

---

**Demonstração Óptica do Algoritmo de Deutsch-Jozsa  
com 1 qubit**

*Mariana Rodrigues Barros*

---

---

Demonstração Óptica do Algoritmo de  
Deutsch-Jozsa com 1 qubit

*Mariana Rodrigues Barros*

Orientador: Prof. Dr. Sebastião José Nascimento de Pádua  
Co - orientador: Prof. Dr. Marcelo de Oliveira Terra Cunha

Dissertação apresentada à Universidade Federal de Minas Gerais como requisito parcial para a obtenção do grau de **Mestre em Física**.

Belo Horizonte  
Abril de 2010

---

# Conteúdo

|   |           |
|---|-----------|
| <b>Agradecimentos</b>   | <b>5</b>  |
| <b>Resumo</b>   | <b>6</b>  |
| <b>Abstract</b>   | <b>7</b>  |
| <b>1 Introdução</b>   | <b>12</b> |
| 1.1 Conversão Paramétrica Descendente . . . . .                                 | 14        |
| 1.2 Modulador Espacial de Luz . . . . .   | 21        |
| 1.2.1 Cristal Líquido Nemático Girado . . . . .                                 | 22        |
| 1.2.2 Propriedades ópticas dos Cristais Líquidos Nemáticos<br>Girados . . . . . | 23        |
| 1.2.3 LC-R2500 . . . . .  | 28        |
| <b>2 Conceitos Fundamentais</b>   | <b>31</b> |
| 2.1 O Qubit . . . . .   | 31        |
| 2.2 A esfera de Bloch . . . . .   | 33        |
| 2.3 Portas Lógicas . . . . .  | 34        |
| <b>3 O Problema de Deutsch</b>  | <b>38</b> |
| 3.1 Paralelismo Quântico . . . . .  | 39        |
| 3.2 O Problema de Deutsch . . . . .   | 41        |
| 3.3 Algoritmo de Deutsch . . . . .  | 43        |
| 3.4 Algoritmo de Deutsch-Jozsa . . . . .  | 46        |
| 3.5 Novo Algoritmo . . . . .  | 48        |

---

**CONTEÚDO** **4**

---

|          |  |           |
|----------|--|-----------|
| <b>4</b> | <b>O Experimento</b>                                   | <b>50</b> |
| 4.1      | Montagem Experimental . . . . .                        | 50        |
| 4.2      | Calibração do SLM . . . . .                            | 52        |
| 4.3      | Posicionando o SLM com relação à Fenda Dupla . . . . . | 57        |
| 4.4      | O Procedimento de Medição . . . . .                    | 58        |
| <b>5</b> | <b>Conclusão</b>                                       | <b>65</b> |

## Agradecimentos

Primeiramente à minha família. Aos meus pais pela inspiração e apoio incondicional, permitindo que isso se realizasse, e ao meu irmão pelo companherismo e amizade. E por me aguentar sempre!

Ao meu orientador, Sebastião de Pádua, por sua grande competência, paciência, confiança e apoio durante os anos de mestrado e iniciação científica.

À tia Zilca e Márcio pelo apoio desde que mudei para Bh.

Aos amigos do laboratório José, Breno, Wanderson, Marcos, Pierre e Olavo pela amizade e grandes contribuições ao trabalho.

À todos amigos da física, em especial a Lili pelas conversas e desabafos!

Ao Vagner, meu primeiro orientador, por seu grande incentivo.

Ao Marcelo Terra por sua contribuição teórica para implementação dessa dissertação.

A todos os membros do EnLight.

À Capes pelo apoio financeiro.

---

## Resumo

Neste trabalho implementamos o algoritmo de Deutsch-Jozsa com 1 qubit removendo uma redundância neste, o que reduziu o tamanho do registro e simplificou a função avaliação. Para isso, usamos pares de fótons gerados pela conversão paramétrica descendente, onde um deles é usado como trigger e o outro atravessa uma fenda dupla saindo em um estado de superposição de caminhos, ou seja, um qubit. Usando um modulador espacial, que coloca fases no caminho dos fótons e detectando em coincidência, demonstramos o algoritmo de Deutsch-Jozsa com fótons, e usando apenas 1 qubit.

---

## Abstract

In this work we implement the Deutsch-Jozsa algorithm with one qubit by removing a redundancy on it, which reduces the size of the register and simplifies the function evaluation. In order to do this, we used a pair of photons produced by down conversion, where one of them is used as trigger and the other passes through a double slit; as a result its output is in a superposition of paths, i.e., one qubit. Using a spatial light modulator (SLM) that puts phases on the paths of the photons, and detecting in coincidence, we demonstrate the Deutsch-Jozsa algorithm with photons, and using only one qubit.

---

## Lista de Figuras

- 1.1 Diagrama de energia simplificado da conversão paramétrica descendente. . . . . 15
  - 1.2 Geometria da conversão paramétrica descendente . . . . . 15
  - 1.3 Representação geométrica da condição de casamento de fase: a adição vetorial dos vetores de onda da luz convertida parametricamente deve ser igual ao vetor de onda da luz do pump. Isso é equivalente à conservação do momento. . . . . 16
  - 1.4 Casamento de fase é do tipo I. Nesse caso, o índice de refração para ambos fótons será representado por uma esfera e a solução para as condições de casamento de fase correspondem a interseção dessas duas esferas. O espectro resultante consiste em emissões de cones concêntricos. A figura mostra uma projeção desse processo de casamento de fase no plano que contem o eixo óptico [18]. . . . . 17
  - 1.5 Casamento de fase tipo II. Os fótons produzidos tem polarizações ortogonais, tais que um sempre vê índice de refração ordinário (representado pela esfera), enquanto o índice de refração visto pelo outro fóton irá depender da direção de propagação com respeito ao eixo óptico (representado pelo elipsóide de revolução em torno da direção de EO) [18]. . . . . 18
-

|      |  |    |
|------|--|----|
| 1.6  | a) Conversão Paramétrica Descendente do Tipo I: Os fótons gêmeos têm polarização ortogonal à do laser. Os cones internos possuem fótons com maior energia. b) Visão frontal. As marcas com X ligadas por uma linha pontilhada indicam regiões em que se encontram alguns dos possíveis pares de fótons gêmeos gerados. . . . .   | 19 |
| 1.7  | a) Conversão Paramétrica Descendente do Tipo II: Os fótons do feixe extraordinário têm mesma polarização do feixe de bombeamento (pump) e os do ordinário têm polarização ortogonal. Os cones internos possuem fótons com maior energia. b) Visão frontal. As marcas com X ligadas por uma linha pontilhada indicam regiões em que se encontram pares de fótons gêmeos. . . . .  | 20 |
| 1.8  | Organização Molecular de diferentes tipos de cristais líquidos: (a) nemáticos; (b) esméticos; (c) colestéricos. . . . .  | 22 |
| 1.9  | Propagação da luz em um cristal líquido nemático. Nesse diagrama o ângulo de giro é de $90^\circ$ . . . . .  | 23 |
| 1.10 | Um LCTV colocado entre um conjunto de polarizadores propriamente orientados (P1,P2) e placas de onda (W1,W2), podem agir como um modulador de fase ou de amplitude, somente [28]. . . . .  | 28 |
| 1.11 | LC-R2500 Spatial Light Modulator . . . . .   | 29 |
| 1.12 | Escalas de cinza. A Fig.(a) mostra uma determinada escala de cinza preenchendo totalmente o display do LCD. Por outro lado, a Fig.(b) mostra duas escalas de cinza dividindo igualmente a tela do display. Imagens como a apresentada na Fig.(b) são utilizadas quando queremos modificar a amplitude ou a fase de um feixe em relação ao outro, quando cada um deles é transmitido por uma das fendas de uma mesma fenda dupla. . . . . | 29 |
| 2.1  | Representação de um qubit na esfera de Bloch . . . . .   | 33 |

---

---

|     |  |    |
|-----|--|----|
| 2.2 | Representação Diagramática de Algumas Portas de um Qubit. Aqui mostramos a ação das portas X, Z e Y, respectivamente, quando as operamos num estado inicial $\alpha  0\rangle + \beta  1\rangle$ . . . . .   | 35 |
| 2.3 | Representação Diagramática da Porta Fase . . . . .   | 36 |
| 2.4 | Representação Diagramática da Porta $U_{CNOT}$ . . . . .   | 37 |
| 3.1 | Imagem da transformação unitária $U_f$ correspondendo a avaliação da função $f(x)$ . As linhas superiores e inferiores representam os registros dados e alvo, respectivamente. . . . .   | 40 |
| 3.2 | Algoritmo para resolver o problema de Deutsch usando um computador quântico. . . . .   | 43 |
| 3.3 | Circuito quântico para implementar o algoritmo de Deutsch . . . . .  | 45 |
| 3.4 | Circuito quântico esquematizando o algoritmo de Deutsch - Jozsa. $\hat{H}_{tot}$ representa uma transformação Hadamard aplicada em cada qubit do registro de controle. $\hat{U}_{f-c-N}$ representa a operação da porta $f - controlled - NOT$ . . . . . | 47 |
| 3.5 | Algoritmo proposto por Collins <i>et al.</i> A notação é a mesma da figura 3.4 com a porta $f - controlled$ no lugar da porta $f - controlled - NOT$ . . . . .   | 49 |
| 4.1 | Aparato experimental usado para implementar o algoritmo de Deutsch - Jozsa com um qubit. . . . .   | 51 |
| 4.2 | Aparato experimental usado para calibrar a fase fornecida pelo SLM: a)interferômetro de Michelson; b)fenda dupla usada para gerar interferência . . . . .  | 54 |
| 4.3 | Sistema óptico que compõe o SLM . . . . .  | 54 |
| 4.4 | Motagem experimental utilizada na segunda calibração. . . . .  | 55 |
| 4.5 | Medidas de contagens (a.1 e b.1) e coincidências (a.2 e b.2) para as polarizações de $90^\circ$ (a.1 e a.2) e $75^\circ$ (b.1 e b.2). . . . .  | 56 |
| 4.6 | Imagens das fendas utilizando as escalas de cinza e polarizações de saída presentes na tabela acima. A imagem (a) corresponde a diferença de fase zero, a imagem (b) corresponde a diferença de fase $\pi$ . . . . .                                     | 57 |
| 4.7 | Medidas dos padrões de interferência utilizando os dados da tabela. . . . .  | 58 |

---

|      |  |    |
|------|--|----|
| 4.8  | A figura mostra duas escalas de cinza dividindo igualmente a tela do display de LCD. Tal figura foi utilizada quando queríamos modificar a fase de um feixe em relação ao outro, quando cada um deles é transmitido por uma das fendas de uma mesma fenda dupla. . . . . | 59 |
| 4.9  | Gráficos dos Padrões de Interferência para as fases $0$ e $\pi$ aplicadas no SLM. . . . .  | 60 |
| 4.10 | Imagem das fendas utilizando as escalas de cinza e as polarizações de entrada e saída encontradas na última calibração. . . .  | 62 |
| 4.11 | Gráficos dos Padrões de Interferência para as fases $0$ e $\pi$ aplicadas no SLM. . . . .  | 63 |
| 4.12 | Histograma da medida do Algoritmo de Deutsch, demonstrando o comportamento de interferência construtiva e destrutiva, simulando as funções balanceadas e constantes. . . . .   | 63 |

---

# Capítulo 1

## Introdução

A imagem moderna da ciência da computação foi proposta em 1936 por Alan Turing, que desenvolveu em detalhe o modelo de computador programável conhecido como Máquina de Turing.

Na tentativa de responder a questão de que se existira um modelo definitivo, ao menos em princípio, pelo qual todas as questões matemáticas pudessem ser resolvidas, ele analisou o que uma pessoa faz durante um processo de raciocínio e, então, começou a mapear esse processo como uma “máquina teórica” que operaria em símbolos de acordo com regras elementares precisamente definidas, o que em linguagem moderna chamamos de algoritmo [1]. Ele mostrou que existe uma máquina de Turing Universal, capaz de simular qualquer máquina de Turing. Até agora estávamos considerando as máquinas de Turing construídas somente com um propósito específico. A máquina universal nos permite rodar todas as máquinas de Turing em uma geral, que compreende todas as outras. Desta forma, para cada algoritmo passível de ser realizado existe um equivalente na Máquina de Turing Universal.

A indústria da computação tem então alcançado um crescimento extraordinário, tanto que em 1965, baseada nas observações de Gordon Moore que o número de transistores por circuito integrado tinha tido um crescimento exponencial desde que aqueles foram inventados, foi estabelecida a Lei de Moore, a qual diz que a capacidade dos computadores dobra aproximadamente a cada dois anos, para um custo financeiro constante.

No entanto, esse crescimento começa encontrar dificuldades à medida

---

que o tamanho dos componentes fica menor. Extrapolando a lei de Moore, poderíamos estimar que ao redor do ano de 2020 deveremos atingir o tamanho atômico para estocar informação num único bit. Nesse ponto, os efeitos quânticos se tornam inevitavelmente dominantes [4].

Em 1982, Feynman propôs o uso de dispositivos que tirassem proveito da mecânica quântica para definir um aparato computacional capaz de simular eficientemente qualquer sistema físico o que levou ao desenvolvimento do conceito moderno de computação quântica [9].

Assim, na fronteira entre a física quântica, a computação, e a matemática surgiu um novo campo de pesquisa: a informação quântica. A idéia principal é tratar a informação com base na mecânica quântica, tal que a computação e comunicação sejam feitas principalmente através de sistemas quânticos. O objetivo, então, é construir um aparelho que processe informação e realize operações lógicas tirando proveito das leis da mecânica quântica, além de desenvolver ferramentas que permitam testar seus princípios teóricos, tornando suas previsões mais intuitivas.

Um computador quântico executa cálculos fazendo uso direto de propriedades da mecânica quântica, tais como sobreposição de estado e interferência. Simplificando, eles podem processar um grande número de entradas clássicas com uma única avaliação e fazem o uso do paralelismo quântico inerente, associado ao princípio de superposição, para destacar a saída desejável [2,4].

As propostas para implementação de um computador quântico são diversas, tais como ressonância magnética nuclear (NMR) com moléculas em um líquido, armadilhas de íons, eletrodinâmica quântica de cavidades (QED) [5] e pontos quânticos [6]; mas ainda é muito cedo para dizer qual delas deverá ser a mais apropriada para construção de um hardware [4].

#### *Disposição do trabalho*

Neste trabalho implementamos o algoritmo de Deutsch-Jozsa com 1 qubit usando pares de fótons gerados pela conversão paramétrica descendente, onde um deles é usado como trigger e o outro atravessa uma fenda dupla saindo em um estado de superposição de caminhos, ou seja, um qubit. Usando um modulador espacial, que coloca fases no caminho dos fótons e detectando

---

em coincidência, demonstramos o algoritmo de Deutsch-Jozsa com fótons, e usando apenas 1 qubit. Como o algoritmo de Deutsch-Jozsa com 1 qubit será demonstrado com pares de fótons gerados através do processo óptico não-linear da conversão paramétrica descendente, começaremos abordando tal assunto no capítulo 1, juntamente com a teoria sobre moduladores espaciais de luz (usado para colocar fases no caminho dos fótons). No capítulo 2 veremos os conceitos fundamentais da computação quântica e as ferramentas necessárias para entendê-la. Em seguida, no capítulo 3, revisaremos conceitos sobre paralelismo quântico, algoritmo de Deutsch e o algoritmo de Deutsch-Jozsa. No capítulo 4 introduziremos a proposta para o algoritmo de Deutsch com um qubit, realizando um experimento para testá-la. Para encerrar, apresentaremos no capítulo 5 as conclusões e perspectivas futuras.

## 1.1 Conversão Paramétrica Descendente

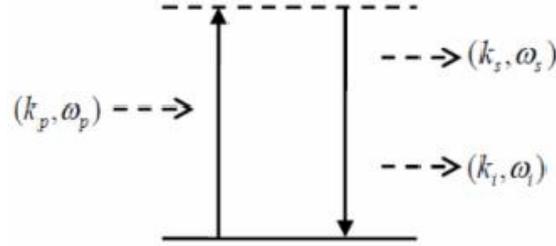
A conversão paramétrica descendente (CPD) é um processo óptico resultante da interação não linear de um campo eletromagnético com um meio material onde pares de fótons (conhecidos como *signal* e *idler*) podem ser gerados quando um feixe de laser incide em um cristal. Ela tem sido utilizada em vários experimentos recentemente, onde é particularmente útil como fonte de luz para testes fundamentais de mecânica quântica, já que os fótons *idler* e *signal*, gerados no processo, são produzidos como pares correlacionados.

No processo, três feixes de luz são acoplados na interação dentro de um meio óptico não linear. Como mostrado no diagrama de níveis simplificado na Figura 1.1, o feixe do *pump* excita os elétrons no meio não linear para um estado virtual e o decaimento espontâneo do estado virtual contribui para emissão de pares de fótons com frequência mais baixa. No processo, conhecido como conversão paramétrica descendente (CPD), os fótons *idler* e *signal* (fótons gêmeos) são gerados simultaneamente [17].

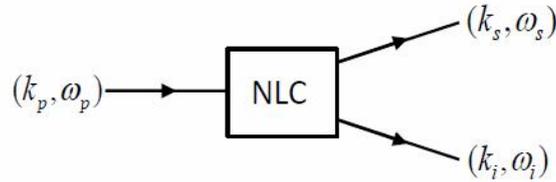
Ou seja, no processo de CPD um fóton de energia  $\hbar\omega_p$  incide em um cristal não linear e é convertido, espontaneamente, em outros dois fótons com energia  $\hbar\omega_i$  (fóton *idler*) e  $\hbar\omega_s$  (fóton *signal*), mais baixas. Figura 1.2 [19].

