

UNIVERSIDADE FEDERAL DA CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA
COORDENAÇÃO DE PÓS-GRADUAÇÃO EM FÍSICA

DISSERTAÇÃO DE MESTRADO

Estado Binomial no Interferômetro de Mach-Zehnder
Igor Santos Oliveira

CAMPINA GRANDE

- 2014 -

UNIVERSIDADE FEDERAL DA CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA
COORDENAÇÃO DE PÓS-GRADUAÇÃO EM FÍSICA

DISSERTAÇÃO DE MESTRADO

Estado Binomial no Interferômetro de Mach-Zehnder
Igor Santos Oliveira

Dissertação realizada sob a orientação do Prof. Dr. Aercio F. Lima, apresentada à Unidade Acadêmica de Física em complementação aos requisitos para obtenção do título de Mestre em Física.

CAMPINA GRANDE

- 2014 -

O48e Oliveira, Igor Santos.
 Estado binomial no interferômetro de Mach-Zehnder / Igor Santos
 Oliveira. – Campina Grande, 2014.
 61 f. : il. color.

 Dissertação (Mestrado em Física) – Universidade Federal de Campina
 Grande, Centro de Ciências e Tecnologia, 2014.
 "Orientação: Prof. Dr. Aercio F. Lima".
 Referências.

 1. Física Quântica. 2. Comunicação Quântica. 3. Interferômetro de
 Mach-Zehnder I. Lima, Aercio F. II. Título.

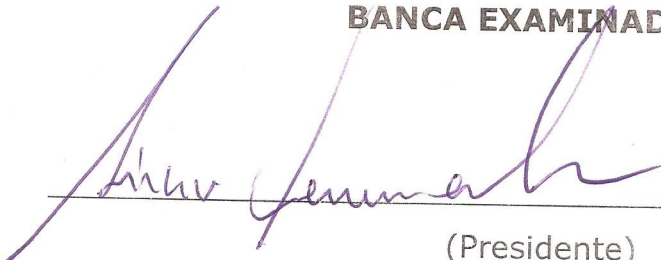
CDU 530.145(043)

IGOR SANTOS OLIVEIRA

ESTADO BINOMIAL NO INTERFERÔMETRO DE MACH-ZEHNDER

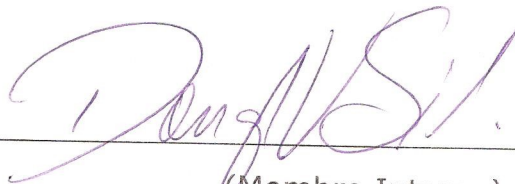
Dissertação aprovada em 21/03/2014

BANCA EXAMINADORA



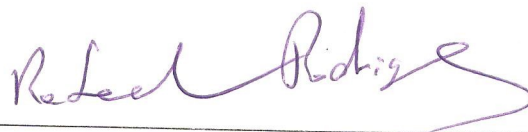
(Presidente)

Prof. Dr. Aécio Ferreira de Lima
Unidade Acadêmica de Física – UFCG



(Membro Interno)

Prof. Dr. Douglas Vitoreti da Silva
Unidade Acadêmica de Física – UFCG



(Membro Externo)

Prof. Dr. Rafael de Lima Rodrigues
Unidade Acadêmica de Educação – UFCG

AGRADECIMENTOS

Agradecimentos a CAPES pelo financiamento do trabalho, a Unidade Acadêmica de Física e aos professores que contribuíram na construção do conhecimento necessário para me tornar um físico, ao professor Dr. Aécio F. Lima pela orientação deste trabalho e ao professor Dr. Danievertton Moretti por ceder o suporte necessário para o estudo. Agradeço a contribuição do professor Dr. Lucca Pezze que ajudou no desenvolvimento de um dos resultados. Agradeço aos amigos que ajudaram durante todo o mestrado: Danilo Moreira, Christian Preker e Vivianni Cordeiro. Agradeço a meus pais Natã Oliveira e Rejane Oliveira, pois investiram na minha carreira científica e acreditaram no meu potencial. Agradeço a Banca examinadora por comparecer e contribuir no melhoramento do trabalho

RESUMO

A criptografia quântica é o futuro da segurança da comunicação, o primeiro protocolo que usa as teorias quânticas é o BB84 que pode ser aplicado usando a polarização da luz ou a fase. No caso da fase essa comunicação pode ser feita usando o Interferômetro de Mach-Zehnder quântico para fazer superposição de fótons e oferecer segurança na comunicação devido à incerteza na fase dos fótons detectados.

O estado de número, que é o estado dos fótons individuais, é o caso ideal para a comunicação, onde a fase é indefinida e com máxima incerteza. Por outro lado, o estado coerente é o mais usual e consegue ter uma incerteza satisfatória na fase, porém não é um estado para uma comunicação segura, pois se trata de um estado considerado clássico da luz.

O estado binomial é um estado interpolador entre o estado coerente e o estado de número, essa interpolação é alcançada através dos limites adequados os parâmetros que os define. Com isso é possível ter um estado não clássico que permite ter maior incerteza na fase e com resultados mais satisfatórios do que o encontrado para o coerente.

ABSTRACT

The quantum cryptography is the future of secure communication, the first protocol using the quantum theory is the BB84 which can be applied using polarization or phase. In the case of phase this communication can be made using the Mach-Zehnder quantum interferometer to make superposition of photons and provide security in communication due to the uncertainty in the phase of the detected photons.

The number state, that is the state of single photons, is the ideal case for communication, where the phase is undefined and with maximum uncertainty. On the other hand, the coherent state is the most usual and can have a satisfactory uncertainty in phase, however is not a state to secure communication, because it is a state regarded classic light.

The binomial state is a state interpolator between the coherent state and number state, this interpolation is achieved through the appropriate limits on parameters that defines them. With this is possible to have a non-classical state that allows having greater uncertainty in phase and with more satisfactory results than found for the coherent.

Conteúdo

1	Introdução	1
2	Modelos de Comunicação Quântica	3
2.1	Criptografia	3
2.2	Protocolo BB84	5
2.3	Interferômetro de March-Zehnder Quântico	11
3	Beam Splitter e o Interferômetro	19
3.1	Teoria quântica do Beam Splitter	19
3.2	Interferômetro na Representação de Schwinger	29
4	Estado Coerente no Interferômetro de Mach-Zehnder	32
4.1	O Estado Coerente	32
4.2	Estado Coerente como entrada no Interferômetro de Mach-Zehnder . .	36
4.3	Detecção da fase no limite quântico	39
5	Estado Binomial no Interferômetro de Mach-Zehnder	47
5.1	O Estado Binomial	47
5.2	Estado Binomial como Entrada no Interferômetro de Mach-Zehnder . .	50
5.3	Detecção da Fase para o Estado Binomial	52
6	Conclusão	58

Capítulo 1

Introdução

O interferômetro de Mach-Zehnder (IMZ) é um equipamento chave na medição de efeitos quânticos em diversos sistemas físicos, tendo aplicações com validade em um amplo domínio do micro escala a macro escala podendo ser utilizado em modelos de estruturas aerodinâmicas, medidas da aceleração da gravidade, etc...[7]. O objetivo primordial do IMZ é estimar a fase com a maior precisão mesmo na presença de fontes ruidosas. Os recentes avanços tecnológicos já possibilitam em situações cuidadosamente controladas, reduzir ou compensar o ruído clássico ao nível irreduzível, a saber, o ruído quântico. É bem conhecido na literatura que a precisão na fase pode ser ampliada se estados não clássicos são injetados nas portas do IMZ [9], ou seja, quando a incerteza da estimativa da fase é mínima. O estado que possui melhor definição na fase, a semelhança dos estados clássicos da luz, é o estado coerente que é considerado o mais clássico dos estados quânticos da luz, por possuir amplitude e fase bem definidos, no entanto não é útil quando se deseja utiliza-lo em protocolos de comunicação quântica segura. Na grande maioria dos esquemas de comunicação quântica utiliza-se o estado de número. No entanto existe um estado que interpola entre o estado de número e coerente que é o estado binomial[17].

Neste trabalho investigamos o comportamento da fase do estado binomial ao ser injetado em uma das portas do IMZ e comparando os resultados já esperados quando o estado coerente é utilizado [14]. Também é estabelecida a base teórica do funciona-

mento do Beam Splitter (BS) quântico. Para esse fim seguimos o roteiro estabelecido na literatura [11] fazendo uso da representação de Schwinger, tendo como objetivo central obter uma estimativa confiável para a fase gerado no esquema do IMZ, investigamos a sugestão fornecida em [14] para a estimativa na fase, que usa a informação de Fisher.

O trabalho está organizado da seguinte forma: no capítulo 2 encontra-se os modelos de comunicação quântica do código de polarização, que foi o primeiro esquema idealizado por [3] chamado de protocolo BB84, e o modelo de código de fase que é gerado no IMZ [6]. No capítulo 3 encontra-se as teorias do BS individual e o IMZ usando as representações de Schwinger[10]. O capítulo 4 apresenta a teoria do estado coerente, o uso desse estado como entrada no IMZ para analisar os estados de saída e o calculo feito para a estimativa da fase [14]. No capítulo 5 encontra-se a teoria do estado binomial, o uso desse estado como entrada no IMZ para analisar estado de saída e o calculo da informação de Fisher comparando resultados com o estado coerente [17].

Capítulo 2

Modelos de Comunicação Quântica

2.1 Criptografia

A criptografia é uma técnica no qual a informação legível pode ser transformada em um código ilegível, de forma que apenas o destinatário consiga ler, o que torna difícil de outra pessoa ler. O código criado para codificar a informação é chamado de chave criptográfica onde apenas o emissor e o receptor da informação tem o conhecimento da chave.

Historicamente a criptografia vem causando conflitos entre criadores de chaves e quebradores de códigos, pois com o avanço da matemática e da tecnologia, o sigilo de informações vem sendo ameaçada. Um exemplo simples é a criptografia feita a partir de cifras, onde um texto pode ter todas as letras trocadas por símbolos, que neste caso será a chave, e o quebrador de código pode usar um pouco de probabilidade para decifrar o texto, uma vez conhecendo o idioma, pode-se ver a letra que aparece com mais frequência nas palavras, depois a segunda letra com mais frequência e assim por diante. Nos casos de hoje, temos máquinas que podem fazer buscas e cálculos em alta velocidade, com computadores de alto processamento, facilitando ainda mais a quebra de códigos.

O esquema a seguir mostra passo a passo de como uma mensagem é criptografada

e enviada. Alice tem uma mensagem que é criptografada por uma chave (como trancar com cadeado) que é enviada para um canal de comunicação insegura, em outra parte a chave é enviada para Bob em um canal de comunicação segura, Bob terá a mensagem criptografada e uma chave que deverá “abrir” o código (destravar o cadeado) e assim poder ler a mensagem.

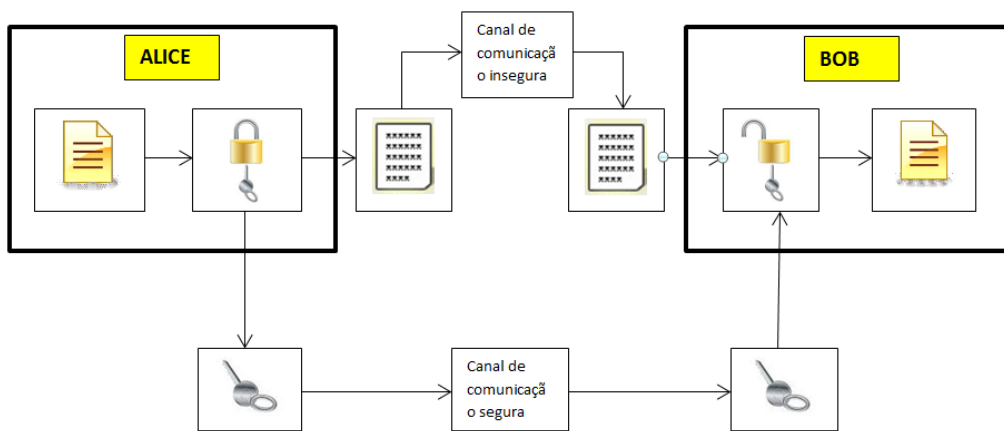


Figura 2.1: Modelo de criptografia clássica

A segurança nos códigos tem grande importância na atualidade, pois a tecnologia nos levou a criação de um mundo digital onde transações bancárias, cartão de créditos, serviços secretos, entre outros tem a necessidade de obter um sigilo poderoso.

O avanço da tecnologia e da computação trouxe chaves mais seguras com a criação de algoritmo de criptografia, atualmente a mais segura é o algoritmo RSA criado pelos professores Ronald Rivest, Adi Shamir e Leonard Adleman, professores do MIT. É um sistema de chaves assimétricas que utiliza a teoria clássica dos números. É dividida em duas chaves, a chave pública acessível a todos e uma chave privada que é mantida em sigilo, porém as chaves públicas só podem ser abertas através da chave privada. O algoritmo RSA é usado na internet em e-mails, compras online e por empresas, porém, ainda sofre ameaças de hackers, pois como se trata de um sistema clássico de algoritmos, ainda sim pode ser quebrado.[1]

Supondo uma comunicação entre um emissor (Alice) e um receptor (Bob) enviando

informação através de um canal clássico, um agente externo (Eva) pode monitorar a comunicação sem que Alice e Bob percebam, pois qualquer informação clássica pode ser clonada, neste caso, Eva pode interceptar a chave enviada por Alice e enviar de volta a Bob.

Para garantir a segurança da informação, foi criada a Criptografia Quântica que usa as teorias quânticas da física para a criação de chaves quânticas seguras. A dualidade onda-partícula do fóton é um dos elementos a serem explorado onde é possível criar chaves quânticas de duas formas, ou por polarização, ou pela fase de um pulso de fótons.[2]

2.2 Protocolo BB84

No início do século XX, a revolução da ciência, com as novas teorias físicas, deu origem a explicações de vários fenômenos começando com a correção da catástrofe ultravioleta, logo em seguida, veio à teoria da dualidade onda-partícula da luz onde Einstein mostra que a luz pode se comportar como partículas chamadas de fótons. A comprovação desse fenômeno veio com o experimento do Efeito Fotoelétrico, sugerido por Einstein e comprovado por Compton, em que fótons se chocavam com elétrons causando um choque mecânico, fenômeno que acontece apenas com partículas.

Partindo da teoria quântica em que luz pode ser partícula, surgiu à ideia de criar uma forma de comunicação em que poderia utilizar a teoria quântica para uma transmissão de informação segura de invasores, neste caso, a polarização do fóton seria a ferramenta ideal.

O primeiro modelo da informação quântica foi proposto por Charles H. Bennett e Gilles Brassard em 1984 [3], o protocolo BB84 que recebe as iniciais de seus sobrenomes e o ano de publicação. O modelo utilizado consiste de quatro formas de polarização do fóton que formam duas bases, a primeira é a base A com polarização de horizontal com ângulo de 0° e vertical com ângulo de 90° , a segunda é a base B com polarizações

diagonais de 45° e 135° .

Para simular o funcionamento do protocolo, usou-se um transmissor (Alice) um receptor (Bob) e um agente externo (Eva) com a finalidade de descobrir a informação que Alice enviou para Bob. As informações transmitidas são equivalentes ao código binário usado na computação, sendo que, para a informação quântica, os chamados Qubits, que obedece às propriedades quântica. Podemos considerar fótons linearmente polarizados como Qubits, representado da seguinte maneira: o vetor \uparrow como $|1\rangle_A$, o vetor \rightarrow como sendo $|0\rangle_A$, o vetor \nwarrow como sendo $|1\rangle_B$ e o vetor \nearrow como sendo $|0\rangle_B$ que são as bases a serem usadas.

Alice irá tentar comunicação com Bob, para isso ela deverá escolher quais bases deverão ser usadas para codificar a mensagem variando entre a base A e a base B. Após a transmissão do código, Bob detecta cada fóton e ambos informam quais bases usaram por meio de comunicação pública (telefone), porém não revela qual “0” ou qual “1” foram enviados, mas divulgam os resultados em que coincidiu a mesma base descartando os resultados distintos. A tabela a seguir, mostra uma simulação de como é feita a troca das chaves quânticas e a perda de alguns fótons que Bob não consegue ler.

Sequência de bit de Alice	1	0	1	0	0	1	1	0	0	1	1	0	1
Base escolhida por Alice	A	B	A	A	B	A	B	B	A	B	A	A	B
Fótons enviados por Alice	\uparrow	\nearrow	\uparrow	\leftarrow	\nearrow	\uparrow	\nwarrow	\nearrow	\leftarrow	\nwarrow	\uparrow	\leftarrow	\nwarrow
Base escolhida por Bob	A	A	B	B	A	A	A	B	B	A	A	B	B
Bit recebido por Bob	1	1		0	1	1		0			1	0	1
Bob informa fóton detectado	A	A		B	A	A		B			A	B	B
Alice informa base correta	Ok					Ok		Ok			Ok		Ok
Informações compartilhadas	1					1		0			1		1

Figura 2.2: troca de chave feita por Alice e Bob.

