

Aprovado em 23 de janeiro de 2020.

BANCA EXAMINADORA

Prof. Daniel Jost Brod (Orientador – IF/UFF)

Prof. Daniel Jonathan (IF-UFF)

Prof. Antônio Zelaquett Khoury (IF-UFF)

Niterói
2020

Agradecimentos

Aos meus pais, meu mestre e meu grande amigo.

Resumo

Nesse trabalho vamos abordar computação quântica com óptica linear. Para tal, apresentaremos uma análise dos conceitos fundamentais da óptica quântica, envolvendo a quantização do campo eletromagnético, a representação dos estados de Fock e aparatos ópticos lineares.

Em seguida discutiremos aspectos básicos da computação quântica e quais recursos são necessários para construir um computador quântico, para podermos responder perguntas além das capacidades dos nossos computadores atuais. Apresentaremos também um modelo que permite realizar a computação através do processo de medida, o que será particularmente útil para implementação em óptica linear.

Por fim, uniremos esses dois ramos da física. Mostraremos como é possível codificar bits quânticos nos estados do campo eletromagnético e como gerar a dinâmica necessária para a computação sobre esses estados, discutindo possíveis obstáculos e vantagens tecnológicas.

Palavras-chaves: computação quântica, óptica linear, fótons, q-bits.

Abstract

In this work we discuss linear-optical quantum computing (LOQC). At first, we analyse the basic concepts of quantum optics, such as quantization of the eletromagnetic field, Fock state representation and linear-optical elements.

We also discuss what is quantum computing and what resources are necessary to build a quantum computer, hopefully one that can solve problems beyond the capabilities of our current computational devices. We also discuss the measurement-based model of quantum computing, which is especially suited for a linear-optical implementation.

Finally, we join this two branches of physics. We discuss how to store quantum information, or quantum bits, in the state of the eletromagnetic field and how to can generate the necesssary dynamics on these states.

Key-words: Quantum computing, optics, q-bits, photons.

Sumário

Capítulo 1

Introdução

A computação quântica é um ramo da física que obteve um destaque considerável na última década devido ao seu potencial de resolver problemas até então considerados intratáveis pelos nossos computadores atuais [1]. Por ser uma ciência nova, ainda estamos no início da caminhada que nos levará a um computador quântico capaz de resolver problemas que de fato não conseguimos resolver atualmente.

Existem diversas formas de construir um computador quântico. Essas arquiteturas envolvem a codificação da informação quântica em sistemas como armadilhas de íons, circuitos supercondutores, ressonância magnética nuclear, pontos quânticos e fótons [2]. Devido às características distintas desses sistemas físicos, cada arquitetura apresenta suas vantagens e desvantagens tecnológicas. Atualmente, empresas e grupos de pesquisa por todo o mundo estão em uma corrida para descobrir qual será a implementação definitiva.

A empresa americana Google anunciou recentemente o maior computador quântico funcional do mundo com 53 q-bits supercondutores , o que coloca essa arquitetura na atual liderança da corrida [3]. No entanto, é fato reconhecido pela própria Google que não temos a tecnologia necessária para operar mais de 400 q-bits dessa maneira. O maior desafio para q-bits supercondutores são as baixas temperaturas necessárias para a supercondutividade, o que consome muitos recursos. Portanto, para construir computadores quânticos úteis ainda é necessário buscar outras abordagens tecnológicas e arquiteturas.

Frente a esse desafio, uma alternativa popular é a computação quântica com óptica linear (*linear optical quantum computing*, ou LOQC), que envolve o processamento de q-bits fotônicos utilizando apenas elementos ópticos lineares e medidas. Um dos motivos desse destaque é o grande potencial que sistemas ópticos apresentam para a comunicação. Os fótons são partículas que tendem a preservar suas propriedades físicas mesmo se propagando por longas distâncias, o que os torna candidatos naturais para transmissão de informação quântica. Dessa forma, mesmo que a LOQC não seja a arquitetura definitiva para computação, o armazenamento e processamento de informação quântica baseada

em fótons serão necessários para a integração entre computadores quânticos ou entre seus componentes. É importante notar que, embora q-bits supercondutores tenham momentaneamente a vantagem na corrida pela implementação de computadores quânticos, grandes avanços foram feitos recentemente na área de óptica linear experimental, como um experimento com 20 fótons propagando em 60 modos [4].

Nesse trabalho vamos discutir as primeiras propostas teóricas da LOQC, que foram responsáveis por provar que é possível, em princípio, construir um computador quântico nessa arquitetura [5].

Capítulo 2

História e definições

Vamos analisar a codificação de informação em sistemas quânticos através de óptica linear, por isso se faz necessário definir o conceito mais fundamental da ótica quântica, o fóton. Neste capítulo faremos uma análise histórica de como essa ideia foi inicialmente proposta e quais experimentos e teorias foram responsáveis pelo seu estabelecimento. Em seguida faremos uma dedução teórica da quantização do campo eletromagnético para definir propriamente os conceitos mencionados nos capítulos posteriores.

2.1 A história do fóton

O conceito de fóton foi proposto pela primeira vez por Albert Einstein em seu memorável artigo "Sobre um ponto de vista heurístico relativo à produção e transformação da luz" [6], publicado em 1905. Nesse trabalho, Einstein descreve o efeito fotoelétrico dos metais com uma exatidão sem precedentes, apenas considerando que a luz (i.e., radiação eletromagnética) era composta por pacotes ou quanta de energia. Max Planck fez uma hipótese análoga em seus trabalhos sobre a radiação de corpo negro, cinco anos antes [7].

Esse modelo quantizado contradisse a teoria mais aceita da época, que descrevia a luz a partir das equações de Maxwell e, consequentemente, das equações de onda para o campo elétrico e magnético. Essas equações não impunham vínculos a respeito da continuidade do espectro de energia de uma onda eletromagnética, então era tido como fato que as energias formavam um contínuo. A teoria ondulatória da luz previa corretamente uma gama enorme de fenômenos verificados extensivamente, como por exemplo a interferência de fenda dupla, e isso atribuía-a um posto alto no arcabouço teórico da época.

Esse debate teve uma virada dramática devido aos experimentos de Arthur Compton, em 1923, nos quais ele detectou o espalhamento inelástico de raios-x por elétrons livres em um condutor [8]. No contexto da óptica, o espalhamento inelástico está associado a uma diferença entre os comprimentos de onda incidente e espalhado da onda em questão. Essa diferença de comprimentos de onda (i.e., *"Compton Shift"*) não era descrita pela

teoria clássica de espalhamento proposta por Rayleigh [9], que previa apenas espalhamento elástico para radiação incidindo sobre cargas livres. Compton descobriu esse fenômeno e propôs uma nova teoria para descrevê-lo. A ideia central de sua descrição foi tratar a radiação eletromagnética como tendo energia e momento bem definidos, analogamente ao que foi feito por Einstein no efeito fotoelétrico.

As teorias mencionadas acima obtiveram um grande sucesso experimental, no entanto não foram suficientes para comprovar a quantização da luz. Eventualmente surgiram teorias semi-clássicas que previam um campo clássico acoplado a uma matéria quantizada, como o modelo BKS proposto por Bohr, Kramers e Slater [10]. Passaram-se décadas até que a ideia de um quanta de luz fosse amplamente adotada como nos dias de hoje.

A partir da década de 80, foram realizados diversos experimentos que evidenciaram a natureza quântica da luz. Por exemplo, em 1987, foi descoberto o efeito Hong-Ou-Mandel, descrito na seção 3.4. A óptica quântica é a teoria que melhor descreve os resultados experimentais atuais, e agora vamos nos ater a essa teoria.

2.2 A quantização do campo eletromagnético

A descrição mais abrangente para a quantização da luz advém da teoria quântica de campos e da segunda quantização. Por simplicidade optaremos pela formulação da quantização canônica, e veremos que essa será suficiente para os nossos fins. Além disso, seremos breves na descrição devido ao amplo conhecimento do tema. Para uma análise mais detalhada, veja [11].

Na mecânica clássica, a descrição do movimento de sistemas oscilantes se dá por meio da análise dos modos normais de vibração, que são movimentos em que todos os graus de liberdade oscilam com a mesma frequência. Um resultado particularmente útil oriundo dessa teoria é que o Hamiltoniano de um sistema oscilante com N graus de liberdade pode ser escrito como uma soma de Hamiltonianos de N osciladores harmônicos independentes [12]. De forma análoga é possível descrever o campo eletromagnético a partir de seus modos normais. Veremos que, assim como no contexto mecânico, será possível escrever a energia do campo como uma soma de termos matematicamente idênticos a Hamiltonianos de osciladores harmônicos.

Para descrever quanticamente um sistema qualquer de forma rigorosa é necessário escrever a energia, i.e., Hamiltoniana do sistema em função de um conjunto de variáveis canônicas (q_i, p_i). Com essas variáveis, as equações de movimento tomam a forma das

equações de Hamilton:

$$\dot{q}_i = \frac{\partial H}{\partial p_i},$$
$$\dot{p}_i = -\frac{\partial H}{\partial q_i}.$$

Note que essas equações envolvem apenas uma coordenada generalizada e seu momento conjugado por vez. Em Hamiltonianos separáveis isso implica um desacoplamento entre as variáveis canônicas.

As equações de Maxwell descrevem a dinâmica do campo eletromagnético. Na ausência de cargas e correntes, elas tomam a forma

$$\boldsymbol{\nabla} \cdot \mathbf{E} = 0,$$
$$\boldsymbol{\nabla} \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t},$$
$$\boldsymbol{\nabla} \cdot \mathbf{B} = 0,$$
$$\boldsymbol{\nabla} \times \mathbf{B} = \frac{1}{c^2}\frac{\partial \mathbf{E}}{\partial t}.$$

Essas equações diferenciais parciais envolvem as seis coordenadas espaciais contínuas dos campos $\mathbf{E}$ e $\mathbf{B}$. Em função dessas coordenadas as equações de movimento acoplam os infinitos graus de liberdade do campo, e portanto não formam um conjunto de variáveis canônicas necessário para a quantização [11]. Para encontrar variáveis que desacoplem as equações de Maxwell podemos realizar uma expansão em modos normais. Sem perda de generalidade, realizaremos essa expansão a partir do potencial, $\mathbf{A}$, no calibre de Coulomb. Os campos em função desse são

$$\mathbf{B} = \boldsymbol{\nabla} \times \mathbf{A}, \tag{2.1}$$
$$\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t}. \tag{2.2}$$

A expansão dos campos em modos normais pode ser feita em termos de alguma base de funções ortonormais. Utilizaremos a expansão nos modos de Fourier, que equivale à base de ondas planas. Em aplicações físicas mais concretas, nem sempre é conveniente usar como base ondas que se estendem até o infinito com intensidade, frequência, e direção de propagação constantes. Nesses casos torna-se necessária a expansão em outros conjuntos ortonormais de funções que atendam aos vínculos impostos pela física da situação. Como estamos descrevendo o campo no vácuo, na ausência de fontes, vamos prosseguir com a expansão em Fourier. Ela é dada por

$$\mathbf{A}(\mathbf{r}, t) = \sum_l \epsilon_l \frac{A_l}{\omega_l} \left[\alpha_l e^{i\mathbf{k}_l \cdot \mathbf{r} - \omega t} + \alpha_l^* e^{-i\mathbf{k}_l \cdot \mathbf{r} - \omega t}\right], \tag{2.3}$$

onde A_l, ω_l e $\mathbf{k}_l$ são a amplitude, frequência e vetor de onda do modo l, e o versor ϵ_l indica a polarização. A função α_l e seu complexo conjugado são as variáveis normais, que aparecem como consequência da expansão em Fourier.

A partir das equações de Maxwell, é possível escrever a energia associada ao campo eletromagnético como a integral em um volume V da densidade de energia.

$$H = \frac{\epsilon_0}{2} \int_V d^3r \left[E^2 + B^2\right].$$

Se substituirmos (2.3) em (2.1) e (2.2) é possível obter a expansão em Fourier dos campos **E** e **B**. A partir dessas é possível reescrever a equação acima como

$$H = \sum_m \frac{1}{2}(P_m^2 + \omega_m^2 Q_m^2), \tag{2.4}$$

onde

$$Q_l = \sqrt{\frac{4\epsilon_0 V}{\omega_l}} A_l \,\mathrm{Re}\{\alpha\},$$
$$P_l = \sqrt{\frac{4\epsilon_0 V}{\omega_l}} A_l \,\mathrm{Im}\{\alpha\}.$$

Para essas variáveis vale

$$\frac{dQ_l}{dt} = \frac{\partial H_l}{\partial P_l},$$
$$\frac{dP_l}{dt} = \frac{\partial H_l}{\partial Q_l}.$$

Observe que a evolução temporal das variáveis depende apenas das coordenadas e momentos conjugados de cada modo. Assim, encontramos variáveis dinâmicas que atendem às equações de Maxwell e para as quais as equações de movimento do campo tomam a forma desacoplada desejada. Essas são as chamadas quadraturas do campo, e são as variáveis canônicas para o campo eletromagnético sobre as quais aplicaremos a quantização. Podemos ver que a Hamiltoniana do campo após essa mudança de coordenadas tomou a forma de uma soma de Hamiltonianas de osciladores harmônicos independentes correspondentes a cada modo normal.

Por enquanto, fizemos manipulações sobre o campo clássico para facilitar o processo de quantização. Temos agora todas as ferramentas necessárias. Como dita o processo de quantização canônica, para cada par de variáveis Q_l e P_l associamos observáveis quânticos descritos por operadores $\hat{Q}_l$ e $\hat{P}_l$ que satisfazem às relações de comutação:

$$\left[\hat{Q}_l, \hat{P}_{l'}\right] = i\hbar\delta_{l,l'}.$$

Montamos agora o operador Hamiltoniano do sistema substituindo as variáveis canônicas pelos seus respectivos operadores na expressão (2.4). O Hamiltoniano resultante é idêntico ao de um conjunto de osciladores quânticos independentes. A solução para esse Hamiltoniano é amplamente conhecida: a energia de cada oscilador é discretizada em quanta de $\hbar\omega_l$, e é possível indexar os auto-estados de energia do conjunto pelo número de

excitações ou quanta de energia em cada oscilador. Denominamos essas excitações dos modos normais do campo de fótons e chamamos os auto-estados de estados de Fock.

É possível ainda definir operadores de criação ($a_m^\dagger$) e aniquilação (a_m) para os modos individuais. Esses operadores não-hermitianos aumentam e diminuem em uma unidade, respectivamente, o número de fótons em cada modo. Seja $|n_m\rangle$ o estado correspondente a n_m fótons no modo m, escrevemos

$$a_m |n_m\rangle = \sqrt{n_m}\, |n_m - 1\rangle \,, \tag{2.5}$$

$$a_m^\dagger |n_m\rangle = \sqrt{n_m + 1}\, |n_m + 1\rangle \,, \tag{2.6}$$

$$\left[a_m, a_n^\dagger\right] = \delta_{m,n}. \tag{2.7}$$

O operador número total de fótons é definido como

$$N = \sum_l a_l^\dagger a_l,$$

onde $a_l^\dagger a_l$ é o operador número do modo l. Esse nome se justifica pois qualquer estado de Fock é autovetor desse operador e o autovalor correspondente é o número de fótons do estado. A intensidade de um feixe luminoso no contexto quântico é interpretada como o valor esperado do operador número.

