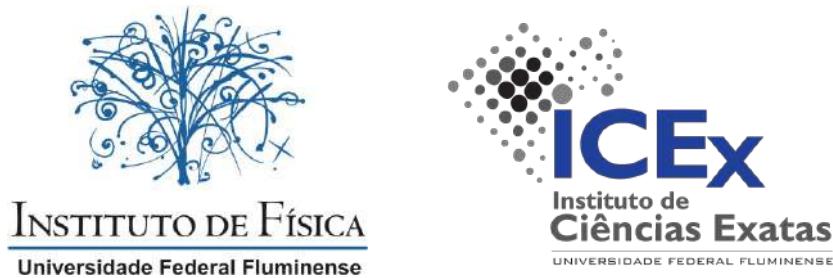


Universidade Federal Fluminense



Proposta de circuito óptico para Transformada de Fourier Quântica de qbits codificados em graus de liberdade da luz

Bianca Maia Gomes

Volta Redonda
2025

Bianca Maia Gomes

Proposta de circuito óptico para Transformada de Fourier Quântica de qbits codificados em graus de liberdade da luz

Dissertação de Mestrado apresentada ao programa de Pós-Graduação em Física da Universidade Federal Fluminense, como parte dos requisitos necessários para obtenção do Título de Mestre em Física.

Universidade Federal Fluminense – UFF

Instituto de Física

Instituto de Ciências Exatas

Programa de Pós-Graduação em Física

Orientador: Prof. Dr. José Augusto Oliveira Huguenin

Volta Redonda – RJ

2025

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

G633p

Gomes, Bianca Maia

Proposta de circuito óptico para Transformada de Fourier
Quântica de qubits codificados em graus de liberdade da luz /
Bianca Maia Gomes. - 2025.
97 p.: il.

Orientador: José Augusto Oliveira Huguenin.
Dissertação (mestrado)-Universidade Federal Fluminense,
Instituto de Física, Niterói, 2025.

1. Informação quântica. 2. Transformada quântica de
Fourier. 3. Circuitos ópticos lineares. 4. Graus de liberdade
da luz. 5. Produção intelectual. I. Huguenin, José Augusto
Oliveira, orientador. II. Universidade Federal Fluminense.
Instituto de Física. III. Título.

CDD - XXX

Bianca Maia Gomes

Proposta de circuito óptico para Transformada de Fourier Quântica de qbits codificados em graus de liberdade da luz

Dissertação de Mestrado apresentada ao programa de Pós-Graduação em Física da Universidade Federal Fluminense, como parte dos requisitos necessários para obtenção do Título de Mestre em Física.

Trabalho aprovado. Volta Redonda – RJ, 21 de fevereiro de 2025:

**Prof. Dr. José Augusto Oliveira
Huguenin
Orientador**

**Prof. Dr. Alcenísio José de Jesus Silva
(UFAL)
Membro Externo**

**Prof. Dr. Marcelo Silva Sarandy
(IF/UFF)
Membro Interno**

Volta Redonda – RJ
2025

Agradecimentos

Primeiramente, gostaria de agradecer aos meus pais e ao meu irmão, por todo o apoio e carinho durante todos esses anos. Sou grata também à minha sobrinha canina, Zoe, pelas doses de fofura.

Também dedico meus agradecimentos ao meu orientador, Prof. José Huguenin, por toda a paciência, insistência e inspiração no processo de orientação desta dissertação. Obrigada por me aceitar no mestrado e pela confiança em dar continuidade nessa ideia.

Aos amigos que me acompanham desde o início, João Vitor, Tainara e Rafael, meus eternos agradecimentos por me suportar até aqui. Aos meus amigos e colegas de laboratório, principalmente ao Daniel, Guilherme, Lucas e Gabe, obrigada por toda a ajuda, mentoria, pelo café com fofoca todas as tardes e por entender meu senso de humor pouco convencional. Aos velhos amigos que escolheram outros caminhos ou que não me conheceram no ambiente acadêmico, obrigada por continuar a me acolher. Aos novos amigos, obrigada pela esperança no que está por vir.

Agradeço também aos professores e colegas do departamento de Física de Volta Redonda pela dedicação em compreender, com excelência, o que entendemos por ciência. Obrigada por tornar esse ambiente enriquecedor.

Por último, agradeço à parte de mim que se recusou a desistir e continuou mesmo com pouquíssimas horas de sono.

Agradeço também à CAPES, órgão financiador deste trabalho, por permitir minha dedicação exclusiva para realizá-lo.

*"Hoje, todos os sonhos da humanidade são amaldiçoados de alguma forma.
Sonhos lindos, mas amaldiçoados."*
Hayao Miyazaki

Resumo

Informação quântica pode ser processada por meio de sistemas ópticos que dependem de graus de liberdade de luz, como a polarização da luz, modos transversos e o caminho de propagação do feixe — aproveitados para o presente trabalho. Essa viabilidade surge por meio da transformação de cada um desses graus de liberdade por dispositivos ópticos específicos — placas de onda, prismas e divisores de feixe — resultando em uma configuração que incorpora três q-bits em um único feixe de luz. Dentro dessa estrutura, uma proposta de circuito óptico para a Transformada Quântica de Fourier é desenvolvida. Para a implementação da Transformada Quântica de Fourier, as portas de fase são essenciais e soluções para esses desafios são estudadas. Nossos resultados de simulação computacional obtidos por este estudo podem oferecer insights valiosos sobre a eficácia da integração de graus de liberdade de luz para processamento de informações quânticas em circuitos ópticos.

Palavras-chaves: Transformada quântica de Fourier; Circuitos ópticos; Graus de liberdade da luz.

Abstract

Quantum information can be processed through optical systems relying on light degrees of freedom, such as the polarization of light, transverse modes and the beam propagation path – harnessed for the present work. This feasibility arises through the transformation of each of these degrees of freedom by specific optical devices – wave-plates, prisms, and beam splitters – resulting in a configuration that embeds three q-bits within a single light beam. Within this framework, an optical circuit proposal for the Quantum Fourier Transform is developed. For the implementation of Quantum Fourier Transform, phase gates are essentials and solutions for these challenges are studied. Our computational simulation results obtained by this study may offer valuable insights on the effectiveness of the integration of light degrees of freedom for quantum information processing in optical circuits.

Key-words: Quantum Fourier Transform; Optical circuits; Degrees of freedom of light.

Listas de ilustrações

Figura 1 – Exemplos de portas lógicas clássicas fundamentais.	7
Figura 2 – Circuito lógico XOR.	7
Figura 3 – Porta lógica reversível NOT.	8
Figura 4 – Representação de um qubit arbitrário $ \psi\rangle$ na esfera de Bloch.	9
Figura 5 – Circuito quântico para uma operação <i>controlled-U</i> .	11
Figura 6 – Porta SWAP.	14
Figura 7 – Circuito quântico para produção de estados maximamente emaranhados de Bell.	15
Figura 8 – Circuito quântico para produção de estados maximamente emaranhados tripartites GHZ.	17
Figura 9 – Estados fundamentais de polarização da luz: linear, circular e elíptica.	21
Figura 10 – Esfera de Poincaré para a polarização.	23
Figura 11 – Placa de onda.	24
Figura 12 – Feixe gaussiano.	26
Figura 13 – Perfil transverso de intensidade e de fase para os modos de Hermite-Gauss.	27
Figura 14 – Perfil transverso de intensidade e de fase para os modos de Laguerre-Gauss.	28
Figura 15 – Esfera de Poincaré para os modos transversos.	29
Figura 16 – Prisma de Dove.	30
Figura 17 – Conversor astigmático.	30
Figura 18 – Esfera de Poincaré para o caminho.	31
Figura 19 – Representação dos divisores de feixe.	32
Figura 20 – Circuito quântico generalizado da QFT.	39
Figura 21 – Circuito da QFT para 3 qbits.	40
Figura 22 – Circuito da iQFT para 3 qbits.	40
Figura 23 – Circuito quântico para a QPE.	42
Figura 24 – Ordem de codificação dos graus de liberdade.	46
Figura 25 – Proposta de circuito óptico para reprodução experimental da QFT.	46
Figura 26 – Preparação do estado tripartite inicial no circuito óptico proposto para a QFT.	47
Figura 27 – Porta de fase geométrica que reproduz a porta quântica T.	48
Figura 28 – Perfil de intensidade dos estados $ 000\rangle$ e QFT $ 000\rangle$.	52
Figura 29 – Vetores na esfera de Bloch para o estado inicial $ 000\rangle$ e os resultados QFT $ 000\rangle$.	53
Figura 30 – Distribuições de amplitudes e fases para os estados $ 000\rangle$ e QFT $ 000\rangle$.	54
Figura 31 – Perfil de intensidade dos estados $ 010\rangle$ e QFT $ 010\rangle$.	55

Figura 32 – Vetores na esfera de Bloch para os resultados dos estados $ 010\rangle$ e QFT $ 010\rangle$.	56
Figura 33 – Distribuições de amplitudes e fases para os estados $ 010\rangle$ e QFT $ 010\rangle$.	57
Figura 34 – Perfil de intensidade dos estados $ 101\rangle$ e QFT $ 101\rangle$.	58
Figura 35 – Vetores na esfera de Bloch para os resultados dos estados $ 101\rangle$ e QFT $ 101\rangle$.	59
Figura 36 – Distribuições de amplitudes e fases para os estados $ 101\rangle$ e QFT $ 101\rangle$.	60
Figura 37 – Perfil de intensidade dos estados $ 111\rangle$ e QFT $ 111\rangle$.	61
Figura 38 – Vetores na esfera de Bloch para os resultados dos estados $ 111\rangle$ e QFT $ 111\rangle$.	62
Figura 39 – Tomografia dos estados $ 111\rangle$ e QFT $ 111\rangle$.	63
Figura 40 – Perfil de intensidade dos estados $ GHZ\rangle$ e QFT $ GHZ\rangle$.	64
Figura 41 – Tomografia dos estados $ GHZ\rangle$ e QFT $ GHZ\rangle$.	65

Lista de tabelas

Tabela 1 – Funções booleanas de portas lógicas fundamentais.	6
Tabela 2 – Tabela-verdade de portas lógicas fundamentais.	6
Tabela 3 – Codificação da informação quântica nos graus de liberdade da luz.	33
Tabela 4 – Fatores de fase da QFT para a base computacional com 3 qbits.	41
Tabela 5 – Tabela de correspondência entre resultados numéricos e a direção de propagação do circuito.	49

Lista de abreviaturas e siglas

DFT	Transformada discreta de Fourier, do inglês <i>Discrete Fourier Transform</i> .
FFT	Transformada rápida de Fourier, do inglês <i>Fast Fourier Transform</i> .
QFT	Transformada quântica de Fourier, do inglês <i>Quantum Fourier Transform</i> .
QPE	Algoritmo quântico de estimativa de fase, do inglês <i>Quantum Phase Estimation</i> .
PBS	Divisor de feixe polarizado, do inglês <i>Polarized Beam Splitter</i> .
TBS	Divisor de modos transversos, do inglês <i>Transverse Beam Splitter</i> .
BS	Divisor de feixe, do inglês <i>Beam Splitter</i> .
SWP	Placa de onda S, do inglês <i>S Wave Plate</i> .
HWP	Placa de meia onda, do inglês <i>Half Wave Plate</i> .
QWP	Placa de quarto de onda, do inglês <i>Quarter Wave Plate</i> .
DP	Prisma de Dove, do inglês <i>Dove Prism</i> .
CL	Lentes cilíndricas, do inglês <i>Cylindrical lenses</i> .
CCD	Dispositivo de carga acoplada, do inglês <i>Charged coupled device</i> .
OAM	Momento angular orbital, do inglês <i>Orbital angular momentum</i> .

Sumário

Introdução	1	
1	FUNDAMENTOS DE INFORMAÇÃO QUÂNTICA	5
1.1	Computação clássica	5
1.2	Unidade básica de informação quântica binária: qbit	8
1.3	Circuitos quânticos	10
1.3.1	Portas lógicas quânticas	11
1.3.2	Estados emaranhados	15
2	GRAUS DE LIBERADE A LUZ COMO RECURSO PARA INFORMAÇÃO QUÂNTICA	19
2.1	Os graus de liberdade da luz	19
2.1.1	Polarização	19
2.1.2	Modos transversos: Hermite-Gauss e Laguerre-Gauss	25
2.1.3	Caminho	31
2.2	Codificação da informação quântica	32
3	A TRANSFORMADA QUÂNTICA DE FOURIER	35
3.1	A transformada rápida de Fourier	35
3.2	Transformada quântica de Fourier	37
3.3	O algoritmo quântico de estimativa de fase	41
4	PROPOSTA DE CIRCUITO ÓPTICO DE ESTADOS TRIPARTITES PARA A QFT	45
4.1	Circuito óptico com os graus de liberdade da luz: polarização, modos de Hermite-Gauss e o caminho	45
4.2	Simulação computacional	48
5	RESULTADOS	51
5.1	Resultados da base computacional $000\rangle$	51
5.2	Resultados da base computacional $010\rangle$	55
5.3	Resultados da base computacional $101\rangle$	58
5.4	Resultados da base computacional $111\rangle$	61
5.5	Resultados do estado maximamente emaranhado $GHZ\rangle$	64
6	CONCLUSÕES E PERSPECTIVAS FUTURAS	67

Introdução

No ínicio século XX, o matemático Alan Turing, pai da computação, introduziu o conceito das Máquinas de Turing [1], um modelo abstrato de computação capaz de simular qualquer algoritmo, o que se tornou a base teórica para os primeiros computadores modernos, como o ENIAC [2] e o Colossus [3], desenvolvidos na década de 1940. Essas máquinas, embora gigantescas e limitadas, motivadas marjoritariamente por questões geoestratégicas da segunda guerra mundial, marcaram o início da era da computação digital. A invenção do transistor na década de 1950 revolucionou a tecnologia, permitindo a miniaturização dos componentes e o surgimento dos computadores pessoais [4]. Em 1965, Gordon Moore formulou a Lei de Moore [5], prevendo que o número de transistores em um circuito integrado dobraria a cada dois anos, uma tendência que se manteve válida por décadas e impulsionou avanços exponenciais no poder de processamento. No entanto, essa tendência está próxima de atingir seu limite físico de redução, com transistores atuais medindo apenas 2 nanômetros, o que levou a comunidade científica a buscar alternativas tecnológicas.

Na perspectiva da comunidade científica, a proposta de Paul Benioff, que consiste na concepção de um modelo análogo ao das máquinas de Turing, porém embasado em princípios da mecânica quântica [6], em união com as observações de Richard Feynman sobre simulações computacionais quânticas durante uma conferência [7], contribuiram para direcionar uma alternativa para o problema da expansão de poder computacional, conhecida como *computação quântica*. Em meados da década de 80, o físico inglês David Deutsch foi responsável pela tese encarregada da declaração de que um dispositivo de computação universal poderia simular qualquer processo físico [8], o princípio de Church-Turing-Deutsch.

A informação quântica é fundamentada em princípios da mecânica quântica, como a superposição e o emaranhamento, que permitem que sistemas quânticos processem e armazenem dados de maneiras radicalmente diferentes dos sistemas clássicos. Enquanto os computadores tradicionais operam com bits que assumem valores binários (0 ou 1), os computadores quânticos utilizam *qbits* (os bits quânticos) [9], que podem existir em uma superposição de estados, permitindo a execução de operações paralelas em grande escala. Além disso, o emaranhamento quântico que abre portas para protocolos de comunicação e processamento de informações impossíveis de serem realizados classicamente [10].

Naturalmente, para realizar computação quântica é obrigatório a existência de um dispositivo de arquitetura embasada nos postulados da mecânica quântica. Ainda nos paralelos com a arquitetura de computadores clássicos, outra alternativa para escalonar

o poder de processamento da informação é a computação óptica. Utilizando fôtons em vez de elétrons para processar informações, ela promete maior velocidade e eficiência energética, especialmente em aplicações como processamento de sinais e comunicação de dados [11]. No entanto, essa abordagem ainda enfrenta desafios significativos, como a dificuldade de integração com a eletrônica convencional e a falta de componentes ópticos escaláveis e economicamente viáveis [12]. Em contraste, os computadores quânticos fotônicos buscam combinar as vantagens da óptica com os princípios da informação quântica. Nessa arquitetura, os fôtons são utilizados como qubits, explorando sua capacidade de superposição e emaranhamento para realizar operações quânticas. Essa abordagem é particularmente atraente devido à baixa taxa de decoerência dos fôtons, o que os torna candidatos ideais para a transmissão e processamento de informações quânticas em longas distâncias [13]. No entanto, a construção de computadores quânticos fotônicos também enfrenta desafios técnicos, como a geração eficiente de estados emaranhados e a implementação de portas lógicas quânticas robustas.

A implementação de protocolos e algoritmos quânticos em circuitos ópticos lineares clássicos tem se mostrado uma abordagem promissora para explorar as vantagens da computação quântica experimentalmente sem a necessidade de sistemas quânticos completos [14]. Também é particularmente útil para testar e validar algoritmos quânticos em ambiente controlado, além de servir como ponte para a computação clássica e quântica. Uma das possibilidades decorrentes disso, é a codificação da informação nos graus de liberdade da luz, como a polarização, os modos transversos e a direção de propagação (caminho). Essa versatilidade permite a implementação de protocolos quânticos complexos em sistemas ópticos, utilizando componentes ópticos relativamente simples em um único feixe luminoso [15, 16].

Com isso, na presente dissertação, o objetivo principal é o desenvolvimento uma proposta de circuito óptico linear (clássico) tripartite que reproduza a Transformada de Fourier quântica [17, 18] com os graus de liberdade da luz. A transformada quântica de Fourier é uma componente essencial para algoritmos focados em problemas de periodicidade, como, por exemplo, o algoritmo de Shor para fatoração de números primos [19], que é uma ameaça para alguns modelos de distribuição de chaves criptográficas.

Portanto, essa dissertação está organizada em cinco capítulos, cada um dedicado a explorar aspectos fundamentais e aplicações práticas da computação quântica em sistemas ópticos, com foco na implementação da Transformada Quântica de Fourier (QFT) utilizando graus de liberdade da luz. A seguir, apresentamos uma visão geral da estrutura e dos temas abordados em cada capítulo.

No Capítulo 1, são apresentados os fundamentos da informação quântica, estabelecendo uma base teórica para a compreensão dos conceitos que serão explorados ao longo do trabalho. Iniciamos com uma revisão dos princípios da computação clássica e

então avançamos para os fundamentos de informação quântica, dando ênfase ao princípio de superposição e ao emaranhamento quântico.

O Capítulo 2 é dedicado à exploração dos graus de liberdade da luz como recursos para a codificação de informação quântica. Inicialmente, são apresentados os principais graus de liberdade da luz: polarização, modos transversos (Hermite-Gauss e Laguerre-Gauss) e caminho de propagação. Cada um desses graus de liberdade é detalhado, com ênfase em suas propriedades físicas e como podem ser manipulados por dispositivos ópticos, como placas de onda, prismas e divisores de feixe. Em seguida, discutimos a codificação da informação quântica nesses graus de liberdade, estabelecendo uma analogia entre os estados quânticos e as propriedades da luz.

No Capítulo 3, o foco é base teórica da Transformada Quântica de Fourier (QFT), um componente central em muitos algoritmos quânticos. Iniciamos revisando as propriedades da transformada de Fourier clássica e então, definimos a quântica. O capítulo também aborda a aplicação da QFT em algoritmos quânticos, como o algoritmo de estimativa de fase (QPE) e o algoritmo de Shor.

O Capítulo 4 apresenta a proposta de um circuito óptico tripartite para a implementação da QFT, utilizando os graus de liberdade da luz: polarização, modos transversos e caminho de propagação. Detalhamos a estrutura do circuito, incluindo a preparação do estado inicial, a realização das transformações quânticas e a tomografia dos estados resultantes. Discutimos os desafios técnicos envolvidos na implementação experimental e apresentamos soluções para superar esses obstáculos. O capítulo também inclui uma descrição da simulação computacional desenvolvida para validar a proposta, utilizando o formalismo de Jones para modelar os dispositivos ópticos e as transformações quânticas.

Por fim, o Capítulo 5 é dedicado à apresentação e análise dos resultados obtidos com a simulação computacional do circuito óptico proposto. São discutidos os perfis de intensidade e fase dos estados transformados pela QFT, tanto para estados da base computacional quanto para estados maximamente emaranhados. Através de tomografias quânticas, analisamos a distribuição de intensidade e as fases relativas dos estados, comparando os resultados com as previsões teóricas.

1 Fundamentos de informação quântica

O objetivo de iniciar a presente dissertação com uma apresentação concisa dos conceitos que regem a teoria da informação quântica, bem como sua intrínseca conexão com os postulados da mecânica quântica, concentra-se em construir uma ponte direta com a codificação em sistemas ópticos. Entretanto, antes de prosseguir com a analogia direta entre a óptica e a computação quântica, devemos contemplar os conceitos fundamentais da computação clássica.

1.1 Computação clássica

Dos primeiros protótipos inspirados pelas máquinas de Turing [1] até os supercomputadores com placas de vídeo integradas, o que sustenta o processamento da informação é a existência de uma unidade básica de informação, *bit*, essencialmente correspondente à lógica binária.

Na mecânica estatística, a fórmula da entropia de Boltzmann é usada para calcular a entropia e o número de microestados de um determinado sistema microcanônico [20]. De forma análoga, na teoria da informação, para um conjunto finito de probabilidades $\{p_1, \dots, p_n\}$ e uma base logaritma b arbitrária, porém fixa, a função

$$H(p_1, \dots, p_n) := - \sum_{i=1}^n p_i \log_b p_i, \quad (1.1)$$

é denominada *entropia de Shannon* [21]. Note que quando a entropia for máxima, isto é, no caso de probabilidades equiprováveis, $H = \log n$ assume o formato da proposta original de Boltzmann.

Na presente discussão, o caso de maior relevância é quando temos a base 2 do logaritmo,

$$H(p) = -p \log p - (1-p) \log (1-p). \quad (1.2)$$

Além de ser um caso particular valioso para generalização do comportamento côncavo da função entropia, a *entropia de Shannon binária* também estabelece um limite teórico inferior para a compressão de dados sem perda de informação, facilitando o processamento e armazenamento eficientes de informações. Em resumo, significa que por símbolo, há somente dois valores possíveis [22], definindo assim, o que é conhecido por *unidade básica de informação binária*.

Consequentemente, as operações em um computador clássico são executadas por circuitos lógicos booleanos [23, 24]. Em outras palavras, os processadores são capazes de traduzir ao usuário dois únicos valores: 0 ou 1, respectivamente, falso ou verdadeiro. Os componentes desses circuitos são conhecidos como *portas lógicas*.

Algumas das portas lógicas fundamentais são representadas pelas funções booleanas expressas na Tabela 1. Note que as operações dessas funções são realizadas através da aritmética modular.

Porta Lógica	Função Booleana
AND	$A \cdot B$
OR	$A + B$
XOR	$A \oplus B$
NOT	\bar{A}

Tabela 1 – Funções booleanas de algumas portas lógicas fundamentais.

A porta **AND** realiza uma operação de multiplicação booleana, retornando verdade (1) somente quando ambas as entradas são verdadeiras. A porta **OR** executa uma operação de soma booleana, retornando 1 quando pelo menos uma das entradas for 1. A porta **XOR**, no que lhe concerne, gera um resultado verdadeiro sempre quando o número de entradas 1 for ímpar. A porta **NOT** inverte o valor da entrada, retornando o oposto do valor fornecido. E essas são as operações base para a construção de circuitos digitais complexos e são amplamente aplicadas em processadores para realizar cálculos.

Elas também podem ser representadas através de tabelas-verdades, como na Tabela 2.

