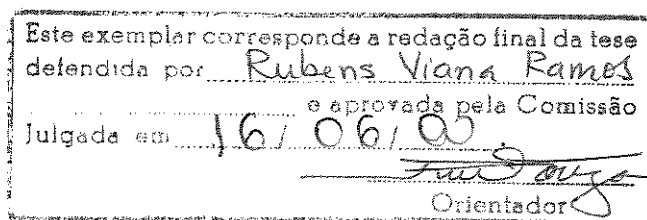


TESE DE DOUTORADO
UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO - FEEC
DEPARTAMENTO DE MICROONDA E ÓPTICA - DMO



**CONTRIBUIÇÕES ÀS COMUNICAÇÕES
QUÂNTICAS EM REDES ÓPTICAS**

UNICAMP
BIBLIOTECA CENTRAL
SEÇÃO CIRCULANTE

ALUNO: RUBENS VIANA RAMOS
ORIENTADOR: PROF. DR. RUI FRAGASSI SOUZA
BANCA: PROF. DR. ANTÔNIO SÉRGIO BEZERRA SOMBRA
PROF. DR. ANTÔNIO VIDIELLA BARRANCO
PROF. DR. EVANDRO CONFORTI
PROF. DR. ALDÁRIO CHRESTANI BORDONALLI
PROF. DR. EDSON MOSCHIM

CAMPINAS, 16 DE JUNHO DE 2000



200017112

UNIDADE	80
N.º CHAMADA:	UNICAMP
	R147c
V.	Ex.
TOMBO BC/	43007
PROC.	16-278100
C	☐
D	☒
PREC@	R\$11.00
DATA	07/11/00
N.º CPD	

CM-00147195-1

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

R147c Ramos, Rubens Viana
Contribuições às comunicações quânticas em redes
ópticas / Rubens Viana Ramos.--Campinas, SP: [s.n.],
2000.

Orientador: Rui Fragassi Souza.

Tese (doutorado) - Universidade Estadual de
Campinas, Faculdade de Engenharia Elétrica e de
Computação.

1. Comunicações óticas. 2. Ressonadores. 3. Ótica
quântica. 4. Teoria da informação. 5. Interferômetros. I.
Souza, Rui Fragassi. II. Universidade Estadual de
Campinas. Faculdade de Engenharia Elétrica e de
Computação. III. Título.

RESUMO

Esta tese trata da comunicação quântica, interferométrica e polarimétrica, em redes ópticas. Inicialmente usa-se a discretização de modos contínuos e o operador de Pegg-Barnett para a obtenção das funções densidade de probabilidade, do número de fótons e da fase, de um estado coerente, a partir da envoltória do campo. Estas são calculadas numericamente em uma simulação do tipo Monte Carlo. O método é usado na simulação do protocolo quanto-criptográfico BB84 em um interferômetro a fibra óptica. Em seguida, propomos um equalizador óptico, estrutura física e algoritmo de equalização, para corrigir a variação da polarização devido à propagação na fibra óptica. Definimos, também, o grau de pureza para estados quânticos e encontramos sua relação com os conceitos mais comuns da teoria quântica da informação, como entropia quântica, fidelidade e informação mútua. Completamos descrevendo os estados quânticos entrelaçados e as medidas de entrelaçamento. Por fim, apresentamos o ressonador não-linear a fibra, RNL, o acoplador não-linear a fibra, ANL, e o efeito de birrefringência em fibra no regime não-linear. Em particular, mostramos a possibilidade de controle e sincronização de RNLs usando controladores nebulosos, bem com a possibilidade de variação da curva de transmissividade do ANL com a variação do perfil da constante de acoplamento. Aproveitamos as características destes dispositivos em comunicações quânticas.

ABSTRACT

This thesis deals with interferometric and polarimetric quantum communication in optical networks. We span from quantum optics till set ups of optical communications systems using non-linear optical devices, including the math behind the quantum information theory. We start using continuous mode discretization and the Pegg-Barnett phase operator in a method to obtain both the photon number and the phase probability density functions, of a coherent state, from the electric field envelope. Then, we apply the method in a simulation of the quantum-cryptographic protocol BB84, in a lossy and dispersive fibre interferometer. In continuation, an optical equaliser, with its structure and equalisation algorithm, is proposed in order to correct the scrambled polarisation due to the propagation in the fibre. After this, we define the degree of purity for quantum states, in a two-dimensional Hilbert space, and we find out its relationship with the quantum entropy. Then, we attack the most common quantum information concepts as quantum distinguishability, fidelity and mutual information using the degree of purity. At last, we describe the quantum entanglement and the most common measure entanglement. Finally, we show, using numerical simulations, the behaviour of a non-linear fiber resonator, RNL, of a non-linear fibre coupler, ANL, and of the fibre birefringence effect in non-linear regime. In particular, we demonstrate the possibility of control and synchronization of RNLs with fuzzy controllers, as well as the possibility of changing the transmissivity curve of an ANL with the variation of its coupler coefficient profile. We apply those non-linear devices in quantum communications systems.

AGRADECIMENTOS

Quero expressar meus sinceros agradecimentos a todos os autores dos trabalhos citados nas referências, os quais muito me ensinaram, aos amigos do DMO pelos agradáveis momentos, em especial a Cosme, Frasson e Márcia, pela inestimável ajuda. Aos amigos Vítor, Caio, Fábio, Niudomar, Ricardo, Ricardo Fialhos, Kleber Zuza e Rodrigo Cavalcanti, pelo companheirismo, amizade, incentivo, conselhos e colaboração durante a vida acadêmica. Ao professor Sérgio Sombra, do Depto. de Física da Universidade Federal do Ceará, UFC, pelas discussões sobre a tese. Ao professor Vidiella Barranco, do Instituto de Física Gleb Wataghin da Universidade Estadual de Campinas, UNICAMP, pelas discussões de óptica quântica. Ao colega Vadim Makarov, do Department of Physical Electronics da Norwegian University of Science and Technology, NTNU, pelas discussões sobre criptografia quântica experimental. Ao professor Rui Fragassi Souza que, dotado de notória simplicidade, honestidade e competência, me confiou a produção desta tese e muito me honrou com sua amizade, estando sempre presente quando as dificuldades técnicas e pessoais apareceram. A todos os demais professores do DMO que muito contribuíram para a minha formação científica. A CAPES por financiar este trabalho. Aos membros da banca pelas colaborações à tese. A Fabiana Campos Neres, mais que amiga, mais que companheira, razão de felicidade e exemplo de caráter. A meu pai José Pedro Nogueira, minha mãe Maria Nilza Viana e meus irmãos Márcio, Nilma e Mara que, em todos os momentos, estavam presentes dando todo apoio para que meus objetivos fossem alcançados. Por Fim, a Deus a quem tudo devo.