Esses fótons são intimamente correlacionados em vários parâmetros, tais como tempo de emissão, direção e energia [18]. A previsão de propriedades

---



**Figura 1.1:** Diagrama de energia simplificado da conversão paramétrica descendente.



**Figura 1.2:** Geometria da conversão paramétrica descendente

como a polarização e a direção de emissão dos fótons criados depende da utilização das condições de casamento de fase. A primeira condição é conservação de energia:

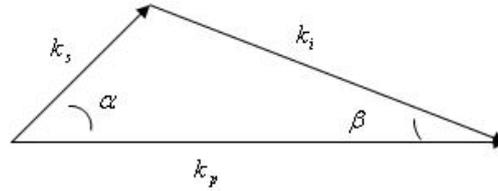
$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i \quad (1.1)$$

A segunda condição é a conservação do momento (representada geometricamente pela Figura 1.3):

$$\hbar\vec{k}_p = \hbar\vec{k}_s + \hbar\vec{k}_i. \quad (1.2)$$

Há, no entanto, cristais anisotrópicos nos quais os índices de refração dependem da direção na qual a onda propaga e na orientação da sua polarização com respeito ao eixo óptico (EO).

A direção que define o EO é tal que uma onda viajando ao longo daquela direção verá o mesmo índice - chamado de índice de refração ordinário,  $n_o$  - independente de sua polarização. Se a onda viaja em qualquer outra direção, ela pode ver um dos dois índices de refração dependendo da orientação da



**Figura 1.3:** Representação geométrica da condição de casamento de fase: a adição vetorial dos vetores de onda da luz convertida parametricamente deve ser igual ao vetor de onda da luz do pump. Isso é equivalente à conservação do momento.

sua polarização em relação ao plano formado pelo vetor  $\vec{k}$  e o eixo óptico.

Se a onda for polarizada perpendicularmente ao plano formado por EO e o vetor  $\vec{k}$ , ela terá  $n_o$  e será chamada de onda ordinária. Caso contrário, ela terá um índice de refração que depende no ângulo de propagação com respeito ao eixo óptico,  $n(\theta)$ , e varia elipticamente entre  $n_o$  e o chamado índice de refração extraordinário,  $n_e$ . Por analogia, essa onda é chamada de onda extraordinária.

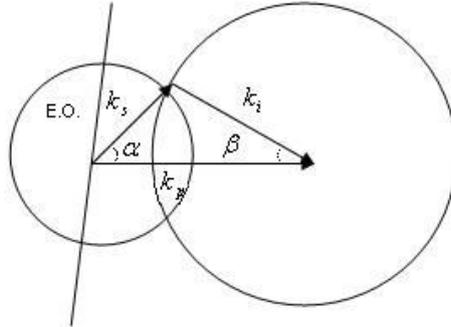
Esses índices de refração diferentes disponíveis no mesmo material significam que selecionando diferentes índices para o pump, signal e idler as condições de casamento de fase podem ser encontrados.

As diferentes condições de casamento de fase, que levam à conservação da energia e do momento, também levam a uma certa distribuição espacial de frequências e restringem a polarização dos fótons que são convertidos no cristal. Devido à simetria em torno da direção de propagação, a luz convertida é gerada em forma de cones de luz. É possível visualizar qualitativamente essas estruturas por meios de uma construção geométrica, baseada na forma dos índices de refração.

O casamento de fase pode ser do tipo I, que é caracterizado pelo signal e pelo idler compartilhando a mesma polarização (perpendicular à polarização do pump); e do tipo II, onde o par apresenta polarizações ortogonais entre si e uma delas é igual ao pump.

As Figuras 1.4 e 1.5 mostram as condições de casamento de fase determinadas nas formas dos índices de refração. Para entendê-las vamos supor que

as frequências sejam fixas.



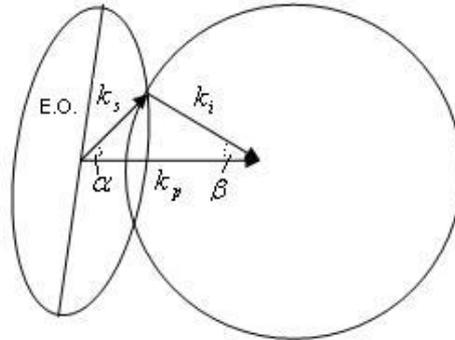
**Figura 1.4:** Casamento de fase é do tipo I. Nesse caso, o índice de refração para ambos fótons será representado por uma esfera e a solução para as condições de casamento de fase correspondem a interseção dessas duas esferas. O espectro resultante consiste em emissões de cones concêntricos. A figura mostra uma projeção desse processo de casamento de fase no plano que contem o eixo óptico [18].

Se desenharmos um vetor representando o signal nós sabemos que sua cauda deve coincidir com a calda do vetor do pump; agora podemos escolher o ângulo no qual o vetor é orientado mas esse ângulo determina o comprimento do vetor:

$$|\vec{k}| = \frac{w}{c}n(\theta, w)$$

Escolhendo todos os ângulos possíveis nós podemos mapear as diferentes posições para a cabeça do vetor da onda signal na superfície. Já que fixamos as frequências, essa superfície será dada pela dependência de  $n$  com o ângulo  $\theta$ . No caso que o signal vê o índice de refração ordinário não haverá dependência e, portanto, a superfície será uma esfera; se por outro lado, o índice é o extraordinário, então, a superfície será um elipsóide de revolução.

Esse mesmo procedimento pode ser seguido para o fóton idler, mas desta vez a cabeça do vetor será fixa na cabeça do vetor do pump e a calda que varrerá sua posição dependendo da orientação. É claro que a frequência tem que ser conjugada àquela escolhida para o signal. Ainda, as posições para



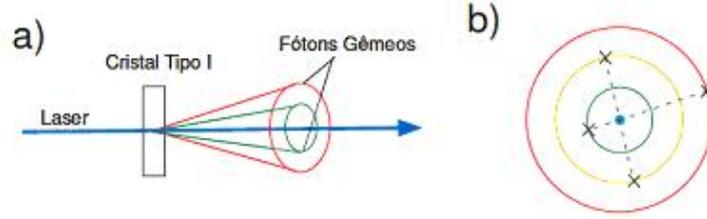
**Figura 1.5:** Casamento de fase tipo II. Os fótons produzidos tem polarizações ortogonais, tais que um sempre vê índice de refração ordinário (representado pela esfera), enquanto o índice de refração visto pelo outro fóton irá depender da direção de propagação com respeito ao eixo óptico (representado pelo elipsóide de revolução em torno da direção de EO) [18].

a calda irão varrer uma superfície que depende do índice de refração. Uma vez que as superfícies correspondendo ao sinal e ao idler estão no lugar, podemos ver que são dados pela curva resultante da interseção entre elas somente lugares onde as condições de casamento de fase são conhecidas.

Quando temos casamento de fase tipo I, as superfícies representando os índices são esferas e portanto, a luz será emitida em cones concêntricos nos quais todos compartilham o eixo de simetria definido pela direção de propagação do feixe do pump. A abertura de cada cone é determinada pela frequência da luz. Como mostrado na Figura 1.6:

Já no casamento de fase tipo II, ficarão duas séries de cones concêntricos, uma série sendo ordinariamente polarizada e a outra extraordinariamente polarizada; ainda, o ângulo de abertura depende da frequência, como mostrado na Figura 1.7.

É bem conhecido que em um dielétrico não linear, um campo elétrico incidente  $\mathbf{E}$  criará polarização  $\mathbf{P}$  tendo contribuições que não são somente lineares em  $\mathbf{E}$ . Em um tratamento mais formal, o hamiltoniano é dado por [20,21,25]:



**Figura 1.6:** a) Conversão Paramétrica Descendente do Tipo I: Os fótons gêmeos têm polarização ortogonal à do laser. Os cones internos possuem fótons com maior energia. b) Visão frontal. As marcas com X ligadas por uma linha pontilhada indicam regiões em que se encontram alguns dos possíveis pares de fótons gêmeos gerados.

$$H = \frac{1}{2} \int_V P_i(\mathbf{r}, t) E_i(\mathbf{r}, t) dV \quad (1.3)$$

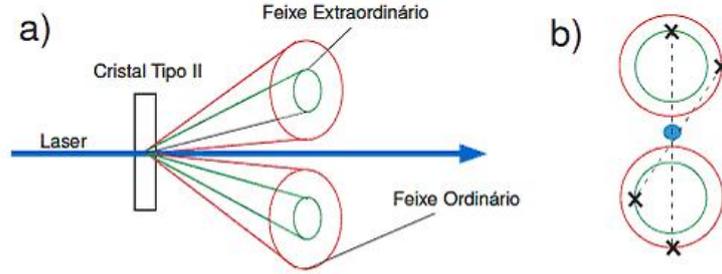
Como a resposta desses materiais ao campo eletromagnético é uma resposta não linear, podemos expressar a polarização como um tensor. O termo de segunda ordem da polarização do meio é:

$$P_i \rightarrow \tilde{\chi}_{ijk}^2 E_j E_k. \quad (1.4)$$

Onde  $\tilde{\chi}_{ijk}^2$  é o tensor susceptibilidade elétrica de segunda ordem. Esse termo é responsável pelos processos de mistura de três ondas, no qual a CPD faz parte. Isso faz uma contribuição à energia do campo eletromagnético da forma:

$$H_I = \frac{1}{2} \int_V P_i(\mathbf{r}, t) E_i(\mathbf{r}, t) d^3x = \frac{1}{2} \int_V \tilde{\chi}_{ijk} E_i(\mathbf{r}, t) E_j(\mathbf{r}, t) E_k(\mathbf{r}, t) d^3x \quad (1.5)$$

Nas referências [16,17,23,26] encontramos que o estado quântico da CPD em uma interação de primeira ordem, considerando o tratamento perturbativo multimodo da CPD, é



**Figura 1.7:** a) Conversão Paramétrica Descendente do Tipo II: Os fótons do feixe extraordinário têm mesma polarização do feixe de bombeamento (pump) e os do ordinário têm polarização ortogonal. Os cones internos possuem fótons com maior energia. b) Visão frontal. As marcas com X ligadas por uma linha pontilhada indicam regiões em que se encontram pares de fótons gêmeos.

$$|\psi(t)\rangle = |vac\rangle_{s,i} + \eta \frac{\delta w^{3/2}}{2\pi^{1/2}} \sum_{w_1} \sum_{w_2} \sum_{w_3} \phi(w_2, w_3; w_1) \frac{\text{sen}\Omega t_1/2}{\Omega/2} \times \exp^{i\Omega(t-t_1/2)} \exp^{-i(\mathbf{k}_2+\mathbf{k}_3-\mathbf{k}_1)\mathbf{r}_o} V(w_1) |w_2\rangle_s |w_3\rangle_i$$

onde  $\phi(w_2, w_3; w_1) = M \prod_{j=1}^3 \left(\frac{w_j}{w_{j0}}\right)^{1/2} \times \prod_{j=1}^3 \left[\frac{\text{sen}(k_1+k_2-k_3)_m l_m/2}{(k_1+k_2-k_3)_m/2}\right]$  é a função espectral, que incorpora a dependência da frequência,  $\delta w$  é o espaçamento de modo,  $V$  é a amplitude da onda monocromática de bombeamento (pump),  $|vac\rangle_{s,i}$  é o estado do vácuo,  $\eta$  é a magnitude da contribuição perturbativa e  $w_1$ ,  $w_2$  e  $w_3$  são as frequências do pump, do signal e do idler, respectivamente.

O estado acima foi obtido utilizando - se a expansão do operador evolução temporal e restringindo a expansão à primeira ordem. Portanto, apenas a geração de um par de fótons é considerada. Ver [16]. Esse estado exibe algumas características não intuitivas. Podemos ver que a soma sobre as frequências não permite fatorização em um produto de estados idler e signal. Logo, dizemos que os fótons idler e signal estão *emaranhados* no domínio da frequência.

Portanto, o estado do fóton idler é governado por observações feitas no fóton signal, mesmo que os dois fótons estejam muito separados quando a

medida é feita, não havendo tempo para os dois se comunicarem um com o outro. Para maiores informações sobre a CPD, ver [16,17].

## 1.2 Modulador Espacial de Luz

Displays de cristal líquido são aparatos óptico-elétricos que podem modular um feixe de luz. Isso é possível porque eles são estruturas compostas de pixels\* que podem ser usadas para produzir amplitudes espacialmente dependentes e/ou modulação de fase de um feixe de luz incidente [32,34].

Vários avanços na tecnologia têm permitido o uso de LCDs comerciais, extraídos de projetores de vídeos, para construir imagens óticas em tempo real. Avanços teóricos e metodológicos têm permitido o controle destes dispositivos como moduladores espaciais de luz (SLM), que podem ser usados para a modulação de fase ou de amplitude apenas, quando selecionamos propriamente as configurações de entrada e saída [27].

Os SLMs são usados principalmente para mostrar imagens e para construir lentes digitais e hologramas. No entanto, por causa de sua versatilidade experimental como dispositivos programáveis, seu uso tem sido considerado na área de óptica quântica.

Cristais líquidos programáveis foram usados como um sistema de varredura em microscopia de varredura [28]. Mais recentemente, um LCD programável foi usado para realizar simulações óticas de algoritmos quânticos [29]. Lentes e um LCD programável foram usados para introduzir variações de fase espacial no perfil de um feixe ótico clássico, simulando os algoritmos de Deutsch-Jozsa e Grover. Um sistema semelhante foi também usado para testar a simulação de um operador de Hadamard ótico via a simulação ótica do algoritmo de Deutsch [30].

O estado de cristal líquido é um estado da matéria que tem características de líquidos e de cristais. As moléculas que compõem esses cristais são

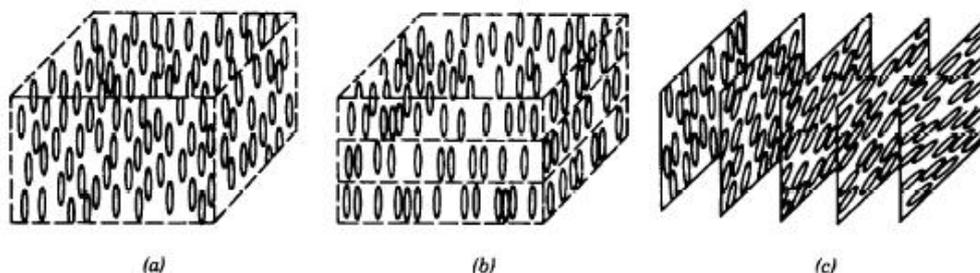
---

\*Pixel : (aglutinação de Picture e Element) é o menor elemento num dispositivo de exibição, ao qual é possível atribuir-se uma cor. De uma forma mais simples, um pixel é o menor ponto que forma uma imagem digital, sendo que o conjunto de milhares de pixels formam a imagem inteira.

---

moléculas orgânicas alongadas em um eixo [36], as quais possuem ordem orientacional, como os cristais, mas não têm ordem posicional, como os líquidos.

Existem três tipos (fases) de cristais líquidos (Figura 1.8) [21,35]: os cristais líquidos **nemáticos**, onde as moléculas do cristal tendem a ser paralelas umas com as outras, mas suas posições são aleatórias; os **esméticos**, que possuem ordenação em orientação e em posição; e os **colestéricos**, no qual os planos de moléculas que compõem o cristal sofrem uma rotação helicoidal em torno de seu eixo.



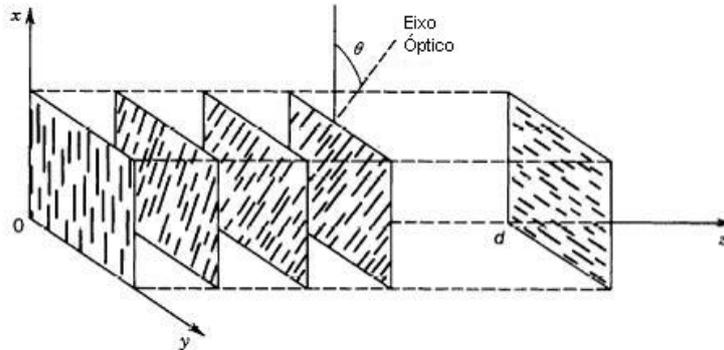
**Figura 1.8:** Organização Molecular de diferentes tipos de cristais líquidos: (a) nemáticos; (b) esméticos; (c) colestéricos.

### 1.2.1 Cristal Líquido Nemático Girado

Cristais líquidos nemáticos girados são um tipo especial de cristal líquido nemático [21,35] no qual uma rotação helicoidal em torno de seu eixo é imposta por forças externas, elétricas ou mecânicas. A diferença entre eles e os colestéricos é que neles essa característica é imposta, enquanto nos colestéricos ela é permanente.

O cristal líquido nemático girado é um meio opticamente homogêneo anisotrópico (ou seja, suas propriedades variam com a direção) que age localmente como um cristal uniaxial, com o eixo óptico paralelo à direção molecular.

Para facilitar o estudo desses cristais, o dividimos em camadas finas perpendiculares ao eixo de giro, onde cada uma delas age como um cristal uniaxial, com o eixo óptico rodando gradualmente de uma maneira helicoidal (Figura 1.9).



**Figura 1.9:** Propagação da luz em um cristal líquido nemático. Nesse diagrama o ângulo de giro é de  $90^\circ$ .

Devido à sua natureza anisotrópica, os cristais líquidos podem ser utilizados como retardadores de onda ou rotadores de polarização, pois na presença de um campo elétrico externo, sua orientação molecular é modificada, acarretando uma variação da fase, amplitude ou direção de polarização da luz transmitida ou refletida por este. Esses dispositivos são particularmente úteis para tecnologia de displays.