A	B	A AND B	A OR B	A XOR B	NOT A
0	0	0	0	0	1
0	1	0	1	1	1
1	0	0	1	1	0
1	1	1	1	0	0

Tabela 2 – Tabela-verdade para portas lógicas conhecidas na computação.

É imediatamente observável que as portas lógicas AND, OR e XOR, dependem de dois valores de entradas em sua atuação, que consiste em, respectivamente, retornar "verdadeiro" quando são iguais, diferentes de zero e exclusivamente diferentes entre si. As representações lógicas dessas estão dispostas na Figura 1.

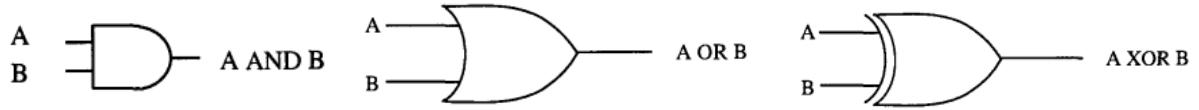


Figura 1 – Exemplos de portas lógicas clássicas. Da esquerda para a direita, estão posicionadas as portas AND, OR e XOR. Fonte: [25].

Uma computação é definida como uma sequência finita de operações elementares, denominadas circuitos, aplicada à alguma *string* de bits (sequência de bits) de entrada cujo resultado é a transformação final dessa ação. Por consequência, existe um conjunto de portas lógicas capazes de formar qualquer função de entrada e saída finita, denominadas *portas lógicas universais*.

Nesse contexto, a simbologia é particularmente útil para *circuitos lógicos*, que são constituídos por esse conjunto de operações universais e, portanto, na maioria dos casos, realizam tarefas mais complexas. Na Figura 2 está ilustrada uma alternativa à porta XOR.

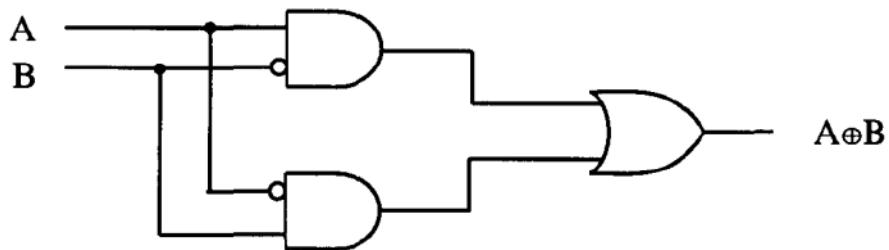


Figura 2 – Circuito lógico para a porta lógica XOR, reproduzido por duas AND e uma única OR. Fonte: [25].

Concebida dessa forma, a XOR recebe dois valores iniciais que passam simultaneamente por duas portas AND e então se encontram em uma porta OR, garantindo a mesma aritmética exibida na tabela 2.

Para finalizar, é evidente que os circuitos lógicos inevitavelmente tendem a dissipar energia, gradualmente causando a perda de informação do sistema [26]. Isto é, conforme a densidade do circuito aumenta, sua entropia também. Entretanto, no caso dos *circuitos lógicos reversíveis*, isto é, operações do qual pode-se recuperar perfeitamente os dados de entrada através da saída, a entropia é conservada.

No modelo de computação clássica, a única porta lógica reversível é a porta NOT. Como explicitado na tabela-verdade, seu papel é inverter o valor booleano. A Figura 3 ilustra sua representação lógica.

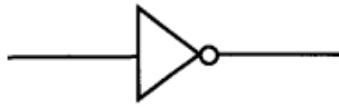


Figura 3 – A porta lógica NOT é a única porta lógica clássica reversível. Fonte: [25].

Logo, ao considerar um automôto logicamente reversível, também conceitua-se um modelo de computação reversível [27]. Esse conceito é essencial no processamento de informação quântica, dado que as operações são inherentemente reversíveis. A reversibilidade dos operadores quânticos garante a conservação da entropia do sistema [28], algo crucial para preservação da informação e para eficiência energética, além de colaborar para redução significativa da complexidade de problemas computacionais.

1.2 Unidade básica de informação quântica binária: qbit

No geral, um estado quântico de dimensão n é uma combinação linear de n bases ortonormais pertencentes ao espaço de Hilbert H_n . Logo, um sistema de dois níveis é constituído por duas bases ortonormais pertencentes ao espaço de Hilbert bidimensional H_2 , em notação de Dirac [29],

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{e} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad (1.3)$$

que formam a base computacional quântica.

Portanto, a unidade básica de informação quântica binária, qbit, é definida como um estado quântico puro, isto é, uma superposição da base computacional, representada por

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1.4)$$

com coeficientes complexos $\alpha, \beta \in \mathbb{C}$, que diretamente relacionados com o conceito de potencial probabilístico [30], são as amplitudes de probabilidades dos estados básicos para previsão dos resultados finais. Por consequência, considera-se o princípio de normalização,

$$|\alpha|^2 + |\beta|^2 = 1, \quad (1.5)$$

com

$$\alpha = \cos \frac{\theta}{2}, \quad \beta = e^{i\phi} \sin \frac{\theta}{2} \quad (1.6)$$

sendo $e^{i\phi}$ o fator de fase relativa.

Logo, substituindo as coordenadas polares (1.6) na equação (1.4),

$$|\psi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right) \quad (1.7)$$

onde $e^{i\gamma}$ é o fator de fase global. Entretanto, como esse fator não tem efeito observável, segue que

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle. \quad (1.8)$$

Portanto, sendo os ângulos θ e ϕ , respectivamente, polar e azimutal, a determinação arbitrária desses definem um ponto qualquer na esfera tridimensional denominada *esfera de Bloch*. Os extremos longitudinais são referentes à base computacional e os latitudinais, os estados de superposição. Na Figura 4, está disposta uma ilustração desse artifício geométrico.

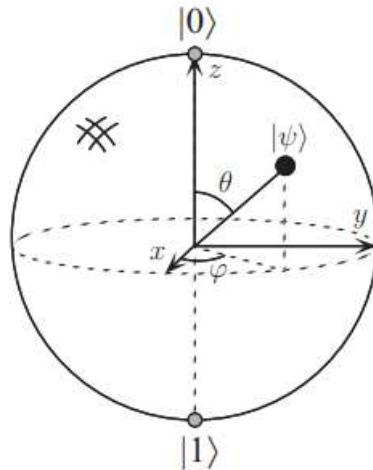


Figura 4 – Representação de um qubit arbitrário $|\psi\rangle$ na esfera de Bloch. Fonte: [9].

Além disso, em um sistema composto por n qubits, os 2^n estados individuais associados a cada qbit não representam todos os estados possíveis do sistema. Em vez disso, eles formam uma nova base computacional, conhecida como base de produto tensorial, que permite descrever estados mais complexos, como superposições e emaranhamentos, fundamentais para o processamento de informação quântica [31].

$$|\psi_0 \dots \psi_n\rangle = |\psi_0\rangle \dots |\psi_n\rangle = |\psi_0\rangle \otimes \dots \otimes |\psi_n\rangle, \quad (1.9)$$

que sempre é um produto tensorial de ordem n da base bidimensional. Então, considerando o conjunto finito $\mathbb{B}^n = \{0, 1\}^n$,

$$|\psi\rangle = \sum_{(x_1, \dots, x_n) \in \mathbb{B}^n} c_{x_1, \dots, x_n} |x_1, \dots, x_n\rangle \quad (1.10)$$

descreve o estado quântico para n qubits. Naturalmente,

$$\sum_{x \in \mathbb{B}^n} |c_x|^2 = 1 \quad (1.11)$$

com $c_x \in \mathbb{C}$ as amplitudes de cada elemento da nova base. Nota-se que, uma vez que a dimensão da base computacional da composição de qubits é 2^n , haverá também 2^n coeficientes complexos.

Em conjunto, essas definições constituem os fundamentos do processamento da informação quântica: o qbit, a superposição e a composição de estados múltiplos. Enquanto o estado não é colapsado (medido), as possíveis operações não são restritas à binariedade por causa da superposição, possibilitando assim, o paralelismo quântico. Esse é um conceito base para uma diversidade de algoritmos quânticos para resolução de problemas complexos conhecidos. No geral, são processados por intermédio de um *circuito quântico*.

1.3 Circuitos quânticos

A evolução temporal de um sistema quântico, como afirma o sexto postulado da mecânica quântica [32], é governada pela equação de Schrödinger dependente do tempo,

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \mathcal{H}(t) |\psi(t)\rangle, \quad (1.12)$$

onde $|\psi(t)\rangle$ é um estado quântico arbitrário, $\mathcal{H}(t)$ é o autovalor do observável hamiltoniano $\hat{\mathcal{H}}$, que define os níveis de energia do estado quântico, e t é a variável temporal. Além disso, para um instante de tempo inicial t_0 , considera-se o seguinte problema de autovalores,

$$|\psi(t)\rangle = \mathcal{U} |\psi(t_0)\rangle, \quad (1.13)$$

logo, para o problema da equação (1.12) e um avanço infinitesimal no tempo dt ,

$$\mathcal{U}(t_0 + dt, t_0) = 1 - \frac{i\mathcal{H}dt}{\hbar} \quad (1.14)$$

é denominado *operador de evolução temporal*. Como o hamiltoniano \mathcal{H} é um observável e, portanto, um operador hermitiano, consequentemente a evolução no tempo também será, isto é,

$$\mathcal{U}(t, t_0) \mathcal{U}^\dagger(t, t_0) = 1. \quad (1.15)$$

A unitariedade é uma propriedade fundamental, pois preserva a norma dos estados quânticos, assegurando a conservação da probabilidade total do sistema conforme sua evolução temporal, ou seja,

$$\sum_{x'} |c_{x'}(t_0)|^2 = \sum_{x'} |c_{x'}(t)|^2, \quad (1.16)$$

comportamento que é diretamente explicitado através da expansão da equação (1.10) para os instantes t e t_0 .

Com essa exposição, define-se que para um operador hermitiano arbitrário $\hat{\Omega}$, a evolução temporal desse é igualmente hermitiana, além de unitária, descrita por [33]:

$$\mathcal{U}(t_0 + dt, t_0) = 1 - \frac{i\hat{\Omega}dt}{\hbar}. \quad (1.17)$$

Na computação quântica, as portas lógicas são definidas como operadores unitários que agem sobre os estados quânticos. Em virtude disso, da unitariedade do operador de evolução temporal, o estado inicial pode ser recuperado a partir do estado transformado, invertendo a operação. Portanto, toda porta lógica quântica é intrinsecamente reversível, em contraste com o modelo de computação clássico [34].

Assim como na computação clássica, um circuito quântico é composto de múltiplas portas quânticas universais [31], [8], interconectadas e, portanto, executa determinado algoritmo ou protocolo de informação quântica. Na Figura 5, está uma representação gráfica de um circuito quântico. Cada linha horizontal representa um qbit do circuito. Nesse, há uma operação controlada no circuito, onde uma linha vertical conecta os qbits alvo (a operação U) e controle (o círculo preto). Após essa transformação, o segundo qbit é medido.

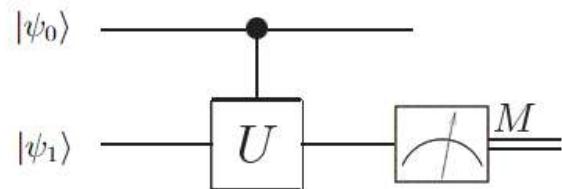


Figura 5 – Circuito quântico para uma operação *controlled-U*. Fonte: [9].

1.3.1 Portas lógicas quânticas

A superposição é uma propriedade essencial para a computação quântica, dado que possibilita o uso do *parallelismo quântico* em determinados algoritmos [35]. Por esse motivo, a primeira porta lógica quântica a ser apresentada, é a porta Hadamard,

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (1.18)$$

do qual a aplicação na base computacional transforma os estados $|0\rangle$ e $|1\rangle$, respectivamente, em superposições equilibradas

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{e} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (1.19)$$

Ou ainda, generalizando a transformada de Hadamard para n qubits,

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle \langle y|, \quad (1.20)$$

processa a informação de todo o circuito simultaneamente. É notável que, diferente do paralelismo na computação clássica, somente um circuito é o suficiente para o processamento paralelo.

Com base nas matrizes de Pauli σ_x , σ_y e σ_z da mecânica quântica, além da identidade omitida por sua trivialidade, as matrizes

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \text{e} \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (1.21)$$

representam as portas de Pauli.

Além disso, há também as portas de fase,

$$P \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}, \quad (1.22)$$

que, resumidamente, adicionam determinada fase relativa na base computacional $|1\rangle$. Dessa forma, as mais amplamente utilizadas são para os ângulos $\phi = \pi/2$ e $\phi = \pi/4$, respectivamente,

$$S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad \text{e} \quad T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}. \quad (1.23)$$

As portas de rotação, por sua vez, provocam uma rotação completa do vetor na esfera de Bloch, em torno dos eixos x , y ou z , alterando as bases computacionais como um todo. As representações matriciais para essas rotações são:

$$R_x(\theta) \equiv \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i \sin\left(\frac{\theta}{2}\right) \\ -i \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}, \quad (1.24)$$

para a porta $R_x(\theta)$, que realiza uma rotação de θ radianos em torno do eixo x , transformando a amplitude da base computacional e a posição do estado na direção desse eixo. De modo análogo,

$$R_y(\theta) \equiv \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}, \quad (1.25)$$

representa a rotação no estado quântico em torno do eixo y . Agora, a transformação

$$R_z(\theta) \equiv \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}, \quad (1.26)$$

denominada porta $R_z(\theta)$, rotaciona em torno do eixo z , sem alterar a amplitude dos estados da base, assim aplicando uma fase relativa. Logo, consiste em uma porta lógica crucial em muitos algoritmos quânticos, pois permite a manipulação da fase sem alterar as probabilidades de medida.

As *portas controladas*, por sua vez, são operações essenciais para implementar interações entre os qbits, possibilitando o emaranhamento. Normalmente possuem uma condicional centrada na transformação de um *alvo* do circuito, caso o estado do *controle* atenda aos critérios específicos. São, justamente, o tipo de circuito quântico exposto na Figura 5.

A porta *controlled-not*, do inglês, "não-controlada", aplica uma inversão, equivalente a uma soma na aritmética modular de base 2, no qbit alvo quando o estado do controle é $|1\rangle$. Supondo um circuito de dois qbits, sendo o primeiro o controle e o segundo o alvo, a matriz que representa essa operação é

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (1.27)$$

Por intermédio de uma composição sequencial dessa porta, como na Figura 6, produz-se a porta lógica conhecida como SWAP. Sua função é realizar a troca dos estados de dois qbits de forma bidirecional, sem afetar o restante do circuito.

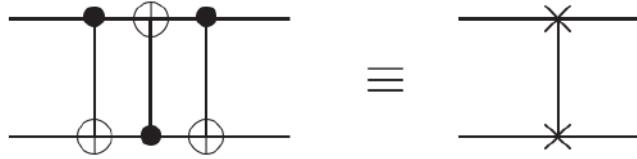


Figura 6 – Porta SWAP (direita) constituída da sequência de portas CNOT (esquerda). Fonte: [9].

Elas também são essenciais em algoritmos quânticos para reordenar ou reorganizar qubits em estados intermediários ou finais, especialmente em aplicações de otimização e simulação. É representada matricialmente como

$$SWAP \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (1.28)$$

Para n qubits, a generalização pode ser expressa como

$$\text{CNOT}_{(n)} = I^{\otimes(n-1)} \otimes X, \quad (1.29)$$

onde X representa a operação de inversão aplicada ao alvo e $I^{\otimes(n-1)}$ é a identidade para os qubits não afetados por ela. O caso particular para três qubits é conhecido como *porta de Toffoli* [36], de modo que a generalização de ordem superior também pode ser nomeada assim. Composições derivadas também podem ser generalizadas.

A porta de *controlled-Z*, por conseguinte, transforma o estado base $|1\rangle$ de acordo com a porta Z. Possui representação matricial como

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \quad (1.30)$$

Sob outra perspectiva, a porta Z pode ser interpretada como uma ocorrência particular da porta P, da equação (1.22), quando o ângulo $\phi = \pi$. Consequentemente, isso também vale para a porta controlada, generalizada como

$$CP(\phi) = I^{\otimes(n-1)} \otimes \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}. \quad (1.31)$$

1.3.2 Estados emaranhados

O emaranhamento quântico é um fenômeno quântico que descreve a correlação não local entre partículas, isto é, a medida de uma partícula quântica emaranhada com outra fornece, simultaneamente, informação sobre ambas [37]. Inicialmente explorado no famoso paradoxo EPR, somente com a formalização das desigualdades de Bell que as investigações para a não-localidade começaram a ser desenvolvidas experimentalmente. No geral, a violação da desigualdade de Bell, demonstrada em experimentos subsequentes [38], [39], não apenas fundamentou a existência de correlações quânticas, como também pavimentou o caminho para um recurso essencial para computação e criptografia quântica.

Logo, definidas as portas Hadamard e a CNOT, unificadas como na Figura 1.33, elas produzem um estado emaranhado de Bell.

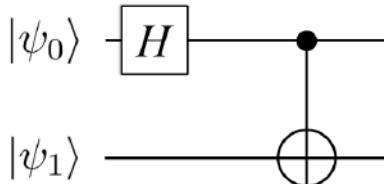


Figura 7 – Circuito quântico para produção de estados maximamente emaranhados de Bell.
Fonte: Autoria própria.

O primeiro qbit é representado por $|\psi_0\rangle$, enquanto que o segundo por $|\psi_1\rangle$. Nisso, supondo um estado inicial $|\psi\rangle \equiv |11\rangle$, o circuito ao ser iniciado pela porta de superposição, será transformado como $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle$. Como o controle da porta controlada está no primeiro qbit, então, resulta em $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. De modo análogo, o procedimento pode ser repetido para todos os estados base $|00\rangle$, $|01\rangle$ e $|10\rangle$, com os respectivos, além do próprio $|11\rangle$, resultados expostos na equação (1.32).

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{1.32}$$

Ou ainda, compactando,

$$|\beta_{nm}\rangle = \frac{|0n\rangle + (-1)^m |1\bar{n}\rangle}{\sqrt{2}}, \tag{1.33}$$

onde $(-1)^m$ introduz uma fase dependendo do valor de m , útil para controlar a simetria e a coerência entre os estados durante manipulações experimentais, e $\bar{n} = 1 - n$ representa a soma de módulo 2.

Observe a impossibilidade de escrever $|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle$ para os estados emaranhados, uma vez que as portas quânticas envolvidas os *correlacionam* de modo que a independência entre eles é inviável.

Para além disso, os estados GHZ (estados de Greenberger–Horne–Zeilinger), extendem o conceito para sistemas compostos por três ou mais componentes [40], [41], [42]. Não se restringe como uma generalização do entrelaçamento bipartido para n qbits, ou seja, diretamente das equações (1.32) e (1.33), como também permite emaranhamento multipartido. Sistemas compostos por múltiplas partículas demonstram a estrutura não-separável em diferentes camadas [43]. Retornando ao caso bipartido $|\beta_{00}\rangle$ e incluindo um novo qbit, inicializado inicialmente como $|\psi_2\rangle \equiv |0\rangle$, que é o alvo de uma outra porta não-controlada, resulta em

$$\begin{aligned} |\beta_{00}\rangle \otimes |0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |0\rangle \quad \rightarrow \\ \rightarrow \quad |\beta_{00}\rangle \otimes |0\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \end{aligned} \tag{1.34}$$

Portanto, o estado emaranhado tripartite proveniente desse cenário é dado por:

$$|GHZ\rangle_{000} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{1.35}$$

O procedimento também pode ser repetido de modo análogo para obtenção do estado:

$$|GHZ\rangle_{010} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle). \tag{1.36}$$

Esse processo pode ser generalizado para n qbits. Para $n = 3$ qbits, o estado está representado enquanto circuito quântico na Figura 8. A realização do circuito quântico depende somente da inserção de uma porta Hadamard no primeiro qbit e duas CNOT consecutivas interligando controle e alvo em sequência nos outros dois qbits. Para um circuito generalizado, basta dar continuidade ao processo das portas controladas até chegar no último qbit.

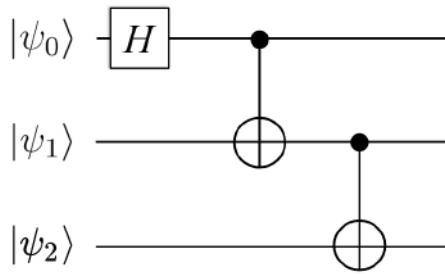


Figura 8 – Circuito quântico para produção de estados maximamente emaranhados tripartites GHZ. Fonte: Autoria própria.

Anteriormente, foi apresentado o conceito de *universalidade quântico*. Em resumo, é uma constatação de que existem conjuntos de portas quânticas básicas, que em determinada sequência constituem outras portas quânticas. Frequentemente, são considerados conjuntos formados pela porta não-controlada e as outras portas básicas de um qbit [44], [45], selecionadas de acordo com as exigências do problema. Entretanto, na computação quântica, a transição de um conjunto para o outro não possui um custo computacional elevado (complexidade de ordem logarítmica). Com isso, o conjunto mais simples possível é uma composição como {Toffoli, H , T } [46]. A partir dela, qualquer computação quântica pode ser aproximada por via do Teorema de Solovay-Kitaev [47]. Caracterizando, portanto, que os elementos essenciais para a universalidade são a superposição, o emaranhamento e amplitudes complexas.

A exploração dos fundamentos da informação quântica, desde os conceitos básicos da computação clássica até a introdução dos qbits e dos circuitos quânticos, estabelece uma base sólida para compreender as potencialidades e os desafios da computação quântica. A transição da lógica binária clássica para a superposição quântica e o emaranhamento evidencia uma mudança paradigmática no processamento de informação, onde a reversibilidade e a manipulação de estados quânticos abrem caminho para algoritmos e protocolos que superam as limitações dos sistemas clássicos. Neste capítulo, foram apresentados os pilares teóricos que sustentam a teoria da informação quântica, desde a definição da unidade básica de informação clássica até os estados emaranhados. Esses conceitos não apenas fundamentam a teoria da computação quântica, mas também conectam-se diretamente com aplicações práticas, como a codificação em sistemas ópticos, que será explorada nos capítulos subsequentes. A partir dessa base teórica, é possível avançar para a discussão de algoritmos quânticos, protocolos de comunicação e simulações quânticas, que serão abordados ao longo desta dissertação, consolidando a ponte entre a teoria e a prática na era da informação quântica.

2 Graus de liberdade a luz como recurso para informação quântica

Dos modelos de arquiteturas vigentes e promissores para os computadores quânticos, destaca-se os *computadores fotônicos*, particularmente no contexto de pesquisas de fronteira [48]. Nesse sentido, uma das propostas para realizações experimentais é por meio da codificação da informação quântica nos graus de liberdade da luz: a polarização, os modos transversos e o caminho.

Com isso, também considerando a possibilidade de analogia entre circuitos ópticos clássicos e quânticos [49], esse capítulo é dedicado a codificação e manipulação da informação com os graus de liberdade da luz.

2.1 Os graus de liberdade da luz

Os graus de liberdade da luz referem-se aos diferentes parâmetros que podem ser manipulados para descrever o comportamento da luz em um sistema físico. Os principais incluem a polarização, referente a orientação das oscilações do campo elétrico, os modos transversos, sobre a distribuição espacial do campo eletromagnético, e o caminho, que indica a direção de deslocamento da onda no espaço.

As principais referências consultadas para essa discussão foram [50], [51] e [52].