À minha família, o maior presente que Deus me deu. Em especial à minha avó, Francisca Viana, que em vida, sem que percebesse, foi exemplo de bondade, caridade e amor ao próximo.

A busca exagerada da objetividade e do imediatismo, para atender às necessidades do "mercado" e não do ser humano, ainda que importante, nos desvia de uma reflexão mais profunda e concisa da ciência como fonte de informações e recursos prolongadores da vida.

Rubens Viana Ramos

SUMÁRIO

INTRODUÇÃO	1
Capítulo I	
ESTADOS COERENTES EM CRIPTOGRAFIA QUÂNTICA	
1.1 Introdução	6
1.2 Estados Coerentes em Criptografia Quântica	6
<i>Conclusões do Capítulo I</i>	31
Capítulo II	
MATRIZ DENSIDADE E MATRIZ COERÊNCIA EM COMUNICAÇÃO QUÂNTICA	
2.1 Introdução	33
2.2 Matrizes Densidade e Coerência em Comunicação Polarimétrica	33
2.2.1 Probabilidade dos resultados de medições de polarização com matriz coerência (J) e parâmetros de Stokes (S)	34
2.2.2 Medidas de distância entre estados quânticos de polarização usando J e S	36
2.2.3 Correção da variação da polarização em um sistema quântico polarimétrico	39
2.3 Grau de Pureza para Matrizes Densidade, g_p	41
2.3.1 Medida de distância entre estados quânticos utilizando g_p	46
2.3.2 Canal ruidoso e informação mútua utilizando g_p	50
2.4 Considerações sobre Estados Quânticos Entrelaçados	53
<i>Conclusões do Capítulo II</i>	62
Capítulo III	
DISPOSITIVOS ÓPTICOS NÃO-LINEARES EM SISTEMAS DE COMUNICAÇÃO QUÂNTICA	
3.1 Introdução	63
3.2 Ressonador Não-linear a Fibra - RNL	63
3.2.1 Controle e Sincronização de RNLs	66
3.3 Acoplador Não-linear a Fibra - ANL	74
3.4 Birrefringência	80
3.5 Aplicação dos Dispositivos Não-lineares em Comunicações Quânticas	81
<i>Conclusões do Capítulo III</i>	86
Capítulo IV	
CONCLUSÕES E PERSPECTIVAS	
4.1 Conclusões	87

4.2 Perspectivas	88
REFERÊNCIAS BIBLIOGRÁFICAS	89
<i>APÊNDICE A - Princípios Básicos de Mecânica Quântica e Estados Quânticos da Luz</i>	97
<i>APÊNDICE B - Quantização do Campo Eletromagnético</i>	115
<i>APÊNDICE C - Criptografia Quântica</i>	123
<i>APÊNDICE D - Probabilidade e Teoria da Informação</i>	138
<i>APÊNDICE E - Polarização da Luz</i>	143
<i>APÊNDICE F - Teoria Quântica da Informação</i>	148

INTRODUÇÃO

O crescente aumento do comércio eletrônico e de transações financeiras e bancárias pela internet se alia à contra-espionagem industrial e militar, bem como ao anti-terrorismo, em uma demanda por sistemas de segurança de dados de alta confiabilidade. Nesta linha, diversos algoritmos de criptografia foram desenvolvidos. Entretanto, todos eles sofrem do mesmo problema: a chave, sequência de bits que atua como parâmetro no algoritmo de encriptação e desencriptação das mensagens, precisa ser enviada a todos os usuários legítimos da comunicação. Se, durante o envio da chave, o canal de comunicação for monitorado e alguns bits da chave forem obtidos, as mensagens enviadas *a posteriori* poderão ser decifradas através de algoritmos adequados. Assim, surgiu a necessidade de um protocolo de distribuição da chave que fosse realmente imune ao monitoramento do canal por intrusos. A solução deste problema surgiu com a proposição de um protocolo de *criptografia quântica*, em 1984, conhecido como BB84. Nos anos que se seguiram, dois novos protocolos foram propostos, Ekert-91 e BB92. Todos estes protocolos garantem a transmissão segura da chave fazendo uso de princípios fundamentais da física e, por isso, a inviolabilidade é assegurada. Mais ainda, o protocolo de criptografia quântica permite, às partes autorizadas da comunicação, identificar se o canal de comunicação está, ou não, sendo observado por um intruso.

A óptica se apresenta como o principal suporte experimental da criptografia quântica e diversos protótipos desta têm sido implementados com sucesso. Nesses sistemas ópticos, a informação quântica pode ir codificada na polarização, sistema polarimétrico, ou na fase, sistema interferométrico. Ambos os sistemas suportam os protocolos, BB84 e BB92, baseados no princípio da complementaridade, e Ekert-91, baseado na correlação entre estados quânticos entrelaçados.

Após a proposição da criptografia quântica, a teoria quântica da informação (TQI) começou a ser desenvolvida, teoria esta que dá o suporte matemático, no contexto de telecomunicações, aos sistemas de comunicação quântica. A TQI usa vários conceitos da mecânica quântica e os aplica em comunicações. Daí surgem os conceitos de *informação quântica*, cuja unidade é o *qubit*, de *purificação*, usada para recuperar a pureza de estados quânticos entrelaçados mistos e de *fidelidade*, que indica a qualidade de um canal quântico. O resultado mais impressionante desta teoria é a teleportação do fóton. Ela consiste do envio da informação quântica do transmissor ao receptor, localmente espaçados, sem que o fóton portador da informação seja realmente enviado. No entanto, deve haver uma comunicação clássica entre as partes para que a teleportação se complete. Quando a teleportação é de um transmissor para mais que um receptor, ocorre um telecompartilhamento. O diagrama de blocos da Fig. 11 ilustra a região de atuação da comunicação quântica.

