UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA
DOUTORADO EM ENGENHARIA DE TELEINFORMÁTICA

CLAUDOMIR PINTO DE SOUSA

COMPARADOR QUANTUM-ÓPTICO DE SEQUÊNCIA DE BITs E APLICAÇÕES

FORTALEZA-CE
2021

CLAUDOMIR PINTO DE SOUSA

COMPARADOR QUANTUM-ÓPTICO DE SEQUÊNCIA DE BITs E APLICAÇÕES

Tese apresentada ao Curso de Doutorado Acadêmico em Engenharia de Teleinformática do Programa de Pós-Graduação em Teleinformática do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de Concentração: Eletromagnetismo Aplicado.
Orientador: Prof. Dr. João Batista Rosa Silva

Fortaleza-CE
2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S696c Sousa, Claudomir Pinto.
COMPARADOR QUANTUM-ÓPTICO DE SEQUÊNCIA DE BITs E APLICAÇÕES / Claudomir Pinto de Sousa. – 2021.
56 f. : il.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2021.
Orientação: Prof. Dr. João Batista Rosa Silva .

1. Computação quântica. 2. efeito Kerr não linear. 3. comparador quantum-óptico de sequência de bits.

CDD 621.38

CLAUDOMIR PINTO DE SOUSA

COMPARADOR QUANTUM-ÓPTICO DE SEQUÊNCIA DE BITs E APLICAÇÕES

Tese apresentada ao Curso de Doutorado Acadêmico em Engenharia de Teleinformática do Programa de Pós-Graduação em Teleinformática do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de Concentração: Eletromagnetismo Aplicado.
Orientador: Prof. Dr. João Batista Rosa Silva

Aprovada em: 29/06/2021.

BANCA EXAMINADORA

_____
Prof. Dr. João Batista Rosa Silva (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Jose Augusto Oliveira Huguenin,
Universidade Federal Fluminense (UFF)

_____
Prof. Dr. Liliana Sanz de la Torre
Universidade Federal Uberlândia (UFU)

_____
Prof. Dr. Askery Alexandre Canabarro Barbosa da Silva
Universidade Federal do Alagoas (UFAL)

_____
Prof. Dr. Rubens Viana Ramos
Universidade Federal do Ceará (UFC)

Dedico este título de Doutor adquirido com tanto esforço e dedicação aos meus pais ”In Memorian”, a minha esposa Roberta e meu filho Rodrigo, por estarem sempre ao meu lado, pelo incentivo e apoio em todas as minhas escolhas e decisões.

AGRADECIMENTOS

Agradeço primeiramente a Deus por todas as bênçãos recebidas, dando-me força e saúde. Agradeço a minha Família, que foi minha fonte de inspiração de onde tive o exemplo de luta e incentivo para sempre buscar os meus ideais.

Agradeço em especial, ao meu orientador professor Dr. João Batista Rosa Silva por sua grande dedicação ao trabalho, e conduta de amigo, as quais permitiram que eu conseguisse realizar este trabalho.

Agradeço também aos professor Dr. Rubens que contribuiu diretamente para o desenvolvimento dessa tese e na autoria do artigo.

Quero agradecer também, a Prof(a). Hilma, por sua conduta e coerência nas disciplinas, incentivo e orientações, e aos demais colegas de laboratório que fazem parte do grupo GIQ: George Barbosa, Samy Clever, Ranara, Daniel, Ítalo, Gisele, Joacir, e Danilo, por todo apoio, parceria e ajuda em aulas, e o companheirismo fundamental que torna esse grupo unido e forte. E aos demais que atualmente não estão presentes no grupo: Fernando e Glaucionor, Paulo Regis, Geovan e Franklin, mas, sempre que possível comparecem, e contribuem com sua parcela de conhecimento.

Agradeço a CAPES pelo incentivo financeiro, disponibilizando esse recurso para as despesas rotineiras, e a todos que de uma alguma forma, me ajudaram nesta conquista.

“Após um fracasso, analise a trilha percorrida. Nela encontrará o ponto onde errou, e corrigindo os planos poderá iniciar nova jornada, e tentar outra vez.”
(Max Weber)

RESUMO

A computação quântica tem atraído muita atenção por causa de seu poder computacional em comparação a computação clássica e, consequentemente, vários algoritmos quânticos foram propostos na literatura. No entanto, o hardware capaz de implementar tais algoritmos ainda é um desafio. Neste trabalho, fornecemos um hardware óptica para implementação de um comparador de sequência de bits quânticos, QBSC, para qubit baseado em polarização, usando o efeito Kerr não linear. O QBSC é uma estrutura importante para a implementação de declarações condicionais em algoritmos quânticos.

Palavras-chave: Computação quântica, efeito Kerr não linear, comparador quantum-óptico de sequência de bits.

ABSTRACT

Quantum computing has attracted much attention because of its computational power compared to classical computing and, consequently, several quantum algorithms have been proposed in the literature. However, hardware able to implement such algorithms is still a challenge, In this work, we provide an optical setup for implementation of a quantum bit string comparator, QBSC, for polarization-based qubit, using the non-linear Kerr effect. The QBSC is an important structure for implementation of conditional statements in quantum algorithms.

Keywords: Quantum computation, Non-linear Kerr effect, Quantum bit string comparator.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

QBSC	Comparador Quantum-Óptico de Strings de Bit.
QND	Medição Quântica não demolidora.
LOQC	Computação Quântica usando óptica linear.
BS	Divisor de feixes.
PBS	Divisor de feixe polarizado.
PM	Modulador de fase.
EPR	Einstein-Podolsky-Rosen.
QPUs	Unidades de Processamento Quântico.
TEM	Transversal Eletromagnética.
LOCC	Operações Locais de Comunicação Clássica.
CNOT	Controlled-NOT.
CSWAP	Controlled-SWAP
POVM	Positive Operator Valued Measure

1. INTRODUÇÃO

A computação quântica (CQ) está surgindo como uma grande promessa para resolver problemas e executar cálculos que a computação clássica não pode solucionar, como fatorar números primos grandes [1] e realizar pesquisas rápidas e eficientes sobre um grande banco de dados [2], problemas, relacionados à inteligência artificial, distribuição quântica de chaves, criptografia, modelagem financeira e previsão do tempo [3].

Um dos maiores desafios é desenvolver os elementos básicos da computação quântica em um sistema físico que seja confiável podendo avaliar o desempenho da operação de maneira eficiente. Uma das primeiras propostas para implementar a computação quântica foi a aplicação da fotônica (óptica linear), onde cada qubit é codificado em fóton único existente em dois modos ópticos (polarização, fase, tempo, por exemplo) [4].

No entanto, a realização da computação quântica e suas vantagens como o processamento de algoritmo requer dispositivos de hardware capazes de codificar as informações quânticas, realizar uma lógica quântica, e resolver sequências de cálculos complexos baseados em mecânica quântica [5].

Nos últimos anos, tem ocorrido grandes esforços experimentais para construir dispositivos para computação quântica com o propósito de demonstrar novos sistemas. A engenharia de ponta vem demostrando muito empenho para desenvolverem as unidades de processamento quântico (QPUs) capazes de realizar demonstrações em pequena escala de computação quântica. As QPUs desenvolvidas por fornecedores comerciais como IBM, Google, D-Wave, Rigetti e IonQ estão entre uma lista crescente de dispositivos que demonstraram os elementos fundamentais necessários para a computação quântica [6].

Existem muitas tecnologias possíveis disponíveis para a construção de computadores quânticos, classificadas tipicamente pela maneira como os qubits de informação são armazenados, esses dispositivos devem atender a vários critérios funcionais para realizar cálculos quânticos confiáveis [7].

Apesar do grande progresso de desenvolvimento e controle de qubits, os dispositivos de computação quântica são bastante propensos a erros comparados com os circuitos digitais convencionais. Assim, entender e suavizar os processos de falhas em dispositivos de qubit é um aspecto crítico do desenvolvimento da computação quântica [8].

Em CQ, também são particularmente úteis algoritmos que visam encontrar o maior (ou menor) valor em um banco de dados, e organizá-los de forma crescente e/ou decrescente.

Assim, a realização física de um sistema comparador de sequências qubits que seja capaz de comparar e classificar sequências de bits é um passo importante em direção à implementação de vários algoritmos quânticos [9-15].

Portanto, este trabalho tem como propósito apresentar uma proposta de um comparador quatum-óptico de sequências de bits (QBSC), de qubits codificados na polarização de fótons únicos, a partir de dispositivos ópticos lineares e não lineares (efeito Kerr). O QBSC é um circuito quântico que compara sequências de bits e identifica se elas são iguais ou, de outra forma, qual delas representa o maior ou menor valor binário [16]. O mesmo sistema pode ser aplicado em algoritmo quântico de classificação e na geração de estados de Bell.

Para um melhor embasamento da proposta do QBSC, este trabalho está organizado da seguinte forma. No Capítulo 2, são apresentados os principais fundamentos teóricos para o entendimento do QBSC. No Capítulo 3, apresentamos e analisamos o sistema óptico capaz de comparar duas sequências bits codificados em qubits de polarização que usa o efeito Kerr não linear para realização de medição quântica não demolidora (QND). No Capítulo 4, mostraremos uma aplicação do QBSC com uma porta SWAP controlada baseada em CNOT proposta [17] e um sistema gerador de estados de Bell baseado no QBSC proposto apresentado. Por fim, as conclusões e perspectivas de trabalhos são apresentadas.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Introdução

Neste capítulo, são apresentados alguns conceitos importantes para auxiliar na compreensão da Tese. Na Seção 2.2, são apresentadas as definições em CQ, como: o conceito de qubit, portas lógicas quânticas de um qubit e de múltiplos qubit com destaque para as portas CNOT e CSWAP, e, em seguida, o emaranhamento quântico é descrito brevemente. Na Seção 2.3 destacamos os dispositivos ópticos usados nesse trabalho como: fotodetectores, moduladores de fase, divisores de feixe, e divisores de feixes polarizados. Abordaremos as representações físicas do qubit: o fóton único polarizado e o estado coerente. Os parâmetros de Stokes, que corresponde uma maneira de mensurar a intensidade do campo eletromagnético a partir de sua polarização, são descritos sucintamente para estados coerentes bimodais. Por fim, a não linearidade e o efeito Kerr cruzado que desempenha um papel crucial na realização de medição quântica não demolidora é brevemente apresentada.

2.2. Computação quântica

A Computação Quântica (CQ) corresponde a aplicação de operações, teorias e postulados da Mecânica Quântica para fins de computação, com o intuito de desenvolver um computador quântico capaz de processar as informações de forma eficiente, mesmo não se conhecendo por completo o limite dessa capacidade [18].

Nesse tópico apresentaremos conceitos da computação quântica que serão necessários para a compreensão e entendimento do funcionamento QBSC. Entre eles estão: qubits, o conceito geral de medição quântica, portas lógicas, entrelaçamento, estado de Bell e circuitos quânticos.

2.2.1. *Bit quântico*

Em computação quântico, um sistema de dois estados distinguíveis é utilizado para representar um bit, sendo, então, chamado de quantum bit (ou qubit). O qubit tem possibilidade de existir (ou de estar) em dois estados 0 ou 1 (representados por $|0\rangle$ ou $|1\rangle$), essa característica é possível graça à propriedade de superposição dos estados quânticos respectivamente, um qubit têm singularidade de encontrar-se em uma mistura desses dois estados simultaneamente o que é conhecido como uma superposição coerente de estados. Em termos matemáticos, o estado

geral de um qubit (denotado usualmente por $|\psi\rangle$) é descrito por um vetor unitário no espaço de Hilbert ($\mathcal{H}$) bidimensional (C^2). O bit quântico (qubit) é a unidade básica da computação quântica. Em contraste com o sistema clássico, significa que esses estados podem ser representados por um vetor no espaço de Hilbert bidimensional, dados por [19]:

$$|\psi\rangle = a|0\rangle + b|1\rangle = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix}. \tag{2.1}$$

As amplitudes *a* e *b* em (2.1) correspondem a números complexos que satisfazem a condição, $|a|^2 + |b|^2 = 1$. Esses dois estados possíveis são denotados por kets $|0\rangle$ e $|1\rangle$ que formam uma base para este espaço chamada de base computacional. Os kets $|0\rangle$ e $|1\rangle$ representam os vetores:

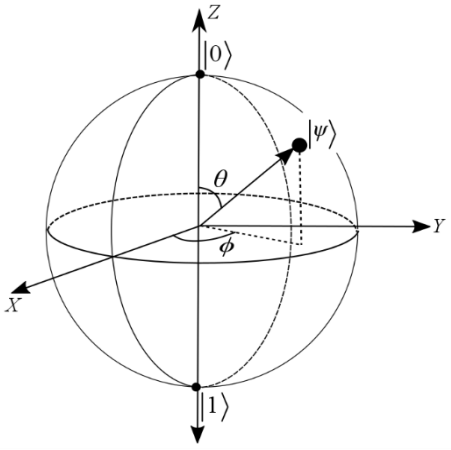
$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad \text{e} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}. \tag{2.2}$$

A forma geral do estado puro de um qubit é mostrado em (2.3) e representado na esfera de Bloch conforme mostrado na Figura 2.1 [19].

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi} sen\left(\frac{\theta}{2}\right)|1\rangle, \tag{2.3}$$

onde: *i* corresponde ao parâmetro complexo, com ϕ e θ, variando $0 \leq \phi < 2\pi$, $0 \leq \theta \leq \pi$.

Figura 2.1. Representação de um qubit na esfera de Bloch.



Fonte: [19].

2.2.2. *Portas quânticas*

As portas quânticas são operadores matriciais unitários cuja finalidade de manipular a informação, e, a partir de então, possibilitar a construção de circuitos para sistemas quânticos.

Uma matriz unitária é toda matriz quadrada M tal que $MM^* = I$, com M^* sendo a conjugada transposta de M e I a matriz identidade. Uma consequência fundamental desse fato é que toda computação quântica deve ser reversível [20]. Nas subseções seguintes, apresentaremos as principais portas quânticas de um, dois e três qubits e suas respectivas operações que foram usadas nesse trabalho.

2.2.3. *Portas quânticas de um qubit*

Portas quânticas de um qubit correspondem a todo o conjunto de operações que processam apenas um qubit obtendo na saída também apenas um qubit. Considerando as portas clássicas, estas possuem apenas duas portas de um bit que são a identidade, que não altera o bit de entrada em relação ao de saída e a porta NOT, que modifica o bit de entrada em relação ao de saída de 0 para 1 e 1 para 0. Já as portas quânticas são várias, pois um qubit é um vetor no espaço de Hilbert de duas dimensões, assim o número de portas é a quantidade de matrizes unitárias 2×2. Um conjunto de matrizes bastante significativo para a base da computação quântica são as matrizes de Pauli, pois são matrizes complexas 2×2 hermitianas e unitárias, sendo assim consideradas portas lógicas quânticas de 1 qubit. Suas representações matriciais são:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ e } \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.4}$$

As respectivas operações sobre o qubit $a|0\rangle + b|1\rangle$, corresponde:

$$a|0\rangle + b|1\rangle \xrightarrow{\sigma_x} a|1\rangle + b|0\rangle, \quad a|0\rangle + b|1\rangle \xrightarrow{\sigma_y} ia|1\rangle - ib|0\rangle \text{ e } a|0\rangle + b|1\rangle \xrightarrow{\sigma_z} a|0\rangle - b|1\rangle.$$

Outras funções logicas que podemos citar é a porta quântica Hadamard ou simplesmente *H*, largamente utilizada para gerar superposições de estados, a matriz associada a operação *H* corresponde.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.5}$$

A aplicação de *H* em (2.5) aos estados da base computacional |0⟩ e |1⟩, em (2.2), gera superposições igualmente distribuídas onde a probabilidade de se obter um dos estados ao realizar uma medição no qubit é a mesma, 50%, ou seja, $|0\rangle \xrightarrow{H} \left(|0\rangle + |1\rangle\right)/\sqrt{2}$ e $|1\rangle \xrightarrow{H} \left(|0\rangle - |1\rangle\right)/\sqrt{2}$.