Um estado importante que é singular nessa descrição é o estado que descreve a ausência de fótons, o equivalente ao vácuo material no contexto do eletromagnetismo. Esse é o chamado estado de vácuo e o denotaremos por $|\varnothing\rangle$. Se aplicarmos qualquer operador de aniquilação ao estado de vácuo, obteremos por definição o vetor nulo, pois não é possível aniquilar um quanta de um estado que não possui nenhum. Existe uma física rica por trás desse estado, que advém do fato de que a energia de um oscilador harmônico quântico desprovido de excitações não é nula, o que também ocorre para o campo eletromagnético. No entanto, não abordaremos os chamados "efeitos de vácuo quântico" aqui, pois nas aplicações práticas de computação quântica a ordem de grandeza das flutuações de energia de vácuo são muito menores do que as energias típicas dos fótons. Para uma discussão detalhada dessa fenomenologia, ver [13].

Podemos descrever estados do campo em termos dos operadores que criam esses estados a partir do vácuo. Por exemplo, considere o estado $|n_l\rangle$ que corresponde a n_l fótons em um dado modo l e seja $a_l^\dagger$ o operador de criação desse modo. Podemos escrever

$$|n_l\rangle = \frac{(a_l^\dagger)^{n_l}}{\sqrt{n_l!}} |\varnothing\rangle \,. \tag{2.8}$$

Para estados de muitos modos com números arbitrários de fótons, podemos repetir o procedimento descrito acima na ordem que desejarmos, pois os operadores de diferentes modos comutam [veja a equação (2.7)]. Um estado de Fock arbitrário pode ser escrito então como

$$|n_1, n_2, \ldots\rangle = \frac{(a_1^\dagger)^{n_1}, (a_2^\dagger)^{n_2} \ldots}{\sqrt{n_1! n_2! \ldots}} |\varnothing\rangle \,,$$

e um estado geral da radiação é uma superposição dos estado de Fock.

Para um estado de um fóton em apenas dois modos, 1 e 2, será conveniente usar a seguinte notação

$$|1,0\rangle_{12} \rightarrow \text{“fóton no modo 1”} \tag{2.9}$$

$$|0,1\rangle_{12} \rightarrow \text{“fóton no modo 2”}. \tag{2.10}$$

Ela será particularmente útil quando abordarmos a codificação q-bits utilizando fótons, na seção 5.1

2.3 Polarização

Um grau de liberdade que merece atenção pela sua popularidade na computação quântica com óptica linear é a polarização. No eletromagnetismo clássico, ela está relacionada à direção e sentido do campo elétrico, porém é possível defini-la para o campo magnético ou para potencial vetor. Considere uma onda plana de vetor de onda $\mathbf{k}$, amplitude E_o, frequência ω e versor de polarização $\hat{\mathbf{n}}$, podemos representá-la como

$$\mathbf{E}(\mathbf{r},t) = E_o e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)}\hat{\mathbf{n}}.$$

Pela lei de Gauss, temos

$$\begin{aligned} \boldsymbol{\nabla}\cdot\mathbf{E} &= 0 \\ iE_0(\mathbf{k}\cdot\hat{\mathbf{n}})e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)} &= 0 \\ \mathbf{k}\cdot\hat{\mathbf{n}} &= 0. \end{aligned}$$

Podemos ver que o vetor de polarização é sempre perpendicular à direção de propagação, isso se traduz no fato das ondas eletromagnéticas serem transversas. Para cada modo de propagação espacial, indexado por um vetor de onda, temos dois modos de polarização independentes representados por dois versores ortogonais. É possível que esses versores tenham componentes complexas, fazendo com que a direção da polarização varie no tempo e seja circular ou elíptica [14]. Por exemplo, os versores

$$\epsilon_L = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix} \quad \text{e} \quad \epsilon_R = \begin{pmatrix}1\\ -i\end{pmatrix}$$

representam as polarizações circulares no sentido anti-horário e horário, respectivamente. Se as magnitudes das componentes reais e imaginárias não forem iguais, ocorre a polarização elíptica.

Podemos ver que, mesmo classicamente, os vetores de polarização pertencem a um espaço vetorial complexo de norma unitária, ou seja, um espaço de Hilbert de dimensão dois. De fato, o espaço da polarização é isomorfo ao espaço dos estados de um sistema de

spin $\frac{1}{2}$ ou qualquer outro sistema quântico de dois níveis (q-bit). Isso torna os estados de polarização de um fóton candidatos naturais para o armazenamento de informação quântica, como veremos na seção 5.1.

De forma análoga ao que ocorre para os modos espaciais, no nível quântico as polarizações podem ser consideradas modos normais do campo, e teremos estados de Fock correspondentes. O aspecto quântico advém da possibilidade de superposição entre diferentes estados de polarização. Associamos a base dos autovetores da matriz de Pauli σ_Z às polarizações horizontal e vertical, $\{H, V\}$,

$$|H\rangle \equiv a_H^\dagger |\varnothing\rangle = |1,0\rangle_{HV} \quad \text{e} \quad |V\rangle \equiv a_H^\dagger |\varnothing\rangle = |0,1\rangle_{HV},$$

onde aqui cometemos um abuso de notação, pois no formalismo da segunda quantização os estados são definidos apenas pelo número de fótons em cada modo, então não podemos utilizar um *ket* com um parâmetro de polarização como por exemplo $|H\rangle$.

Uma outra base possível é a diagonal, que associamos aos autovetores da matriz de Pauli σ_X. Ela é dada por

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \qquad \text{e} \qquad |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle). \tag{2.11}$$

Se precisarmos considerar os graus de liberdade espacial e de polarização ao mesmo tempo, fazemos, por exemplo

$$a_{1H}^\dagger |\varnothing\rangle = |H,0\rangle_{12} \rightarrow \text{um fóton horizontal no modo 1} \tag{2.12}$$

$$a_{2H}^\dagger a_{2V}^\dagger |\varnothing\rangle = |0,HV\rangle_{12} \rightarrow \text{um fóton horizontal e outro vertical no modo 2} \tag{2.13}$$

$$a_{1H}^\dagger a_{2V}^\dagger |\varnothing\rangle = |H,V\rangle_{12} \rightarrow \text{um fóton horizontal em 1 e outro vertical em 2} \tag{2.14}$$

Utilizando combinações lineares similares podemos descrever os graus de liberdade de direção de propagação e polarização do campo. É possível também descrever outros graus de liberdade como a frequência, o tempo de emissão ou detecção (*time-bin*), perfil transverso, *etc.*. Para mais detalhes sobre esses outros modos, ver [2].

Capítulo 3

Óptica linear

Definimos o sistema físico que será o nosso q-bit e os estados que o representam. No entanto, para entender o processamento dessa informação é necessário descrever a dinâmica desse sistema. Apresentaremos o formalismo para descrever a evolução temporal dos estados de Fock a partir dos seus operadores de criação e aniquilação, e em seguida definiremos quais das dinâmicas possíveis podem ser classificadas como óptica linear e por que elas são do nosso interesse. Para exemplificar, apresentaremos alguns aparatos ópticos capazes de realizar essas dinâmicas.

3.1 Evolução dos modos

Usualmente, descrevemos a dinâmica de sistemas quânticos a partir da forma diferencial da equação de Schröedinger, que define o operador Hamiltoniano como o gerador da evolução temporal do sistema:

$$\hat{H} \left|\psi\right\rangle = i\hbar \frac{d}{dt} \left|\psi\right\rangle . \tag{3.1}$$

Escrita dessa forma, essa equação descreve transformações contínuas sobre os estados. A partir de sua solução e do estado do sistema em $t = 0$ é possível ter acesso ao sistema em um instante t arbitrário. Esse formalismo é muito útil e elegante em diversas aplicações, como por exemplo no átomo de hidrogênio e no oscilador harmônico. Em certos sistemas, todavia, pode ser muito custoso ou desnecessário descrever os estados a todo instante de tempo. Em todas as aplicações apresentadas aqui, de fato só nos interessam os estados anterior e posterior à evolução temporal, como é o caso dos divisores de feixes e deslocadores de fase descritos na seção 3.3.

Por essas razões é preferível uma formulação discreta da evolução temporal, onde o estado final é obtido aplicando um operador unitário sobre o estado inicial. A equação de

Schröedinger no caso discreto assume a forma

$$|\psi(t)\rangle = U\,|\psi(0)\rangle\,,$$
$$U = e^{-iHt/\hbar}.$$

Além disso, optaremos pela representação de Heisenberg, onde se observa a dinâmica dos operadores enquanto os estados se mantém fixos no tempo. Essa representação é particularmente conveniente na óptica por diversas razões. Uma delas é que já existe um estado por definição fixo no tempo que é o estado de vácuo, dessa forma podemos analisar a dinâmica sobre os operadores e em seguida aplicar os operadores evoluídos no vácuo de acordo com a equação (2.8). Outra vantagem é que no contexto da óptica linear as transformações sofridas pelos operadores são consideravelmente mais simples do que as sofridas pelos estados associados, como veremos na discussão sobre aparatos lineares, na seção 3.3.

Vamos mostrar como descrever a dinâmica do campo nessa representação. Seja $a^\dagger$ o operador de criação de um modo arbitrário. Se o sistema sofreu uma evolução temporal dada por U, então o operador de criação evolui para outro operador, $a^\dagger(t)$, de acordo com

$$a^\dagger(t) = Ua^\dagger U^\dagger. \tag{3.2}$$

No caso particular da óptica linear o operador $a^\dagger(t)$ pode ser identificado como outro operador de criação de algum modo que respeita às relações de comutação em (2.7).

Para obter o estado após a evolução temporal basta aplicar o novo operador de criação no vácuo, ou seja,

$$|\psi(t)\rangle = a^\dagger(t)\,|\varnothing\rangle = Ua^\dagger U^\dagger\,|\varnothing\rangle\,.$$

Para um número arbitrário de fótons em diversos modos, basta repetir o processo acima para todos os operadores de criação.

3.2 Óptica linear

No contexto do eletromagnetismo clássico, a óptica linear é um sub-conjunto das dinâmicas possíveis para a luz que envolve a propagação em meios lineares. Nesses meios vale a relação entre o campo de polarização e o campo elétrico:

$$\mathbf{P} = \epsilon_0 \chi \mathbf{E}. \tag{3.3}$$

É possível definir linearidade para o campo magnético, mas como não lidaremos com as propriedades magnéticas nesse trabalho, vamos deixar de lado essa análise. Para mais detalhes ver [14].

Podemos ver que o campo de polarização, que representa a resposta do material ao campo elétrico, é proporcional ao campo. Surpreendentemente, grande parte dos aparatos

ópticos comuns em laboratórios como lentes, divisores de feixes e placas de polarização são de fato sistemas lineares. Esses sistemas atendem a um conjunto de propriedades, são elas:

- Se luz monocromática atravessar um meio linear, a luz de saída necessariamente possui a mesma frequência da luz incidente.
- Dois campos E_a e E_b passando por um elemento linear dão origem a campos de saída, E_c e E_d, que devem ser combinações lineares dos campos de entrada. Isso é equivalente à equação matricial

$$\begin{pmatrix} E_c \\ E_d \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} E_a \\ E_b \end{pmatrix}$$

  Como veremos na seção 3.3, se houver conservação de energia a matriz acima deve ser unitária. Para mais campos de entrada a relação ainda é linear e dada por matrizes de dimensão maior.

No contexto da óptica quântica, a dinâmica é descrita a partir de transformações sobre os operadores de criação e aniquilação. Na óptica linear, essas transformações devem ser lineares, ou seja, os operadores de criação devem ser levados em combinações lineares deles mesmos pela evolução temporal. Formalmente, se o modo $a_j \in \{a_1, a_2, \dots a_k\}$ sofre uma dinâmica linear, então o operador b_j, que descreve o modo após a evolução temporal, é dado por

$$U a_j U^\dagger = b_j = \sum_k U_{jk} a_k + V_{jk} a_k^\dagger. \tag{3.4}$$

Cometemos um abuso de notação ao representar a matriz que gera a evolução temporal (U) e a matriz que dá a combinação linear entre os modos (U_{jk}) pela mesma letra. A matriz no lado esquerdo da equação acima é a mesma da equação (3.2) e atua em todo o espaço de Fock. A segunda possui dimensão m por m para um conjunto de m modos que são envolvidos na transformação linear.

Se houver conservação do número de fótons, a matriz V_{jk} deve ser nula. Além disso é necessário que a matriz U_{jk} seja unitária para que as relações de comutação fundamentais sejam mantidas.

Os Hamiltonianos que geram essa classe de dinâmicas são quadráticos nos operadores de criação e aniquilação [2]. No entanto, neste trabalho nos interessarão apenas os que contém combinações do tipo $a_n^\dagger a_m + a_m^\dagger a_n$, pelo seguinte motivo: esses Hamiltonianos aniquilam um fóton em um modo e criam em outro, de forma a manter o número total de fótons, e portanto a energia, constantes. Consequentemente, esses Hamiltonianos da chamada óptica linear *passiva* comutam com o operador número total de fótons. Divisores de feixes e deslocadores de fase ideais são exemplos de elementos lineares passivos, e trataremos apenas desse sub-grupo da óptica linear daqui em diante.

Uma limitação da óptica linear é que, apenas com elementos lineares não é possível gerar *interações* entre fótons. De fato, fótons naturalmente não interagem entre si, a não ser por não-linearidades que no geral são muito fracas ou experimentalmente difíceis de produzir. Isso se mostrará uma das maiores dificuldades para a computação com óptica linear pois, para gerar as portas de dois q-bits essenciais para a computação quântica universal (seção 4.4), é necessário que se crie emaranhamento entre os estados físicos que representam os q-bits. No entanto, é possível contornar essa dificuldade utilizando medidas para gerar não linearidades, como veremos posteriormente no protocolo KLM descrito na seção 5.2.

3.3 Aparatos ópticos

Vamos mostrar exemplos de equipamentos que são cotidianos em laboratórios de óptica quântica e que são de fato capazes de gerar transformações lineares nos operadores de criação e aniquilação dos modos. A partir desses aparatos e de detectores será possível realizar todo o processamento de informação proposto ao longo deste trabalho.

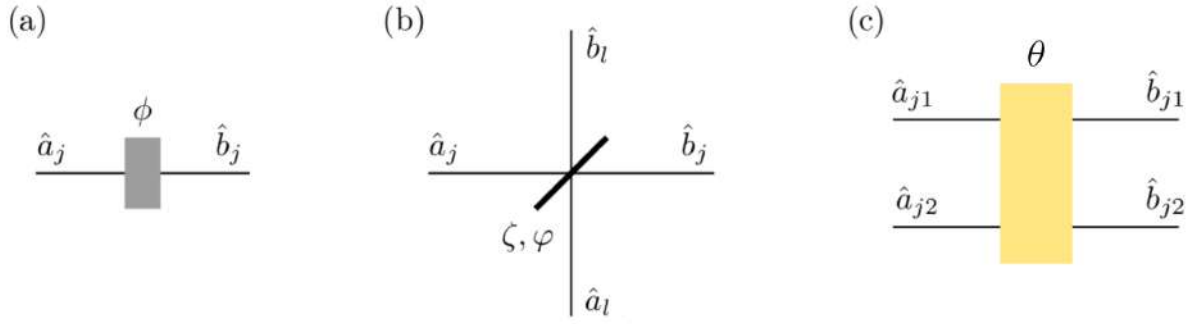

Figura 1 – Representações gráficas do deslocador de fase, divisor de feixes e placa de polarização respectivamente. Os modos indexados por b representam a saída. Em (c) temos dois modos espaciais com polarizações 1 e 2 ortogonais. Adaptada de [2].

3.3.1 Deslocador de fase

Considere um fóton no modo representado pelo operador $a_j^\dagger$, com comprimento de onda k_j incidindo sobre um dielétrico de comprimento l e índice de refração n_r [figura 1-(a)]. O fóton de saída terá as mesmas características espaciais do fóton de entrada, a não ser por uma defasagem dada por $\phi = n_r kl$. Um Hamiltoniano capaz de gerar esse "*phase shift*" é dado por

$$H(\phi) = \hbar\phi a_j^\dagger a_j,$$

que gera a transformação

$$b_j^\dagger = e^{i\phi a_j^\dagger a_j} a_j^\dagger e^{-i\phi a_j^\dagger a_j} = e^{i\phi} a_j^\dagger.$$

Na última equação usamos a relação de operadores

$$e^{\mu B} A e^{-\mu B} = A + \mu[B, A] + \frac{\mu^2}{2!}[B, [B, A]] + ...,$$

onde B é Hermitiano.