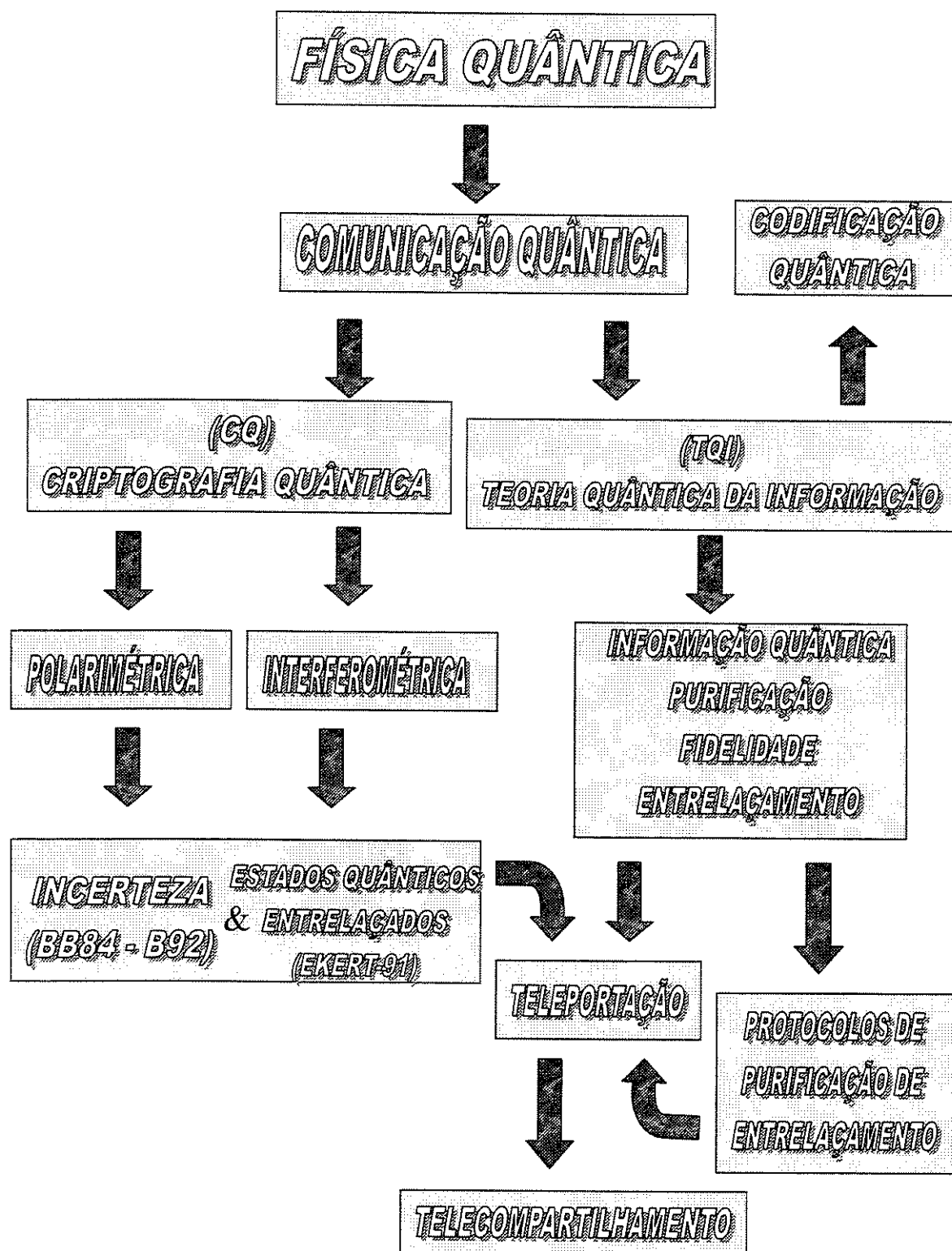


Fig. I1 - Diagrama esquemático da física quântica da informação.

Na Fig. 12 apresentamos, em diagrama de blocos, as partes de um sistema de comunicação quântica. Como a informação quântica é transportada por fótons, o primeiro bloco a ser considerado é a fonte de luz. A informação é portada por luz de um fóton. O modo mais simples de obtermos este tipo de luz, de forma aproximada, é aplicando uma forte atenuação no estado coerente na saída do laser. A consequência deste método é uma baixa taxa de transmissão, uma vez que muitos pulsos simplesmente não aparecerão na saída do atenuador. Esta fonte de luz serve para os protocolos que levam a informação na coerência, como o BB84 e o B92 [Ref. C1]. Se a informação é portada na correlação, então uma fonte EPR, que é baseada na conversão paramétrica descendente [Ref. C13], deve ser usada. Ela gera um par de fótons entrelaçados (fótons gêmeos). Um fóton do par deve ser entregue ao transmissor da informação e o outro fóton ao receptor. Os fótons produzidos pela fonte são então codificados, em polarização ou fase, segundo o sistema usado, polarimétrico ou interferométrico, e enviados pelo canal quântico, em geral um fibra óptica. A codificação consiste no uso de duas bases, B_1 e B_2 , onde cada base é composta por dois estados ortogonais entre si e não ortogonais com os estados da outra base. Os estados de uma base representam os bits 1 e 0. Nos protocolos quanto-criptográficos a escolha do bit e da base é aleatória, por isso, os moduladores de fase e polarizadores são controlados eletronicamente através de um *software* adequado. Ao passar pelo canal quântico, a informação quântica sofre perturbações clássicas e quânticas devido à interação com o meio. Estas interações provocam a descoerência e a des correlação dos estados quânticos. Por isso, é necessário o desenvolvimento de protocolos quânticos de purificação de entrelaçamento. Em geral, estes protocolos fazem com que as partes interessadas na comunicação realizem uma série de medidas, troca de informações clássicas e operações unitárias, esta última dependente do resultado das etapas anteriores, para transformar o estado misto resultante da interação com o meio, novamente em um estado puro. No receptor ocorre a decodificação dos bits através de um processo de medição. O fóton é detectado por um fotodiodo de avalanche (APD), que tem como vantagem o ganho e, como principal desvantagem, o alto ruído (*dark current*). Por isso, o APD deve ser resfriado, atualmente em 173 K, para minimizar o ruído. Por fim, deve existir uma sincronização temporal entre as ações do transmissor e do receptor. Dentre outras coisas, esta sincronização permite, por exemplo, a desconsideração de fotocontagens, devido ao ruído, nos instantes de tempo em que não é esperado a chegada de um pulso. Nesta tese, procuramos abordar a consideração da óptica quântica em comunicações ópticas, o uso da óptica clássica para tratar problemas clássicos em sistemas quânticos, a abordagem da teoria quântica da informação e a proposição de configurações de dispositivos ópticos capazes de realizar a troca de dados quânticos. Procuramos também fornecer, nos apêndices, a teoria necessária para o entendimento da tese. Assim, dividimos a tese em 4 capítulos e 6 apêndices.