2.1.1 Polarização

Além do ângulo reto entre seus campos elétrico e magnético, as ondas eletromagnéticas possuem suas vibrações transversais concentradas perpendicularmente em relação à direção de propagação no espaço. A polarização da luz é caracterizada pelo comportamento dessas oscilações, ou seja, pela orientação que os campos vetoriais oscilam. Quando o campo elétrico oscila em uma única direção, diz-se que a luz é *polarizada*. Entretanto, o mais comum de encontrar na natureza é a situação em que as componentes vetoriais oscilam dispersamente em direções distintas, equivalendo dizer que a luz natural é "não polarizada", ou *aleatoriamente polarizada* [53].

Com a solução trivial para uma onda plana monocromática que se propaga na direção z ,

$$\vec{E}(r, t) = \vec{E}_0 e^{i(kr, -\omega t)}, \quad (2.1)$$

que quando perfeitamente monocromática é polarizada, descreve-se as oscilações em módulo, direção e sentido do campo elétrico,

$$\vec{E}(z, t) = (E_{0x}\hat{x} + e^{i\delta} E_{0y}\hat{y})e^{i(k \cdot z - \omega t)}. \quad (2.2)$$

Comparando brevemente as duas equações para a onda plana, observa-se que, além de considerar as componentes do plano x e y , respectivamente, as amplitudes E_{0x} e E_{0y} , agora há o fator exponencial de diferença de fase $\delta = \delta_y - \delta_x$.

Dependendo da diferença entre as fases e as amplitudes, a polarização assumirá propriedades condizentes com um dos casos: polarização linear, circular ou elíptica, embora as duas primeiras classificações sejam casos particulares da última [50].

A *polarização linear* ocorre quando a diferença de fase é do tipo $\delta = n\pi$ com n inteiro positivo ou negativo. Deste modo, a parte imaginária do fator de fase relativa na componente do plano y será anulada,

$$\vec{E}(z, t) = E_x(z, t) + E_y(z, t) = (\hat{x}E_x \pm \hat{y}E_y)e^{i(k \cdot z - \omega t)}. \quad (2.3)$$

Está claro que o ângulo θ entre as componentes do campo elétrico, definindo, portanto, a orientação da polarização, é descrito como

$$\tan(\theta) = \frac{E_{0y}}{E_{0x}}. \quad (2.4)$$

É também evidente que para determinados ângulos a componente do plano x permanecerá enquanto a do plano y é anulada, configurando assim a *polarização horizontal*. Caso contrário, tem-se a *polarização vertical*. Em especial, destaca-se quando as duas componentes são idênticas $E_x = E_y$, isto é, quando o ângulo entre elas é $\theta = 45$ e o vetor resultante está na diagonal do plano. Isso forma o estado de *polarização à ±45* e equivale à uma operação de superposição. Frequentemente, utiliza-se essa angulação para reproduzir uma porta Hadamard utilizando a polarização como grau de liberdade.

Na *polarização circular*, por sua vez, a diferença de fase será fracionária e dada por $\delta = n\pi + \frac{\pi}{2}$, para n inteiro positivo ou negativo. Nota-se que a soma do último fator indica um deslocamento de fase e também que as componentes de amplitude do campo elétrico são idênticas $E_x = E_y = E_0$ (vetor resultante diagonal). Logo,

$$\vec{E}(z, t) = E_0(\hat{x} \pm i\hat{y})e^{i(k \cdot z - \omega t)}. \quad (2.5)$$

Importante a observação do sinal na equação (2.5). Para sinal positivo, assim como no caso linear, n é par e então há uma *polarização circular à direita*. Para sinal negativo, n é ímpar e há uma *polarização circular à esquerda*.

Quando as amplitudes do campo elétrico diferem, $E_{0x} \neq E_{0y}$, e a fase relativa do plano y permanece, é o caso da *polarização elíptica*,

$$\vec{E}(z, t) = (E_{0,x}\hat{x} \pm iE_{0,y}\hat{y})e^{i(k \cdot z - \omega t)}. \quad (2.6)$$

A equação (2.6) explicita perfeitamente o porquê dos outros casos serem particularidades dela. Com amplitudes iguais, a polarização é circular, sem deslocamento de fase, é linear. Sem esforço, o sinal continua a determinar a paridade de n : quando positivo, *polarização elíptica à direita*, e quando negativo, *polarização elíptica à esquerda* [54].

Na Figura (9), estão desenhados os vetores campo elétrico de cada respectivo estado polarização no plano transverso. Da esquerda para a direita, a polarização linear, circular e elíptica.

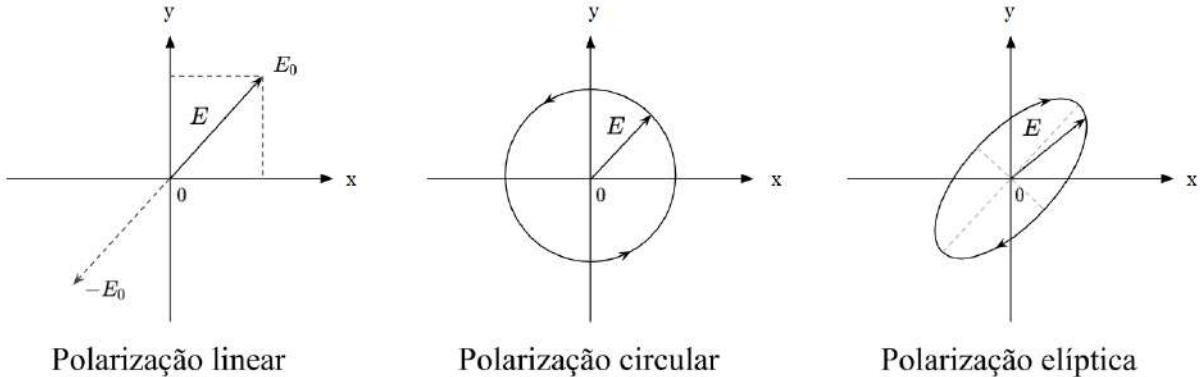


Figura 9 – Da esquerda para a direita, polarização linear, circular e elíptica. Fonte: Autoria própria.

Agora, para definir a polarização a partir da intensidade, primeiramente, considere as bases de polarização

$$\begin{aligned} \hat{e}_1 &= \hat{x} & [\text{polarização horizontal}] \\ \hat{e}_2 &= \hat{y} & [\text{polarização vertical}] \\ \hat{e}_3 &= \frac{\hat{x} + i\hat{y}}{\sqrt{2}} & [\text{polarização circular à direita}] \\ \hat{e}_4 &= \frac{\hat{x} - i\hat{y}}{\sqrt{2}} & [\text{polarização circular à esquerda}] \end{aligned} \quad (2.7)$$

e, também, as amplitudes complexas,

$$E_1 = a_1 e^{i\delta_1},$$

$$E_2 = a_2 e^{i\delta_2},$$

$$E_+ = a_+ e^{i\delta_+},$$

$$E_- = a_- e^{i\delta_-}.$$

Com isso, o campo elétrico $\hat{\mathcal{E}}$, pode ser descrito em termos das componentes associadas às bases lineares (\hat{e}_1, \hat{e}_2) e, por sua vez, o campo \hat{E}_{+-} com relação a base circular (\hat{e}_+, \hat{e}_-) , respectivamente,

$$\hat{\mathcal{E}}_{1,2} = E_1 \hat{e}_1 + E_2 \hat{e}_2, \quad (2.8)$$

$$\hat{\mathcal{E}}_{+-} = E_+ \hat{e}_+ + E_- \hat{e}_-. \quad (2.9)$$

Logo, os *parâmetros de Stokes* na base linear são definidos como [55]:

$$\mathcal{S}_0 = |\hat{e}_1 \cdot \hat{\mathcal{E}}|^2 + |\hat{e}_2 \cdot \hat{\mathcal{E}}|^2 = a_1^2 + a_2^2, \quad (2.10)$$

$$\mathcal{S}_1 = |\hat{e}_1 \cdot \hat{\mathcal{E}}|^2 - |\hat{e}_2 \cdot \hat{\mathcal{E}}|^2 = a_1^2 - a_2^2, \quad (2.11)$$

$$\mathcal{S}_2 = 2 \operatorname{Re} ((\hat{e}_1 \cdot \hat{\mathcal{E}})(\hat{e}_2 \cdot \hat{\mathcal{E}})^*) = 2a_1 a_2 \cos(\delta_2 - \delta_1), \quad (2.12)$$

$$\mathcal{S}_3 = 2 \operatorname{Im} ((\hat{e}_1 \cdot \hat{\mathcal{E}})(\hat{e}_2 \cdot \hat{\mathcal{E}})^*) = 2a_1 a_2 \sin(\delta_2 - \delta_1). \quad (2.13)$$

O parâmetro \mathcal{S}_0 é a intensidade total da onda eletromagnética; \mathcal{S}_1 representa a diferença de intensidade entre as polarizações horizontal e vertical; \mathcal{S}_2 está associado à intensidade das polarizações inclinadas ($+45$ e -45); \mathcal{S}_3 descreve a intensidade correspondente às polarizações circulares direita (\hat{e}_+) e esquerda (\hat{e}_-). Analogamente, para a base circular, os parâmetros são:

$$\mathcal{S}_0 = a_+^2 + a_-^2, \quad (2.14)$$

$$\mathcal{S}_1 = a_+^2 - a_-^2, \quad (2.15)$$

$$\mathcal{S}_2 = 2a_+ a_- \cos(\delta_- - \delta_+), \quad (2.16)$$

$$\mathcal{S}_3 = 2a_+ a_- \sin(\delta_- - \delta_+). \quad (2.17)$$

Observa-se que os parâmetros \mathcal{S}_2 e \mathcal{S}_3 carregam informações de fase, tanto para a base linear, quanto para a circular.

Os parâmetros de Stokes descrevem completamente o estado de polarização de uma onda eletromagnética, quantificando a intensidade total e sua distribuição entre as

componentes de polarização. Os parâmetros \mathcal{S}_2 e \mathcal{S}_3 carregam informações sobre a fase relativa entre as componentes do campo elétrico, essenciais para caracterizar polarizações circulares e elípticas. A relação entre os parâmetros de Stokes é dada por

$$\mathcal{S}_0^2 = \mathcal{S}_1^2 + \mathcal{S}_2^2 + \mathcal{S}_3^2, \quad (2.18)$$

que é a equação da *esfera de Poincaré*, exposta na Figura 10.

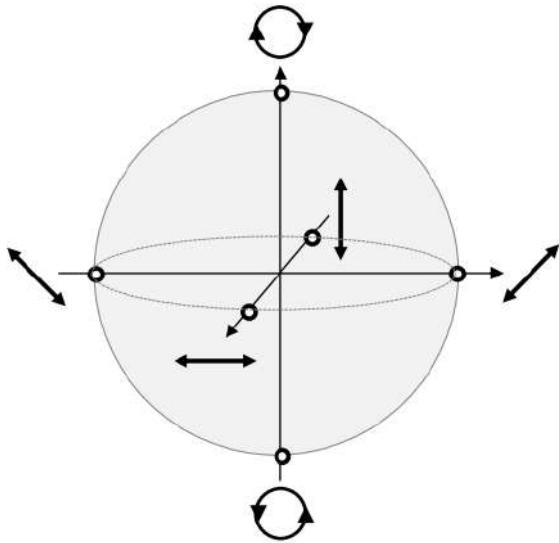


Figura 10 – Esfera de Poincaré para a polarização. Fonte: [51].

A esfera de Poincaré demonstra a correspondência entre os estados de polarização e os pontos na sua superfície. Estados de polarização completamente linear estão localizados nos pontos da circunferência equatorial, nos extremos se localizam os estados diagonais, nos pontos intermediários os estados horizontal e vertical. Os estados de polarização circular estão localizados nos polos. Em qualquer ponto arbitrário da esfera, estão os estados elipticamente polarizados, com intensidade proporcional à distância do centro da esfera [56].

Um artifício crucial para codificação da polarização da luz como informação quântica, é o *formalismo dos vetores e das matrizes de Jones* [57], [58]. Com esse, a luz polarizada pode ser escrita como:

$$\vec{E} = \begin{bmatrix} E_x(t) \\ E_y(t) \end{bmatrix} = \begin{bmatrix} E_{0x}e^{i\phi_x} \\ E_{0y}e^{i\phi_y} \end{bmatrix} = E_{0x}e^{i\phi_x} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + E_{0y}e^{i\phi_y} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad (2.19)$$

onde E_{0x} e E_{0y} são as amplitudes das componentes x e y, respectivamente. Reescrevendo como combinação linear, nota-se a evidente semelhança com a base computacional. Agora, pode-se representar um feixe luminoso paralelizado como um vetor de Jones \vec{E}_0 , que

irá incidir em determinado dispositivo óptico \mathcal{A} (uma matriz de Jones) e, emergindo dessa interação, um novo vetor transformado \vec{E} . Com essas considerações, todo o processo percorrido pelo feixe luminoso se resume a um problema de autovalores:

$$\vec{E} = \mathcal{A}\vec{E}_0. \quad (2.20)$$

O dispositivo óptico responsáveis pelas transformações na polarização são conhecidos como *placas de onda*. São materiais birrefringentes, possuem índices de refração distintos entre os eixos perpendiculares e, por consequência, a velocidade de propagação nos meios será diferente também. Os eixos são denominados *eixo rápido* e *eixo lento*. Além disso, eles possuem alguma espessura d . Há uma representação gráfica do dispositivo na Figura 11.

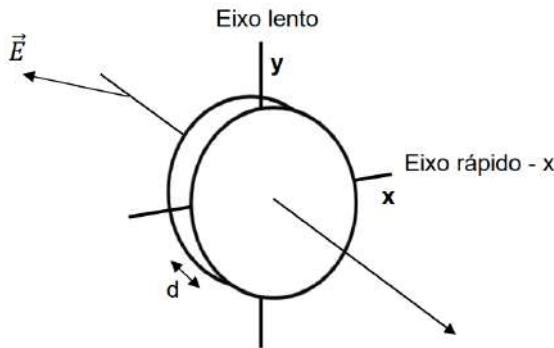


Figura 11 – Placa de onda. Fonte: [51]

A placa de meia-onda (HWP), do inglês, *half-wave plate*, possui diferença de caminho óptico $\lambda/2$. Sendo θ é o ângulo que o eixo rápido faz com a horizontal. A representação dessa placa em formalismo de Jones é

$$HWP = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}. \quad (2.21)$$

A placa de quarto de onda (QWP), do inglês, *quarter-wave plate*, possui diferença de caminho óptico $\lambda/4$ e o ângulo entre o eixo rápido e a horizontal continua sendo θ . Sua representação matricial é

$$QWP = \begin{pmatrix} \cos^2(\theta) + i\sin^2(\theta) & \cos(\theta)\sin(\theta)(1-i) \\ \cos(\theta)\sin(\theta)(1-i) & i\cos^2(\theta) + \sin^2(\theta) \end{pmatrix}. \quad (2.22)$$

A SWP, do inglês *S wave plate*, é uma placa de onda superestrutura que converte polarização linear incidente em polarização radial ou azimutal dependendo da sua configuração angular. Ela também pode ser utilizada para converter polarização circular em um

feixe que carrega momento angular orbital (OAM) [59], aplicando uma fase que varia de acordo com a posição transversal no feixe, o que modifica a distribuição de intensidade e fase da luz. No geral, são dispositivos valiosos para a manipulação transversal da luz, permitindo a geração de feixes complexos com propriedades específicas. Por exemplo, como serão explicados na próxima secção, ao incidir com um feixe gaussiano fundamental (com perfil de intensidade padrão de feixes luminosos), ao projetá-lo numa SWP adequadamente configurada, é possível transformar transversalmente esse em modos de Hermite-Gauss, que serão explicados a seguir.

2.1.2 Modos transversos: Hermite-Gauss e Laguerre-Gauss

Em contraste com as ondas planas, feixes luminosos não se propagam no infinito. Na realidade, a invariância translacional desse é perdida e a direção de propagação não é mais restrita. Além disso, seu perfil de intensidade tende a ser deformado, isto é, a distribuição da luz aumenta espacialmente. Não é a única alteração possível no visual do feixe luminoso: os modos transversos dizem respeito aos padrões de distribuição do perfil de intensidade e, também, fase da luz nas direções perpendiculares à propagação [53].

Partindo desse princípio, seja a equação de Helmholtz, representação independente do tempo da equação de onda,

$$(\nabla^2 + k^2)A_j(r, \omega) = 0, \quad (2.23)$$

onde $A_j(r, \omega)$ é o j-ésimo vetor pontencial do domínio de frequência

$$A_j(r, t) = \int_0^\infty d\omega A_j(r, \omega) e^{i\omega t}, \quad (2.24)$$

e $\omega = ck$. A solução trivial dessa equação para uma onda plana se propagando na direção z é um *Ansatz* do tipo

$$A_j(r, \omega) = \psi_j(r, \omega) e^{ikz}. \quad (2.25)$$

Substituindo a solução na equação (2.23) e utilizando a aproximação paraxial $2ik\partial_z\psi_j \gg \partial_z^2\psi_j$, é possível encontrar

$$\frac{\partial^2\psi_j}{\partial x^2} + \frac{\partial^2\psi_j}{\partial y^2} = -2ik\frac{\partial\psi_j}{\partial z}, \quad (2.26)$$

que é a equação de onda paraxial, ou ainda, a *equação paraxial de Helmholtz*. Vale a observação de que com uma simples troca da dependência espacial por uma dependência temporal, essa equação diferencial parcial torna-se semelhante à equação de onda quântica.

A solução fundamental dessa equação resulta no que é conhecido como *feixe gaussiano*,

$$\psi_j(x, y, z) = \frac{2^{1/2}}{\pi^{1/2} w(z)} \exp\left(-\frac{x^2 + y^2}{w^2(z)}\right) \exp\left(-i\frac{k(x^2 + y^2)}{2R(z)} + i\phi(z)\right), \quad (2.27)$$

onde o raio de curvatura do feixe é

$$R(z) = z + \frac{z_R^2}{z}, \quad (2.28)$$

e a fase de Gouy dada por

$$\phi(z) = \arctg\left(\frac{z}{z_R}\right), \quad (2.29)$$

e o comprimento de Rayleigh definido como

$$z_R = \frac{\pi\omega_0^2}{\lambda}, \quad (2.30)$$

sendo w_0 a largura na posição $z = 0$, de acordo com a variação que é proporcional a essa, descrita por

$$w(z) = w_0 \sqrt{1 + \left(\frac{z}{z_R}\right)^2}. \quad (2.31)$$

Todas essas grandezas e parâmetros relativos à equação paraxial estão esquematizadas na Figura 12. Nessa representação, a variação da largura do feixe gaussiano, se propagando na direção k_z , transita de ω_0 na origem até $2\omega_0$, definida por um ângulo arbitrário θ , no comprimento de Rayleigh.

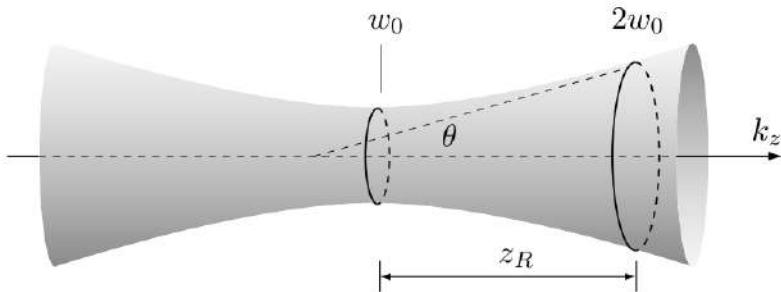


Figura 12 – Feixe gaussiano. Fonte: [60]

Além da solução fundamental há duas famílias de soluções de ordem maiores, os modos de Hermite-Gauss e os modos de Laguerre-Gauss. Encontrar ambas famílias de

soluções é um trabalho árduo e não precisa ser acrescentado na presente discussão, analisar as somente as soluções já é o suficiente. Para mais detalhes, é recomendado consultar a referência [60].

Em primeiro lugar, considera-se a solução da equação paraxial em coordenadas cartesianas, os chamados modos de Hermite-Gauss.

$$H_{m,n}(r) = \psi_{m,n}(x, y, z) = \frac{C_{m,n}}{w(z)} H_n \frac{\sqrt{2}x}{w(z)} H_m \frac{\sqrt{2}y}{w(z)} e^{\left(-\frac{x^2+y^2}{w^2(z)}\right)} e^{\left(-i\frac{k(x^2+y^2)}{2R(z)}\right)} e^{(-i(n+m+1)\phi(z))} \quad (2.32)$$

Os polinômios de Hermite H_n e H_m são definidos por suas ordens dadas, respectivamente, por n e m . É direto que a escolha das ordens $m = n = 0$ resulta na solução fundamental. Em contrapartida, ao aumentar a ordem n o perfil de intensidade do feixe tende a se dividir verticalmente, ou a divisão ocorre horizontalmente conforme a ordem m cresce. O padrão de divisão do perfil de intensidade dos modos $H_{m,n}$ está bem representando à direita da Figura (13). As linhas nodais do modo $H_{1,2}$ demonstram como ocorre a simultaneidade dessas divisões horizontais e verticais.

Perfil transverso de intensidade e fase para os modos de Hermite-Gauss

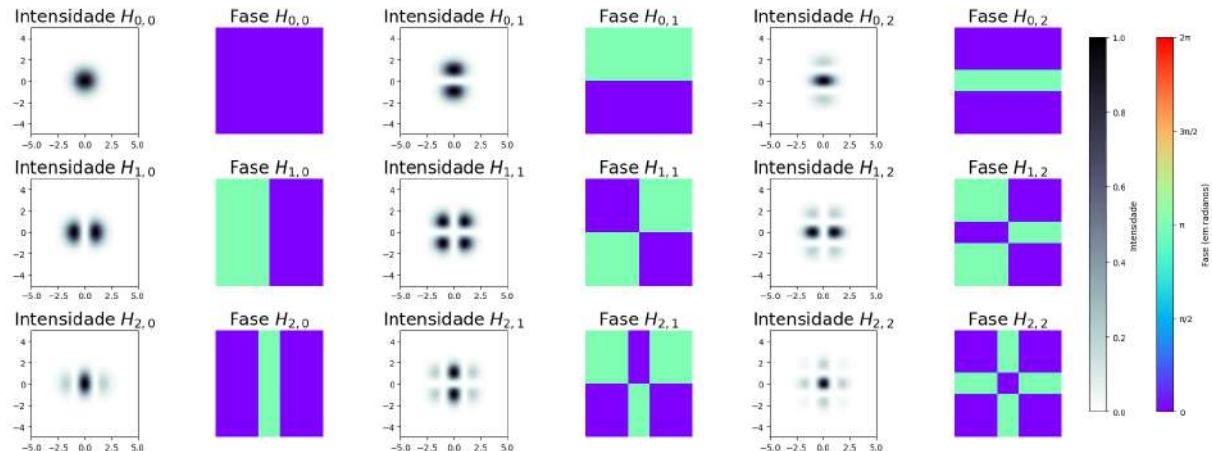


Figura 13 – Perfil transverso de intensidade e de fase para os modos $H_{m,n}$. Imagens obtidas com *python*. Fonte: Autoria própria.

Agora, dada a resolução da equação paraxial em coordenadas cilíndricas, tem-se os modos de Laguerre-Gauss.

$$L_l^\rho(r) = \psi_l^\rho(r, z, \xi) = \left[\sqrt{\frac{2\rho!}{\pi w^2(z)(\rho + |l|)!}} \left[\frac{\sqrt{2}r}{w(z)} \right]^{|l|} e^{\left(-\frac{r^2}{w^2(z)}\right)} \right] \times \left[L_l^p \left[\frac{2r^2}{w^2(z)} \right] e^{i[kz - (2\rho + |l| + 1)\phi + \frac{kr^2}{2R(z)} + l\xi]} \right] \quad (2.33)$$

Como esperado, essas soluções dependem dos polinômios de Laguerre L_l^p . Os índices que substituem as ordens das soluções anteriores são chamados de *índice radial* p , diretamente

relacionado com o número de anéis na distribuição de intensidade, e *índice azimutal* l , associado à singularidade de fase ξ na origem do plano. Consequência disso é que todos os modos L_l^p para $l \neq 0$ apresentam *momento angular orbital* (OAM), do inglês, *orbital angular momentum* [50].