3.3.2 Divisor de feixes

Se fizermos um feixe luminoso luz incidir sobre uma peça fina feita de um material linear semi-transparente, parte será refletida e parte será transmitida e teremos dois feixes ejetados do material. A fração de luz refletida ou transmitida depende dos coeficientes de transmissão e reflexão do material. No entanto, se incidirmos dois feixes, ambos serão parcialmente refletidos e teremos novamente dois feixes de saída, mas agora cada um dos deles será composto por partes de ambos os feixes de entrada. Nesse tipo de aparato, denominado *divisor de feixes*, ocorre uma mistura de dois modos espaciais. Classicamente, podemos pensar que de fato as amplitudes de cada campo de entrada são parcialmente refletidas e transmitidas, o que faz sentido num contexto onde a energia das ondas é contínua e permite divisões infinitesimais.

Para descrever um divisor de feixes quântico não é mais possível pensar da mesma forma. Como a energia se propaga em pacotes indivisíveis, cada um deles deve ou ser refletido ou transmitido pelo divisor de feixes. Pela interpretação estatística, associamos os coeficientes de transmissão e reflexão às probabilidades de um fóton incidente ser transmitido ou refletido.

Considere dois modos incidentes denotados por $a_j^\dagger$ e $a_l^\dagger$, e dois modos de saída $b_j^\dagger$ e $b_l^\dagger$ [figura 1-(b)]. Um Hamiltoniano que descreve um divisor de feixes para esses modos é [2]

$$H_{jl} = \hbar\zeta e^{i\varphi} a_j^\dagger a_l + \hbar\zeta e^{-i\varphi} a_l^\dagger a_j,$$

onde ζ está associado à transmissividade do material e φ denota a defasagem devido a possíveis coberturas sobre a superfície semi-refletora. Fisicamente, podemos ver que esse Hamiltoniano cria um fóton no modo j enquanto aniquila outro em l e vice versa, como é esperado de um divisor de feixes.

Para obter a evolução dos modos, fazemos

$$\begin{aligned} b_j^\dagger &= e^{\frac{i}{\hbar}H_{jl}} a_j^\dagger e^{-\frac{i}{\hbar}H_{jl}} = \cos(\zeta) a_j^\dagger + i e^{i\varphi} \sin(\zeta) a_l^\dagger \\ b_l^\dagger &= e^{\frac{i}{\hbar}H_{jl}} a_l^\dagger e^{-\frac{i}{\hbar}H_{jl}} = i e^{-i\varphi} \sin(\zeta) a_j^\dagger + \cos(\zeta) a_l^\dagger. \end{aligned}$$

Podemos reescrever a expressão acima pela relação matricial

$$\begin{pmatrix} b_j \\ b_l \end{pmatrix} = \begin{pmatrix} \cos\zeta & i e^{i\varphi}\sin\zeta \\ i e^{-i\varphi}\sin\zeta & \cos\zeta \end{pmatrix} \begin{pmatrix} a_j \\ a_l \end{pmatrix}. \tag{3.5}$$

As defasagens $ie^{\pm\varphi}$ são necessárias para que transformação seja unitária, o que será essencial na seção 3.4, onde abordaremos o efeito Hong-Ou-Mandel. Podemos identificar os coeficientes de reflexão como $R = \sin^2\zeta$ e $T = 1 - R = \cos^2\zeta$ [15].

3.3.3 Placas de polarização

No divisor de feixes trabalhamos com dois modos que diferem pela direção de propagação, e não fizemos menção à polarização desses modos. No entanto, se tivermos dois feixes com mesma direção de propagação e polarizações distintas, podemos aplicar sobre esse par de feixes uma dinâmica matematicamente equivalente à do divisor de feixes, mas sobre os modos de polarização. Através da utilização de placas de meia onda e quarto de onda podemos relacionar os modos de entrada e saída de forma idêntica à equação (3.5), como indicado na figura 1-(c). Para duas polarizações H e V, basta fazer a associação $a_j \to a_H$ e $a_l \to a_V$. Os parâmetros ζ e φ nesse contexto são ângulos de rotação na esfera de Bloch ou Poincaré, que definiremos na seção 4.2.2.

Também é possível misturar os perfis espaciais e de polarização. Isso se dá por meio do PBS (*polarizing beam splitter*, ou divisor de feixes de polarização). Esse aparato separa um feixe polarizado em dois feixes com polarizações ortogonais, e as intensidades dos feixes refletido e transmitido dependem das amplitudes do feixe incidente em cada uma das polarizações selecionadas. Podemos também pensar no funcionamento do PBS no regime de fótons individuais. Considere um PBS que transmite a polarização horizontal e reflete a vertical. Se incidirmos um fóton polarizado no estado

$$|\psi\rangle = \frac{1}{2}|1,0\rangle_{HV} + \frac{\sqrt{3}}{2}|0,1\rangle_{HV}\,, \tag{3.6}$$

ele será transmitido com probabilidade $\frac{1}{4}$ e refletido com probabilidade $\frac{3}{4}$. Os tipos relevantes de PBS's estão ilustrados na figura 2.

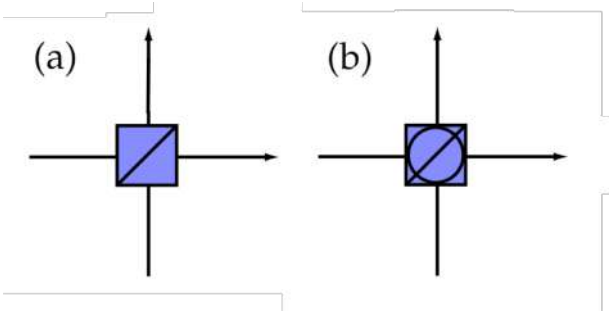

Figura 2 – Divisores de feixes de polarização nas bases (a)-$\{H, V\}$ e (b)-$\{A, D\}$ [ver equação 2.11]. Adaptada de [16].

Se agora pensarmos em dois modos espaciais de entrada l e j, a transformação

correspondente ao PBS seria [16]:

$$a_{jH} \to b_{jH}, \tag{3.7}$$

$$a_{jV} \to b_{lV}, \tag{3.8}$$

$$a_{lH} \to b_{lH}, \tag{3.9}$$

$$a_{lV} \to b_{jV}. \tag{3.10}$$

Utilizando placas de polarização e PBS's é possível separar espacialmente um feixe em quaisquer duas polarizações arbitrárias.

3.3.4 Interferômetros

Se combinarmos um divisor de feixes com um deslocador de fase é possível gerar qualquer transformação de óptica linear sobre dois modos espaciais, como indicado na equação (3.5), onde descrevemos essa dinâmica a partir de uma matriz unitária 2×2. Para N modos, podemos representar essas transformações como matrizes unitárias $N \times N$. Chamamos esses aparatos de *interferômetros N-port*, como ilustrado na figura 3.

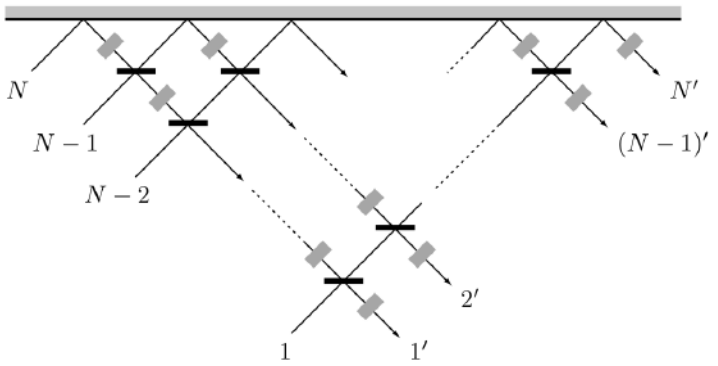

Figura 3 – Um interferômetro para realizar uma dinâmica linear sobre N modos utilizando apenas divisores de feixes e deslocadores de fase. Retirado de [2].

Um aparato óptico que mistura um grande número de modos pode ser muito complexo e de difícil implementação realista. No entanto, foi mostrado por *Reck et al (1994)* que um *N-port* arbitrário pode ser decomposto em divisores de feixes de dois modos e deslocadores fase [2][1]. Esse é um resultado crucial para a óptica linear, pois ele nos diz que podemos realizar transformações lineares arbitrariamente complexas partir de dois aparatos ópticos que são cotidianos e de fácil implementação. Essa decomposição será muito útil para o processamento de informação, pois nos permite realizar tarefas computacionais a partir de um conjunto pequeno de aparatos.

[1] Como vimos anteriormente, a descrição da dinâmica de um divisor de feixes é matematicamente idêntica à das placas de polarização atuando sobre esse grau de liberdade. Por isso é possível provar a mesma decomposição para os modos de polarização.

3.4 O Efeito Hong-Ou-Mandel

Aqui apresentaremos uma aplicação do formalismo descrito nesse capítulo que será importante quando analisarmos o emaranhamento entre fótons, na seção 4.3. Veremos como as características ondulatórias e corpusculares da luz se tornam evidentes em certos regimes, e como o formalismo da óptica quântica é capaz de descrever corretamente essa dualidade. Além disso, essa teoria prevê resultados que seriam inconcebíveis e de fato impossíveis no contexto das teorias clássicas tanto para ondas e partículas.

Considere um interferômetro de Mach-Zender [2]. Esse equipamento consiste em dois modos espaciais de entrada misturados em dois divisores de feixes com um deslocador de fase entre eles, como ilustrado na figura 4. Incidimos um feixe em um dos modos de entrada, dividindo-o no primeiro divisor de feixes. Em seguida, defasamos o segundo modo por ϕ, e após a passagem pelo segundo divisor de feixes medimos a intensidade dos campos resultantes. A defasagem em apenas um dos modos gera interferência, e para qualquer caso não trivial haverá uma diferença de intensidade entre os dois feixes de saída. Essa diferença de intensidade é completamente descrita pelo eletromagnetismo clássico, que prevê a intensidade do campo nos modos de saída do interferômetro proporcional a $(1 \pm \cos\phi)/2$.

É possível descrever esse fenômeno quanticamente. Se incidirmos um fóton sobre esse interferômetro, a probabilidade de o detectarmos no mesmo modo na saída é também $(1 + \cos\phi)/2$. O interessante é que as visões quântica e clássica preveem os mesmos resultados nesse experimento. No geral, se consideramos que a luz é formada por pacotes e descrevemos a dinâmica desses pacotes a partir dos campos clássicos, conseguimos prever todos os fenômenos de um único fóton. Podemos dizer que fótons isolados obedecem a uma mecânica ondulatória clássica. Veremos as consequências desse fato para a capacidade da óptica linear de realizar computação quântica (seção 5.1).

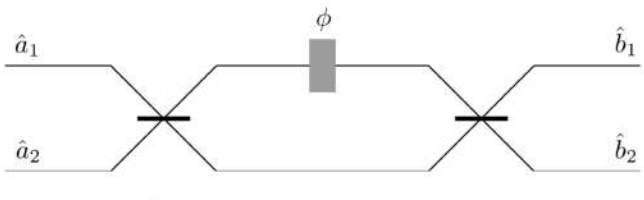

Figura 4 – Interferômetro de Mach-Zender com um deslocador de fase no primeiro modo. Retirado de [2]

.

O quadro muda se analisarmos a interferência de mais de um fóton. Considere um divisor de feixes 50:50, podemos representar a transformação correspondente substituindo

$\zeta = \frac{\pi}{4}$ e $\varphi = \frac{\pi}{2}$ na equação (3.5). A matriz resultante é

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

Se incidirmos dois fótons idênticos sobre o divisor de feixes, denotados pelos modos de entrada $a_j^\dagger$ e $a_l^\dagger$, o estado inicial será caracterizado pelo operador $a_j^\dagger \otimes a_l^\dagger \equiv a_j^\dagger a_l^\dagger$. Podemos obter a transformação sobre os modos aplicando a matriz acima sobre esses operadores. Ela é

$$b_j^\dagger = \frac{1}{\sqrt{2}}(a_j^\dagger - a_l^\dagger),$$
$$b_l^\dagger = \frac{1}{\sqrt{2}}(a_j^\dagger + a_l^\dagger).$$

Portanto o divisor de feixes gera a transformação

$$a_j^\dagger a_l^\dagger \to \left(\frac{a_j^\dagger - a_l^\dagger}{\sqrt{2}}\right)\left(\frac{a_j^\dagger + a_l^\dagger}{\sqrt{2}}\right) = \tfrac{1}{2}(a_j^\dagger a_j^\dagger + a_j^\dagger a_l^\dagger - a_l^\dagger a_j^\dagger - a_l^\dagger a_l^\dagger). \tag{3.11}$$

Se os dois fótons de entrada forem rigorosamente idênticos, podemos aplicar as relações de comutação fundamentais de (2.7), e teremos que os dois termos do meio na equação acima se cancelam, obtendo o estado final

$$\frac{1}{2}((a_j^\dagger)^2 - (a_l^\dagger)^2)\,|\varnothing\rangle = \frac{|2,0\rangle_{jl} - |0,2\rangle_{jl}}{\sqrt{2}}. \tag{3.12}$$

Podemos ver que existe zero probabilidade dos dois fótons saírem por modos diferentes. Pensando em fótons não idênticos, aqui indexados por a e b, incidindo sobre o divisor de feixes, teríamos quatro possibilidades para a reflexão ou transmissão:

- Caso 1: Os dois fótons são transmitidos.
- Caso 2: Os dois fótons são refletidos.
- Caso 3: O fóton a é refletido e o fóton b é transmitido
- Caso 4: O fóton a é transmitido e o fóton b refletido.

Os casos estão ilustrados na figura 5, e estão associados aos quatro termos da equação (3.11). A não ocorrência dos casos 1 e 2 é o chamado efeito Hong-Ou-Mandel (HOM). Observe como esse é um efeito genuinamente quântico no sentido de que se descrevêssemos os fótons a partir de uma mecânica ondulatória clássica obteríamos probabilidades diferentes de zero para os quatro casos.

Uma das interpretações do efeito HOM é que, pelo fato dos fótons serem idênticos, é impossível distinguir os estados dos casos 1 e 2, e a mudança de fase causada pelo divisor

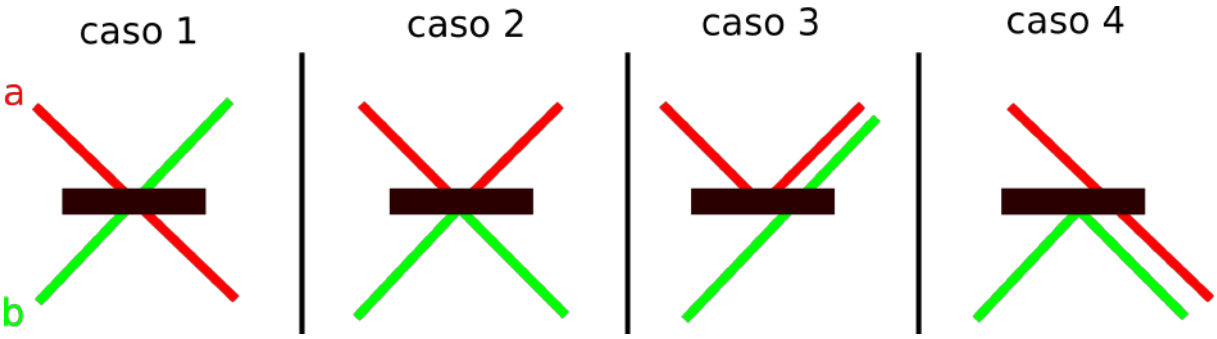

Figura 5 – Casos possíveis de reflexão e transmissão de dois fótons incidindo sobre um divisor de feixes

de feixes faz com que as amplitudes relacionadas a esses estados se cancelem. Dizemos que ocorreu uma interferência destrutiva entre dois fótons. Note a diferença em relação à interferência de um fóton analisada no início dessa seção.