O Capítulo I trata da utilização da fibra óptica como um canal quântico onde procuramos determinar como as estatísticas de número de fótons e fase, de um estado quântico coerente, se modificam quando o campo se propaga ao longo da fibra. Para isso, procedemos a quantização da envoltória do campo na fibra usando o formalismo de discretização de modos contínuos e o operador fase em um espaço de dimensão finita. Utilizamos o processo em uma simulação do protocolo quanto-criptográfico BB84, em um interferômetro a fibra.

O Capítulo II pode ser dividido em duas partes. Na primeira, usando apenas a abordagem clássica de luz polarizada, matriz transferência, matriz coerência e parâmetros

de Stokes, propomos um equalizador óptico, estrutura e algoritmo de equalização, para corrigir a perturbação da polarização devido à variação aleatória da birrefringência na fibra óptica em um sistema quântico polarimétrico. Na segunda parte, definimos o grau de pureza de estados quânticos e sua relação com a entropia. Abordamos, então, a teoria quântica da informação usando o grau de pureza. Finalizamos com uma descrição dos estados quânticos entrelaçados e das medidas de entrelaçamento.

No Capítulo III, iniciamos com a caracterização numérica dos dispositivos ópticos não-lineares a fibra: o ressonador não-linear (RNL) e o acoplador não-linear (ANL), bem como o efeito de birrefringência quando da propagação em regime não-linear. Mostramos que podemos controlar (regime caótico) e sincronizar (regime periódico) RNLs usando controladores nebulosos, bem como podemos mudar a curva de transmissividade de um ANL mudando o perfil do coeficiente de acoplamento. Por fim, apresentamos o uso destes dispositivos não-lineares em sistemas de comunicações quânticas polarimétricos e interferométricos.

O Capítulo IV apresenta as conclusões e propõe alguns trabalhos futuros, que podem tomar esta tese como referência inicial.

Nos apêndices apresentamos a teoria necessária ao entendimento da tese. Descrevemos, nos Apêndices A e B, sem muito rigor matemático, os princípios básicos de mecânica quântica, os estados quânticos da luz e a quantização do campo eletromagnético. O Apêndice C versa sobre a criptografia quântica e seus protocolos. O Apêndice D aborda a teoria da probabilidade e da informação clássica, enquanto que, o Apêndice E, trata da polarização da luz. Finalmente, o Apêndice F detalha importantes conceitos da teoria quântica da informação.

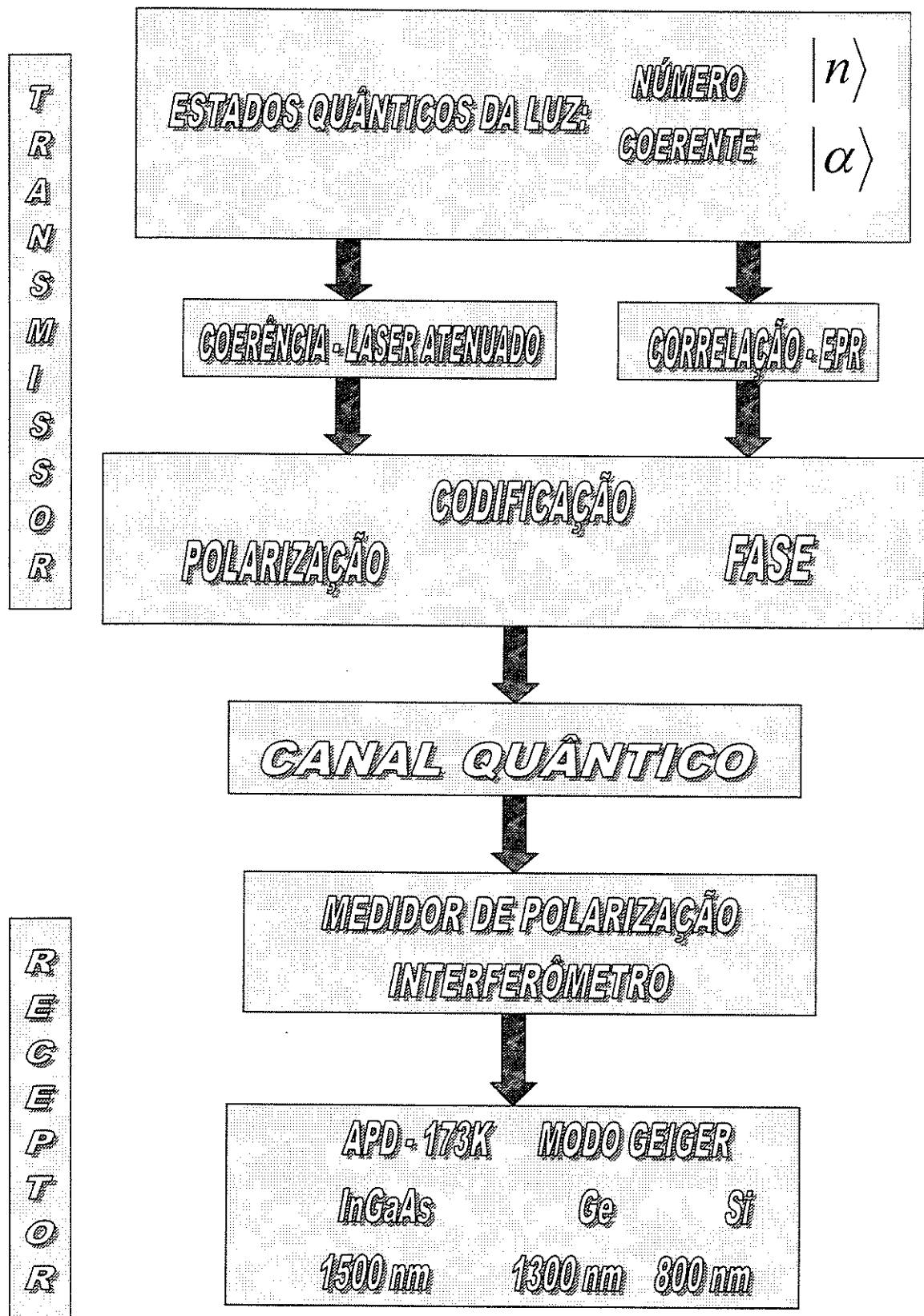


Fig. I2 - Diagrama esquemático de um sistema de CQ.