A porta de fase *P* é representado na sua forma geral pela matriz.

$$P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}, \tag{2.6}$$

correspondendo as portas *S*, *Z* e *T*, para os casos em que ϕ é igual a $\pi/2$, π, $\pi/4$. Respectivamente. A porta *S* introduz uma fase relativa $e^{i\pi/2} = i$ no estado do qubit, a matriz referente a operação *S* é dado por:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \tag{2.7}$$

ou seja, aplicada *S* a um estado genérico obtemos: $\alpha|0\rangle + \beta|1\rangle \xrightarrow{S} \alpha|0\rangle + i\beta|1\rangle$.

A porta Z, já foi mencionada em (2.4), e a porta T ou porta $\pi/8$, introduz uma fase relativa $e^{i\pi/4} = \sqrt{2}(1+i)/2$, no estado do qubit, a matriz referente a operação *T* é dado por:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix},$$

ou seja, aplicada *S* a um estado genérico obtemos: $\alpha|0\rangle + \beta|1\rangle \xrightarrow{T} \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$.

As portas lógicas quânticas de um qubit apresentadas acima são apenas para exemplificar as operações sobre o estado e a informação associada no nível quântico.

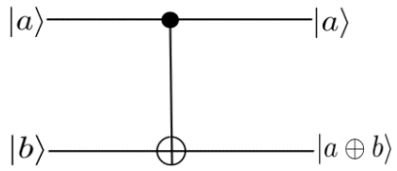
2.2.4. *Portas quânticas de múltiplos qubits*

Nas operações sobre *n* qubits, podemos citar algumas portas de múltiplos qubit, como as portas: SWAP, Toffoli, Fredkin, NOT controlada (CNOT).

A porta CNOT é que iremos destacar nesse trabalho, pois será aplicada ao QBSC proposto. Na Seção 4.1 foi desenvolvido uma configuração a partir de uma porta SWAP controlada colocada na saída do QBSC. Nessa aplicação, a porta SWAP é composta por três portas CNOT.

Uma porta CNOT de dois qubits têm seu funcionamento descrito pelo diagrama da Figura 2.2.

Figura 2.2. Representação para a porta Controlled-NOT (CNOT).



Fonte: Próprio autor.

Na Figura 2.2, $a \oplus b$ é a operação de ou-exclusivo (XOR) entre os bits a e b. Entra o estado $|a\rangle \otimes |b\rangle = |a,b\rangle$ e sai o estado $|a, a \oplus b\rangle$. Uma maneira diferente de interpretar essa operação é: o qubit $|a\rangle$ é o qubit de controle que ativa (se $a = 1$) ou não (se $a = 0$) a porta X (NOT) ao qubit $|b\rangle$. Essa transformação é dada pela matriz [21].

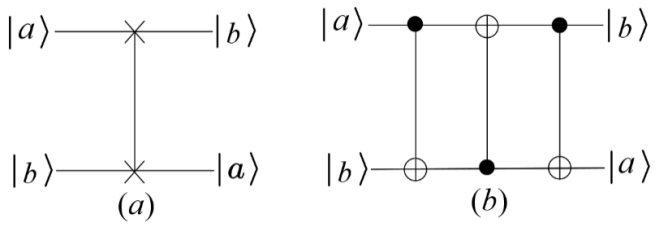
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.8}$$

A porta CNOT é uma porta muito importante para a composição de operações mais complexas. A operação composta por uma porta CNOT, sobre par de bits que estão na base computacional, esta descrita abaixo:

$$|00\rangle \xrightarrow{CNOT} |00\rangle, |01\rangle \xrightarrow{CNOT} |01\rangle, |10\rangle \xrightarrow{CNOT} |11\rangle, |11\rangle \xrightarrow{CNOT} |10\rangle.$$

Uma outra porta quântica de dois qubits, e que pode ser construída a partir de CNOT's, é a porta SWAP. Essa operação pode ser realizada por três portas CNOT's conforme mostrado na Figura 2.3 e que realize a seguinte operação:$|a,b\rangle \rightarrow |b,a\rangle$. Atualmente, várias portas NOT-Controlada (CNOT) para qubits fotônicos usando óptica linear foram propostas [22-27] e demonstradas [28-32]. Porém para uma aplicação do circuito proposto para o QBSC em uma porta Swap, realizando a função de um algoritmo ordenador de sequência de bits, foi utilizada a CNOT óptica proposta por [17].

Figura 2.3. Representação para a (a) porta SWAP e (b) a partir de três portas CNOT.



Fonte: Próprio autor.

Sua representação matricial corresponde a:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.9}$$

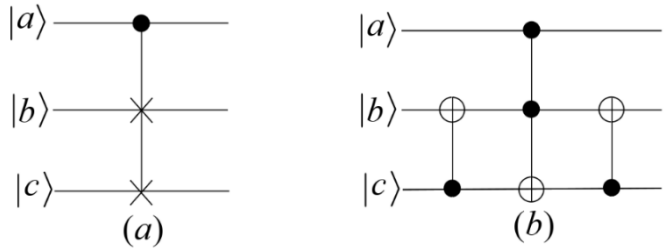
A porta SWAP realiza a seguintes operações sobre os qubtis:

$$|00\rangle \xrightarrow{SWAP} |00\rangle,\ |01\rangle \xrightarrow{SWAP} |10\rangle,\ |10\rangle \xrightarrow{SWAP} |01\rangle,\ |11\rangle \xrightarrow{SWAP} |11\rangle.$$

Já uma porta quântica de três qubits usada nesse trabalho foi a porta Fredklin ou SWAP controlada (CSWAP) como mostrada da Figura 2.4. Nesse tipo de porta, o qubit $|a\rangle$ é o controle da porta SWAP aplicada sobre $|b,c\rangle$. Logo, dado o estado de $|a,b,c\rangle$, se $|a\rangle = |0\rangle$, a saída da porta CSWAP será $|a,b,c\rangle$, caso contrário ($|a\rangle = |1\rangle$), será $|a,c,b\rangle$. A matriz de transformação da porta CSWAP é dada por.

$$\text{CSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.10}$$

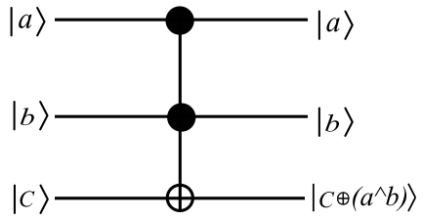
Figura 2.4. Representação para a (a) porta CSWAP e (b) porta C^n-NOT a partir de três CNOT.



Fonte Próprio Autor.

O funcionamento da porta Toffoli (C^2-NOT) é bastante semelhante a CNOT, que também é uma porta controlada, só que nesse caso, com 3 qubits de entrada, sendo dois qubits de controle ($|a\rangle$ e $|b\rangle$) e um qubit alvo ($|c\rangle$) conforme mostrado na Figura 2.5.

Figura 2.5. Representação para a porta Toffoli controlada.



Fonte Próprio Autor.

Caso os qubits $|a\rangle$ e $|b\rangle$ sejam iguais à $|1\rangle$ é ativada a operação NOT sobre qubit $|c\rangle$, caso contrário o qubit $|c\rangle$ não é alterado. Essa transformação é dada pela matriz:

$$C^2\text{-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.11}$$

A ação da matriz C^2-NOT pode ser definida pela operação da porta na base computacional associada, ou seja,

$$|000\rangle \xrightarrow{C^2\text{-NOT}} |000\rangle,\ |001\rangle \xrightarrow{C^2\text{-NOT}} |001\rangle,\ |010\rangle \xrightarrow{C^2\text{-NOT}} |010\rangle,\ |011\rangle \xrightarrow{C^2\text{-NOT}} |011\rangle,$$
$$|100\rangle \xrightarrow{C^2\text{-NOT}} |100\rangle,\ |101\rangle \xrightarrow{C^2\text{-NOT}} |101\rangle,\ |110\rangle \xrightarrow{C^2\text{-NOT}} |111\rangle,\ |111\rangle \xrightarrow{C^2\text{-NOT}} |110\rangle.$$

2.2.5. *Emaranhamento quântico*

Na computação quântica um aspecto fundamental é o emaranhamento ou entrelaçamento de estados quânticos. Para se obter estados emaranhados, precisamos de portas (operações) sobre múltiplos qubits [33].

Analisando o emaranhamento, pode-se concluir que corresponde a uma forma de conexão “forte” entre estados quânticos, pois, em uma observação sobre um dos subsistemas emaranhados é possível saber qual será o resultado da medição sobre o outro subsistema, o emaranhamento não depende da distância entre os subsistemas [34].

O início das discussões e questionamento sobre emaranhamento ocorreram em 1935 quando Boris Podolski, Nathan Rosen e Albert Einstein, em seu famoso artigo conhecido como paradoxo EPR, ou EPR, propuseram um experimento imaginário, que julgavam determinar se a mecânica quântica seria uma teoria incompleta da natureza [19].

As operações em computação e comunicação clássica, são preparadas utilizando apenas operações locais (em cada parte separadamente), correspondendo a uma classe de operações comuns que recebeu a sigla LOCC (do inglês *Local Operations and Classical Communication*). O emaranhamento possui uma característica não local da mecânica quântica, ou seja, uma conexão entre sistemas de duas ou mais partículas, em um sistema emaranhado os elementos apresentam-se ligados intrinsicamente como se fossem apenas um objeto, mesmo estando afastados um do outro em longas distâncias [35].

Para sistemas de duas componentes, cujo estado total $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, representado pela matriz densidade ρ_{AB} de dois estados quânticos $|\psi_A\rangle$ e $|\psi_B\rangle$ puros, onde $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ corresponde a um estado geral do sistema representado por:

$$\left|\psi_{AB}\right\rangle = \sum_{i,j}^{x_A,x_B} C_{i,j}\left|a_i\right\rangle \otimes \left|b_j\right\rangle, \tag{2.12}$$

Sendo x_A e x_B as dimensões dos sistemas $|\psi_A\rangle$ e $|\psi_B\rangle$ respectivamente, e $|\psi_{AB}\rangle$ corresponde ao produto tensorial dos sistemas citados, ambos pertencentes ao espaço de Hilbert $\mathcal{H}$.

O estado puro $|\psi_{AB}\rangle$ é dito separável se for possível escrevê-lo na forma $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, diante dessa afirmação uma das maneiras de medir a presença de emaranhamento de um sistema, é medir uma das componentes da pureza desse sistema. Portanto, se a matriz densidade do sistema for gerado por um sistema com a forma, $|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$, ou seja, o sistema total é emaranhado.

Consequentemente um estado puro emaranhado é um estado puro não separável, essa afirmação possibilita apenas a distinção entre estados separáveis e emaranhados, mas não é claro os vários níveis de emaranhamentos contidos nos estados, determinar o grau do emaranhamento não é trivial, é necessário uma análise dos quantificadores de emaranhamento [35].

O conceito de emaranhamento evoluiu, se estendendo a estados mistos, analisando um sistema de dois estados quânticos $|\psi_A\rangle$ e $|\psi_B\rangle$ mistos, representados por uma matriz densidade $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, e forma geral dada por:

$$\rho = \sum_i p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|, \tag{2.13}$$

o estado, é dito separável quando pode ser expresso como uma soma convexa dos estados resultante do produto $\rho_i^A \otimes \rho_i^B$, obedecendo a expressão, $\rho = \sum_i p_i\left(\rho_i^A \otimes \rho_i^B\right)$, caso contrário o estado será emaranhado, e o máximo emaranhamento é aquele em que ρ_A e ρ_B são maximamente mistos, isto é, aquele em que o traço da matriz $\rho_{A(B)} = Tr\left(\rho_{A(B)}^2\right)$ é mínimo [36].

Entretanto, o emaranhamento é um recurso físico, existindo várias formas consistentes de medir o grau de emaranhamento, tais como a entropia de Von Neumann [37], a concorrência [38], a transposição parcial positiva (PPT) e a negatividade [39], mas, o objetivo dessa tese não é destacar essas técnicas. Nesse tópico apenas vamos destacar a importância de estados emaranhados, buscando entender suas propriedades, geração e aplicações para informação e computação quântica.

Diante desses argumentos pode-se citar vários estados emaranhados, os mais conhecidos são os estados GHZ (Greenberger–Horne–Zeilinger) e os de Bell, esse segundo com foco nessa tese, onde na Seção 4.2 é proposto um circuito gerador de estados de Bell para qubits de polarização.

As medições de Bell projetam estados de sistemas de dois níveis sobre o conjunto de estados puros maximamente emaranhados ortogonais, (estados de Bell) ou seja, possuem o mais forte grau de correlação não local possível, servindo de base para espaços de dois qubits. A principal motivação para estudar os estados de Bell vem do fato de que eles são ingredientes chave na informação quântica [40].

Os estados de Bell são:

$$\left|\beta_{00}\right\rangle = \frac{\left|00\right\rangle + \left|11\right\rangle}{\sqrt{2}}, \tag{2.14}$$

$$\left|\beta_{01}\right\rangle = \frac{\left|01\right\rangle + \left|10\right\rangle}{\sqrt{2}}, \tag{2.15}$$

$$\left|\beta_{10}\right\rangle = \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}}, \tag{2.16}$$

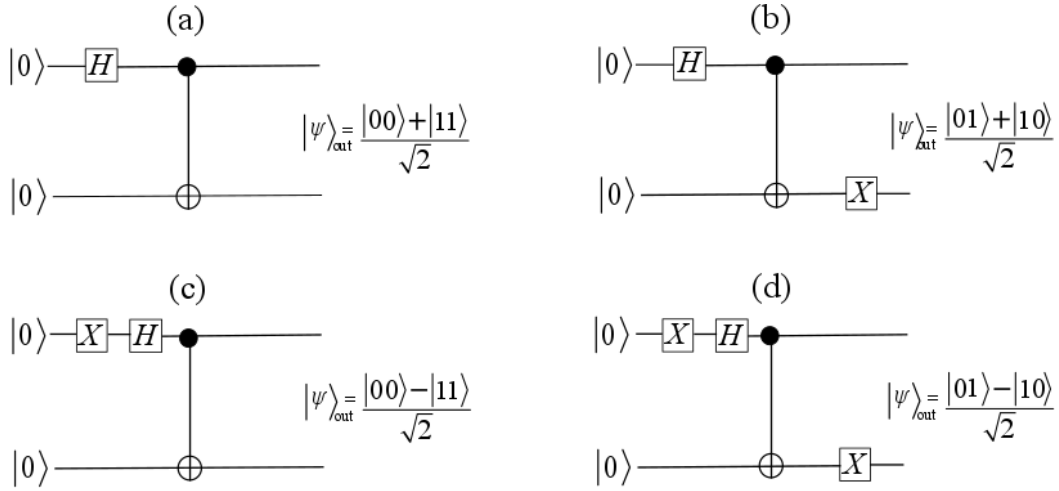
$$\left|\beta_{11}\right\rangle = \frac{\left|00\right\rangle - \left|11\right\rangle}{\sqrt{2}}. \tag{2.17}$$

Os estados de Bell podem ser gerados a partir de circuitos quânticos associando portas de 1 qubit e múltiplos qubits.