É interessante observar que bases diferentes podem detectar a mesma informação do

bit, mas não o mesmo bit, pois quando enviado um fóton $|1\rangle_A$ e o receptor coloca base B, poderá ser identificado tanto 0 quanto 1, com probabilidade de 50%, isso acontece devido ao princípio da incerteza de Heisenberg. Outro ponto a ser observado é alguns fótons que se perdem na transmissão podendo ocorrer à perda de suas características no decorrer do caminho, isso acontece devido a interferências da natureza como o ruído ou até mesmo falhas no canal de comunicação.

Para testar a segurança do sistema, é adicionada a agente externa Eva, que será a invasora, com objetivo de conseguir decodificar a mensagem enviada para Bob sem que ninguém saiba. Usando as teorias quânticas, quando Eva interferir no sistema irá danificar os fótons fazendo com que Bob receba informação errada, ela também não poderá medir o fóton por causa do princípio da incerteza, logo, não poderá fazer cópias dos fótons. Outra forma de descobrir um espião no sistema é quando Alice e Bob, usando um subconjunto dos resultados, verificam a coincidência nos resultados, assim eles irão perceber falhas nas medições mesmo tendo sido medidos na mesma base. Esse teste sinaliza que alguém tentou ler a informação, polarizou de forma errada e enviou para Bob. Com a evidência que tentaram ler os Qubits, Alice e Bob devem desconsiderar a informação transmitida e com isso reiniciar o processo de troca de informação.

O princípio da incerteza na polarização dificulta as medidas feitas por Eva, um exemplo simples é de um fóton enviado com polarização de 45° onde Eva tenta medir com a base A, neste caso o fóton terá probabilidade de passar com 0° e com 90° , ou até mesmo não passar, facilitando a identificação de um invasor na comunicação.

Existem algumas estratégias de espionagem que faz com que Eva consiga medir uma pequena taxa de fótons de modo que ela seja confundida com um ruído [2], porém não é o foco desse trabalho atacar o protocolo BB84 e sim explicar a sua ideia.

Usando as notações da Mecânica Quântica, é possível observar uma superposição em algumas medidas já citadas quando se fala no princípio da incerteza, porém agora

fazemos analogia ao gato de Schrödinger, sendo neste caso, um fóton que foi enviado na base B e que foi medido pela base A.

Primeiro observa-se como a luz foi enviada. O estado de polarização do fóton será representado em três dimensões, onde a direção z indicará que o fóton com polarização nessa direção, analogamente para as direções no plano xy. Sem perda de generalidade podemos considerar que as duas direções ortogonais de interesse, podem ser representadas no plano xy ($\phi = \frac{\pi}{2}$). Sendo assim temos que analisar o ângulo formado na polarização através de coordenadas esféricas, ou seja, θ que varia de 0 a $\frac{2}{\pi}$. Será analisada apenas a variação de θ , pois só será mostrado o comportamento da polarização. Neste protocolo são usadas duas bases com cada uma tendo dois estados ortogonais de polarização.

Usando a base A como $\theta_1 = 0^\circ$ e $\theta_2 = \frac{\pi}{2}$, e seus auto-estados sendo $|1\rangle_A$ e $|0\rangle_A$, respectivamente. Analogamente para a base B, usa-se $\theta_1 = \frac{\pi}{4}$ e $\theta_2 = \frac{3\pi}{4}$, com os respectivos auto estados $|1\rangle_B$ e $|0\rangle_B$.

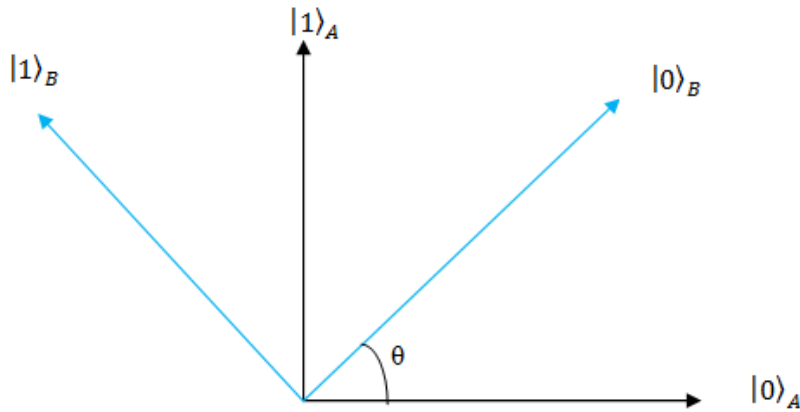


Figura 2.3: Base B formada através da rotação de eixo da base A.

Com isso, sendo $\theta = \frac{\pi}{4}$:

$$|0\rangle_B = a|0\rangle_A + b|1\rangle_A = \cos\left(\frac{\pi}{4}\right)|0\rangle_A + \sin\left(\frac{\pi}{4}\right)|1\rangle_A = \frac{1}{\sqrt{2}}|0\rangle_A + \frac{1}{\sqrt{2}}|1\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \quad (2.2.1)$$

$$|1\rangle_B = a|0\rangle_A + b|1\rangle_A = \text{sen}\left(\frac{3\pi}{4}\right)|0\rangle_A + \text{cos}\left(\frac{3\pi}{4}\right)|1\rangle_A = \frac{1}{\sqrt{2}}|0\rangle_A - \frac{1}{\sqrt{2}}|1\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A - |1\rangle_A) \quad (2.2.2)$$

Isso mostra que a base é apenas a rotação do eixo xy, e também prova que o auto estado da base B pode ser escrito como combinação linear dos auto estados da base A.

Em questão da medida, quando Bob tenta medir $|1\rangle_A$, a probabilidade de acerto é de $\left(\frac{1}{\sqrt{2}}\right)^2 = 0,5$ independente do resultado de Eva, mas para uma chave muito grande a probabilidade é de $(0,5)^n$ sendo n o numero de vezes que Eva interferiu na medida, ou seja, a probabilidade de acerto tende a zero.

A aplicação de um experimento que simula o protocolo BB 84 apresenta alguns problemas, o primeiro é polarizar uma pequena taxa de fótons que só seria ideal se os fótons fossem emaranhados, caso contrário se torna difícil enviar uma polarização exata para emitir a Bob. O segundo problema é a distancia, pois existe muita perda no caminho devido ao meio externo que facilmente interfere nas propriedades dos fótons. O primeiro protótipo experimental [5] usa um flash muito fraco emitido por um diodo de luz verde que emite uma sequencia aleatória de Qubits ao longo de uma conexão no espaço livre de aproximadamente 30 cm de comprimento. Um computador contem software que representam Alice e Bob e Eva foi usada para controlar a transmissão. Alice é uma fonte que produz feixes de pulsos incoerentes de 5s de duração e numa taxa de repetição de alguns quilohertz. Esse feixe foi colimado passando por um filtro espectral e polarizador. A intensidade média do feixe foi muito baixa com uma média de 0,1 fótons por pulso. Isso é, em média apenas 1 em 10 do pulso cronometrado contem um fóton, assim Alice se aproxima de um fóton individual onde a probabilidade de ter mais de um fóton por pulso é de 0,005 onde apenas 1 em 20 pode conter 2 ou mais fótons. Alternando aleatoriamente a tensão do Pocker's cell para cada pulso, onde o Pocker's cell é um aparelho que faz a rotação na polariza do pulso, Alice poderia

codificar aleatoriamente seu bit escolhido em qualquer base de polarização de forma circular ou linear. Bob, por sua vez, deve escolher aleatoriamente a tensão do seu Pocker's cell independente da escolha de Alice, ligado por uma polarizador de calcita que divide os feixes em polarizações verticais ou horizontais. Os dois feixes passam por um fotomultiplicador com sensibilidade suficiente para detectar o fóton único. Bob faz a escolha da base, circular ou linear, e com isso foi determinado a voltagem da Pocker's cell (1 ou 0) que foi enviado para o detector. [6]

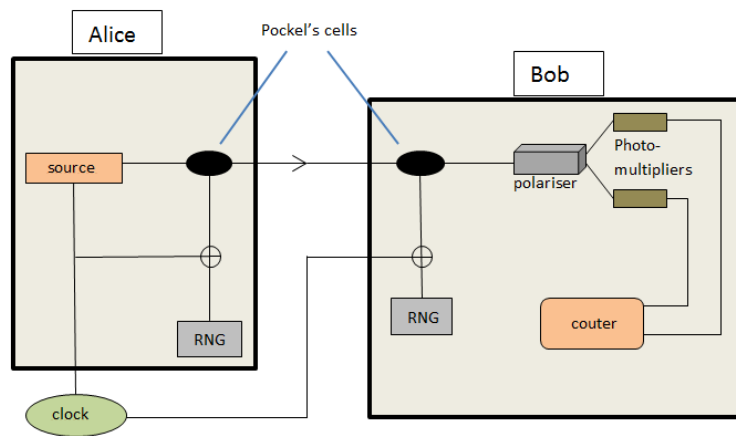


Figura 2.4: Esquema ilustrativo do primeiro experimento a demonstrar a criptografia quântica. As bases são formadas pelo Pockel's cell que muda a polarização do feixe através da voltagem e dois relógios que vai garante o tempo de medida para cada Qubits.

Como esperado, na prática, os fatores experimentais no sistema real muda consideravelmente o protocolo de transmissão no caso ideal já discutido. Isso acontece devido a alguns fatores. O primeiro é que Alice não envia fótons individuais e sim um pulso multe fótons, isso faz com que Eva detecte um fóton de todo o pulso sem que seja detectada. O segundo é que a eficiência do detector é muito baixa sendo em torno de 9%, ou seja, Bob falha na medida dos fótons enviado por Alice. Ainda existe uma perda adicional no canal de transmissão reduzindo o número de fótons que chega até Bob, porém não é um problema tão grave já que a chave é estabelecida apenas pelos bits que foi medido por Bob de modo que a segurança do canal não seja comprometida por perdas, porém, as medidas podem obter erros por causa do ruído, o que pode causar

uma medida sem que nenhum fóton tenha chegado e assim medir uma polarização incorreta, podendo ser por desalinhamento ótico. Esse ruído ocorre aleatoriamente e leva a uma taxa de erro, que suficientemente grande, pode mascarar o erro causado por um intruso, esse ruídos são chamados de “dark counts” (contagem de escuro) que são fótons gerados por excitação térmica dentro do diodo emissor do laser. Para contornar essa situação, Bob coloca seus detectores a disparar no intervalo de tempo durante cada período do relógio para quando um fóton é reconhecido, isso exige que a duração do pulso de Alice seja mais curta que o período do relógio. Para que essa contagem seja eficaz, o numero de contagem escura que ainda resta deve ser apenas uma fração da taxa total de bits que recebido. Estas condições impõem limites da intensidade da fonte, da eficiência dos fotodetectores e das perdas no canal de transmissão. A equipe da IBM-Montreal conseguiu superar todas essas dificuldades e realizou o experimento de com transmissão de chaves durante 10 minutos que rendeu uma chave de 105 bits em que a informação esperada por Eva sobre a chave foi estimada em 6×10^{-171} bits. [5][6].

O sucesso desse modelo demonstrando tamanha segurança ainda acarreta problemas, pois foi um experimento com o único objetivo de demonstrar a segurança proposta pela teoria, porém não pode ser aplicado comercialmente devido a distancia com que a informação caminha de Alice até Bob.

2.3 Interferômetro de March-Zehnder Quântico

O Interferômetro de Mach Zehnder (IMZ) é um aparato experimental cujo objetivo é de um único feixe de luz construir um padrão de interferência, isso acontece devido a dois espelhos divisores de feixe (Beam Splitter)(BS) e dois espelhos de reflexão total. O feixe de luz é dividido em dois feixes em um dos BS, onde cada feixe é refletido em cada espelho respectivo ao seu caminho, os feixes se reencontram em outro BS e em um aparato é observado um padrão de interferência. O interferômetro pode ser montado

de duas formas, um modelo clássico e um modelo quântico, isso depende apenas de como a luz é colocada no experimento, porém, para o caso da informação quântica só interessa o modelo quântico, pois é preciso construir Qubits, que neste caso, será uma pequena taxa de fótons emitida por um laser de Diodo.

A comunicação quântica feita a partir do IMZ é semelhante ao protocolo BB84, sendo a diferença na forma em que as bases estão sujeitas. Devido às limitações em fazer um esquema de polarização, no IMZ às bases serão formadas pela fase com que os feixes são enviados. A vantagem desse experimento é que pode fazer comunicação por fibra ótica, o que faz aumentar a distancia de comunicação entre Alice e Bob, porém continua sujeita a ruídos e perdas de informação por falhas na fibra ótica.

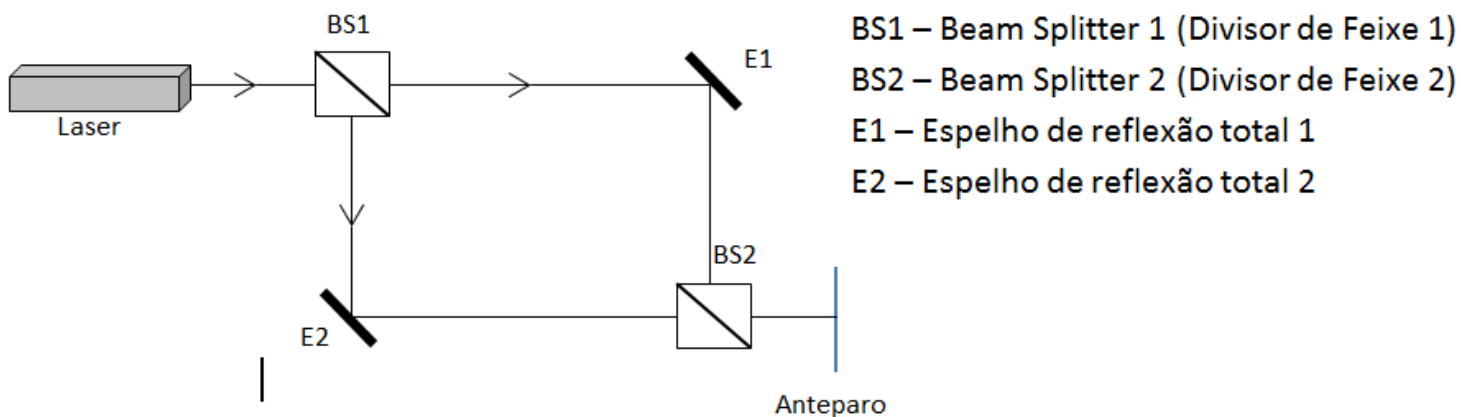


Figura 2.5: Modelo simples do Interferometro de March Zehnder. Um único feixe de entrada produzindo padrão de interferencia a saída

A figura 5 mostra o interferômetro no seu modelo clássico que é semelhante ao experimento de dupla fenda, onde os feixes divididos se encontram fazendo franjas de interferência no anteparo, porém, é possível usar o mesmo esquema para o modelo quântico apenas trocando anteparos por detectores e o laser sendo atenuado para a menor taxa de fótons possível. [7] Para a informação quântica é necessário observar o IMZ quântico. Um caso ideal seria com uma fonte que emite fótons individuais. Semelhante à fenda dupla, o fóton ao passar pelo primeiro BS, tomaria dois caminhos simultâneos, onde se encontraria no segundo BS fazendo a interferência “dele com ele

mesmo”. O fóton neste caso está em um estado de superposição no qual o percurso se torna indistinguível, equação para esses estado pode ser escrito por,

$$\psi(x, t) = \frac{1}{\sqrt{2}}(\psi_A + \psi_B) \quad (2.3.3)$$

O que a Mecânica Quântica propõe é que o fóton combina consigo mesmo construtivamente nas regiões de detecção, com isso, sendo emitidos vários fótons, é possível ver o padrão de interferência. Semelhante ao experimento da dupla fenda, onde a partir do momento em que se tenta observar por qual fenda o fóton passa o padrão de interferência deixa de aparecer, no IMZ ao tentar medir o fóton em qualquer um dos percursos, o padrão de interferência também deixa de aparecer e o fóton irá passar em um dos dois caminhos quebrando assim o estado de superposição.

A comunicação quântica no IMZ de forma ideal terá metade do interferômetro responsável pela emissão de Qubits e a outra metade para a detecção, ou seja, metade sendo Alice e a outra metade sendo Bob. As chaves, que agora são dados pela fase, podem sair com fase de $\phi = 0, \frac{\pi}{2}, \pi$ e $\frac{3\pi}{2}$. Uma propriedade ótica de reflexão de onda, é que toda onda refletida em uma superfície tem sua fase alterada em $\frac{\pi}{2}$, no caso do BS tem 50% de reflexão e 50% de transmissão, isso significa que a parte transmitida não terá a fase alterada, enquanto a refletida sofrerá uma mudança na fase de $\frac{\pi}{2}$. Acontece de forma semelhante a uma onda mecânica em uma corda com uma de suas extremidades presa a uma superfície. Essa teoria se torna importante para a explicação de dois moduladores de fase que será colocado por Alice e Bob, pois na comunicação apenas interessa as interferências construtivas, causados por fótons coincidentes entre Alice e Bob, onde os moduladores serão responsáveis por construí-los às bases. A recombinação pode ser mostrada através dos coeficientes de transmissão e reflexão como mostra a figura a seguir.