CAPÍTULO I

ESTADOS COERENTES EM CRIPTOGRAFIA QUÂNTICA

1.1 Introdução

Os sistemas de comunicações quânticas utilizam luz de fótons isolados. Na prática, este estado de um fóton isolado é aproximado por uma fonte de luz no estado coerente fortemente atenuada. Assim sendo, dedicamos este capítulo ao entendimento do estado quântico coerente. Para isto, usamos o formalismo da discretização de modos contínuos e do operador fase definido em um espaço de dimensão finita, para calcularmos as distribuições do número de fótons e da fase de um pulso gaussiano coerente. Analisamos o efeito da propagação deste pulso na fibra óptica e, ao final do capítulo, simulamos o protocolo BB84, usando estados coerentes contínuos, em um interferômetro a fibra usado em criptografia quântica.

1.2 Estados Coerentes em Criptografia Quântica

Assumimos, inicialmente, que a fibra óptica é linear, dispersiva e com perdas. A linearidade é devido às baixas intensidades dos campos envolvidos em comunicações quânticas. A fibra a ser considerada é monomodo degrau e, por isso, a dispersão considerada será apenas a dispersão material. Esta dispersão será levada em conta através do parâmetro fenomenológico macroscópico permissividade dielétrica, uma vez que o estudo da dispersão através da interação átomo-campo é muito complexa e foge aos objetivos do presente texto. Por fim, as perdas representam um fator extra de complexidade e serão abordadas, no momento oportuno, apenas através de considerações clássicas uma vez que, nas fibras ópticas, na região de interesse, elas são devidas principalmente ao espalhamento e não à absorção.

Tradicionalmente, a quantização do campo eletromagnético tem sido realizada em cavidades. Nestas, a cada automodo discreto é associado um oscilador harmônico quântico [Apêndices A e B]. Na fibra óptica, no contexto de comunicações à distância, esta abordagem não é adequada pois a fibra, nem de longe, lembra uma cavidade. A abordagem proposta para esta situação, e a que usaremos aqui, é a de modos contínuos [Refs. 1.1, 1.2]. O campo elétrico, suposto linearmente polarizado, que se propaga na fibra, é da forma:

$$E(r, \phi, z, t) = \alpha(z, t) f(r, \phi) \exp(-i\omega_0 t) \exp(i\beta z) \quad , \quad (1.1)$$

onde $\alpha(z, t)$ é a envoltória do campo montada em uma portadora de frequência angular ω_0 . $f(r, \phi)$ é a distribuição radial do campo, sendo considerada constante, e β é a constante de propagação do modo. Com a condição de normalização da potência do modo:

$$\int_0^{2\pi} \int_0^\infty |f(r, \phi)|^2 r dr d\phi = 1 , \quad (1.2)$$

o processo de quantização recai apenas sobre a envoltória do campo uma vez que o Hamiltoniano do campo dependerá apenas de sua envoltória. Iniciando a quantização do campo na fibra, descreveremos os campos contínuos em óptica quântica seguindo as Referências 1.1, 1.2 e 1.3. Os estados quânticos da luz estão expostos no Apêndice A e a quantização discreta do campo eletromagnético está detalhada no Apêndice B. O estado de número para modos contínuos é representado por [Ref. 1.3]:

$$|n\rangle = \frac{1}{\sqrt{n!}} \int_0^\infty \Psi(\omega_1, \omega_2, \dots, \omega_n) \hat{a}^+(\omega_1) \dots \hat{a}^+(\omega_n) d\omega_1 \dots d\omega_n |0\rangle \quad (1.3)$$

com a normalização:

$$\int_0^\infty |\Psi(\omega_1, \omega_2, \dots, \omega_n)|^2 d\omega_1 \dots d\omega_n = 1 . \quad (1.4)$$

O estado $|0\rangle$ é o estado vácuo do contínuo e deve obedecer a relação:

$$\hat{a}(\omega)|0\rangle = 0 , \quad (1.5)$$

onde $\hat{a}(\omega)$ é o operador *aniquilação* do contínuo. O índice inferior na integral da Eq. (1.3) inicia-se em 0 para que frequências negativas não sejam levadas em conta, uma vez que implicariam em fótons de energia negativa. Pela Eq. (1.4) podemos inferir que a função $|\Psi(\omega_1, \omega_2, \dots, \omega_n)|^2 d\omega_1 d\omega_2 \dots d\omega_n$ dá a probabilidade de haver um fóton em cada um dos intervalos $(\omega_i, \omega_i + d\omega_i)$, com $i=1, 2, \dots, n$. Suponhamos que a função Ψ possa ser fatorada em:

$$\Psi(\omega_1, \omega_2, \dots, \omega_n) = \sigma_1(\omega_1) \dots \sigma_n(\omega_n) , \quad (1.6)$$

sendo $|\sigma_i(\omega_i)|^2 d\omega_i$ a probabilidade do fóton se encontrar no intervalo $(\omega_i, \omega_i + d\omega_i)$. Substituindo a Eq. (1.6) na Eq. (1.3), obtemos:

$$|n\rangle = \frac{1}{\sqrt{n!}} \int_0^\infty \sigma_1(\omega_1) \dots \sigma_n(\omega_n) \hat{a}^+(\omega_1) \dots \hat{a}^+(\omega_n) d\omega_1 \dots d\omega_n |0\rangle \Rightarrow \quad (1.7)$$

$$|n\rangle = \frac{1}{\sqrt{n!}} \left(\int_0^\infty \sigma_1(\omega_1) \hat{a}^+(\omega_1) d\omega_1 \dots \int_0^\infty \sigma_n(\omega_n) \hat{a}^+(\omega_n) d\omega_n \right) |0\rangle . \quad (1.8)$$