A Figura 2.6 mostra que a partir de portas de um qubits (H e X) e de uma porta de dois qubits (CNOT), na ordem apresentada, é possível desenvolver circuitos capazes de gerar os estados de Bell (2.14)-(2.17) a partir do estado de entrada |00⟩.

Os estados emaranhados são recursos que podem ser usadas em computação e comunicação quânticas [41], aplicados por exemplo na codificação superdensa, teletransporte quântico, correção quântica de erros e distribuição quântica de chaves criptográfica [37], [42], substituindo tarefas que até então eram implementadas usando apenas recursos clássicos.

Figura 2.6. Circuitos gerador de estados de Bell, construído a partir de portas Hadamard (*H*), NOT (*X*) e NOT controlada (CNOT).



Fonte: Próprio autor.

2.3. Dispositivos ópticos, qubits fotônicos, parâmetros de Stokes e QND

Nessa Seção conceituaremos os principais dispositivos ópticos utilizados nesse trabalho. Abordaremos sobre qubits fotônicos e os parâmetros de Stokes para estados coerentes bimodais. Apresentaremos os princípios básicos de medição quântica não demolidora (QND).

2.3.1. *Fotodetectores*

Os tipos de fotodetectores mais utilizados em comunicações ópticas para detecção do fóton único são os fotodiodos de avalanche (FDA ou APD) e o fotodiodo PIN. O fotodiodo é um dispositivo de junção semicondutora P-N ou P-I-N, e quando ocorre a absorção dos fótons, sua corrente aumenta. A avalanche corresponde a uma corrente elétrica de magnitude crescente atravessando o fotodiodo e despois de iniciada deve ser anulada para não danificar o componente.

Um fotodetector é qualificado pela sua eficiência quântica e sua contagem de escuro. A eficiência quântica (η) de um detector de fótons, corresponde quando o fotodetector identifica um fóton e realiza sua medição. A contagem de escuro (P_{Dark}) de um fotodetector, corresponde quando mesmo sem detectar fóton (não chega luz) o fotodetector registra uma medição. A probabilidade de detecção de *n* fóton em um fotodetector real pode ser escrita como [43]:

$$P_n = 1-(1-\eta)^n\left(1-P_{Dark}\right). \tag{2.18}$$

Considerando um fotodetector ideal $\eta = 1$ e $P_{Dark} = 0$.

Para um estado coerente a probabilidade de detecção de um fóton em fotodetectores com eficiência quântica (η) e contagem de escuro (P_{Dark}) corresponde [43]:

$$P_{Det} = 1-(1-P_{Dark})e^{-|\alpha|^2\eta} \tag{2.19}$$

2.3.2. *Moduladores de fase*

Moduladores de fase (PM) óptica se baseiam em materiais que permitem que a fase da luz seja modulada em função da tensão ou corrente elétricas de acionamento [44]. O modulador de fase, por sua vez, adiciona uma fase θ ao sinal óptico que o atravessa. O operador unitário correspondente é:

$$\hat{U}(\theta) = e^{i\theta\hat{a}^\dagger\hat{a}}, \tag{2.20}$$

onde θ corresponde a fase adicionada ao sinal que passa por PM, e $\hat{a}$ operador de aniquilação e $\hat{a}^\dagger$ operador de criação. Se o sinal de entrada for um estado coerente $|\alpha\rangle$ em (2.19), na saída do *PM*, o estado será [45]:

$$\hat{U}(\theta)|\alpha\rangle = \left|e^{i\theta}\alpha\right\rangle. \tag{2.21}$$

2.3.3. *Divisores de feixes*

Outro componente é o divisor de feixe (BS) mostrado na Figura 2.7. Fisicamente, trata-se de um espelho semi-refletor. Quando a luz incide sobre este espelho, parte será refletida e parte será transmitida [46].

Um único modo de luz entra no divisor de feixe em cada uma das duas entradas (α_{in} e β_{in}) do BS. Uma fração da energia da luz em cada modo é transmitida $T = cos^2(\theta)$ e refletida $R = 1 - T = sen^2(\theta)$. O ângulo θ depende de fatores do material que constitui o BS e da orientação espacial do espelho. Ao passar pelo divisor de feixe, o estado dos dois modos de entrada irá evoluir de acordo com a transformação.

$$|\psi\rangle_1|\phi\rangle_2 \rightarrow U(\theta)|\xi\rangle_1|\zeta\rangle_2, \tag{2.22}$$

onde, $U(\theta)$ é o operador unitário dado por

$$U(\theta) = e^{\theta(\hat{a}_1\hat{a}_2^\dagger - \hat{a}_1^\dagger\hat{a}_2)}. \tag{2.23}$$

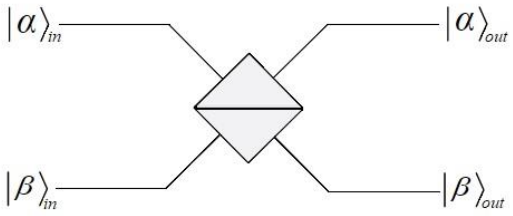
Assim, quando dois estados coerentes $|\alpha\rangle_1$ e $|\beta\rangle_2$ passam pelo BS conforme mostrado na Figura 2.7 seu estado na saída (α_{out} e β_{out}) será.

$$|\alpha\rangle_1|\beta\rangle_2 \xrightarrow{BS} |cos(\theta)\alpha - sen(\theta)\beta\rangle_1 |cos(\theta)\beta + sen(\theta)\alpha\rangle_2 . \quad (2.24)$$

Se $\theta = \pi/4$, tem-se um BS balanceado ($T = R$) e os modos na saída são:

$$|\alpha,\beta\rangle_{12} \xrightarrow{BS} \left|\frac{\alpha-\beta}{\sqrt{2}}, \frac{\alpha+\beta}{\sqrt{2}}\right\rangle_{12} . \quad (2.25)$$

Figura 2.7. O divisor de feixe com transmissão T e reflexão R.

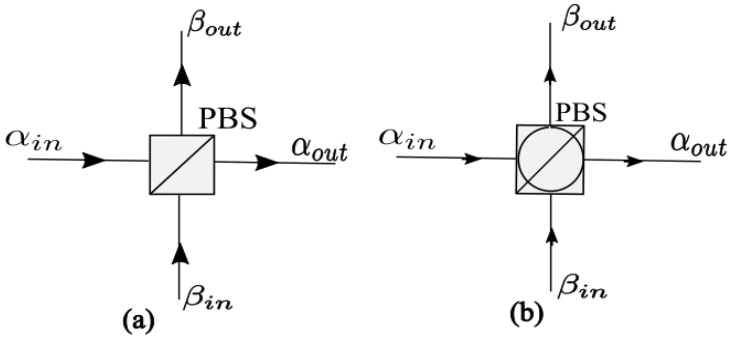


Fonte: Próprio autor.

2.3.4. *Divisor de feixe por polarização*

Outro elemento óptico linear que destacamos aqui é o divisor de feixe de polarização (PBS) conforme mostrado na Figura 2.8. Esse dispositivo direciona a luz nas entradas (α_{in} e β_{in}) para uma das saídas (α_{out} e β_{out}) conforme o estado de polarização. Por exemplo, se o PBS está configurado para funcionar na base HV (polarização horizontal e vertical), Figura 2.8(a), a luz polarizada horizontalmente na entrada α_{in} (β_{in}) é transmitida diretamente para saída α_{out} (β_{out}), por outro lado, se a luz na entrada α_{in} (β_{in}) estiver polarizada na vertical, a mesma será direcionada para saída β_{out} (α_{out}). Funcionamento análogo é para o PBS operando na base diagonal (+45º e -45º), Figura 2.8(b).

Figura 2.8. Divisor de feixe polarizando em diferentes bases de polarização. (a) A base horizontal-vertical. (b) O base diagonal.



Fonte: [43].

2.3.5. *Qubits de polarização e de estados coerentes*

Uma forma simples de representação física de um qubit é a polarização do campo eletromagnético de um fóton (horizontal-*H* e vertical-*V*), conhecida como qubit de polarização [5], [24], [43], [47-48]. Neste caso, os qubits lógicos são codificados por $|0\rangle=|H\rangle$ e $|1\rangle=|V\rangle$. Apesar da simplicidade deste tipo de qubit, para a sua codificação e decodificação, são usados de placas de meia-onda, quarto de onda e divisores de feixes por polarização. Um problema para esse tipo de qubit é o transporte em fibras ópticas devido a descoerência que atuará na atenuação (ou no caso de fótons isolados, absorção), despolarização e/ou dispersão dos qubits.

Outra forma de representação física de qubit em óptica é por meio de estados coerentes. Os estados coerentes são auto-estados do operador de aniquilação $\hat{a}$ (criação, $\hat{a}^\dagger$), com autovalor complexo α ($\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$), e foram introduzidos por R. J. Glauber em 1963 [49]. Eles podem ser escritos na base dos estados de Fock (estados de número de fótons):

$$\left|\alpha\right\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\left|n\right\rangle. \tag{2.26}$$

A ortogonalidade entre os dois estados que representam os qubits lógicos é fundamental em informação quântica, para uma correta distinção das informações. O produto interno entre $|\alpha\rangle$ e $|\beta\rangle$, dois estados coerentes, é dado por:

$$\left\langle\alpha\middle|\beta\right\rangle = \exp\left\{\frac{1}{2}\left[2\alpha^*\beta - \left(|\alpha|^2 + |\beta|^2\right)\right]\right\}. \tag{2.27}$$

Assim, os qubits lógicos são codificados usando $|0\rangle = |-\alpha\rangle$ e $|1\rangle = |\alpha\rangle$, sendo α um número real. Para esse tipo de codificação tem-se:

$$\left|\left\langle\alpha\middle|-\alpha\right\rangle\right|^2 = e^{-4|\alpha|^2}. \tag{2.28}$$

Portanto, para garantir a ortogonalidade entre os estados $|-\alpha\rangle$ e $|\alpha\rangle$, $|\alpha|^2 \geq 4$ [50].

2.3.6. *Parâmetros quânticos de Stokes, e polarização de estados coerentes*

Os parâmetros Stokes podem ser estendidos ao domínio quântico porque podem ser facilmente traduzidos em observáveis verdadeiramente quânticos. Para um sistema quântico, os parâmetros de Stokes são os mesmos operadores correspondentes aos parâmetros de Stokes clássicos [51].

$$S_0 = \hat{a}_1^\dagger.\hat{a}_1 + \hat{a}_2^\dagger.\hat{a}_2, \tag{2.29}$$

$$S_1 = \hat{a}_1^{\dagger}.\hat{a}_1 - \hat{a}_2^{\dagger}.\hat{a}_2^{\dagger}, \tag{2.30}$$

$$S_2 = \hat{a}_1^{\dagger}.\hat{a}_2 + \hat{a}_2^{\dagger}.\hat{a}_1, \tag{2.31}$$

$$S_3 = i\left(\hat{a}_1^{\dagger}.\hat{a}_2 - \hat{a}_2^{\dagger}.\hat{a}_1\right). \tag{2.32}$$

Os termos $\hat{a}$ e $\hat{a}^{\dagger}$ correspondem os operadores de criação e aniquilação, respectivamente aplicados ao primeiro modo do estado, da mesma forma que $\hat{a}$ e $\hat{a}^{\dagger}$ são os operadores de criação e aniquilação, respectivamente aplicados ao segundo modo do estado. Os operadores S_1, S_2 e S_3, não comutam, não sendo possível medir qualquer dois desses parâmetros ao mesmo tempo e obter com certeza seus valores. As relações de comutação desses operadores são:

$$\left[S_n, S_k\right] = i2\varepsilon_{kmn} S_m, \tag{2.33}$$

$$\left[S_0, S_l\right] = 0, \quad l = 1,2,3, \quad n,m,k = 1,2,3. \tag{2.34}$$

Os valores médios e as variâncias dos parâmetros quânticos de Stokes de um estado coerente bimodal $|\alpha,\beta\rangle$ ($|\alpha\rangle$ corresponde à componente da luz polarizada na horizontal e $|\beta\rangle$ a componente polarizada na vertical) são dados por:

$$\left|\alpha,\beta\right\rangle = \sum_{n=0}^{\infty} e^{\frac{-|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}}\left|n\right\rangle \otimes \sum_{k=0}^{\infty} e^{\frac{-|\beta|^2}{2}} \frac{\beta^k}{\sqrt{k!}}\left|k\right\rangle, \tag{2.35}$$

$$\left\langle S_0 \right\rangle = \left|\alpha\right|^2 + \left|\beta\right|^2, \tag{2.36}$$

$$\left\langle S_1 \right\rangle = \left|\alpha\right|^2 - \left|\beta\right|^2, \tag{2.37}$$

$$\left\langle S_2 \right\rangle = (\alpha^* \beta + \alpha\beta^*), \tag{2.38}$$

$$\left\langle S_3 \right\rangle = i(\alpha^* \beta - \alpha\beta^*). \tag{2.39}$$

Os resultados (2.36)-(2.39) são iguais aos valores obtidos classicamente. Entretanto, esses operadores apresentam flutuações, que são demostrados pelas suas variâncias, as quais são definidas como [52]:

$$V_l = \left\langle (\Delta\hat{S})_l^2 \right\rangle = \left\langle \hat{S}_l^2 \right\rangle - \left\langle \hat{S}_l \right\rangle^2, l = \{0,1,2,3\}, \tag{2.40}$$

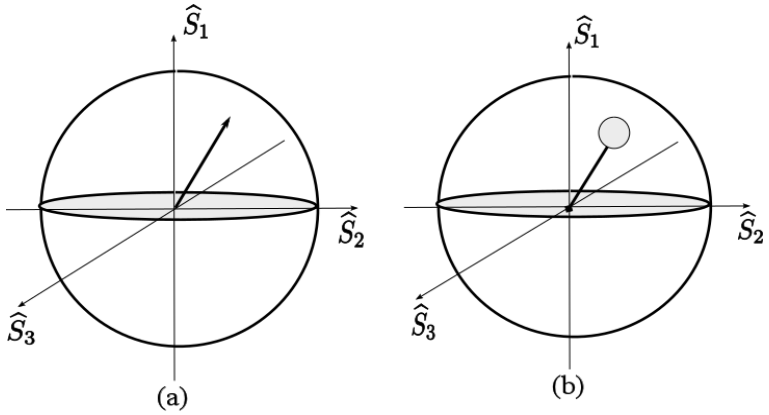
$$\left\langle \hat{S}_l^x \right\rangle = \left\langle \alpha,\beta \middle| \hat{S}_l^x \middle| \alpha,\beta \right\rangle, \text{ para } l \in \{0,1,2,3\}, \text{ e } x \in \{1,2\}. \tag{2.41}$$

A partir do resultado adquirido em (2.36)-(2.39) e substituindo em (2.40), obtemos:

$$V_n = |\alpha|^2 + |\beta|^2 \text{, para } n \in \{1,2,3\}. \tag{2.42}$$

As variâncias de um estado coerente são representadas por um ponto na esfera de Poincaré representados por uma distribuição de probabilidade de estados sobre essa esfera conforme mostrado na Figura 2.9.