Neste caso o interferômetro é equilibrado, $|R|^2 = |T|^2 = \frac{1}{2}$, onde Bob mantém sua fase colocada em zero e Alice entre zero e π , Bob ver o pulso surgir no braço

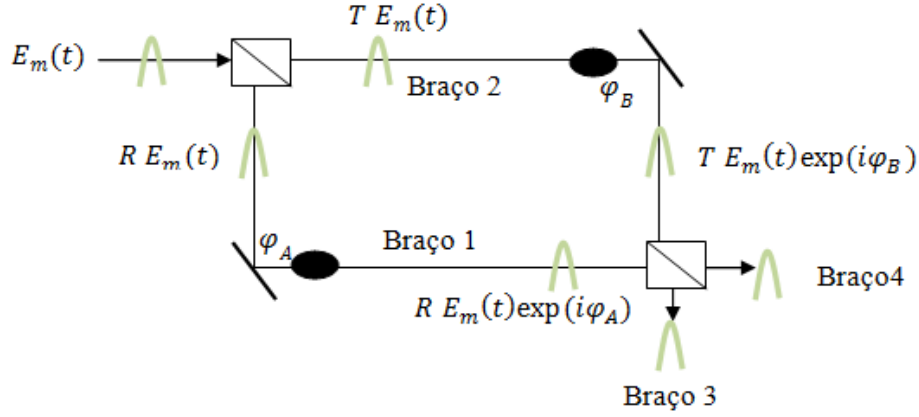


Figura 2.6: Pulso clássico enviado por Alice. Os coeficientes de transmissão e reflexão dentro do interferômetro pode resultar nas intensidades de saída no braço 3 e 4

4 ou 3, respectivamente. Com isso a mudança de fase $(0) \equiv 1$, a mudança de fase $(\pi) \equiv 0$, o braço 3 $\equiv 1$, o braço 4 $\equiv 0$, havendo uma comunicação binária entre Alice e Bob. O pulso incidente de intensidade $|E_m(t)|^2$ é dividido em dois feixes de intensidades $|R|^2 |E_m(t)|^2$ e $|T|^2 |E_m(t)|^2$. Na separação, pode-se considerar que um feixe é transmitido, seguindo em frente, e o outro feixe é refletido sofrendo uma mudança de $\frac{\pi}{2}$ na fase, dessa forma, sendo a intensidade proporcional ao quadrado do campo elétrico, são calculados os seguintes valores:

Intensidade no Braço 3:

$$I_3 = E_m^2(t) \left\{ 1 - 4 |R|^2 |T|^2 \cos^2 \left(\frac{\phi_A - \phi_B}{2} \right) \right\} \quad (2.3.4)$$

Intensidade no Braço 4:

$$I_4 = 4 E_m^2(t) |R|^2 \cos^2 \left(\frac{\phi_A - \phi_B}{2} \right) \quad (2.3.5)$$

Para um interferômetro sem perda (ideal), onde $|R|^2 + |T|^2 = 1$, com BS idênticos e os espelhos refletores com reflexão total. O feixe transmitido e refletido no primeiro divisor de feixe será de mesma intensidade e não haverá perdas no sistema, porem a uma diferença de fase de $\frac{\pi}{2}$ quando o feixe é refletido, neste caso se for enviado um Qubit $|0\rangle_A$, a parte transmitida continuará $|0\rangle_A$ e a parte refletida, com a diferença

de fase, tornam-se $|1\rangle_A$. Esse exemplo seria o caso do fóton individual em seu estado de número, ou seja, um caso completamente ideal e teórico para exemplificar a comunicação. A figura a seguir mostra todo o comportamento do Qubit durante o percurso no interferômetro, dessa forma podemos deduzir as informações na saída.

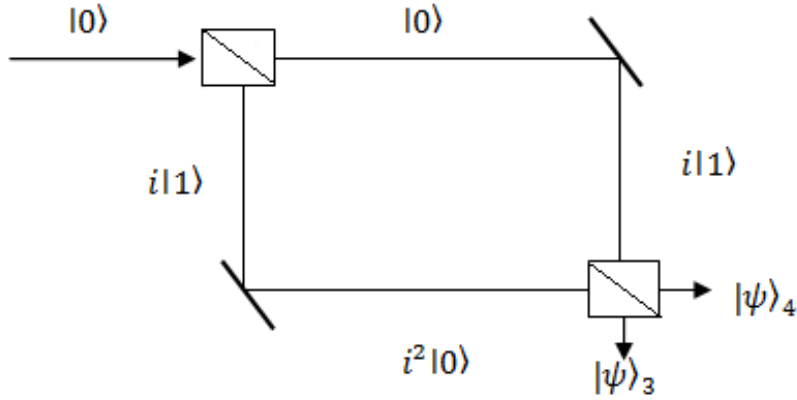


Figura 2.7: Interferômetro ideal sem moduladores de fase. O Qubit sofre uma variação de $\frac{\pi}{2}$ ao passar por cada espelho.

Da mesma forma escrita na figura, vamos analisar o Qubit $|0\rangle$ sem a presença de moduladores de fase. Sendo um Qubit um auto-estado do fóton a variação é dada por:

$$|0\rangle \xrightarrow{\frac{\pi}{2}} e^{i\frac{\pi}{2}} |1\rangle = i |1\rangle \xrightarrow{\frac{\pi}{2}} e^{i\frac{\pi}{2}} |0\rangle = i^2 |0\rangle \dots \quad (2.3.6)$$

Analisando agora os qubits detectados no braço 3 e no braço 4, tem-se uma superposição, pois chegarão feixes de duas direções recombinando-se nos dois braços. Para o braço 3, podemos medir a superposição, do feixe transmitido $i|1\rangle$ e o feixe refletido $i^3|1\rangle$, da seguinte forma:

$$|\psi\rangle_3 = i|1\rangle + i^3|1\rangle = i|1\rangle - i|1\rangle = 0 \quad (2.3.7)$$

O mesmo para o braço 4:

$$|\psi\rangle_4 = i^2|0\rangle - i^2|0\rangle = -2|0\rangle \quad (2.3.8)$$

Neste caso, como o feixe não tem perdas, Bob detecta o qubit $|0\rangle$ com alta probabilidade, pois no braço 3 não chegará o feixe por ser uma interferência destrutiva.

Adicionando os moduladores de fase, assim como visto no esquema com polarização, os moduladores servirão como bases que deverão ser escolhidos aleatoriamente. Como visto na figura 2.6, Alice tem um modulador ϕ_A e Bob tem um modulador ϕ_B , eles deverão escolher bits de acordo com as tabelas dado por [6] escrito abaixo.

Tabela 2.1: Esquema de codificação empregada por Alice. O valor do bit será dado de acordo com a configuração do modulador podendo ter duas formas de codificação do mesmo bit.

Alice	
Definição da Fase	Valor do Bit
0	0
π	1
$\pi/2$	0
$3\pi/2$	1

Tabela 2.2: Sistema de medição de bits empregado por Bob. O fóton medido no braço 3 é lido como 1 e, o fóton medido no braço 4, é lido como 0. A escolha da configuração do modulador dá a Bob dois códigos diferentes para o mesmo bit.

Bob	
Definição da Fase	Valor do Bit
0	0 (braço 4)
	1 (braço 3)
$\pi/2$	0 (braço 4)
	1 (braço 3)

Bob define cada braço da saída para uma medida, o braço 4 para medir o Qubit 0 e o braço 3 para medir o Qubit 1. Quando a diferença de fase entre ϕ_A e ϕ_B for de 0 ou π , Alice e Bob estão usando bases compatíveis e obtêm resultados determinísticos, no caso em que a diferença seja de $\pi/2$ ou $3\pi/2$, o fóton pode ir a um detector ou a outro causando uma incerteza na medição. A tabela a seguir dado por [8] mostra um esquema simples de como foi as medidas.

No caso em que a diferença de fase é de $\pi/2$ ou de $3\pi/2$, as bases são incompatíveis e os fótons escolhe aleatoriamente em qual porta irá sair. Uma observação a ser feita é que a distância dos dois caminhos devem se manter estável, pois um caminho

Tabela 2.3: Comunicação feita com o código de fase no IMZ entre Alice e Bob para quatro estos

Alice		Bob		
Valor do Bit emitido	ϕ_A	ϕ_B	$\phi_A - \phi_B$	Valor do Bit medido
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$?
0	$\pi/2$	0	$\pi/2$?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$?
1	$3\pi/2$	$\pi/2$	π	1

muito longo pode alterar a fase do fóton gerando uma diferença de fase causando erro nas medidas. Para uma análise mais geral, podemos comparar com o código de fase explicado no BB84, onde fótons com polarizações em diagonal entram em superposição quando passa em um polarizador vertical/horizontal. Usando a fase do fóton individual é possível calcular a probabilidade devido ao estado ser descrito no espaço Hilbert bidimensional, com isso, o estado de saída de Alice pode ser dado por:

$$|\psi_{Alice}(\varphi_A)\rangle = \frac{1}{\sqrt{2}} \{|1, 0\rangle + i \exp(i\varphi_A) |0, 1\rangle\} \quad (2.3.9)$$

A notação $|1, 0\rangle$ e $|0, 1\rangle$ representam os estados do braço 1 e do braço 2, podendo ser usados como bases do fóton individual no interferômetro medido pelo espaço de Hilbert bidimensional. O fóton transmitido será o estado $|1, 0\rangle$, pois, desta notação, significa que passou um fóton no braço 2 e nenhum no braço 1, já o transmitido será $|0, 1\rangle$ significando que passou um fóton no braço 1 e nenhum no braço 2. Esses estados formam uma superposição quântica mostrado na equação (2.3.9), onde o termo do braço 1 apresenta a variação $\exp(i\varphi_A)$ devido ao modulador de fase. Dessa forma, se

torna possível mostrar os estados escolhidos por Alice que podem ser:

$$|\psi_{Alice}(0)\rangle = \frac{1}{\sqrt{2}} \{|1, 0\rangle + i |0, 1\rangle\} \quad (2.3.10)$$

$$|\psi_{Alice}(\pi)\rangle = \frac{1}{\sqrt{2}} \{|1, 0\rangle - i |0, 1\rangle\} \quad (2.3.11)$$

$$|\psi_{Alice}(\pi/2)\rangle = \frac{1}{\sqrt{2}} \{|1, 0\rangle - |0, 1\rangle\} \quad (2.3.12)$$

$$|\psi_{Alice}(3\pi/2)\rangle = \frac{1}{\sqrt{2}} \{|1, 0\rangle + |0, 1\rangle\} \quad (2.3.13)$$

Onde os estados $|\psi_{Alice}(0)\rangle$ e $|\psi_{Alice}(\pi)\rangle$ são ortonormais assim como $|\psi_{Alice}(\pi/2)\rangle$ e $|\psi_{Alice}(3\pi/2)\rangle$. Pode-se dizer que essas bases tem máxima incompatibilidade, que é a situação da polarização circular e linear. A expansão do estado 0 nas bases $\pi/2$ e $3\pi/2$ é dado por:

$$|\psi_{Alice}(0)\rangle = \frac{1}{2} (1 - i) |\psi_{Alice}(\pi)\rangle + \frac{1}{2} (1 + i) |\psi_{Alice}(3\pi/2)\rangle \quad (2.3.14)$$

Que substituindo as equações (2.3.12) e (2.3.13) volta a equação (2.3.10). Sendo que a medida do estado 0 nas bases $\pi/2$ e $3\pi/2$ pode produzir um resultado probabilístico com 50% de chance de de leitura do bit incorreto. Se Bob seleciona seu modulador de fase entre 0 e $\pi/2$, ele consegue ter uma base de medida.

Com a comunicação feita entre Alice e Bob, os procedimentos após as medidas serão iguais aos mostrados no protocolo BB84 onde os dois se comunicam por um canal publico e combinam as bases que deram certo.

Para a implementação experimental, é necessário o entendimento da teoria do BS e de estados quânticos usados em laboratórios, todas elas serão explicados no próximo capítulo.

Capítulo 3

Beam Splitter e o Interferômetro

Um dos experimentos mais importantes da Mecânica Quântica foi à comprovação da dualidade onda-partícula tanto do fóton quanto do elétron. O experimento da dupla fenda mostra que uma única partícula pode tomar dois caminhos diferentes simultaneamente quando não há presença de um observável, e causar um padrão de interferência, ou seja, partículas que se comportam como onda.

O Beam Splitter é um espelho semi-refletor que tem o objetivo de dividir um feixe de luz em dois, porém quanticamente pode ser visto como um experimento de dupla fenda, onde um único fóton pode tomar dois caminhos diferentes simultaneamente. Neste capítulo será mostrada toda a teoria quântica de um BS junto à montagem do IMZ Quântico com dois BS para formar padrões de interferência.

3.1 Teoria quântica do Beam Splitter

Em um tratamento clássico de feixes de luz entrando em um BS, torna-se fácil observar o comportamento do feixe depois do BS, o que acontece é que um feixe clássico tem uma taxa de fótons muito alta e que em um BS 50:50 (50% refletor e 50% transmissor), por exemplo, a soma das intensidades do feixe transmitido e o feixe refletido dá o feixe emitido. Porém quando temos um emissor de poucos fótons ou até mesmo de um fóton individual temos resultados diferentes devido ao comportamento que deixa de

ser clássico para ser quântico.

Analisando um feixe clássico passando por um BS sem perdas, um campo complexo de amplitude E_1 é dividido em dois feixes de amplitude E_2 e E_3 onde esses são os feixes refletidos e transmitidos respectivamente como mostra na figura a seguir.

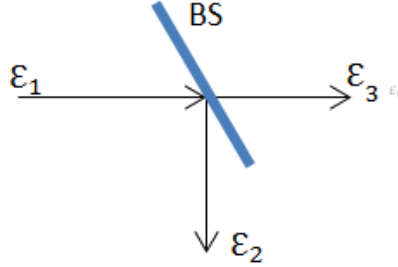


Figura 3.1: Esquema do BS clássico. Um campo eletromagnético de entrada gerando um campo refletido e outro transmitido.

Assim é possível dizer que a intensidade dos feixes refletidos e transmitidos é de $E_2 = rE_1$ e $E_3 = tE_1$ respectivamente, que para um BS de 50:50 tem-se $|r| = |t| = 1/\sqrt{2}$. Como foi imposta uma situação ideal de um BS sem perda, a intensidade do feixe de entrada deve ser igual à soma das intensidades dos dois feixes de saída:

$$|E_1|^2 = |E_2|^2 + |E_3|^2 \quad (3.1.1)$$

Isso implica dizer que:

$$|r|^2 + |t|^2 = 1 \quad (3.1.2)$$

Para tratar o problema quanticamente poderíamos trocar a amplitude E_i pelo o operador de aniquilação bosônico \hat{a}_i ($i=1,2,3\dots$) com $\hat{a}_2 = r\hat{a}_1$ e $\hat{a}_3 = t\hat{a}_1$ como mostra a figura a seguir:

Porém isso é uma descrição errada da mecânica quântica, pois todos esses operadores satisfaz a relação de comutação a seguir.

$$\left[\hat{a}_i, \hat{a}_j^\dagger \right] = \delta_{ij}, \quad \left[\hat{a}_i, \hat{a}_j \right] = 0 = \left[\hat{a}_i^\dagger, \hat{a}_j^\dagger \right], \quad (i, j = 1, 2, 3) \quad (3.1.3)$$

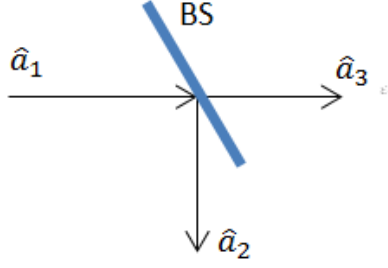


Figura 3.2: Esquema ERRADO do modelo quântico do BS. Um estado de entrada não pode gerar dois estados de saída como descrito na figura

Sendo que, na forma escrita anteriormente, comutando os operadores encontra-se:

$$\begin{aligned}
 [\hat{a}_2, \hat{a}_2^\dagger] &= |r|^2 [\hat{a}_1, \hat{a}_1^\dagger] = |r|^2, \\
 [\hat{a}_3, \hat{a}_3^\dagger] &= |t|^2 [\hat{a}_1, \hat{a}_1^\dagger] = |t|^2, \\
 [\hat{a}_2, \hat{a}_3^\dagger] &= rt^* \neq 0, \text{ etc.}
 \end{aligned}
 \tag{3.1.4}$$

Essas expressões não preservam a relação de comutação, ou seja, não corresponde a uma descrição quântica correta do BS. Isso acontece pelo fato de ter uma porta de entrada que não está sendo considerada, classicamente essa porta não tem efeito nenhum nas portas de saída, porém quanticamente essa porta é um campo quantizado chamado de estado de vácuo ou vácuo quântico que é o estado de mais baixa energia da natureza. O operador do vácuo é representado como \hat{a}_0 e faz parte do estado de entrada junto com o \hat{a}_1 , porem em braços diferentes, isso dá a possibilidade de ter um BS assimétrico. Desta forma é possível escrever:

$$\begin{aligned}
 \hat{a}_2 &= r\hat{a}_1 + t'\hat{a}_0, \\
 \hat{a}_3 &= t\hat{a}_1 + r'\hat{a}_0
 \end{aligned}
 \tag{3.1.5}$$

ou em termos de matriz

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \begin{pmatrix} t' & r \\ r' & t \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix}
 \tag{3.1.6}$$