Se as funções σ_i são localizadas, isto é, são não-nulas numa região estreita do espectro, então, para que o lado direito das Eqs.(1.7) e (1.8) não se anulem, iremos tomar $\sigma_i = \sigma_j$ para todo i e j . Com isto, chegamos a:

$$|n\rangle = \frac{1}{\sqrt{n!}} \left(\int_0^\infty \sigma(\omega) \hat{a}^+(\omega) d\omega \right)^n |0\rangle . \quad (1.9)$$

Por outro lado, do ponto de vista clássico, é intuitivo que, dada uma densidade espectral de energia $|\alpha(\omega)|^2$, correspondendo à intensidade do campo eletromagnético, o número de fótons no intervalo $(\omega, \omega + d\omega)$ é proporcional a $|\alpha(\omega)|^2 d\omega$. No caso particular do campo eletromagnético só ter um fóton, se a condição

$$\int_0^\infty |\alpha(\omega)|^2 d\omega = 1 \quad (1.10)$$

é satisfeita, então $|\alpha(\omega)|^2 d\omega$ dá a probabilidade do fóton pertencer ao intervalo $(\omega, \omega + d\omega)$. Logo, para o estado de um fóton, temos:

$$|\sigma(\omega)|^2 = |\alpha(\omega)|^2 . \quad (1.11)$$

Ainda, usando a densidade espectral de energia temos, segundo o teorema clássico de Rayleigh [Ref. 1.4], que o valor da energia do sinal $\alpha(\omega)$ é:

$$E = \int_0^\infty |\alpha(\omega)|^2 d\omega , \quad (1.12)$$

onde o índice inferior em (1.12) inicia-se em 0 por assumirmos $\alpha(\omega)$ estreita e centrada na frequência positiva ω_0 . Seja, agora, o conjunto de funções complexas $\{\xi_i(\omega)\}$ com $i = 1, 2, 3, \dots, \infty$, as quais satisfazem as condições de completeza e ortonormalidade, respectivamente [Refs. 1.1, 1.2]:

$$\sum_{i=1}^\infty \xi_i(\omega) \xi_i^*(\omega') = \delta(\omega - \omega') \quad (1.13)$$

$$\int_0^\infty d\omega \xi_i(\omega) \xi_j^*(\omega) = \delta_{ij} , \quad (1.14)$$

onde "*" significa "tomar o complexo conjugado". Fazendo uso das Eqs. (1.13) e (1.14) para expandir o sinal $\alpha(\omega)$, temos:

$$\alpha(\omega) = \sum_i C_i \xi_i(\omega) \quad (1.15)$$

$$C_i = \int_0^\infty \alpha(\omega) \xi_i^*(\omega) d\omega . \quad (1.16)$$

Substituindo (1.15) em (1.12) e fazendo uso das Eqs. (1.13) e (1.14), encontramos que:

$$E = \int_0^\infty |\alpha(\omega)|^2 d\omega = \sum_{\substack{i,j \\ i \neq j}} C_i C_j^* \int_0^\infty \xi_i(\omega) \xi_j^*(\omega) d\omega + \sum_i |C_i|^2 \int_0^\infty |\xi_i(\omega)|^2 d\omega = \sum_i |C_i|^2 \quad . \quad (1.17)$$

Portanto, a energia do sinal é distribuída entre as componentes da expansão segundo os valores dos $|C_i|^2$. Como a energia é quantizada, a mínima energia (quantum) no modo i da expansão (1.15) deve ser dada por [Ref. 1.2]:

$$\Delta E_i = \int_0^\infty \hbar \omega |\xi_i(\omega)|^2 d\omega \quad . \quad (1.18)$$

Obviamente, para que a Eq. (1.18) seja finita, $|\xi_i(\omega)|^2$ deve ser não nulo apenas em um número finito de regiões finitas do espectro. Para estados de número, a energia total deve ser então:

$$E = \sum_i n_i \Delta E_i \quad , \quad (1.19)$$

sendo n_i o número de quanta do modo i da expansão (1.15). Igualando as Eqs. (1.19) e (1.17) obtemos n_i em função da densidade espectral de energia e das funções de expansão:

$$|C_i|^2 = n_i \Delta E_i \Rightarrow \quad (1.20)$$

$$n_i = \frac{\left| \int_0^\infty \alpha(\omega) \xi_i^*(\omega) d\omega \right|^2}{\int_0^\infty \hbar \omega |\xi_i(\omega)|^2 d\omega} \quad . \quad (1.21)$$

A Eq. (1.21) é apenas uma aproximação clássica para o cálculo do número de fótons, a partir da envoltória do campo, para estados de número.

De volta à argumentação quântica, no caso do guia de onda suportar vários modos todos devem ser quantizados. Nesta situação, a energia total do campo é a soma da energia dos diferentes modos, indicados pelo sub-índice k , e o Hamiltoniano total é dado por [Ref. 1.2]:

$$\hat{H} = \sum_k \int_0^\infty \hbar \omega \hat{a}_k^+(\omega) \hat{a}_k(\omega) d\omega \quad , \quad (1.22)$$

e os operadores aniquilação, $\hat{a}_k$, e criação, $\hat{a}_k^+$, obedecem as seguintes relações de comutação [Ref 1.2]:

$$[\hat{a}_k(\omega), \hat{a}_m^+(\omega')] = \delta_{km} \delta(\omega - \omega') \quad (1.23)$$

$$[\hat{a}_k(\omega), \hat{a}_m(\omega')] = [\hat{a}_k^+(\omega), \hat{a}_m^+(\omega')] = 0 \quad . \quad (1.24)$$