Figura 2.9. Representação dos parâmetros de Stokes na esfera de Poincaré; (a) clássico, (b) quântico.



Fonte: próprio autor.

Usando um operador unitário nos dois modos polarizados dos estados $|\alpha,\beta\rangle$, é possível aplicar um deslocamento de fase ϕ, tornando os estados em $\left|\alpha e^{i\theta/2}, \beta e^{i\theta/2}\right\rangle$, o operador unitário U_ϕ , é [53], [54].

$$U_\phi = e^{i\phi \hat{S}_1/2}. \tag{2.43}$$

No entanto para aplicar uma rotação geométrica θ sobre os mesmos estados, o operador unitário R_θ corresponde a:

$$R_\theta = e^{i\theta \hat{S}_3/2}. \tag{2.44}$$

Logo, $\left|\alpha, \beta\right\rangle = \left|\beta sen(\theta) + \alpha cos(\theta), \beta cos(\theta) - \alpha sen(\theta)\right\rangle$ [55].

Se os parâmetros de Stokes são nulos, classicamente a luz é considerada despolarizada, mas, em uma perspectiva quântica, esse fato não é o suficiente para garantir essa afirmação. Logo um feixe de luz é considerado despolarizado, se ao aplicar um operador unitário de rotação sobre as componentes ortogonais de um estado, as propriedades dos observáveis permanecem inalteradas [56], caracterizada pela expressão:

$$\left[\rho, \hat{S}_3\right] = \left[\rho, \hat{S}_1\right] = 0, \tag{2.45}$$

sendo ρ à matriz densidade do estado quântica do campo eletromagnético. Um estado despolarizado pode ser representado da forma geral, como:

$$\rho = \sum_n P_n \frac{1}{n+1} \sum_{k=0}^{n} |n-k\rangle|k\rangle\langle k|\langle n-k|, \tag{2.46}$$

onde, P_n corresponde a função de probabilidade do número de fótons considerando os modos de polarização da luz.

2.3.7. *Medição quântica não demolidora (QND)*

A Medição Quântica não Demolidora (QND) é um conceito importante que foi desenvolvido neste contexto de forma que permite medições repetidas do mesmo autovalor. O QND foi descoberto enquanto buscava-se a detecção ideal de ondas gravitacionais [57]. Como um detector de ondas gravitacionais pode ser modelado como um oscilador harmônico, não demorou muito para se estender esse processo de medida para a radiação eletromagnética, que segue as mesmas equações no caso do campo livre [58], [59]. A principal característica de uma medida QND é que torna possível medir um observável de um sistema sem que sua evolução seja alterada.

O método QND pode ser usado para medir quantidades que correspondem a um operador que se conserva da evolução livre do sistema quântico. A interação entre o aparelho de medição e o sistema medido foi adequadamente planejada para que os autovetores desses operadores não sofram alterações durante a medição. Essa estratégia permite que o dispositivo forneça um resultado preciso, mesmo quando o tempo de resposta for longo comparado ao tempo característico do sistema [60].

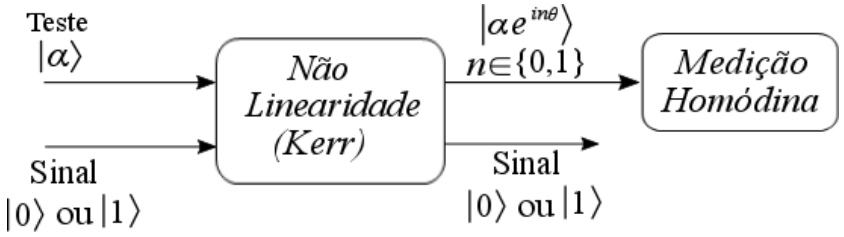
As interações entre fótons ativadas por mecanismos ópticos não lineares desempenham um papel importante no processamento quântico da informação. De fato, os fótons são portadores ideais de informação quântica, pois, são capazes de se propagar à velocidade da luz e, em geral, não são afetados pelo ambiente [61].

Esquemas bem-sucedidos e amplamente explorados para melhorar a não-linearidade de fase são baseados em interações com o meio Kerr entre um campo de teste e um de sinal [62]. Basicamente, a medição QND é baseada no Efeito Kerr, quando n fótons $|n\rangle$ e um estado coerente $|\alpha\rangle$ se propagam em um meio com não-linearidade Kerr cruzada, o estado coerente capta um deslocamento de fase que depende do tempo t de interação e da força do coeficiente não linear κ e do número de fótons do estado sinal, ou seja:

$$e^{i\frac{H_{QND}t}{h}}\left[a|0\rangle+b|n\rangle\right]_s|\alpha\rangle_p=a|0\rangle_s|\alpha\rangle_p+b|n\rangle_s|\alpha e^{in\kappa t}\rangle_p, \quad (2.47)$$

Em (2.46), $H_{QND}=h\kappa a_s^\dagger a_s a_t^\dagger a_t$ é o hamiltoniano, κ é o parâmetro de não linearidade é $a_s^\dagger(a_s)$ são os operadores de criação (aniquilação) do modo sinal enquanto $a_t^\dagger(a_t)$ são os operadores de criação (aniquilação) do modo de teste. O esquema é indicado na Figura 2.10.

Figura 2.10. Medição quântica não demolidora para detecção da presença ou não de um fóton.



Fonte: Próprio autor.

A medição da fase *f* do feixe de teste por detecção homódina determina o número de fótons *n*, do modo sinal, uma vez que $\phi=n\theta$ sendo $\theta=\kappa t$. Por isso, o meio Kerr é colocado dentro de um interferômetro de Mach-Zehnder. Para ser possível detectar a presença de um fóton único, a condição $\theta|\alpha|^2\gg 1$ deve ser satisfeita [63] e [64], onde $|\alpha|^2$ é o número médio de fótons do estado coerente $|\alpha\rangle$.

No entanto, a medição de QND no nível de um único fóton ainda é um problema desafiador. Tecnicamente, a não linearidade dos materiais normais é muito fraca para induzir um grande deslocamento de fase por fóton. Embora a não linearidade Kerr cruzada possa ser melhorada usando o sistema de átomos, normalmente, um fóton único pode causar apenas uma mudança de fase na escala mrad [65]. Dois experimentos recentes em modulação de fase usando Kerr cruzada foram [66], [67], que demonstraram a mudança de fase π rad em nível de fóton único através da não linearidade de Kerr cruzada dos átomos.

Dessa forma, esquemas de medições eficientes e práticos que permitam a integração em redes quânticas estão em carência. Ao longo dessas linhas experimentais, guias de ondas de cristal fotônicos foram propostas e demonstraram ser viáveis para medição QND, embora sejam limitadas pelas propriedades do material [68], mesmo assim muitas demonstrações experimentais foram realizadas nos campos da óptica quântica [69-72], física atômica [73-75] e sistemas de cavidade-QED [76], [77].

3. COMPARADOR QUANTUM-ÓPTICO DE SEQUÊNCIA DE BIT (QBSC)

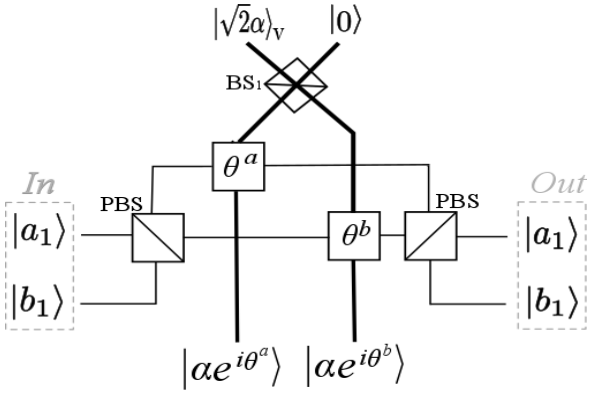
3.1. Introdução

Este Capítulo apresenta a análise do desempenho do hardware óptico capaz de comparar duas sequências de qubits codificados na polarização a partir da detecção quântica não demolidora (QND). Na Seção 3.2 é descrito o funcionamento inicial de uma célula básica do comparador quantum-óptico de sequência de qubits (QBSC), e em seguida, a mesma célula básica é estendida para *n* qubits e seu desempenho é analisado. Na Seção 3.3 é proposta uma outra versão para um QBSC com medição binária ao invés de medição polarimétrica conforme usado na seção anterior que é capaz discriminar dois qubits.

3.2. Implementação óptica do QBSC

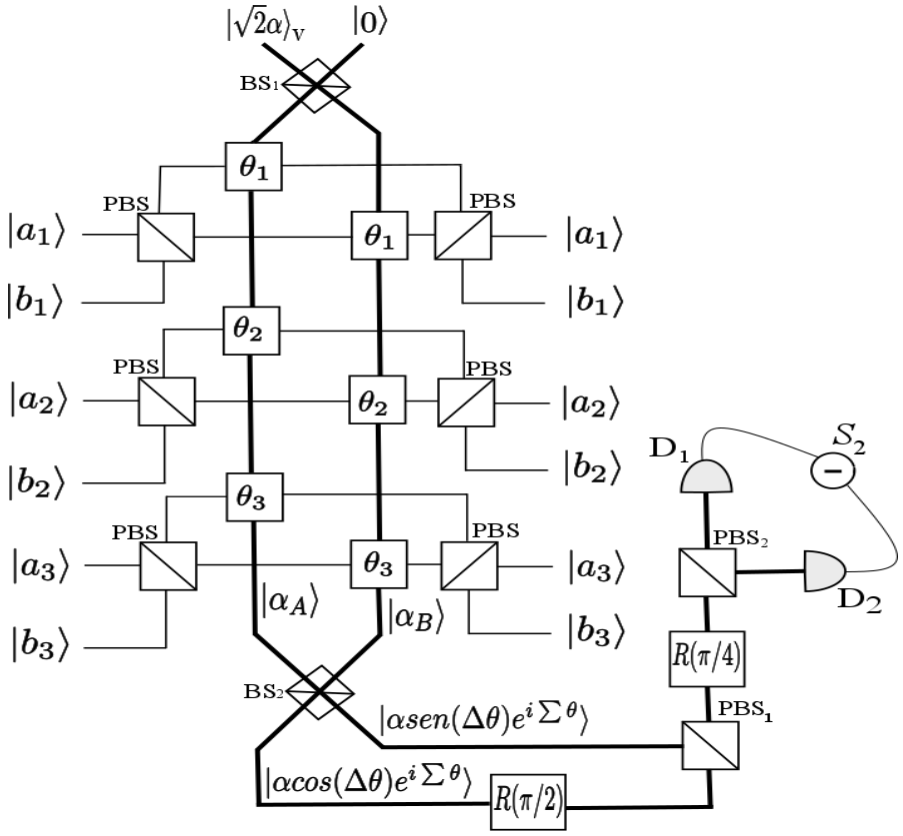
A célula básica óptica que é capaz de comparar dois bits (QBSC) é mostrada na Figura 3.1. Conforme descrito no Capítulo 2, o qubit de polarização $|V\rangle$ que representa o bit lógico '1' é refletido, enquanto o qubit de polarização $|H\rangle$ (bit lógico '0') é transmitido nos divisores de feixes por polarização (PBS's). O estado coerente $|\sqrt{2}\alpha, 0\rangle$ está polarizado verticalmente. Somente o fóton único no modo vertical modulará a fase do estado coerente $|\alpha, \alpha\rangle$ ($|\sqrt{2}\alpha, 0\rangle \xrightarrow{BS} |\alpha, \alpha\rangle$) ao passar pelos meios não lineares (Kerr cruzado), θ^a e θ^b. Obtendo o seguinte estado na saída no aparato básico mostrado na Figura 3.1: $|\alpha e^{i\theta^a}, \alpha e^{i\theta^b}\rangle$, onde a = 1 se $|a\rangle = |V\rangle$ e a = 0 se $|a\rangle = |H\rangle$. A mesma codificação se aplica ao qubit $|b\rangle$. Um QBSC completo que compara duas sequências ($|a\rangle = |a_1,a_2,a_3\rangle$ e $|b\rangle = |b_1,b_2,b_3\rangle$) com três qubits cada, é mostrado na Figura 3.2.

Figura 3.11. Célula óptica básica do QBSC.



Fonte: Próprio autor.

Figura 12. QBSC para três célula óptica básica.



Fonte: Próprio autor.

Como se pode observar na Figura 3.2, existem três células básicas. Os estados coerentes $|\alpha_A\rangle$ e $|\alpha_B\rangle$ obtém um deslocamento de fase acumulado pelos meios não lineares θ_1, θ_2 e θ_3 que depende dos códigos binários $A = \{a_1, a_2, a_3\}$ e $B = \{b_1, b_2, b_3\}$:

$$|\alpha_A\rangle = |\alpha \exp(\theta_1^{a_1} + \theta_2^{a_2} + \theta_3^{a_3})\rangle. \tag{3.1}$$

$$|\alpha_B\rangle = |\alpha \exp(\theta_1^{b_1} + \theta_2^{b_2} + \theta_3^{b_3})\rangle. \tag{3.2}$$

Estes estados, (3.1)-(3.2), sofrem interferência no divisor de feixe BS_2, e os estados de saída serão:

$$|\alpha sin(\Delta\theta)e^{i\Sigma\theta}\rangle_V, \tag{3.3}$$

$$|\alpha cos(\Delta\theta)e^{i\Sigma\theta}\rangle_V, \tag{3.4}$$

$$\Delta\theta = \left[(\theta_1^{a_1} + \theta_2^{a_2} + \theta_3^{a_3}) - (\theta_1^{b_1} + \theta_2^{b_2} + \theta_3^{b_3})\right]/2, \tag{3.5}$$

$$\Sigma\theta = \left[(\theta_1^{a_1} + \theta_2^{a_2} + \theta_3^{a_3}) + (\theta_1^{b_1} + \theta_2^{b_2} + \theta_3^{b_3})\right]/2. \tag{3.6}$$

O estado (3.4) passa pelo rotacionador de polarização $R(\pi/2)$, mudando sua polarização para *H*, então os dois estados coerentes (3.3)-(3.4) são reunidos pelo PBS_1 em um estado $|\psi\rangle$, resultando em:

$$|\psi\rangle = |\alpha sin(\Delta\theta) e^{i\Sigma\theta}\rangle_V \, |\alpha cos(\Delta\theta) e^{i\Sigma\theta}\rangle_H . \tag{3.7}$$

Em seguida. $|\psi\rangle$ passa pelo rotacionador de polarização $R(\pi/4)$, mudando a base de polarização do estado $|\psi\rangle$ para base diagonal $(\pm 45^o)$. Por fim o estado $|\psi\rangle$ tem suas polarizações separadas pelo PBS_2, atingindo os detectores D_1 e D_2 que formam um polarímetro que mede a diferença de potência óptica do sinal, que corresponde ao parâmetro de Stokes S_2. O valor médio e a variância de S_2 são dados por:

$$\langle S_2 \rangle = |\alpha|^2 \, sin(2\Delta\theta), \; V_2 = |\alpha|^2 . \tag{3.8}$$

Considerando

$$\theta_1 > \theta_2 + \theta_3 \text{ e } \theta_2 > \theta_3, \tag{3.9}$$

obtém-se:

$$\text{se } \langle S_2 \rangle > 0 , \text{ temos } A > B , \tag{3.10}$$

$$\text{se } \langle S_2 \rangle = 0 , \text{ temos } A = B , \tag{3.11}$$

$$\text{se } \langle S_2 \rangle < 0, \text{ temos, } A < B. \tag{3.12}$$

Diferentes sequências binárias resultarão em diferentes valores médios das distribuições de $\langle S_2 \rangle$, no entanto, a variância será sempre igual a $|\alpha|^2$. Se assumirmos que D_1 e D_2 são contadores de fóton único, a distribuição de probabilidade de $\langle S_2 \rangle$ é uma distribuição de Skellam, representada nas Figuras 3.3, 3.4, e 3.5, para três códigos binários específicos com $|\alpha|^2$= 500, onde *k* é um inteiro da função de Bessel modificada $I_k(x)$ de primeiro tipo (ver ANEXO B).