### 1.2.2 Propriedades ópticas dos Cristais Líquidos Nemáticos Girados

A partir das referências [21,35] podemos ver como ocorre a mudança na polarização durante a propagação da luz no cristal líquido: considerando a propagação da luz ao longo do eixo de giro (eixo  $z$ ) de um cristal líquido nemático girado e assumindo que o ângulo de giro varia linearmente com  $z$ ,

$$\theta = \alpha z$$

nesse caso  $\alpha$  é o coeficiente de giro dado em graus/comprimento e o ângulo  $\theta$  corresponde ao ângulo entre o eixo óptico e a direção  $x$ . Por exemplo, em um cristal líquido de tamanho  $d$ , o ângulo de giro é  $\alpha d$ .

O coeficiente de atraso na fase é dado por:

$$\beta = d(n_e - n_o)k_o$$

onde  $n_e$  corresponde ao índice de refração extraordinário, ou seja, índice de refração para a polarização paralela ao plano formado pelo eixo óptico com  $x$  e  $n_o$  corresponde ao índice de refração ordinário, para polarização perpendicular ao eixo óptico. A célula de CL é completamente descrita pelo coeficiente de giro  $\alpha$  e pelo coeficiente de atraso  $\beta$ .

A seguir suporemos que o cristal líquido que tem  $\beta \gg \alpha$ , isto é, vários ciclos de atrasos na fase são introduzidos antes que o eixo óptico gire apreciavelmente. Considere que o cristal líquido de comprimento  $d$  é dividido em  $N$  camadas de larguras iguais  $\Delta z = \frac{d}{N}$ . A posição de cada camada é dada por  $z = z_m = m\Delta z$  e o eixo óptico de cada camada faz um ângulo  $\theta_m = m\Delta\theta$  com o eixo  $x$ , e  $\Delta\theta = \alpha\Delta z$ . O índice  $m$  refere-se a camada  $m$ .

A matriz de Jones para a camada  $m$  é dada por:

$$T_m = R(-\theta_m)T_rR(\theta_m)$$

onde  $T_r$  corresponde a matriz de Jones para o retardo com eixo na direção  $x$ :

$$T_r = \begin{bmatrix} \exp(-in_e k_o \Delta z) & 0 \\ 0 & \exp(-in_o k_o \Delta z) \end{bmatrix}.$$

A matriz  $R(\theta_m)$  corresponde a matriz de rotação para a camada  $m$ :

$$R(\theta_m) = \begin{bmatrix} \cos\theta_m & \sin\theta_m \\ -\sin\theta_m & \cos\theta_m \end{bmatrix}.$$

Reescrevendo  $T_r$  em termos de  $\beta$  e considerando  $(n_e + n_o)k_o/2 = \phi$ , obtemos:

$$T_r = \exp(-i\phi\delta z) \begin{bmatrix} \exp(-i\beta\frac{\Delta z}{2}) & 0 \\ 0 & \exp(i\beta\frac{\Delta z}{2}) \end{bmatrix}.$$

A matriz de Jones resultante do produto das  $N$  camadas em que se foi dividido o cristal líquido é:

$$T = \prod_{m=1}^N T_m = \prod_{m=1}^N R(-\theta_m)T_rR(\theta_m).$$

Como

$$R(\theta_m)R(-\theta_{m-1}) = R(\theta_m - \theta_{m-1}) = R(\Delta\theta)$$

$$\begin{aligned} & \begin{pmatrix} \cos(\theta_m) & \text{sen}(\theta_m) \\ -\text{sen}(\theta_m) & \cos(\theta_m) \end{pmatrix} \begin{pmatrix} \cos(\theta_{m-1}) & \text{sen}(\theta_{m-1}) \\ -\text{sen}(\theta_{m-1}) & \cos(\theta_{m-1}) \end{pmatrix} = \\ & \begin{pmatrix} \cos(\theta_m - \theta_{m-1}) & \text{sen}(\theta_m - \theta_{m-1}) \\ -\text{sen}(\theta_m - \theta_{m-1}) & \cos(\theta_m - \theta_{m-1}) \end{pmatrix}, \end{aligned}$$

temos:

$$T = R(-\theta_N)[T_r R(\Delta\theta)]^N R(\theta_1).$$

com

$$T_r R(\Delta\theta) = \begin{bmatrix} \exp(-i\beta\frac{\Delta z}{2}) & 0 \\ 0 & \exp(i\beta\frac{\Delta z}{2}) \end{bmatrix} \begin{bmatrix} \cos(\alpha\Delta z) & \text{sen}(\alpha\Delta z) \\ -\text{sen}(\alpha\Delta z) & \cos(\alpha\Delta z) \end{bmatrix}.$$

Visto que  $\alpha \ll \beta$ , podemos assumir que  $R(\Delta\theta)$  é aproximadamente uma matriz identidade e obtemos:

$$\begin{aligned} T & \approx R(-\theta_N)[T_r]^N R(\theta_1) = R(-\alpha N\Delta z) \begin{bmatrix} \exp(-i\beta\frac{\Delta z}{2}) & 0 \\ 0 & \exp(i\beta\frac{\Delta z}{2}) \end{bmatrix}^N \\ & = R(-\alpha N\Delta z) \begin{bmatrix} \exp(-i\beta N\frac{\Delta z}{2}) & 0 \\ 0 & \exp(i\beta N\frac{\Delta z}{2}) \end{bmatrix}. \end{aligned}$$

Considerando o limite  $N \rightarrow \infty$ ,  $\Delta z \rightarrow 0$ ,  $N\Delta z \rightarrow d$ , então:

$$T \approx R(-\alpha d) \begin{bmatrix} \exp(-i\beta\frac{d}{2}) & 0 \\ 0 & \exp(i\beta\frac{d}{2}) \end{bmatrix}$$


---

Temos então um atraso  $\beta d$  do eixo lento ao longo da direção  $x$ , seguido por um giro da polarização de  $\alpha d$ . Portanto, vemos que o campo elétrico de um feixe de luz ao ser transmitido por um cristal líquido sofre um deslocamento de fase longitudinal e uma rotação em sua polarização.

Displays de cristal líquido nemático girado (LCDs) têm sido largamente utilizados como moduladores espaciais de luz [28]. Esse tipo de modulador consiste em uma camada muito fina de cristal líquido colocada entre duas placas paralelas de vidro nas quais eletrodos transparentes são padronizados. As moléculas alongadas de cristal líquido são alinhadas ao longo da direção de polimento de uma camada de revestimento para os eletrodos em cada uma das placas de vidro de cobertura e são normalmente organizados com um ângulo de giro determinado pela orientação relativa das duas placas. O ângulo de giro de uma superfície para a outra é em geral de  $90^\circ$ .

Essa estrutura girada gera uma anisotropia óptica macroscópica no LCD. A orientação das moléculas de cristal líquido pode ser modificada aplicando um campo elétrico externo que muda a anisotropia do material produzindo birrefringência que pode ser controlada mudando o campo elétrico aplicado. Para aplicações mais comuns esses dispositivos são usados entre polarizadores lineares cruzados para obter dessa forma modulação de intensidade.

Em geral, os LCDs produzem modulação de fase e de amplitude acopladas como função da voltagem aplicada. Esse efeito de acoplamento deteriora a resposta para elementos ópticos ideais que são projetados para funções de fase ou amplitude, somente. No entanto, recentemente foi mostrado que é possível obter modulação somente de fase ou somente de amplitude usando configurações de polarização elíptica [27].

Recentemente, a fabricação de LCDs evoluiu para a produção de dispositivos com um grande número de pixels que podem ser endereçados individualmente. Dessa forma, é possível controlar a fase ou a amplitude de toda uma frente de onda que incide no modulador, controlando a fase ou a amplitude de cada pequena porção do feixe passando através de cada pixel do LCD.

Em [34] foi mostrado que um SLM pode ser visto como “uma transformação ativa em experimentos de óptica quântica para manipulação de fótons vindo de conversão paramétrica espontânea”.

---

Como o SLM acopla o grau de liberdade espacial do fóton transmitido com sua polarização, através de uma medida projetiva no espaço de Hilbert de polarização, ele permite o controle da transmissão de aberturas que determinam as amplitudes reais dos estados de qudits espaciais. Assim, a superposição coerente de um estado de qudit espacial pode ser modificada considerando a capacidade de modulação de amplitude dos SLMs.

Sabemos que na conversão paramétrica um fóton do feixe de bombeamento (*pump*) origina dois outros com energia mais baixa quando incidimos o feixe de bombeamento em um cristal não linear. Nesse processo, a forma do espectro angular do campo elétrico do feixe *pump* incidente é transferida para o estado de dois fótons gerados pela CPD [25]. A modificação do espectro angular do feixe de laser que gera os pares de fótons permite o controle das propriedades de correlação transversal dos campos convertidos parametricamente.

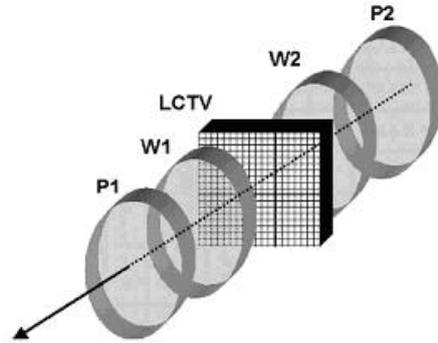
Dessa forma, usando um SLM (composto de dois polarizadores e um display de cristal líquido nemático girado) colocado no caminho de propagação do fóton idler, ficou mostrado que o uso de moduladores espaciais de luz, ao invés de fendas múltiplas pré-fabricadas, para definir o espaço de Hilbert de estados de qudits espaciais é uma técnica vantajosa para gerar novos estados.

Nesse experimento, o fóton signal foi usado como trigger para a detecção do fóton idler, usado para codificar o estado de um qudit de quatro dimensões. Assim, monitorando as contagens de coincidências eles puderam ver como o estado do qudit idler estava sendo modificado pelo SLM. Dessa forma, foi possível usar a capacidade do SLM de fazer modulação de amplitude para alterar, independentemente, cada transmissão nas fendas, modificando o estado inicial de superposição do qudit espacial.

Um LCTV (display de cristal líquido televisivo) colocado entre um conjunto de polarizadores e placas de onda propriamente orientados, como mostrado na Figura 1.10, pode agir somente como modulador de fase [28]. Pela programação das mudanças de fase introduzidas no feixe de iluminação pixel por pixel, é possível gerar uma modulação de fase em toda a frente de onda. Programando diferentes funções de fase espaciais pode-se obter uma mudança de fase total similar àquelas introduzidas por lentes esféricas e cilíndricas.

A possibilidade de programar vários elementos ópticos individualmente

---



**Figura 1.10:** Um LCTV colocado entre um conjunto de polarizadores propriamente orientados (P1,P2) e placas de onda (W1,W2), podem agir como um modulador de fase ou de amplitude, somente [28].

ou simultaneamente é uma característica única que o torna extremamente versátil.

### 1.2.3 LC-R2500

Recentemente, uma nova tecnologia de LCD's, baseados em cristal líquido em silício (LCoS), tem atraído um interesse considerável devido à algumas importantes melhorias na fabricação, levando em muitos aspectos a uma performance superior. Os displays de LCoS são baseados na tecnologia de silício CMOS\*, que permite um display relativamente barato mostrando uma resolução alta. Eles são displays reflexivos que, devido à passagem dupla pelo aparato, permite um aumento dinâmico na gama de modulação, que é especialmente importante em aplicações que requerem uma modulação de fase de uma onda incidente. Simultaneamente, eles têm um tamanho de célula pequeno, que permite uma resposta rápida [33].

No nosso experimento usamos um modulador espacial de luz modelo LC-R2500 (Figura 1.11) produzido pela Holoeye Photonics [37,38]. Ele é cons-

---

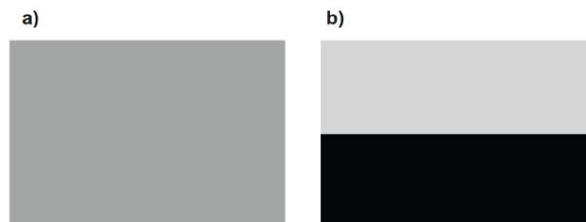
\*CMOS: é uma sigla, em inglês, para semiconductor metal-óxido complementar. É um tipo de tecnologia empregada na fabricação de circuitos integrados onde se incluem elementos de lógica digital, microprocessadores, etc. O “complementary”, em seu nome, vem do fato de que esta tecnologia utiliza os dois tipos de transistores MOSFET, o MOSFET canal N e o MOSFET canal P, de tal modo que um deles “complementa” o outro.

---

tituído de um microdisplay de cristal líquido sobre silício (LCoS) reflexivo monocromático diagonal de 2,46cm do tipo nemático girado de 45°. Os pixels são quadrados com separação de  $19\mu\text{m}$  e resolução XGA (  $1024 \times 768$  pixels), com entrada de dados digitais e escalas de cinza digitalmente controladas com 256 níveis de cinza (GL), de 0 a 255, como mostra a figura 1.12. A comunicação entre o SLM e o computador é feita através de uma saída DVI (Digital Visual Interface) que é conectada na saída de vídeo do computador. O mesmo reconhece o SLM como sendo um segundo monitor. A variação da amplitude e fase é feita através de um programa que utiliza escalas de cinza (GL) como parâmetros de entrada [31].



**Figura 1.11:** LC-R2500 Spatial Light Modulator



**Figura 1.12:** Escalas de cinza. A Fig.(a) mostra uma determinada escala de cinza preenchendo totalmente o display do LCD. Por outro lado, a Fig.(b) mostra duas escalas de cinza dividindo igualmente a tela do display. Imagens como a apresentada na Fig.(b) são utilizadas quando queremos modificar a amplitude ou a fase de um feixe em relação ao outro, quando cada um deles é transmitido por uma das fendas de uma mesma fenda dupla.

Logo, para cada escala de cinza escolhida no programa será associada

uma tensão [21], na qual o pixel do SLM será energizado, provocando um reordenamento das moléculas do display e proporcionando, assim, as alterações de fase e amplitude desejadas.

A relação escala de cinza versus tensão não é linear, por isso o programa possui uma curva Gama. Nessa curva não linear, obtém-se uma variação linear da escala de cinza e da fase. É importante observarmos que a mudança na escala de cinza, ou seja, na fase leva também a uma mudança na polarização da luz refletida.

Esse modulador permite, dependendo da polarização incidente, modular amplitude e fase. Em nosso experimento, porém, usamos elementos ópticos tal que o modulador funciona para uma certa faixa de tensão, apenas como um modulador de fase.

## Capítulo 2

# Conceitos Fundamentais

### 2.1 O Qubit

Um qubit corresponde à unidade fundamental de informação quântica assim como o bit é a unidade fundamental de informação clássica. Ele pode ser implementado fisicamente, mas por hora vamos tratá-lo como um objeto matemático abstrato, para que possa ser construída uma teoria geral da informação quântica que não dependa de um sistema específico para sua implementação [2,10].

Na realização clássica do bit ele é um sistema que é designado a ter dois estados distintos, por exemplo: sim ou não, verdadeiro ou falso, 0 ou 1. Portanto, o análogo quântico do bit, o qubit, também pode ser relacionado ao grau de liberdade de um sistema de dois níveis, por exemplo: a polarização de fótons, estados eletrônicos do átomo, etc. Basicamente, qualquer sistema quântico que tem pelo menos dois estados pode servir como um qubit [8,14].

Um sistema quântico é dito ter  $n$  qubits se o vetor de estado que descreve o sistema quântico é definido em um estado de Hilbert de  $2^n$  dimensões, que possui  $2^n$  estados quânticos mutuamente ortogonais disponíveis. Nós iremos escrever dois estados ortogonais de um qubit como vetores da base  $\{|0\rangle, |1\rangle\}$ . Generalizando,  $2^n$  estados mutuamente ortogonais de  $n$  qubits podem ser escritos como  $\{|i\rangle\}$ , onde  $i$  é um número binário de  $n$ -bits. Por exemplo, para três qubits temos [11]

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}.$$

---

Logo, o qubit é um sistema de dois níveis, descrito em um espaço de Hilbert complexo de duas dimensões, cujos estados podem ser  $|0\rangle$ ,  $|1\rangle$  ou uma combinação linear dos dois:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.1)$$

onde  $\alpha$  e  $\beta$  são complexos. Colocando de outra forma, o estado de um qubit é um vetor em um espaço vetorial complexo de duas dimensões, e  $|0\rangle$  e  $|1\rangle$  são os chamados estados da base computacional, formando uma base ortornormal nesse espaço vetorial [2,4].