Um detalhe importante é que o efeito HOM reflete a natureza bosônica dos fótons. Se realizássemos um experimento análogo com férmions idênticos, ocorreriam sempre os casos 1 e 2, enquanto os casos 3 e 4 teriam probabilidade 0. Isso se deve ao fato das relações de comutação fundamentais de férmions envolverem o anti-comutador dos operadores de criação [13] ao invés do comutador como na equação (2.7). Esse experimento demonstra que férmions tendem a ficar em estados distintos enquanto bósons tendem a ocupar o mesmo estado. De fato, o análogo ao efeito HOM para o caso fermiônico é o princípio da exclusão de Pauli. Dizemos que esses são *efeitos de partículas idênticas*.

Em computação quântica, sempre damos atenção a efeitos puramente quânticos que contrastam com as nossas intuições clássicas. Exemplos são efeitos de partículas idênticas e violações da desigualdade de Bell (seção 4.3). Esses efeitos tornam a computação genuinamente quântica, no sentido de permitir os computadores quânticos realizar tarefas que um computador clássico não conseguiria. Analisaremos em detalhe essas e outras propriedades do processamento de informação quântica no próximo capítulo, para então unir todos esses conceitos posteriormente.

Capítulo 4

Computação Quântica

Vamos deixar a óptica de lado momentaneamente para falar sobre computação quântica. Discutiremos um pouco os conceitos mais básicos da computação clássica, e como podemos traduzi-los para o contexto quântico. Em seguida mostraremos como o emaranhamento de sistemas pode ser interpretado no escopo dessa teoria, e como ele é uma ferramenta fundamental para os futuros computadores quânticos. Também abordaremos a ideia de computação quântica universal, que é o ponto de partida teórico que utilizaremos para abordar computação quântica com óptica linear (LOQC). Ao final apresentaremos uma importante aplicação que é o teletransporte quântico, que apesar de simples possui um grande potencial para comunicações e também para LOQC.

4.1 Computação Clássica

A criação dos computadores revolucionou a tecnologia no final do século XX, e nos dias de hoje praticamente todas as nossas atividades estão de alguma forma ligadas à esses dispositivos. Tudo isso se deve à excelente capacidade dos computadores atuais de resolver problemas que nós seríamos incapazes de resolver pela nossa própria capacidade computacional.

A função de um computador, em última instância, é realizar um processamento de informação, que nada mais é do que realizar uma tarefa específica sobre algum objeto de entrada. Fisicamente, isso significa receber um sistema físico que codifique uma informação e realizar sobre ele alguma dinâmica específica para que o novo sistema codifique corretamente a informação do resultado da computação. Para o contexto real, os nossos computadores recebem conjuntos de informação codificada em bits, e realizam um conjunto de transformações controladas sobre esses bits para obter novos bits de saída.

O bit é a unidade mais fundamental de informação abstrata, que pode assumir apenas dois valores, 0 ou 1, sim ou não, mais ou menos, *etc.* Qualquer conjunto binário de elementos pode ser interpretado como um bit. Transformações sobre bits podem ser

entendidas como funções que relacionam um conjunto de bits a outro, assim como funções reais relacionam $\mathbb{R}\to\mathbb{R}$. Em computação chamamos essas operações sobre bits de *portas lógicas.*

Se pensarmos em apenas um bit, existem quatro portas possíveis.

- A identidade, que não altera o valor do bit.
- A porta NOT, que troca o valor do bit de 0 para 1 e vice-versa.
- A porta constante igual a 0, correspondente à função $f(x) = 0$.
- A porta constante igual a $f(x) = 1$.

Para dois bits existem diversas portas, por exemplo as portas AND, OR e NAND, descritas na tabela abaixo.

Entradas		Saídas		
		AND	OR	NAND
0	0	0	0	1
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

Tabela 1 – Tabela verdade das portas lógicas AND, OR e NAND.

Na ciência da computação, é desejável resolver as tarefas utilizando um mesmo conjunto finito de portas lógicas. De fato, os nossos computadores precisam ser programados com uma quantidade finita de informação. Além disso, é tecnologicamente mais simples implementar um computador que opera com poucas portas. Os *transistores*, por exemplo, só são capazes de aplicar a porta NAND. Utilizando apenas essa porta é possível realizar qualquer tarefa computacional, e por isso a chamamos de *universal* para a computação clássica, como mostrado em [1]. Um circuito de portas NAND está ilustrado na figura 6. Analogamente, é possível definir um conjunto universal de portas para a computação quântica, como veremos na seção 4.4.

Apesar da porta NAND ser universal, existem tarefas que precisam de um número tão grande de aplicações dessa porta que nós os consideramos intratáveis. De fato, muitos problemas conhecidos hoje precisariam de mais que a idade do universo para serem resolvidos mesmo com os supercomputadores atuais. A teoria de *complexidade computacional* é um ramo da ciência da computação que tem como um dos objetivos classificar os problemas conhecidos de acordo com o tempo necessário para resolvê-los, ou sua *complexidade.*

Uma das classes de complexidade importantes dessa teoria é a classe **P**. Dizemos que uma tarefa computacional está em **P** se a quantidade de portas universais necessárias

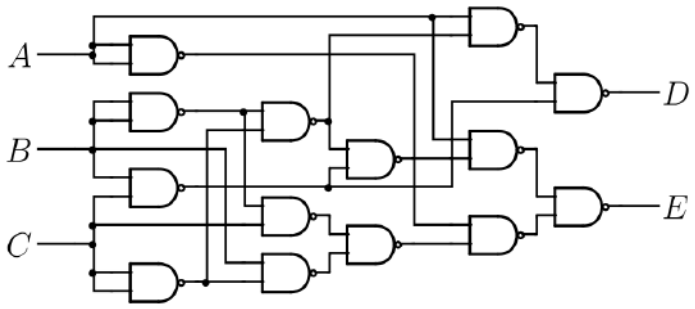

Figura 6 – Uma computação clássica arbitrária que envolve apenas a porta NAND. Aqui temos três bits de entrada {A,B,C} e dois de saída {A,B,C}.

para realizá-la cresce no máximo como um polinômio com o tamanho do problema a ser resolvido. Por exemplo, calcular o produto de duas matrizes $N \times N$ pelo método algébrico está em **P**, pois requer da ordem de N^3 portas. A classe **P** engloba as tarefas que podem ser resolvidas *eficientemente* por computadores clássicos. Existem definições mais formais dessa e de outras classes de complexidade em [1].

4.2 Bits Quânticos

4.2.1 Um novo paradigma de informação

Para que seja possível a implementação de bits em computadores de fato, é necessário que exista algum sistema físico responsável por representar os valores 0 ou 1. Em princípio, qualquer sistema de dois estados (clássico) pode ser um bit, como por exemplo uma moeda apoiada sobre um plano, onde associamos "cara"$\rightarrow$ 0 e "coroa"$\rightarrow$ 1.

Nos dias de hoje, o sistema físico mais utilizado para esse fim são os *transistores*. Esses são os dispositivos semicondutores que compõe os nossos processadores. Com eles é possível realizar a codificação e computação dos bits em um circuito elétrico. Em poucas palavras, o valor (ou *estado*) de um bit depende da passagem ou da ausência da corrente por um dado ponto do circuito.

Tanto as moedas quanto os circuitos de transistores podem ser descritos pelas leis da mecânica e do eletromagnetismo clássico, e por isso dizemos que o bit é uma unidade de informação clássica. Existem sistemas, no entanto, que se comportam de acordo com conjunto distinto de leis fundamentais, os chamados sistemas quânticos. Podemos usar as propriedades únicas desses sistemas para idealizar uma nova unidade de informação. Definimos o bit quântico (*q-bit*) como um sistema de dois níveis abstrato. Esses sistemas podem ser descritos por um espaço de Hilbert bidimensional formado por combinações lineares (ou *superposições*) de dois vetores ortogonais que associaremos aos valores 0 e 1. Dizemos que esses vetores formam a *base computacional*. O estado de um q-bit arbitrário

pode ser escrito como

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{4.1}$$

onde $|\alpha|^2$ e $|\beta|^2$ são as probabilidades de se medir o valor desse q-bit nos valores 0 e 1, respectivamente. Segue disso que $|\alpha|^2 + |\beta|^2 = 1$, e isso garante a normalização do espaço de Hilbert.

É possível observar o valor de um bit clássico sem que seu valor seja alterado. No entanto uma medida de um q-bit colapsa o seu estado para um dos estados determinados 0 ou 1, i.e., as medidas destroem a superposição. Por essa propriedade de sistemas quânticos é necessário que se tome cuidado adicional durante a computação. Em diversos casos realizamos toda a computação sem medir o estado para preservar a informação contida nas amplitudes da superposição.

4.2.2 Portas de um q-bit

Assim como na computação clássica, é possível definir portas lógicas que atuam sobre um conjunto de q-bits. Trataremos inicialmente das portas que atuam sobre apenas um, e veremos como já aparecem diferenças drásticas do caso clássico.

Para apenas um bit, existem apenas quatro portas possíveis, como vimos na seção 4.1. Isso se deve ao fato do bit ser caracterizado por um número inteiro que pode assumir apenas dois valores. O q-bit, no entanto, é definido por duas amplitudes complexas e contínuas α e β, e qualquer transformação sobre essas amplitudes irá necessariamente alterar o estado do q-bit. De fato existe um conjunto infinito não enumerável de estados de um q-bit, e isso leva também a um conjunto igualmente infinito de transformações nesses q-bits.

Como um q-bit é um sistema quântico representado por um vetor, podemos pensar nas portas lógicas como operadores no espaço desses vetores. No entanto, é necessário que esses operadores ou transformações lineares preservem a normalização dos estados, ou seja, devem ser unitários.

Portas notáveis para um q-bit são dadas pelas quatro matrizes de Pauli, são elas:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{4.2}$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.3}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{4.4}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4.5}$$

Podemos identificar a porta X como o análogo quântico da porta NOT da computação clássica, visto que sua atuação nos elementos da base computacional é levar $|0\rangle$ em $|1\rangle$ e vice versa. Seus autovetores são

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{4.6}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4.7}$$

e os de Y são

$$|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \tag{4.8}$$

$$|\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle). \tag{4.9}$$

Os autovetores de Z são os próprios vetores da base computacional. As matrizes de Pauli são uma base para o espaço das matrizes complexas unitárias 2×2, ou seja, a partir de combinações lineares delas é possível gerar qualquer operação de um q-bit.

Um fato importante sobre transformações unitárias é que elas podem ser interpretadas como rotações e reflexões em um espaço vetorial abstrato. Existe uma forma muito conveniente para representar estados e operadores de um q-bit que se baseia nessa idealização. Como podemos descrever os estados a partir de dois parâmetros complexos, podemos fazer a parametrização

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\,. \tag{4.10}$$

Podemos associar os parâmetros θ e ϕ aos ângulos polar e azimutal das coordenadas de um ponto sobre a superfície de uma esfera de raio unitário, e a cada ponto associamos um estado, de acordo com a figura 7. Essa é a chamada representação da *esfera de Bloch*. Os estados sobre os eixos x, y, z da esfera são os autovetores das matrizes de pauli X, Y, Z.

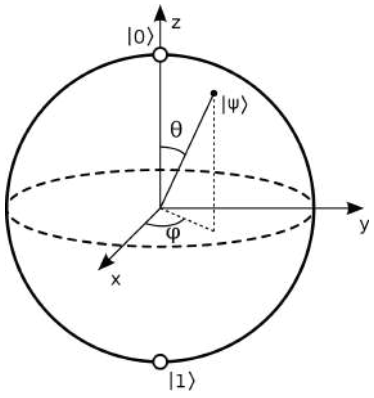

Figura 7 – Um q-bit arbitrário representado na esfera de Bloch.

A grande vantagem dessa representação é que podemos interpretar as portas de um q-bit como rotações sobre essa esfera, e podemos identificá-las a partir de um eixo e

um ângulo de rotação específicos. Por exemplo, a porta *Hadamard*, fundamental para a computação quântica, dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{4.11}$$

pode ser entendida como uma rotação de π sobre o eixo da direção do versor $\hat{n} = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ na esfera de Bloch [1]. Essa porta leva $|0\rangle \to |+\rangle$, $|1\rangle \to |-\rangle$ e vice-versa. Sempre que é necessário gerar superposição de algum q-bit podemos utilizar essa porta, e por isso ela aparece em grande partes dos algoritmos quânticos.

A partir das exponenciais complexas das matrizes de Pauli é possível gerar operadores de rotação em torno dos eixos cartesianos da esfera de Bloch, um exemplo delas é a rotação de um ângulo ξ em torno do eixo x

$$R_x(\xi) \equiv e^{-i\xi X/2} = \begin{bmatrix} \cos\frac{\xi}{2} & -i\sin\frac{\xi}{2} \\ -i\sin\frac{\xi}{2} & \cos\frac{\xi}{2} \end{bmatrix},$$

onde usamos o fato de que para um unitário A tal que $A^2 = I$, então

$$e^{iAx} = \cos(x)I + i\sin(x)A. \tag{4.12}$$

Outra porta interessante é a porta que aplica um fase relativa ϕ entre as duas amplitudes de um q-bit, a porta de *fase*:

$$F(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}. \tag{4.13}$$

Veremos na seção 5.1 que as portas Hadamard e $F(\phi)$ são facilmente implementadas fisicamente com o uso de divisores de feixes e deslocadores de fase.

4.3 Emaranhamento e portas de dois q-bits

Os estados que representam diversos q-bits são representados em um espaço de Hilbert que é o produto tensorial dos espaços de cada q-bit. Para dois q-bits, por exemplo, a base computacional seria o conjunto $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. No caso geral, o espaço para n q-bits possui dimensão 2^n.

Pelas propriedades dos espaços vetoriais formados por produtos tensoriais, existem certos vetores que não podem ser escritos como produto tensorial dos estados dos subsistemas. Quando um sistema se encontra nesses estados ditos *emaranhados*, não podemos descrever cada parte do sistema separadamente. É como se de alguma forma as componentes perdessem a individualidade e se comportassem apenas como um todo inseparável. Por exemplo, considere o estado de Bell:

$$|\beta_{00}\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}. \tag{4.14}$$

De fato ele não pode ser escrito como um produto de dois estados de um q-bit, ou seja, não existem $\alpha, \beta, \gamma, \delta$ tais que:

$$|\beta_{00}\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle)(\gamma\,|0\rangle + \delta\,|1\rangle). \tag{4.15}$$

O emaranhamento entre sistemas é uma propriedade que só pode ser entendida pelas leis da mecânica quântica, e por isso existem fenômenos causados pelo emaranhamento que contrastam com as nossas noções cotidianas (e clássicas) de realidade. Esse contraste instigou um intenso debate entre a comunidade científica, marcado pelo famoso artigo de Einstein, Podolsky e Rosen (EPR): "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" [17], publicado em 1935. Nesse trabalho os autores apresentam um experimento mental para investigar a "estranha ação à distância" causada pelo emaranhamento. A conclusão final de EPR é que a mecânica quântica não é uma descrição completa da realidade pois as correlações previstas entre sistemas emaranhados violam princípios naturais que para eles eram necessariamente atendidos:

- ***Realismo***: Os observáveis físicos possuem valores bem definidos a todo instante de tempo, independente da medida por um observador.
- ***Localidade***: Só pode haver influência de um ponto do espaço até outro se houver algum ente, como um *campo*, no espaço entre eles responsável por propagar essa informação. Como o mediador de informação mais rápido conhecido é o campo eletromagnético, o princípio da localidade implica diretamente que nenhuma informação pode se propagar numa velocidade superior à da luz, um dos postulados da relatividade restrita.