O efeito de ambos índices podem ser observados também através da Figura (14). Conforme aumenta-se o número do índice radial a tendência é proporcionalmente aumentar o número de anéis. O índice azimutal provoca uma divisão semelhante à dos modos HG, agindo tanto na intensidade concentrada no centro quanto nos anéis.

Perfil transverso de intensidade e fase para os modos de Laguerre-Gauss

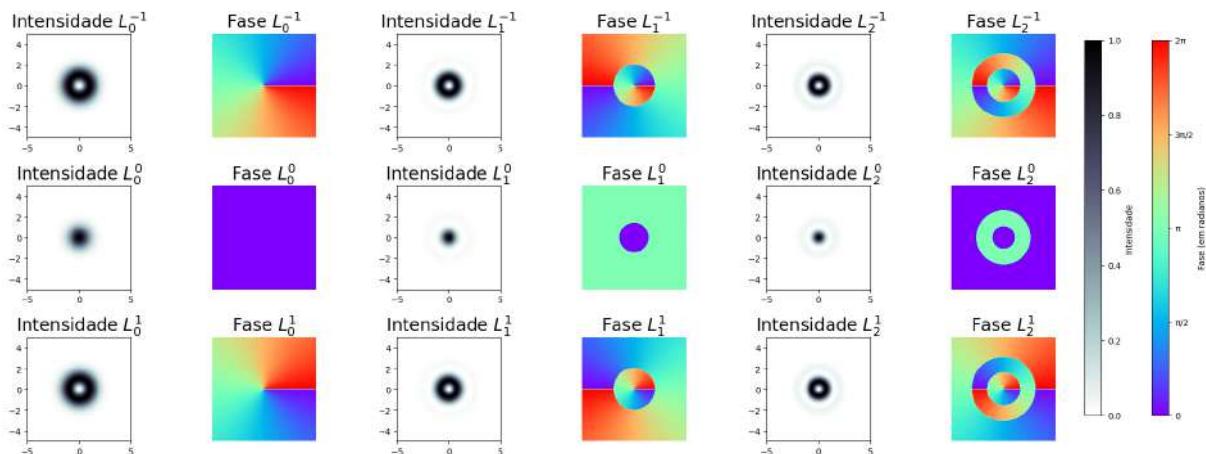


Figura 14 – Perfil transverso de intensidade e de fase para os modos LG_p^l . Imagens obtidas com *python*. Fonte: Autoria própria.

Os modos de Hermite-Gauss e Laguerre-Gauss de primeira ordem representam sistemas de dois níveis e podem ser experimentalmente manipulados com facilidade. Além disso, há a possibilidade de relacionar os dois modos como combinações lineares de um com outro [61]:

$$L_0^{\pm 1} = \frac{1}{\sqrt{2}}(H_{1,0} \pm iH_{0,1}) \quad (2.34)$$

E também que os modos de Hermite-Gauss podem ser escritos como combinação linear dos seus próprios modos horizontal e vertical,

$$H_{0,1}^\theta = \cos(\theta)H_{1,0} + \sin(\theta)H_{0,1} \quad (2.35)$$

Para o ângulo $\theta = \pm\pi/4$ tem-se as seguintes equações,

$$H_{0,1}^{\pi/4} = \frac{1}{\sqrt{2}}(H_{1,0} + H_{0,1}) \quad \text{e} \quad H_{0,1}^{-\pi/4} = \frac{1}{\sqrt{2}}(H_{1,0} - H_{0,1}). \quad (2.36)$$

Sendo assim, conclui-se que a combinação linear de ambos os modos tranversos discutidos pode reproduzir superposição. Logo, como desejado, os modos de Hermite-Gauss e Laguerre-Gauss de primeira ordem são graus de liberdade que possuem todas as condições necessárias para codificar a informação quântica.

Então, como demonstrado em [51], é possível desenhar uma esfera de Poincaré para os modos transversos, como está na Figura 15.

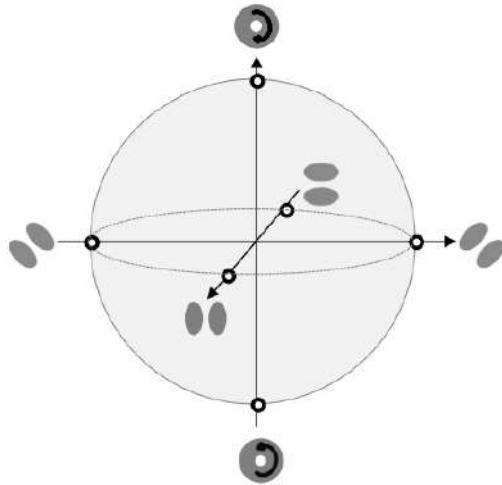


Figura 15 – Esfera de Poincaré para os modos transversos. Fonte: [51].

Nos polos norte e sul, respectivamente, estão os modos de Laguerre-Gauss de primeira ordem L_0^1 e LG_0^{-1} . Na linha do equador, os modos de Hermite-Gauss também de primeira ordem, HG_{01} e HG_{10} , além dos rotacionados nos extremos, $H_{0,1}^{\pi/4}$ e $H_{0,1}^{-\pi/4}$. Qualquer outro ponto na esfera são modos intermediários entre as duas famílias de soluções.

Os dispositivos ópticos que vão operar transformações nos modos transversos são generalizados como:

$$C(\theta, \phi) = \begin{pmatrix} \cos^2(\theta) + e^{i\phi} \sin^2(\theta) & \cos(\theta) \sin(\theta)(e^{i\phi} - 1) \\ \cos(\theta) \sin(\theta)(e^{i\phi} - 1) & e^{i\phi} \cos^2(\theta) + \sin^2(\theta) \end{pmatrix}, \quad (2.37)$$

sendo θ o ângulo de inclinação e ϕ , a fase associada ao elemento óptico, que pode variar dependendo do tipo de transformação que ele realiza. São conhecidos como *conversores astigmáticos*.

Quando $\phi = \pi$, descreve-se um *prisma de Dove*, um prisma triangular com base de trapézio de largura L , altura h e laterais inclinadas à $\alpha = 45^\circ$. A luz incidente sofrerá um processo de reflexão interna, portanto, ao sair pela face oposta, será rotacionada à $\theta_e = 180^\circ$ e também invertida. A depender dos modos transversos desejados, basta rotacionar o prisma em sua base à determinado ângulo Φ , como mostra a Figura 16.

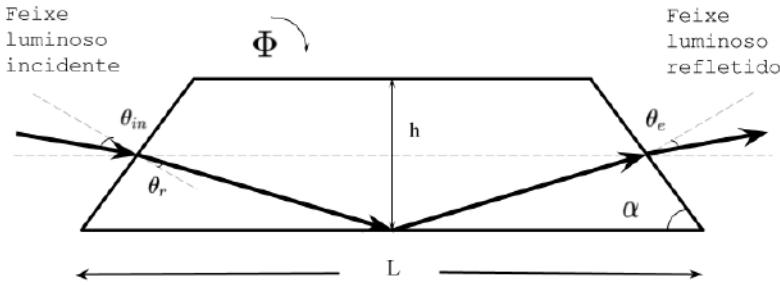


Figura 16 – Prisma de Dove. Fonte: Autoria própria.

Esse dispositivo é descrito matricialmente como:

$$C(\theta, \pi) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}. \quad (2.38)$$

Quando há uma defasagem de $\phi = \pi/2$, significa que deve existir uma distância $d = \sqrt{2}f$ entre um par de lentes cilíndricas com determinada distância focal f . Esse arranjo transforma modos de Hermite-Gauss, de primeira ordem, em modos de Laguerre-Gauss com singularidades de fase. A Figura 17 ilustra a montagem desse dispositivo óptico.

Geralmente, esse conversor de modos costuma ser representado matricialmente como:

$$C(\theta, \pi/2) = \begin{pmatrix} \cos^2(\theta) + i\sin^2(\theta) & \cos(\theta)\sin(\theta)(1-i) \\ \cos(\theta)\sin(\theta)(1-i) & i\cos^2(\theta) + \sin^2(\theta) \end{pmatrix}. \quad (2.39)$$

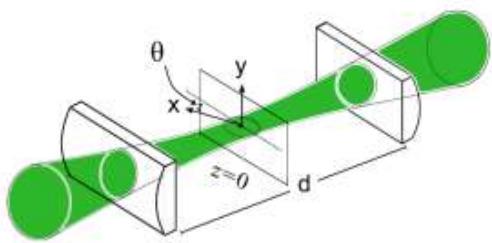


Figura 17 – Conversor astigmático. Fonte: [62].

2.1.3 Caminho

Por fim, é denominado caminho, o grau de liberdade referente à direção de propagação da luz. Estabelecido o comportamento ondulatório da luz clássica, o fluxo de energia é descrito pelo vetor de Poynting [53],

$$S = \frac{1}{\mu_0} (B \times E), \quad (2.40)$$

sendo μ_0 a susceptibilidade magnética no vácuo. Equivale dizer que a energia está fluindo paralelamente à direção de propagação da luz.

Portanto, a informação quântica pode ser codificada no caminho de propagação do feixe luminoso. Do mesmo modo, como foi para a polarização e para os modos transversos, há uma representação na esfera de Poincaré para o caminho na Figura 18.

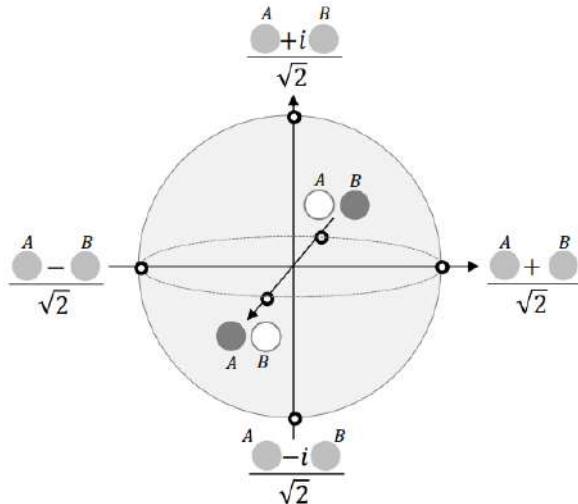


Figura 18 – Esfera de Poincaré para o caminho. Fonte: [51].

Na linha do equador, estão situados dois caminhos A e B, para cada ponto no ponto médio da circunferência, um deles está acesso e o outro apagado. Nos extremos do equador, estão as possibilidades de caminho dividido. Nos polos, a repartição conta com a presença de fase relativa.

Geralmente, o percurso do feixe luminoso é desviado através de espelhos. Mas, além desses, há um dispositivo óptico, um cubo, que transmite e reflete a luz parcialmente, de acordo com suas propriedades materiais. Ele é chamado divisor de feixe (BS), ou *beam-splitter*, em inglês. A matriz para um BS perfeitamente balanceado, isto é, que divide ambas as partes igualmente, é dada por

$$BS = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2.41)$$

Há também o divisor de feixe polarizado (PBS), ou *polarized beam-splitter*, em inglês. Em resumo, é um cubo com espelho que não apenas reflete e transmite o caminho, mas também separa as polarizações.

Na Figura 19 estão representadas as atuações de ambos divisores de feixes. Na esquerda, tem-se o PBS, que usualmente divide o feixe luminoso selecionando com base na sua polarização: a polarização horizontal é transmitida enquanto que a vertical é refletida. Na direita, há o BS, que idealmente transmite e reflete a luz de forma igualitária.

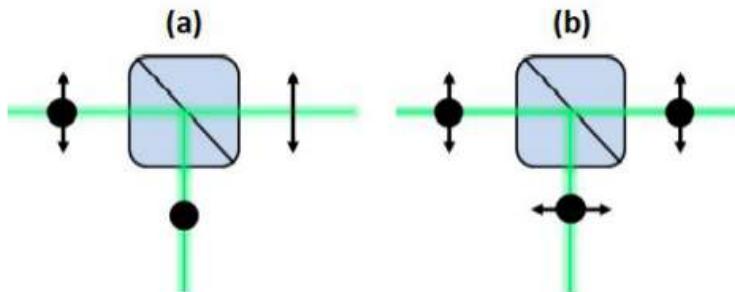


Figura 19 – Representação dos divisores de feixes: a) PBS e b) BS. Fonte: [63].

2.2 Codificação da informação quântica

No objetivo de codificar a informação nos graus de liberdade da luz, é indispensável definir as bases computacionais para cada um deles. Ao considerar a esfera de Bloch, apresentada anteriormente na Figura 4, e compará-la com as esferas de Poincaré, individualmente, constrói-se uma ponte para a analogia direta entre elas.

Logo, para a polarização, com os elementos da linha do equador de sua esfera, é possível codificar $|H\rangle$ como a polarização horizontal, $|V\rangle$ para a polarização vertical, $|D\rangle$ como a polarização diagonal e $|E\rangle$ como a polarização anti-diagonal. No caso das polarizações circulares, estas estão associadas aos polos norte e sul da esfera de Poincaré, sendo fundamentais para codificar superposições com diferença de fase. A polarização circular direita $|R\rangle$ é descrita como $\frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ e corresponde ao polo positivo no eixo y da esfera de Bloch. Já a polarização circular esquerda $|L\rangle$ é representada por $\frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$ e está associada ao polo negativo no eixo y .

Do mesmo modo, para os modos transversos, a associação ocorre da seguinte maneira: $|h\rangle$ é o modo HG_{10} , $|v\rangle$ é HG_{01} , $|+\rangle$ corresponde a uma superposição simétrica dos modos transversos, como $\frac{1}{\sqrt{2}}(HG_{10} + HG_{01})$, e $|-\rangle$ é representado por uma superposição assimétrica, como $\frac{1}{\sqrt{2}}(HG_{10} - HG_{01})$. Os modos de Laguerre-Gauss nos polos sul e norte são correspondentes às superposições com diferença de fase, como mostra a equação (2.34).

Por fim, para o grau de liberdade do caminho, as diferentes trajetórias que o feixe luminoso pode percorrer serão associadas com os estados quânticos. Isso ocorre

considerando dois caminhos distintos, u (*up*) e d (*down*), respectivamente, caminho superior e inferior. Logo, a superposição $|+\rangle = \frac{1}{\sqrt{2}}(|u\rangle + |d\rangle)$, correspondendo a uma divisão coerente entre os dois caminhos e, a superposição $|-\rangle = \frac{1}{\sqrt{2}}(|u\rangle - |d\rangle)$ indica uma diferença de fase entre os caminhos.

A Tabela 3 demonstra as equivalências dos graus de liberdade com a base computacional quântica.

Codificação da informação quântica nos graus de liberdade da luz			
Informação quântica	Polarização	Modos transversos	Caminho
$ 0\rangle$	$ H\rangle$	$ h\rangle$	$ u\rangle$
$ 1\rangle$	$ V\rangle$	$ v\rangle$	$ d\rangle$
$ +\rangle$	$\frac{1}{\sqrt{2}}(H\rangle + V\rangle)$	$\frac{1}{\sqrt{2}}(h\rangle + v\rangle)$	$\frac{1}{\sqrt{2}}(u\rangle + d\rangle)$
$ -\rangle$	$\frac{1}{\sqrt{2}}(H\rangle - V\rangle)$	$\frac{1}{\sqrt{2}}(h\rangle - v\rangle)$	$\frac{1}{\sqrt{2}}(u\rangle - d\rangle)$
$ R\rangle$	$\frac{1}{\sqrt{2}}(H\rangle + i V\rangle)$	$\frac{1}{\sqrt{2}}(h\rangle + i v\rangle)$	$\frac{1}{\sqrt{2}}(u\rangle + i d\rangle)$
$ L\rangle$	$\frac{1}{\sqrt{2}}(H\rangle - i V\rangle)$	$\frac{1}{\sqrt{2}}(h\rangle - i v\rangle)$	$\frac{1}{\sqrt{2}}(u\rangle - i d\rangle)$

Tabela 3 – Codificação das bases computacionais da informação quântica nos graus de liberdade da luz, incluindo a polarização, os modos transversos e o caminho. Fonte: Autoria própria.

3 A transformada quântica de Fourier

Nesse capítulo, a discussão será centrada na Transformada Quântica de Fourier (QFT, do inglês *Quantum Fourier Transform*), base fundamental de algoritmos quânticos para solução de problemas com características periódicas. Antes, deve-se discorrer brevemente sobre a transformada clássica e as possibilidades decorrentes de sua discretização, no objetivo de demonstrar o potencial de seu análogo quântico.

3.1 A transformada rápida de Fourier

Na física matemática, frequentemente há expressões como

$$g(x) = \int_a^b f(t)K(x,t)dt, \quad (3.1)$$

onde a função $g(x)$ é definida como a *transformada integral* de $f(t)$, com a transformação sendo configurada pelos limites a, b e o núcleo $K(x,t)$ que permanecerão os mesmos para quaisquer pares de funções. Portanto, as fórmulas integrais que definem a transformada de Fourier e sua inversa são

$$\begin{aligned} F(\omega) &= \sqrt{\frac{1}{2\pi}} \int_{-\infty}^{+\infty} f(t)e^{i\omega t} dt \\ f(t) &= \sqrt{\frac{1}{2\pi}} \int_{-\infty}^{+\infty} F(\omega)e^{-i\omega t} d\omega \end{aligned}, \quad (3.2)$$

com $f(t)$ sendo a função temporal e $F(\omega)$ a transformação de fase. Através da decomposição da exponencial em ondas senoidais (par) e cossenoidais (ímpar), respectivamente,

$$\begin{aligned} F(\omega)_s &= \sqrt{\frac{2}{\pi}} \int_0^{\infty} f(t)\sin(\omega t)dt \\ F(\omega)_c &= \sqrt{\frac{2}{\pi}} \int_0^{\infty} f(t)\cos(\omega t)dt \end{aligned}. \quad (3.3)$$

o caráter ondulatório da transformada é evidenciado, e, por consequência, seu amplo emprego em problemas de processamentos de sinais. No contexto da óptica, ela é responsável pela transição da informação de uma onda eletromagnética monocromática do espaço temporal para o espaço de frequência, ou seja, nos permite acesso à informação de fase do sistema [64].

Há determinados contextos em que os dados de entrada do sinal são discretos, como, por exemplo, em problemas físicos complexos de serem resolvidos analiticamente

que podem ser solucionados por métodos numéricos de discretização do domínio. Além disso, nos computadores clássicos, o processamento de sinais é inherentemente discretizado, já que operam através de valores binários. Portanto, parcela considerável de problemas na ciência da computação podem ser solucionados pela transformada *discreta* de Fourier, definida como

$$F(x_p) = \sqrt{\frac{1}{2}} \sum_{k=0}^{N-1} e^{2\pi i kp/N} f(x_k), \quad (3.4)$$

onde $x_k = 2\pi k/N$ são os pontos do domínio do tempo discretizado no intervalo $(0, 2\pi)$, $F(x_p)$ os coeficientes no domínio de frequência e N o número de pontos. Define-se também a inversa

$$f(x_j) = \sqrt{\frac{1}{2}} \sum_{p=0}^{N-1} e^{-2\pi i jp/N} F(x_p). \quad (3.5)$$

Mesmo que amplamente utilizada no processamento digital, a discretização sozinha não é eficiente na resolução de problemas complexos, dada sua complexidade computacional de ordem quadrática $O(N^2)$.

Dante disso, com a finalidade de superar essa limitação, procedimentos para obtenção da transformada rápida de Fourier foram desenvolvidos [65]. Em resumo, o princípio do processo comumente aplicado consiste no método de divisão e conquista. Considerando o número de pontos do domínio como $N = 2^m$, para algum inteiro m , é possível decompor a equação (3.4) em subdomínios, igualmente divididos, par e ímpar. Portanto,

$$F(x_p) = \sqrt{\frac{1}{2}} \left[\sum_{k=0}^{N/2-1} e^{2\pi i \frac{2kp}{N}} f(x_{2k}) + \sum_{k=0}^{N/2-1} e^{2\pi i \frac{(2k+1)p}{N}} f(x_{2k+1}) \right]. \quad (3.6)$$

Com a simplificação dos expoentes

$$\begin{aligned} e^{2\pi i \frac{2kp}{N}} &= e^{2\pi ikp/(N/2)} \\ e^{2\pi i \frac{(2k+1)p}{N}} &= e^{2\pi ik/(N/2)} e^{2\pi ip/N}, \end{aligned} \quad (3.7)$$

e sua respectiva substituição,

$$F(x_p) = \sqrt{\frac{1}{2}} \left[\sum_{k=0}^{N/2-1} e^{2\pi ikp/(N/2)} f(x_{2k}) + e^{2\pi ip/N} \sum_{k=0}^{N/2-1} e^{2\pi ik/(N/2)} f(x_{2k+1}) \right], \quad (3.8)$$

resultando finalmente na expressão recursiva:

$$F(x_p) = \sqrt{\frac{1}{2}} [F_{even}(x_p) + e^{2\pi i p/N} F_{odd}(x_p)]. \quad (3.9)$$

O algoritmo de Cooley-Tukey, como ficou conhecido, tem preferência, principalmente, por sua versatilidade e pelo notável ganho de complexidade computacional de ordem logarítmica $O(N \log N)$. Resumindo, em comparação com a transformada discreta, que analisa o sinal ponto a ponto para decompor sequencialmente suas frequências componentes em complexidade computacional $O(N^2)$, para $N = 2^m$ pontos no domínio, a estratégia da transformada rápida consiste em dividir esse domínio em duas partes (par e ímpar). Entretanto, mesmo com essa otimização, o sistema ainda depende da lógica sequencial, isto é, precisa calcular cada subproblema (subdomínio) de forma independente antes de recombinar os resultados. Essa dependência inerente impõe um limite com o qual é possível aumentar a eficiência na resolução desses problemas.

Alternativamente, o algoritmo pode ser explicado através da decomposição da matriz DFT, definida por

$$F_n := \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \dots & \omega_n^{(n-1)} \\ 1 & \omega_n^2 & \omega_n^4 & \dots & \omega_n^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{(n-1)} & \omega_n^{2(n-1)} & \dots & \omega_n^{(n-1)^2} \end{bmatrix}, \quad (3.10)$$

sendo $\omega_n := \exp\left(\frac{2\pi i}{n}\right)$. Nesse contexto, F_n representa um operador que realiza a transformada discreta para uma sequência de n bits. Essa decomposição é entendida por meio da natureza recursiva do algoritmo: inicialmente, a matriz $n \times n$ é reduzida em submatrizes $n/2$, separando partes par e ímpar, até que o processo é encerrado ao atingir dimensão $n = 2$ [66].

No geral, a estratégia de divisão e conquista é essencial para a adaptação do procedimento para implementações que demandam uso de *hardware*, como, por exemplo, unidades de processamento gráfico, para otimização de problemas computacionalmente difíceis. Desse método, a paralelização das operações pode ser partitionada em subproblemas menores, ou seja, reduzir em submatrizes, portanto otimizando o desempenho em sistemas com múltiplos núcleos ou unidades de processamento em paralelo [67].

3.2 Transformada quântica de Fourier

A transformação do espaço de posição para o espaço de momento, ou seja, que permite acesso à informação de fase do sistema quântico, é definida pelo operador quântico

$$F := \frac{1}{\sqrt{2^n}} \sum_{x,y=0}^{2^n-1} \exp\left(2\pi i \frac{xy}{2^n}\right) |y\rangle \langle x| \quad (3.11)$$

sendo $|x\rangle, |y\rangle$ vetores de base do espaço de Hilbert $\mathbb{H}^{\otimes n}$. Considerando a propriedade de ortogonalidade dos estados quânticos, então

$$F|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \exp\left(2\pi i \frac{xy}{2^n}\right) |y\rangle \quad (3.12)$$

definindo $|x\rangle$ como a superposição de estados da base computacional e n o número de qubits.