Podendo agora representar o esquema de forma correta

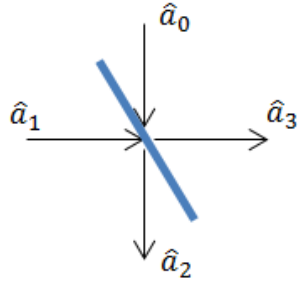


Figura 3.3: Esquema CERTO do modelo quântico do BS. o vácuo quântico representado por \hat{a}_0 entra pela porta onde não passa fótons

Fazendo novamente a comutação é possível ver os seguintes resultados

$$\begin{aligned}
 [\hat{a}_2, \hat{a}_2^\dagger] &= |r|^2 + |t'|^2 \\
 [\hat{a}_3, \hat{a}_3^\dagger] &= |r'|^2 + |t|^2 \\
 [\hat{a}_2, \hat{a}_3^\dagger] &= rt^{**} + t'r'^* \\
 [\hat{a}_3, \hat{a}_2^\dagger] &= tr^* + r't'^*
 \end{aligned} \tag{3.1.7}$$

satisfazendo as relações a seguir, fica fácil ver que todas as comutações satisfaz a equação (3.1.3)

$$|r'| = |r|, \quad |t'| = |t|, \quad |r|^2 + |t|^2 = 1, \quad r^*t' + r't'^* = 0 \quad e \quad r^*t + r't'^* = 0 \tag{3.1.8}$$

Essas relações são conhecidas como as relações de reciprocidade e também pode ser derivada com base na conservação de energia. Pode-se também enfatizar que o BS contruido para que a diferença da fase entre o refletido e o transmitido é de $e^{\pm i\pi/2}$ ou simplesmente $\pm i$, ou seja, o refletido sofre uma mudança de fase de $\pi/2$ gerando uma relação nos estados de entrada e saída da seguinte forma:[9]

$$\begin{aligned}\hat{a}_2 &= \frac{1}{\sqrt{2}} (\hat{a}_0 + i\hat{a}_1) \\ \hat{a}_3 &= \frac{1}{\sqrt{2}} (i\hat{a}_0 + \hat{a}_1)\end{aligned}\tag{3.1.9}$$

No modelo de Schrödinger é possível saber o estado de saída do BS quando já se sabe o estado de entrada, isso acontece devido à ação dos operadores de criação e aniquilação agindo no estado do vácuo dos meios de saída, ou seja, antes do BS existem dois estado que pode ser de número e vácuo, por exemplo, e na saída já existem dois estados de vácuo que sofrerão a ação dos operadores de criação e aniquilação construindo assim o estado de saída. Quando não existe nenhum estado de saída podemos considerar a seguinte transformação

$$|0\rangle_0 |0\rangle_1 \xrightarrow{BS} |0\rangle_2 |0\rangle_3\tag{3.1.10}$$

Um exemplo é quando temos um único fóton entrando em uma das portas e o vácuo quântico entrando na outra porta $|0\rangle_0 |1\rangle_1$ que pode ser escrito como $\hat{a}_1^\dagger |0\rangle_0 |0\rangle_1$. Para o BS descrito na equação (3.1.9) temos o seguinte operador $\hat{a}_1^\dagger = (i\hat{a}_2^\dagger + \hat{a}_3^\dagger) / \sqrt{2}$, dessa forma o estado de saída que inicialmente está igual a equação (3.1.10) torna-se:

$$|0\rangle_0 |1\rangle_1 \xrightarrow{BS} \frac{1}{\sqrt{2}} (i\hat{a}_2^\dagger + \hat{a}_3^\dagger) |0\rangle_2 |0\rangle_3 = \frac{1}{\sqrt{2}} (i|1\rangle_2 |0\rangle_3 + |0\rangle_2 |1\rangle_3)\tag{3.1.11}$$

Este resultado mostra que um fóton único passando por um BS causa uma superposição entre os dois braços de saída, onde o feixe é transmitido e refletido com iguais probabilidades porem com fases diferentes. Segundo [9] o BS é um dispositivo ativo que não cria nem destroi fótons, apenas gera a superposição.

Por outro lado, a transformação entre os estados de saída e de entrada devem ser unitária e podendo reescrever a equação (3.1.6) como

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \hat{U}^\dagger \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix} \hat{U}\tag{3.1.12}$$

Onde \hat{U} é um operador unitário. Essa transformação é a fórmula do BS no modelo de Heisenberg. Em termos dos operadores criação e aniquilação dado pela equação (3.1.9) o operador de rotação pode ser escrito da seguinte forma:

$$\hat{U} = \exp \left[i \frac{\pi}{4} \left(\hat{a}_0^\dagger \hat{a}_1 + \hat{a}_0 \hat{a}_1^\dagger \right) \right] \quad (3.1.13)$$

As duas representações, tanto de Schrödinger quando de Heisenberg, representam as transformações em um estado quântico qualquer, isso conclui que o BS é apenas um operador responsável por gerar uma superposição no estado, porém ainda existe uma representação que mostra mais características as essa transformação e que gera medidas experimentais, a representação de Schwinger. Essa representação faz correspondência ao grupo SU(2) e SU(3) e mostra a rotação nos vetores tridimensionais do momento angular quântico. O vetor momento angular pode ser escrito como:

$$\mathbf{J} = \begin{pmatrix} J_x \\ J_y \\ J_z \end{pmatrix} = \frac{1}{2} \begin{pmatrix} a^\dagger b + b^\dagger a \\ -i (a^\dagger b - b^\dagger a) \\ a^\dagger a + b^\dagger b \end{pmatrix} \quad (3.1.14)$$

que é comprovado pela relação de comutação canônica

$$[J_i, J_j] = i \epsilon_{ijk} J_k, \text{ etc.} \quad (3.1.15)$$

ou seja

$$[J_x, J_y] = i J_z, \text{ etc.} \quad (3.1.16)$$

e o módulo quadrado de \mathbf{J} como sendo

$$J^2 = \frac{a^\dagger a + b^\dagger b}{2} \left(\frac{a^\dagger a + b^\dagger b}{2} + 1 \right) = \frac{N_a + N_b}{2} \left(\frac{N_a + N_b}{2} + 1 \right) \quad (3.1.17)$$

onde $N_a = a^\dagger a$ e $N_b = b^\dagger b$ é o operador de número de fótons das portas a e b respectivamente.

O J^2 é relacionado como o número total de fótons no sistema, que se conserva dependendo do numero total de fótons no sistema óptico inteiro. J_z é a diferença de intensidade entre as portas a e b. J_x e J_y são os termos responsáveis pela diferença de fase. Em questão da medida para os estados de Fock, a informação da diferença de fase dos estados de entradas é indeterminada, no entanto, a diferença de fase da dos estados de saída são determinados e medidos, pois o BS troca a intensidade e a flutuação entre a entrada e a saída do feixe. O esquema dado por [10] mostra como acontece as medições para o caso clássico em que levamos em consideração os campos eletromagnéticos nas portas, como por exemplo o estado coerente, que será explicado no próximo capítulo, e os relacionam com os momentos angulares J_x e J_y .

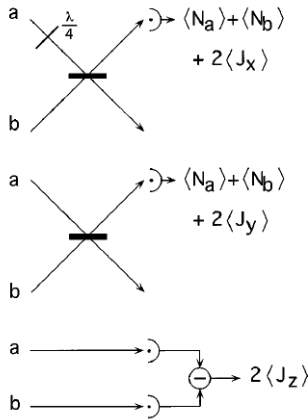


Figura 3.4: Figura retirada de [10] que mostra as medidas físicas na representação de Schwinger nos fotodetectores em termos das três componentes do momento angular

A equação a seguir mostra a relação entre os campos e os momentos angulares onde ϕ_a e ϕ_b são números reais que representam o ângulo da fase de cada braço.

$$\left[E_a^{(-)} + E_b^{(-)} \right] \left[E_a^{(+)} + E_b^{(+)} \right] = N_a + N_b + 2J_x \cos(\phi_a - \phi_b) + 2J_y \sin(\phi_a - \phi_b) \quad (3.1.18)$$

Os auto estados de J^2 e J_z são idênticos aos auto estados dos números de fótons N_a e N_b , ou seja:

$$|n_a n_b\rangle = |j \mu\rangle_z \quad (3.1.19)$$

Sendo n_a e n_b autovalores de N_a e N_b e os autovalores de J^2 é $j(j+1)$ e o autovalor de J_z é μ . Logo obtemos a seguinte relação

$$\begin{aligned} j &= \frac{n_a + n_b}{2} = \frac{N}{2} \\ \mu &= \frac{n_a - n_b}{2} \end{aligned} \quad (3.1.20)$$

Onde N é o número total de fótons. Com essas propriedades é possível "transformar" número de fótons em momento angular, dois exemplos fáceis de verificar, uma é de N fótons entrando em uma porta e nenhum entrando na outra resultando em $|N0\rangle = |jj\rangle_z$ e outra é a entrada de fótons gêmeos que resulta em $|\frac{N}{2} \frac{N}{2}\rangle = |j0\rangle_z$.

Na representação de Schwinger, a rotação dos estados de entrada é equivalente ao modelos de Heisenberg

$$J^{out} = e^{i\alpha J_z} e^{i\beta J_y} e^{i\gamma J_z} J^{in} e^{-i\alpha J_z} e^{-i\beta J_y} e^{-i\gamma J_z} \quad (3.1.21)$$

e ao modelo de Schrödinger

$$|\psi_{out}\rangle = e^{-i\alpha J_z} e^{-i\beta J_y} e^{-i\gamma J_z} |\psi_{in}\rangle \quad (3.1.22)$$

Em um BS sem perdas, como já foi visto, a diferença de fase entre os feixes transmitido e refletido é de $\pi/2$, isso corresponde a uma matriz

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \begin{pmatrix} r & \pm it \\ \pm it & r \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix} \quad (3.1.23)$$

onde r e t são raízes quadrada do coeficiente de intensidade de fresnel, para isso é preciso usar um formalismo para um sistema de quatro portas em termos da rotação e do espaço tridimensional abstrato demonstrado por Yurke [15] que é análogo ao formalismo do vetor de Bloch de um sistema atômico de dois níveis ou do vetor de polarização

da esfera de Poincaré.

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \begin{pmatrix} \cos\frac{\beta}{2}e^{i(\alpha+\gamma)/2} & \text{sen}\frac{\beta}{2}e^{i(\alpha-\gamma)/2} \\ -\text{sen}\frac{\beta}{2}e^{-i(\alpha-\gamma)/2} & \cos\frac{\beta}{2}e^{-i(\alpha+\gamma)/2} \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix} \quad (3.1.24)$$

Onde α , β e γ são os angulos de Euler.

O importante desse formalismo é que qualquer perda passiva em um sistema óptico de quatro portas é descrito por uma matriz 2×2 . Essa matriz opera como um vetor bidimensional onde cada componente são as duas amplitudes de campo em cada porta do sistema.

Existe uma correspondencia entre os coeficientes de reflexão e transmissão com os angulos da equação (3.1.24) onde $\alpha = -\gamma$, $\beta = \pm\varphi = \pm 2\arccos(r)$ para $(0 \leq \varphi \leq \pi)$

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \begin{pmatrix} \cos\frac{\varphi}{2} & \pm i\text{sen}\frac{\varphi}{2} \\ \pm i\text{sen}\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix} \quad (3.1.25)$$

ou correspondendo ao grupo SU(3) envolvendo os vetores de momento angular segundo [11]

$$e^{-i\varphi J_x} \begin{pmatrix} J_x^{in} \\ J_y^{in} \\ J_z^{in} \end{pmatrix} e^{i\varphi J_x} = \begin{pmatrix} J_x^{out} \\ J_y^{out} \\ J_z^{out} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & \pm\text{sen}\varphi \\ 0 & \mp\text{sen}\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} J_x^{in} \\ J_y^{in} \\ J_z^{in} \end{pmatrix} \quad (3.1.26)$$

que equivale a rotação da luz de $\pm\varphi$ em torno do eixo x. No caso do BS sem perdas a rotação é de $\pi/2$ em torno de x isso faz com que a equação (3.1.21) fique

$$J_z^{out} = e^{\mp i\frac{\pi}{2}J_x} J_z^{in} e^{\pm i\frac{\pi}{2}J_x} = \mp J_y^{in} \quad (3.1.27)$$

ou da equação (3.1.22) fica

$$|\psi_{out}\rangle = e^{\pm i\frac{\pi}{2}J_x} |j\mu\rangle_z = |j \pm \mu\rangle_y \quad (3.1.28)$$

Estas equações mostra um resultado interessante, prova que a medida da diferença de intensidade fora do BS trás informação sobre a diferença de fase na sua entrada, é fácil observar na equação (3.1.27) que, falando agora do Interferômetro de Mach

Zehnder na região onde se encontra os dois BS, só é preciso se preocupar com as propriedades quânticas da intensidade da luz antes e depois dos dois BS's para obter informações sobre θ , ou seja, não há necessidade de uma definição de um operador de fase quântica para modelar as medições de um interferômetro.[10]

Sabendo que as transformações são unitárias e existe a aplicação de uma matriz de rotação já citada na equação (3.1.13), na representação de Schwinger essa matriz é escrita em termos de j e μ e tem a seguinte forma ([10][12])

$$d_{\mu'\mu}^j = \langle j\mu' | e^{-i\varphi J_y} | j\mu \rangle = \left[\frac{(j+\mu)!(j-\mu)!}{(j+\mu')!(j-\mu')!} \right]^{\frac{1}{2}} \left(\sin \frac{\varphi}{2} \right)^{\mu-\mu'} \left(\cos \frac{\varphi}{2} \right)^{\mu+\mu'} \times P_{j-\mu}^{(\mu-\mu', \mu+\mu')}(\cos \varphi) \quad (3.1.29)$$

Para o deslocamento da fase é fácil observar que o BS causa uma mudança no ângulo da seguinte forma

$$e^{-i\theta J_z} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix} e^{-i\theta J_z} = \begin{pmatrix} a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix} \quad (3.1.30)$$

que significa uma rotação de θ em torno do eixo z, tomando essa a referencia os ângulos de Euler são $\alpha + \gamma = \theta$ e $\beta = 0$ que significa apenas rotações no eixo x e y alterando a interferência entre J_x e J_y sem alterar a intensidade J_z , com isso o momento angular pode ser escrito como

$$\mathbf{J}^{out} = e^{i\theta J_z} \mathbf{J}^{in} e^{-i\theta J_z} \quad (3.1.31)$$

$$|\psi_{out}\rangle = e^{-i\theta J_z} |\psi_{in}\rangle \quad (3.1.32)$$

Toda a matemática e formalismo apresentados nesta seção são apenas ferramentas para as futuras aplicações nos próximos capítulos.

3.2 Interferômetro na Representação de Schwinger

Já foi comentado sobre o Interferômetro de Mach Zehnder com dois BS no capítulo anterior, nesta seção será apresentado rapidamente o interferômetro usando a teoria do momento angular quântico e a forma de medição da intensidade e da fase.

A interferometria o IMZ apresenta três operações unitárias devido ao primeiro BS na entrada, a uma mudança de fase θ e ao segundo BS na saída [10]. Essas operações podem ser representadas como

$$|\psi_{out}\rangle = e^{-i\frac{\pi}{2}J_x} e^{-i\theta J_z} e^{i\frac{\pi}{2}J_x} |\psi_{in}\rangle = e^{-i\theta J_y} |\psi_{in}\rangle \quad (3.2.33)$$

que é simplificado como uma rotação de mudança de fase do interferômetro em volta do eixo y ($\alpha = \gamma = 0, \beta = \theta/2$) ou seja

$$e^{-i\theta J_y} \begin{pmatrix} J_x^{in} \\ J_y^{in} \\ J_z^{in} \end{pmatrix} e^{i\theta J_y} = \begin{pmatrix} J_x^{out} \\ J_y^{out} \\ J_z^{out} \end{pmatrix} = \begin{pmatrix} \cos\theta & 0 & -\sin\theta \\ 0 & 1 & 0 \\ \sin\theta & 0 & \cos\theta \end{pmatrix} \begin{pmatrix} J_x^{in} \\ J_y^{in} \\ J_z^{in} \end{pmatrix} \quad (3.2.34)$$

Uma observação sobre esta equação é a mudança da variável φ para θ . Isso acontece por não tratar apenas do BS individual e sim da montagem do interferômetro, logo existe uma diferença de fase distinta entre os dois casos.