Essas duas premissas constituem o paradigma do realismo local. De fato as leis da mecânica quântica são incompatíveis com essas duas hipóteses. [1]

Para EPR a natureza não poderia ser descrita por uma teoria intrinsecamente probabilística. Eles acreditavam em um conjunto variáveis ocultas não previstas pela mecânica quântica, e que as previsões probabilísticas das superposições são apenas uma aproximação estatística da descrição determinística do sistema a partir das variáveis ocultas.

Em 1964, John Bell deu sequência ao debate no seu artigo *"On the Einstein-Podolsky-Rosen Paradox"* [18], onde apresenta um conjunto de resultados revolucionários para o nosso entendimento da natureza. Primeiramente, ele deduz uma desigualdade envolvendo as correlações entre sistemas emaranhados que qualquer teoria de variáveis ocultas realista e local deve satisfazer, a chamada desigualdade de Bell. Em seguida, ele mostra que as correlações previstas pela mecânica quântica em certos casos podem violar essa desigualdade. Bell conclui seu trabalho afirmando que a natureza de fato não pode ser realista e local e

que a mecânica quântica fornece uma descrição completa da natureza, pelo fato dos valores dos observáveis não estarem definidos até que seja feita uma medida. Em suas palavras: "*As previsões estatísticas da mecânica quântica são incompatíveis com predeterminação separável*".

Violações da desigualdade de Bell são uma das propriedades mais misteriosas dos sistemas quânticos, e é possível utilizar essa propriedade para realizar tarefas computacionais impossíveis para computadores clássicos. Como o emaranhamento é responsável por esse comportamento puramente quântico, ele é um recurso essencial para a computação quântica, e a principal forma de criar estados emaranhados é através das chamadas *portas de dois q-bits*.

Analogamente aos estados emaranhados, existem portas que não podem ser escritas como produto tensorial de portas de dimensão menor. Chamaremos essas de portas de dois q-bits. Um fato importante sobre essa classe de operadores é que, com exceção da porta SWAP (que troca o estado de dois q-bits), eles são capazes de gerar emaranhamento entre os q-bits, i.e., se aplicarmos uma porta desse tipo em algum estado produto como o da equação (4.15), geralmente obtemos um estado emaranhado como resultado. A simples tarefa de preparar um estado de Bell a partir de estados da base computacional não pode ser realizada apenas com produtos tensoriais de portas de um q-bit, como é mostrado em [1]. De fato a grande maioria dos protocolos de computação quântica requerem a atuação de alguma porta de dois q-bits.

Uma importante porta desse tipo é a porta *controlled-not*, C-NOT ou C-X. Essa porta atua sobre a base computacional assim como a porta C-NOT clássica atua sobre dois bits. Sua atuação equivale a alterar o valor do segundo bit (q-bit alvo) se o primeiro (q-bit de controle) estiver no estado $|1\rangle$. Como essa porta realiza uma operação no segundo q-bit condicionada no valor do primeiro, não podemos pensar em como ela atua em cada um dos q-bits separadamente, o que justifica ela ser uma porta de dois q-bits. A representação matricial da porta C-X é

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4.16}$$

Outra porta que será essencial no contexto da óptica linear é a porta C-Z, que aplica uma porta Z sobre o segundo q-bit condicionada no valor do primeiro. Sua representação matricial é

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{4.17}$$

4.4 Computação Quântica Universal

Na seção 4.1 mencionamos que qualquer problema computacional pode ser resolvido por um conjunto finito de portas que chamamos de universais, por mais complexo que o problema seja. Também vimos que o número de portas utilizadas para realizar a tarefa é uma medida dos recursos necessários para tal. Se for necessária uma quantidade exponencial de recursos, consideramos que o problema não pode ser resolvido eficientemente por um computador clássico.

Vamos apresentar um raciocínio análogo para a computação quântica. É necessário quantificar de alguma forma os recursos necessários para resolver problemas para que possamos implementar um computador quântico funcional. Além disso, essa análise nos permitirá inferir quais problemas são possíveis de se resolver por um computador quântico.

Assim como no caso clássico é preciso encontrar um conjunto de portas quânticas universais. Uma computação quântica arbitrária sobre n q-bits é equivalente a uma operação unitária sobre estados de dimensão 2^n, e podemos representar essa transformação como uma matriz unitária $2^n \times 2^n$. Para realizar uma dinâmica desejada sobre esses estados precisamos encontrar um conjunto finito de operadores unitários capazes de gerar todos as outros, e aqui ilustraremos o raciocínio para encontrá-los. Alguns detalhes dessa prova fogem ao escopo deste trabalho, para uma demonstração detalhada veja [1].

O raciocínio se baseia uma sequência de resultados da álgebra linear:

- É possível decompôr qualquer matriz unitária de dimensão d em $d(d-1)/2$ matrizes de dois níveis. Essas matrizes por definição atuam em apenas dois elementos da base por vez.
- Toda matriz de dois níveis pode ser decomposta em produtos de C-X e portas de um q-bit. Aqui deixamos o produto tensorial com a identidade nas demais dimensões implícito.
- Toda porta de um q-bit pode ser aproximada com precisão arbitrária a partir das portas Hadamard e T, definida por

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Esse último decorre do fato que a porta $THTH$ é uma rotação de um ângulo θ definido implicitamente por $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$ ao redor do eixo $\hat{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ na esfera de Bloch, enquanto a porta $HTHT$ é uma rotação do mesmo ângulo ao redor do eixo $\hat{m} = (\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$. Um fato importante é que o ângulo θ é um múltiplo irracional de π. Assim, podemos ligar dois pontos quaisquer do ciclo trigonométrico a partir de

rotações sucessivas de θ. Consequentemente, a partir de H e T é possível gerar rotações de ângulos arbitrários ao retor dos dois eixos não paralelos $\hat{n}$ e $\hat{m}$.

Um resultado importante da mecânica analítica é que qualquer rotação em três dimensões pode ser decomposta em três rotações ao redor de dois eixos não paralelos, o que chamamos decomposição em *ângulos de Euler* [12]. Como o espaço de transformações sobre um q-bit é isomorfo ao espaço das rotações em três dimensões, é possível fazer uma decomposição análoga. De fato, qualquer porta U pode ser escrita como

$$U(\alpha, \beta, \gamma) = R_{\hat{n}}(\alpha) R_{\hat{m}}(\beta) R_{\hat{n}}(\gamma),$$

onde α, β e γ podem ser interpretados como os ângulos de Euler.

As portas Hadamard e T são capazes de gerar essas rotações, logo podem gerar qualquer porta de um q-bit. Combinando esses resultados, concluímos que o conjunto formado pelas portas C-X, H e T é universal para a computação quântica.

Podemos finalmente definir que uma dada tarefa pode ser realizada eficientemente por um computador quântico se o número de portas universais necessária para a computação cresce no máximo com um polinômio com o tamanho do problema.

Note que investigamos se é possível ou não gerar todas as portas com esse conjunto universal, e não nos preocupamos com a eficiência. Surpreendentemente, todos os processos da decomposição descritos acima requerem um número polinomial de portas, com exceção de um. Vimos que podemos decompôr um unitário de dimensão d em $d(d-1)/2$ matrizes de dois níveis. No entanto, d cresce exponencialmente com o número de q-bits, então decompôr um unitário de n q-bits requer $2^n(2^n-1)/2 \sim 2^{2n}$ portas de um ou dois q-bits, o que não é eficiente. Podemos ver que no geral as tarefas requerem um número exponencial de portas, isso reflete o fato de que existem tarefas intratáveis até para um computador quântico.

Podemos encontrar outros conjuntos universais buscando portas que simulem o conjunto descrito acima. Dependendo da implementação física escolhida para construir o computador quântico, certos conjuntos podem ser mais tecnologicamente vantajosos que outros. Por exemplo para implementação com óptica linear a porta C-Z é mais simples de implementar do que a porta C-X, e convém escolher um conjunto universal que a contenha.

4.5 Aplicação: Teletransporte Quântico

Considere o seguinte problema: Duas pessoas, Alice e Bob estão separadas por uma longa distância e Alice deseja enviar um q-bit em um estado desconhecido $|\psi\rangle$ para Bob. Supomos que é possível realizar comunicação clássica entre as partes.

Se o problema fosse enviar um bit clássico, bastaria Alice medir o valor do seu bit e enviá-lo para Bob através do canal de comunicação. Por se tratar de um sistema clássico,

uma medida do valor do bit não provoca nenhuma influência sobre o seu estado, e esse estado pode ser determinado univocamente com apenas uma medida.

No caso quântico, o problema se complica. O q-bit é caracterizado por uma superposição dada por duas amplitudes complexas. Se realizarmos uma medida sobre o q-bit, colapsamos a superposição para um dos dois estados da base computacional e a informação contida nas amplitudes é perdida. O máximo que Alice pode fazer é aplicar portas sobre o seu q-bit e realizar medidas. Com o resultado de apenas uma medida Alice vai obter apenas o valor 0 ou 1, e toda a informação contida nas amplitudes será perdida.

Essa dificuldade de descobrir toda a informação sobre o sistema é uma consequência do fato que as amplitudes das superposições dos sistemas quânticos não são considerados observáveis físicos, e é impossível ter acesso à elas através de medidas em uma cópia do sistema.

Para realizar essa tarefa precisamos de uma abordagem diferente: é necessário que se mantenha o estado em superposição para que a informação não se perca, e utilizaremos as propriedades do emaranhamento para fazê-lo. A ferramenta fundamental para esse processo é um estado de Bell da equação (4.14). Considere que é possível separar espacialmente os dois q-bits desse estado e entregá-los a Alice e Bob. Dessa forma, Alice fica com o q-bit $|\psi\rangle$ e uma das partes do par emaranhado, enquanto Bob fica com a outra. O estado inicial dos três q-bits é portanto:

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle \\ &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ &= \frac{1}{\sqrt{2}}\left[\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)\right] \end{aligned}$$

Agora Alice aplica uma porta C-X entre os seus dois q-bits para gerar emaranhamento entre eles, e em seguida é aplicada uma Hadamard ao primeiro q-bit. Esse processo está

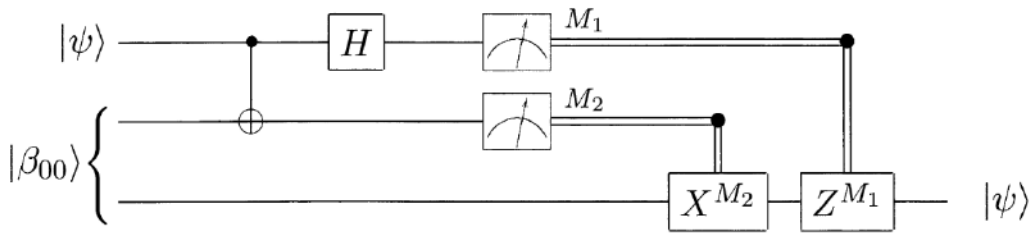

Figura 8 – Teletransporte quântico representado no modelo de circuitos. As linhas horizontais representam os q-bits. As portas aplicadas vão da esquerda para a direita, sendo a primeira porta a C-X. O símbolo $\oplus$ indica o q-bit de alvo. Retirado de [1]

ilustrado no diagrama de circuitos da figura 8. O estado após essas operações é

$$\begin{aligned}|\psi_1\rangle =& \frac{1}{2}\Big[|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) \\ &+ |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)\Big]\end{aligned}$$

Agora Alice mede os seus dois q-bits na base computacional (essa sequência de C-X, Hadamard e medida são chamados de medida na base de Bell). Essa medida gera uma influência dinâmica sobre o q-bit na posse de Bob: o estado desse q-bit antes da medida era uma superposição de todos os termos entre parênteses na equação acima, e a medida induz um colapso dessa superposição em um desses quatro estados.

O ponto mais importante é que o resultado da medida de Alice nos permite saber para qual das quatro possibilidades o estado de Bob colapsou. Se Alice utilizar o canal de comunicação para informar a Bob o resultado de sua medida, ele será capaz de recuperar o estado $|\psi\rangle$ realizando operações de acordo com a informação dada. Por exemplo, se Alice medir o estado $|00\rangle$, então Bob sabe que seu q-bit já está no estado $|\psi\rangle$ e nenhuma operação é necessária. Se for medido o estado $|11\rangle$, Bob precisa realizar uma porta X e em seguida trocar o sinal da amplitude relacionada ao estado $|1\rangle$, que pode ser feita aplicando a porta Z.

Uma ressalva é necessária. O teletransporte quântico não viola o princípio da causalidade, pois a informação sobre o q-bit de Alice só chega a Bob no momento que é feita a comunicação clássica entre eles, e essa necessariamente é transmitida no máximo na velocidade da luz.

4.6 Computação baseada em medidas

Toda computação quântica consiste em realizar uma dinâmica específica sobre um sistema quântico. As diversas arquiteturas para computadores quânticos existentes utilizam formas diferentes de gerar essa dinâmica. Até agora descrevemos a computação a partir de uma transformação unitária atuando sobre o estado que codifica a entrada do problema. O *modelo de circuitos* que utilizamos para descrever o protocolo de teletransporte é um exemplo dessa evolução unitária, e é útil pois permite uma representação didática. Em alguns sistemas físicos é possível implementar esse modelo. Existem, no entanto, formas alternativas de se realizar computação universal que não se baseiam em aplicar operações diretamente sobre os q-bits. Existe um modelo no qual é possível aplicar medidas adaptativas sobre um estado emaranhado de diversos q-bits para que a influência das medidas propague a dinâmica. Essa é a chamada computação baseada em medidas e nessa seção vamos mostrar como ela pode ser realizada.

Começamos mostrando uma forma de aplicar uma porta Z em um q-bit apenas utilizando medidas adaptativas. Considere o q-bit de entrada no estado $|\psi\rangle$ e um q-bit

auxiliar (ou *ancilla*) inicializado em $|0\rangle$. O procedimento consiste em gerar emaranhamento entre os dois q-bits para em seguida realizar uma medida sobre o primeiro q-bit, o que pode ser obtido pelo circuito da figura 9.

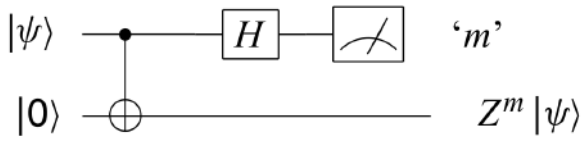

Figura 9 – Porta Z por medidas. Retirado de [2].

Note a semelhança com o protocolo de teletransporte quântico, descrito na seção anterior. Podemos encarar a porta Hadamard seguida da medida de uma medida na base dos autovalores de X [equações (4.6) e (4.7)]. Pensando dessa forma esse protocolo só envolve a porta C-X seguida de uma medida.

Analisando a evolução dos estados, considerando $|\psi\rangle$ como um q-bit genérico [equação (4.1)], o estado de entrada é

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle$$

e o estado antes da medida é

$$\frac{|0\rangle}{\sqrt{2}} \otimes (\alpha|0\rangle + \beta|1\rangle) + \frac{|1\rangle}{\sqrt{2}} \otimes (\alpha|0\rangle - \beta|1\rangle).$$

Podemos ver que se a medida resultar 0 o processo não aplica porta alguma. Portanto é necessário que se realize o processo novamente até que se obtenha o resultado desejado. O importante é que o algoritmo em si pode mudar dependendo das medidas. Por isso dizemos que essa computação requer *medidas adaptativas*.