Podemos aproximar a distância de Bhattacharya entre duas distribuições de Skellam diferentes por;

$$D = \frac{1}{4} \frac{\left(\langle S_2(\Delta\theta_1)\rangle - \langle S_2(\Delta\theta_2)\rangle\right)^2}{\text{var}\left(S_2(\Delta\theta_1)\right) + \text{var}\left(S_2(\Delta\theta_2)\right)} = \frac{1}{8|\alpha|^2} \left[|\alpha|^2 \, sin(2\Delta\theta_1) - |\alpha|^2 \, sin(2\Delta\theta_2) \right]^2 . \tag{3.13}$$

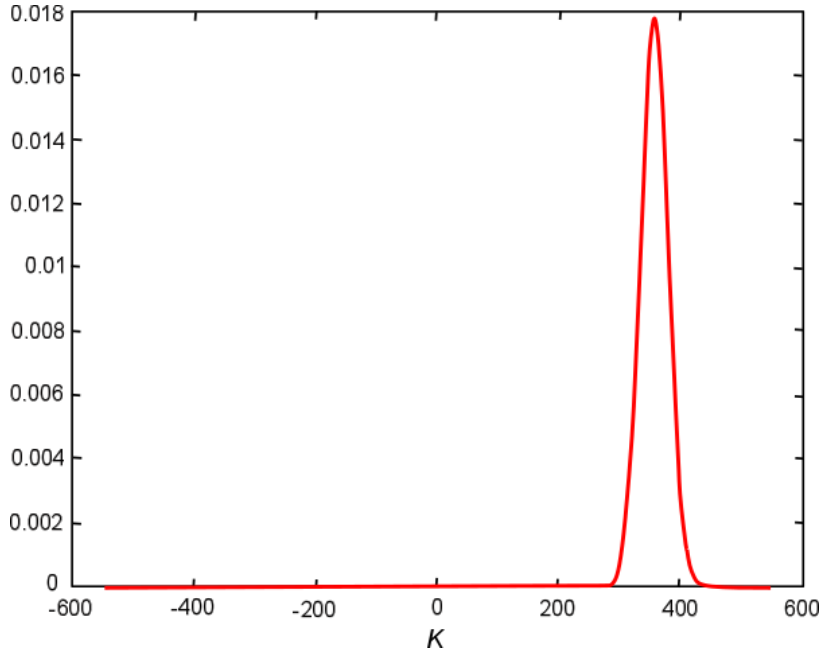
Assim, a distância entre as distribuições para os resultados ”iguais” ($\Delta\theta = 0$), “maior que” ou ‘menor que” ($\Delta\theta = \pm\Delta\theta_{min}$) é equivalente a

$$D = \frac{|\alpha|^2}{8} sin^2(2\Delta\theta_{\min}). \quad (3.14)$$

A Equação (3.14) implica que, quanto maior o número de bits, maior deve ser $|\alpha|^2$ e menor será $\Delta\theta_{min}$ para manter uma taxa de erro baixa. Por exemplo, escolhendo $\theta_1 = \pi/4$, $\theta_2 = \pi/8$ e $\theta_3 = \pi/16$, pode-se facilmente notar que a Equação (3.9) está satisfeita. Além disso, $\Delta\theta_{min} = \pm[\theta_1 - (\theta_2 + \theta_3)] = \pm\theta_3 = \pm\pi/16$ (que aparece na comparação das sequências de bits {[100], [011]} e {[000], [001]}). Neste caso, usando $|\alpha|^2 = 500$ ($D = 25$), a sobreposição entre as distribuições para $S_2(\Delta\theta = 0)$ e $S_2(\Delta\theta = \pi/16)$ é quase zero, o que implica uma taxa de erro próxima à zero.

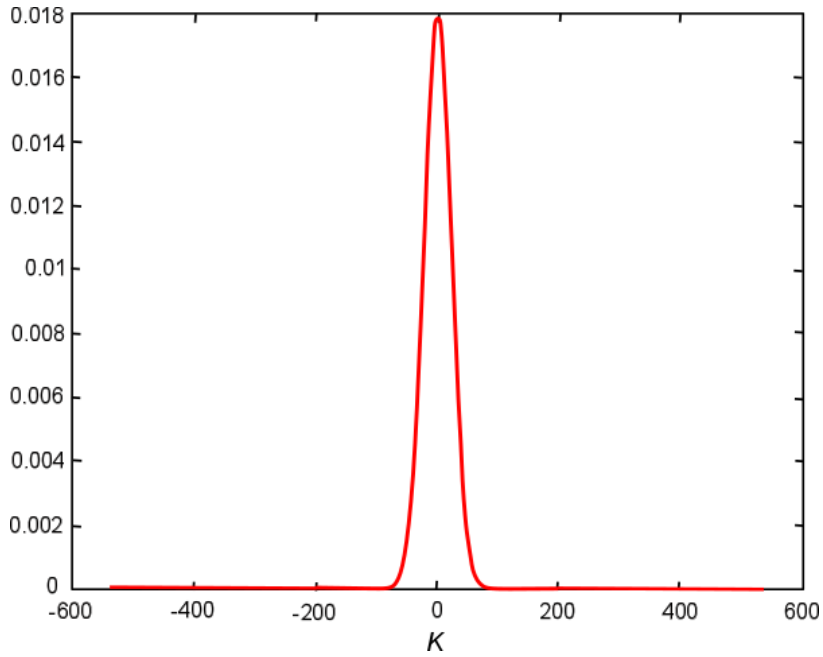
Embora tenhamos mostrado apenas a versão de três qubits, as extensões para um número maior de qubits são simples e possíveis. Para n qubits, a configuração geral passará a ser: $\theta_1 = \pi/4$, $\theta_2 = \theta_1/2$, $\theta_3 = \theta_1/2^2$, ..., $\theta_n = \theta_1/2^{n-1}$. Neste caso, $\Delta\theta_{min} = \pm\theta_1/2^{n-1}$. Para um dado valor de D de acordo com a Equação (3.14), o número médio de fótons do estado coerente usado é $|\alpha|^2 = 8D/sin^2(2\theta_1/2^{n-1})$. Para manter a sobreposição entre as distribuições próximas de zero usamos $D = 25$. Portanto, $|\alpha|^2 = 200/(\pi/2^n)^2$, onde foi usado $sin(\theta) \approx \theta$. Por exemplo, para dez qubits, teremos $|\alpha|^2 = 200/(\pi/2^{10})^2 \approx 2{,}125\times10^7$.

Figura 13. Distribuição de probabilidade do valor médio do parâmetro S_2 com variância V_2 para as sequências $A = \{0,0,1\}$ e $B = \{0,0,0\}$.



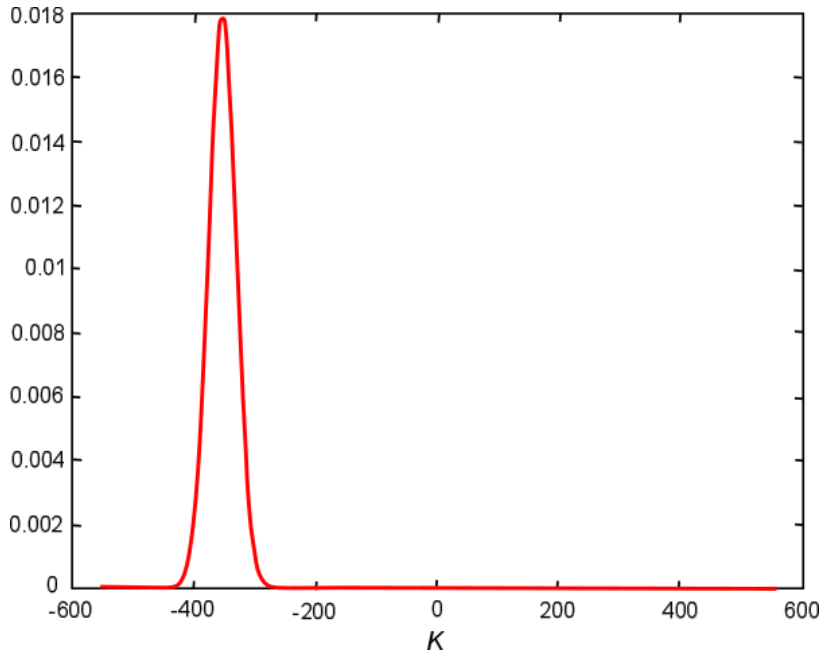
Fonte: Próprio autor.

Figura 14. Distribuição de probabilidade do valor médio do parâmetro S_2 com variância V_2 para as sequências A = {0,0,0} e B = {0,0,0}.



Fonte: Próprio autor.

Figura 15. Distribuição de probabilidade do valor médio do parâmetro S_2 com variância V_2 para as sequências A = {0,0,0} e B = {0,0,1}.



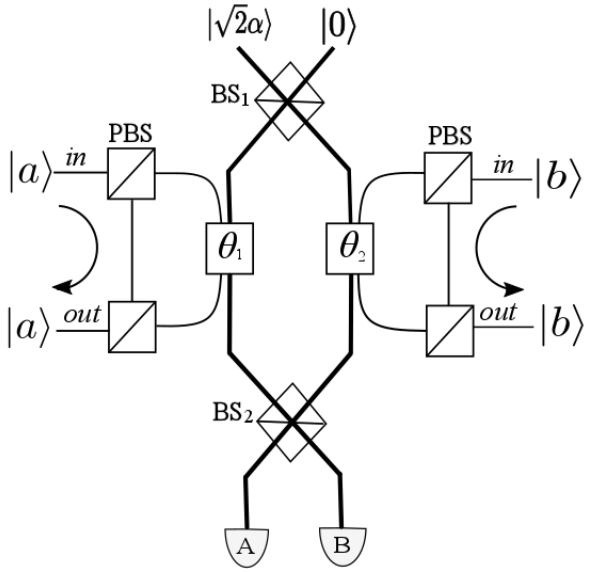
Fonte: Próprio autor.

3.3. QBSC com detecção binária ou contadores de fótons

A partir da proposta da célula óptica básica do QBSC para 2 qubits apresentado na Figura 3.1, desenvolvemos uma outro versão de um QBSC, também para 2 qubits com um sistema de medição mais simples.

A principal diferença entre os dois aparatos ópticos do QBSC propostos, apesar do hardware óptico apresentado na Figura 3.7 ter dois PBS adicionais, está no sistema de medição dos estados coerentes: no QBSC mostrado na Figura 3.2 foi usado um sistema polarímetro enquanto o sistema de medição usado no QBSC mostrado na Figura 3.7 é do tipo de detecção binária (*on-off*). Essa nova versão proposta pode usar fotodiodos PIN para identificar se os qubits são iguais ou diferentes ou contadores de fótons se deseja conhecer os valores dos qubits comparados. O funcionamento e a codificação desse tipo de QBSC é o mesmo do comparador descrito na Seção 3.2.

Figura 16. Célula óptica QBSC com sistema de detecção binária.



Fonte: Próprio autor.

Na Figura 3.6 o estado de entrada, considerando os possíveis estados de $|a,b\rangle$, corresponde a;

$$\begin{aligned}|\psi\rangle_{in} &\simeq |a,b\rangle_{ab}|\alpha,\alpha\rangle_{12} \\ &= |HH\rangle_{ab}|\alpha,\alpha\rangle_{12} + |HV\rangle_{ab}|\alpha,\alpha\rangle_{12} + |VH\rangle_{ab}|\alpha,\alpha\rangle_{12} + |VV\rangle_{ab}|\alpha,\alpha\rangle_{12}.\end{aligned} \tag{3.15}$$

E o estado após passar pelos meios Kerr (θ_1 e θ_2) será;

$$|\psi\rangle \simeq |HH\rangle_{ab}\left|\alpha e^{i\theta_1},\alpha e^{i\theta_2}\right\rangle_{12} + |HV\rangle_{ab}\left|\alpha e^{i\theta_1},\alpha\right\rangle_{12} + |VH\rangle_{ab}\left|\alpha,\alpha e^{i\theta_2}\right\rangle_{12} + |VV\rangle_{ab}|\alpha,\alpha\rangle_{12}. \tag{3.16}$$

Então, se $\theta_1 = \theta_2 = \pi$, o estado de saída, após o BS_2 e antes de *A* e *B*, será;

$$|\psi\rangle_{out} \simeq |HH\rangle_{ab}\left|0,-\sqrt{2}\alpha\right\rangle_{12} + |HV\rangle_{ab}\left|-\sqrt{2}\alpha,0\right\rangle_{12} + |VH\rangle_{ab}\left|\sqrt{2}\alpha,0\right\rangle_{12} + |VV\rangle_{ab}\left|0,\sqrt{2}\alpha\right\rangle_{12}. \tag{3.17}$$

Analisando os estados de saída (3.17), verifica-se que:

- Se A e B forem fotodetectores simples, sempre que ocorrer detecção em A e não houver detecção em B, concluir-se que os qubits $|a\rangle$ e $|b\rangle$ são diferentes. e o contrário, sempre que ocorrer detecção em B e não houver detecção em A pode-se concluir que os qubits $|a\rangle$ e $|b\rangle$ são iguais, mas, nesse caso não é possível diferenciar a ordem dos bits detectados.
- Mas, se A e B forem contadores de fótons, conclui-se que, se ocorrer a contagem par de fótons em A e não houver detecção em B, $a > b$ ($|a,b\rangle = |V,H\rangle$), mas se a contagem for impar em A, $a < b$ ($|a,b\rangle = |H,V\rangle$). Por outro lado, se não houve contagem de fótons em A e ocorrer uma contagem par de fótons em B, $a = b$ ($|a,b\rangle = |V,V\rangle$), mas se a contagem for ímpar em B, $a = b$ ($|a,b\rangle = |H,H\rangle$).

Portanto, o aparato óptico apresentado na Figura 3.6 pode funcionar como circuito de discriminador quantidade ou qualitativo de dois qubits conforme o tipo de detectores utilizados.