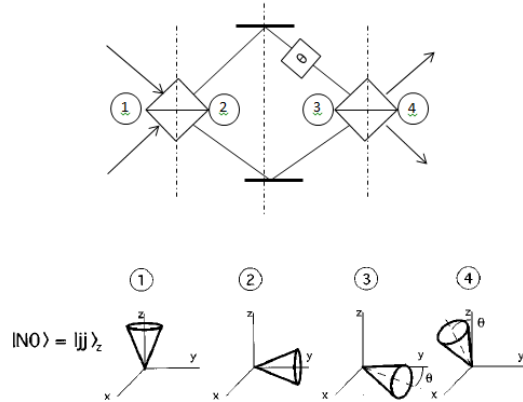


Figura 3.5: Figura retirada de [10] que mostra o passo a passo das rotações do momento angular

Ilustrado o IMZ, sendo agora com a representação de Schwinger, a diferença de

intensidade da saída do interferômetro dado por $N_a - N_b$ é dado pela projeção de \mathbf{J} no eixo z e a diferença de fase da entrada a e b dado por $\phi_a - \phi_b$ é dado pela projeção do angulo azimutal de \mathbf{J} no plano xy. Para apenas o fóton individual na entrada do IMZ, é escrito como $|N0\rangle = |jj\rangle_z$, isso significa que $\mu = j$ vindo da equação (3.1.20) o que na ilustração a cima forma um cone de geratriz $[j(j+1)]^{1/2}$ e altura j que sofre as rotações devido a cada passo. Do passo 1 para o passo 2 acontece uma rotação de $\pi/2$ em torno do eixo x, do passo 2 para o passo 3 passa por um defasador que causa uma mudança θ do eixo em que ja se encontra, do passo 3 para o passo 4, onde passa pelo segundo BS, acontece mais uma rotação em torno de x. Na ilustração também fica fácil entender o porque de todos esses passos poder ser generalizado com apenas uma mudança de θ no eixo y dado pela equação (3.2.33).

Essa figura também ilustra a incerteza de Heisenberg entre as componentes do momento angular na representação de Schwinger. Antes de calcular isso é preciso saber que a relação de incerteza de Heisenberg entre a diferença do número de fótons e a diferença da fase é dada por

$$\Delta(N_a - N_b) \Delta(\phi_a - \phi_b) \geq 1 \quad (3.2.35)$$

Isso significa que um mínimo $\Delta(\phi_a - \phi_b)$ depois de entrar no BS é equivalente ao máximo $\Delta(N_a - N_b)$ em algum ponto, no entanto fica claro que a incerteza máxima na intensidade depois do BS é obtida a partir da máxima incerteza antes do BS devido a rotação de $\pi/2$ do estado. Com as informações a cima sobre o cone, com teorema de Pitágoras é calculado a base do mesmo como sendo \sqrt{j} que corresponde a $\Delta J_{x,y} = \sqrt{j}$ o que faz ocorrer após o BS no limite padrão ([13],[10]).

$$\Delta(\phi_a - \phi_b) \geq \frac{1}{\Delta(N_a - N_b)} = \frac{1}{2\sqrt{j}} = \frac{1}{\sqrt{2N}} \quad (3.2.36)$$

A mudança de fase θ , que pode ser identificada na saída do interferômetro, pode ser medido pelas intensidades subtraída dos dois detectores nos braços de saída do

IMZ. Esta diferença é proporcional a diferença de um operador de número onde os operadores $(\hat{a}, \hat{a}^\dagger)$ representa um detector e os operadores $(\hat{b}, \hat{b}^\dagger)$ o outro detector, ou seja, esse operador número é dado por $\hat{O} = \hat{a}\hat{a}^\dagger - \hat{b}\hat{b}^\dagger$. Com isso, usando o calculo de propagação de erro, a incerteza da fase medida na saída do IMZ é dado por

$$\Delta\theta = \frac{\Delta O}{\frac{\partial \langle O \rangle}{\partial \theta}} \quad (3.2.37)$$

onde $\Delta O = \sqrt{\langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2}$. O operador número também pode ser escrito em termos de J_z sendo $\hat{O} = J_z$.

A grande importância das equações (3.2.37) é que pode ser medida experimentalmente e é ela que dá as características de uma comunicação quântica onde é preciso ter a mínima incerteza possível na fase medida pelos detectores. Essas equações terão mais clareza nos próximos assuntos abordados quando for aplicado outros estados quânticos e será de grande importância para o resultado deste trabalho.

Capítulo 4

Estado Coerente no Interferômetro de Mach-Zehnder

Neste capítulo é apresentado a respeito de estados coerentes do campo de radiação e seu uso em uma das portas de entrada do IMZ. À semelhança do artigo [14] apresentamos uma discussão sobre a estimação de fase nesse estado. A grande importância deste estado é a sua aproximação clássica, podendo ser chamado de estado semi-clássico, com isso é possível fazer um experimento manipulando o estado de entrada sendo ele o estado coerente.

Vimos até agora, o estado de número $|n\rangle$ que pode representar o fóton individual e que tem uma fase indefinida com distribuição de probabilidade.

4.1 O Estado Coerente

Para existir algum valor no operador do campo elétrico, ou seja, $\langle \hat{E} \rangle \propto \langle f(\hat{a}^\dagger, \hat{a}) \rangle$ nos operadores de criação e aniquilação, que são obrigados a ter uma superposição no estado de número diferindo apenas de ± 1 como $|n\rangle$ e $|n+1\rangle$, ou seja

$$|\psi\rangle = C_n |n\rangle + C_{n+1} |n+1\rangle \quad (4.1.1)$$

Sendo $|C_n|^2 + |C_{n+1}|^2 = 1$. Nos esquemas tradicionais a quantização de um único modo do campo estabelece [9]

$$\begin{aligned}\hat{E}_x(z, t) &\propto (\hat{a} + \hat{a}^\dagger) \text{sen}(kz) \\ \hat{B}_y(z, t) &\propto (\hat{a} - \hat{a}^\dagger) \text{cos}(kz)\end{aligned}\quad (4.1.2)$$

No limite clássico os operadores \hat{a} e \hat{a}^\dagger não podem ser substituídos por variáveis contínuas o que tornaria o campo clássico. A maneira de realizar essa troca de forma consistente é buscar um autoestado do operador aniquilação denotado por $|\alpha\rangle$ e que satisfas a seguinte relação

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle \quad (4.1.3)$$

e de forma arbitrária

$$\langle\alpha| \hat{a}^\dagger = \alpha^* \langle\alpha| \quad (4.1.4)$$

O estado $|\alpha\rangle$ é apenas uma coleção de estados de número $|n\rangle$ que pode ser expandido da seguinte forma

$$|\alpha\rangle = \sum_{n=0}^{\infty} C_n |n\rangle \quad (4.1.5)$$

quando aplicado o operador aniquilação a equação (4.1.2) torna-se

$$\hat{a} |\alpha\rangle = \sum_{n=0}^{\infty} C_n \sqrt{n} |n-1\rangle = \alpha \sum_{n=0}^{\infty} C_n |n\rangle \quad (4.1.6)$$

sabendo que

$$C_n \sqrt{n} = \alpha C_{n-1} \quad (4.1.7)$$

ou ainda mais

$$C_n = \frac{\alpha}{\sqrt{n}} C_{n-1} = \frac{\alpha^2}{\sqrt{n(n-1)}} C_{n-2} = \dots = \frac{\alpha^n}{\sqrt{n!}} C_0 \quad (4.1.8)$$

e o resultado disso é

$$|\alpha\rangle = C_0 \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (4.1.9)$$

O importante deste resultado é ter o autovalor α e um coeficiente real que pode ser definido na normalização, ou seja

$$\langle\alpha|\alpha\rangle = 1 = |C_0|^2 \sum_n \sum_{n'} \frac{\alpha^{*n} \alpha^{n'}}{\sqrt{n!n'}} \langle n|n'\rangle = |C_0|^2 \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |n\rangle \quad (4.1.10)$$

O ultimo termo é uma expansão em série que resulta no termo $|C_0|^2 e^{|\alpha|^2}$ ou seja, o resultado para o coeficiente é $C_0 = \exp\left(-\frac{1}{2}|\alpha|^2\right)$. Dessa forma encontra-se o autoestado escrito como

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (4.1.11)$$

Existe uma realção entre o parâmetro $|\alpha|$ e a amplitude do campo elétrico, isto envolve outra relação entre esse mesmo parâmetro e o operador número de fótons $\hat{n} = \hat{a}^\dagger \hat{a}$ dando um sentido físico para medida de $|\alpha|$ com o valor esperado dado por

$$\bar{n} = \langle\alpha|\hat{n}|\alpha\rangle = \langle\alpha|\hat{a}^\dagger \hat{a}|\alpha\rangle = |\alpha|^2 \quad (4.1.12)$$

onde o $|\alpha|^2$ é apenas o número médio de fótons. Para a flutuação do número de fótons é necessário calcular

$$\langle\alpha|\hat{n}^2|\alpha\rangle = \langle\alpha|\hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a}|\alpha\rangle = \langle\alpha|\hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} + \hat{a}^\dagger \hat{a}|\alpha\rangle = |\alpha|^4 + |\alpha|^2 = \bar{n}^2 + \bar{n} \quad (4.1.13)$$

e com isso é possível determinar

$$\Delta n = \sqrt{\langle n^2 \rangle - \langle n \rangle^2} = \bar{n}^{1/2} \quad (4.1.14)$$

o que é característico no processo de Poisson. Com isso, agora se torna possível obter uma medida do número de fótons no campo. A probabilidade de medir n em um detector é de

$$P_n = |\langle n|\alpha\rangle|^2 = \exp(-\alpha^2) \frac{|\alpha|^{2n}}{n!} \quad (4.1.15)$$

ou para este caso

$$P_n = e^{-\bar{n}} \frac{\bar{n}^n}{n!} \quad (4.1.16)$$

que é uma distribuição de Poisson com uma média de \bar{n} . Para a distribuição do estado coerente, onde o termo em que o autovalor escrito em coordenadas polares $\alpha = |\alpha|^2 e^{i\theta}$ onde o ângulo θ pode ser a fase dos fótons, e a probabilidade corresponde a uma distribuição de fase como

$$P(\phi) = \frac{1}{2\pi} |\langle \phi|\alpha\rangle|^2 = \frac{1}{2\pi} e^{-|\alpha|^2} \left| \sum_{n=0}^{\infty} e^{in(\phi-\theta)} \frac{|\alpha|^n}{\sqrt{n!}} \right|^2 \quad (4.1.17)$$

Para um $|\alpha|^2$ muito grande, a distribuição de Poisson deve se aproximar de uma Gaussiana, isso acontece devido a seguinte aproximação

$$e^{-\frac{|\alpha|^2}{2}} \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2} \approx (2\pi |\alpha|^2)^{1/2} \exp \left[-\frac{(n - |\alpha|^2)^2}{2 |\alpha|^2} \right] \quad (4.1.18)$$

que na equação (4.1.16) fica

$$P(\phi) \approx \left(\frac{2|\alpha|^2}{\pi} \right)^{1/2} \exp [-2|\alpha|^2 (\phi - \theta)^2] \quad (4.1.19)$$

onde a Gaussiana atinge um pico em $\phi = \theta$ além de se tornar mais estreito com o aumento de $\bar{n} = |\alpha|^2$, assim como mostra na figura a seguir

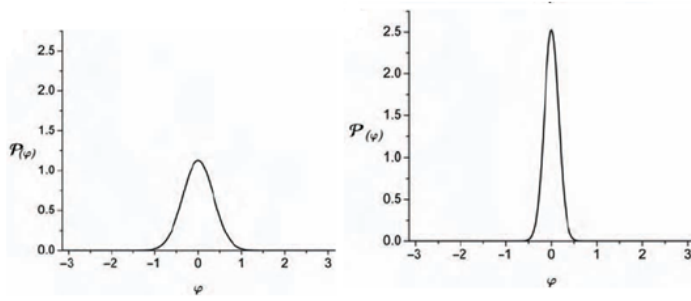


Figura 4.1: Figura retirada de [9] mostrando a distribuição de fase para o estado coerente com $\theta = 0$ sendo $\bar{n} = 2$ para o gráfico da esquerda e $\bar{n} = 10$ para o gráfico da direita

4.2 Estado Coerente como entrada no Interferômetro de Mach-Zehnder

No capítulo anterior foi visto o estado de número como entrada no IMZ junto com o vácuo quântico, agora será trocado o estado de número pelo estado coerente mantendo o vácuo quântico. Antes disso é preciso saber o que acontece quando esses estados passam por um BS.

Na teoria demonstrada em [9] é apresentado um outro operador chamado de operador deslocamento, esse operador é responsável por deslocar o vácuo, um mecanismo para a geração de estados coerentes, esse operador é definido como

$$\hat{D}(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a}) \quad (4.2.20)$$

e o estado coerente dado por

$$|\alpha\rangle = \hat{D}(\alpha) |0\rangle \quad (4.2.21)$$

Desta forma, é possível escrever os estados de entrada, que agora são o estado coerente e o estado de vácuo, como $|0\rangle_0 |\alpha\rangle_1 = \hat{D}_1(\alpha) |0\rangle_0 |0\rangle_1$ e com isso é possível fazer a primeira operação no IMZ que é passar pelo primeiro BS.

$$|0\rangle_0 |\alpha\rangle_1 \xrightarrow{BS1} \exp(\alpha \hat{a}_1^\dagger - \alpha^* \hat{a}_1) |0\rangle_2 |0\rangle_3 \quad (4.2.22)$$

Porém, como já foi visto no capítulo anterior, temos que escrever esses operadores \hat{a}_1^\dagger e \hat{a}_1 em termos de \hat{a}_2 , \hat{a}_2^\dagger , \hat{a}_3 e \hat{a}_3^\dagger . Para isso usamos as equações de (3.1.9) que por substituição encontramos

$$\begin{aligned}\hat{a}_1^\dagger &= \frac{1}{\sqrt{2}} \left(i\hat{a}_2^\dagger + \hat{a}_3^\dagger \right) \\ \hat{a}_1 &= \frac{1}{\sqrt{2}} \left(-i\hat{a}_2 + \hat{a}_3 \right)\end{aligned}\tag{4.2.23}$$

e com isso reescrevemos (4.2.21) como

$$\begin{aligned}|0\rangle_0 |\alpha\rangle_1 &\xrightarrow{BS1} \exp \left[\frac{\alpha}{\sqrt{2}} \left(i\hat{a}_2^\dagger + \hat{a}_3^\dagger \right) - \frac{\alpha^*}{\sqrt{2}} \left(-i\hat{a}_2 + \hat{a}_3 \right) \right] |0\rangle_2 |0\rangle_3 \\ &= \exp \left[\left(\frac{i\alpha}{\sqrt{2}} \hat{a}_2^\dagger - \frac{i\alpha^*}{\sqrt{2}} \hat{a}_2 \right) \right] \exp \left[\left(\frac{\alpha}{\sqrt{2}} \hat{a}_3^\dagger - \frac{\alpha^*}{\sqrt{2}} \hat{a}_3 \right) \right] |0\rangle_2 |0\rangle_3 \\ &= \left| \frac{i\alpha}{\sqrt{2}} \right\rangle_2 \left| \frac{\alpha}{\sqrt{2}} \right\rangle_3\end{aligned}\tag{4.2.24}$$

Esse ultimo termo é escrito devido a ter os operadores \hat{D}_2 e \hat{D}_3 na equação, voltando a escrever o estado coerente semelhante a o da equação (4.2.20). O próximo passo é a mudança de fase que está presente em um dos caminhos, porém não se tratando de um único BS e sim de um IMZ no caso quântico, não é possível saber em qual dos braços está cada estado da equação (4.2.23), logo será escrito como

$$|0\rangle |\alpha\rangle \xrightarrow{BS1} \left| \frac{i\alpha}{\sqrt{2}} \right\rangle \left| \frac{\alpha}{\sqrt{2}} \right\rangle\tag{4.2.25}$$

e ignorando as mudanças de fase comum de cada espelho, considerando apenas a mudança de fase causada pelo defasador, a transformação fica

$$\left| \frac{i\alpha}{\sqrt{2}} \right\rangle \left| \frac{\alpha}{\sqrt{2}} \right\rangle \xrightarrow{\theta} \left| \frac{ie^{i\theta}\alpha}{\sqrt{2}} \right\rangle \left| \frac{\alpha}{\sqrt{2}} \right\rangle\tag{4.2.26}$$

no segundo BS acontece a superposição dos dois estados de chegada fazendo uma

soma entre eles para gerar o estado de saída, isso resulta em

$$\left| \frac{ie^{i\theta}\alpha}{\sqrt{2}} \right\rangle \left| \frac{\alpha}{\sqrt{2}} \right\rangle \xrightarrow{BS2} \left| \frac{-e^{i\theta}\alpha}{\sqrt{2}} + \frac{\alpha}{\sqrt{2}} \right\rangle \left| \frac{ie^{i\theta}\alpha}{\sqrt{2}} + \frac{i\alpha}{\sqrt{2}} \right\rangle = \left| \frac{i(e^{i\theta} + 1)\alpha}{\sqrt{2}} \right\rangle \left| \frac{(1 - e^{i\theta})\alpha}{\sqrt{2}} \right\rangle \quad (4.2.27)$$

isso pode ser ilustrado da seguinte maneira

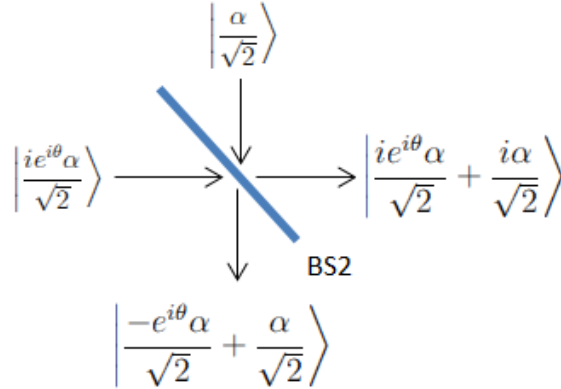


Figura 4.2: Ilustração dos estados de saída do BS2, estados que são medidos nos detectores.