A partir de um protocolo semelhante é possível descrever a formação dos *estados cluster*, que são a base para obter uma computação universal através das medidas. Esse raciocínio é analisado em detalhe em [2].

Assim como fizemos para a porta Z, é possível construir um circuito para aplicar a porta $XHU_z(\alpha)$ através de medidas, onde $U_z(\alpha)$ é uma rotação de um ângulo α ao redor do eixo Z. Esse circuito está ilustrado na figura 10.

Como a parte do algoritmo que gera emaranhamento acontece no início da computação e não depende da rotação que desejamos fazer, podemos interpretar esse protocolo como uma medida de um observável de um estado já emaranhado. Medir observáveis em computação quântica equivale a medir em uma base diferente da base computacional, ou seja, na base de um outro operador que não Z. Nesse caso medimos o operador $M(\alpha) = U_z(\alpha)XU_z(\alpha)$.

A partir de concatenações do processo acima é possível gerar qualquer porta de um q-bit. Assim como na seção 4.4, utilizaremos a decomposição em ângulos de Euler para

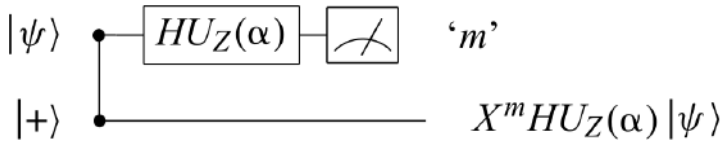

Figura 10 – Circuito para aplicação de $U_z(\alpha)$. A linha vertical conectada por dois pontos é a representação da porta C-Z. Note como ela não discrimina os q-bits de controle e alvo. Retirado de [2].

provar a universalidade da computação baseada em medidas. Devemos ser capazes de gerar três rotações arbitrárias ao redor de dois eixos não paralelos (nesse caso X e Z), ou seja a porta

$$U = U_z(\gamma)U_x(\beta)U_z(\alpha)$$

Uma relação importante é que uma rotação em torno de z por um ângulo ξ arbitrário pode ser transformada em uma rotação do mesmo ângulo em torno de x via

$$HU_z(\xi)H = U_x(\xi).$$

Dessa forma

$$U = HHU_z(\gamma)HU_z(\beta)HU_z(\alpha).$$

É possível aplicar essa porta sobre um q-bit concatenando três vezes o algoritmo para aplicar a porta $XHU_z(\alpha)$ com outros ângulos, como ilustrado na figura 11

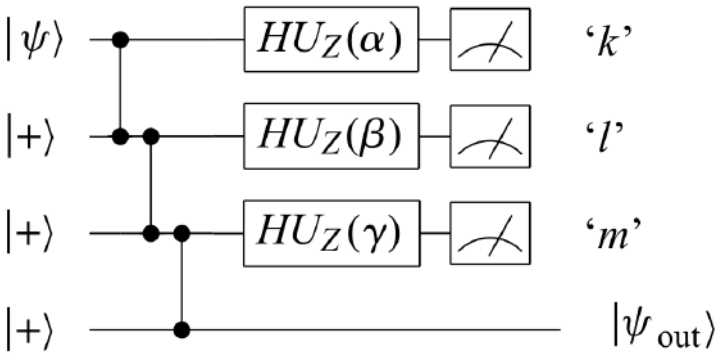

Figura 11 – Circuito universal para portas de um q-bit baseado em medidas. Retirado de [2].

Com

$$\begin{aligned}|\psi_{out}\rangle &= (X^m HU_z(\gamma))(X^l HU_z(\beta))(X^k HU_z(\alpha))\,|\psi\rangle \\ &= X^m Z^l X^k H R_z((-1^l)\gamma)R_x((-1)^k\beta)R_z(\alpha)\,|\psi\rangle\,,\end{aligned}$$

onde comutamos todas as portas X e Z para obter a forma da decomposição em ângulos de Euler. Note a forma como os resultados das medidas influenciam o procedimento: cada

ângulo de rotação ou as bases em que são feitas as medidas depende do resultado da medidas dos q-bits anteriores. Por isso é necessário que se realize as medidas em uma ordem específica para que a computação funcione corretamente, por isso chamamos esse modelo de *"one-way" model*.

Mostramos que somente com medidas adaptativas em diferentes bases sobre um estado emaranhado é possível realizar qualquer porta de um q-bit. Na dedução acima o estado emaranhado era formado por $|\psi\rangle$ e três estados $|+\rangle$ ligados por portas C-Z. É possível começar com com apenas estados $|+\rangle$ ligados por portas C-Z, e a tarefa de preparar o estado de entrada pode ser uma parte da computação.

Definimos como um *cluster* esses estados emaranhados formados por diversas aplicações da porta C-Z a um conjunto de estados $|+\rangle$. Eles são o recurso utilizado para se realizar a computação nesse modelo. Uma característica essencial do *one-way model* é que uma vez estabelecido o emaranhamento entre os estados de entrada (chamamos essa etapa de preparar o *cluster)*, não é necessária a aplicação de nenhuma porta adicional pois toda a computação subsequente é realizada pelas medidas adaptativas. Isso significa que a parte que envolve portas de dois q-bits pode ser realizada antes que a computação comece, ou *offline*.

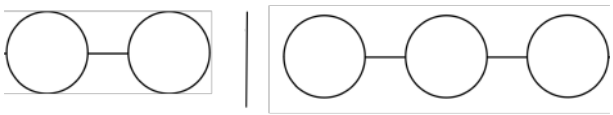

Figura 12 – Representações dos estado de Bell e GHZ como clusters.

Existe uma representação gráfica dos estados *cluster*. Para cada estado $|+\rangle$ associamos um círculo (ou vértice), enquanto as ligações de portas C-Z são representadas por linhas (ou arestas). Como as portas C-Z entre diferentes q-bits comutam, não é necessário estabelecer um ordenamento entre elas para gerar um *cluster*. Nessa representação podemos representar estados emaranhados conhecidos como os estados de Bell [equação (4.14)] e o estado Greenberger–Horne–Zeilinger (GHZ), dado por

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \tag{4.18}$$

como correntes unidimensionais de dois e três q-bits, respectivamente, como indicado na figura 12.

Começamos a computação medindo um dos q-bits, e a base em que serão feitas as próximas medidas dependem do resultado dessa primeira, e assim por diante.

Podemos representar também a aplicação de duas portas em sequência nesse formalismo. Considere que aplicamos a porta U_1 e depois U_2 para uma entrada no estado $|\psi\rangle$. O conjunto de medidas de U_1 resulta no novo estado de entrada para o conjunto de medidas

de U_2. No entanto todas as medidas associadas a U_1 comutam com todas as portas C-Z associadas a U_2. Portanto podemos trazer todas essas operações de emaranhamento das duas aplicações para o início da computação, e obtemos um único *cluster* para em seguida aplicar apenas as medidas [19].

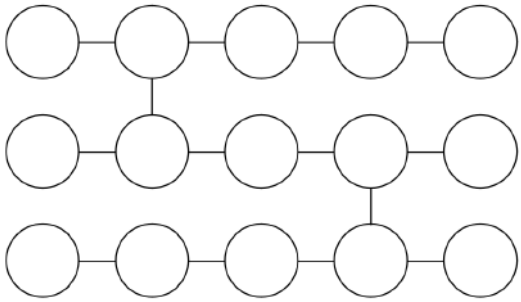

Figura 13 – Um cluster que envolve portas de um e dois q-bits. Os q-bits lógicos são representados pelas linhas horizontais, assim como no modelo de circuitos, e as portas C-Z entre esses q-bits são as arestas verticais.

Até agora vimos como a computação de um q-bit pode ser toda realizada como medidas adaptativas sobre um estado *cluster*. No entanto para fazer computação quântica universal é necessário gerar emaranhamento entre diferentes q-bits (seção 4.4). Uma porta capaz desse feito é a própria C-Z, como vimos na seção 4.3. Essa é a melhor escolha para esse modelo pois podemos unir as C-Z associadas ao emaranhamento entre q-bits com as associadas à preparação do cluster, e novamente essas portas comutam com todas as medidas e por isso podemos também aplicá-las *off-line*. Como os *clusters* de um q-bit podem ser representados por uma sequência de vértices de uma cadeia unidimensional, podemos aplicar as portas entre q-bits por arestas ligando duas cadeias horizontais. Clusters universais, portanto, podem ser representados por redes quadradas bidimensionais, como ilustrado na figura 13.

Esse modelo permite uma flexibilidade muito maior sobre a possibilidade de erro de uma porta de dois q-bits. Aplicando essas portas *off-line*, podemos identificar os casos de falha e tentar novamente sem muitos prejuízos à computação. Veremos que esse modelo computacional é um candidato conveniente para a LOQC, pois as portas de dois q-bits são de fato um grande desafio para essa arquitetura. Esse será o tema do próximo capítulo.

Capítulo 5

Computação quântica com óptica linear

Definidos os conceitos básicos da óptica linear e da computação quântica, é hora de unir essas duas análises para mostrar como é possível realizar computação utilizando fótons. Primeiro, mostraremos três formas de se codificar e manipular os q-bits utilizando aparatos ópticos. Veremos que existem vantagens e desvantagens tecnológicas para cada tipo de codificação. Além disso apresentaremos propostas de como gerar emaranhamento entre fótons, i.e., aplicar portas de dois q-bits, e as dificuldades envolvidas nesse processo. Por fim, apresentaremos um modelo para construir estados *cluster* universais a partir de óptica linear. Veremos como a computação baseada em medidas analisada no capítulo anterior é uma candidata natural para a LOQC.

5.1 Tipos de codificação

O primeiro passo para idealizar uma arquitetura de computação quântica é encontrar um sistema quântico de dois níveis em que tenhamos controle sobre os parâmetros. Vimos na seção 2.2 que os estados do campo eletromagnético podem ser caracterizados pelo número de fótons em cada um dos infinitos modos possíveis. Portanto para codificar um q-bit óptico basta escolher dois estados desse espaço de Fock.

Vamos começar com a codificação mais simples do ponto de vista conceitual. Considere apenas um fóton em um modo. Nessa codificação os estados da base computacional correspondem ao vácuo e ao estado correspondente ao fóton no dado modo. Temos

$$\begin{aligned} |0\rangle &\rightarrow |\varnothing\rangle \\ |1\rangle &\rightarrow a_l^\dagger |\varnothing\rangle = |0, ..., 1, ..., 0\rangle . \end{aligned}$$

Essa é a chamada codificação *single-rail*, e nela o grau de liberdade do q-bit é o número de fótons. Podemos ver que essa codificação é eficiente no sentido de precisar de um número de modos que cresce linearmente com o número de q-bits.

Apesar de simples, essa codificação apresenta sérias dificuldades tecnológicas para sua implementação. Como vimos na seção 3.2, os aparatos cotidianos como divisores de feixes e placas de onda são elementos que conservam o número de fótons. Assim, apenas com óptica linear passiva não somos capazes de realizar transformações sobre um q-bit codificado dessa forma.

Alternativamente, podemos utilizar um único fóton para codificar n q-bits em um interferômetro *N-port*. O procedimento consiste em associar cada elemento da base computacional a um dos modos espaciais ou portas do interferômetro. Por exemplo, para uma operação em três q-bits teríamos oito modos associados aos estados $\{|000\rangle, |010\rangle, ..., |111\rangle\}$.

Podemos facilmente aplicar transformações sobre um e dois q-bits em um *N-port*. Por exemplo, podemos implementar a porta Hadamard utilizando um divisor de feixes e dois deslocadores de fase de $-\pi/2$ em cada um dos modos. A porta C-X consiste em uma simples trocas dos modos que correspondem aos estados $|10\rangle$ e $|11\rangle$. Ilustramos essas portas na figura 14.

Devido à equivalência matemática entre as representações de polarização e espacial, é possível em princípio criar um interferômetro que opera da mesma forma sobre esse outro grau de liberdade.

Essa codificação de fato nos permite realizar qualquer computação quântica arbitrária com aparatos ópticos conhecidos. Há um problema, no entanto, com a escalabilidade desse modelo. Como precisamos de um modo para cada elemento da base computacional, para uma computação de n q-bits precisaríamos de 2^n modos. Consequentemente, o número de portas e aparatos ópticos cresce exponencialmente com o número de q-bits, o que não pode ser considerado uma codificação eficiente.

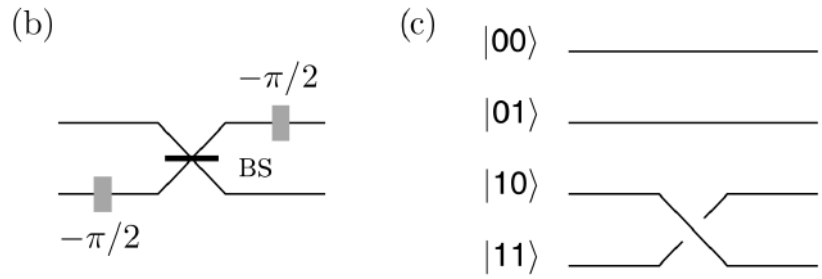

Figura 14 – Representações das portas (a)- Hadamard e (b)-C-X na codificação *N-port*. Retirado de [2].

Não é surpreendente que esse sistema não seja universal para computação quântica. Vimos, na seção 3.4, que efeitos de interferência de apenas um fóton geram a mesma física que ondas eletromagnéticas clássicas. Se um sistema clássico fosse capaz de realizar computação quântica universal, não precisaríamos fazer computadores quânticos. Na codificação *N-port*, em vez de um fóton, poderíamos realizar a computação através de um

feixe clássico, e obteríamos o mesmo resultado. De fato, é necessário que haja efeitos de interferência entre mais de um fóton para implementar computação quântica universal, como o efeito Hong-Ou-Mandel (seção 3.4).

A codificação mais útil para os nossos fins é chamada codificação *dual-rail*. Ela consiste em associar cada q-bit a um fóton em superposição de dois modos. Podemos ver que para n q-bits teremos n fótons e $2n$ modos, o que é uma escalabilidade aceitável. Considerando inicialmente um q-bit nos modos espaciais 1 e 2 temos, de acordo com a notação das equações (2.9) e (2.10),

$$|0\rangle \rightarrow a_1^\dagger |\varnothing\rangle = |1,0\rangle_{12} \tag{5.1}$$

$$|1\rangle \rightarrow a_2^\dagger |\varnothing\rangle = |0,1\rangle_{12} \tag{5.2}$$

Nessa codificação as portas de um q-bit equivalem a transformações unitárias sobre os modos $a_1^\dagger$ e $a_2^\dagger$ [2]. Novamente usando os resultados da seção 3.3.4, podemos afirmar que a partir de divisores e feixes e deslocadores de fase é possível gerar qualquer transformação unitária sobre dois modos espaciais, e portanto sobre um q-bit nessa codificação.

Como o espaço de polarização é um espaço de Hilbert de dimensão dois, como vimos na seção 2.3, esse grau de liberdade é um candidato natural para ser um q-bit. É possível, e em muitos casos conveniente, realizar a codificação *dual-rail* com dois estados ortogonais de polarização, como por exemplo, na base horizontal e vertical. A base computacional nesse caso é

$$|0\rangle \rightarrow a_H^\dagger |\varnothing\rangle = |H\rangle \tag{5.3}$$

$$|1\rangle \rightarrow a_V^\dagger |\varnothing\rangle = |V\rangle \tag{5.4}$$

Novamente é possível usar a equivalência entre as representações para mostrar que podemos igualmente gerar qualquer portas de um q-bit sobre um estado de polarização através das placas de onda. Em diversas aplicações utilizamos as duas representações, e a tradução pode ser feita através dos divisores de feixes por polarização, analisados na seção 3.3.