Como cada modo (distribuição espacial do campo) pode ser trabalhado individualmente (sem acoplamento), e realmente usaremos apenas um (fibra monomodo), abandonaremos o sub-índice k . Observemos que a introdução do conjunto de funções $\{\xi_i(\omega)\}$ possibilitou transformar a energia do contínuo numa soma discreta de quanta, Eq. (1.19). Esta característica é favorável, pois facilita o tratamento matemático. Fazendo agora:

$$\sigma(\omega) = \sum_i b_i \xi_i(\omega) \quad (1.25)$$

e substituindo a Eq. (1.25) na Eq. (1.9), obtemos para o estado de número:

$$|n\rangle = \frac{1}{\sqrt{n!}} \left(\int_0^\infty \sum_i b_i \xi_i(\omega) \hat{a}^+(\omega) d\omega \right)^n |0\rangle = \frac{1}{\sqrt{n!}} \left(\sum_i b_i \hat{A}^+(\xi_i) \right)^n |0\rangle, \quad (1.26)$$

onde [Ref. 1.2]:

$$\hat{A}^+(\xi_i) = \int_0^\infty \xi_i(\omega) \hat{a}^+(\omega) d\omega \quad (1.27)$$

é um operador criação discreto. Usando as Eqs.(1.23), (1.24) e (1.27), encontramos que:

$$[\hat{A}(\xi_i), \hat{A}^+(\xi_j)] = \delta_{ij} \quad (1.28)$$

$$[\hat{A}(\xi_i), \hat{A}(\xi_j)] = [\hat{A}^+(\xi_i), \hat{A}^+(\xi_j)] = 0. \quad (1.29)$$

Cada operador criação $\hat{A}^+(\xi_i)$ criará n_i fótons no i -ésimo modo. Como o conjunto inteiro tem n fótons, a condição:

$$n = \sum_i n_i \quad (1.30)$$

deve ser satisfeita. Depois que os n fótons forem alocados em alguns dos modos, os demais deverão ter o coeficiente $b_i = 0$. Por exemplo, se o campo tem 10 fótons, com $n_3 = 10$ e $n_i = 0$, $i = 0, 1, 2, 4, \dots$, então:

$$\sigma(\omega) = b_3 \xi_3(\omega). \quad (1.31)$$

Mais ainda, suponhamos, por exemplo, que n fótons estejam alocados apenas nos dois primeiros modos, então a Eq. (1.26) se reduz a:

$$|n\rangle = \frac{1}{\sqrt{n!}} \left\{ \sum_{m=1}^{n-1} r_m [\hat{A}^+(\xi_1)]^m [\hat{A}^+(\xi_2)]^{n-m} b_1^m b_2^{n-m} \right\} |0\rangle, \quad (1.32)$$

onde o fator r_m dá a multiplicidade do termo, uma vez que, devido às Eqs.(1.28) e (1.29), a ordem dos modos não influencia no resultado final. Portanto, o estado $|n\rangle$ é uma superposição (soma) do produto dos estados criados pelos operadores $\hat{A}^+(\xi_i)$, onde cada termo da superposição se diferencia pelo número de fótons em cada modo, mas mantendo a soma do número de fótons constante. No caso geral, onde os modos povoados não são conhecidos, um termo genérico da Eq. (1.26) é da forma:

$$\frac{1}{\sqrt{n!}} \prod_i r_i b_i^{n_i} [\hat{A}^+(\xi_i)]^{n_i} . \quad (1.33)$$

A equação para o estado de número do contínuo, dada na Referência 1.2, é:

$$|n\rangle = |n_1\rangle \otimes |n_2\rangle \otimes \dots \otimes |n_i\rangle \otimes \dots = \prod_{i=1}^{\infty} \frac{1}{\sqrt{n_i!}} [\hat{A}^+(\xi_i)]^{n_i} |0\rangle , \quad (1.34)$$

sendo $|n_i\rangle$, $i = 1, 2, \dots$, os estados número, para cada oscilador individual. Observando a Eq. (1.33), vemos que a Eq. (1.34) pode ser obtida através do colapso (redução do somatório a um dos termos do mesmo) da Eq. (1.26), se os coeficientes b_i satisfizerem a relação:

$$\frac{r_i b_i^{n_i}}{\sqrt{n!}} = \frac{1}{\sqrt{n_i!}} . \quad (1.35)$$

A Eq. (1.27) transformou o estado contínuo num produto tensorial de osciladores discretos e, para cada um destes, são definidos os operadores criação, aniquilação e número. Se o estado do contínuo é o estado de número, então cada oscilador individual também estará num estado de número, e a soma dos quanta dos osciladores individuais é igual ao número de quanta do estado contínuo (Eq. (1.30)). O operador número do i -ésimo oscilador individual é dado por:

$$\hat{n}_i |n_i\rangle = \hat{A}^+(\xi_i) \hat{A}(\xi_i) |n_i\rangle = n_i |n_i\rangle \quad (1.36)$$

e, usando a teoria quântica de osciladores harmônicos discretos [Ref. 1.2 e Apêndices A e B], temos:

$$\hat{A}(\xi_i) |n_i\rangle = \sqrt{n_i} |n_i - 1\rangle \quad (1.37)$$

$$\hat{A}^+(\xi_i) |n_i\rangle = \sqrt{n_i + 1} |n_i + 1\rangle \quad (1.38)$$

$$\hat{A}(\xi_i) |0\rangle = 0 . \quad (1.39)$$

Por fim, os estados $|n_i\rangle$ são ortonormais, isto é, [Ref. 1.2]:

$$\langle n_i | m_i \rangle = \delta_{nm} . \quad (1.40)$$

O número total de partículas do contínuo é dado por [Refs. 1.1, 1.2, 1.3]:

$$\hat{N} = \int_0^{\infty} \hat{a}^+(\omega) \hat{a}(\omega) d\omega . \quad (1.41)$$

Usando as Eqs. (1.13) e (1.14) para inverter a Eq. (1.27), obtemos:

$$\hat{a}^+(\omega) = \sum_{i=1}^{\infty} \hat{A}^+(\xi_i) \xi_i^*(\omega) . \quad (1.42)$$

Substituindo (1.42) em (1.41), o número de fótons fica também dado por [Ref. 1.2]:

$$\hat{N} = \sum_{i=1}^{\infty} \hat{A}^+(\xi_i) \hat{A}(\xi_i) = \sum_{i=1}^{\infty} \hat{n}_i . \quad (1.43)$$