Com isso é possível calcular a diferença de fase medida nos detectores segundo a equação (3.2.37) onde, neste caso, o operador número $\hat{O} = \hat{a}^\dagger \hat{a} - \hat{b}^\dagger \hat{b}$ tem o $\hat{a}^\dagger \hat{a}$ representando o primeiro estado de saída e o $\hat{b}^\dagger \hat{b}$ o segundo estado de saída, com isso calcula-se

$$\begin{aligned} \langle \hat{O} \rangle &= \left\langle \frac{-i(e^{-i\theta} + 1)\alpha}{\sqrt{2}} \left| \hat{a}^\dagger \hat{a} \right| \frac{i(e^{i\theta} + 1)\alpha}{\sqrt{2}} \right\rangle - \left\langle \frac{(1 - e^{-i\theta})\alpha}{\sqrt{2}} \left| \hat{b}^\dagger \hat{b} \right| \frac{(1 - e^{i\theta})\alpha}{\sqrt{2}} \right\rangle \\ &= |\alpha|^2 \cos\theta \end{aligned} \quad (4.2.28)$$

É importante destacar que o estado coerente, por mais que tenha características clássicas, ela é um estado fundamentado pela mecânica quântica e carrega consigo a flutuação do vácuo que impõe limites sobre a precisão na medição da fase [9]. Assim

é possível medir a incerteza da fase com a equação (3.2.37) onde

$$\Delta\theta = \frac{1}{\sqrt{\bar{n}} |\text{sen}\theta|} \quad (4.2.29)$$

onde $\bar{n} = |\alpha|^2$. Isso mostra que a incerteza da fase depende da fase relativa θ e que a mínima incerteza é encontrada para $\theta = \pi/2$ onde $\Delta\theta_{min} = 1/\sqrt{\bar{n}}$. Essa é o melhor valor que se pode chegar para estados semi-clássicos. No entanto é possível ultrapassar este limite, chamado de limite quântico padrão, a partir de estados com comportamentos não clássicos para fazer interferometria. De fato, o limite fundamental na incerteza da fase, conhecido como o limite de Heisenberg, pode ser $\Delta\theta_H = 1/\bar{n}$ que é o limite para a precisão de medidas em escalas quânticas. Esse limite não é facilmente alcançado e tem sido um dos grandes objetivos da óptica quântica, pois a detecção é de sinais tão fracos que podem ser confundidos facilmente com ruídos. Esse é o assunto do trabalho de [14] e que é motivação para este trabalho, o melhoramento da precisão na detecção da fase.

4.3 Detecção da fase no limite quântico

Nesta seção será discutido uma forma de melhorar a sensibilidade na fase segundo [14], o modelo usado aqui servirá de base para usar em outros estados quânticos.

Usando o estado coerente com um estado não clássico, de uma forma que pode ser aplicado em um experimento, a incerteza da fase pode ser escrita como

$$\Delta\theta = \frac{1}{\sqrt{p\bar{n}} \text{sen}\theta} \quad (4.3.30)$$

onde p é o número de medidas independentes. Já foi visto, a condição ideal da equação (4.3.29) é quando $\theta = \pi/2$ onde a diferença do número médio de fótons varia mais rapidamente com a fase, porém na maioria das vezes θ varia entre 0 e π e isso faz com que a confiança na fase seja muito baixo a ponto de ser desconsiderado.

A análise sobre essas medidas foram primeiramente noticiado por [15] onde o estimador de fase não leva em conta todas as informações disponíveis principalmente as flutuações do número total de fótons nas portas de saída. Uma possível saída para este problema foi confirmado pela análise de Cramer-Rao lower bound (CRLB), que, para um dado estado de entrada e escolha de um observável, a incerteza da estimação da fase será de

$$\Delta\theta_{CRLB} = \frac{1}{\sqrt{pF(\theta)}} \quad (4.3.31)$$

sendo $F(\theta)$ a informação de Fisher que para este caso será uma função dependente de θ . A informação de Fisher é uma teoria de medida que incorpora o observador do fenômeno sob medida. Por esta teoria, o observador torna-se um coletor de dados e um ativador do fenômeno que dá origem aos dados, aplica-se a todos os cenários onde os dados quantitativos dos experimentos repetíveis podem ser coletados.. A ideia mostrada por J. A. Wheeler (1990; 1994) diz que "Todas as grandezas físicas são informações da teoria de origem e este é um universo participativo, ou seja, o observador participante dá origem à informação, e informação dá origem à física." [16].

Para o problema da medida de fase no interferômetro, o parâmetro θ a ser medido, terá a influencia do observador na fase gerado no IMZ. Isso faz com que a probabilidade de medir os fótons nos braços de saída do interferômetro com diferença de fase θ seja dada pela informação de fisher a seguir

$$F(\theta) = \sum_{N_C, N_D} \left[\frac{1}{P(N_C, N_D|\theta)} \right] \left[\frac{\partial P(N_C, N_D|\theta)}{\partial \theta} \right]^2 \quad (4.3.32)$$

Para medir $F(\theta)$ será necessário calcular a probabilidade de detectar, N_C e N_D , número de partículas que saem das portas de saída C e D dado uma fase θ no interferômetro, sendo os estados de entrada o estado coerente e o estado de vácuo, ou seja

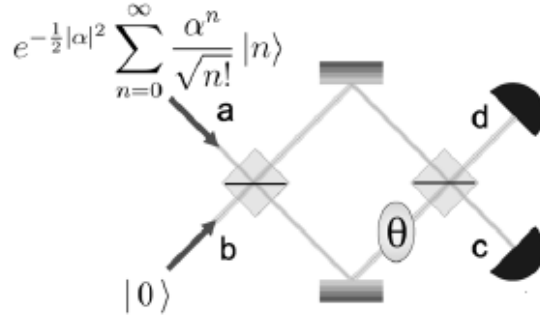


Figura 4.3: Figura retirada de [14] com a ilustração do IMZ usando o estado coerente como entrada na porta a e o estado de vácuo como entrada na porta b

$$P(N_C, N_D|\theta) = |\langle N_C | \langle N_D | e^{-i\theta J_y} |\alpha\rangle |0\rangle|^2 \quad (4.3.33)$$

Nesta equação é presente o termo do momento angular responsável pela polarização, neste caso o momento angular sofre uma rotação e com isso é preciso transformar os termos para usar a representação de Schwinger que resultará no termo da matriz de rotação dado pela equação (3.1.29). Os termos serão reescritos da seguinte maneira [10]

$$\langle N_C N_D | = {}_z \langle j \mu | \quad (4.3.34)$$

$$|n0\rangle = |j \nu\rangle_z \quad (4.3.35)$$

Além das seguintes transformações

$$P(N_C, N_D|\theta) = P(\mu|\theta, j, \nu) \quad (4.3.36)$$

$$j = \frac{N_C + N_D}{2} = \frac{n}{2} \quad (4.3.37)$$

$$\mu = \frac{n}{2} = j \quad (4.3.38)$$

$$\nu = \frac{N_C - N_D}{2} \quad (4.3.39)$$

e assim é possível chegar a uma probabilidade em termos da matriz rotação

$$\begin{aligned}
P(\mu|\theta, j, \nu) &= \left| e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^{2n}}{\sqrt{n!}} \langle j\mu | e^{-i\phi J_y} | j\nu \rangle_z \right|^2 \\
&= \left| e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^{2n}}{\sqrt{n!}} \sqrt{\frac{(j+\mu)!(j-\mu)!}{(j+\nu)!(j-\mu)!}} \left(\cos\frac{\theta}{2}\right)^{\mu+\nu} \left(\sen\frac{\theta}{2}\right)^{\mu-\nu} \right|^2
\end{aligned} \tag{4.3.40}$$

usando a equação (4.3.38) os termos que se somam na equação se tornam

$$\mu + \nu = j + \nu = \frac{N_C + N_D}{2} + \frac{N_C - N_D}{2} = N_C \tag{4.3.41}$$

$$\mu - \nu = j - \nu = \frac{N_C + N_D}{2} - \frac{N_C - N_D}{2} = N_D \tag{4.3.42}$$

substituindo (4.3.41),(4.3.42) e (4.3.37) em (4.3.40) a equação se torna

$$P(\mu|\theta, j, \nu) = P(N_C, N_D|\theta) = e^{-|\alpha|^2} \frac{\alpha^{2(N_C+N_D)}}{N_C!N_D!} \left(\cos\frac{\theta}{2}\right)^{2N_D} \left(\sen\frac{\theta}{2}\right)^{2N_C} \tag{4.3.43}$$

Neste ultimo passo o somatório não aparece devido ao número total de fóton ser $n = N_C + N_D$ além de já fazer a operação do módulo. Esse é o termo necessário para calcular a informação de Fisher, porém é necessário fazer uma modificação, usar o número relativo de partícula $N_r = N_C + N_D$ cujo probabilidade é calculado como

$$P(N_r|\theta) = \sum_{N_C, N_D} P(N_C, N_D|\theta) \delta_{N_C - N_D, N_r} \tag{4.3.44}$$

onde substituindo (4.3.43) em (4.3.44) já considerando $\delta_{N_C - N_D, N_r} = 1$ e que $N_C = N_r + N_D$

$$\begin{aligned}
P(N_r|\theta) &= \sum_{N_D=0}^{\infty} \frac{\alpha^{2(N_r+2N_D)}}{(N_r + N_D)!N_D!} \left(\cos^2\frac{\theta}{2}\right)^{N_D} \left(\sen^2\frac{\theta}{2}\right)^{(N_r+N_D)} \\
&= |\alpha|^{2N_r} e^{-|\alpha|^2} \left(\sen^2\frac{\theta}{2}\right)^{N_r} \sum_{N_D=0}^{\infty} \frac{|\alpha|^{4N_D}}{(N_r + N_D)!N_D!} \left(\cos^2\frac{\theta}{2}\right)^{N_D} \left(\sen^2\frac{\theta}{2}\right)^{N_D}
\end{aligned} \tag{4.3.45}$$

sendo que $\sen\theta = 2\sen\theta/2\cos\theta/2$ que modifica o termo dentro do somatório, dessa forma esse termo separadamente pode ser escrito como

$$\begin{aligned}
& \frac{|\alpha|^{4N_D}}{(N_r + N_D)!N_D!} \left(\frac{\text{sen}\theta}{2} \right)^{2N_D} = \\
& = \frac{1}{(N_r + N_D)!N_D!} \left(\frac{|\alpha|^2 \text{sen}\theta}{2} \right)^{2N_D} \tag{4.3.46}
\end{aligned}$$

voltado ao calculo anterior, a equação fica

$$P(N_r|\theta) = |\alpha|^{2N_r} e^{-|\alpha|^2} \left(\text{sen}^2 \frac{\theta}{2} \right)^{N_r} \sum_{N_D=0}^{\infty} \frac{1}{(N_r + N_D)!N_D!} \left(\frac{|\alpha|^2 \text{sen}\theta}{2} \right)^{2N_D} \tag{4.3.47}$$

Agora será usado uma ferramenta da física-matemática que é a função de Bessel (Simbolizado por I_n). Essa função tem a seguinte forma

$$\sum_{k=0}^{\infty} \frac{1}{(n+k)!k!} x^k = x^{-n/2} I_n(2\sqrt{x}) \tag{4.3.48}$$

isso faz com que a equação (4.3.47), onde substitui $n = N_r$ e $x = \left(\frac{|\alpha|^2 \text{sen}\theta}{2} \right)^2$ para ficar

$$\begin{aligned}
P(N_r|\theta) &= |\alpha|^{2N_r} e^{-|\alpha|^2} \left[\left(\text{sen}^2 \frac{\theta}{2} \right)^2 \right]^{N_r} \left(\frac{|\alpha|^2 \text{sen}\theta}{2} \right)^{-N_r} I_{N_r} \left(2\sqrt{\left(\frac{|\alpha|^2 \text{sen}\theta}{2} \right)^2} \right) \\
&= \frac{e^{-|\alpha|^2} \left(\text{sen}^2 \frac{\theta}{2} \right)^{N_r}}{\left(\frac{\text{sen}\theta}{2} \right)^{N_r}} I_{N_r} (|\alpha|^2 \text{sen}\theta) \\
&= \frac{e^{-|\alpha|^2} \left(\text{sen}^2 \frac{\theta}{2} \right)^{N_r}}{\left(\text{sen} \frac{\theta}{2} \cos \frac{\theta}{2} \right)^{N_r}} I_{N_r} (|\alpha|^2 \text{sen}\theta) \\
&= e^{-|\alpha|^2} \left(\text{tg} \frac{\theta}{2} \right)^{N_r} I_{N_r} (|\alpha|^2 \text{sen}\theta) \tag{4.3.49}
\end{aligned}$$

Assim chega a probabilidade em função da função de Bessel, porém é preciso ver se essa probabilidade é normalizada, ou seja

$$\sum_{N_r=-\infty}^{\infty} P(N_r|\theta) = 1 \tag{4.3.50}$$

fazendo as operações matemáticas chega-se ao seguinte resultado

$$\begin{aligned} \sum_{N_r=-\infty}^{\infty} P(N_r|\theta) &= \sum_{N_r=-\infty}^{\infty} e^{-|\alpha|^2} \left(tg \frac{\theta}{2} \right)^{N_r} I_{N_r} (|\alpha|^2 \text{sen}\theta) = \\ &= e^{-|\alpha|^2} \sum_{N_r=-\infty}^{\infty} \left(tg \frac{\theta}{2} \right)^{N_r} I_{N_r} (|\alpha|^2 \text{sen}\theta) \end{aligned} \quad (4.3.51)$$

Fazendo a transformação

$$\sum_{k=-\infty}^{\infty} I_k(x)t^k = \exp \left[\frac{1}{2}x \left(t + \frac{1}{t} \right) \right] \quad (4.3.52)$$

onde, separadamente, a parte dentro do somatório fica

$$\begin{aligned} e^{-|\alpha|^2} \sum_{N_r=-\infty}^{\infty} \left(tg \frac{\theta}{2} \right)^{N_r} I_{N_r} (|\alpha|^2 \text{sen}\theta) &= \exp \left[\frac{|\alpha|^2 \text{sen}\theta}{2} \left(tg \frac{\theta}{2} + \frac{1}{tg \frac{\theta}{2}} \right) \right] = \\ &= \exp \left[\frac{|\alpha|^2 \text{sen}\theta}{2} \left(\frac{\text{sen} \frac{\theta}{2}}{\cos \frac{\theta}{2}} + \frac{\cos \frac{\theta}{2}}{\text{sen} \frac{\theta}{2}} \right) \right] = \\ &= \exp \left[\frac{|\alpha|^2 \text{sen}\theta}{2} \left(\frac{\text{sen}^2 \frac{\theta}{2} + \cos^2 \frac{\theta}{2}}{\text{sen} \frac{\theta}{2} \cos \frac{\theta}{2}} \right) \right] = \\ &= \exp \left[\frac{|\alpha|^2 \text{sen}\theta}{2 \text{sen} \frac{\theta}{2} \cos \frac{\theta}{2}} \right] = e^{|\alpha|^2} \end{aligned} \quad (4.3.53)$$

Voltando a equação (4.3.51) é visto que

$$\sum_{N_r=-\infty}^{\infty} P(N_r|\theta) = e^{-|\alpha|^2} e^{|\alpha|^2} = 1 \quad (4.3.54)$$

Logo é uma função normalizada. Agora é preciso saber o desvio padrão que dará a precisão nas medidas, para este caso é necessário mostrar se a probabilidade achada resulta em um desvio $(\Delta N_r)^2 = |\alpha|^2$ sabendo que $(\Delta N_r)^2 = \langle N_r^2 \rangle - \langle N_r \rangle^2$, ou seja, é preciso calcular cada termo separadamente. Calculando o $\langle N_r \rangle$:

$$\sum_{N_r=-\infty}^{\infty} N_r P(N_r|\theta) = N_r e^{-|\alpha|^2} \sum_{N_r=-\infty}^{\infty} \left(tg \frac{\theta}{2} \right)^{N_r} I_{N_r} (|\alpha|^2 \text{sen}\theta) \quad (4.3.55)$$