4. APLICAÇÕES DO QBSC

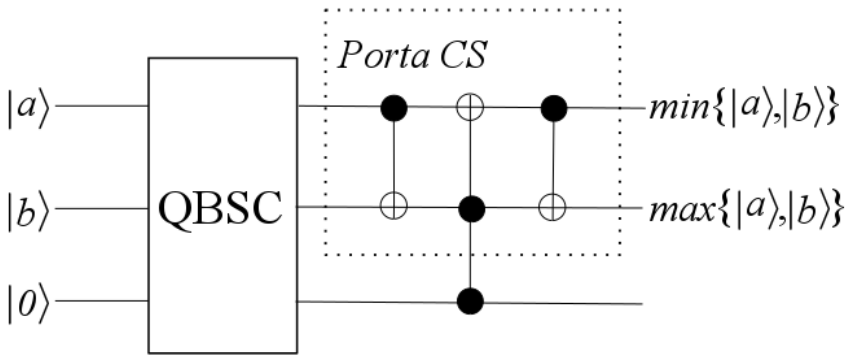
4.1. Introdução

Nesse capítulo propomos duas aplicações usando QBSC: um hardware óptico que implementa um algoritmo ordenador de sequências de qubits e um gerador de estados de Bell.

4.2. Aplicação do QBSC como ordenador de sequências de qubits

Apresentamos uma proposta de circuito baseado no QBSC mostrado na Figura 3.2 que é capaz de implementar o algoritmo quântico de ordenação de qubits descrito em [31]. Esse circuito é mostrado na Figura 4.1 e uma porta CSWAP é usada na saída do QBSC. Nesse caso, a porta CSWAP é composta por três portas CNOTs. Assim, para implementar o circuito quântico na Figura 4.1, precisamos de portas CNOTs para qubits de polarização. Existem diferentes implementações de portas CNOTs. Aqui nós consideramos o descrito em [17]. Como utiliza apenas dispositivos ópticos lineares para implementar uma função não linear, é uma porta probabilística. A porta CNOT para qubits de polarização usando óptica linear é mostrada na Figura 4.2 [17].

Figura 17. Circuito de ordenação quântica com QBSC e uma porta CSWAP (CS).



Fonte: Próprio autor.

A configuração óptica mostrada na Figura 4.2 implementa a porta CNOT somente quando um fóton único é detectado em D_1 ou D_2 e outro fóton único é detectado em D_3 ou D_4. O estado de saída da configuração na Figura 4.1 é [17]:

$$\left|\Psi_f\right\rangle = \frac{1}{4}\left[\left|+,\ H\right\rangle\left|\psi_1\right\rangle + \left|-,\ H\right\rangle\left|\psi_2\right\rangle + \left|+,V\right\rangle\left|\psi_3\right\rangle + \left|-,V\right\rangle\left|\psi_4\right\rangle\right] + \frac{\sqrt{3}}{2}\left|\Psi_u\right\rangle, \tag{4.1}$$

$$\left|\psi_1\right\rangle = \left[\alpha\lambda\left|HH\right\rangle_{ct} + \ \alpha\sigma\left|HV\right\rangle_{ct} + \beta\lambda\left|VV\right\rangle_{ct} + \ \beta\sigma\left|VH\right\rangle_{ct}\right], \tag{4.2}$$

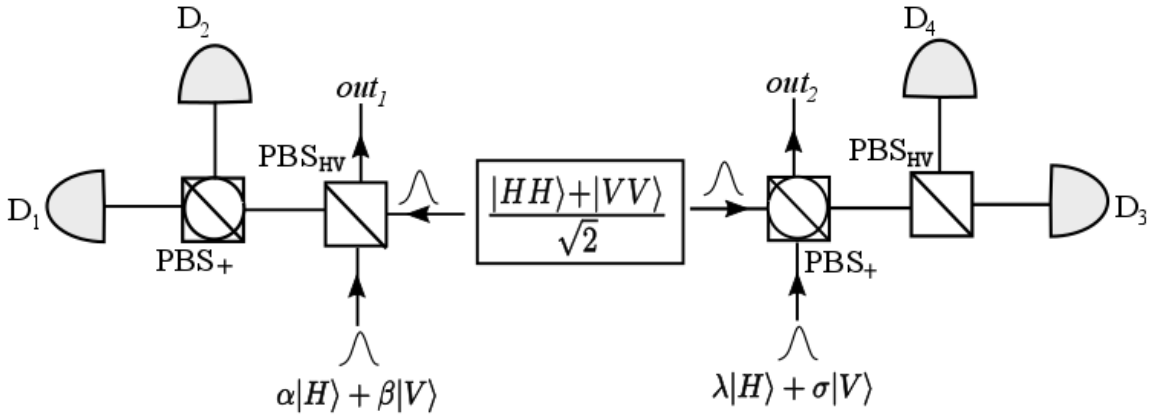
$$|\psi_2\rangle = \left[-\alpha\lambda|HH\rangle_{ct} - \alpha\sigma|HV\rangle_{ct} + \beta\lambda|VV\rangle_{ct} + \beta\sigma|VH\rangle_{ct}\right] = \left[(XZX \otimes I)\right]|\psi_1\rangle, \quad (4.3)$$

$$|\psi_3\rangle = \left[\alpha\lambda|HV\rangle_{ct} + \alpha\sigma|HH\rangle_{ct} + \beta\lambda|VH\rangle_{ct} + \beta\sigma|VV\rangle_{ct}\right] = \left[(I \otimes X)\right]|\psi_1\rangle, \quad (4.4)$$

$$|\psi_4\rangle = \left[-\alpha\lambda|HV\rangle_{ct} - \alpha\sigma|HH\rangle_{ct} + \beta\lambda|VH\rangle_{ct} + \beta\sigma|VV\rangle_{ct}\right] = (XZX \otimes I)(I \otimes X)|\psi_1\rangle. \quad (4.5)$$

Em (4.1) $|\Psi_u\rangle$ é a parte inútil que contém as situações em que nenhum ou dois fótons foram detectados em $D_{1\text{-}2}$ e/ou $D_{3\text{-}4}$. Além disso, $|+, H(V)\rangle$ significa um fóton único indo para D_1 e outro fóton único indo para D_3 (D_4), enquanto $|-, H(V)\rangle$ um fóton único indo para D_2 e outro fóton único indo para D_3 (D_4). Considerando a correção de erros (por exemplo, detecções em D_2 e D_3 → XZX no qubit de controle) requeridas por $|\psi_2\rangle, |\psi_3\rangle$ e $|\psi_4\rangle$, a probabilidade de sucesso é 1/4. Por outro lado, se em vez do estado emaranhado $(|HH\rangle + |VV\rangle)/2^{1/2}$ se usar o estado desemaranhado $(|HH\rangle + |VH\rangle)/2^{1/2}$, então a operação realizada é a operação Identidade com probabilidade de sucesso também igual a 1/4.

Figura 18. Porta CNOT implementada com dispositivos ópticos lineares: divisores de feixe de polarização PBS, PBSHV (PBS em base horizontal-vertical), PBS± (PBS em base diagonal ($\pi/4$, $3\pi/4$)). D_{1-4} são detectores de fótons únicos.



Fonte: [17].

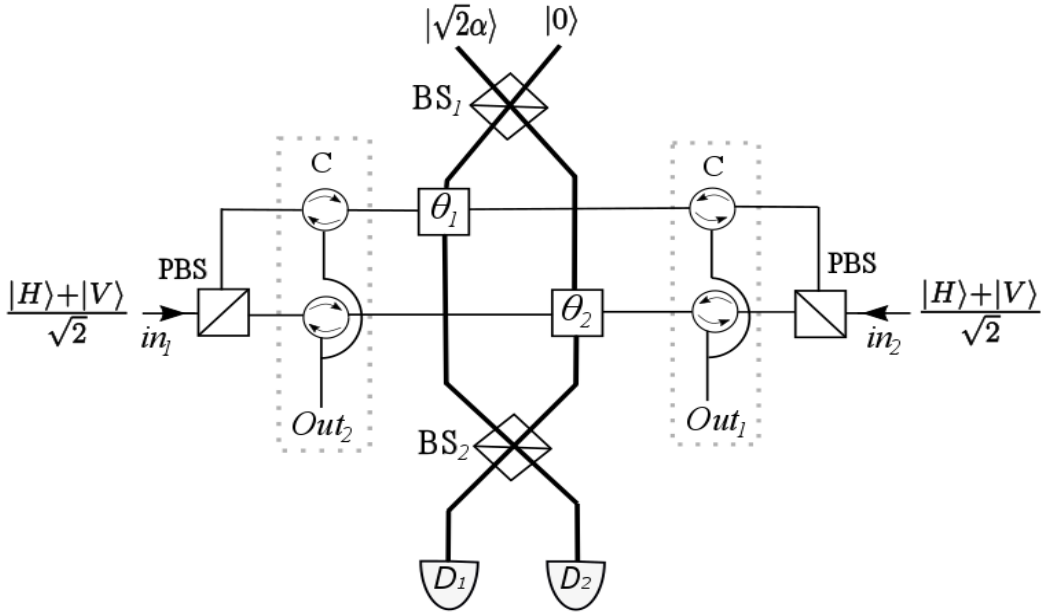
A porta CS na Figura 4.1 pode ser construída com três CNOTs do tipo mostrado na Figura 4.1. O sinal do parâmetro Stokes S_2 medido é usado para selecionar entre uma fonte de pares de fótons emaranhados que produz $(|HH\rangle + |VV\rangle)/2^{1/2}$ e a fonte de pares de fótons desmaranhados que produz $(|HH\rangle + |VH\rangle)/2^{1/2}$. Usando três dessas portas CNOTs ou Identidade, a probabilidade de sucesso é de 1/64 por bit (a CNOT invertida tem a mesma probabilidade de sucesso que a CNOT comum). A porta CS em [31] tem probabilidade de

sucesso igual a 1/162. Para trocar sequências com *n* qubits, *n* portas CS são usadas, portanto, a probabilidade total de sucesso é $(1/64)^n$.

4.3. Aplicação do QBSC como gerador de estados de Bell

Os estados de Bell são fundamentais para comunicação e computação quânticas, portanto, baseado na Figura 4.3, apresentamos uma aplicação do QBSC como gerador de estados de Bell para qubits de polarização e seu aparato óptico é mostrado na Figura 4.3.

Figura 19. Circuito gerador de estados de Bell.



Fonte: Próprio autor.

Na Figura 4.3, o par de estados coerentes $|\alpha,\alpha\rangle$, na saída do BS_1, é modulado tanto por $|H\rangle$ quanto $|V\rangle$ conforme os estados de entradas em in_1 e in_2 $[(|H\rangle+|H\rangle)/2^{1/2}]$. Antes de cada saída, Out_1 e Out_2, circuladores ópticos (C) foram posicionados que permitem a luz passar apenas no sentido indicado. O estado de entrada do circuito corresponde a

$$\begin{aligned}|\psi\rangle_{in} &= \left(\frac{|H\rangle+|V\rangle}{\sqrt{2}}\right)_1 \otimes \left(\frac{|H\rangle+|V\rangle}{\sqrt{2}}\right)_2 \otimes |\alpha\rangle_A \otimes |\alpha\rangle_B = \\ &= \frac{1}{2}\left(|HH\rangle_{12}|\alpha\rangle_A|\alpha\rangle_B + |HV\rangle_{12}|\alpha\rangle_A|\alpha\rangle_B + |VH\rangle_{12}|\alpha\rangle_A|\alpha\rangle_B + |VV\rangle_{12}|\alpha\rangle_A|\alpha\rangle_B\right).\end{aligned} \tag{4.6}$$

Considerando a sincronização perfeita entre os qubits de polarização e os estados coerentes em θ_1 e θ_2, o estado resultando antes do BS_2 é

$$|\psi\rangle_{out} = \frac{1}{2}\Big(|HH\rangle_{12}|\alpha\rangle_A|\alpha e^{i2\theta_2}\rangle_B + |HV\rangle_{12}|\alpha e^{i\theta_1}\rangle_A|\alpha e^{i\theta_2}\rangle_B + |VH\rangle_{12}|\alpha e^{i\theta_1}\rangle_A|\alpha e^{i\theta_2}\rangle_B + |VV\rangle_{12}|\alpha e^{i2\theta_1}\rangle_A|\alpha\rangle_B\Big). \quad (4.7)$$

Se $\theta_1 = \theta_2 = \pi/2$, então, o estado (4.7) será

$$|\psi\rangle_{out} = \frac{1}{2}\Big(|HH\rangle_{12}|\alpha\rangle_A|-\alpha\rangle_B + |HV\rangle_{12}|i\alpha\rangle_A|i\alpha\rangle_B + |VH\rangle_{12}|i\alpha\rangle_A|i\alpha\rangle_B + |VV\rangle_{12}|-\alpha\rangle_A|\alpha\rangle_B\Big). \quad (4.8)$$

E após o BS_2, estado na saída é

$$|\psi\rangle_{out} = \frac{1}{\sqrt{2}}\left[\left(\frac{|HH\rangle_{12}+|VV\rangle_{12}}{\sqrt{2}}\right)|\pm\sqrt{2}\alpha\rangle_A|0\rangle_B + \left(\frac{|HV\rangle_{12}+|VH\rangle_{12}}{\sqrt{2}}\right)|0\rangle_A|i\sqrt{2}\alpha\rangle_B\right] \quad (4.9)$$

Analisando o estado (4.9), conclui-se: quando houver apenas detecção em D_A (*on*) e nenhuma detecção em D_B (*off*), o estado gerado nas saídas Out_1 e Out_2 é o estado emaranhado $|\beta_{00}\rangle = |HH\rangle + |VV\rangle/2^{1/2}$ (2.13); caso contrário, quando houver detecção apenas no D_B, o estado gerado será $|\beta_{01}\rangle = |HV\rangle + |VH\rangle/2^{1/2}$ (2.15).

A Tabela 4.1 mostra todos os estados de Bell gerados pelo sistema mostrado na Figura 4.3 conforme os estados de entrada: $|\pm\rangle = |H\rangle \pm |V\rangle/2^{1/2}$.

Tabela 4.1. Estados de Bell produzidos pelo gerador proposto a partir dos estados de entrada.

Entrada 1 (In 1)	***Entrada 2 (In 2)***	D_1	D_2	***Estado gerado***
$\|+\rangle(\|-\rangle)$	$\|+\rangle(\|-\rangle)$	*on*	*off*	$\|\beta_{00}\rangle$ *(2.14)*
		off	*on*	$\|\beta_{01}\rangle$ *(2.15)*
$\|-\rangle(\|+\rangle)$	$\|-\rangle(\|+\rangle)$	*off*	*on*	$\|\beta_{10}\rangle$ *(2.16)*
		on	*off*	$\|\beta_{11}\rangle$ *(2.17)*

Fonte: Próprio Autor.

CONCLUSÃO

O comparador de sequência de qubits permite a implementação de algoritmos quânticos usando declarações condicionais, uma estrutura fundamental para o projeto de algoritmos. Isso aumenta o número de aplicações onde os algoritmos quânticos podem ser usados e, ao mesmo tempo, aproxima os programadores quânticos de técnicas de sucesso usadas na computação clássica baseada em comparações.

Neste trabalho, apresentamos uma configuração óptica para implementação prática do QBSC. A não linearidade cruzada de Kerr desempenha um papel crucial, portanto, novos materiais com alto valor de κ permitirão a implementação prática do QBSC aqui proposto. Os três parâmetros importantes no QBSC proposto são: o número de qubits, a taxa de erro aceitável é $|\alpha|^2$, e a potência óptica do estado coerente. A taxa de erro diminui quando $|\alpha|^2$ aumenta. Em geral, quando o número de qubits aumenta, a potência óptica necessária para manter uma taxa de erro baixa aumenta exponencialmente, portanto, para este tipo de tecnologia, o número de qubits não pode ser muito grande.