Como os vetores da base são definidos a menos de uma fase global, sem significado físico, e  $\alpha$  e  $\beta$  obedecem à condição de normalização,

$$|\alpha|^2 + |\beta|^2 = 1,$$

podemos escolher  $\alpha$  real e positivo, e  $\beta$  complexo (exceto para o estado de base  $|\Psi\rangle = |1\rangle$ , onde  $\alpha = 0$  e  $\beta = 1$  real). Então, o estado genérico de um qubit pode ser escrito como:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, 0 \leq \theta \leq \pi, 0 \leq \phi \leq \pi. \quad (2.2)$$

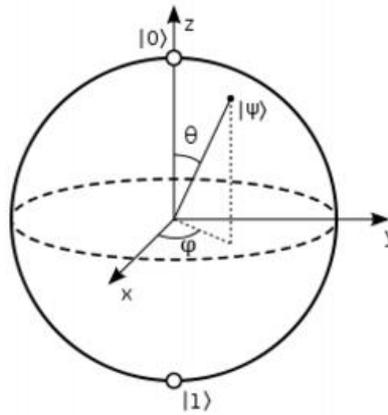
Portanto, o qubit reside num vetor de estado, parametrizado por variáveis contínuas  $\alpha$  e  $\beta$  (ou  $\theta$  e  $\phi$ ). Embora isso pode nos levar a pensar que uma quantidade infinita de informação possa ser armazenado num qubit, de acordo com a mecânica quântica só podemos obter 0 ou 1 quando o medimos. Então, se medirmos um qubit - se fizermos uma medição que projete o qubit na base  $\{|0\rangle, |1\rangle\}$  -, encontraremos o estado 0 com probabilidade  $|\alpha|^2$  ou estado 1 com probabilidade  $|\beta|^2$ . Ou seja, numa única medição obtemos somente um bit de informação sobre o estado do qubit [2,3,8,12].

Dessa forma, devemos ter em mente que os computadores quânticos se sobressaem com relação aos clássicos devido à interferência. O fato que estados quânticos podem ser superposições da base computacional dá origem um paralelismo intrínseco que não está disponível na computação clássica [4,13].

## 2.2 A esfera de Bloch

Quando pensamos em qubits podemos fazer uma outra representação útil, na superfície de uma esfera, conhecida como *esfera de Bloch*. Tal representação nos fornece uma figura geométrica do qubit, assim como das transformações que podemos realizar no seu estado.

Vimos na equação (2.1) que  $\alpha$  e  $\beta$  satisfazem a condição de normalização  $|\alpha|^2 + |\beta|^2 = 1$ . Assim, o estado do qubit pode ser representado por um ponto numa esfera de raio unitário, onde  $\theta$  e  $\phi$  definem esse ponto.



**Figura 2.1:** Representação de um qubit na esfera de Bloch

Podemos, também, pensar na esfera de Bloch num espaço de coordenadas cartesianas de 3 dimensões, tal que o estado (2.2) possa ser escrito da seguinte forma:

$$|\psi\rangle = \begin{bmatrix} \sqrt{\frac{1+z}{2}} \\ \frac{x+iy}{\sqrt{2(1+z)}} \end{bmatrix} \quad (2.3)$$

tendo em mente que  $x = \cos\phi\sin\theta$ ,  $y = \sin\phi\sin\theta$ ,  $z = \cos\theta$ . Assim, as componentes  $(x,y,z)$  do vetor de Bloch indicam um ponto na esfera de Bloch, e eles devem satisfazer a condição de normalização [2,4,9]  $x^2 + y^2 + z^2 = 1$ .

## 2.3 Portas Lógicas

Na computação clássica temos um conjunto de portas elementares que permitem a implementação de qualquer computação complexa. Da mesma forma, a computação quântica possui um conjunto de portas universais, que a partir dessas conseguimos aproximar qualquer outra porta. Isso é o que nos permite não ter que modificar o *hardware* de nossa máquina cada vez que mudarmos nosso problema [2,4,9,14].

Operações unitárias simples em qubits são chamadas ‘portas lógicas’ quânticas [11]. Sabemos que as operações em um qubit devem preservar a condição de normalização  $|\alpha|^2 + |\beta|^2 = 1$ , dessa forma, elas podem ser descritas por matrizes unitárias  $2 \times 2$ . Por exemplo, definindo uma matriz  $X$ :

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.4)$$

e escrevendo o estado  $\alpha|0\rangle + \beta|1\rangle$  sob a forma  $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ , podemos então aplicá-la nesse estado:

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}. \quad (2.5)$$

A única condição imposta sobre uma matriz que representa uma porta quântica é aquela de uma matriz  $U$  unitária, isto é:  $U^\dagger U = I$  onde  $U^\dagger$  é a adjunta de  $U$ , e  $I$  a matriz identidade  $2 \times 2$ . Dessa forma, qualquer matriz unitária determina uma porta lógica quântica válida. O resultado disso é que existem infinitas matrizes unitárias  $2 \times 2$ , ou seja, infinitas portas de um qubit. No entanto, decompondo-as em outras mais elementares é possível aproximar qualquer porta de um qubit [2].

Nesse contexto, temos as matrizes de Pauli, que são exemplos de portas quânticas de um qubit representadas pelas matrizes  $X$  (conhecida como porta quântica NOT),  $Y$  e  $Z$ :

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Outras portas de um qubit são as Hadamard e Fase. Uma transformação unitária move o estado do qubit de um ponto da esfera de Bloch para outro ponto e isso pode ser obtido usando somente as portas Hadamard e a família de portas Fase [4,14].

Todas essas portas agem em um único qubit, e podem ser alcançadas pela ação de algum Hamiltoniano na equação de Schrödinger, já que eles todos são operadores unitários [11].

$$\begin{aligned} \alpha |0\rangle + \beta |1\rangle &\text{ — } \boxed{X} \text{ — } \beta |0\rangle + \alpha |1\rangle \\ \alpha |0\rangle + \beta |1\rangle &\text{ — } \boxed{Z} \text{ — } \alpha |0\rangle - \beta |1\rangle \\ \alpha |0\rangle + \beta |1\rangle &\text{ — } \boxed{Y} \text{ — } i(\beta |0\rangle - \alpha |1\rangle) \end{aligned}$$

**Figura 2.2:** Representação Diagramática de Algumas Portas de um Qubit. Aqui mostramos a ação das portas X, Z e Y, respectivamente, quando as operamos num estado inicial  $\alpha |0\rangle + \beta |1\rangle$ .

A porta Hadamard é uma das portas quânticas mais úteis, e é definida como

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (2.6)$$

Seu papel é transformar a base  $\{|0\rangle, |1\rangle\}$  em uma outra nova base  $\{|+\rangle, |-\rangle\}$ , cujos estados são uma superposição dos estados da base computacional :

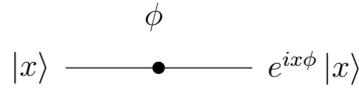
$$\begin{aligned} H |0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \\ H |1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \end{aligned}$$

Como  $H^2 = I$ , a transformação inversa  $H^{-1} = H$ . Note que  $H$  é Hermitiana,  $(H^T)^* = H$ . Na representação da esfera de Bloch, ela equivale a uma rotação da esfera em torno do eixo  $\hat{y}$  de  $90^\circ$ , seguida de uma reflexão sobre o plano  $\hat{x}$ - $\hat{y}$ . Na Figura 2.2 temos a representação diagramática de algumas portas de um qubit.

A porta Fase é definida como

$$R_Z(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}. \quad (2.7)$$

Ela transforma  $|0\rangle$  em  $|0\rangle$  e  $|1\rangle$  em  $e^{i\delta}|1\rangle$ . Sua ação é mostrada na Figura 2.3. Como fases globais não tem nenhum significado físico, os estados da base computacional  $|0\rangle$  e  $|1\rangle$ , permanecem inalterados. Já que, de acordo com os postulados da mecânica quântica, fases relativas são observáveis, estados genéricos são mudados pela aplicação da porta Fase [2,4].



**Figura 2.3:** Representação Diagramática da Porta Fase

A Não-Controlada (CNOT, do inglês *Controlled NOT*) é uma das portas quânticas mais importantes, sendo um exemplo de porta no espaço de dois qubits. Ela é definida na base computacional como  $|x\rangle|y\rangle \rightarrow |x\rangle|x \oplus y\rangle$ , onde o símbolo  $\oplus$  significa soma módulo dois, ou seja,  $1 \oplus 1 = 0$ ,  $0 \oplus 0 = 0$ ,  $1 \oplus 0 = 1$  e  $0 \oplus 1 = 1$ . Assim,

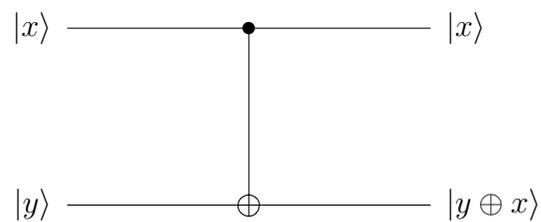
$$\begin{aligned} U_{CNOT} |00\rangle &= |00\rangle, U_{CNOT} |01\rangle = |01\rangle, \\ U_{CNOT} |10\rangle &= |11\rangle, U_{CNOT} |11\rangle = |10\rangle. \end{aligned}$$

Onde a forma matricial é dada por:

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (2.8)$$

Podemos observar que a porta ficará apta quando o primeiro qubit, o controle, estiver no estado  $|1\rangle$  lógico, permitindo a mudança do estado lógico do segundo qubit, o alvo.

A representação diagramática da porta  $U_{CNOT}$  é mostrada na Figura 2.4, onde as linhas nos circuitos quânticos representam uma evolução temporal.



**Figura 2.4:** Representação Diagramática da Porta  $U_{CNOT}$ .

Ressaltamos que uma computação universal pode ser realizada com este conjunto de portas (Hadamard, Fase e CNOT) [2].

Resumindo, uma seqüência de portas quânticas atuando sobre vários qubits determina um circuito quântico. Após o processamento dos qubits realizamos a leitura desses por meio de medições projetivas ou generalizadas [14].

## Capítulo 3

# O Problema de Deutsch

Uma máquina de computação é qualquer sistema físico cuja evolução dinâmica parte de um conjunto de estados de entrada para um conjunto de estados de saída. Os estados são “etiquetados” de alguma maneira canônica, onde a máquina é preparada com alguma marcação de entrada e, da mesma forma, o estado de saída é medido [45].

Qualquer tarefa realizada por um computador segue um algoritmo, ou seja, um conjunto abstrato de instruções. Um algoritmo clássico pode ser descrito como uma seqüência de operações lógicas realizadas em uma seqüência de bits, governadas pelas leis da mecânica clássica. Já os algoritmos quânticos são seqüências de evoluções unitárias realizadas em qubits, que podem existir como uma superposição de seqüências clássicas [44]. Ou seja, um algoritmo quântico é qualquer processo físico que utiliza efeitos quânticos para realizar tarefas computacionais úteis [8].

A computação quântica baseia-se no processamento de bits de informação que podem ser superposições de 0's e 1's lógicos. Enquanto a coerência mútua entre um conjunto qubits é preservada [57], eles podem simultaneamente tomar mais de um valor, usufruindo de um fenômeno conhecido como paralelismo quântico. Assim, algoritmos podem ser planejados tomando vantagem desse efeito para resolver alguns problemas mais rapidamente do que com um computador clássico [48]. Dessa forma, os algoritmos quânticos têm um ganho sobre os clássicos, já que podem realizar algumas tarefas com muito mais rapidez.

---

No entanto, como já mencionamos anteriormente, quando um qubit é observado por um agente externo, a coerência com outros qubits do sistema é parcialmente perdida. Essa perda de coerência faz com que não possamos acessar toda informação que estaria contida nele [59]. Desse modo, a praticidade de usar o paralelismo quântico é dependente da nossa habilidade de construir uma máquina capaz de preservar a coerência quântica durante os cálculos [48,60].

Então, a questão chave para a viabilidade de computadores quânticos é manter a coerência quântica numa implementação real. Para isso, os dispositivos lógicos, o esquema para sua interconexão, e o método para preparar e extrair as entradas e saídas do computador devem ser tais que consigam isso [15,48].

### 3.1 Paralelismo Quântico

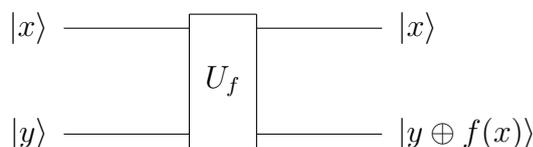
O paralelismo quântico é o que possibilita, por exemplo, calcular uma certa função  $f(x)$  para vários valores de  $x$  ao mesmo tempo. Isto nos é permitido, pois a mecânica quântica aceita estados superpostos, e assim, podemos executar a operação  $f(x)$  sobre um estado  $x$  composto pela superposição linear de vários outros estados, diferentemente do paralelismo clássico, no qual vários circuitos diferentes são acionados simultaneamente para calcular  $f(x)$ , para diferentes valores de  $x$ . No entanto, não é possível extrair todas essas informações com uma única medida.

Imagine uma função  $f(x) : \{0,1\} \rightarrow \{0,1\}$  de um único bit, domínio e imagem. Com a computação atual podemos determinar o valor de  $f(x)$  substituindo  $x$  por qualquer um dos valores contido em seu domínio. Mas só poderemos fazer esse cálculo para um único valor de  $x$  por vez [2,9].

Em um computador quântico, a computação de  $f(x)$  corresponde a uma evolução unitária  $U_f$ , definida pelo mapeamento  $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ , em que  $\oplus$  indica a adição de módulo 2. O primeiro registro ( $x$ ) é chamado de registro de “dados”, e o segundo ( $y$ ) de “registro alvo” (Figura 3.1).

A entrada  $|x\rangle$  é carregada para garantir que  $U_f$  seja unitária para todo  $f(x)$  possível. Se  $y = 0$ , o estado final do segundo qubit é justamente  $f(x)$ .

---



**Figura 3.1:** Imagem da transformação unitária  $U_f$  correspondendo a avaliação da função  $f(x)$ . As linhas superiores e inferiores representam os registros dados e alvo, respectivamente.

Agora, suponha que o registro de dados seja ajustado como uma superposição de valores, digamos,  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  (que pode ser criada por uma porta Hadamard atuando sobre o estado  $|0\rangle$ ). Então, aplicando  $U_f$  temos,

$$U_f |x\rangle \otimes |0\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}. \quad (3.1)$$

Podemos ver que os termos dessa soma contêm informação sobre ambos  $f(0)$  e  $f(1)$ , como se tivéssemos avaliado  $f(x)$  para dois valores de  $x$  simultaneamente, um efeito denominado “paralelismo quântico”. Contudo, esse paralelismo não é de utilidade imediata. Para se tornar útil, a computação quântica requer algo mais além do simples paralelismo; ela requer a capacidade de extrair a informação da resposta obtida, pois em geral, esta também estará em um estado superposto [2,8,9].

Note que o estado de saída é um estado emaranhado dos registros de entrada e saída. De fato, o fenômeno de superposição é uma característica de sistemas clássicos lineares e qualquer efeito dependendo somente de superposição pode ser facilmente implementado em um sistema clássico. No entanto, o fenômeno de emaranhamento\* quântico não tem análogo clássico e seu papel fundamental na computação quântica tem sido discutido e elaborado [8,56,58].

---

\*Um estado quântico puro  $|\Psi\rangle$  num espaço de Hilbert  $H$  de  $n$  qubits é dito ser separável (com respeito aos espaços fatores  $\{H_1, H_2, \dots, H_n\}$ ) quando pode ser fatorado como se segue:  $|\Psi\rangle = \prod_{i=1}^n |\psi_i\rangle$ , onde  $|\psi_i\rangle \in H_i$ . Caso contrário, o estado é chamado *emaranhado*. O emaranhamento permite que dois ou mais objetos estejam de alguma forma tão ligados tal que um não possa ser corretamente descrito sem que a sua contra-parte seja mencionada, mesmo que os objetos possam estar espacialmente separados. Para mais informações, ver [44,62].

---

## 3.2 O Problema de Deutsch

O problema de Deutsch foi proposto por Deutsch [45], e a solução para um bit foi dada no mesmo artigo. A extensão para o caso geral de  $n$  bits foi dada por Deutsch e Jozsa [47]. Os algoritmos nesses primeiros trabalhos foram melhorados substancialmente por Cleve, Ekert, Macchiavello e Mosca [61].

O algoritmo original de Deutsch funciona somente de forma probabilística; Deutsch e Jozsa avançaram no problema para obter um algoritmo determinístico, mas o método deles precisava avaliar a função duas vezes, em contraste com os algoritmos aprimorados existentes. No entanto, convencionou-se referir-se a esses algoritmos como os algoritmos de Deutsch e de Deutsch-Jozsa, em homenagem aos dois imensos passos que foram dados: a demonstração concreta por Deutsch de que um computador quântico poderia fazer alguma coisa mais rapidamente do que um clássico, e a extensão por Deutsch e Jozsa que demonstraram pela primeira vez que essa economia de tempo podia ser escalada para sistemas maiores [2]. Essa economia de tempo se dá quando estamos comparando o algoritmo de Deutsch com o algoritmo clássico determinístico. Mas se considerarmos o algoritmo clássico probabilístico temos aí outro problema.

O problema de Deutsch foi descrito por Chuang [48] como o seguinte jogo. Alice, em Amsterdã, seleciona um número  $x$  de 0 a  $2^n - 1$ , e o manda em uma carta para Bob, em Boston. Bob calcula alguma função  $f(x)$  e a responde com o resultado, que é ou 1 ou 0. Agora, Bob concordou usar somente dois tipos de função, ou do tipo 1, que é constante para todos os valores de  $x$ , ou do tipo 2, que é balanceada, no sentido que será igual a 1 para exatamente metade dos valores de  $x$ , e 0 para a outra metade. A missão de Alice é determinar com certeza que tipo de função Bob escolheu correspondendo com ele o menor número de vezes. Quão rápido ela pode conseguir isso?

No caso clássico, Alice pode mandar para Bob somente um valor de  $x$  em cada carta. Na pior situação, Alice precisará consultar Bob pelo menos  $\frac{2^n}{2} + 1$  vezes, já que ela pode receber, por exemplo,  $\frac{2^n}{2}$  zeros antes de finalmente receber um 1, dizendo a ela que a função de Bob é do tipo 2. O melhor algoritmo clássico que ela pode usar, portanto, requer  $\frac{2^n}{2} + 1$  consultas. Note que em cada carta, Alice manda para Bob  $n$  bits de informação.