Com isso, como a informação está codificada na base binária quântica, a partir das frações binárias

$$0.a_1a_2 \cdots a_m := \frac{a_1}{2} + \frac{a_2}{4} + \cdots + \frac{a_m}{2^m} = \sum_{l=1}^m a_l 2^{-l} \quad (3.13)$$

pode-se escrever o decimal fracionário como

$$x = \sum_{j=0}^{n-1} x_j 2^j \quad (3.14)$$

e, portanto, substituindo-o na equação (3.12), resulta na seguinte notação

$$F|x\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} [|0\rangle + e^{2\pi i 0.x_j \dots x_0} |1\rangle]. \quad (3.15)$$

Com a observação das transformações provocadas na base computacional, nota-se a possibilidade de descrever essa com um conjunto de portas controladas de fase, sempre ponderadas pelo alvo do circuito até serem reduzidas a porta de identidade [68].

Também em representação de matrizes:

$$F = \frac{1}{\sqrt{2^n}} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega_n & \dots & \omega_n^{2^n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{2^n-1} & \dots & \omega_n^{(2^n-1)^2} \end{bmatrix}, \quad (3.16)$$

com $\omega_n = \exp\left(\frac{2\pi i}{2^n}\right)$ e n o número de qubits.

O circuito quântico generalizado está exibido na Figura (20).

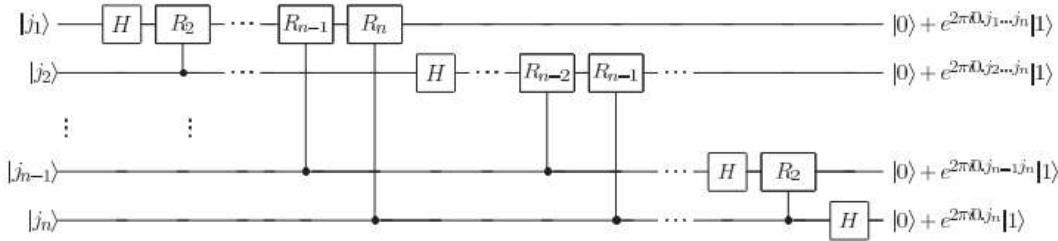


Figura 20 – Circuito quântico generalizado da QFT. Fonte: [9].

Observe que, pela recursividade do circuito, conforme prossegue-se de $|j_i\rangle$ para $|j_{i+1}\rangle$ sendo $i \in [1, n]$, a quantidade de operações controladas de fase é reduzida. Para $|j_n\rangle$ a única transformação controlada resulta na identidade e, portanto, o último qbit não sofre transformações de fase em sua base computacional, que somente é superposta pela porta Hadamard que encerra o processo.

É conveniente destacar ainda que há um total de $n(n + 1)/2$ portas de fase provocando rotações nesse circuito. Consequentemente, a complexidade desse algoritmo será da ordem quadrática $O(n^2)$, em contraste com as complexidades de seus análogos clássicos (DFT e FFT). Essa otimização decorre do processamento paralelo da informação. Ao preparar os qbits em superposição antes das transformações de fase, todas as frequências potenciais são avaliadas simultaneamente. Essa diferença radical na arquitetura computacional — aliada à capacidade de amostrar apenas as frequências significativas — fundamenta o ganho de desempenho exponencial em comparação com os análogos clássicos, como, por exemplo, o algoritmo de Shor [17].

Outra consideração é que ao final do circuito, o estado inicial $|j_1 j_2 \cdots j_n\rangle$ é devolvido como $|j_n j_{n-1} \cdots j_1\rangle$. Por isso, comumente, adiciona-se uma quantidade de $n/2$ portas SWAP no estágio final do circuito, realizando as trocas em pares (o qbit central $(n - 1)/2$ permanece inalterado, caso n seja ímpar). Essa adição não altera a complexidade do circuito, quanto menos seu objetivo. Na maioria das vezes, é apenas um artifício útil para apresentação dos resultados.

A transformada quântica de Fourier inversa, ou iQFT (do inglês, *inverse Quantum Fourier Transform*), pode ser implementada utilizando um circuito quântico semelhante. A principal diferença reside na alteração das fases dos termos da matriz de Fourier, que agora são complexos conjugados das fases R_n . Matematicamente, ela é descrita pelo operador quântico:

$$F^{-1} := \frac{1}{\sqrt{2^n}} \sum_{x,y=0}^{2^n-1} \exp\left(-2\pi i \frac{xy}{2^n}\right) |y\rangle \langle x|. \quad (3.17)$$

Em outros termos, pode-se afirmar que o circuito quântico para a iQFT é análogo ao definido para a QFT, podendo descrevê-lo por um conjunto de portas controladas de

fase, porém com a fase invertida, sendo sua implementação igualmente beneficiada pela recursividade e estrutura hierárquica dos subíndices.

No presente contexto, em que o objetivo é propor um circuito óptico tripartite, dirige-se atenção exclusiva para o caso particular do sistema composto para $n = 3$ qbits.

Por intermédio do circuito para a QFT, representado na Figura 21, nota-se que as associações de fase controlada são $R_n \equiv P(\theta = \pi/4) \equiv T$ e $R_{n-1} \equiv P(\theta = \pi/2) \equiv S$, portas quânticas contempladas na equação (1.22).

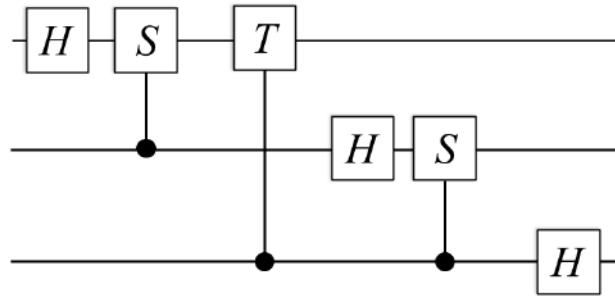


Figura 21 – Circuito da QFT para 3 qbits. Fonte: Autoria própria.

Para a transformada inversa, exposta na Figura 22, as associações ocorrem pelo complexo conjugado das portas de fase para o circuito direto, isto é, $R_n^\dagger \equiv P(\theta = -\pi/4) \equiv T^\dagger$ e $R_{n-1}^\dagger \equiv P(\theta = -\pi/2) \equiv S^\dagger$.

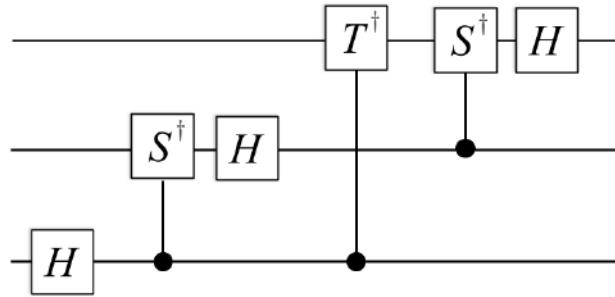


Figura 22 – Circuito da iQFT para 3 qbits. Fonte: Autoria própria.

Além disso, considerando os elementos da base computacional para $n = 3$ qbits e usando as frações binárias da equação (3.15), calcula-se os fatores de fase. A tabela 4 apresenta as associações entre base computacional e fatores de fase. A segunda coluna mostra a fração binária $0.x_2x_1x_0$, obtida a partir da decomposição do número $x = x_2x_1x_0$

no sistema binário. A terceira coluna exibe o fator de fase correspondente, que é o termo de fase aplicado na QFT.

Base computacional	Fração binária	Fator de fase
$ 000\rangle$	$0.000_2 = 0$	1
$ 001\rangle$	$0.001_2 = \frac{1}{8}$	$e^{\pi i/4}$
$ 010\rangle$	$0.010_2 = \frac{1}{4}$	i
$ 011\rangle$	$0.011_2 = \frac{3}{8}$	$e^{3\pi i/4}$
$ 100\rangle$	$0.100_2 = \frac{1}{2}$	-1
$ 101\rangle$	$0.101_2 = \frac{5}{8}$	$e^{5\pi i/4}$
$ 110\rangle$	$0.110_2 = \frac{3}{4}$	$-i$
$ 111\rangle$	$0.111_2 = \frac{7}{8}$	$e^{7\pi i/4}$

Tabela 4 – Fatores de fase da QFT para os estados da base computacional com 3 qbits. Fonte: Autoria própria.

Observe a periodicidade das exponencias dos estados que possuem o último qbit na base computacional $|1\rangle$. Os expoentes seguem uma sequência artimética com uma distância de $\pi/2$ entre o atual e o sucessor. Consequentemente, ela também é cíclica e retornará para o valor inicial após completar uma rotação completa (2π). Essa progressão aritmética para esses estados evidencia o comportamento estruturado da QFT em termos de rotações no espaço de Hilbert.

Em adição, é válida a recordação das seguintes simplificações:

$$\begin{aligned} e^{2\pi i(1/8)} &= e^{\pi i/4}, & e^{2\pi i(1/4)} &= i, & e^{2\pi i(3/8)} &= e^{3\pi i/4}, \\ e^{2\pi i(5/8)} &= e^{5\pi i/4}, & e^{2\pi i(3/4)} &= -i, & e^{2\pi i(7/8)} &= e^{7\pi i/4}. \end{aligned}$$

3.3 O algoritmo quântico de estimativa de fase

Com a exposição sobre os pormenores da transformada quântica de Fourier, constata-se que uma das principais propriedades dela é a sua periodicidade, que permite a decomposição de estados quânticos em uma base de frequências. Sendo assim, encontra-se essencial aplicabilidade disso em algoritmos de busca de períodos.

A estimativa de fase quântica (QPE, do inglês, *quantum phase estimative*) [69] é um procedimento central para determinados algoritmos quânticos, sobretudo como sub-rotina do algoritmo de Shor e também em circuitos variacionais [70], [71]. Basicamente, ela consiste em resolver um problema de autovalor para um operador unitário arbitrário U , autovetor $|u\rangle$ com autovalor associado $e^{2\pi i\phi_u}$,

$$U |u\rangle = e^{2\pi i \phi_u} |u\rangle, \quad (3.18)$$

onde ϕ_u é uma fase desconhecida a ser estimada. O circuito quântico desse algoritmo está na Figura (23).

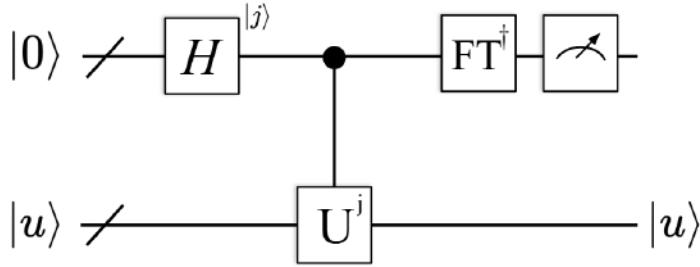


Figura 23 – Circuito quântico para o algoritmo da estimativa de fase quântica. Fonte: Autoria própria.

O primeiro registrador (com a barra denota um conjunto de linhas) é inicializado com $t = n + [\log(2 + 1/2\epsilon)]$ qubits em $|0\rangle$, com ϵ sendo o erro máximo tolerável. O segundo registrador inicia no estado $|u\rangle$ com uma quantidade suficiente para performar a operação caixa-preta U . Com isso, o circuito quântico inicialmente é descrito como

$$|\Phi\rangle = |0\rangle |u\rangle. \quad (3.19)$$

Em seguida, ocorre a aplicação da transformação de Hadamard no primeiro registrador,

$$|\Phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle |u\rangle, \quad (3.20)$$

e também a porta controlada com alvo no segundo registrador, considerando a equação (3.18), possibilita escrever o estado final como

$$|\Phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i j \phi_u} |j\rangle |u\rangle. \quad (3.21)$$

Consequentemente, o segundo estágio da estimativa é a aplicação da transformada quântica inversa de Fourier no primeiro registrador, resultando em

$$|\Phi\rangle = |\tilde{\phi}_u\rangle |u\rangle, \quad (3.22)$$

onde $|\tilde{\phi}_u\rangle$ é associado ao autovalor $\tilde{\phi}_u$ após a medição, que devolve uma boa estimativa para a fase inicialmente desconhecida ϕ_u .

O algoritmo de Shor revolucionou a computação quântica ao demonstrar que problemas intratáveis classicamente, como a fatoração de inteiros e o logaritmo discreto, podem ser resolvidos eficientemente com os computadores quânticos. Ele é elegantemente composto por duas sub-rotinas: uma clássica e uma quântica. A parte clássica é responsável por reduzir o problema de fatoração ao problema de busca de períodos de uma função modular [17], além de ser encarregada do pós-processamento. A sub-rotina quântica foca em estimar esse período com o uso do algoritmo QPE, sinalizando o papel indispensável da transformada quântica inversa de Fourier.

Sintetizando, a transformação do problema de fatoração em busca de período inicia-se na escolha de um número inteiro aleatório a , compreendido no intervalo $1 < a < N$, e com $\text{mdc}(a < N) = 1$ (caso contrário, o algoritmo já encontrou um fator não trivial de N e é encerrado). Com isso, define-se a função modular

$$f(x) = a^x \mod N, \quad (3.23)$$

cujo período r deve ser o menor inteiro positivo tal que $a^r \equiv 1 \mod N$.

Agora, retornando ao algoritmo de estimativa de fase, o primeiro registro é iniciado com $t = O(n \log N)$ qubits (para precisão), enquanto que o segundo armazenará a função $f(x)$. Resumindo, o estado que descreve o circuito agora é

$$|\Phi\rangle = |0\rangle^{\otimes t} |0\rangle. \quad (3.24)$$

Como anteriormente explicado, prossegue-se para aplicar a transformação de superposição $H^{\otimes t}$ no primeiro registro e também a operação controlada U no segundo,

$$|\Phi\rangle = \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle |0\rangle \rightarrow |\Phi\rangle = \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle |a^x \mod N\rangle. \quad (3.25)$$

Nesse momento, o segundo registrador deve colapsar para o estado $|u\rangle$ com $f(x) = u$, resultando em

$$|\Phi\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle |u\rangle, \quad (3.26)$$

onde $m \approx 2^t/r$ e também o primeiro registro torna-se uma superposição periódica, com x_0 o menor valor para a função $f(x)$ e r o período desejado.

Logo, finalmente, aplica-se a iQFT no primeiro registro,

$$|\Phi\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i x_0 l / r} \left| l \cdot \frac{2^t}{r} \right\rangle, \quad (3.27)$$

transformando a periodicidade em picos de probabilidade correspondentes aos múltiplos de $2^t/r$. Ela decodifica as fases $e^{2\pi i(x_0+kr)/2^t}$ em estados da base computacional, concentrando as probabilidades em valores $|\tilde{\phi}\rangle$ onde $\tilde{\phi} \approx l \cdot 2^t/r$ após a medição [9].

Finalizando, após a medida do primeiro registrador que retorna a fase estimada, o pós-processamento clássico é encarregado de calcular os fatores não triviais de N com

$$\text{mdc}(a^r/2 \pm 1, N), \quad (3.28)$$

somente se r seja par e $a^{r/2} \not\equiv -1 \pmod{N}$. Caso contrário, o procedimento é repetido.

O ganho de complexidade computacional em comparação com os métodos clássicos é de ordem exponencial, possibilitando a fatoração de números primos grandes em tempo razoável. Consequentemente, ele é uma ameaça para a criptografia de chaves assimétricas RSA [72] e até mesmo para o protocolo de troca de chaves de Diffie–Hellman baseado em curvas elípticas [73].

Nesse capítulo, foi demonstrado que a transformada quântica de Fourier tem capacidade de decompor estados quânticos em uma base de frequências, possibilitando o emprego de algoritmos como o de estimativa de fase, que auxilia na resolução de problemas classicamente intratáveis. No entanto, a implementação prática desses algoritmos enfrenta desafios significativos, como a decoerência e o controle preciso de portas quânticas de fase. Diante disso, no próximo capítulo, será abordada a proposta de um circuito óptico experimental que reproduz a transformada quântica de Fourier para três qubits codificados nos graus de liberdade da luz, no objetivo de conceber uma implementação viável e compacta em sistemas ópticos clássicos.

4 Proposta de circuito óptico de estados tri-partites para a QFT

Na procura por arquitetura de computadores quânticos escaláveis e tolerantes a falhas, os computadores fotônicos são uma das alternativas mais promissoras [74], [75]. Naturalmente, diante disso, outras propostas de circuito óptico para a transformada quântica de Fourier já foram desenvolvidas no ínicio desse século [76], dependendo apenas do caminho como grau de liberdade da luz. Expandindo esses horizontes, alguns produtos dos computadores quânticos canadenses da Xanadu [77], [78], permitem a manipulação de circuitos experimentais que usam a polarização e o caminho como graus de liberdade [79].

Entretanto, na segunda metade da década passada, foi proposto um circuito experimental, com feixes luminosos clássicos, que reproduz o protocolo do teleporte quântico com os três graus de liberdade da luz [15]. Portanto, com essa alternativa de codificação da informação nos modos transversos, a discussão volta-se para uma explicação detalhada do circuito óptico proposto no presente trabalho.

4.1 Circuito óptico com os graus de liberdade da luz: polarização, modos de Hermite-Gauss e o caminho

Embora pode-se imaginar diferentes configurações para codificar a informação nos graus de liberdade da luz, com a restrição de que o estado inicial seja preparado em uma única entrada do feixe luminoso, o desafio de reproduzir experimentalmente as portas controladas de fase deve ser superado. Então, seja cada grau de liberdade na base horizontal e vertical, respectivamente, dado por: $\{\psi_h, \psi_v\}$ para os modos transversos de *Hermite-Gauss*, $\{\hat{e}_H, \hat{e}_V\}$ para a polarização e $\{\chi_0, \chi_1\}$ para a direção de propagação. Com isso,

$$\mathcal{W} = \{\hat{e}_H, \hat{e}_V\} \otimes \{\psi_h, \psi_v\} \otimes \{\chi_0, \chi_1\} \quad (4.1)$$

será a ordem de codificação dos graus de liberdade no circuito óptico. A Figura 24 explicita a correspondência diretamente.

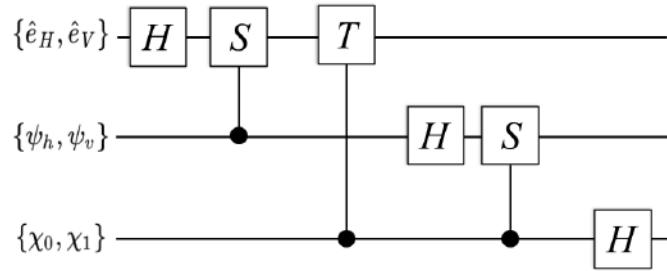


Figura 24 – Ordem de codificação dos graus de liberdade. Fonte: Autoria própria.

O primeiro qbit é codificado na polarização da luz por conveniência de realização experimental, dado que esse sofre duas transformações de fase que podem ser facilmente reproduzidas por meio de placas de onda. Um desenho do circuito óptico da QFT está na Figura 25 e demonstra a praticabilidade experimental.

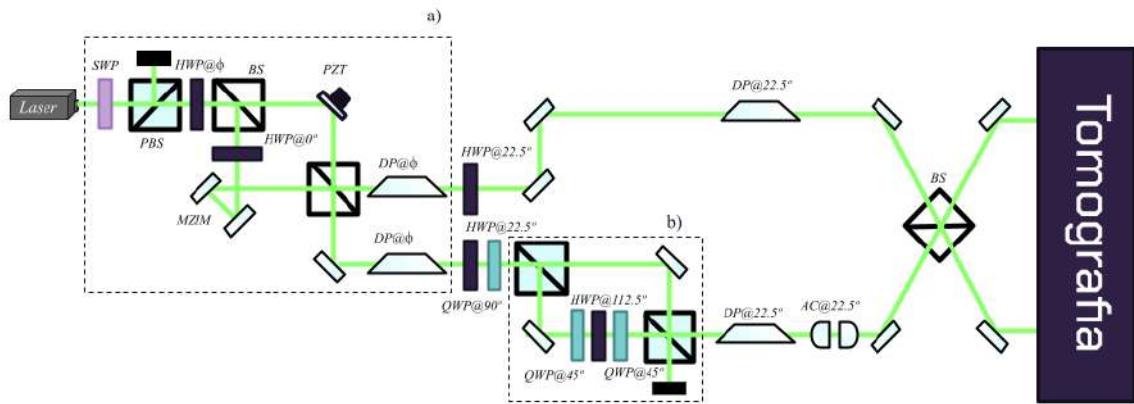


Figura 25 – Proposta de circuito óptico da Transformada Quântica de Fourier usando os graus de liberdade da luz. Em a) está a etapa de preparação do estado de entrada. Em b) está destacado o uso de portas de fase geométricas na polarização da luz. Fonte: Autoria própria.

O circuito está dividido em três etapas: a preparação do estado inicial, a transformada quântica de Fourier e a tomografia.

Na primeira etapa, o modo transverso HG_{10} (ou HG_{01}) é preparado por intermédio de uma *SWP* e um *PBS*. Além disso, para ajuste da polarização inicial desejada, coloca-se uma *HWP* em determinado ângulo ϕ . Logo, como os graus de liberdade que

desempenharão o papel de controle das portas de fase, os modos transversos e o caminho, o interferômetro que deve ser realizado configura um *transverse-mode beam splitter* (TBS) [80]. É um aparato semelhante ao interferômetro de Mach-Zehnder, com um *PZT* e um *MZIM* para ajuste de fases, além de uma *HWP@0°* posicionada em um dos braços, que irá distribuir os modos entre os caminhos. Após isso, para ajustes dos modos de Hermite-Gauss de entrada, posiciona-se um prisma de Dove em cada caminho, que deve ser rotacionado em ângulo ϕ , a depender do modo transverso desejado. Esse processo está detalhado na Figura (26).

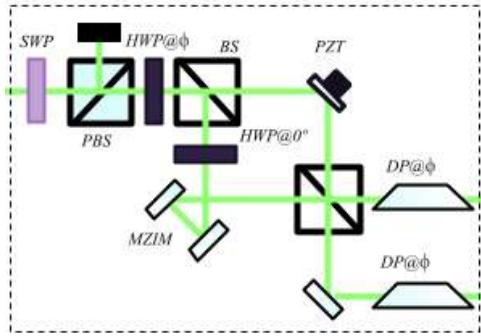


Figura 26 – Preparação do estado tripartite inicial no circuito óptico proposto para a QFT.
Fonte: Autoria própria.

Ao visualizar o desenho, é evidente a possibilidade de reproduzir os estados da base computacional com os graus de liberdade da luz. Mas também é possível reproduzir estados maximamente emaranhados posicionando uma placa de meia onda *HWP@22.5°* antes do TBS, que será responsável pela superposição nos modos transversos e na direção de propagação do feixe luminoso. O prisma de Dove ficará encarregado de ajustar os modos de Hermite-Gauss para reproduzir as equações (1.35) e (1.36).

O processo que simula experimentalmente a QFT é simplesmente uma associação direta dos operadores quânticos com as matrizes que representam os dispositivos ópticos do respectivo grau de liberdade. Portanto, esse será iniciado com a inserção da *HWP@22.5°* nos dois caminhos, como analogia direta à porta Hadamard na polarização. Logo, no caminho χ_1 , recordando das regras que definem as portas controladas (transformam apenas a base computacional $|1\rangle$), uma *HWP@90°* para desempenhar o papel da porta quântica S.