5.2 O protocolo KLM

Vimos que é possível aplicar facilmente portas de um q-bit sobre fótons na codificação *dual-rail*. Podemos, a princípio, implementá-las deterministicamente, no sentido de que não existe probabilidade de falha além de possíveis ruídos advindos da tecnologia envolvida, como falha nos detectores, perda de fótons etc.

As portas de dois q-bits, por outro lado, são mais problemáticas. Fótons, por não possuírem massa ou carga, interagem menos com a matéria do que outras partículas fundamentais. Isso é ótimo do ponto de vista de comunicação, pois a informação quântica

contida em um fóton tende a permanecer intacta,i.e., livre de descoerência mesmo para propagação a longas distâncias. No entanto uma das tarefas essenciais que um computador quântico precisa realizar é gerar quantidades arbitrárias de emaranhamento entre as partes do sistema que codificam os q-bits. Para criar esse emaranhamento é necessário que haja alguma interação, mesmo que indireta, entre os q-bits.

Considere a simples tarefa de preparar um estado de Bell, que é parte do protocolo de teletransporte que vimos na seção 4.5, além de diversas outras tarefas computacionais. Na codificação de polarização, isso equivale a fazer

$$|HH\rangle \rightarrow \frac{|HH\rangle + |VV\rangle}{\sqrt{2}}. \tag{5.5}$$

Em termos dos operadores de criação temos (ignorando a normalização)

$$a_H^\dagger a_H^\dagger \rightarrow a_H^\dagger a_H^\dagger + a_V^\dagger a_V^\dagger \neq (U_{11}a_H^\dagger + U_{12}a_V^\dagger)(U_{21}a_H^\dagger + U_{22}a_V^\dagger), \tag{5.6}$$

onde a última expressão equivale a uma transformação genérica de óptica linear passiva U, definida na equação (3.4). De fato é impossível criar um par de Bell deterministicamente a partir de estados produto apenas com transformações que levam operadores de criação em combinações lineares deles mesmos.

É necessário, portanto, encontrar alguma forma alternativa de gerar uma dinâmica não-linear sobre os fótons. Em 2000, Knill, Laflamme e Milburn (KLM) mostraram como é possível, em princípio, contornar essa dificuldade [5].

Primeiro, eles mostraram como é possível implementar uma porta C-Z probabilística utilizando a influência dinâmica das medidas. Vamos mostrar como podemos construir essa porta, e para fins didáticos vamos primeiro ilustrá-la como o interferômetro dotado de uma operação não linear chamada NS (*non-linear sign shift*).

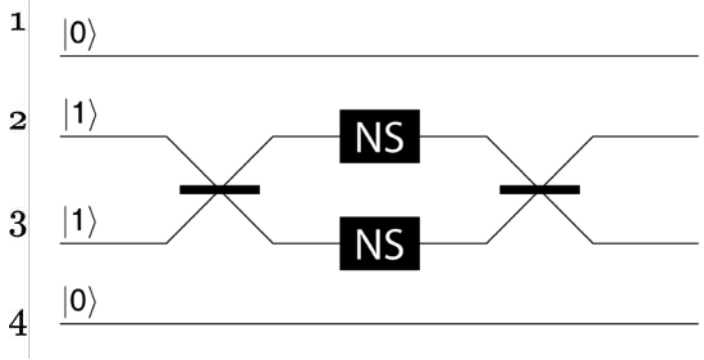

Figura 15 – Circuito que implementa a porta C-Z probabilística. Adaptada de [2].

O circuito óptico que implementa a porta C-Z está ilustrado na figura 15. A operação de um modo NS atua da seguinte forma: se ela receber o vácuo ou o um único fóton ela atua como a identidade, mas se receber dois fótons ela aplica um deslocamento de fase de

π, ou seja,

$$|0\rangle \to |0\rangle\,, \tag{5.7}$$
$$|1\rangle \to |1\rangle\,, \tag{5.8}$$
$$|2\rangle \to -|2\rangle\,. \tag{5.9}$$

Essa transformação não corresponde a uma operação linear. Um deslocador de fase usual poderia fazer

$$|0\rangle \to |0\rangle\,,$$
$$|1\rangle \to e^{i\phi}|1\rangle\,,$$
$$|2\rangle \to e^{i2\phi}|2\rangle\,,$$

no entanto não existe ϕ tal que $e^{i\phi} = 1$ e $e^{2i\phi} = -1$.

Vamos analisar como o circuito da figura 15 opera para os quatro estados da base computacional na codificação *dual rail*. A atuação da porta C-Z deve ser uma fase de π sobre o estado $|11\rangle$ e a identidade no resto. Vamos indexar cada uma das portas do interferômetro como $\{1, 2, 3, 4\}$, como indicado na figura. O funcionamento dessa porta requer que os fótons sejam idênticos.

- $|00\rangle$ - Incidimos fótons nos braços 1 e 4, que não possuem nenhum elemento óptico. Os dois se propagam inalterados até o fim e temos trivialmente a identidade.

- $|01\rangle$ e $|10\rangle$ - Nos dois casos um dos fótons não é alterado, enquanto o outro entra no primeiro divisor de feixes. Os estados que entram nas portas NS são superposições do vácuo com estados de um fóton. As portas NS atuam como a identidade nesses estados, e o segundo divisor de feixes reverte a ação do primeiro. Novamente temos a identidade.

- $|11\rangle$ - Os fótons incidem nos modos 2 e 3. Assim, temos dois fótons idênticos incidindo sobre o primeiro divisor de feixes. Pelo efeito Hong-Ou-Mandel (seção 3.4) teremos os dois fótons saindo por um dos braços e passando por alguma da portas NS, o que causará uma aplicação da fase de π. O segundo divisor de feixes retorna os fótons ao estado inicial, mas com um sinal negativo devido à porta NS. A saída é portanto o estado $-|11\rangle$, como desejado.

Uma forma de implementar a porta NS consiste em um interferômetro *3-port*, ilustrado na figura 16. As transmissividades dos divisores de feixes são tais que

$$\eta_1{}^2 = \eta_3{}^2 = 1/(4 - 2\sqrt{2}) \qquad \text{e} \qquad \eta_2{}^2 = 3 - 2\sqrt{2}.$$

Na primeira porta temos o estado de entrada. Na segunda e terceira temos modos auxiliares, um deles inicializado com um fóton e o outro no vácuo. Além disso, usamos

três divisores de feixes e dois detectores nas portas auxiliares. Se medirmos um fóton e o vácuo nos detectores corretos (como indicado na figura) saberemos que a porta foi aplicada corretamente.

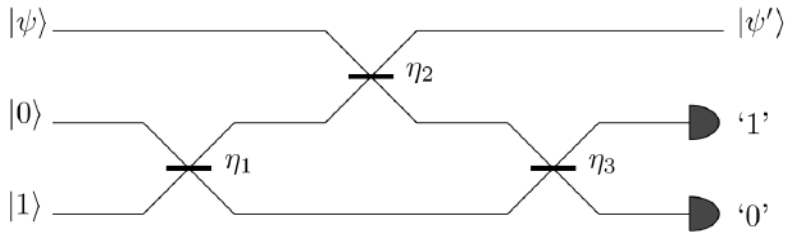

Figura 16 – Circuito para a porta NS. Os valores nos detectores correspondem às medições que indicam sucesso. Retirado de [2].

Fica clara a natureza probabilística dessa porta, pois é possível que os fótons de entrada sejam enviados para qualquer uma das três portas. Isso pode causar, por exemplo, que uma entrada $|0\rangle$ retorne $|1\rangle$, o que obviamente não corresponde a uma aplicação correta. A probabilidade de sucesso dessa porta é 1/4 [2].

É importante diferenciar os casos de erro possíveis. Considere $n \in \{|0\rangle, |1\rangle, |2\rangle\}$ fótons de entrada.

(i) Vácuo nos dois detectores. Nesse caso, o fóton de ancilla foi para a porta de saída junto com os fótons de entrada, e obteremos um estado com número de fótons $n + 1$, com possíveis mudanças de fase.

(ii) Detectamos 01 (lembre que 10 indica sucesso). Neste caso o número de fótons na saída está correto, mas foram aplicadas mudanças de fase indesejadas.

(iii) Detectamos mais de um fóton. Isso indica que uns dos fótons da entrada foi parar em um dos detectores.

Nos casos (i) e (ii) é possível realizar mais operações (possivelmente envolvendo mais medidas e fótons auxiliares) de forma a corrigir o erro, pois toda a informação sai pela porta de saída, apenas com algum ruído.

O terceiro caso no entanto configura um erro catastrófico. Ao detectar acidentalmente um dos fótons de entrada adquirimos conhecimento sobre esse estado, o que destrói a superposição e consequentemente a informação quântica. Nesse caso de erro é impossível recuperar o estado original e a computação falha [2].

A probabilidade de sucesso dessa porta NS é 1/4 e, como cada porta C-Z requer que as duas portas NS funcionem, a probabilidade total é 1/16. Para uma computação com N dessas portas precisaríamos rodar o circuito, em média, 16^N vezes para ter uma probabilidade apreciável de uma computação correta, o que é exponencial no número de

portas. Fica claro que precisaríamos de uma quantidade imensa de recursos para realizar uma computação quântica arbitrária dessa forma. Se temos apenas portas probabilísticas, precisamos de alguma forma retirar a aplicação dessas portas do circuito [15].

Uma forma de adaptar a computação a portas C-Z probabilísticas foi apresentada também por KLM. Para ilustrar como foi idealizado o chamado "*teleportation trick*" considere que desejamos aplicar a porta C-Z sobre dois q-bits de entrada que denotaremos por $|\phi_1\rangle$ e $|\phi_2\rangle$. Através do protocolo de teletransporte quântico (seção 4.5) podemos enviar $|\phi_1\rangle$ e $|\phi_2\rangle$ para dois q-bits auxiliares ao custo de um par de Bell, uma medida na base de Bell e correções baseadas nessas medidas.

Podemos aplicar a porta C-Z sobre os q-bits teletransportados, o que a princípio não nos ajuda muito. No entanto, agora podemos comutar a porta C-Z pelas correções X e Z dos teletransportes para trazê-la para o início da computação. Isso pode ser feito facilmente pelo fato de a porta C-Z ser uma porta de Clifford, pois uma porta de Clifford sempre leva portas de Pauli em portas de Pauli por conjugação. Dessa forma, conseguimos trazer a aplicação da porta C-Z para a parte *off-line* da computação ao custo de portas X e Z adicionais (como indica a figura 17).

Agora o fato de a porta ser probabilística não é mais tão problemático. Na parte *off-line* não é necessário que todas as portas C-Z funcionem simultaneamente, dessa forma podemos repetir a aplicação até obter sucesso em cada uma delas separadamente (chamamos isso de *pós-seleção*). Precisamos de 16 tentativas em média para que cada porta funcione, então precisamos de $16N$ tentativas para um circuito de N portas C-Z. Observe que agora temos um número polinomial, e obtemos a escalabilidade necessária.

Um aparente problema está nas medidas de Bell, que costumam precisar de uma aplicação da porta C-X, de implementação tão difícil quanto a da porta C-Z. Para esse fim KLM desenvolveram um protocolo de teletransporte que não utiliza portas C-X, ao custo

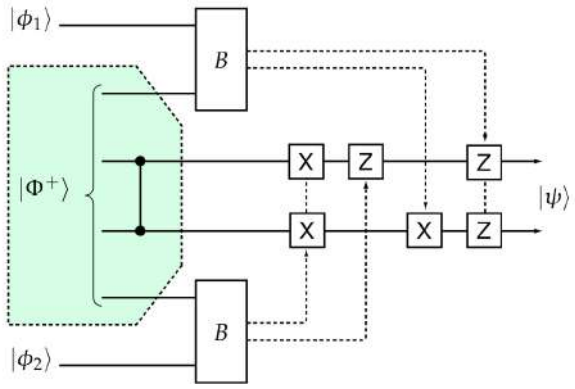

Figura 17 – Circuito para trazer a porta C-Z para o início da computação. A caixa denotada por "B" corresponde a uma medida na base de Bell e as linhas pontilhadas indicam as correções do protocolo de teletransporte padrão.

de perda do funcionamento determinístico.

O teletransporte adaptado de KLM, apesar de ser também probabilístico, nos permite utilizar n fótons auxiliares para aumentar arbitrariamente a probabilidade de sucesso, dada por $n/(n+1)$ [15]. Para que a porta C-Z funcione precisamos de dois teletransportes, então a probabilidade de sucesso por porta é $n^2/(n+1)^2$. Podemos ver claramente a melhora em relação à aplicação direta, para uma probabilidade de falha baixa o ruído correspondente é muito mais tratável pela correção quântica de erros.

KLM mostraram que é possível aplicar portas de dois q-bits eficientemente sobre fótons utilizando apenas óptica linear passiva e medidas adaptativas. No entanto esse processo, apesar de eficiente, ainda é extremamente custoso. Para uma porta C-Z com 95% de probabilidade de sucesso o número estimado de operações necessárias é da ordem de 10^4 [16], o que é um grande avanço sobre a aplicação direta mas ainda assim um número muito alto. Outro problema é que os detectores precisam discriminar perfeitamente o número de fótons. É necessário que um deles detecte o vácuo sem erro, o que também é experimentalmente desafiador [2].

5.3 Clusters ópticos

Na seção anterior, vimos que implementar o modelo de circuitos de computação quântica com óptica linear é possível em princípio. No entanto, também podemos pensar em LOQC em outros modelos de computação. Um exemplo é o modelo de computação baseada em medidas (seção 4.6). Nesta seção mostraremos uma forma de construir estados *cluster* eficientemente com óptica linear beseada nas chamadas *portas de fusão*.

Portas de fusão são operações de óptica linear que nos permitirão aumentar probabilisticamente o tamanho de um estado cluster. Existem dois tipos de portas de fusão, tipo 1 e tipo 2, que diferem em sua eficiência e nos erros que causam quando falham. Vamos analisar em detalhe o funcionamento da porta de fusão tipo 1.