Modificando a equação (4.3.52) para usar na equação a cima, separadamente possível reescreve-la como

$$\begin{aligned} t \frac{\partial}{\partial t} \sum_{k=-\infty}^{\infty} I_k(x) t^k &= \sum_{k=-\infty}^{\infty} I_k(x) k t^k = \\ &= \frac{tx}{2} \exp \left[\frac{x}{2} \left(t + \frac{1}{t} \right) \right] \left(1 - \frac{1}{t^2} \right) \end{aligned} \quad (4.3.56)$$

que, ao retornar a equação fica

$$\sum_{N_r=-\infty}^{\infty} N_r P(N_r|\theta) = N_r e^{-|\alpha|^2 \frac{tg \frac{\theta}{2}}{2} |\alpha|^2 \frac{sen \theta}{2}} \exp \left[\frac{|\alpha|^2 \frac{sen \theta}{2} \left(\frac{tg^2 \frac{\theta}{2} + 1}{tg \frac{\theta}{2}} \right) \right] \left(1 - \frac{1}{tg^2 \frac{\theta}{2}} \right) \quad (4.3.57)$$

onde, fazendo as substituições trigonométricas e simplificando toda a equação, o resultado é

$$\langle N_r \rangle = \sum_{N_r=-\infty}^{\infty} N_r P(N_r|\theta) = |\alpha|^2 \cos \theta \quad (4.3.58)$$

Agora será necessário calcular $\langle N_r^2 \rangle$ que será de maneira semelhante resultando em

$$\langle N_r^2 \rangle = \sum_{N_r=-\infty}^{\infty} N_r^2 P(N_r|\theta) = |\alpha|^4 \cos^2 \theta + |\alpha|^2 \quad (4.3.59)$$

Calculando agora o desvio padrão

$$(\Delta N_r)^2 = \langle N_r^2 \rangle - \langle N_r \rangle^2 = |\alpha|^4 \cos^2 \theta + |\alpha|^2 - |\alpha|^2 \cos^2 \theta = |\alpha|^2 \quad (4.3.60)$$

Como essas informações é possível de certeza calcular a informação de Fisher, retornando a equação (4.3.31), porém ainda tem uma ultima operação antes de chegar ao resultado final deste problema, nesta equação será calculado a parte diferencial separadamente da seguinte maneira

$$\begin{aligned}
\frac{dP(N_r|\theta)}{d\theta} &= e^{-|\alpha|^2} \frac{N_r}{\text{sen}\theta} \left(tg\frac{\theta}{2} \right)^{N_r} I_{N_r} (|\alpha|^2 \text{sen}\theta) \\
&\quad + e^{-|\alpha|^2} \left(tg\frac{\theta}{2} \right)^{N_r} |\alpha|^2 \cos\theta \left(\frac{N_r}{2} I_{N_r} (|\alpha|^2 \text{sen}\theta) + I_{N_r+1} (|\alpha|^2 \text{sen}\theta) \right) = \\
&= P(N_r|\theta) \left[\frac{N_r}{\text{sen}\theta} + |\alpha|^2 \cos\theta \left(\frac{N_r}{2} + \frac{I_{N_r+1} (|\alpha|^2 \text{sen}\theta)}{I_{N_r} (|\alpha|^2 \text{sen}\theta)} \right) \right] \quad (4.3.61)
\end{aligned}$$

E, substituindo de volta na informação de Fisher, o resultado será

$$F(\theta) = \sum_{N_r=-\infty}^{\infty} P(N_r|\theta) \left[N_r \left(\frac{1}{\text{sen}\theta} + \frac{|\alpha|^2 \cos\theta}{2} \right) + |\alpha|^2 \cos\theta \frac{I_{N_r+1} (|\alpha|^2 \text{sen}\theta)}{I_{N_r} (|\alpha|^2 \text{sen}\theta)} \right]^2 \quad (4.3.62)$$

A partir de agora esse calculo deve ser feito em um software matemático onde é possível encontrar o seguinte resultado

$$F(\theta) = |\alpha|^2 \text{sen}^2\theta \quad (4.3.63)$$

Que se confirma para $\theta = \pi/2$ onde a equação (4.3.30) fica

$$\Delta\theta = \frac{1}{\sqrt{p\bar{n}}} \quad (4.3.64)$$

O que faz o resultado ser próximo ao limite de Heisenberg. Este resultado foi obtido em [14]. Aqui agradecemos a colaboração de L. Pezzé que explicitou os detalhes aqui apresentado.

Capítulo 5

Estado Binomial no Interferômetro de Mach-Zehnder

Neste capítulo será analisado o estado binomial junto ao estado de vácuo, ambos como estados de entrada, no IMZ. Essa é a principal proposta deste trabalho onde será analisado teoricamente, assim como foi no capítulo anterior para o estado coerente, o estado de saída e a sensibilidade da fase para o estado binomial, porém, antes deste resultado é importante explicar esse estado e suas propriedades.

5.1 O Estado Binomial

Até agora este trabalho tratou apenas de dois estados, o estado de número $|n\rangle$ e o estado coerente $|\alpha\rangle$ usando todos como entrada no IMZ. Eles são facilmente entendido como por exemplo, um único fóton pode ser criado no seu primeiro estado de excitação, ou seja, a emissão de um único fóton gera o estado para um fóton, já para o estado coerente acontece devido a interação de cargas clássicas. O estado binomial $|\eta, M\rangle$, por sua vez, é um estado que interpola entre esses dois podendo usar propriedades de ambos os estados quando alterado o seu limite, pode-se dizer que o estado binomial é uma combinação linear de n estados $|0\rangle, |1\rangle, \dots, |M\rangle$ com os coeficientes escolhidos de tal modo que a distribuição de probabilidade dos fótons de contagens seja binomial com média de ηM . Esse estado pode ser gerado quando cada um dos M fótons são

emitidos com probabilidade η , ou seja, uma condição em que a molécula pode ser excitada a um subnível M . Um caso especial é o estado de Bernoulli generalizados e misturados que acontece para $M = 1$. [17]

O estado binomial é definido como:

$$|\eta, M\rangle = \sum_{n=0}^M \beta_n^M |n\rangle \quad (5.1.1)$$

onde

$$\beta_n^M = \left[\binom{M}{n} \eta^n (1 - \eta)^{M-n} \right]^{1/2} \quad (5.1.2)$$

O estado $|\eta, M\rangle$ define o estado de um simples modo do campo eletromagnético cujo a densidade de probabilidade para o número de fótons seja binomial. Os termos $\eta, (1 - \eta)$ são as probabilidades de dois possíveis resultados do teste de Bernoulli, ou seja, η de sucesso e $(1 - \eta)$ de falha [18]. A probabilidade para que n fótons sejam produzidos com $M > n$ maneiras de produzi-las é dado por $|\beta_n^M|^2$. Nesta definição, o estado binomial é normalizado desde que

$$\langle \eta, M | \eta, M \rangle = \sum_{n=0}^M \binom{M}{n} \eta^n (1 - \eta)^{M-n} = 1 \quad (5.1.3)$$

e o número médio de fótons dado por

$$\langle \eta, M | \hat{n} | \eta, M \rangle = \langle \hat{n} \rangle_{\eta, M} = \sum_{n=0}^M n |\beta_n^M|^2 = \eta M \quad (5.1.4)$$

É possível calcular o desvio padrão, mas antes é preciso calcular $\langle \hat{n}^2 \rangle$ que resulta em

$$\langle \hat{n}^2 \rangle_{\eta, M} = (\eta M)^2 + \eta (1 - \eta) M \quad (5.1.5)$$

e dessa forma tem-se

$$(\Delta n)^2 \equiv \langle \Delta n \rangle_{\eta, M}^2 = \langle \hat{n}^2 \rangle_{\eta, M} - \langle \hat{n} \rangle_{\eta, M}^2 = \eta (1 - \eta) M \quad (5.1.6)$$

A grande importância do estado binomial é quando se manipula os valores de η e M . Para $\eta = 0$, com M finito, o estado binomial se reduz a estado de vácuo, para $\eta = 1$ e M finito reduz para o estado de número $|n = M\rangle$. No limite em que $\eta \rightarrow 0$ e $M \rightarrow \infty$, onde $\eta M = \text{constante} = \alpha$, o estado binomial se aproxima do estado coerente. Ainda falta analisar a aplicação dos operadores de criação e aniquilação, que no estado binomial está presente como

$$\hat{a} |\eta, M\rangle = \sum_{n=0}^M \beta_n^M n^{1/2} |n-1\rangle \quad (5.1.7)$$

sendo que $\beta_n^M n^{1/2} = (\eta M)^{1/2} \beta_{n-1}^{M-1}$ que torna a equação anterior em

$$\hat{a} |\eta, M\rangle = (\eta M)^{1/2} \sum_{n=0}^M \beta_{n-1}^{M-1} |n-1\rangle \quad (5.1.8)$$

Nesta equação, o somatório inicia para $n = 1$, é visível que o termo $n = 0$ não aparece, com isso, é possível chamar $l = n - 1$, ou seja

$$\hat{a} |\eta, M\rangle = (\eta M)^{1/2} \sum_{l=0}^{M-1} \beta_l^{M-1} |l\rangle = (\eta M)^{1/2} |\eta, M-1\rangle \quad (5.1.9)$$

que é o operador aniquilação atuando no estado binomial, para o operador criação fica

$$\hat{a}^\dagger |\eta, M\rangle = \sum_{n=0}^M \beta_n^M (n+1)^{1/2} |n+1\rangle \quad (5.1.10)$$

sendo que $\beta_n^M (n+1)^{1/2} = (n+1) [\eta(M+1)]^{-1/2} \beta_{n+1}^{M+1}$ e fazendo as substituições necessárias encontra-se o resultado

$$\hat{a}^\dagger |\eta, M\rangle = \frac{1}{\sqrt{\eta(M+1)}} \hat{n} |\eta, M+1\rangle \quad (5.1.11)$$

Quando aplicado n vezes esses operadores os resultados são

$$\hat{a}^n |\eta, M\rangle = \begin{cases} \left[\frac{\eta^n M!}{(M-n)!} \right]^{1/2} |\eta, M-n\rangle, & n \leq M \\ 0, & n > M \end{cases} \quad (5.1.12)$$

$$\hat{a}^{\dagger n} |\eta, M\rangle = \left[\frac{M!}{\eta^n (M+n)!} \right]^{1/2} \hat{n} (\hat{n} - 1) \dots (\hat{n} - n + 1) |\eta, M + 1\rangle \quad (5.1.13)$$

Essas são algumas das propriedades para o estado binomial que será usado neste trabalho, o próximo passo é analisar este estado no IMZ que será discutido na próxima seção.

5.2 Estado Binomial como Entrada no Interferômetro de Mach-Zehnder

Sabendo de todas as propriedades do estado binomial, agora será feito, de maneira semelhante ao capítulo anterior, o estado binomial junto ao estado de vácuo como entrada no IMZ e saber qual o estado de saída. O método não será igual ao usado com o estado coerente, pois não terá o operador deslocamento, porém terá a mesma lógica usado para o estado de número. O primeiro passo é a passagem pelo primeiro BS, para isso é preciso saber como acontece a rotação quando aplicado o operador de criação, para um caso mais simples

$$U \hat{a}_1^\dagger U^\dagger = \frac{i\hat{a}_2^\dagger + \hat{a}_3^\dagger}{\sqrt{2}} \quad (5.2.14)$$

e para o caso do estado binomial

$$U \frac{(\hat{a}_1^\dagger)^n}{\sqrt{n!}} U^\dagger = \frac{(i\hat{a}_2^\dagger + \hat{a}_3^\dagger)^n}{(\sqrt{2})^n \sqrt{n!}} \quad (5.2.15)$$

logo, para o primeiro BS o estado tem a seguinte mudança

$$|0\rangle_0 |\eta, M\rangle_1 = \sum_{n=0}^M \beta_n^M (\hat{a}_1^\dagger)^n \sqrt{n!} |0\rangle_0 |0\rangle_1 \xrightarrow{BS1} \sum_{n=0}^M \beta_n^M \frac{(i\hat{a}_2^\dagger + \hat{a}_3^\dagger)^n}{(\sqrt{2})^n \sqrt{n!}} |0\rangle_2 |0\rangle_3 \quad (5.2.16)$$

sendo que o termo $(i\hat{a}_2^\dagger + \hat{a}_3^\dagger)^n$ pode ser escrito como um binômio de Newton, e com isso o auto estado $|0\rangle_2 |0\rangle_3$ será transformados sabendo que $(\hat{a}^\dagger)^l |0\rangle = \sqrt{l!} |l\rangle$, ou seja

$$\begin{aligned}
\sum_{n=0}^M \beta_n^M \frac{(i\hat{a}_2^\dagger + \hat{a}_3^\dagger)^n}{(\sqrt{2})^n \sqrt{n!}} |0\rangle_2 |0\rangle_3 &= \sum_{n=0}^M \beta_n^M \frac{1}{(\sqrt{2})^n \sqrt{n!}} \sum_{l=0}^n i^l \frac{n!}{l!(n-l)!} \left[(\hat{a}_2^\dagger)^l + (\hat{a}_3^\dagger)^{n-l} \right] |0\rangle_2 |0\rangle_3 = \\
&= \sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} \sum_{l=0}^n i^l \frac{1}{\sqrt{l!}\sqrt{(n-l)!}} |l\rangle_2 |n-l\rangle_3 \quad (5.2.17)
\end{aligned}$$

Desconsiderando as mudanças de fase comum de cada espelho, considerando apenas a mudança de fase causada pelo defasador onde o mesmo opera com uma rotação

$$U_\theta = \exp \left[-i\theta \left(\hat{a}_2^\dagger \hat{a}_2 - \hat{a}_3 \hat{a}_3^\dagger \right) \right] \quad (5.2.18)$$

que causa a seguinte transformação

$$\sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} \sum_{l=0}^n i^l \frac{1}{\sqrt{l!}\sqrt{(n-l)!}} |l\rangle_2 |n-l\rangle_3 \xrightarrow{\theta} \sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} \sum_{l=0}^n i^l \frac{e^{-i\theta(2l-n)}}{\sqrt{l!}\sqrt{(n-l)!}} |l\rangle_2 |n-l\rangle_3 \quad (5.2.19)$$

o ultimo passo do IMZ será o segundo BS, mas antes, é interessante reescrever a equação em função dos operadores de criação, pois só assim é mais fácil analisar o que acontece no segundo BS, dessa forma,

$$\begin{aligned}
&\sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} \sum_{l=0}^n i^l \frac{e^{-i\theta(2l-n)}}{\sqrt{l!}\sqrt{(n-l)!}} |l\rangle_2 |n-l\rangle_3 = \\
&= \sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} \sum_{l=0}^n i^l \frac{e^{-i\theta(2l-n)}}{\sqrt{l!}\sqrt{(n-l)!}} \frac{\left[(\hat{a}_2^\dagger)^l + (\hat{a}_3^\dagger)^{n-l} \right]}{\sqrt{l!}\sqrt{(n-l)!}} |0\rangle_2 |0\rangle_3 \quad (5.2.20)
\end{aligned}$$

que ao passar pelo segundo BS resulta em

$$\begin{aligned}
&\sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} \sum_{l=0}^n i^l \frac{e^{-i\theta(2l-n)}}{\sqrt{l!}\sqrt{(n-l)!}} \frac{\left[(\hat{a}_2^\dagger)^l + (\hat{a}_3^\dagger)^{n-l} \right]}{\sqrt{l!}\sqrt{(n-l)!}} |0\rangle_2 |0\rangle_3 \xrightarrow{BS2} \\
&\xrightarrow{BS2} \sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} \sum_{l=0}^n i^l \frac{e^{-2i\theta l}}{(\sqrt{2})^l (\sqrt{2})^{n-l}} \frac{(\hat{a}_0^\dagger - i\hat{a}_1^\dagger)^l (\hat{a}_1^\dagger - i\hat{a}_0^\dagger)^{n-l}}{l!(n-l)!} |0\rangle_0 |0\rangle_1 \quad (5.2.21)
\end{aligned}$$

Desmontando o binómio de Newton e fazendo algumas manipulações matemáticas, é possível chegar a uma equação parecida com a de entrada, ou seja

$$\sum_{n=0}^M \beta_n^M \frac{\sqrt{n!}}{(\sqrt{2})^n} e^{-i\theta n} \frac{(2\hat{a}_1^\dagger e^{-2i\theta})^n}{(\sqrt{2})^n} |0\rangle_0 |0\rangle_1 = \sum_{n=0}^M \beta_n^M e^{-i\theta n} |0\rangle_0 |n\rangle_1 \quad (5.2.22)$$

Esse estado de saída é conhecido como estado de Bernoulli que depende da fase. A propriedade desse estado depende da escolha da fase, para um número aleatório de fases, o estado é chamado de estado misto de Bernoulli e a distribuição de Bernoulli na contagem de fótons o torna um estado sub-poissoniano que é, também, ante agrupado. O estado de Bernoulli representa uma combinação normalizada para o estado do fóton $|0\rangle$ e $|1\rangle$ com os coeficientes complexos adequado [17]. Quando os coeficientes são aleatórios o resultado é o estado misto de Bernoulli.

Este resultado encontrado no IMZ mostra uma forma de se conseguir o estado de Bernoulli, existe outra forma de recriar esse estado a partir da excitação de uma molécula com um decaimento não radioativo descrevendo o campo resultante de um fóton único. Para o objetivo deste trabalho que é a informação quântica é importante ver que esses estados são interpoladores, é possível fazer manipulações para conseguir o estado coerente e o estado de número como já foi visto, mas principalmente pode ser uma forma mais eficiente para experimentação. Na próxima seção será mostrada a sensibilidade da fase para o estado Binomial para comparar com o estado coerente para mostrar a qualidade do estado para a informação quântica usando o IMZ.