Apresentamos também um hardware óptico, a partir do QBSC proposto, que é capaz de implementar um algoritmo quântico de ordenação de sequências de qubits conforme descrito em [28]. Também foi proposto um circuito óptico gerador de estados de Bell baseado no QBSC que é possível gerar todos os estados de Bell para qubits de polarização. Existem várias aplicações desses estados para a computação e comunicação quânticas, por exemplo: codificação superdensa, teletransporte quântico, correção quântica de erros e distribuição quântica de chaves criptográfica. Outras dificuldades de implementação dos sistemas propostos com dispositivos discretos em fibra óptica são a sincronização e despolarização da luz.

Entre as perspectivas de atividades decorrentes desse trabalho, podemos destacar:

- Análise do desempenho do sistema proposto considerando dispositivos reais;
- utilização do sistema para outros tipos físicos de qubits;
- avaliar a possibilidade de desenvolvimento de protocolos e algoritmos de comunicações para comunicações quânticas;
- desenvolvimento de um modelo do sistema integrado em silício.

REFERÊNCIAS

[1] SHOR, Peter, W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM review**, v. 41, n. 2, p. 303-332, 1999.

[2] GROVER, Lov, K. Quantum mechanics helps in searching for a needle in a haystack. **Physical review letters**, 79(2), 325, 1997.

[3] MASOUD, Mohseni; PETER, Read; HARTMUT, Neven; BOIXO, Sergio. Commercialize quantum technologies in five years. **Nature News**, v. 543, n. 7644, p. 171, 2017.

[4] MILBURN, Gerard, J. Quantum optical Fredkin gate. **Physical Review Letters**, v. 62, n. 18, p. 2124, 1989.

[5] KNILL, Emanuel; LAFLAMME, Raymond; MILBURN, Gerald. A scheme for efficient quantum computation with linear optics. **Nature**, v. 409, n. 6816, p. 46, 2001.

[6] LINKE, Norbert M.; MASLOV, Dmitri; ROETTELER, Martin; DEBNATH, Shantanu; FIGGATT, Caroline; LANDSMAN, Kevin; WRIGHT, Kenneth; MONROE, Christopher. Experimental comparison of two quantum computing architectures. **Proceedings of the National Academy of Sc**iences, v. 114, n. 13, p. 3305-3310, 2017..

[7] PÉREZ-DELGADO, Carlos A.; KOK, Pieter. Quantum computers: Definition and implementations**. Physical Review A**, v. 83, n. 1, p. 012303, 2011.

[8] SILVA, Marcus, P.; LANDON-CARDINAL Olivier; POULIN, David. Practical characterization of quantum devices without tomography, **Physical Review Letters**, v. 107, n. 21, 2011.

[9] OLIVEIRA, Sena D.; DE SOUSA, Benicio P.; RAMOS, Viana R. Quantum search algorithm using quantum bit string comparator. **International Telecommunications Symposium**. IEEE, p. 582-585, 2006.

[10] DE SOUSA, Benicio P.; RAMOS, Viana R. Multiplayer quantum games and its application as access controller in architecture of quantum computers. **arXiv preprint arXiv**:**0802.3684**, 2008.

[11] YUAN, Suzhen; MAO, Xia; Li, Tian; Xue, Yuli; Chen, Lijiang. Quantum morphology operations based on quantum representation mode. **Quantum Information Processing**, v. 14, n. 5, p. 1625-1645, 2015.

[12] CARAIMAN, Simona; MANTA, Vasile. Histogram-based segmentation of quantum images. **Quantum Information Processing**, v. 14, n. 5, p. 1625-1645, 2015.

[13] SHI, Jin Jing; SHI, Rong Hua; GUO, Ying; PENG, XiaoQi, TANG, Ying. Batch proxy quantum blind signature scheme. **Science China Information Sciences**, v. 56, n. 5, p. 1-9, 2013.

[14] BOTSINIS, Panagiotis; ALANIS, Dimitrios; BABAR, Zunaira; NGUYEN, Hung Viet; CHANDRA, Daryus; NG, Soon Xin; HANZO, Lajos. Quantum-aided multiuser transmission in non-orthogonal multiple access systems. **IEEE Access**, v. 4, p. 7402-7424, 2016.

[15] YAN, Fei; ILIYASU, Abdullah; VENEGAS-ANDRACA, Salvador. A survey of quantum image representations. **Quantum Information Processing**, v. 15, n. 1, p. 1-35, 2016.

[16] OLIVEIRA, Sena, D.; RAMOS, Viana R. Quantum bit string comparator: circuits and applications. **Quantum Computers and Computing**, v. 7, n. 1, p. 17-26, 2007.

[17] SILVA, João, B.; RAMOS, Viana R. Implementations of Quantum and Classical Gates With Linear Optical Devices and Photon Number Quantum Non-Demolition Measurement for Polarization Encoded Qubits. **Physics Letters A**, v. 359, n. 6, p. 592-596, 2006.

[18] AARONSON, Scott. The limits of quantum computers. **Scientific American**, v. 298, n. 3, p. 62-69, 2008.

[19] NIELSEN, Michael, A.; CHUANG, Isaac, L. **Quantum Computation and Quantum Information**, Cambridge University Press, 2002.

[20] RIEFFEL, Eleanor; POLAK, Wolfgang. An introduction to quantum computing for non-physicists. **ACM Computing Surveys (CSUR)**, v. 32, n. 3, p. 300-335, 2000.

[21] PHILLIP, Kaye; RAYMOND, Laflamme; MICHELE; Mosca. **An Introduction. To Quantum Computing**. Oxford University Press on Demand, 2007.

[22] HOFMANN, Holger, F.; TAKEUCHI, Shigeki. Quantum phase gate for photonic qubits using only beam splitters and post selection. **Physical Review A**, v. 66, n. 2, p. 024308, 2002.

[23] RALPH, Timothy, C.; LANGFORD, Nathan; BELL, Tamyka; WHITE, Andrew. Linear optical controlled-NOT gate in the coincidence basis. **Physical Review A**, v. 65, n. 6, p. 062324, 2002.

[24] RALPH, Timothy, C.; WHITE, Andrew; MUNRO, William; MILBURN, Gerald. Simple scheme for efficient linear optics quantum gates. **Physical Review A**, v. 65, n. 1, p. 012314, 2001.

[25] NIELSEN, Michael, A. Optical Quantum Computation Using Cluster States. **Physical review letters**, v. 93, n. 4, p. 040503, 2004.

[26] PITTMAN, Todd, B; JACOBE, Bart, C; FRANSON, James, D. Demonstration of nondeterministic quantum logic operations using linear optical elements. **Physical Review Letters**, v. 88, n. 25, p. 257902, 2002.

[27] SANAKA, Kaoru; KAWAHARA, Karin; KUGA, Takahiro. Experimental probabilistic manipulation of down-converted photon pairs using unbalanced interferometers. **Physical Review A**, v. 66, n. 4, p. 040301, 2002.

[28] O'BRIEN Jeremy, L.; PRYDE, Geoff, J.; WHITE, Andrew, G; RALPH, Timothy, C.; BRANNING, David. Demonstration of an all-optical quantum controlled-NOT gate. **Nature**, v. 426, n. 6964, p. 264-267, 2003.

[29] O'BRIEN Jeremy, L.; PRYDE, Geoff, J.; GILCHRIST, Alexei; JAMES, Daniel, F. V.; LANGFORD, Nathan, K.; RALPH, Timothy, C.; WHITE, Andrew, G. Quantum process tomography of a controlled-NOT gate. **Physical review letters**, v. 93, n. 8, p. 080502, 2004.

[30] ZHAO, Zhi; ZHANG, An-Ning; CHEN, Yu-Ao; ZHANG, Han; DU, Jiang-Feng; YANG, Tao; PAN, Jian-Wei. Experimental demonstration of a nondestructive controlled-NOT quantum gate for two independent photon qubits. **Physical review letters**, v. 94, n. 3, p. 030501, 2005.

[31] CHENG, Sheng-Tzong; WANG, Chun-Yen. Quantum switching and quantum merge sorting. **IEEE Transactions on Circuits and Systems I: Regular Papers**, v. 53, n. 2, p. 316-325, 2006.

[32] ONO, Takafumi; RYO, Okamoto; TANIDA, Masato; HOFMANN, Holger F.; TAKEUCH, Shigeki. Implementation of a quantum controlled-SWAP gate with photonic circuits. **Scientific reports**, v. 7, n. 1, p. 1-9, 2017.

[33] PITTMAN, Todd, B; JACOBE, Bart, C; FRANSON, James, D. Probabilistic quantum logic operations using polarizing beam splitters. **Physical Review A**, v. 64, n. 6, p. 062311, 2001.

[34] GIUSTINA, Marise; VERSTEEGH, Marijn A. M.; WENGEROWSKY, Sören; HANDSTEINER, Johannes; HOCHRAINER, Armin; PHELAN, Steinlechner, F. Significant-loophole-free test of Bell's theorem with entangled photons. **Physical review letters**, v. 115, n. 25, p. 250401, 2015.

[35] THEW, Roy, T; ACIN, Antonio; ZBINDEN, Hugo; GISIN, Nicolas. Bell-Type Test for Energy Time Entangled Qutrits. **Physical review letters**, v. 93, n. 1, p. 010503, 2004.

[36] LI, Jun, L.; QIAO, Cong-Feng. A necessary and sufficient criterion for the separability of quantum state. **Scientific reports**, v. 8, n. 1, p. 1-9, 2018.

[37] WOOTTERS, William, K. Entanglement of Formation of an Arbitrary State of two Qubits. **Physical Review Letters**, v. 80, n. 10, p. 2245, 1998.

[38] HORODECKI, Michał; HORODECKI, Paweł; HORODECKI, Ryszard. Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps. **Physics Letters A**, v. 283, n. 1-2, p. 1-7, 2001.

[39] VIDAL, Guifré; WERNER, Reinhard, F. Computable Measure of Entanglement. **Physical Review A**, v. 65, n. 3, p. 032314, 2002.

[40] LÜTKENHAUS, Norbert; CALSAMIGLIA, John; SUOMINEN, Kalle-Antti. Bell measurements for teleportation. **Physical Review A**, v. 59, n. 5, p. 3295, 1999.

[41] REIMER, Christian; KUES, Michael; ROZTOCKI, Piotr; WETZEL, Benjamin; GRAZIOSO, Fabio; LITTLE, Brent E; ... & MORANDOTTI, Roberto. Generation of multiphoton entangled quantum states by means of integrated frequency combs. **Science**, v. 351, n. 6278, p. 1176-1180, 2016.

[42] BOUWMEESTER, Dirk; ZEILINGER, Anton. The Physics of Quantum Information: Basic Concepts. **In the Physics of Quantum Information**, p. 1-14. Springer, Berlin, Heidelberg, 2000.

[43] DERENIAK, Eustace, L.; CROWE, Devon, G. **Optical Radiation Detectors**. John Wiley & Sons, New York, 1984.

[44] WINZER peter; ESSIAMBRE, René-Jean. Advanced optical modulation formats. **Optical Fiber Telecommunications**, VB, n. 5, p. 23-93, 2008.

[45] OLIVEIRA, Marcus; VASCONCELOS, Hilma; SILVA, João. A probabilistic Cnot gate for coherent state qubits. **Physics Letters A**, vol. 377, n. 39, p. 2821-2825, 2013.

[46] LEONHARDT, Ulf. **Measuring the quantum state of light**. Cambridge University press, V. 22, 1997.

[47] PITTMAN, Todd, B; JACOBE, Bart, C; FRANSON, James, D. Experimental Demonstration of a Quantum Circuit using Linear Optics Gates. **Physical Review A**, v. 71, n. 3, p. 032307, 2005.

[48] SPEDALIERI, Federico M.; LEE, Hwang; DOWLING, Jonathan. High-Fidelity Linear Optical Quantum Computing With Polarization Encoding. **Physical Review A**, v. 73, n. 1, p. 012334, 2006.

[49] GLAUBER, Roy, J. The Quantum Theory of Optical Coherence. **Physical Review**, v. 130, n. 6, p. 2529, 1963.

[50] VASCONCELOS, Hilma. **Topics in Coherent State Quantum Computation and State Purification**. University of Notre Dame, 2006.

[51] XIAO, Zheng; SHAO, Qiang Ma; GUO, Feng, Zhang; HENG, Fan; WU; Ming, Liu. Unified and exact framework for variance-based uncertainty relations. **Scientific reports**, v. 10, n. 1, p. 1-14, 2020.

[52] LUIS, Alfredo. Degree of Polarization in Quantum Optics. **Physical review A**, v. 66, n. 1, p. 013806, 2002.

[53] ROBSON, Brian Albert. **The Theory of Polarisation Phenomena**. Clarendon, Oxoford, 1974.

[54] USACHEV, Pavel; SÖDERHOLM, Jonas; GUNNAR, Björk; TRIFONOV, Alexei. Experimental verification of differences between classical and quantum polarization properties. **Optics communications**, v. 193, n. 1-6, p. 161-173, 2001.

[55] CHIRKIN, Anatolii, S.; ORLOV, Andrei, A.; PARASHCHUK, Yu, D. Quantum theory of two-mode interactions in optically anisotropic media with cubic nonlinearities: Generation of quadrature-and polarization-squeezed light. **Quantum electronics**, v. 23, n. 10, p. 870, 1993.

[56] JAMES, Daniel, V.; AGARWAL, Girish, S. The generalized Fresnel transform and its application to optics. **Optics Communications**, v. 126, n. 4-6, p. 207-212, 1996.

[57] BRAGINSKY, Vladimir, B.; KHALILI, Ya. Quantum nondemolition measurements: the route from toys to tools. **Reviews of Modern Physics**, v. 68, n. 1, p. 1, 1996.

[58] BRUNE, Michel; HAROCHE, Serge; RAIMOND, Jean-Michel; DAVIDOVICH, Luiz; ZAGURY, Nicim. Manipulation of photons in a cavity by dispersive atom-field coupling: Quantum-nondemolition measurements and generation of ‘‘Schrödinger cat’’states. **Physical Review A**, v. 45, n. 7, p. 5193, 1992.

[59] IMOTO, Nobuyuki; HAUS, Hermann, A.; YAMAMOTO, Yoshihisa. Quantum nondemolition measurement of the photon number via the optical Kerr effect. **Physical Review A**, v. 32, n. 4, p. 2287, 1985.

[60] LUPASCU, Adrian; SAITO, Shiro; PICOT, Thibaut; GROOT, P.C.; HARMANS, C.J.P.M.; MOOIJ, J.E. Quantum non-demolition measurement of a superconducting two-level system**. Nature physics**, v. 3, n. 2, p. 119-123, 2007..

[61] KOK, Pieter; MUNRO, William, J.; NEMOTO, Kae; RALPH, Timothy, C.; DOWNLING, Jonathan; MILBURN, Gerald, J. Linear optical quantum computing with photonic qubits. **Reviews of modern physics**, v. 79, n. 1, p. 135, 2007.