---

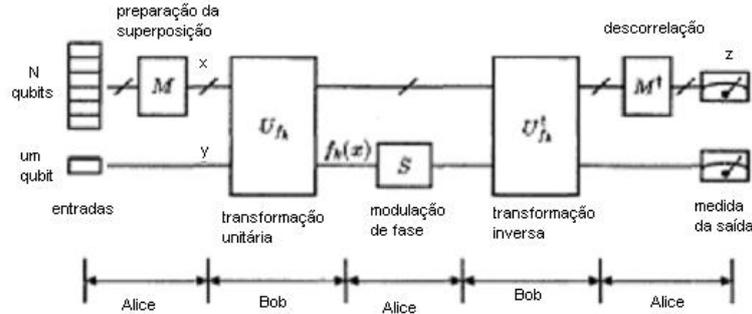
Agora adicionamos uma novidade ao problema. Suponha que Bob e Alice podem trocar bits quânticos (ao invés de somente bits clássicos), e ainda, Bob calcula  $f(x)$  usando uma transformação unitária  $U_f$ . Alice pode agora ter de volta mais de um valor de  $f(x)$  de Bob numa única consulta. Por exemplo, Alice pode mandar para Bob uma armadilha de átomos contendo  $n + 1$  átomos de dois níveis. Os primeiros  $n$  átomos, representando  $x$ , são preparados em uma superposição igual dos seus estados fundamentais e excitados, enquanto o último átomo, um bloco de rascunho para o resultado  $y = f(x)$ , é colocado no seu estado fundamental. Em Boston, Bob usa uma seqüência de pulsos eletromagnéticos para colocar o átomo  $y$  unitariamente no estado  $f(x)$ . Note que  $x$  é uma superposição de todos os valores  $[0, 2^n - 1]$ , e, portanto,  $y$  é deixado em uma superposição de todos os valores possíveis de  $f(x)$ . Contudo, quando Alice recebe a resposta, ela não pode alcançar sua missão simplesmente medindo o átomo  $y$ , já que isso iria colapsar o estado de superposição e dar a ela somente um resultado.

Alice deve ser mais esperta. Ela dá a  $y$  uma fase  $\pi$ , então manda os qubits mais uma vez para Bob. Dessa vez, Bob concorda em calcular  $U_f^+$  ao invés de  $U_f$ , isto é, ele inverte o que ele fez anteriormente, deixando  $y$  no seu estado fundamental. Como  $y$  e  $x$  são emaranhados, esse procedimento também deixa  $n$  qubits de  $x$  com uma fase relativa especial, tal que aqueles valores de  $x$  para qual  $f(x)$  é ímpar, estão  $180^\circ$  fora de fase com os outros valores. Quando Alice recebe o resultado de volta de Bob, ela pode realizar um experimento de interferência para determinar que tipo de função Bob usou, com certeza. Isso é feito usando somente duas consultas.

O único algoritmo quântico seguido por Alice no último caso foi planejado por Deutsch e Jozsa, e uma descrição mais matemática pode ser achada no artigo deles [47]. Um algoritmo esquemático é mostrado na Fig.3.2. Esse desenho e nossa descrição acima destaca as duas diferenças principais entre computação clássica e quântica: (1) informação é representada como bits quânticos, e (2) informação de interações são realizadas usando transformações unitárias. Essas duas mudanças permitem que o problema de Deutsch seja resolvido em um tempo  $O(N)$ , ao invés de um tempo  $O(\exp N)$ . No nosso exemplo, a separação espacial foi usada para elevar artificialmente o custo de calcular  $f(x)$ ; isso não é preciso em geral, onde  $f(x)$  pode ser inerentemente

---

difícil de ser calculada. Nós devemos estudar em seguida como qubits podem ser, em geral, manipulados, interagidos e medidos.



**Figura 3.2:** Algoritmo para resolver o problema de Deutsch usando um computador quântico.

Assim, podemos descrever o problema de Deutsch da seguinte forma: nos é dada uma caixa preta, ou oráculo\*, que implementa a seguinte função  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  e queremos descobrir se esta é constante (retorna sempre 0 ou sempre 1, independentemente da entrada) ou balanceada (o número de vezes que retorna 0 é igual ao número de vezes que retorna 1). Matematicamente, estamos buscando uma propriedade global da função [9].

### 3.3 Algoritmo de Deutsch

O algoritmo de Deutsch talvez seja o exemplo mais simples de um algoritmo quântico que supera um algoritmo clássico. Ele combina o paralelismo quântico com uma outra propriedade conhecida como interferência [2,44].

Na verdade, ele não possui nenhuma aplicação computacional, como o algoritmo de Shor ou Grover, apenas resolve um problema hipotético mostrando o ganho computacional sobre a versão clássica, ou seja, foi criado para mostrar que quanticamente teríamos alguma vantagem sobre a computação clássica [9].

\*O oráculo é uma maneira formal de descrever quantos passos um algoritmo toma; ele é uma função  $f$ , e o número de passos que um algoritmo toma é o número de vezes que  $f$  é avaliado [44].

O algoritmo de Deutsch é um caso particular do algoritmo de Deutsch-Jozsa. Considere uma caixa preta avaliando uma função Booleana\* de um bit  $f : \{0, 1\} \rightarrow \{0, 1\}$ . Há quatro funções, que se diferem na seguinte propriedade global: duas são constantes,

$$\left\{ \begin{array}{l} f(0) = 0 \\ f(1) = 0 \end{array} \right. \text{ ou } \left\{ \begin{array}{l} f(0) = 1 \\ f(1) = 1 \end{array} \right. ,$$

e duas balanceadas,

$$\left\{ \begin{array}{l} f(0) = 0 \\ f(1) = 1 \end{array} \right. \text{ ou } \left\{ \begin{array}{l} f(0) = 1 \\ f(1) = 0 \end{array} \right. .$$

O problema, então, é decidir se uma dada função é constante ou balanceada.

Podemos, também, pensar no problema como o de decidir se uma moeda é normal ou fraudada, onde a moeda é representada por uma função  $f$  que pode tomar como entrada 0 ou 1, e  $f(0)$  representa um lado da moeda,  $f(1)$  o outro. Se a moeda é normal, então os dois lados da moeda são diferentes  $f(0) \neq f(1)$ . Se a moeda é fraudada, ambos os lados são os iguais  $f(0) = f(1)$  [44].

Classicamente, a solução desse problema requer, necessariamente, duas consultas ao oráculo, ou seja, ambos lados da moeda são examinados para determinar se a moeda é normal ou fraudada usando duas avaliações de  $f$ .

Já um computador quântico pode resolver o mesmo problema somente com uma consulta, ou seja, o algoritmo de Deutsch olha ambos lados da moeda numa superposição e determina se ela é normal ou fraudada em somente uma avaliação da função  $f$ .

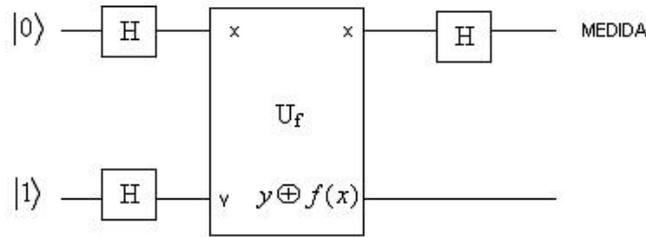
O circuito quântico que implementa o algoritmo de Deutsch é mostrado na Fig.3.3.

Assim como descrito em [4], a função  $f(x)$  é avaliada em computação reversível usando um qubit auxiliar  $|y\rangle$ . A transformação unitária  $U_f$  transforma  $|x\rangle|y\rangle$  em  $|x\rangle|y \oplus f(x)\rangle$ ; isto é, ela modifica o segundo qubit se, e somente se,  $f(x) = 1$ .

---

\*Função Booleana: é uma função do tipo  $f : X \rightarrow B$ , onde  $X$  é um conjunto arbitrário e  $B$  é um domínio booleano. Um domínio booleano  $B$  é um conjunto genérico de 2 elementos, por exemplo,  $B = \{0, 1\}$  cujos elementos são interpretados como valores lógicos, por exemplo, 0 e 1 [63].

---



**Figura 3.3:** Circuito quântico para implementar o algoritmo de Deutsch

O estado inicial dos qubits é  $|\psi_0\rangle = |0\rangle |1\rangle$ . Então, uma porta Hadamard prepara o primeiro qubit na superposição  $(|0\rangle + |1\rangle)/\sqrt{2}$ . Isso irá permitir o computador quântico avaliar ambas  $f(0)$  e  $f(1)$  em uma única rodada. Outra porta Hadamard prepara o qubit auxiliar em  $(|0\rangle - |1\rangle)/\sqrt{2}$ . Isso é fundamental, já que para cada  $x \in \{0, 1\}$  temos

$$U_f |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (3.2)$$

Então, o estado do computador quântico depois da avaliação da função é

$$\frac{1}{\sqrt{2}} [(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle] \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (3.3)$$

O segundo qubit não é mais usado e a partir de agora nós vamos ignorá-lo. A última porta Hadamard deixa o primeiro qubit no estado

$$\frac{1}{2} \{ [(-1)^{f(0)} + (-1)^{f(1)}] |0\rangle + [(-1)^{f(0)} - (-1)^{f(1)}] |1\rangle \}. \quad (3.4)$$

Se  $f(0) = f(1)$ , esse estado é igual a  $|0\rangle = |f(0) \oplus f(1)\rangle$ . Se ao invés  $f(0) \neq f(1)$ , esse estado é  $|1\rangle = |f(0) \oplus f(1)\rangle$ . Em qualquer caso, nós escrevemos o estado final do primeiro qubit como

$$|f(0) \oplus f(1)\rangle.$$

Então, uma medição do primeiro qubit dá com probabilidade 1 a saída 0 se a função é constante e a saída 1 se a função é balanceada. Portanto, uma propriedade global da função  $f(x)$  foi codificada num único qubit depois de uma única chamada de  $f$ . Isso porque um computador quântico pode avaliar ambas  $f(0)$  e  $f(1)$  simultaneamente. O ponto principal aqui é que esses dois

caminhos alternativos são combinados pela porta Hadamard final, dando o padrão de interferência desejado.

Essa computação quântica, embora seja extremamente simples, contém todas as principais características de algoritmos quânticos bem sucedidos [61].

### 3.4 Algoritmo de Deutsch-Jozsa

Agora, para resolver o problema de Deutsch, vamos considerar o algoritmo de Deutsch-Jozsa, que é uma generalização para  $n$  qubits do algoritmo de Deutsch. Logo, temos uma função binária  $f(x) : \{0, 1\}^n \rightarrow \{0, 1\}$ , que é constante ou balanceada, e desejamos determinar, consultando o oráculo, se ela é constante ou balanceada [4].

Isso pode ser resolvido por um algoritmo quântico que requer somente uma avaliação de  $f$ , em contrapartida ao clássico, que precisa avaliar a função  $2^{N-1} + 1$  vezes. Para isso, precisamos de um sistema físico bem definido, chamado de registro total (que é usado para armazenar e recuperar a informação), e de uma seqüência de transformações para serem promulgadas no registro total de tal maneira que produza uma resposta para o problema [51].

O registro total consiste de  $n$  qubits como registro de controle, que é geralmente usado para armazenar os argumentos da função, mais um qubit usado como função registradora, que é usada para avaliar a função. Então, o espaço de Hilbert para o registro total é

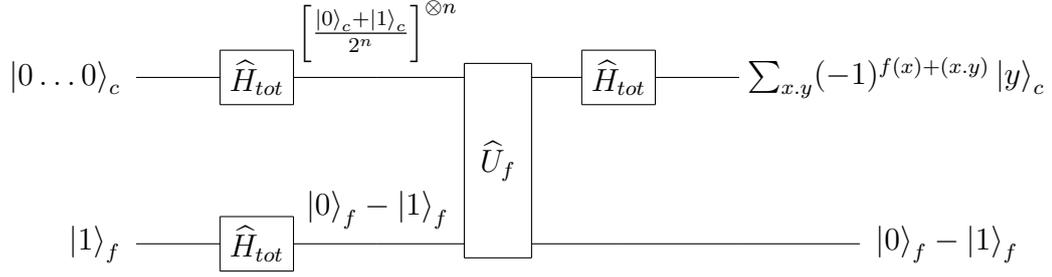
$$H_{total} = H_c \otimes H_f \quad (3.5)$$

onde  $H_c$  é o espaço de Hilbert para o registro de controle e  $H_f$  para a função registradora.

O algoritmo faz o uso do registro total dado na equação (3.5), e segue o mesmo circuito quântico que resolve o algoritmo de Deutsch, mas com  $n$  qubits para armazenar a entrada  $x = x_{n-1}, x_{n-2}, \dots, x_0$ , como mostrado na figura 3.4.

As portas Hadamard são agora aplicadas em paralelo a todos  $n$  qubits,

$$H^{\otimes n} = H \otimes H \otimes \dots \otimes H. \quad (3.6)$$



**Figura 3.4:** Circuito quântico esquematizando o algoritmo de Deutsch - Jozsa.  $\hat{H}_{tot}$  representa uma transformação Hadamard aplicada em cada qubit do registro de controle.  $\hat{U}_{f-c-N}$  representa a operação da porta  $f$ -controlled-NOT.

Isso transforma o estado de entrada  $|0 \dots 0\rangle_c$  em uma superposição sobre todos elementos da base, preparando o caminho para uma avaliação simultânea de  $f$  sobre todos argumentos possíveis.

É fácil checar que a ação de  $H^{\otimes n}$  num estado  $|x\rangle$  da base computacional dá

$$H^{\otimes n} |x\rangle = \prod_{i=0}^{n-1} \left( \frac{1}{\sqrt{2}} \sum_{y_i=0}^1 (1)^{x_i y_i} |y_i\rangle \right) = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \quad (3.7)$$

onde  $x \cdot y$  denota o produto interno de  $x$  e  $y$ , módulo 2 :

$$x \cdot y = x_{n-1}y_{n-1} \oplus x_{n-2}y_{n-2} \oplus \dots \oplus x_0y_0.$$

O circuito na figura 3.4 aplica uma transformação

$$(H^{\otimes n} \otimes H)U_f(H^{\otimes n} \otimes H)$$

ou seja, a porta  $f$ -controlled- NOT,  $\hat{U}_{f-c-N}$ , que faz a avaliação da função, cuja operação numa base ortornormal de  $H_{tot}$  é

$$\hat{U}_{f-c-N} |x\rangle_c |y\rangle_f := |x\rangle_c |y \oplus f(x)\rangle_f,$$

é aplicada, resultando em

$$\left( \frac{1}{2^{n-1}} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot y} |y\rangle \right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (3.8)$$

Isso implica que, no final do circuito, uma medida dos  $n$  qubits na base computacional dá o estado  $|00\dots 0\rangle$  com probabilidade 1 se  $f$  é constante e com probabilidade 0 se  $f$  é balanceada. Portanto, uma única rodada do algoritmo, com uma única consulta a função  $f(x)$ , determina com certeza se  $f$  é constante ou balanceada.

### 3.5 Novo Algoritmo

Em 1998, Collins et al [51], propuseram um novo algoritmo que simplificava o algoritmo de Deutsch - Jozsa eliminando uma redundância nesse.

De acordo com o que vimos anteriormente podemos observar que o único ponto que o emaranhamento entre qualquer um dos qubits do registro total pode ocorrer é durante a avaliação da função [51]. No entanto, também é aparente que a função registradora está no estado  $\frac{1}{\sqrt{2}} [ |0\rangle_f - |1\rangle_f ]$  antes e depois desse passo. Na verdade, é fácil mostrar que

$$\widehat{U}_{f-c-N} |x\rangle_c \frac{1}{\sqrt{2}} [ |0\rangle_f - |1\rangle_f ] = (-1)^{f(x)} |x\rangle_c \frac{1}{\sqrt{2}} [ |0\rangle_f - |1\rangle_f ] \quad (3.9)$$

o que implica que a função registradora do estado de entrada é restrita ao subespaço calibrado por  $[ |0\rangle_f - |1\rangle_f ]$ . Então, não há emaranhamento entre o controle e a função registradora na saída de  $\widehat{U}_{f-c-N}$ .

Logo, não é necessário nenhum acoplamento entre o sistema de dois estados que compreendem o registro de controle e que compreendem a função registradora. Ou seja, a função registradora é redundante.

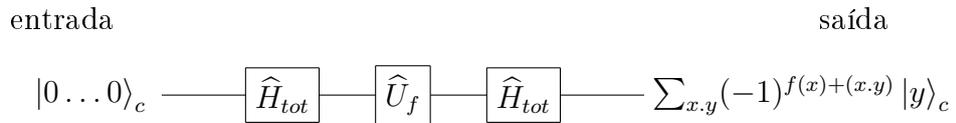
Isso sugere que o algoritmo pode ser modificado eliminando a função registradora enquanto retém o registro de controle do algoritmo anterior. Então, o registro total fica  $H_{total} = H_c$ .

A equação (3.9) sugere que a função avaliação pode ser executada através da porta  $f$ -controlada, cuja operação nos elementos da base do registro de controle é definida como:

$$\widehat{U}_f |x\rangle_c = (-1)^{f(x)} |x\rangle_c. \quad (3.10)$$

De fato, é fácil ver que o efeito de  $\widehat{U}_{f-C-N}$  é idêntico ao de  $\widehat{U}_f \otimes \widehat{I}_f$ , onde  $\widehat{I}_f$  é a identidade em  $H_f$ . Note que isso é inválido para a maioria dos elementos de  $H_c \oplus H_f$ , mas é verdade sempre que o estado de entrada da função registradora está num subespaço calibrado por  $[|0\rangle_f - |1\rangle_f]$ . Claramente,  $\widehat{U}_f$  satisfaz o requerimento que uma porta deve ser um operador unitário.