5.3 Detecção da Fase para o Estado Binomial

Já foi discutida no capítulo anterior a questão da detecção da fase, isto é, a diferença de fase medida pelos detectores, porém para a informação quântica existe a dificuldade de fazer medidas em regimes quânticos que é a presença da incerteza de Heisenberg, no limite em que a quântica e a clássica ficam próximas, existe um limitante chamado de

limite de Heisenberg. Para que a informação quântica se torne realidade, as medidas tem que estar próximo deste limite e assim teremos um fenômeno quântico.

Essa ultima seção mostrara como o estado binomial pode ser usado para estimar a fase fazendo o comparativo com a fase calculada no estado coerente do capítulo anterior assim como é cololado na equação (4.3.30)colocando a informação de Fisher para fazer a aproximação do limite de Heisenberg. Para o calculo da informação de Fisher é necessário saber a probabilidade de se medir N_C e N_D fótons com uma fase θ sendo os estados de entrada o estado binomial e o estado de número, ou seja

$$P(N_C, N_D|\theta) = |\langle N_C | \langle N_D | e^{-i\theta J_y} | \eta M \rangle | 0 \rangle|^2 \quad (5.3.23)$$

é importante observar que não existe muita diferença no calculo feito para chegar as equações (4.3.39) e (4.3.42), pois ambos os estados é dado em função do estado de número $|n\rangle$, ou seja, a única diferença é a parte que fica fora das notações de Schwinger. Com isso a probabilidade de se medir N_c e N_d dado uma diferença de fase θ é dado por

$$P(N_c, N_d|\theta) = \frac{M!}{[M - (N_c + N_d)]!} \eta^{N_c+N_d} (1 - \eta)^{M-(N_c+N_d)} \frac{(\cos \frac{\theta}{2})^{2N_d} (\sen \frac{\theta}{2})^{2N_c}}{N_c! N_d!} \quad (5.3.24)$$

dessa forma, é possível calcular a informação de Fisher dado pela equação (4.3.31). A substituição junto com algumas manipulação algébricas e trigonométricas faz com que a informação de Fisher tenha o seguinte resultado

$$F(\theta) = \sum_{N_c}^M \left(\sum_{N_d}^{M-N_c} \frac{M! \eta^{N_c+N_d} (1 - \eta)^{M+(N_c+N_d)} (\cos \frac{\theta}{2})^{2N_d} (\sen \frac{\theta}{2})^{2N_c}}{[M - (N_c + N_d)]! N_c! N_d!} \left[N_c^2 \cot^2 \frac{\theta}{2} - 2N_c N_d + N_d^2 \tan^2 \frac{\theta}{2} \right] \right) \quad (5.3.25)$$

Onde os limites dos somatórios foram mudados para envolver todos os possíveis fótons em estado binomial. A solução para essa equação foi possível usando software

matemático testando valores para M , o resultado apresentado, para $M = 1, \dots, 4$ foi o seguinte:

- Para $M=1$:

$$F(\theta) = 1\eta \quad (5.3.26)$$

- Para $M=2$:

$$F(\theta) = 2\eta + 2\eta^2 \text{sen}^2\theta \quad (5.3.27)$$

- Para $M=3$:

$$F(\theta) = 3\eta + 3 \cdot 2\eta^2 \text{sen}^2\theta + 3\eta^3 (\text{sen}^2\theta + 1) \quad (5.3.28)$$

- Para $M=4$:

$$F(\theta) = 4\eta + 4 \cdot 3\eta^2 \text{sen}^2\theta + 4 \cdot 3\eta^3 (\text{sen}^2\theta + 1) + O^4(\eta) \quad (5.3.29)$$

Para esses casos já se pode verificar uma repetição nos termos de primeira e segunda ordem que são os que mais importam. Os termos de primeira ordem sempre são $M\eta$ e os de segunda ordem são $M\eta(M-1)\text{sen}^2\theta$, os termos de ordens maiores irão ter valores muito pequenos ao ponto de poder se ignorados já que η é uma taxa de probabilidade e só pode ter valores entre 0 e 1. Comparando esse resultado para o estado coerente é possível ver um gráfico de $F(\theta) \times \theta$ e ver que tanto o estado binomial quanto o estado coerente tem uma forma similar, porém com valores da informações de Fisher diferentes. Na figura (5.1) apresentamos a informação de Fisher em um gráfico $F(\theta) \times \theta$ para o estado binomial com $\eta = 0.1$ e $M = 9$.

Já para o estado coerente, da equação (4.3.62) onde $|\alpha|^2 = \bar{n}$, onde \bar{n} é o número médio de fótons, é possível montar um gráfico para $\bar{n} = 3$, que é dado na figura (5.2).

Outra observação a ser notada é que a dependência em θ em $F(\theta)$ é escalada em potência do parâmetro η .

Quando o η é maior, o gráfico vai tomando outra característica, como o da figura (5.4), o que significa que está se distanciando do estado coerente e se aproximando cada vez mais do estado de número, com isso o valor de $F(\theta)$ fica muito grande.

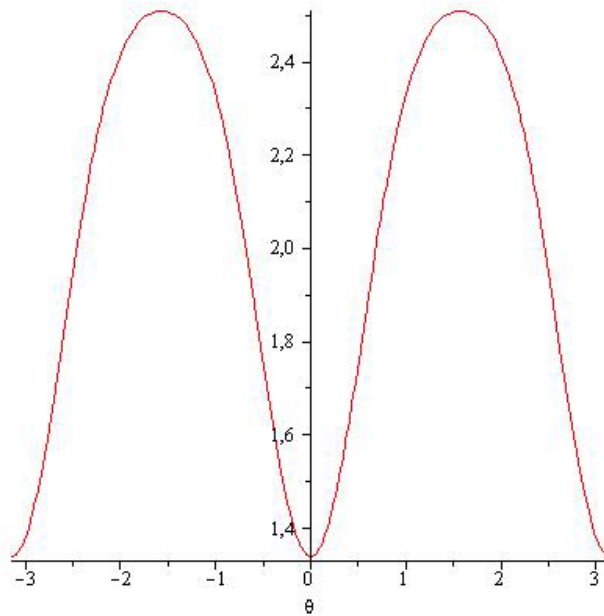


Figura 5.1: Gráfico $F(\theta) \times \theta$ para o estado binomial que mostra o comportamento da fase para um valor de $M = 9$ e $\eta = 0, 1$.

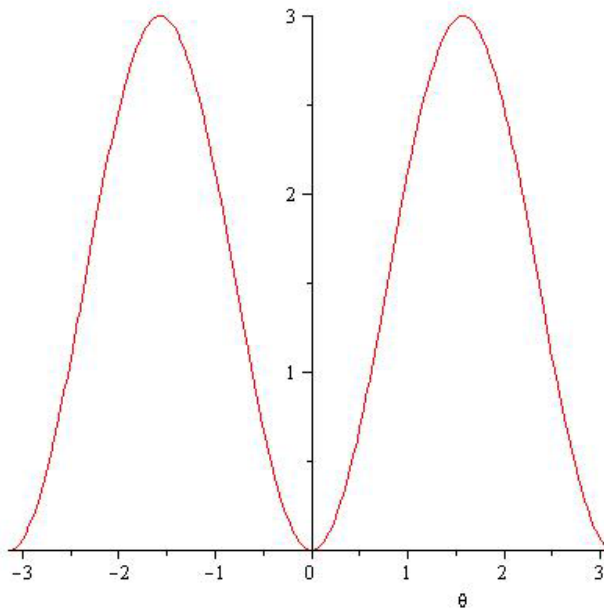


Figura 5.2: Gráfico $F(\theta) \times \theta$ para o estado coerente que mostra o comportamento da fase para um valor de $\bar{n} = 3$.

O que se pode concluir desse resultado é o fato de que o estado binomial pode ser melhor do que o estado coerente em relação a estimativa de fase, pois o termo que destaca a fase no estado binomial está presente na segunda ordem, quando η é pequeno, isso faz com que a informação de Fisher não seja tão dependente da fase assim como

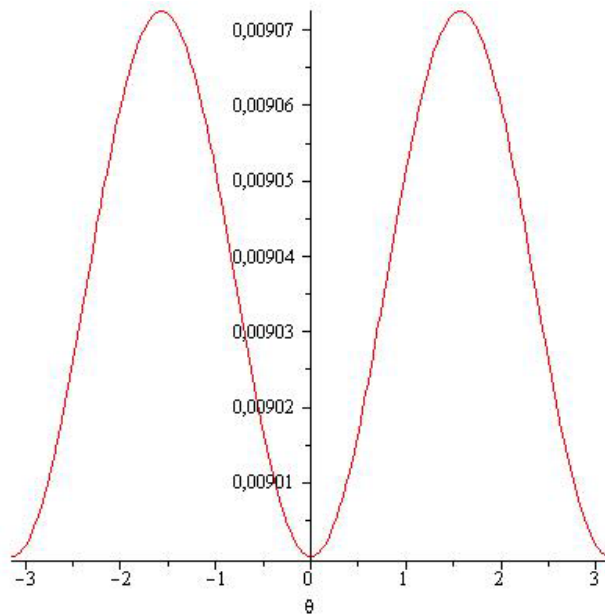


Figura 5.3: Gráfico $F(\theta) \times \theta$ para o estado binomial que mostra o comportamento da fase para um valor de $M = 9$ e $\eta = 0,001$.

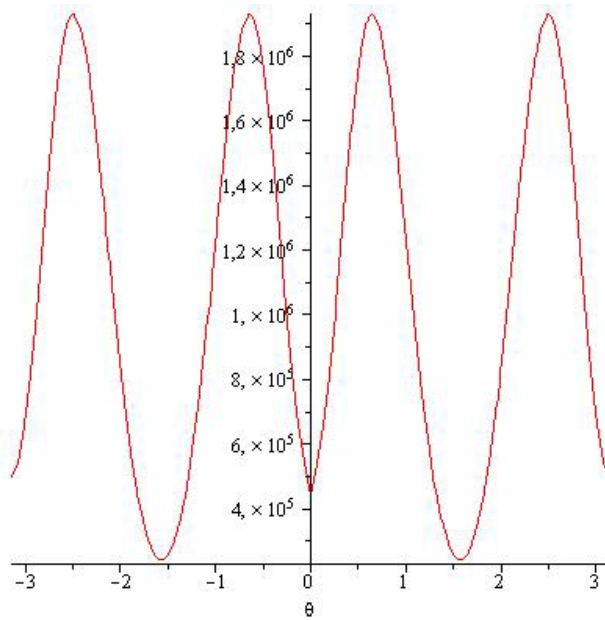


Figura 5.4: Gráfico $F(\theta) \times \theta$ para o estado binomial que mostra o comportamento da fase para um valor de $M = 10$ e $\eta = 0,8$.

é no estado coerente. Importante lembrar que um bom estimador independe da fase, isso se torna claro quando visto os valores que $F(\theta)$ assume nos gráficos mostrados. Quando o estado binomial se aproxima do estado coerente, $F(\theta)$ tem valores pequenos. Quando o mesmo se aproxima do estado de número, $F(\theta)$ tem uma forte variação com

o parâmetro θ . Indicando que o esquema não fornece um bom estimador de fase para esse estado.

Esses resultados confirmam a proposta deste trabalho devido ao comparativo entre o estado binomial e o estado coerente, pois as propriedades citadas por [17] se comprovam também para o cálculo da informação de Fisher. Dessa forma é possível conjecturar um laser que emite fótons em estado coerente, podendo ser atenuado de forma a obter uma estatística de fótons em estado binomial para injetar como entrada no IMZ e verificar o quanto pode ser melhor a estimativa da fase.

Capítulo 6

Conclusão

O objetivo central desse trabalho foi investigar o comportamento da fase do estado interpolador número-coerente quando injetado numa porta do IMZ sendo vácuo na outra. O estado de número, usualmente utilizado nos protocolos de comunicação segura é ainda um desafio tecnológico. As técnicas para a sua obtenção utilizam o estado coerente devidamente atenuado. Nessa direção, a investigação aqui apresentados utilizou o estado binomial que interpola entre o estado de número e o estado coerente.

Conjecturamos que o estado binomial, por ser um estado interpolador, pode ser utilizado nos protocolos usados para a geração de fótons individuais, através da atenuação de lasers. Esses esquemas são aqueles cuja base teórica está relacionada com o BB84 e similares.

A utilização da fase como ferramenta para a codificação informação quântica necessita de uma estimativa confiável da fase. No regime quântico é bem conhecida a dependência do estimados de fase com o valor da fase θ a ser medido é dado por $\Delta\theta = 1/\sqrt{p\bar{n}}\text{sen}\theta$, onde p é o número de medidas independentes, \bar{n} o número médio de fótons.

A dependência do valor da fase é um fator que limita a eficácia de estimativa da fase para fases arbitrária. Entretanto, foi observado que a relação $\Delta\theta$ não leva em conta a estatística das flutuações do número total de fótons nas portas de detecção do IMZ [15]. A melhoria nesse estimador pode ser realizada através de um novo estimador dado pela equação (4.3.30). Esse estimador para o estado coerente é calculado analiticamente e

é independente da θ e é dado pela equação (4.3.63).

Nós objetivamos o novo estimador quando o estado binomial é injetado numa das portas do IMZ. O valor obtido ainda é dependente da fase, porém após uma análise numérica, revela-se uma dependência com o parâmetro η , a partir da segunda ordem, que é a taxa de emissão de fótons no estado binomial.

Isso significa que estados binomiais com $\eta \rightarrow 0$, são bons candidatos para obtenção de uma fase confiável.

Bibliografia

- [1] S.Singh. *O livro dos códigos, A ciência do sigilo do antigo Egito à criptografia quântica*. Editora Record, tradução Jorge Calife, 2001.
- [2] Rigolin G, Rieznik A.A. *Introdução à Criptografia Quântica*. Revista Brasileira de Ensino de Física, v. 27, n. 4, p. 517-526, out. 2005.
- [3] Bennett C.H., Brassard G..*Quantum Cryptography: Public key Distribution and Coin Tossing*. International Conference on Computers Systems and Signal Processing.Bangalori, Índia, Dez. 1984.
- [4] F.L. Marquezino, J.A. Helayel-Neto,Estudo Introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves, Projeto de Iniciação Científica, CPBF.
- [5] Bennet C.H., Bessette F., Brassard G., Salvail L., and Smolin J., 1992, *J. Cryptol.* 5. 3-28.
- [6] Simon J. D. Phoenix, Paul D. Townsend.*Quantum Cryptography: how to beat the code breakers using quantum mechanics*. Contemporary Physics. 1995.
- [7] Ostermann F., Prado S.D. Interpretação da Mecânica Quântica em um interferômetro virtual de Mach-Zehnder. Revista Brasileira de Ensino de Física. Porto Alegre, Rio Grande do Sul, Brasil. Fev. 2005.
- [8] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. *Quantum cryptography* Rev. Mod. Phys. v.74, n. 1, p. 145-195, Mar 2002.

- [9] Gerry C., Knight P.. *Introductory Quantum Optics*. Cambridge University Press, New York, 2005.
- [10] Kim, Taesoo and Pfister, Olivier and Holland, Murray J. and Noh, Jaewoo and Hall, John L. *Influence of decorrelation on Heisenberg-limited interferometry with quantum correlated photons* Phys. Rev. A, v. 57, n. 5, p. 4004-4013, Mai 1998.
- [11] R. A. Campos, B. E. A. Saleh, and M. C. Teich *Quantum-mechanical lossless beam splitter: $SU(2)$ symmetry and photon statistics*, Phys. Rev. A **40**, 1371 (1989).
- [12] L. C. Biedenharn, J. D. Louck, P. A. Carruthers *Angular Momentum in Quantum Physics: Theory and Application*, Massachusetts Institute of Technology, v.8, 1981.
- [13] R. L. Liboff *Introductory Quantum Mechanics*. Cornell University, 1980.
- [14] L. Pezzé, A. Smerzi *Phase Detection at the Quantum Limit with Multiphoton Mach-Zehnder Interferometry* Phys. Rev. Lett. **99**, 223602 (2007)
- [15] B. Yurke *$SU(2)$ and $SU(1,1)$ interferometers*, Phys. Rev. A **33**, 4033 (1986)
- [16] B. Roy Frieden *Science from Fisher Information*. The University of Arizona, Tucson, AZ. (2004)
- [17] D. Stoler, B. E. A. Saleh, M. C. Teich *Binomial states of the quantized radiation field*, OPTICA ACTA, v. 32, no. 3, 345-355 (1985)
- [18] Hong-Chen Fu, R. Sasaki *Probability Distributions and Coherent States of B_r , C_r and D_r Algebras*, Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto 606-01 (1997)
- [19] L. Pezzé, A. Smerzi *Phase Sensitivity of a Mach-Zehnder interferometer* Phys. Rev. A **73**, 011801 (2006)