No espaço dos q-bits, o objetivo dessa porta é receber dois pares de Bell da equação (4.14) e retornar o estado GHZ (4.18). Na codificação *dual-rail*, para cada q-bit associamos um fóton em dois modos (seção 5.1). Como temos dois pares de Bell (quatro q-bits) vamos considerar um circuito com quatro modos espaciais com q-bits codificados na polarização. Dessa forma, temos no total oito modos possíveis. Vamos numerar de 1 a 4 os modos espaciais e trabalharemos a polarização na base $\{H, V\}$. De acordo com a notação das equações (2.12) e (2.13), o estado inicial do sistema é

$$\left(|HH\rangle_{12} + |VV\rangle_{12}\right)\left(|HH\rangle_{34} + |VV\rangle_{34}\right) = \left(a^\dagger_{1H}a^\dagger_{2H} + a^\dagger_{1V}a^\dagger_{2V}\right)\left(a^\dagger_{3H}a^\dagger_{4H} + a^\dagger_{3V}a^\dagger_{4V}\right)|\varnothing\rangle$$

Vamos incidir os modos 2 e 3 sobre um divisor de feixes que transmite a polarização horizontal e reflete a vertical, discutido na seção 3.3.3. Em seguida, aplicamos uma rotação

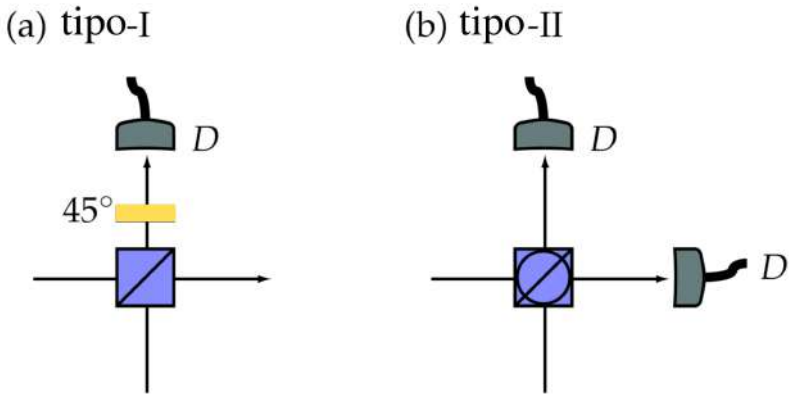

Figura 18 – Circuitos que implementam as portas de fusão. Note que os divisores de feixes de polarização das portas tipo 1 e 2 estão nas bases {H,V} e {D,A} respectivamente [equação (2.11)]. Adaptado de [15].

de $\pi/4$ sobre a polarização do modo 2, como ilustrado na figura 18(a). Isso equivale à porta Hadamard sobre os modos horizontal e vertical. Aplicando essa dinâmica sobre os operadores de criação, temos

$$\begin{aligned}
&\left(a_{1H}^\dagger a_{2H}^\dagger + a_{1V}^\dagger a_{2V}^\dagger\right)\left(a_{3H}^\dagger a_{4H}^\dagger + a_{3V}^\dagger a_{4V}^\dagger\right)\\
&\quad\rightarrow \left(a_{1H}^\dagger a_{2H}^\dagger + a_{1V}^\dagger a_{3V}^\dagger\right)\left(a_{3H}^\dagger a_{4H}^\dagger + a_{2V}^\dagger a_{4V}^\dagger\right)\\
&\quad\rightarrow \left(\frac{a_{1H}^\dagger}{\sqrt{2}}\left(a_{2H}^\dagger + a_{2V}^\dagger\right) + a_{1V}^\dagger a_{3V}^\dagger\right)\left(a_{3H}^\dagger a_{4H}^\dagger + \left(a_{2H}^\dagger - a_{2V}^\dagger\right)\frac{a_{4V}^\dagger}{\sqrt{2}}\right)\\
&\quad\rightarrow \frac{a_{1H}^\dagger a_{2H}^\dagger a_{3H}^\dagger a_{4H}^\dagger}{\sqrt{2}} + \frac{a_{1H}^\dagger a_{2V}^\dagger a_{3H}^\dagger a_{4H}^\dagger}{\sqrt{2}} + \frac{a_{1H}^\dagger a_{4V}^\dagger \left(a_{2H}^\dagger\right)^2}{2} - \frac{a_{1H}^\dagger a_{4V}^\dagger \left(a_{2V}^\dagger\right)^2}{2}\\
&\qquad + a_{1V}^\dagger a_{3V}^\dagger a_{3H}^\dagger a_{4H}^\dagger + \frac{a_{1V}^\dagger a_{2H}^\dagger a_{3V}^\dagger a_{4V}^\dagger}{\sqrt{2}} - \frac{a_{1V}^\dagger a_{2V}^\dagger a_{3V}^\dagger a_{4V}^\dagger}{\sqrt{2}},
\end{aligned}$$

onde suprimimos a normalização.

Se aplicarmos esses operadores sobre o vácuo obtemos o estado

$$\begin{aligned}
&\frac{1}{\sqrt{2}}(|H,H,H,H\rangle_{1234} + |V,H,V,V\rangle_{1234}) + \frac{1}{\sqrt{2}}(|H,V,H,H\rangle_{1234} - |V,V,V,V\rangle_{1234})\\
&\qquad + \frac{1}{2}(|H,HH,0,V\rangle_{1234} - |H,VV,0,V\rangle_{1234}) + |V,0,HV,H\rangle_{1234}
\end{aligned}$$

O último passo consiste em detectar o número de fótons e a polarização do modo 2. Se detectarmos apenas um fóton, obteremos como estado pós-medida um estado emaranhado de três q-bits, o que corresponde aos dois primeiros termos entre parênteses na equação acima. O estado GHZ corresponde ao caso da detecção de polarização horizontal enquanto o caso da vertical é igualmente emaranhado e pode ser transformado no GHZ por operações lineares. A probabilidade de sucesso desse protocolo é, portanto 1/2.

Tanto as portas de fusão quanto o protocolo da seção anterior utilizam pares de Bell previamente preparados como recurso. É possível gerar esses pares a partir de estados

produto utilizando a porta C-Z probabilística da seção anterior. Por ser uma preparação *off-line* podemos pós-selecionar os casos em que a porta funciona [15]. Existem também formas de criar diretamente pares de fótons emaranhados. Uma delas é através da conversão paramétrica descendente, descrita em [20]. De fato o maior desafio não é obter pares de Bell, e sim estados emaranhados de tamanho arbitrário (clusters).

Vamos entender como as portas de fusão podem ser usadas para construir estados cluster. Vimos na seção 4.6 que o par de Bell e o estado GHZ podem ser traduzidos em *clusters* unidimensionais com dois e três vértices, respectivamente. A porta de fusão tipo 1 é capaz de conectar duas correntes menores para gerar uma corrente maior. Se tivéssemos utilizado sistemas emaranhados maiores como entrada, o efeito seria semelhante [16].

Vamos mostrar agora como um erro dessa porta prejudica a construção de um cluster. Identificamos os casos de falha como detecções de (i) dois fótons horizontais, (ii) dois fótons verticais ou (iii) nenhum fóton. Para esses casos os estados pós-medida são

$$\text{(i) e (ii)} \rightarrow |H,0,V\rangle_{134} = |H\rangle_1 \otimes |V\rangle_4 \tag{5.10}$$

$$\text{(iii)} \rightarrow |V,HV,H\rangle_{134} = |V\rangle_1 \otimes |HV\rangle_3 \otimes |H\rangle_4 \tag{5.11}$$

Em todos os casos de falha o estado pós medida é um estado produto. Assim, a falha destrói o emaranhamento entre os pares de Bell. Esse erro é ainda mais catastrófico se tentarmos ligar dois clusters grandes utilizando essa porta. O efeito é que todos os elos associados aos q-bits de entrada são removidos. Graficamente isso equivale a retirar os q-bits do cluster. Se falhássemos ao tentar ligar, por exemplo, duas correntes de q-bits o resultado seria quebrar as duas correntes, o que pode ser um atraso considerável para preparação de *clusters* maiores [16].

Para resolver esse problema existe a porta de fusão do tipo 2, cujo circuito está ilustrado na figura 18(b). Note como nessa porta detectamos dois fótons de entrada, e por isso não podemos utilizá-la para unir dois pares de Bell como a porta anterior. No entanto, de forma análoga ao que foi feito para o tipo 1, é possível mostrar que se aplicarmos essa porta em dois fótons de estados GHZ, obtemos a transformação

$$(|HHH\rangle_{123}+|VVV\rangle_{123})(|HHH\rangle_{456}+|VVV\rangle_{456}) \rightarrow |HHHH\rangle_{1256}+|VVVV\rangle_{1256}\,, \tag{5.12}$$

onde os modos 3 e 4 foram detectados. Essa porta também funciona com probabilidade 1/2, e obtemos a indicação de sucesso quando detectamos um fóton em cada modo espacial. Não mostraremos a dedução desses resultados pois o raciocínio é análogo ao da porta tipo 1.

É possível ligar correntes maiores com a porta tipo 2, e aqui vemos a sua vantagem em relação à porta tipo 1. Considere que desejamos ligar dois *clusters* lineares de cinco vértices, como indicado na figura 19. Se obtivermos sucesso criaremos um elo entre esses dois q-bits e de fato teremos um cluster maior. Em caso de falha, a porta tipo 1 remove

os dois q-bits dos clusters e quebra as correntes originais em correntes menores. A falha da porta tipo 2, por outro lado, também remove os dois q-bits de entrada do *cluster*, mas agora os elos que esses q-bits tinham anteriormente são distribuídos entre os seus antigos vizinhos [15]. Dessa forma, de fato falhamos em aumentar o tamanho do *cluster*, mas conseguimos manter uma parte maior do emaranhamento anterior. Uma falha da porta do tipo 2 para ligar correntes de q-bits apenas encurta as correntes, enquanto a porta 1 as quebra, como vimos anteriormente.

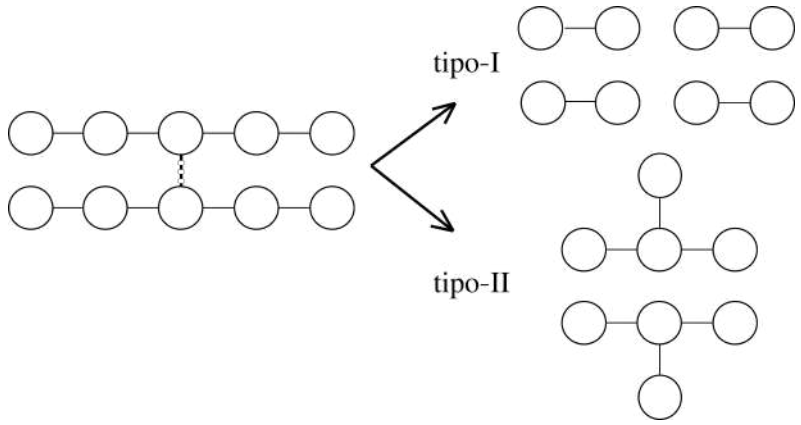

Figura 19 – Casos de falha ao tentar unir duas correntes cinco vértices para as portas de fusão 1 e 2.

A forma mais eficiente de usar essas portas para preperar *clusters* grandes é, portanto, começar criando várias pequenas correntes de três vértices a partir da porta do tipo 1 e de pares de Bell. Em seguida, unimos essas correntes usando a porta do tipo 2 para criar estados emaranhados de quatro q-bits. Então, ligamos as correntes de quatro q-bis novamente usando a porta 2, e prosseguimos assim em diante para aumentar o *cluster*.

Considere que desejamos unir um *cluster* de tamanho N a uma corrente de tamanho m com uma porta de fusão (tipo 2) que funciona com probabilidade p, consumindo dois q-bits da rede. Se obtivermos sucesso aumentamos o tamanho do *cluster* para $N + m - 2$. Em caso de falha, o número cai para $N - 2$. Para que o *cluster* cresça na média, devemos ter [16]

$$p(N + m - 2) + (1 - p)(N - 2) > N, \quad \text{e, portanto,} \quad m > \frac{2}{p},$$

onde o primeiro membro da primeira inequação é o tamanho médio do cluster após a tentativa de crescimento. Para a porta tipo 2 descrita anteriormente $p = 1/2$, e precisamos crescer o *cluster* com correntes com no mínimo $5 > \frac{2}{1/2}$ bits para obter um crescimento na média. Um detalhe importante é que podemos lidar com probabilidades de sucesso reduzidas, por exemplo imperfeições nos detetores, apenas aumentando o tamanho das correntes que usamos para crescer os *clusters*. De fato é possível em princípio criar estados emaranhados arbitrariamente grandes utilizando as portas de fusão.

Como vimos, os recursos necessários para aplicar cada porta de fusão são apenas um divisor de feixes, uma rotação de polarização para a porta 1 e dois detectores, no máximo. De fato, esse método é consideravelmente mais eficiente do que o modelo de circuitos baseado em teletransporte proposto por KLM [15].

Preparado um cluster do tamanho necessário, a computação pode prosseguir com medidas de polarização sobre os q-bits na ordem dada pelo algoritmo, seguindo procedimento descrito na seção 4.6. Esse modelo claramente é um dos mais promissores para se realizar computação universal com óptica linear, pois além de precisar de poucos recursos ele nos permite lidar com a dificuldade de se gerar emaranhamento entre os fótons passando todas as portas de dois q-bits para a parte *off-line*.

Capítulo 6

Conclusão

Vimos que, ao unir a teoria de óptica quântica ao processamento de informação, é possível idealizar como seria um computador quântico formado por fótons, divisores de feixes, placas de polarização *etc.*

Ao longo desse trabalho, consideramos que todas as operações ópticas aplicadas não apresentavam ruído. No entanto, para implementar um computador quântico funcional é necessário levar ruídos experimentais em consideração. Em óptica, por exemplo, é possível que os detectores e fontes falhem, que os fótons se percam, que os divisores de feixe não tenham exatamente a refletividade necessária, *etc.*

O ramo da computação quântica responsável por lidar com esses ruídos é a chamada teoria da *correção quântica de erros.* Essa teoria obteve bastante destaque nos últimos anos, devido a resultados que mostram que é possível realizar computação quântica eficiente mesmo que existam erros, desde que eles sejam suficientemente controlados.

Boa parte das ideias de implementações tecnológicas discutidas aqui foram retiradas de [2, 15, 16]. Essas publicações datam da década de 2000, e o fato é que muito foi feito nessa área desde então. O modelo de computação baseada em medidas ainda é muito utilizado, mas ao invés de se codificar os q-bits no estados de Fock, uma alternativa muito comum tem sido codificá-los nas quadraturas do campo 2.2. Essa é a chamada computação quântica com variáveis contínuas, e está discutida em detalhe em [2].

As possibilidades de aplicação de circuitos ópticos com fótons são diversas, tanto para o processamento de informação e comunicação quânticas quanto para nossa compreensão da natureza quântica do campo eletromagnético. Entre avanços teóricos e experimentais, podemos antecipar computadores baseados em óptica quântica cada vez mais complexos nas próximas décadas.

Referências

1 NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. ed. New York, NY, USA: Cambridge University Press, 2011.

2 KOK, P.; LOVETT, B. W. *Introduction to Optical Quantum Information Processing*. [S.l.]: Cambridge University Press, 2010.

3 ARUTE, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature*, v. 574, p. 505–510, 10 2019.

4 WANG, H. et al. Boson sampling with 20 input photons and a 60-mode interferometer in a 1014-dimensional hilbert space. *Physical Review Letters*, v. 123, 2019. ISSN 1079-7114.

5 KNILL, E.; LAFLAMME, R.; MILBURN, G. A scheme for efficient quantum computation with linear optics. *Nature*, v. 409, p. 46–52, 02 2001.

6 EINSTEIN, A. B. Concerning an heuristic point of view toward the emission and transformation of light. In: . [S.l.: s.n.], 2000.

7 PLANCK, M. Ueber das gesetz der energieverteilung im normalspectrum. *Annalen der Physik*, v. 309, n. 3, p. 553–563, 1901.

8 COMPTON, A. H. A quantum theory of the scattering of x-rays by light elements. *Phys. Rev.*, American Physical Society, v. 21, p. 483–502, May 1923.

9 STRUTT, H. J. W. Lviii. on the scattering of light by small particles. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, Taylor and Francis, v. 41, n. 275, p. 447–454, 1871.

10 BORH, N.; KRAMERS, H. A.; SLATER, J. C. Lxxvi. the quantum theory of radiation. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, Taylor and Francis, v. 47, n. 281, p. 785–802, 1924.

11 GRYNBERG, G. et al. *Introduction to Quantum Optics: From the Semi-classical Approach to Quantized Light*. [S.l.]: Cambridge University Press, 2010.

12 LEMOS, N. *Mecanica Analitica*. [S.l.]: Livraria da Física, 2007.

13 BALLENTINE, L. *Quantum Mechanics*. [S.l.]: Prentice-Hall, 1990. (Prentice Hall advanced reference series). ISBN 9780137468430.

14 JACKSON, J. D. *Classical electrodynamics*. 3rd ed.. ed. New York, NY: Wiley, 1999.

15 KOK, P. et al. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, v. 79, p. 135–174, Jan 2007.

16 KOK, P. Five lectures on optical quantum computing. In: _____. *Theoretical Foundations of Quantum Information Processing and Communication: Selected Topics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. p. 187–219.

17 EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, v. 47, p. 777–780, May 1935.

18 BELL, J. S. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, v. 1, p. 195–200, 1964.

19 JOZSA, R. *An introduction to measurement based quantum computation*. 2005.

20 KWIAT, P. G. et al. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, v. 75, p. 4337–4341, 1995.