Um esquema do algoritmo de Collins é mostrado na Figura 3.5:



**Figura 3.5:** Algoritmo proposto por Collins *et al.* A notação é a mesma da figura 3.4 com a porta *f-controlled* no lugar da porta *f-controlled-NOT*.

Note que este algoritmo requer de fato um qubit a menos. Ou seja, a implementação física requer um sistema de 2 estados a menos.

Assim, podemos concluir que é possível a simplificação do algoritmo existente eliminando a função registradora e redefinindo a função avaliação em termos da porta *f-controlled*.

## Capítulo 4

# O Experimento

Neste trabalho demonstramos o algoritmo de Deutsch-Jozsa com um qubit, usando pares de fótons gerados pela conversão paramétrica descendente, ou fótons gêmeos.

Assim como proposto por Collins et al [51], a implementação do algoritmo de Deutsch-Jozsa com um qubit foi feita removendo uma redundância existente nele, reduzindo o tamanho do registro e simplificando a função avaliação.

### 4.1 Montagem Experimental

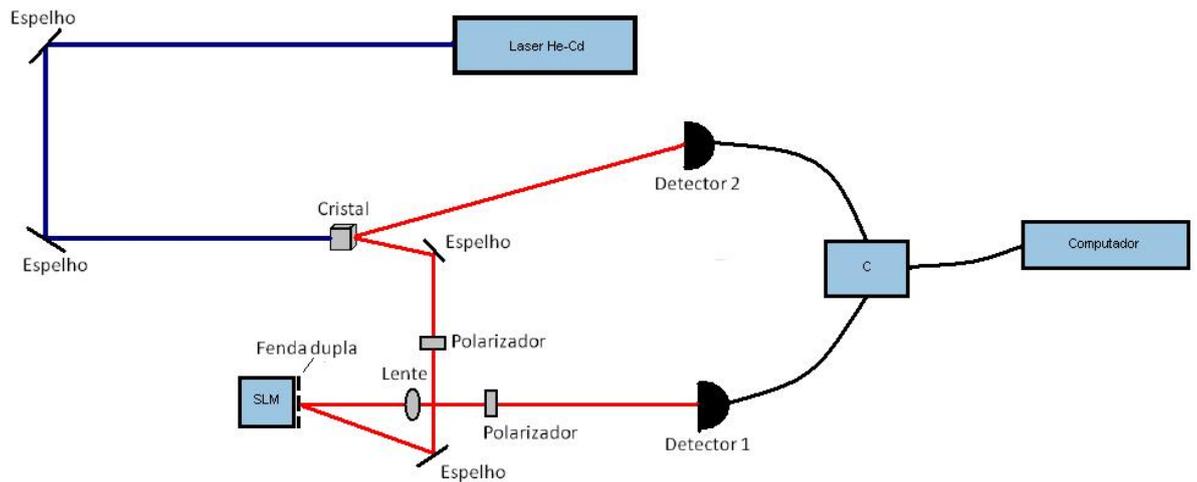
Para realização do experimento usamos o aparato experimental ilustrado na Figura 4.1. Aqui, o feixe de laser de HeCd ( $\lambda = 351nm$ ) incidia em um cristal  $LiIO_3$  tipo I, e pela conversão paramétrica descendente gerava um par de fótons. Um deles era usado como *trigger*\* sendo enviado diretamente para o detector 2, enquanto o outro atravessava uma fenda dupla com separação de  $200\mu m$  e largura das fendas de  $100\mu m$ , saindo em um estado de superposição de caminhos, isto é, um qubit.

---

\*Dizer que estamos usando um dos fótons como trigger equivale a dizer que estamos fazendo o experimento com um fóton do par enquanto o outro incide diretamente em outro detector. Assim, as contagens dos fótons são feitas em coincidências, ou seja, quando no mesmo intervalo de tempo incidirem fótons em ambos detectores sabemos que aqueles são os fótons gêmeos.

---

Usando um modulador espacial de luz (SLM) para colocar fases no caminho dos fótons, e detectando em coincidência, demonstramos o algoritmo de Deutsch-Jozsa com fótons usando apenas um qubit.



**Figura 4.1:** Aparato experimental usado para implementar o algoritmo de Deutsch - Jozsa com um qubit.

Os polarizadores colocados antes e depois do SLM foram utilizados para garantir que a polarização permaneceria a mesma, já que esse não modula somente a fase, mas muda também a polarização. A lente com distância focal  $f$  de  $10\text{cm}$  localizada a uma distância  $f$  do detector foi usada para focalizar os fótons de modo a produzir o padrão de interferência no plano do detector. Dessa forma, o detector 1 era posicionado no plano de Fourier da lente [35]. O ângulo de incidência entre o feixe e a normal do SLM é de aproximadamente dois graus para evitar difração. Cada um dos fótons do par atingia um detector que possuía filtros de interferência centrados em  $(650 \pm 10)\text{nm}$  e uma fenda simples de  $100\mu\text{m}$  de espessura.

*Pin-holes*, que não estão representados na figura, foram utilizados para delimitar o caminho dos fótons e para ajudar o alinhamento, juntamente com um laser de *HeNe*. Fizemos este laser passar pelo mesmo caminho dos fótons gêmeos com a ajuda dos *pin-holes* que estavam fixos pelo caminho. Isso é importante pois assim o alinhamento de lentes, polarizadores e placas torna-se mais simples [31].

No experimento, o SLM modificava o caminho dos fótons acrescentando fases espaciais e a sua função na montagem é o de gerador de funções constantes ou balanceadas. Como a função do algoritmo é determinar se uma função é constante ou balanceada, tínhamos então quatro possibilidades para o caso de um qubit: 1) a ambos caminhos foram acrescentados fase zero ou 2) fase  $\pi$ , representando as duas funções constantes; 3) ao caminho superior foi acrescentado fase  $\pi$  e no inferior fase 0 ou 4) fase 0 ao superior e fase  $\pi$  ao inferior, representando as duas funções balanceadas. Ou seja, o que precisamos é a capacidade de preparar estados  $|0\rangle$  e  $|1\rangle$  e detectar uma propriedade global sobre eles, no caso, a informação sobre a fase.

Como sabemos que o SLM é versátil a ponto de podermos modificar o feixe da luz incidente em determinados pontos, o que tínhamos que fazer, então, era colocar as fases de 0 e  $\pi$  em pontos correspondentes às fendas da fenda dupla, simulando as funções balanceadas e constantes. Ou seja, fazemos do SLM o oráculo do circuito. No entanto, aqui sabemos qual função, constante ou balanceada, pode ser escolhida a priori. O objetivo do experimento é a confirmação do esquema experimental para implementação do algoritmo de Deutsch com um qubit nas variáveis espaciais.

Desse modo, ao medirmos as contagens de coincidências num determinado tempo, o resultado obtido esperado seria de interferência construtiva para as funções constantes e interferência destrutiva para as funções balanceadas.

Em um esquema ideal, deixando os detectores fixos no centro do padrão de interferência detectaríamos zero coincidências no segundo caso e um número de coincidências dependente do fluxo de pares no primeiro.

## 4.2 Calibração do SLM

Em geral, quando LCDs comerciais são usados, o pesquisador não tem acesso aos valores de um conjunto de parâmetros que definem as propriedades de modulação eletro-ópticas do dispositivo de cristal líquido. Por isso, foram propostos uma série de modelos, usualmente baseados no formalismo de polarização das matrizes de Jones [32,39–43], para descrever as capacidades dos LCDs. O formalismo das matrizes de Mueller, que fornece uma alternativa para descrição dos fenômenos de polarização, também foi aplicado para

---

calibrar a resposta dos LCDs [33].

Em nosso laboratório fizemos duas calibrações. Na primeira utilizamos um interferômetro de Michelson, como mostrado na Figura 4.2(a), e comparamos os resultados com os obtidos quando uma fenda dupla é usada para gerar interferência, Figura 4.2(b).

Um laser de He-Ne ( $\lambda = 632nm$ ) passa por um polarizador de entrada a  $45^\circ$ . Depois, incide sobre um divisor de feixes (BS - do inglês, *beam splitter*) sendo dividido em dois feixes com 50% da intensidade do valor inicial. Na figura 4.2(a) um dos feixes segue em direção ao SLM, onde sua intensidade pode ser modificada, e o outro segue em direção a um espelho metálico onde é refletido sem sofrer alterações. Após se reencontrarem no BS eles passam por uma lente com a finalidade de focalizar os fótons de modo a produzir um padrão de interferência no plano do detector. Já no caso da figura 4.2(b), o feixe que iria em direção ao espelho foi bloqueado e logo em frente ao SLM foi colocada uma fenda dupla.

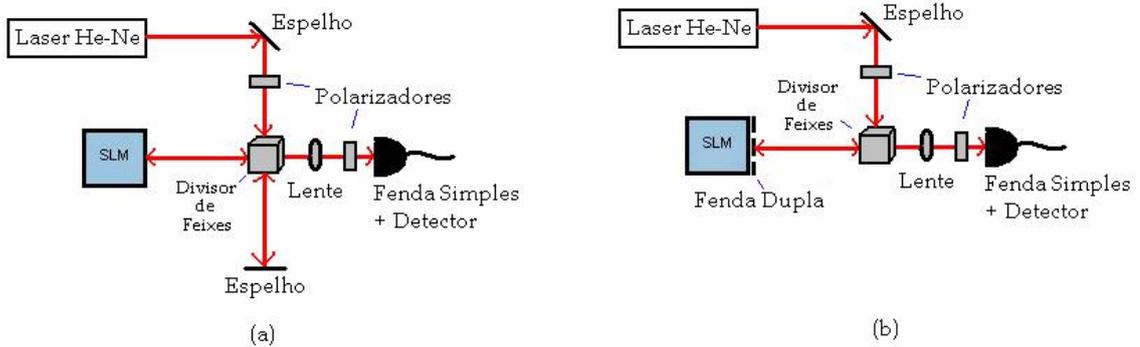
Nos dois interferômetros temos uma função do co-seno da mudança de fase em função das intensidades. Como sabemos que a intensidade em um dos braços do interferômetro de Michelson muda como função da escala de cinza, podemos obter a variação da diferença de fase em função do nível de cinza. A expressão teórica para a diferença de fase entre os dois caminhos é:

$$\Delta\phi = \cos^{-1}\left[\frac{I - I_1 - I_2}{2\sqrt{I_1 I_2}}\right]$$

onde  $I$  é a intensidade total obtida quando os dois feixes estão desbloqueados e  $I_1$  e  $I_2$  representam as intensidades de cada feixe separadamente. No entanto, com essa calibração não conseguimos valores de escalas de cinza que produzam um deslocamento de fase de  $\pi$ . Para mais detalhes, ver [31].

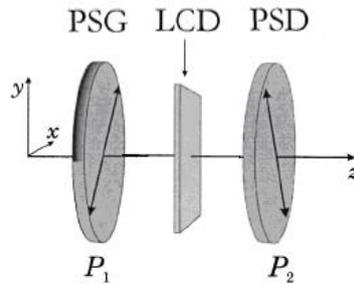
Na segunda calibração foi feito um mapeamento de várias polarizações, no qual mantínhamos fixo o polarizador de entrada (a  $45^\circ$ ) e variávamos as polarizações de saída e as escalas de cinza (GL). Estávamos procurando conjuntos de escala de cinza e polarizações de saída que dessem a diferença de fase  $\pi$  entre dois feixes refletidos por duas regiões do SLM sem atenuação, para ser utilizado nas medidas do algoritmo de Deutsch.

A matriz de Jones (M) fornece as características do SLM em função dos níveis de cinza e do ângulo do polarizador de saída [32]. Um gerador de es-



**Figura 4.2:** Aparato experimental usado para calibrar a fase fornecida pelo SLM: a)interferômetro de Michelson; b)fenda dupla usada para gerar interferência

tado de polarização (PSG), consistindo de um polarizador linear, pode gerar qualquer vetor  $|\theta, \phi\rangle$ , onde  $|\theta, \phi\rangle = \cos\theta |H\rangle + e^{i\phi} \sin\theta |V\rangle$ . De uma maneira similar, um detector de estado de polarização (PSD) detecta a componente do estado de entrada  $|\psi\rangle$  sobre o estado  $|\theta, \phi\rangle$  (Figura 4.3), ou seja, quando projetamos a matriz de Jones na base do polarizador de saída obtemos o estado final do qubit  $|J\rangle$ .



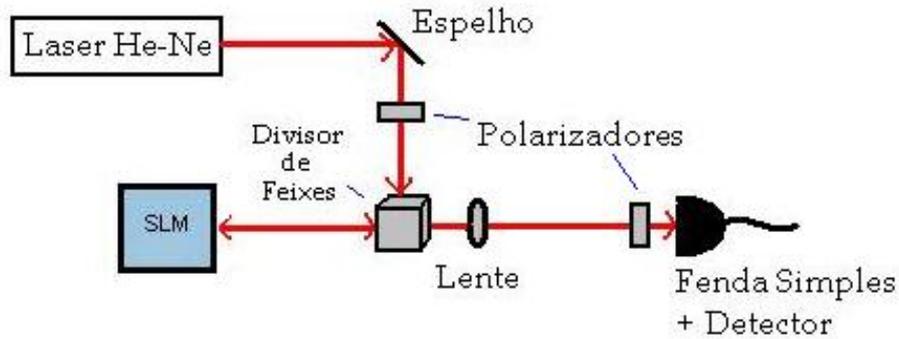
**Figura 4.3:** Sistema óptico que compõe o SLM

Dessa forma, um fóton com polarização inicial  $|\psi\rangle$  (estado de entrada) passa pelo gerador de polarização (PSG), pelo LCD e pelo detector de polarização (PSD) e, por fim, obtemos o estado final do qubit  $|J\rangle$ . Esse processo gera uma modulação de fase e amplitude no fóton medido.

Assim, se tivermos os valores das polarizações de entrada e saída podemos obter valores de escala de cinza que nos dão as diferenças de fase desejadas,

que no nosso caso é de  $\pi$ .

A montagem utilizada foi a da figura 4.4:



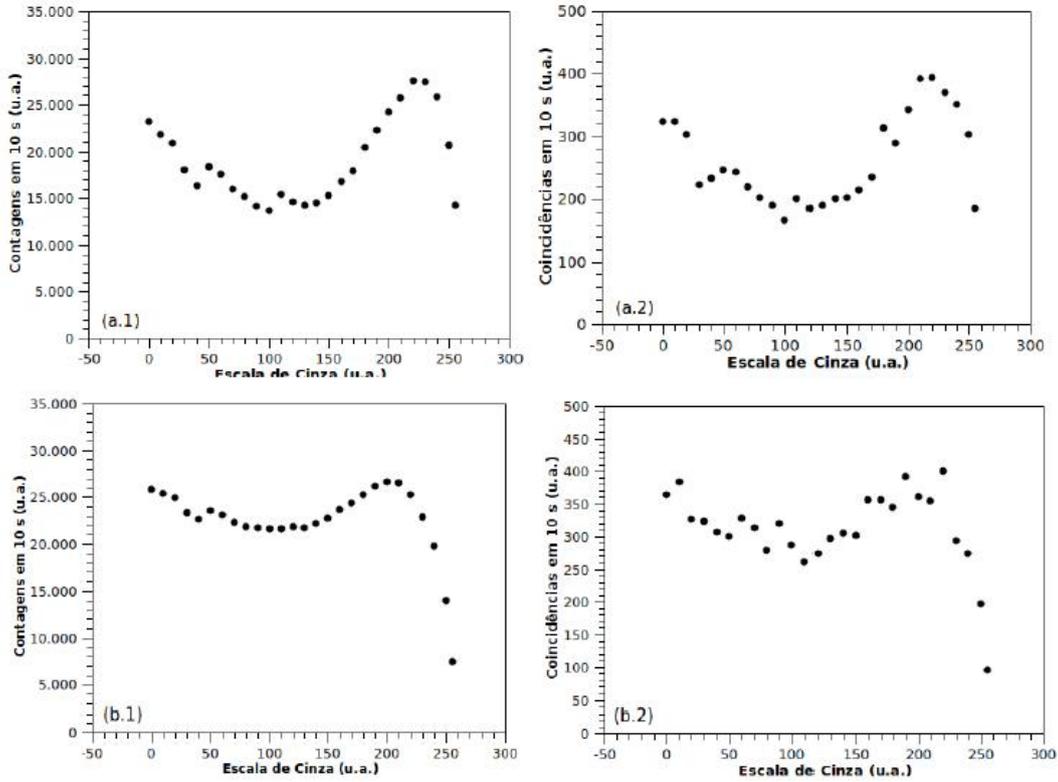
**Figura 4.4:** Motagem experimental utilizada na segunda calibração.

Esta é a mesma utilizada anteriormente (Figura 4.2(b)). A diferença aqui é que nesse caso as medidas são feitas sem a fenda dupla e há a utilização de uma lente convergente a uma distância  $2f$  do SLM e do detector. O papel desta lente é formar a imagem do SLM no detector e determinar se está havendo atenuação quando utilizamos determinadas escalas de cinza e ângulos no polarizador de saída.