Nesse momento, contempla-se o uso de fases geométricas para o grau de liberdade da polarização, descrito pela Figura (27). A fase de Pancharatnam, como também é conhecida, ocorre quando um feixe polarizado percorre uma evolução cíclica em sua polarização, com contribuição geométrica $\theta/2$, sendo θ o ângulo sólido formado pelos estados de polarização ao longo da evolução (um triângulo geodésico) na esfera de Poincaré [52]. Na prática, é uma fase adquirida pelo feixe luminoso que incide em determinado conjunto de elementos birrefringentes, como as placas de onda. Uma configuração padrão

para reproduzir essas evoluções cíclicas é considerar uma placa de meia-onda, com ângulo a depender da rotação desejada, entre duas placas de quarto de onda à 45° .

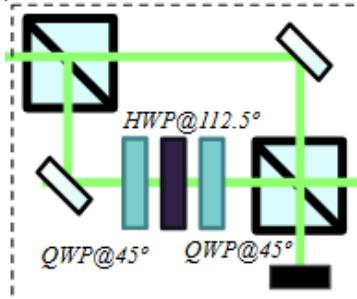


Figura 27 – Porta de fase geométrica para reprodução da porta quântica de fase T. Fonte: Autoria própria.

No caso presente, para reproduzir a porta controlada de fase T, considera-se uma $HWP@112.5^\circ$ posicionada entre duas $QWP@45^\circ$ (que resulta na rotação $R_z(\theta = \pi/4)$) no caminho da reflexão de um PBS , dado que a polarização vertical está associada à base computacional $|1\rangle$.

Agora, dando continuidade, com respeito às transformações no segundo qbit codificado, para a porta de superposição, em cada caminho coloca-se um $DP@22.5^\circ$ e então, uma montagem de duas lentes cilíndricas que formam um conversor astigmático $AC@22.5^\circ$. Finalmente, as direções de propagação do feixe luminoso são unificadas em um BS , a superposição para o caminho.

Ao final, serão realizadas as tomografias para intensidade e fase do feixe intenso. Experimentalmente, a obtenção do perfil de intensidade para o modo transverso resultante ocorre através de uma câmera CCD. Entretanto, as medidas de diferença de fase possuem limitações dependendo do resultado e, portanto, no âmbito do experimento, somente as que podem ser visualizadas por meio da interferência provocada por um feixe luminoso de referência serão coletadas.

4.2 Simulação computacional

Em primeiro lugar, é importante destacar que esse circuito foi desenvolvido para performar em sistemas de feixes luminosos clássicos. Com isso, a simulação computacional foi desenvolvida com base no formalismo de Jones para modelagem dos dispositivos ópticos análogos às portas quânticas. Todos os códigos foram desenvolvidos na linguagem de programação *python*, principalmente pela disponibilidade de conteúdo *open-source*, com uso extensivo das bibliotecas *Qutip* [81] e *LightPipes* [82], para orientação à objetos e auxílio na produção de visualizações gráficas.

O objetivo principal do código é a reconstrução da matriz 3.16 para $n = 3$ qubits, por intermédio da verificação da coincidência dos resultados dessa com o previsto pela literatura.

Além de todos os estados da base computacional, o circuito foi também simulado para os estados maximamente emaranhados. Com a ordenação escolhida para codificar a informação nos graus de liberdade, é imediata a classificação dos resultados correspondentes ao caminho χ_0 e χ_1 . Essa associação está exposta na Tabela 5.

Caminho χ_0	Caminho χ_1
$ 000\rangle$	$ 001\rangle$
$ 010\rangle$	$ 011\rangle$
$ 100\rangle$	$ 101\rangle$
$ 110\rangle$	$ 111\rangle$

Tabela 5 – Tabela de correspondência entre resultados numéricos e a direção de propagação do circuito. Fonte: Autoria própria.

Mesmo com a analogia entre os sistemas clássico e quântico, deve-se apontar que o código é estritamente exclusivo para circuitos com feixes luminosos, dado que é sustentado essencialmente pela formulação de Jones. Um estudo semelhante para computadores fotônicos depende fortemente da simulação dos fôtons e outras considerações tanto computacionais, quanto experimentais.

5 Resultados

Por fim, a discussão é direcionada aos resultados numéricos da simulação computacional. O principal resultado obtido é a matriz apresentada pela equação (3.16) para $n = 3$ qubits, exposta na equação (5.1), onde cada coluna é constituída por um vetor da base computacional transformado.

$$\text{QFT} = \begin{pmatrix} 0.354 & 0.354 & 0.354 & 0.354 & 0.354 & 0.354 & 0.354 & 0.354 \\ 0.354 & 0.25 + 0.25i & 0.354i & -0.25 + 0.25i & -0.354 & -0.25 - 0.25i & -0.354i & 0.25 - 0.25i \\ 0.354 & 0.354i & -0.354 & -0.354i & 0.354 & 0.354i & -0.354 & -0.354i \\ 0.354 & -0.25 + 0.25i & -0.354i & 0.25 + 0.25i & -0.354 & 0.25 - 0.25i & 0.354i & -0.25 - 0.25i \\ 0.354 & -0.354 & 0.354 & -0.354 & 0.354 & -0.354 & 0.354 & -0.354 \\ 0.354 & -0.25 - 0.25i & 0.354i & 0.25 - 0.25i & -0.354 & 0.25 + 0.25i & -0.354i & -0.25 + 0.25i \\ 0.354 & -0.354i & -0.354 & 0.354i & 0.354 & -0.354i & -0.354 & 0.354i \\ 0.354 & 0.25 - 0.25i & -0.354i & -0.25 - 0.25i & -0.354 & -0.25 + 0.25i & 0.354i & 0.25 + 0.25i \end{pmatrix} \quad (5.1)$$

Após o circuito óptico, os estados transformados adquirem fatores de fase dependentes da representação binária referente ao seu índice na base computacional, contemplando os valores expostos na Tabela 4. Então, ao decompor esses em relação à base, cada termo carrega uma fase proporcional ao fator de fase binário, ou simplificando, fatores de fase que são múltiplos do fator binário. Portanto, para comprovar as transformações de fase decorrentes da óptica, considera-se uma comparação com os cálculos teóricos, advindos da substituição direta na equação (3.15).

Com isso, para a análise a seguir, destacam-se as bases computacionais: $|000\rangle$, $|010\rangle$, $|101\rangle$ e $|111\rangle$. Essa decisão é definida com o objetivo de também analisar os resultados para os estados tripartites maximamente emaranhados.

5.1 Resultados da base computacional $|000\rangle$

O primeiro estado a ser analisado é a base computacional $|000\rangle$. Como definido na concepção do circuito óptico, o estado inicial estará no caminho χ_0 , com polarização horizontal $|H\rangle$ e associado aos modos de Hermite-Gauss horizontais $|h\rangle$, configurando a codificação nos graus de liberdade $|000\rangle \equiv |Hhu\rangle$.

É imediata a observação de que esse estado sofrerá somente as transformações de Hadamard, resultando na superposição da base, como demonstram as equações para os vetores coluna (5.2).

$$|000\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{QFT } |000\rangle = \begin{pmatrix} 0.354 \\ 0.354 \\ 0.354 \\ 0.354 \\ 0.354 \\ 0.354 \\ 0.354 \\ 0.354 \end{pmatrix} \quad (5.2)$$

A Figura 28 mostra o perfil transverso de intensidade para o antes e o depois referente ao estado em análise. O perfil transverso que caracteriza o estado inicial (acima) é somente o modo $H_{1,0}$ no caminho χ_0 . Após a transformação do circuito óptico, a intensidade será distribuída para ambos os caminhos e assume um perfil coerente com a superposição imposta, considerando a base dos modos transversos de Hermite-Gauss. Contudo, apesar das aparências, não se deve associar esse perfil transverso aos vórtices ópticos $L_0^{\pm 1}$, dado que as informações de fase diferem.

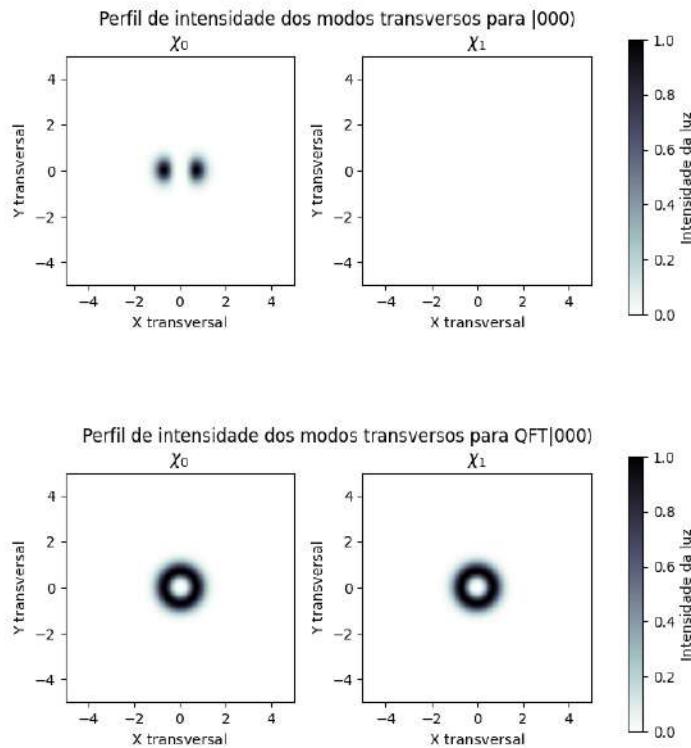


Figura 28 – O perfil de intensidade normalizado para o estado $|000\rangle$ está acima. Abaixo, encontra-se o estado transformado $\text{QFT}|000\rangle$. Imagens obtidas com *python*. Fonte: Autoria própria.

Os vetores na esfera de Bloch na Figura 29 mostram a transformação sofrida em cada qbit codificado. Inicialmente, na imagem acima, todos os vetores são iguais

em amplitude, direção e sentido, apontando para o estado base $|0\rangle$. Abaixo, após a transformação, todos eles estão na superposição $|+\rangle$.

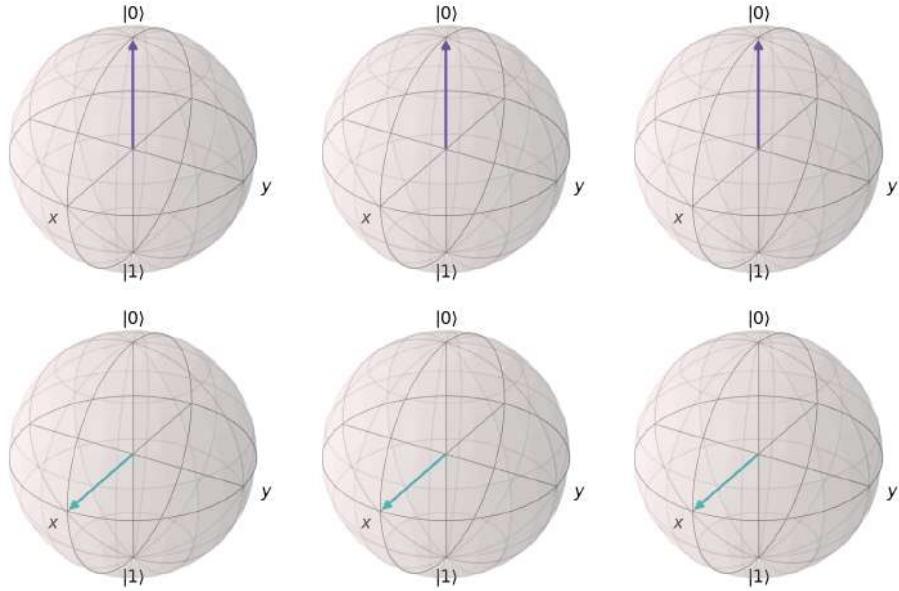


Figura 29 – Vetores na esfera de Bloch para o estado inicial $|000\rangle$ (acima) e os resultados QFT $|000\rangle$ (abaixo). Da esquerda para a direita, tem-se os qbits codificados $|H\rangle$, $|h\rangle$ e $|u\rangle$. Imagens obtidas com *python* e a biblioteca *qutip*. Fonte: Autoria própria.

Nesse momento, considera-se a equação teórica que explicita os fatores de fase para esse estado,

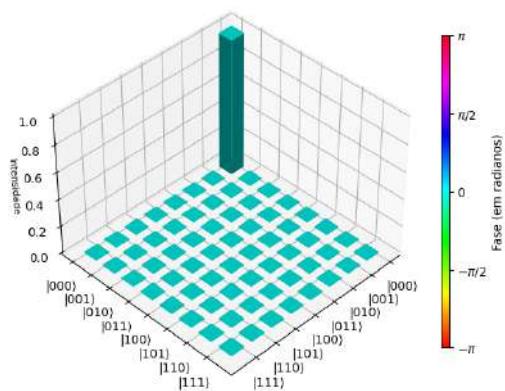
$$\text{QFT } |000\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle), \quad (5.3)$$

constatando imediatamente que são todos nulos. E também, a matriz densidade (5.4), que por definição tem as informações de amplitude e fase simultaneamente,

$$\rho_{|000\rangle} = \begin{pmatrix} 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \\ 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 & 0.125 \end{pmatrix}. \quad (5.4)$$

Logo, normalizando essa matriz, é possível visualizar a distribuição de amplitude e fase através dos histogramas na Figura 30. A altura das barras refere-se à intensidade da

luz (amplitude), enquanto as cores indicam as fases associadas. Nota-se imediatamente que, além da intensidade ser equitativamente distribuída, isso também ocorre para as fases associadas que são nulas. São resultados condizentes com o previsto pela literatura, considerando o fator de fase binário e também, o comportamento intrínseco da superposição provocada no estado inicial.

Distribuição de amplitudes e fases do estado $|000\rangle$ 

Distribuição de amplitudes e fases do estado QFT|000>

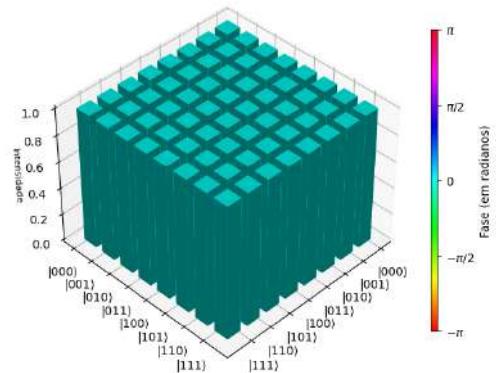


Figura 30 – Histograma das distribuições de intensidade e fase para os estados $|000\rangle$ (esquerda) e QFT $|000\rangle$ (direita). Imagem obtida com *python*. Fonte: Autoria própria.

5.2 Resultados da base computacional $|010\rangle$

Agora, o estado inicial em análise é codificado na polarização horizontal $|H\rangle$, modo transverso $|v\rangle$ e estará no caminho χ_0 , configurando-se em sua totalidade $|010\rangle \equiv |Hvu\rangle$.

A transformação do estado em análise está exposta em (5.5). Observe que os coeficientes da amplitude do estado transformado QFT $|010\rangle$ são idênticos ao caso anterior, QFT $|000\rangle$, e também, através da matriz dos resultados (5.1), que isso igualmente acontece para todas as bases computacionais codificadas no caminho χ_0 . Essencialmente, o que caracteriza cada unicamente, são os fatores de fase associados a cada coeficiente.

$$|010\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{QFT } |010\rangle = \begin{pmatrix} 0.354 \\ 0.354i \\ -0.354 \\ -0.354i \\ 0.354 \\ 0.354i \\ -0.354 \\ -0.354i \end{pmatrix} \quad (5.5)$$

Os perfis transversos da intensidade para entrada e saída, por sua vez, podem ser visualizados na Figura 31.

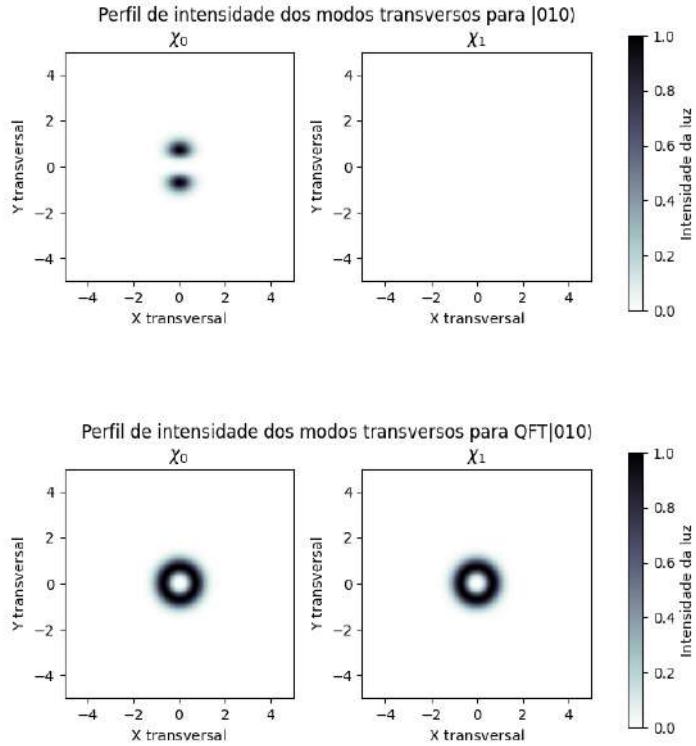


Figura 31 – Acima, está o perfil de intensidade para o estado inicial $|010\rangle$. Abaixo, está o estado transformado QFT $|010\rangle$. Imagens obtidas com *python*. Fonte: Autoria própria.

Acima, o perfil transverso de intensidade do estado inicial caracterizado pelo modo $H_{0,1}$ no caminho χ_0 . Abaixo, para o estado transformado e imediatamente, pode-se identificar a equivalência com o caso anterior, correspondendo à tendência para os estados codificados inicialmente nessa direção de propagação. Entretanto, ainda deve-se analisar as diferenças de fase que caracterizam o estado exclusivamente.

Inicialmente, essas diferenças podem ser observadas diretamente nos vetores das esferas de Bloch, estas expostas na Figura 32, que mostram as rotações dos vetores para essa configuração. Acima, os vetores apontam para seus respectivos estados iniciais. Abaixo, o primeiro qbit é superposto e sofre rotação equivalente a transformação de fase $\theta = \pi/4$. O segundo é rotacionado em relação a transformação $\theta = \pi/2$ e o último, colocado na superposição $|+\rangle$.

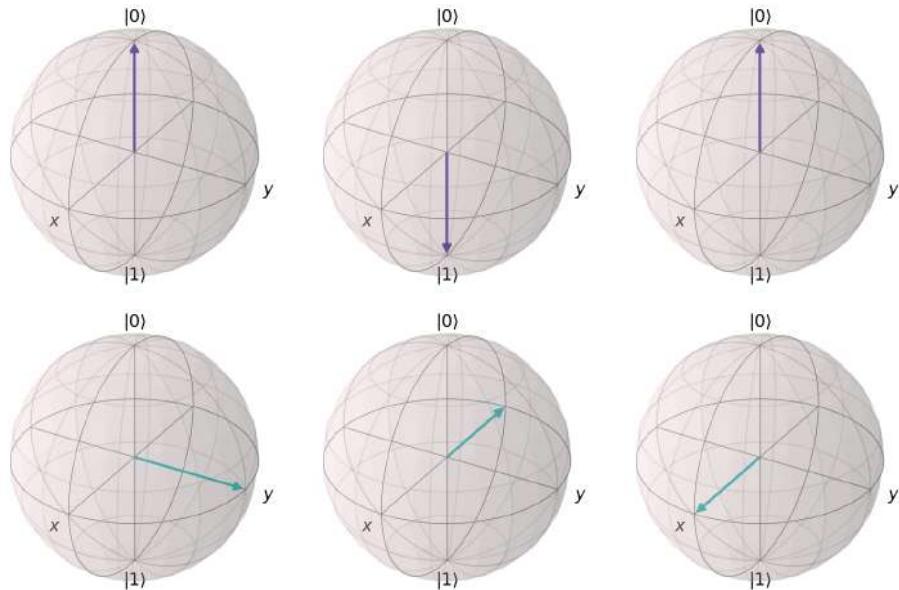


Figura 32 – Vetores na esfera de Bloch, da esquerda para a direita, $|H\rangle$, $|v\rangle$ e $|u\rangle$, para o estado inicial $|010\rangle$ (acima) e final QFT $|010\rangle$ (abaixo). Imagens obtidas com *python*. Fonte: Autoria própria.

Além disso, considerando a expansão dos fatores de fase de acordo com a equação teórica,

$$\begin{aligned} \text{QFT } |010\rangle &= \frac{1}{\sqrt{8}} \left(|000\rangle + e^{i\frac{\pi}{2}} |001\rangle - |010\rangle - e^{i\frac{3\pi}{2}} |011\rangle \right. \\ &\quad \left. + |100\rangle + e^{i\frac{\pi}{2}} |101\rangle - |110\rangle - e^{i\frac{3\pi}{2}} |111\rangle \right), \end{aligned} \quad (5.6)$$

com as devidas simplificações quanto múltiplos do fator de fase binário i . Entretanto, normalizando a matriz densidade do estado transformado QFT $|010\rangle$,

$$\rho_{|010\rangle} = \begin{pmatrix} 0.125 & 0. - 0.125i & -0.125 & 0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 & 0. + 0.125i \\ 0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 & 0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 \\ -0.125 & 0. + 0.125i & 0.125 & -0. - 0.125i & -0.125 & 0. + 0.125i & 0.125 & -0. - 0.125i \\ 0. - 0.125i & -0.125 & -0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 & -0. + 0.125i & 0.125 \\ 0.125 & 0. - 0.125i & -0.125 & 0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 & 0. + 0.125i \\ 0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 & 0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 \\ -0.125 & 0. + 0.125i & 0.125 & -0. - 0.125i & -0.125 & 0. + 0.125i & 0.125 & -0. - 0.125i \\ 0. - 0.125i & -0.125 & -0. + 0.125i & 0.125 & 0. - 0.125i & -0.125 & -0. + 0.125i & 0.125 \end{pmatrix}, \quad (5.7)$$

deve-se considerar o equivalente desses fatores no intervalo de normalização $\{-\pi, \pi\}$, isto é,

$$\begin{aligned} \text{QFT } |010\rangle = \frac{1}{\sqrt{8}} & \left(|000\rangle + e^{i\frac{\pi}{2}} |001\rangle - |010\rangle - e^{-i\frac{\pi}{2}} |011\rangle \right. \\ & \left. + |100\rangle + e^{i\frac{\pi}{2}} |101\rangle - |110\rangle - e^{-i\frac{\pi}{2}} |111\rangle \right). \end{aligned} \quad (5.8)$$

Com isso, o histograma da Figura 33 evidencia as distribuições de amplitude e fase do estado inicial (esquerda) e do estado transformado (direita) nas bases computacionais.

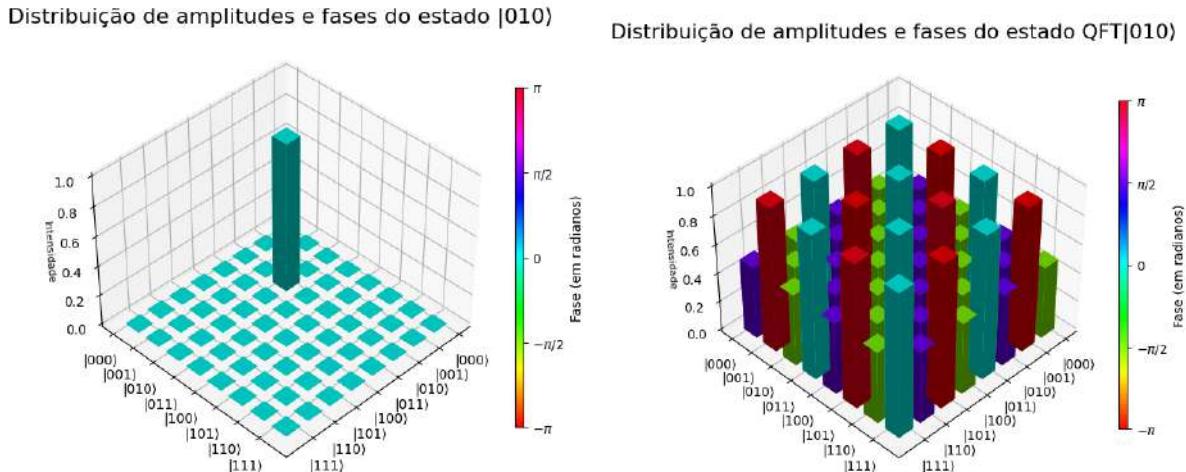


Figura 33 – Histograma das distribuições de intensidade e fase para os estados $|010\rangle$ (esquerda) e $\text{QFT}|010\rangle$ (direita). Imagem obtida com *python*. Fonte: Autoria própria.