[62] LI, Shujing, J.; YANG, X.D.; CAO, X.M.; ZHANG, C.-H; XIE, C.-D.; WANG, H. Enhanced cross-phase modulation based on a double electromagnetically induced transparency in a four-level tripod atomic system. **Physical review letters**, v. 101, n. 7, p. 073602, 2008.

[63] KOK, Pieter; HWANG, Lee; DOWNLING, Jonathan. Single-Photon Quantum-Nondemolition Detectors Constructed with Linear Optics and Projective Measurements. **Physical Review A**, v. 66, n. 6, p. 063814, 2002.

[64] GRANGIER, Philippe; LEVENSON, Juan, A.; POIZAT, Jean, P. Quantum Non-Demolition Measurements in Optics. **Nature**, v. 396, n. 6711, p. 537-542, 1998.

[65] VENKATARAMAN, Vivek; SAHA, Kasturi; GAETA, Alexander. Phase Modulation at the Few-Photon Level for Weak-Nonlinearity-Based Quantum Computing. **Nature Photonics**. v. 7, n. 2, p. 138-141, 2013.

[66] TIARKS, Daniel, SCHMIDT Steffen, REMPE, Gerhard; DUERR, Sebastian. Optical π Phase Shift Created With a Single-Photon Pulse. **Science Advances**, Science Advances, v. 2, n. 4, p. e1600036, 2016.

[67] LIU, Zi-Yu; CHEN, Yi-Hsin; CHEN, Yen-Chun; LO, Hsiang-Yu; TSAI, Pin-Ju; YU, Ite A; CHEN, Ying-Cheng; CHEN, Yong-Fan. Large Cross- Phase Modulations at the Few-Photon Level. **Physical Review Letters**, v. 117, n. 20, p. 203601, 2016.

[68] FUSHMAN, Ilya; VUCKOVIC, Jelena. Analysis of a quantum nondemolition measurement scheme based on Kerr nonlinearity in photonic crystal waveguides. **Optics express**, v. 15, n. 9, p. 5559-5571, 2007.

[69] KÖNIG, F.; BUCHLER, Ben; RECHTENWALD, Thomas; LEUCHS, Gerd; SIZMANN, A. Soliton Backaction-Evading Measurement Using Spectral Filtering. **Physical Review A**, v. 66, n. 4, p. 043810, 2002.

[70] LEVENSON, Marc, D; SHELBY, Robert, M; REID, Margaret; WALLS, Daniel, F. Quantum Nondemolition Detection of Optical Quadrature Amplitudes. **Physical Review Letters**, v. 57, n. 20, p. 2473, 1986.

[71] IMOTO, Nobuyuki; WATKINS, Steve; SASAKI, Y. A Nonlinear Optical-Fiber Interferometer for Nondemolitional Measurement of Photon Number. **Optics communications**, v. 61, n. 2, p. 159-163, 1987.

[72] FRIBERG, Stephen R.; MACHIDA, Susumu; YAMAMOTO, Yoshihisa. Quantum Nondemolition Measurement of the Photon Number of an Optical Soliton. **Physical review letters**, v. 69, n. 22, p. 3165, 1992.

[73] ROCH, Jean-François; Vigneron, Karine; GRELU, Philippe; SINATRA, Alice; POIZAT, Jean, P.; GRANGIER, Philippe. Quantum Non-Demolition Measurements Using Cold Trapped Atoms. **Physical review letters**, v. 78, n. 4, p. 634, 1997.

[74] KUZMICH, Andrey G.; MANDEL, Leslie; BIGELOW, Nicholas P. Generation Of Spin Squeezing Via Continous Quantum Nondemolition Measurement. **Physical Review Letters**, v. 85, n. 8, p. 1594, 2000.

[75] PEIL, Steve; GABRIELSE, Gerald. Observing The Quantum Limit Of An Electron Cyclotron: QND Measurements of Quantum Jumps Between Fock States. **Physical Review Letters**, v. 83, n. 7, p. 1287, 1999.

[76] NOGUES, Gilles; RAUSCHENBEUTEL, Arno; Osnaghi, Stefano; BRUNE, Michel; RAIMOND, Jean-Michel; HAROCHE, Sergi. Seeing a Single Photon Without Destroying it. **Nature**, v. 400, n. 6741, p. 239-242, 1999.

[77] GUERLIN, Christine; BERNU, Julien; DELEGLISE, Samuel; SAYRIN, Clément; GLEYZES, Sébastien; KUHR, Stefan; BRUNE, Michel; RAIMOND, Jean-Michel; HAROCHE, Serge. Progressive Field-State Collapse and Quantum Non-Demolition Photon Counting. **Nature**, v. 448, n. 7156, p. 889-893, 2007.

ANEXOS

Anexo A – Cálculo de $\langle \widehat{S_2} \rangle$ e V^2

Para o QBSC funcionar correntemente é necessário que a polarização do estado coerente ao passar pelos meios não lineares $\theta_1, \theta_2, \theta_3$ que modulam a fase do estado coerente seja horizontal (H).

O cálculo do 2ª parâmetro de Stokes S_2, correspondente à diferença das potencias ópticas do fóton polarizado a -45º e +45º medido pelos detectores D_1 e D_2, que corresponde O valor médio $\langle S_2 \rangle$ e a variância V de S_2 são dados por:

$$\langle S_2 \rangle = (P_{+45})^2 - (P_{-45})^2 . \tag{A.1}$$

$$D_1 = (P_{+45}) = \frac{\alpha cos(\Delta\theta) e^{i\sum\theta} + \alpha sin(\Delta\theta) e^{i\sum\theta}}{\sqrt{2}}. \tag{A.2}$$

$$D_2 = (P_{-45}) = \frac{\alpha cos(\Delta\theta) e^{i\sum\theta} - \alpha cos(\Delta\theta) e^{i\sum\theta}}{\sqrt{2}}. \tag{A.3}$$

Substituindo (P_{+45}) e (P_{-45}) em $\langle S_2 \rangle$, temos:

$$\langle S_2 \rangle = (P_{+45})^2 - (P_{-45})^2 = \left(\frac{\alpha cos(\Delta\theta) e^{i\sum\theta} + \alpha sin(\Delta\theta) e^{i\sum\theta}}{\sqrt{2}} \right)^2 - \left(\frac{\alpha cos(\Delta\theta) e^{i\sum\theta} - \alpha sin(\Delta\theta) e^{i\sum\theta}}{\sqrt{2}} \right)^2 ,$$

$$(P_{+45})^2 = \left(\frac{\alpha cos(\Delta\theta) e^{i\sum\theta} + \alpha sin(\Delta\theta) e^{i\sum\theta}}{\sqrt{2}} \right)^2 = \left(\frac{\alpha . e^{i\sum\theta}}{\sqrt{2}} \right)^2 \left(cos(\Delta\theta) + sin(\Delta\theta) \right)^2$$

$$= \left(\frac{\alpha . e^{i\sum\theta}}{\sqrt{2}} \right)^2 . \left[\left(cos(\Delta\theta) \right)^2 + 2(\cos(\Delta\theta))(sin(\Delta\theta)) + \left(sin(\Delta\theta) \right)^2 \right]. \tag{A.4}$$

$$(P_{-45})^2 = \left(\frac{\alpha cos(\Delta\theta) e^{i\sum\theta} - \alpha sin(\Delta\theta) e^{i\sum\theta}}{\sqrt{2}} \right)^2 = \left(\frac{\alpha . e^{i\sum\theta}}{\sqrt{2}} \right)^2 \left(cos(\Delta\theta) - sin(\Delta\theta) \right)^2$$

$$= \left(\frac{\alpha.e^{i\sum\theta}}{\sqrt{2}}\right)^2 .\left[\left(cos(\Delta\theta)\right)^2 - 2cos(\Delta\theta)sin(\Delta\theta) + \left(sin(\Delta\theta)\right)^2\right] . \qquad (A.5)$$

$$\langle S_2 \rangle = (P_{+45})^2 - (P_{-45})^2 =$$

$$= \left(\frac{\alpha.e^{i\sum\theta}}{\sqrt{2}}\right)^2 .\left[\left(cos(\Delta\theta)\right)^2 + 2(\cos(\Delta\theta))(sin(\Delta\theta)) + \left(sin(\Delta\theta)\right)^2\right] -$$

$$- \left(\frac{\alpha.e^{i\sum\theta}}{\sqrt{2}}\right)^2 .\left[\left(cos(\Delta\theta)\right)^2 - 2(\cos(\Delta\theta))(sin(\Delta\theta)) + \left(sin(\Delta\theta)\right)^2\right]$$

$$= \left(\frac{\alpha.e^{i\sum\theta}}{\sqrt{2}}\right)^2 \left[\left(cos(\Delta\theta)\right)^2 + 2cos(\Delta\theta)\left|sin(\Delta\theta)\right\rangle + \left(sin(\Delta\theta)\right)^2 - \right.$$

$$\left. \left(cos(\Delta\theta)\right)^2 - 2cos(\Delta\theta)sin(\Delta\theta) + \left(sin(\Delta\theta)\right)^2\right]$$

$$= \left(\frac{\alpha.e^{i\sum\theta}}{\sqrt{2}}\right)^2 .\left[\cancel{\left(cos(\Delta\theta)\right)^2} + 2cos(\Delta\theta)sin(\Delta\theta) + \cancel{\left(sin(\Delta\theta)\right)^2}\right.$$

$$\left. - \cancel{\left(cos(\Delta\theta)\right)^2} + 2cos(\Delta\theta)sin(\Delta\theta) - \cancel{\left(sin(\Delta\theta)\right)^2}\right]$$

$$= \left(\frac{\alpha.e^{i\sum\theta}}{\sqrt{2}}\right)^2 .[\overbrace{2\cos(\Delta\theta)sin(\Delta\theta) + 2\cos(\Delta\theta)sin(\Delta\theta)}^{4\left|\cos(\Delta\theta)\right\rangle sin(\Delta\theta)=2.\left(2.\cos(\Delta\theta)sin(\Delta\theta)\right)=2sin(2\Delta\theta)}]$$

$$= \frac{\left(\alpha.e^{i\sum\theta}\right)^2}{\cancel{2}}\cancel{2}sin(2\Delta\theta) = (\alpha^*.\alpha)\overbrace{\left(e^{-i\sum\theta}.e^{i\sum\theta}\right)}^{1}.sin(2\Delta\theta)$$

Resultando em:

$$\langle S_2 \rangle = |\alpha|^2 . sin(2\Delta\theta) . \qquad (A.6)$$

A variância de $\langle S_2 \rangle$ para um estado coerente corresponde a uma distribuição de Poisson, equivalente numericamente ao seu número médio de fótons.

$$V = |\alpha|^2 . \qquad (A.7)$$

ANEXO

Anexo B – Distribuição de probabilidade para $\langle \widehat{S}_2 \rangle$.

O cálculo e plot do gráfico da distribuição de probabilidade para S_2 corresponde a uma distribuição de Skellam.

$$p(k,\mu_1,\mu_2) = Pr = e^{-(\mu_1+\mu_2)}\left(\frac{\mu_1}{\mu_2}\right)^{k/2} I_k\left(2\sqrt{\mu_1\mu_2}\right) \tag{B.1}$$

A distribuição Skellam é a distribuição de probabilidade discreta da diferença N_1-N_2 de duas variáveis aleatórias estatisticamente independentes N_1 *e* N_2 são distribuições de Poisson com os respectivos valores esperados μ_1 e μ_2. Para esse caso usaremos o valor médio $\langle S_2 \rangle$ e a variância *V*.

Onde, $I_k(z)$ é a função de Bessel modificada do primeiro tipo. Como *k* é variável, temos que $I_k(z)=I_{|k|}(z)$.

Logo:

$$\begin{cases} \mu_1 + \mu_2 = \langle S_2 \rangle = |\alpha|^2 .sin(2\Delta\theta) \\ \mu_1 - \mu_2 = V = |\alpha|^2 \end{cases},$$

Somando as funções:

$$\begin{cases} \mu_1 + \cancel{\mu_2} = \langle S_2 \rangle \\ \mu_1 - \cancel{\mu_2} = V \end{cases}$$

$$2\mu_1 = \langle S_2 \rangle + V \longrightarrow \boxed{\mu_1 = \frac{\langle S_2 \rangle + V}{2}} \xrightarrow{ou} \boxed{\mu_1 = \frac{|\alpha|^2\left(1+sin(2\Delta\theta)\right)}{2}}.$$

Substituindo μ_1 em:

$$\mu_1 - \mu_2 = V,$$

$$\frac{\langle S_2 \rangle + V}{2} - \mu_2 = V \longrightarrow \langle S_2 \rangle - V = 2\mu_2 ,$$

$$\boxed{\mu_2 = \frac{\langle S_2 \rangle - V}{2}} \xrightarrow{ou} \boxed{\mu_2 = \frac{|\alpha|^2\left(sin(2\Delta\theta)-1\right)}{2}}.$$

Substituindo μ_1 e μ_2 na função de probabilidade de Skellam, temos:

$$Pr = e^{-(\mu_1+\mu_2)}\left(\frac{\mu_1}{\mu_2}\right)^{k/2} I_k\left(2\sqrt{\mu_1\mu_2}\right),$$

$$Pr = e^{-\left(\frac{V+\langle S_2\rangle}{2}+\frac{\langle S_2\rangle - V}{2}\right)}\left(\frac{\frac{V+\langle S_2\rangle}{2}}{\frac{\langle S_2\rangle - V}{2}}\right)^{k/2} I_k\left(2\sqrt{\left(\frac{V+\langle S_2\rangle}{2}\right).\left(\frac{\langle S_2\rangle - V}{2}\right)}\right),$$

$$Pr = e^{-(\langle S_2\rangle)}\left(\frac{V+\langle S_2\rangle}{\langle S_2\rangle - V}\right)^{k/2} I_k\left(\sqrt{\langle S_2\rangle^2 - V^2}\right),$$

ou,

$$Pr = e^{-|\alpha|^2(sin(2\Delta\theta))}\left(\frac{sin(2\Delta\theta)+1}{sin(2\Delta\theta)-1}\right)^{k/2} I_k\left(|\alpha|^2\sqrt{(sin(2\Delta\theta))^2+1}\right). \quad \text{(B.2)}$$

A partir da equação (B.2) foi possível gerar as curvas de probabilidades a partir das combinações dos bits de saída $A = (a_1, a_2, a_3)$ e $B = (b_1, b_2, b_3)$, e os valores dos demais parâmetros correspondentes são; $|\alpha|^2 = 500$. $\theta_1 = \pi/4$, $\theta_2 = \pi/8$ e $\theta_3 = \pi/16$.

ANEXO

Anexo C – Artigo decorrente da tese

Optical and Quantum Electronics (2019) 51:28
https://doi.org/10.1007/s11082-018-1732-5

CrossMark

Optical quantum bit string comparator

C. P. de Sousa[1] · J. B. R. Silva[1] · R. V. Ramos[1]

Received: 21 July 2018 / Accepted: 19 December 2018 / Published online: 4 January 2019

Abstract
Quantum computation has attracted much attention and several quantum algorithms have been proposed in the literature. However, the hardware able to implement such algorithms is still a challenge. In this work, we provide an optical setup for implementation of a quantum bit string comparator, QBSC, for polarization-based qubit, using the non-linear Kerr effect. The QBSC is an important structure for implementation of conditional statements in quantum algorithms.

Keywords Quantum computation · Non-linear Kerr effect · Quantum bit string comparator