Assim, o procedimento para calibração é feito da seguinte forma: primeiro colocamos o padrão de interferência no máximo, para garantir que a operação realizada não tenha fase, e fixamos a polarização de entrada; em seguida variamos as polarizações de saída de  $-90^\circ$  a  $90^\circ$  com passo de  $15^\circ$  e para cada ângulo obtemos as curvas de intensidade e coincidências em função da escala de cinza. Exemplos para algumas polarizações na Figura 4.5.

A partir destas curvas, procuramos por conjuntos de pontos em que a intensidade de um feixe se manteria inalterado. Assim, encontramos um grande conjunto de pontos que havia a relação de intensidade desejada, para diferentes polarizações de saída.

Em seguida, fizemos medidas das imagens das fendas, para confirmar as intensidades, e dos padrões de interferência, utilizando a fenda dupla logo na frente do SLM, com a finalidade de descobrir se os pares de pontos de intensidade (escalas de cinza) obtidos anteriormente produziam as diferenças de fase desejadas.



**Figura 4.5:** Medidas de contagens (a.1 e b.1) e coincidências (a.2 e b.2) para as polarizações de  $90^\circ$  (a.1 e a.2) e  $75^\circ$  (b.1 e b.2).

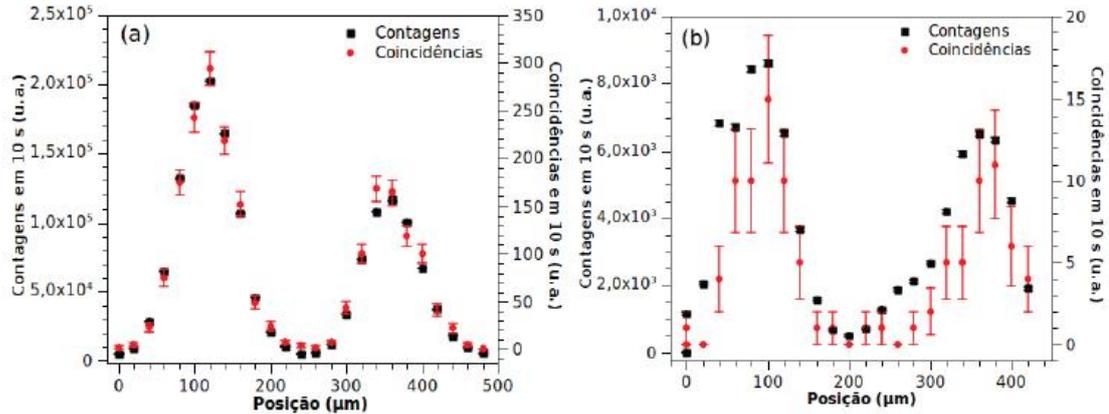
A tabela abaixo mostra as diferenças de fase obtidas para determinadas escalas de cinza nas fendas superior e inferior, com certas polarizações do feixe de saída.

| Fase             | GL da 1 <sup>a</sup> fenda | GL da 2 <sup>a</sup> fenda | Polarização |
|------------------|----------------------------|----------------------------|-------------|
| 0                | 230                        | 180                        | $45^\circ$  |
| $\pi$            | 110                        | 220                        | $90^\circ$  |
| $\frac{\pi}{2}$  | 140                        | 220                        | $90^\circ$  |
| $-\frac{\pi}{2}$ | 240                        | 170                        | $90^\circ$  |

Tabela 4.1: Dados obtidos na calibração do SLM.

As figuras 4.6 e 4.7 mostram as medidas das imagens e dos padrões de interferência, respectivamente, utilizando os pares de fótons gêmeos. Vemos

que para estas escalas de cinza realmente há atenuação bem como a diferença de fase desejada entre os dois feixes que passam pela fenda dupla.

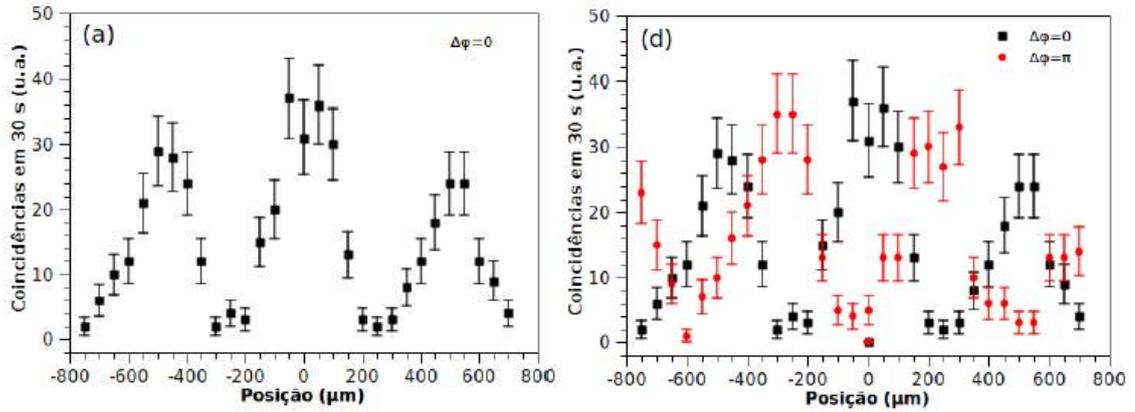


**Figura 4.6:** Imagens das fendas utilizando as escalas de cinza e polarizações de saída presentes na tabela acima. A imagem (a) corresponde a diferença de fase zero, a imagem (b) corresponde a diferença de fase  $\pi$ .

### 4.3 Posicionando o SLM com relação à Fenda Dupla

Uma figura em forma de dois retângulos foi gerada no SLM (Figura 4.8). O primeiro retângulo ocupa a metade superior do SLM e o segundo, a metade inferior. Na figura gerada, a linha que separa os dois retângulos pode ser deslocada, modificando a largura de cada um dos retângulos. Como mencionado anteriormente, para determinarmos escalas de cinza, a atenuação do feixe de luz incidente é grande. No retângulo superior colocamos uma escala de cinza cuja reflexão é máxima e no retângulo inferior, uma escala de cinza cuja reflexão é mínima.

Para coincidir a linha divisória entre os retângulos no SLM com a separação entre as fendas, começamos com a largura do retângulo inferior muito menor que o superior. A fenda dupla foi colocada à uma distância mínima do SLM. Fótons transmitidos pela fenda dupla foram refletidos de volta pelo SLM e coletados no plano da imagem das fendas por um detector de área



**Figura 4.7:** Medidas dos padrões de interferência utilizando os dados da tabela.

grande. Os fótons refletidos foram contados em função da posição da linha divisória. Quando a linha divisória coincide com a parte escura da fenda dupla, o número de fótons se estabiliza formando um platô no gráfico. Nessa situação sabemos que os fótons transmitidos pela fenda superior e refletidos terão uma fase sem caminho diferente da fase do fóton transmitido pela fenda inferior. Desta maneira, encontramos a situação em que a linha divisória dos retângulos coincide com a faixa escura da fenda dupla.

## 4.4 O Procedimento de Medição

O procedimento de medição foi dado da seguinte forma: primeiramente, fizemos medidas dos padrões de interferência dos fótons gêmeos para garantir que estávamos colocando uma diferença de fase  $\pi$  entre as duas fendas. Ou seja, acrescentamos a mesma fase nos dois retângulos do SLM (fase 0, correspondente ao 0 lógico) e medimos um padrão de interferência; depois, acrescentamos uma fase  $\pi$  em um dos retângulos do SLM (correspondendo ao 1 lógico) e detectamos outro padrão de interferência. Os resultados são mostrados no gráfico abaixo (Figura 4.9).

Obsevando o gráfico com diferença de fase  $\pi$  entre as fendas, podemos ver que o máximo do padrão de interferência foi deslocado para posição de



**Figura 4.8:** A figura mostra duas escalas de cinza dividindo igualmente a tela do display de LCD. Tal figura foi utilizada quando queríamos modificar a fase de um feixe em relação ao outro, quando cada um deles é transmitido por uma das fendas de uma mesma fenda dupla.

mínimo, demonstrando que as escalas de cinza aplicadas no SLM provocam uma mudança de fase de  $\pi$  no feixe de luz incidente, tornando-as aptas para o experimento.

Tendo feito essas medidas preliminares, começamos as medidas para teste da implementação do algoritmo de Deutsch-Jozsa com um qubit, com o polarizador de entrada a  $45^\circ$  e o de saída a  $150^\circ$ . Para isso, deslocamos o padrão de interferência para o máximo, fixamos os detectores e capturamos as contagens de fótons num tempo de 1000s para cada função simulada.

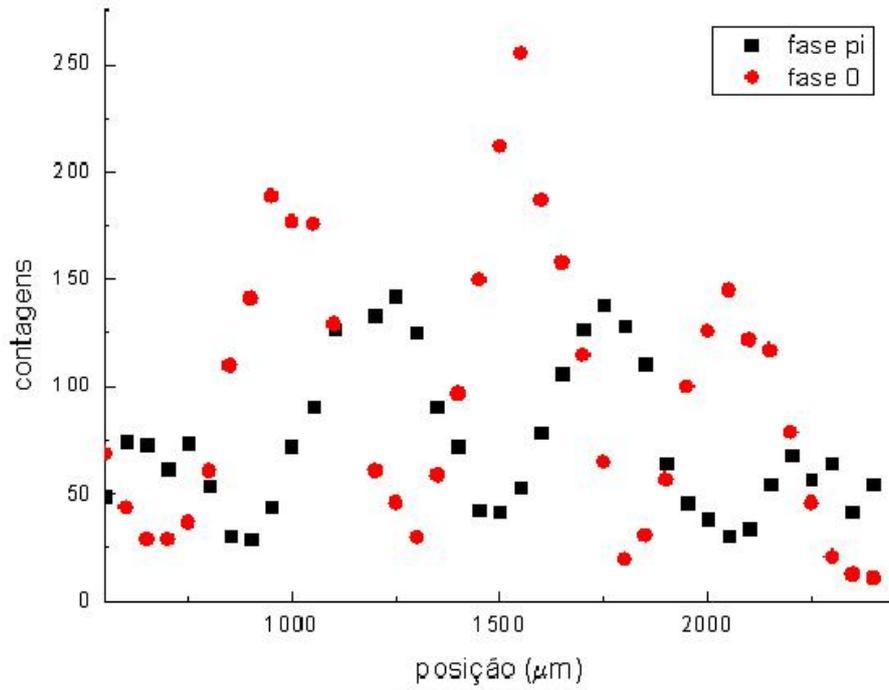
Os resultados foram:

| Fenda Superior | Fenda Inferior | Detector 1 | CNC  | ACC | Tempo de aquisição |
|----------------|----------------|------------|------|-----|--------------------|
| FASE 0         | FASE 0         | 2827252    | 9551 | 575 | 1000 s             |
| FASE $\pi$     | FASE $\pi$     | 2767135    | 9523 | 562 | 2000 s             |
| FASE $\pi$     | FASE 0         | 2739518    | 2739 | 380 | 1500 s             |
| FASE 0         | FASE $\pi$     | 2656476    | 2538 | 321 | 1500 s             |

Tabela 4.2: Dados obtidos das medições para o algoritmo.

onde “CNC” são as contagens em coincidência, “ACC” são as contagens acidentais, e “Detector 1” são as contagens simples do detector 1.

Note que o tempo de aquisição para cada função não foi o mesmo. Isso foi feito para que tivéssemos um erro experimental menor nas contagens de



**Figura 4.9:** Gráficos dos Padrões de Interferência para as fases 0 e  $\pi$  aplicadas no SLM.

fótons.

Dessa forma, foi necessário que fizéssemos um ajuste dos resultados obtidos. Os resultados encontrados para o mesmo tempo de medida são:

| Fenda Superior | Fenda Inferior | CNC           |
|----------------|----------------|---------------|
| FASE 0         | FASE 0         | $8926 \pm 94$ |
| FASE $\pi$     | FASE $\pi$     | $8861 \pm 94$ |
| FASE $\pi$     | FASE 0         | $2142 \pm 46$ |
| FASE 0         | FASE $\pi$     | $2284 \pm 48$ |

Tabela 4.3: Dados obtidos das medições para o algoritmo já normalizado e descontadas as contagens acidentais.

onde CNC são agora as contagens em coincidência para o mesmo tempo de medida já descontadas as contagens acidentais.

Analisando os resultados obtidos vemos que para implementação da função constante utilizando fase 0 nas duas fendas e  $\pi$  nas duas fendas temos con-

tagens de coincidências com variação de aproximadamente 1%. Já na implementação da função balanceada utilizando fase 0 na fenda superior e  $\pi$  na inferior temos 25% de coincidências, enquanto usando fase  $\pi$  na fenda superior e fase 0 na inferior temos 24% com relação a fase 0. Não conseguimos implementar no SLM uma fase  $\pi$  sem atenuação com relação à fase 0. Isso explica a baixa visibilidade obtida, em torno de 75%. Receberemos brevemente um SLM, modulador apenas de fase, que deverá produzir resultados experimentais muito próximos do ideal.

Posteriormente, refizemos a calibração do SLM de modo que conseguíssemos novas polarizações de entrada e saída e novas escalas de cinza para que pudéssemos refazer as medidas do Algoritmo de Deutsch obtendo melhores resultados.

A calibração do SLM foi feita agora variando os polarizadores de entrada e saída e os graus de cinza. Então, novos valores encontrados foram:

| Fase  | GL da 1ª fenda | GL da 2ª fenda | Polarização |
|-------|----------------|----------------|-------------|
| $\pi$ | 30             | 230            | 150°        |

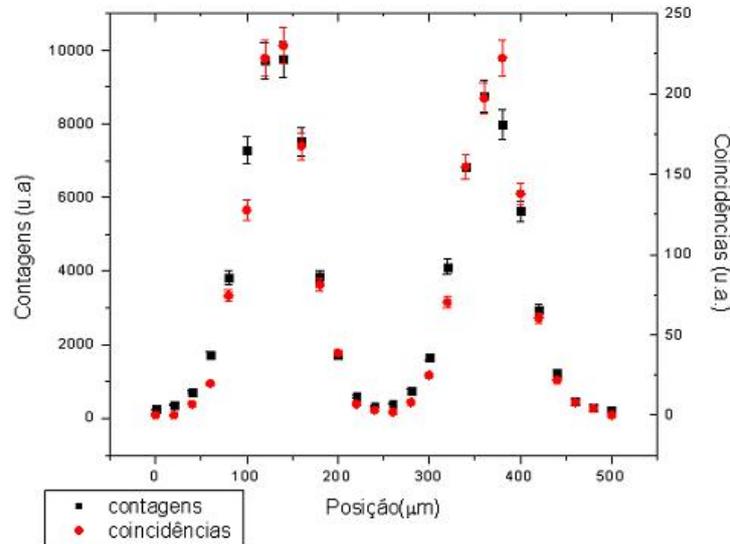
Dados obtidos na nova calibração do SLM.

Posteriormente, fizemos as medidas das imagens das fendas (Figura 4.10) e do padrão de interferência (Figura 4.11). Podemos ver que para essas escalas de cinza não há atenuação, como queríamos para a realização das medidas do algoritmo, e há a diferença de fase desejada entre os dois feixes que passam pela fenda dupla.

Assim, refizemos as medidas do algoritmo de Deutsch. Os resultados encontrados foram:

| Fenda Superior | Fenda Inferior | CNC       |
|----------------|----------------|-----------|
| FASE 0         | FASE 0         | 5116 ± 82 |
| FASE $\pi$     | FASE $\pi$     | 5290 ± 84 |
| FASE $\pi$     | FASE 0         | 330 ± 30  |
| FASE 0         | FASE $\pi$     | 352 ± 31  |

Dados obtidos das medições para o algoritmo já normalizado e descontadas as contagens acidentais.



**Figura 4.10:** Imagem das fendas utilizando as escalas de cinza e as polarizações de entrada e saída encontradas na última calibração.

onde CNC são agora as contagens em coincidência para o mesmo tempo de medida já descontadas as contagens acidentais.

Analisando os resultados obtidos vemos que para implementação da função constante utilizando fase 0 nas duas fendas e  $\pi$  nas duas fendas temos contagens de coincidências com variação de aproximadamente 3%. Já na implementação da função balanceada utilizando fase 0 na fenda superior e  $\pi$  na inferior temos 7% de coincidências, enquanto usando fase  $\pi$  na fenda superior e fase 0 na inferior temos 6% com relação a fase 0.

Assim, podemos observar que ao ajustarmos no SLM as funções balanceadas obtivemos um comportamento de interferência destrutiva, com contagens em coincidência visivelmente menores do que as contagens obtidas para o SLM ajustado nas funções constantes. Como podemos observar no histograma da Figura 4.12. Dessa forma, podemos ver que as intensidades medidas para as funções balanceadas demonstram um comportamento de interferência destrutiva, enquanto as intensidades medidas para as funções constantes demonstram um comportamento de interferência construtiva.