Em primeiro lugar, observa-se que os coeficientes associados com as menores intensidades apresentam predominantemente fases próximas de $\theta = \pm\pi/2$, enquanto os de maior intensidade estão contidos próximos de $\theta = 0$ e $\theta = \pm\pi$, por consequência da normalização da amplitude. No geral, é possível constatar a prevalência dos múltiplos do fator binário de acordo com o previsto teoricamente.

5.3 Resultados da base computacional $|101\rangle$

Nesse caso, a base computacional está codificada na polarização vertical $|V\rangle$, nos modos transversos $|h\rangle$ e no caminho χ_1 , configurando o estado composto inicial $|101\rangle \equiv |Vhd\rangle$. A transformação deste provocada após o circuito óptico é diretamente observável em (5.9). Dessa vez, a transformação sugere um padrão de interferência.

$$|101\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{QFT } |101\rangle = \begin{pmatrix} 0.354 \\ -0.250 + 0.250i \\ -0.354i \\ 0.250 + 0.250i \\ -0.354 \\ 0.250 - 0.250i \\ 0.354i \\ -0.250 - 0.250i \end{pmatrix} \quad (5.9)$$

O perfil transverso de intensidade para a entrada e a saída dessa configuração está exposto na Figura 34.

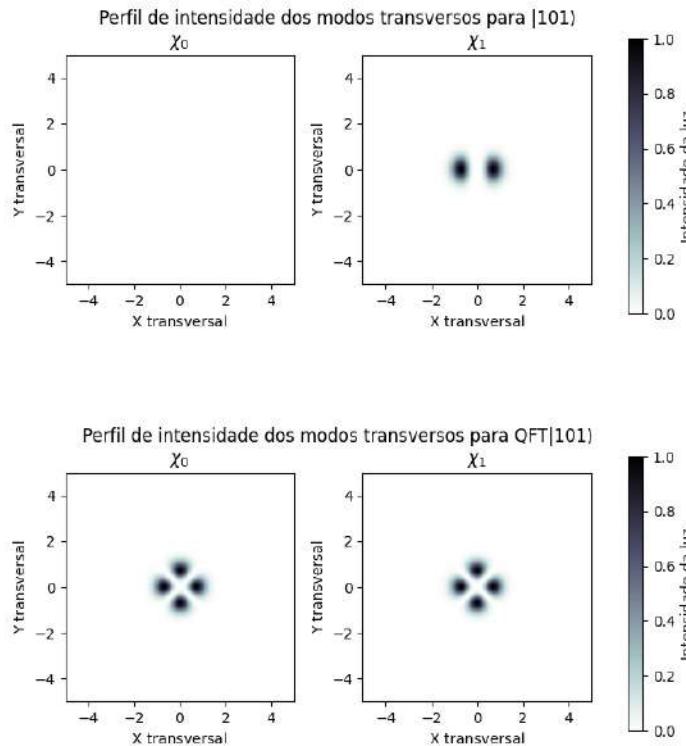


Figura 34 – Perfil de intensidade e fase normalizados da entrada $|101\rangle$ (acima) e QFT $|101\rangle$ (abaixo). Imagens obtidas com *python*. Fonte: Autoria própria.

Para o estado inicial (acima), tem-se somente um modo $H_{1,0}$ no caminho χ_1 . Para a saída (abaixo), as transformações de fase controlada do circuito modificam a

distribuição do perfil de modo que há quatro máximos de intensidade ao redor de uma região central nula, como se dois modos de Hermite-Gauss rotacionados $H_{0,1}^{\pm\pi/4}$ interferissem em um vórtice óptico. Obviamente, esse estado possui relações de fase específicas a serem analisadas.

Em primeira instância, as rotações provocadas pelas transformações de fase podem ser visualizadas diretamente nas esferas de Bloch, expostas na Figura 35.

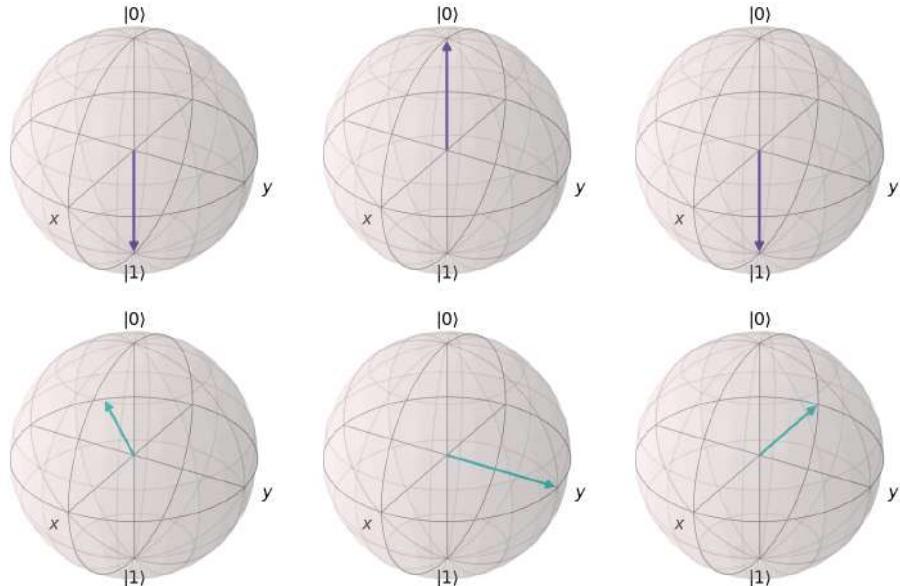


Figura 35 – Vetores na esfera de Bloch, da esquerda para a direita, $|H\rangle$, $|v\rangle$ e $|u\rangle$, para o estado inicial $|101\rangle$ (acima) e final QFT $|101\rangle$ (abaixo). Imagens obtidas com *python*. Fonte: Autoria própria.

Acima, está disposta a ordenação dos vetores do estado inicial. Abaixo, os qbits rotacionados após o circuito óptico. Pensando na sequência de portas controladas envolvidas, é imediato caracterizar que o primeiro qbit é colocado no estado de superposição $|-\rangle$ e então, rotaciona de acordo com a transformação de fase $\theta = \pi/4$. O segundo, além de ser alterado para o estado de superposição $|+\rangle$, também é deslocado em $\theta = \pi/2$. Naturalmente, o último está na superposição $|-\rangle$.

Agora, consideramos a matriz densidade para o estado transformado,

$$\rho_{|101\rangle} = \begin{pmatrix} 0.125 + 0.j & -0.0884 + 0.0884j & 0. - 0.125j & 0.0884 + 0.0884j & -0.125 + 0.j & 0.0884 - 0.0884j & 0. + 0.125j & -0.0884 - 0.0884j \\ -0.0884 - 0.0884j & 0.125 + 0.j & -0.0884 + 0.0884j & 0. - 0.125j & 0.0884 + 0.0884j & -0.125 + 0.j & 0.0884 - 0.0884j & 0. + 0.125j \\ 0. + 0.125j & -0.0884 - 0.0884j & 0.125 + 0.j & -0.0884 + 0.0884j & 0. - 0.125j & 0.0884 + 0.0884j & -0.125 + 0.j & 0.0884 - 0.0884j \\ 0.0884 - 0.0884j & 0. + 0.125j & -0.0884 - 0.0884j & 0.125 + 0.j & -0.0884 + 0.0884j & 0. - 0.125j & 0.0884 + 0.0884j & -0.125 + 0.j \\ -0.125 + 0.j & 0.0884 - 0.0884j & 0. + 0.125j & -0.0884 - 0.0884j & 0.125 + 0.j & -0.0884 + 0.0884j & -0. - 0.125j & 0.0884 + 0.0884j \\ 0.0884 + 0.0884j & -0.125 + 0.j & 0.0884 - 0.0884j & 0. + 0.125j & -0.0884 - 0.0884j & 0.125 + 0.j & -0.0884 + 0.0884j & 0. - 0.125j \\ 0. - 0.125j & 0.0884 + 0.0884j & -0.125 + 0.j & 0.0884 - 0.0884j & -0. + 0.125j & -0.0884 - 0.0884j & 0.125 + 0.j & -0.0884 + 0.0884j \\ -0.0884 + 0.0884j & 0. - 0.125j & 0.0884 + 0.0884j & -0.125 + 0.j & 0.0884 - 0.0884j & 0. + 0.125j & -0.0884 - 0.0884j & 0.125 + 0.j \end{pmatrix}, \quad (5.10)$$

que também terá sua amplitude e intervalo de fase normalizados. Sendo assim, considera-se a expansão dos fatores de fase compreendida no intervalo $\{-\pi, \pi\}$ é

$$\begin{aligned} \text{QFT } |101\rangle = \frac{1}{\sqrt{8}} & \left(|000\rangle + e^{-i\frac{3\pi}{4}} |001\rangle + e^{i\frac{\pi}{2}} |010\rangle + e^{-i\frac{\pi}{4}} |011\rangle \right. \\ & \left. - |100\rangle + e^{i\frac{\pi}{4}} |101\rangle + e^{-i\frac{\pi}{2}} |110\rangle + e^{i\frac{3\pi}{4}} |111\rangle \right). \end{aligned} \quad (5.11)$$

Com isso, as distribuições de amplitude e fases para os estados inicial e transformado estão exibidas na Figura 36. Ao lado esquerdo, está disposto o estado inicial $|101\rangle$. Ao direito, o estado QFT $|101\rangle$.

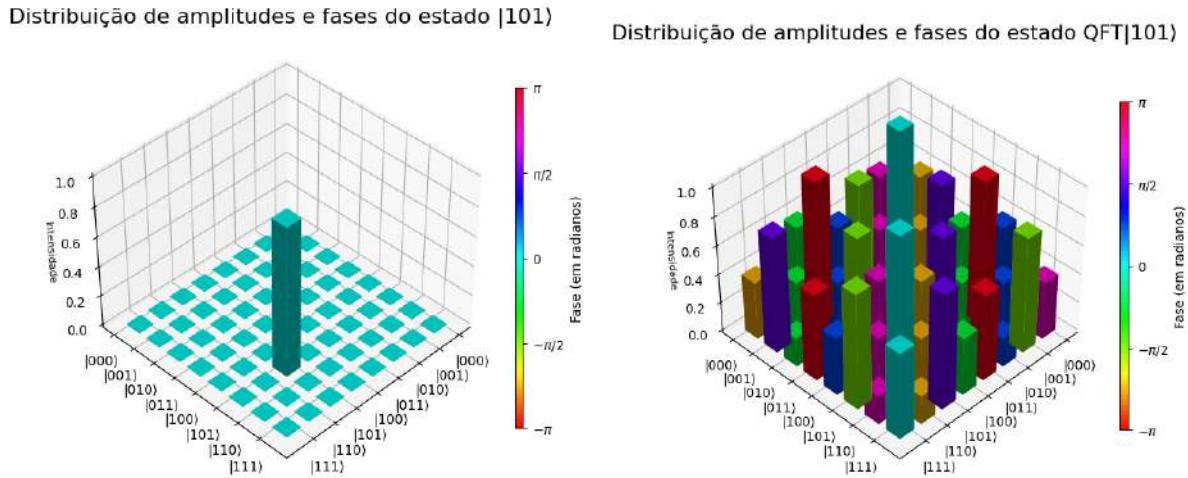


Figura 36 – Histograma das distribuições de intensidade e fase para os estados $|101\rangle$ (esquerda) e QFT $|101\rangle$ (direita). Imagem obtida com *python*. Fonte: Autoria própria.

Para os estados codificados no caminho χ_1 , os fatores de fase binário são uma exponencial complexa, como mostra a Tabela 4. No presente caso, as fases serão múltiplos do fator binário $5\pi i/4$. Ao observar no histograma da direita, imediatamente constata-se a ocorrência dos fatores múltiplos $\theta = \pm 3\pi/4$, $\theta = \pm\pi/2$ e $\theta = \pm\pi/4$ na normalização da matriz densidade. Portanto, os resultados coincidem com a previsão teórica.

5.4 Resultados da base computacional $|111\rangle$

Finalmente, a análise dirige-se ao último estado da base computacional. Ele está codificado na polarização vertical $|V\rangle$, no modo transverso $|v\rangle$ e no caminho χ_1 , caracterizando o estado $|111\rangle \equiv |Vvd\rangle$.

A transformação desse estado está explícita em (5.12). Com isso, pode-se constatar que as amplitudes de todas as bases computacionais em $|d\rangle$ são iguais.

$$|111\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rightarrow \text{QFT } |111\rangle = \begin{pmatrix} 0.354 \\ (0.250 - 0.250j) \\ -0.354j \\ (-0.250 - 0.250j) \\ -0.354 \\ (-0.250 + 0.250j) \\ 0.354j \\ (0.250 + 0.250j) \end{pmatrix} \quad (5.12)$$

O perfil de intensidade para os modos transversos dessa entrada está representado na Figura 37.

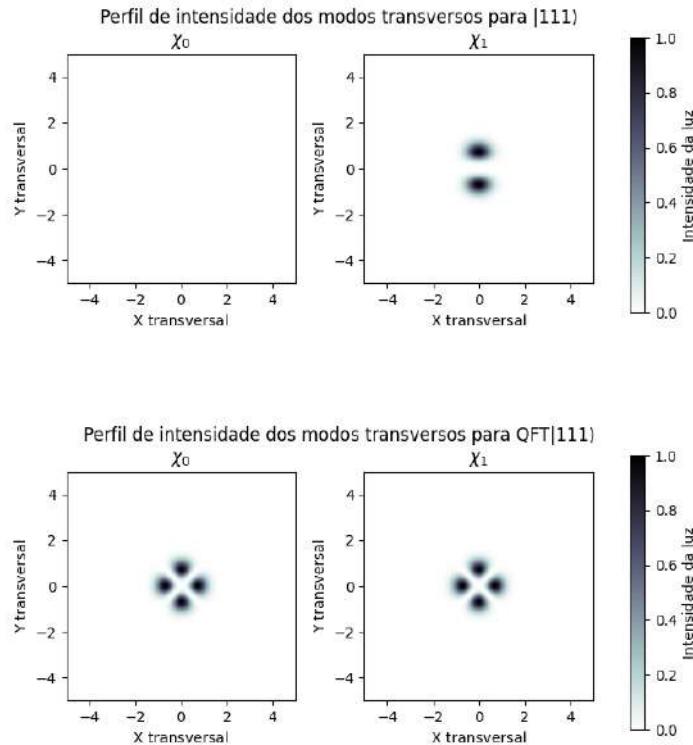


Figura 37 – Perfil de intensidade e fase normalizados da entrada $|111\rangle$ (acima) e $\text{QFT}|111\rangle$ (abaixo). Imagens obtidas com *python*. Fonte: Autoria própria.

Para o estado inicial, há o perfil de intensidade modo transverso $H_{0,1}$ no caminho χ_1 . A distribuição de intensidade para o estado transformado repete o perfil transverso do

estado analisado anteriormente, $|101\rangle$, sugerindo um padrão para os estados codificados no caminho χ_1 , assim como há para a outra direção de propagação do feixe luminoso. Novamente, apesar dessa recorrência, há transformações de fase específicas que devem ser analisadas.

As fases obtidas após o circuito estão contempladas pelas rotações dos vetores na esfera de Bloch, exibida na Figura 38.

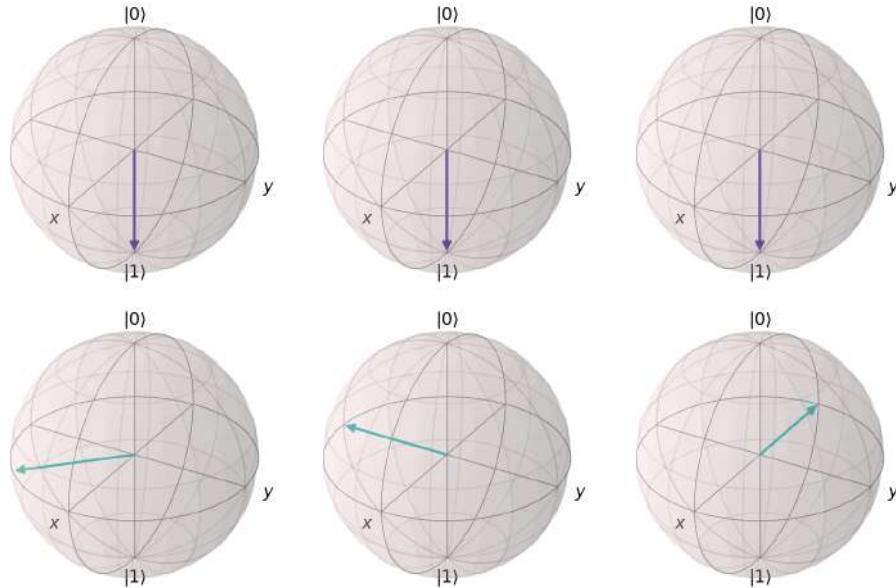


Figura 38 – Vetores na esfera de Bloch, da esquerda para a direita, $|H\rangle$, $|v\rangle$ e $|u\rangle$, para o estado inicial $|111\rangle$ (acima) e final QFT $|111\rangle$ (abaixo). Imagens obtidas com *python*. Fonte: Autoria própria.

Acima, está o estado inicial ($|111\rangle$). Abaixo, o estado transformado (QFT $|111\rangle$). Em termos de rotações provocadas por transformações de fase, essa é a base mais completa, dado que realiza todas as operações controladas. O primeiro qbit após a superposição $|-\rangle$, é deslocado em ângulos $\theta = \pi/2$ e $\theta = \pi/4$. O segundo, igualmente superposto, em $\theta = \pi/2$ e o último estado, como sempre, é apenas superposto.

Logo, seja a matriz densidade do estado QFT $|111\rangle$,

$$\rho_{|111\rangle} = \begin{pmatrix} 0.125 + 0.j & 0.0884 + 0.0884j & 0. + 0.125j & -0.0884 + 0.0884j & -0.125 - 0.j & -0.0884 - 0.0884j & 0. - 0.125j & 0.0884 - 0.0884j \\ 0.0884 - 0.0884j & 0.125 + 0.j & 0.0884 + 0.0884j & 0. + 0.125j & -0.0884 + 0.0884j & -0.125 + 0.j & -0.0884 - 0.0884j & 0. - 0.125j \\ 0. - 0.125j & 0.0884 - 0.0884j & 0.125 + 0.j & 0.0884 + 0.0884j & -0. + 0.125j & -0.0884 + 0.0884j & -0.125 - 0.j & -0.0884 - 0.0884j \\ -0.0884 - 0.0884j & 0. - 0.125j & 0.0884 - 0.0884j & 0.125 + 0.j & 0.0884 + 0.0884j & -0. + 0.125j & -0.0884 + 0.0884j & -0.125 + 0.j \\ -0.125 + 0.j & -0.0884 - 0.0884j & -0. - 0.125j & 0.0884 - 0.0884j & 0.125 + 0.j & 0.0884 + 0.0884j & 0. + 0.125j & -0.0884 + 0.0884j \\ -0.0884 + 0.0884j & -0.125 + 0.j & -0.0884 - 0.0884j & -0. - 0.125j & 0.0884 - 0.0884j & 0.125 + 0.j & 0.0884 + 0.0884j & 0. + 0.125j \\ 0. + 0.125j & -0.0884 + 0.0884j & -0.125 + 0.j & -0.0884 - 0.0884j & 0. - 0.125j & 0.0884 - 0.0884j & 0.125 + 0.j & 0.0884 + 0.0884j \\ 0.0884 + 0.0884j & 0. + 0.125j & -0.0884 + 0.0884j & -0.125 + 0.j & -0.0884 - 0.0884j & 0. - 0.125j & 0.0884 - 0.0884j & 0.125 + 0.j \end{pmatrix}, \quad (5.13)$$

considerando a sua normalização, a expansão teórica dos fatores de fase é

$$\text{QFT } |111\rangle = \frac{1}{2} \left(|000\rangle + e^{-i\frac{\pi}{4}} |001\rangle + e^{-i\frac{\pi}{2}} |010\rangle + e^{-i\frac{3\pi}{4}} |011\rangle - |100\rangle + e^{i\frac{3\pi}{4}} |101\rangle + e^{i\frac{\pi}{2}} |110\rangle + e^{i\frac{\pi}{4}} |111\rangle \right). \quad (5.14)$$

A Figura 39 mostra a distribuição de fases e intensidade para os estados inicial (esquerda) e transformado (direita).

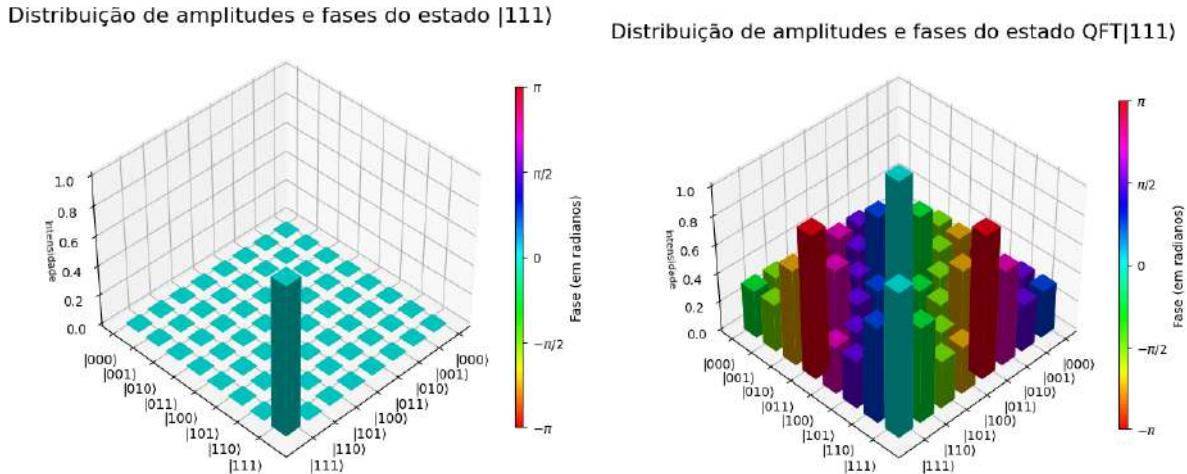


Figura 39 – Histograma tridimensional da tomografia dos estados $|111\rangle$ (esquerda) $\text{QFT}|111\rangle$ (direita). Imagens obtidas com *python*. Fonte: Autoria própria.

Seguindo a lógica progressiva dos múltiplos do fator de fase binário, nota-se imediatamente a ocorrência de mais fatores de fase, compreendidos em $\theta = \pm\pi/4$, $\theta = \pm\pi/2$ e $\theta = \pm3\pi/4$. Ao transicionar esses para o intervalo $\{0, 2\pi\}$, é direto que tratam-se de múltiplos do fator binário $7\pi/4$, condizendo com a teoria.

5.5 Resultados do estado maximamente emaranhado $|GHZ\rangle$

Agora, a análise concentra-se na descrição de um estado dependendo de duas bases computacionais já discutidas: o estado maximamente emaranhado. Escrevendo-o em termos dessas bases codificadas nos graus de liberdade da luz, o estado descrito na equação (1.35) é reescrito como

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|Hhu\rangle + |Vvd\rangle). \quad (5.15)$$

A transformação desse estado $|GHZ\rangle$ para QFT $|GHZ\rangle$ está exposta em (5.16).

$$|GHZ\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rightarrow \text{QFT } |GHZ\rangle = \begin{pmatrix} 0.5 \\ (0.354 - 0.146j) \\ (0.25 - 0.25j) \\ (0.073 - 0.177j) \\ 0 \\ (0.073 + 0.177j) \\ (0.25 + 0.25j) \\ (0.354 + 0.146j) \end{pmatrix} \quad (5.16)$$

Os perfis transversos de intensidade desse estado inicial (acima) e da transformação provocada pela QFT (abaixo) estão ilustrados na Figura 40.

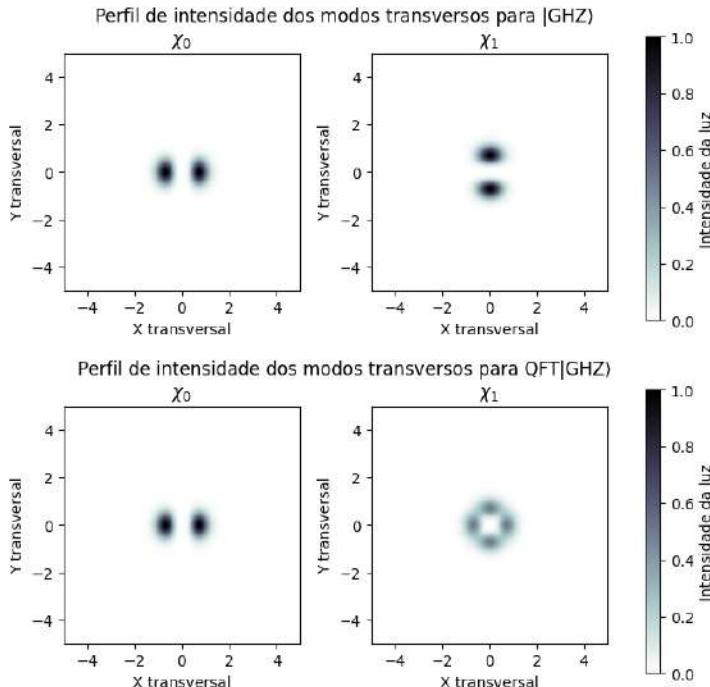


Figura 40 – Perfil de intensidade e fase normalizados da entrada $|GHZ\rangle$ (acima) e $\text{QFT}|GHZ\rangle$ (abaixo). Imagens obtidas com *python*. Fonte: Autoria própria.

O estado inicial é caracterizado por um modo $H_{1,0}$ no caminho χ_0 e por outro

$H_{0,1}$ no caminho χ_1 . Após percorrer o circuito óptico, o feixe luminoso ao incidir no divisor de feixes interfere de modo que a distribuição de intensidade no caminho χ_0 é preservada como um modo transverso $H_{0,1}$ e no caminho χ_1 , os dois modos aparecem menos intensos.

Sobre os coeficientes de fase, deve-se recordar a nulidade dos fatores para o estado $|000\rangle$. Portanto, os múltiplos serão relativos ao fator binário do estado $|111\rangle$, isto é,

$$\text{QFT } |GHZ\rangle = \frac{1}{2} \left(|000\rangle + e^{-i\frac{\pi}{4}} |001\rangle + e^{-i\frac{\pi}{2}} |010\rangle + e^{-i\frac{3\pi}{4}} |011\rangle - |100\rangle + e^{i\frac{3\pi}{4}} |101\rangle + e^{i\frac{\pi}{2}} |110\rangle + e^{i\frac{\pi}{4}} |111\rangle \right). \quad (5.17)$$

A matriz densidade da equação (5.18) mostra um padrão de distribuição de amplitudes característico do emaranhamento.

$$\rho_{|GHZ\rangle} = \begin{pmatrix} 0.2500 + 0.0000j & 0.2134 - 0.0884j & 0.1250 - 0.1250j & 0.0366 - 0.0884j & 0 & 0.0366 + 0.0884j & 0.1250 + 0.1250j & 0.2134 + 0.0884j \\ 0.2134 + 0.0884j & 0.2134 + 0.0000j & 0.1509 - 0.0625j & 0.0625 - 0.0625j & 0 & -0.0000 + 0.0884j & 0.0625 + 0.1509j & 0.1509 + 0.1509j \\ 0.1250 + 0.1250j & 0.1509 + 0.0625j & 0.1250 + 0.0000j & 0.0625 - 0.0259j & 0 & -0.0259 + 0.0625j & 0.0000 + 0.1250j & 0.0625 + 0.1509j \\ 0.0366 + 0.0884j & 0.0625 + 0.0625j & 0.0625 + 0.0259j & 0.0366 + 0.0000j & 0 & -0.0259 + 0.0259j & -0.0259 + 0.0625j & -0.0000 + 0.0884j \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.0366 - 0.0884j & -0.0000 - 0.0884j & -0.0259 - 0.0625j & -0.0259 - 0.0259j & 0 & 0.0366 + 0.0000j & 0.0625 - 0.0259j & 0.0625 - 0.0625j \\ 0.1250 - 0.1250j & 0.0625 - 0.1509j & 0.0000 - 0.1250j & -0.0259 - 0.0625j & 0 & 0.0625 + 0.0259j & 0.1250 + 0.0000j & 0.1509 - 0.0625j \\ 0.2134 - 0.0884j & 0.1509 - 0.1509j & 0.0625 - 0.1509j & -0.0000 - 0.0884j & 0 & 0.0625 + 0.0625j & 0.1509 + 0.0625j & 0.2134 + 0.0000j \end{pmatrix} \quad (5.18)$$

Logo, ao normalizar a matriz, é possível visualizar a distribuição de amplitudes e fase através dos histogramas exibidos na Figura 41.

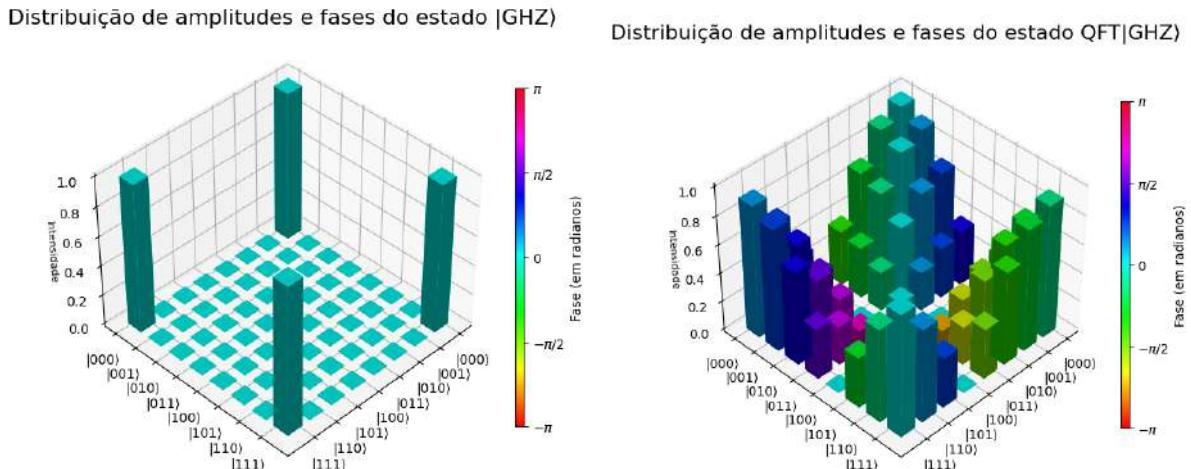


Figura 41 – Histograma tridimensional da tomografia dos estados $|GHZ\rangle$ (esquerda) e QFT $|GHZ\rangle$ (direita). Imagens obtidas com *python*. Fonte: Autoria própria.

Embora associados com bases computacionais diferentes, ou seja, possuem distribuição de fase única, nota-se imediatamente a ocorrência dos mesmos fatores de fase para o estado $|111\rangle$, confirmando a lógica de múltiplos do fator binário $7\pi/4$.

Os padrões de distribuição de intensidade para esse tanto, contemplando tanto o perfil transverso, quanto o histograma, intrigam pela distinção com relação aos estados da base computacional anteriormente discutidos. Em relação ao perfil transverso de intensidade, é possível que ocorra uma sobreposição direta com perdas que retorne o feixe luminoso transformado aos modos de Hermite-Gauss de primeira ordem. Além disso, analisando o histograma, há duas retas concorrentes, onde os valores próximos delas tendem a possuir fases que são frações menores do fator binário. Sendo assim, conclui-se que há um comportamento exclusivo associado com os estados não-separáveis transformados pelo circuito óptico proposto.

6 Conclusões e perspectivas futuras

Nesta dissertação buscamos mostrar a importância do emprego dos graus de liberdade em aplicações para informação quântica. Inspirados por trabalhos anteriores, como, por exemplo, a implementação tripartite do protocolo conhecido como teleporte quântico [15], que demonstram a vantagem da codificação da informação na polarização, nos modos transversos e no caminho, ao considerar que o processamento depende somente de uma entrada do feixe luminoso. Em conjunto com os dispositivos ópticos, temos ao alcance uma base teórica concisa o suficiente para explorar implementações de protocolos e algoritmos quânticos em circuitos ópticos lineares. Em particular, evidenciamos a Transformada Quântica de Fourier, que embora não seja propriamente um algoritmo quântico, desempenha um papel fundamental na codificação eficiente de informações de fase e possui aplicações em problemas de periodicidade, como a estimativa de fase quântica.

Logo, como contribuição inédita desta dissertação, desenvolvemos uma proposta de circuito óptico tripartite com os graus de liberdade da luz para a reprodução da QFT com feixes luminosos clássicos, objetivando sempre superar possíveis obstáculos e desafios experimentais. Dos principais desafios encontrados, destacamos a decisão da ordem de codificação dos graus de liberdade da luz para que o preparo do estado inicial conte a implementação de portas controladas de fase. Consideramos o uso de um divisor de modos transversos [80] para a definí-lo, junto a direção de propagação, como controles das portas de fase. Para reprodução das portas de fase, utilizamos o artifício das portas de fase geométricas da polarização [52]. Além disso, para fins de praticabilidade, ele também foi pensando para ser o mais compacto possível

Contemplando essas dificuldades, uma simulação computacional foi desenvolvida na intenção de analisar a coerência dos resultados da proposta com a literatura vigente. Sendo assim, a modelagem computacional do circuito óptico faz uso extensivo do formalismo de Jones, para os vetores da base computacional e matrizes dos dispositivos ópticos, e teve o código exclusivamente desenvolvido na linguagem de programação *python*.

Para a análise dos resultados computacionais, selecionamos quatro estados da base computacional ($|000\rangle$, $|010\rangle$, $|101\rangle$ e $|111\rangle$) e o estado tripartite maximamente emaranhado ($|GHZ\rangle$). Primeiramente, observamos um padrão do perfil transverso de intensidade com relação ao caminho em que o respectivo estado está codificado. Entretanto, obtemos também uma distribuição única para descrição dos modos transversos do estado emaranhado. Através da tomografia, verificamos a coerência das fases com o previsto teoricamente para os estados base e também o emaranhado.

Como perspectivas futuras, destacamos a implementação experimental do circuito

proposto, utilizando feixes luminosos intensos como prova de princípio. A realização prática do circuito permitirá a validação experimental dos resultados obtidos na simulação e a exploração de possíveis otimizações. Além disso, a investigação da reprodução da QFT em graus de liberdade fotônicos representa uma linha de pesquisa promissora, com potencial para aplicações em computação quântica fotônica.

Em resumo, pretendemos com esta dissertação, contribuir para o avanço das aplicações da computação quântica em sistemas ópticos, por demonstrar a viabilidade do uso de graus de liberdade da luz para implementação de operações quânticas complexas, como a Transformada Quântica de Fourier. A proposta apresentada abre novas possibilidades para realizações experimentais e potenciais simulações computacionais de algoritmos quânticos investidos na resolução de problemas de periodicidade.

Referências

- [1] Alan M. Turing. *On Computable Numbers, with an Application to the Entscheidungsproblem*. Oxford University Press, 1936. [1](#), [5](#)
- [2] T. Haigh, M. Priestley, and C. Rope. *ENIAC in Action: Making and Remaking the Modern Computer*. MIT Press, 2016. [1](#)
- [3] B. J. Copeland. *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*. Oxford University Press, 2006. [1](#)
- [4] J. Bardeen and W. H. Brattain. The transistor, a semi-conductor triode. *Physical Review*, 74(2):230–231, 1948. [1](#)
- [5] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8):114–117, 1965. [1](#)
- [6] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of statistical physics*, 22(5):563–591, 1980. [1](#)
- [7] Richard P Feynman. Simulating physics with computers. In *Feynman and computation*. CRC Press, 2018. [1](#)
- [8] David Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985. [1](#), [11](#)
- [9] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000. [1](#), [9](#), [11](#), [14](#), [39](#), [44](#)
- [10] Charles H Bennett and Stephen J Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992. [1](#)
- [11] B. S. Wherrett and F. A. P. Tooley, editors. *Optical Computing*. Scottish Universities Summer School in Physics, NATO Advanced Study Institute, 1988. Proceedings of the Thirty-Fourth Scottish Universities Summer School in Physics. [2](#)
- [12] F. Kien et al. Introduction to optical computing. In F. Ledermann et al., editors, *Springer Handbook of Optics*, chapter 12, pages 555–567. Springer, 2018. [2](#)

- [13] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of modern physics*, 79(1):135, 2007. [2](#)
- [14] Michael Reck, Anton Zeilinger, Herbert J Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58, 1994. [2](#)
- [15] B Pinheiro da Silva, M Astigarreta Leal, CER Souza, EF Galvão, and AZ Khouri. Spin–orbit laser mode transfer via a classical analogue of quantum teleportation. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 49(5):055501, 2016. [2](#), [45](#), [67](#)
- [16] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum communication. *Reviews of Modern Physics*, 74(1):145, 2002. [2](#)
- [17] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994. [2](#), [39](#), [43](#)
- [18] Richard Cleve and John Watrous. Fast parallel circuits for the quantum fourier transform. *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pages 526–536, 2000. [2](#)
- [19] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. [2](#)
- [20] Ludwig Boltzmann. Über die beziehung zwischen dem zweiten hauptsatze der mechanischen wärmetheorie und der wahrscheinlichkeitsrechnung respektive den sätzen über das wärmegleichgewicht. *Wiener Berichte*, 76:373–435, 1877. [5](#)
- [21] A Ya Khinchin. *Mathematical foundations of information theory*. Courier Corporation, 2013. [5](#)
- [22] Claude Elwood Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948. [5](#)
- [23] George Boole. The calculus of logic. 1848. [6](#)
- [24] Heribert Vollmer. *Introduction to circuit complexity: a uniform approach*. Springer Science & Business Media, 1999. [6](#)
- [25] Richard P. Feynman. *Feynman Lectures on Computation*. Addison-Wesley Publishing Company. Inc, 1996. [7](#), [8](#)
- [26] R Landauer. Irreversibility and heat generation in the computational process. *IBM Journal of research and Development*, 5(3):83, 1961. [7](#)

- [27] Charles H Bennett. Logical reversibility of computation. *IBM journal of Research and Development*, 17(6):525–532, 1973. [8](#)
- [28] Basil Evangelidis. Quantum logic as reversible computing. *arXiv preprint arXiv:2111.07431*, 2021. [8](#)
- [29] Paul Adrien Maurice Dirac. *The principles of quantum mechanics*. Number 27. Oxford university press, 1981. [8](#)
- [30] Vladimir Aleksandrovich Fock. Fundamentals of quantum mechanics. *Mir Publishers*, 1978. [8](#)
- [31] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. *Classical and quantum computation*. Number 47. American Mathematical Soc., 2002. [9](#), [11](#)
- [32] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum Mechanics, Volume 1: Basic Concepts, Tools, and Applications*. Wiley, 1991. [10](#)
- [33] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley Publishing Company. Inc, 1994. [11](#)
- [34] Asher Peres. Reversible logic and quantum computers. *Physical review A*, 32(6):3266, 1985. [11](#)
- [35] Stefano Markidis. What is quantum parallelism, anyhow? In *ISC High Performance 2024 Research Paper Proceedings (39th International Conference)*, pages 1–12. Prometheus GmbH, 2024. [11](#)
- [36] Tommaso Toffoli. Reversible computing. In *Proceedings of the 7th International Colloquium on Automata, Languages and Programming (ICALP)*, pages 632–644, Berlin, Heidelberg, 1980. Springer. Introdução da porta de Toffoli (CCNOT) no contexto de computação reversível. [14](#)
- [37] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964. [15](#)
- [38] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Experimental test of quantum nonlocality in three-photon greenberger–horne–zeilinger entanglement. *Nature*, 403(6769):515–519, 2000. [15](#)
- [39] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell’s inequalities. *Physical review letters*, 49(2):91, 1982. [15](#)

- [40] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. Going beyond bell's theorem. In *Bell's theorem, quantum theory and conceptions of the universe*, pages 69–72. Springer, 1989. [16](#)
- [41] Daniel M Greenberger, Michael A Horne, Abner Shimony, and Anton Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58(12):1131–1143, 1990. [16](#)
- [42] N David Mermin. Quantum mysteries revisited. *Am. J. Phys.*, 58(8):731–734, 1990. [16](#)
- [43] Günther Krenn and Anton Zeilinger. Entangled entanglement. *Physical Review A*, 54(3):1793, 1996. [16](#)
- [44] Adriano Barenco, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical review A*, 52(5):3457, 1995. [17](#)
- [45] Seth Lloyd. Almost any quantum logic gate is universal. *Physical review letters*, 75(2):346, 1995. [17](#)
- [46] Dorit Aharonov. A simple proof that toffoli and hadamard are quantum universal. *arXiv preprint quant-ph/0301040*, 2003. [17](#)
- [47] Alexei Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997. Apresentação formal do Teorema de Solovay-Kitaev. [17](#)
- [48] Rachel Won. The power of light-driven computing. *Nature Photonics*, 17(11):934–936, 2023. [19](#)
- [49] Yifan Sun, Qian Li, Ling-Jun Kong, Jiangwei Shang, and Xiangdong Zhang. Universal classical optical computing inspired by quantum information process. *Annalen der Physik*, 534(12):2200360, 2022. [19](#)
- [50] Marcello H. M. Passos. *Modos spin-órbita como recurso em processos de Informação Quântica (tese de doutorado em física)*. Universidade Federal Fluminense, 2020. [19](#), [20](#), [28](#)
- [51] W. F. Balthazar. *Não-separabilidade de graus de liberdade de um feixe laser e aplicações em informação quântica (tese de doutorado em física)*. Universidade Federal Fluminense, 2016. [19](#), [23](#), [24](#), [29](#), [31](#)
- [52] Guilherme Tadeu Costa da Cruz. Portas de fase com fases geométricas em modos spin-órbita, 2024. Dissertação de Mestrado. [19](#), [47](#), [67](#)

- [53] Eugene Hecht. *Optics*, 5th. Pearson Education India, 2017. 19, 25, 31
- [54] Matthew Schwartz. Lecture 14: Polarization. <https://scholar.harvard.edu/files/schwartz/files/lecture14-polarization.pdf>. 21
- [55] Max Born and Emil Wolf. *Principles of Optics*. Cambridge University Press, 7th edition, 1999. 22
- [56] Dennis Goldstein. *Polarized Light*. CRC Press, 3rd edition, 2011. 23
- [57] Frank L. Pedrotti and Leno S. Pedrotti. *Óptica e Polarização*. Prentice Hall, 1993. Capítulo 14: Matrizes de Jones. 23
- [58] Anthony Gerrard and James M. Burch. *Introduction to Matrix Methods in Optics*. Dover Publications, Mineola, NY, 1994. 23
- [59] Alison M Yao and Miles J Padgett. Orbital angular momentum: origins, behavior and applications. *Advances in optics and photonics*, 3(2):161–204, 2011. 25
- [60] Pieter Kok and Brendon W Lovett. *Introduction to optical quantum information processing*. Cambridge university press, 2010. 26, 27
- [61] E Abramochkin and V Volostnikov. Beam transformations and nontransformed beams. *Optics Communications*, 83(1-2):123–135, 1991. 28
- [62] Daniel Gonzaga Braga. Estudo de discórdia em modos spin-órbita da luz. Dissertação de mestrado, Universidade Federal Fluminense, Volta Redonda, 2021. 30
- [63] Vinicius de Souza Lamego. Proposta de preparação e caracterização de estados x utilizando modos spin-órbita de um feixe laser, 2020. 32
- [64] George B Arfken, Hans J Weber, and Frank E Harris. *Mathematical methods for physicists: a comprehensive guide*. Academic press, 2011. 35
- [65] Ronald N. Bracewell. *The Fourier Transform and Its Applications*. McGraw-Hill, 3rd edition, 1999. 36
- [66] James W Cooley and John W Tukey. An algorithm for the machine calculation of complex fourier series. *Mathematics of computation*, 19(90):297–301, 1965. 37
- [67] Marshall C Pease. An adaptation of the fast fourier transform for parallel processing. *Journal of the ACM (JACM)*, 15(2):252–264, 1968. 37
- [68] Wolfgang Scherer. *Mathematik Der Quanteninformatik*. Springer, 2016. 38
- [69] A Yu Kitaev. Quantum measurements and the abelian stabilizer problem. *arXiv preprint quant-ph/9511026*, 1995. 41

- [70] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021. [41](#)
- [71] Chen-Yu Liu, Kuan-Cheng Chen, and Chu-Hsuan Abraham Lin. Learning quantum phase estimation by variational quantum circuits. In *2024 International Joint Conference on Neural Networks (IJCNN)*, pages 1–6. IEEE, 2024. [41](#)
- [72] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. [44](#)
- [73] Martin Roetteler, Michael Naehrig, Krysta M Svore, and Kristin Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In *Advances in Cryptology—ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part II* 23, pages 241–270. Springer, 2017. [44](#)
- [74] Shuntaro Takeda and Akira Furusawa. Toward large-scale fault-tolerant universal photonic quantum computing. *APL Photonics*, 4(6), 2019. [45](#)
- [75] M. AbuGhanem. Photonic quantum computers, 2024. [45](#)
- [76] Yacob Ben-Aryeh Ronen Barak. Quantum fast fourier transform and quantum computation by linear optics. *Optical Society of America*, September 7, 2006. [45](#)
- [77] H Aghae Rad, T Ainsworth, RN Alexander, B Altieri, MF Askarani, R Baby, L Banchi, BQ Baragiola, JE Bourassa, RS Chadwick, et al. Scaling and networking a modular photonic quantum computer. *Nature*, pages 1–8, 2025. [45](#)
- [78] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022. [45](#)
- [79] Strawberry Fields. Polarization demo. https://strawberryfields.ai/photonics/demos/run_polarization.html, 2023. Acesso em: 02/2025. [45](#)
- [80] Hiroyuki Sasada and Megumi Okamoto. Transverse-mode beam splitter of a light beam and its application to quantum cryptography. *Physical Review A*, 68(1):012323, 2003. [47](#), [67](#)
- [81] J. R. Johansson, P. D. Nation, and F. Nori. QuTiP 2: A Python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 184:1234–1240, 2013. [48](#)

- [82] G. van Rossum and OpticsPy Team. Lightpipes: A python optical toolkit for beam propagation. <https://opticspy.github.io/lightpipes/index.html>, 2025. Accessed: 2025-01-14. 48