Logo, os resultados obtidos estão em acordo com o que esperávamos teoricamente para o algoritmo de Deutsch com um qubit. Ou seja, demonstramos

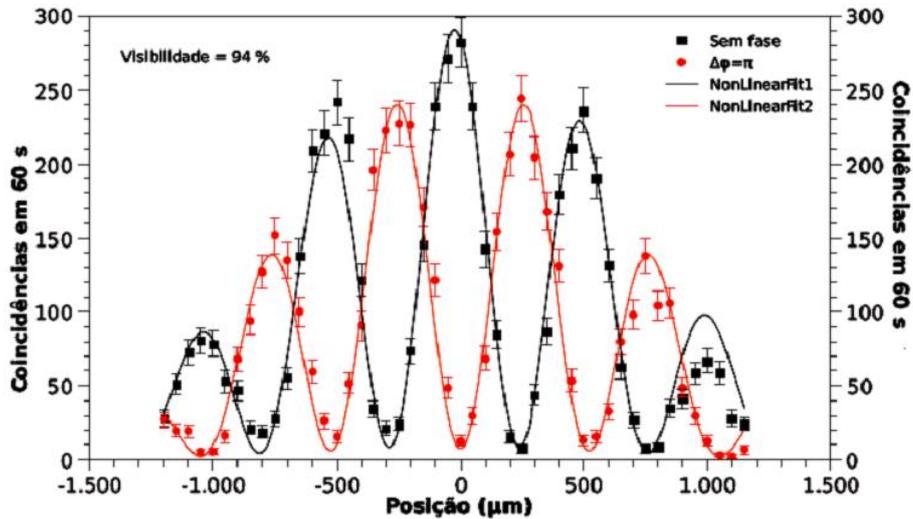


Figura 4.11: Gráficos dos Padrões de Interferência para as fases 0 e  $\pi$  aplicadas no SLM.

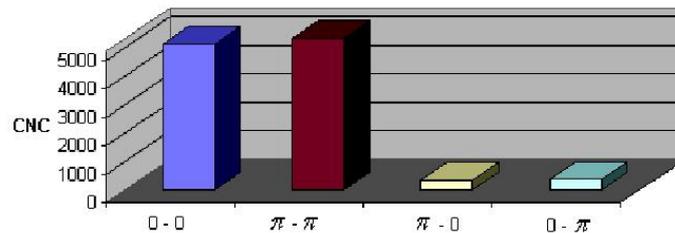


Figura 4.12: Histograma da medida do Algoritmo de Deutsch, demonstrando o comportamento de interferência construtiva e destrutiva, simulando as funções balanceadas e constantes.

a implementação física do algoritmo de Deutsch, onde o sistema utilizado foi estados fotônicos de 1 qubit nas variáveis de caminho.

A computação quântica utilizando fótons é bastante atraente pelo ponto de vista que esses são partículas sem carga, relativamente fáceis de serem gerados e medidos, e têm pouca interação com o meio. Além do formalismo teórico que os descreve, que é fundamental para entendermos o funcionamento de um computador quântico no laboratório.

Podemos pensar, também, no uso de fótons em computação quântica como uma ferramenta para entender o comportamento da natureza no que se

diz respeito à fenômenos quânticos, bem como desenvolver novas tecnologias baseadas no seu formalismo para aplicação em outros sistemas [2].

---

## Capítulo 5

### Conclusão

O tema central deste trabalho foi a implementação do algoritmo de Deustch com um qubit. Com esse fim utilizamos um modulador espacial de luz (SLM) para introduzir fases no feixe incidente de forma que esse produzisse funções balanceadas e constantes, fazendo o papel do Oráculo na determinação da função.

O experimento foi realizado com pares de fótons gêmeos gerados pelo processo de Conversão Paramétrica Descendente. Um deles era usado como *trigger* enquanto o outro atravessava uma fenda dupla saindo em um estado de superposição de caminhos, isto é, um qubit.

No capítulo I estudamos a Conversão Paramétrica Descendente. Vimos os casamentos de fase tipo I e tipo II e visualizamos essas estruturas por meio de uma construção geométrica. Ainda, discutimos sobre o emaranhamento dos estados produzidos pelo processo.

Em seguida, revimos os cristais líquidos. Vimos que eles podem ser de três tipos: nemáticos, esméticos e colestéricos. Estudamos os cristais líquidos nemáticos girados e suas propriedades ópticas, já que esses são muito úteis em tecnologia de *displays*, pois aplicando um campo elétrico externo sobre eles suas moléculas podem ser arrançadas de maneira que podem servir como retardadores de onda e rotadores de polarização. Ainda no mesmo capítulo falamos sobre o modulador utilizado no experimento, o LC - R 2500.

No capítulo 2, focamos nos conceitos fundamentais da informação quântica. Estudamos o qubit, sua representação na esfera de Bloch e descrevemos

---

as portas lógicas quânticas de qubits únicos.

No capítulo 3 apresentamos os conceitos básicos de computação quântica: o que é uma máquina de computação, algoritmos, algoritmos quânticos e paralelismo quântico. Discutimos a computação quântica, que baseia-se no processamento de bits de informação que podem ser superposições de 0's e 1's lógicos, e usufrui do paralelismo quântico para resolver alguns problemas mais rapidamente do que com um computador clássico.

Depois, introduzimos o Problema de Deutsch, que é apresentado da seguinte forma: nos é dada uma caixa preta, ou oráculo e queremos descobrir se uma função que atua sobre qubits é constante (retorna sempre 0 ou sempre 1, independentemente da entrada) ou é balanceada (o número de vezes que retorna 0 é igual ao número de vezes que retorna 1). Matematicamente, estamos buscando uma propriedade global da função, dada por  $f(0) \oplus f(1)$ . Em seguida, apresentamos os algoritmos de Deutsch e sua generalização para  $n$  qubits, o de Deutsch - Jozsa, que resolvem o problema de Deutsch. Esse é o exemplo mais simples de um algoritmo quântico que supera um algoritmo clássico, combinando o paralelismo quântico a outra propriedade de interferência. Na verdade, ele não possui nenhuma aplicação computacional, como o algoritmo de Shor ou Grover, apenas resolve um problema hipotético mostrando o ganho computacional sobre a versão clássica, ou seja, foi criado para mostrar que quanticamente teríamos alguma vantagem sobre a computação clássica. Por fim, introduzimos o algoritmo proposto por Collins *et al*, que simplifica o algoritmo de Deutsch - Jozsa eliminando uma redundância nesse, o que faz com que a implementação física requeira um sistema de 2 estados a menos.

No capítulo 4 explicamos como foi feita a calibração de fase do SLM no laboratório e o posicionamento do SLM com relação à fenda dupla para coincidir a linha divisória entre os retângulos no SLM com a separação entre as fendas. Ainda, apresentamos o aparato experimental utilizado, que consistiu de um laser HeCd cujo feixe incidiu em um cristal  $LiIO_3$  tipo I, e pela conversão paramétrica descendente gerou pares de fótons gêmeos. Usando um modulador espacial de luz, o LC R - 2500, para colocar fases no caminho dos fótons, e detectando em coincidência, demonstramos o algoritmo de Deutsch-Jozsa com fótons usando apenas um qubit.

---

Como a função do algoritmo é determinar se uma função é constante ou balanceada, tínhamos então quatro possibilidades para o caso de um qubit: 1) Ambos caminhos são acrescentados fase zero ou 2) acrescentando fase  $\pi$ , representando duas funções constantes; 3) em um caminho é acrescentado fase  $\pi$  e em outro fase 0 ou 4) no primeiro é acrescentado fase 0 e no outro é acrescentado fase  $\pi$ , representando duas funções balanceadas.

Logo, o que tínhamos que fazer era colocar através do SLM fases de 0 e  $\pi$  em pontos correspondentes às fendas duplas, simulando as funções balanceadas e constantes. Desse modo, ao medirmos as contagens de coincidências num determinado tempo, o resultado obtido esperado seria de interferência construtiva para as funções constantes e interferência destrutiva para as funções balanceadas.

Os resultados obtidos foram tais que na implementação da função balanceada, fases 0 e  $\pi$  (ou  $\pi$  e 0) nas fendas superiores e inferiores, obtivemos 25% (ou 24%) do número de coincidências detectado quando a função é constante (mesmas fases) e os detectores estão posicionados no centro do padrão de interferência.

Assim, pudemos observar que ao ajustarmos no SLM as funções balanceadas obtivemos um comportamento de interferência destrutiva, com contagens em coincidência visivelmente menores do que as contagens obtidas para o SLM ajustado nas funções constantes, demonstrando um comportamento de interferência construtiva. Esse resultado demonstra um possível esquema de implementação do algoritmo de Deutsch usando um só estado de 1 qubit nas variáveis de caminho.

Uma perspectiva futura interessante seria a generalização do algoritmo para  $n > 2$ , bem como a busca de possíveis generalizações do problema de Deutsch para outras dimensões, por exemplo, envolvendo qutrits.

---

## Bibliografia

- [1] A. Galindo e M. A. Martín-Delgado, *Information and computation: Classical and quantum aspects*, Rev.of Modern Physics, volume 74, 347423, (2002).
  - [2] M. A. Nielsen e I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press: Cambridge, (2000).
  - [3] C. Cohen-Tannoudji, B. Diu e F. Laloe, *Quantum Mechanics - Volume Two*, John Wiley and Sons, Inc. and Hermann, Cap. XIV, (1977).
  - [4] G. Benenti, G. Casati e G. Strini, *Principles of Quantum Computation and Information*, World Scientific, (2004).
  - [5] M. Pavicic, *Quantum computation and quantum communication ; Theory and Experiments*, Springer, (2005).
  - [6] IBM Research Projects, <http://www.research.ibm.com/sscomputing/>.
  - [7] D-Wave Systems: The Quantum Computing Company, <http://www.dwavesys.com/index.php?page=company>.
  - [8] D. Bouwmeester, A. Ekert e A. Zeilinger, *The Physics of Quantum Information*, Springer, (2000).
  - [9] Álvaro Nunes de Oliveira, Dissertação de Mestrado, UFMG (2003).
  - [10] Leonardo Teixeira Neves, Dissertação de Mestrado, UFMG (2002).
  - [11] Steane, Andrew, *Quantum Computing*, Department of Atomic and Laser Physics, University of Oxford. Disponível em: [http://xxx.lanl.gov/PS\\_cache/quant-ph/pdf/9708/9708022v2.pdf](http://xxx.lanl.gov/PS_cache/quant-ph/pdf/9708/9708022v2.pdf)
-

- 
- [12] Preskill, John, *Lecture Notes for Physics 229: Quantum Information and Computation*, California Institute of Technology, September, (1998).  
Disponível em: <http://www.theory.caltech.edu/~preskill/ph299>
- [13] Stephen Patrick Walborn, Tese de Doutorado, UFMG (2004).
- [14] Wilson Ricardo Matos Rabelo, Tese de Doutorado, UFMG (2006).
- [15] D. DiVincenzo, Phys. Rev. A, 50, 1015, (1995).
- [16] L. Mandel e E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press: Cambridge (1995).
- [17] Lijun Wang, Tese de Doutorado, University of Rochester (1992).
- [18] Antía Lamas Linhares, Tese de Doutorado, University of Oxford (2002).
- [19] Gustavo de Aquino Moreira Lima, Tese de Doutorado, UFMG (2006).
- [20] Pablo Lima Saldanha, Dissertação de Mestrado, UFMG (2006).
- [21] Juliana Gontijo Fonseca, Dissertação de Mestrado, UFMG (2009).
- [22] Olavo Cosme da Silva, Dissertação de Mestrado, UFMG (2004).
- [23] T. P. Grayson e G. A. Barbosa, *Spatial properties of spontaneous parametric down-conversion and their effect on induced coherence without induced emission*, Physical Review A, 49,2948-2961, (1994).
- [24] G.Kh. Kitaeva and A.N. Penin, *Spontaneous Parametric Down-Conversion*, JETP Letters, 82, No 6, (2005).
- [25] C.K. Hong e L. Mandel, *Theory of parametric frequency down conversion of light*, Physical Review A, 31, 2409, (1985).
- [26] L.Wang, X. Zou e L. Mandel, *Induced coherence without induced emission*, Physical Review A, 44,4614, (1991).
- [27] A. Márquez et al., *Quantitative prediction of the modulation behavior of twisted nematic liquid crystal displays based on a simple physical model*, Opt. Eng. 40, 2558, (2001).
-

- 
- [28] M.G. Capuleto, et al., *Scanning mechanism based on a programmable liquid crystal display*, Opt. Commun., 232, 107, (2004).
- [29] G. Puentes, et al., *Optical simulation of quantum algorithms using programmable liquid-crystal displays*, Phys. Rev. A, 69, 042319, (2004).
- [30] D. Francisco, et al., *Optical simulation of the quantum Hadamard operator*, Opt. Commun., 268, 340, (2006).
- [31] Wanderson Maia Pimenta, Dissertação de Mestrado, UFMG (2010).
- [32] I. Moreno, et al., *Jones matrix method for predicting and optimizing the optical modulation properties of a liquid-crystal display*, J. Appl. Phys., 94, 3697-3702, (2003).
- [33] A. Márquez, et al., *Mueller-Stokes characterization and optimization of a liquid crystal on silicon display showing depolarization*, Opt. Express, 16, 1669-1685, (2008).
- [34] G. Lima, et al., *Manipulating spatial qudit states with programmable optical devices*, Opt. Express 17, 10688-10696, (2009).
- [35] Bahaa E. A. Saleh, Malvin Carl Teich, *Fundamentals of Photonics*, Wiley-Interscience, (1991).
- [36] Chris Desimpel, Tese de Doutorado, Universiteit Gent (2006).
- [37] Martin Stütz, *Qutrit-Manipulation mit aktiven Phasenhologrammen*, Institut für Experimentalphysik der Universität Wien.
- [38] página da Holoeye Photonics: <http://www.holoeye.com>.
- [39] K. Lu e B.E.A. Saleh, *Theory and design of the liquid crystal TV as an optical spatial phase modulator*, Opt. Eng., 29, 240-246, (1990).
- [40] A. Márquez, J. Campos, M. J. Yzuel, I. Moreno, J. A. Davis, C. Iemmi, A. Moreno e A. Robert, *Characterization of edge effects in twisted nematic liquid crystal displays*, Opt. Eng., 39, 3301-3307, (2000).
-

- 
- [41] Q. Wang e S. He, *A new effective model for the director distribution of a twisted nematic liquid crystal cell*, J. Opt. A: Pure Appl. Opt. 7, 438-444, (2005).
- [42] V. Durán, J. Lancis, E. Tajahuerce, e Z. Jaroszewicz, *Equivalent retarder-rotator approach to on-state twisted nematic liquid crystal displays*, J. Appl. Phys., 99, 113101-113106, (2006).
- [43] D. Goldstein, *Polarized Light*, Marcel Dekker, (2004).
- [44] V. Vedral, *Introduction to Quantum Information Science*, Oxford University Press: New York, (2006).
- [45] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. R. Soc. Lond. A, 400, 97 - 117, (1985).
- [46] D. Deutsch, *Quantum computational networks*, Proc. R. Soc. Lond. A, 425, 73 - 90, (1989).
- [47] D. Deutsch, e R. Jozsa, *Rapid solution of problems by quantum computation*, Proc. R. Soc. Lond. A, 439, 553 - 558, (1992).
- [48] I.L. Chuang, e Y. Yamamoto, *Simple Quantum Computer*, Phys. Rev. A, vol. 52, number 5, (1995).
- [49] I.L. Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung e S. Lloyd, *Experimental realization of a quantum algorithm*, Nature, vol. 393, (1998).
- [50] S. Guide, M. Riebe, G.P.T Lancaster, C. Becher, J. Eschner, H. Häffner, Schmidt - F.Kaler, I.L. Chuang, R. Blatt, *Implementation of the DeutschJozsa algorithm on an ion-trap quantum computer*, Nature, vol. 421, (2003).
- [51] D. Collins, K.W. Kim, W.C. Holton, *Deutsch-Jozsa algorithm as a test of quantum computation*, Phys. Rev. A, Rapid Com., Third Series, vol. 58, number 3, (1998).
- [52] D. Wei, J. Luo, X. Sun, X.Zeng, *Realization of Deutsch-like algorithm using ensemble computing*, Physics Letters A, 319, 267 - 272, (2003).
-

- 
- [53] P. Bianucci, A. Muller, C.K. Shih, Q.Q. Wang, Q.K. Xue, C. Piermarocchi, *Experimental realization of the one qubit Deutsch-Jozsa algorithm in a quantum dot*, Phys. Rev. B, 69, 161303(R), (2004).
- [54] A.N. de Oliveira, S.P. Walborn, C.H. Monken, *Implementing the Deutsch algorithm with polarization and transverse spatial modes*, J. Opt. B: Quantum and Semiclass. Opt., 7, 288 - 292, (2005).
- [55] A.P dos Santos, A.T. Avelar, B. Baseia, *Implementação do algoritmo de Deutsch - Jozsa via interação dispersiva em cavidade supercondutora*, Anais do V Congresso de Pesquisa, Ensino, e Extensão, Campus Samambaia - 06 a 10 de outubro de 2008.
- [56] R. Jozsa, Entanglement and Quantum Computation in the Geometric Universe, 369, eds. S. Huggett, L. Mason, K.P.Tod, S.T.Tsou and N.M.J Woodhouse, Oxford University Press, (1998).
- [57] R.Jozsa e B. Schumacher, *A New Proof of the Quantum Noiseless Coding Theorem*, J. Mod. Opt. 41, 2343, (1994).
- [58] A. Ekert e R. Jozsa, *Quantum algorithms: entanglementenhanced information processing*, Phil Trans. Roy. Soc. London Ser A, 356, 1769, (1998).
- [59] R. Landauer, J. Stat. Phys. 54, 516 (1989).
- [60] W.G. Unruh, *Maintaining coherence in quantum computers*, Phys. Rev. A 51, 992, (1995).
- [61] R. Cleve, A. Ekert, C. Macchiavello e M. Mosca, *Quantum algorithms revisited*, Proc. R. Soc. Lond. A, 454, 339 - 354, (1998).
- [62] A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. 47 (10): 777780, (1935).
- [63] Comtet, L. *Boolean Algebra Generated by a System of Subsets*. §4.4 in Advanced Combinatorics: The Art of Finite and Infinite Expansions, rev. enl. ed. Dordrecht, Netherlands: Reidel, pp. 185-189, (1974).
-