Como anteriormente afirmado, a cada função ξ_i (oscilador individual) está associado um operador número, $\hat{n}_i$. Usando as Eqs. (1.28) e (1.29) temos, ainda, que [Ref. 1.2]:

$$[\hat{n}_i, \hat{n}_j] = 0 . \quad (1.44)$$

Substituindo a Eq. (1.42) na Eq. (1.22), o Hamiltoniano do campo fica na forma [Ref 1.2]:

$$\hat{H} = \sum_{i,j} \hat{A}^+(\xi_i) A(\xi_j) \int_0^{\infty} \hbar \omega \xi_i^*(\omega) \xi_j(\omega) d\omega = \sum_i \hat{n}_i \Delta E_i + \sum_{\substack{i,j \\ i \neq j}} \hat{A}^+(\xi_i) A(\xi_j) \int_0^{\infty} \hbar \omega \xi_i^*(\omega) \xi_j(\omega) d\omega \quad (1.45)$$

e o valor esperado da energia do sistema no estado de número é [Ref 1.2]:

$$\langle n | \hat{H} | n \rangle = \sum_{i=1}^{\infty} n_i \int_0^{\infty} \hbar \omega |\xi_i(\omega)|^2 d\omega = \sum_{i=1}^{\infty} n_i \Delta E_i . \quad (1.46)$$

A Eq. (1.45) é interessante pois ela nos diz que, apesar do número de fótons do contínuo ser igual à soma do número de fótons dos osciladores individuais, a energia do contínuo não é igual à soma da energia dos osciladores individuais. Isto ocorre devido ao último termo da Eq. (1.45) (termo cruzado), implicando que a energia dos fótons do contínuo não é bem definida. Isto pode ser observado através da variância (incerteza) da energia do estado de número do contínuo, dada por [Ref. 1.2]:

$$(\Delta \hat{H})^2 = \sum_{i,j} n_i n_j \left| \int_0^{\infty} \hbar \omega \xi_i^*(\omega) \xi_j(\omega) d\omega \right|^2 + \sum_i n_i \left\{ \int_0^{\infty} (\hbar \omega)^2 |\xi_i(\omega)|^2 d\omega - \left(1 + n_i \right) \left(\int_0^{\infty} \hbar \omega |\xi_i(\omega)|^2 d\omega \right)^2 \right\} , \quad (1.47)$$

que não se anula. Entretanto, se as funções $\xi_i(\omega)$ forem centradas em diferentes valores de ω e com largura bem pequena, de forma a tornar o termo cruzado da Eq. (1.45) nulo, poderemos obter fótons bem definidos.

Até o presente momento temos considerado apenas o estado de número; agora observaremos o estado coerente do contínuo. Primeiramente observemos que, devido à ortonormalidade dos estados número, eles formam uma base para o espaço de Hilbert de dimensão infinita. Assim, tal como a Eq. (1.34) para o estado de número, o estado coerente pode ser representado pelo produto tensorial [Refs. 1.1, 1.2]:

$$|\alpha\rangle = |\alpha_1\rangle \otimes \dots \otimes |\alpha_i\rangle \otimes \dots = \prod_i |\alpha_i\rangle, \quad (1.48)$$

onde cada estado do produto tensorial obedece à equação que define os estados coerentes (autoestados do operador aniquilação) [Ref. 1.2]:

$$\hat{A}(\xi_i)|\alpha_i\rangle = \alpha_i|\alpha_i\rangle, \quad (1.49)$$

sendo α_i um escalar complexo arbitrário. Usando (1.49) em (1.48) obtemos:

$$\hat{A}(\xi_i)|\alpha\rangle = \alpha_i|\alpha\rangle. \quad (1.50)$$

Expandindo o estado $|\alpha_i\rangle$ na base de estados de número, temos:

$$|\alpha_i\rangle = \sum_{n_i=0}^{\infty} \langle n_i | \alpha_i \rangle |n_i\rangle = \sum_{n_i=0}^{\infty} \exp\left(-\frac{|\alpha_i|^2}{2}\right) \frac{\alpha_i^{n_i}}{\sqrt{n_i!}} |n_i\rangle, \quad (1.51)$$

onde $|\langle n_i | \alpha_i \rangle|^2$ dá a probabilidade do estado $|\alpha_i\rangle$ ter n_i fótons [Apêndice A]. Trabalhando com as Eqs. (1.34) e (1.51), chegamos a:

$$|\alpha_i\rangle = \exp\left(-\frac{|\alpha_i|^2}{2}\right) \sum_{n_i=0}^{\infty} \frac{(\alpha_i \hat{A}^+(\xi_i))^{n_i}}{n_i!} |0\rangle. \quad (1.52)$$

Se usarmos o operador deslocamento generalizado de Glauber [Refs. 1.1, 1.2] que gera estados coerentes a partir do vácuo, temos [Ref. 1.2]:

$$\hat{D}(\xi_i, \alpha_i) = \exp[\alpha_i \hat{A}^+(\xi_i) - \alpha_i^* \hat{A}(\xi_i)] \quad (1.53)$$

$$|\alpha_i\rangle = \hat{D}(\xi_i, \alpha_i)|0\rangle \quad (1.54)$$

e, portanto [Ref. 1.2]:

$$|\alpha\rangle = \prod_i \hat{D}(\xi_i, \alpha_i) |0\rangle = \exp\left(\sum_i \alpha_i \hat{A}^+(\xi_i) - HC\right) |0\rangle, \quad (1.55)$$

onde HC representa o Hermiteano conjugado do termo anterior. Trabalhando o termo dentro da exponencial da Eq. (1.55), temos:

$$\sum_i \alpha_i \hat{A}^+(\xi_i) = \sum_i \int_0^\infty \alpha_i \xi_i(\omega) \hat{a}^+(\omega) d\omega = \int_0^\infty \left[\sum_i \alpha_i \xi_i(\omega) \right] \hat{a}^+(\omega) d\omega = \int_0^\infty \alpha(\omega) \hat{a}^+(\omega) d\omega, \quad (1.56)$$

onde

$$\alpha(\omega) = \sum_i \alpha_i \xi_i(\omega). \quad (1.57)$$

Substituindo (1.56) em (1.55), obtemos:

$$|\alpha\rangle = \exp\left(\int_0^\infty d\omega \alpha(\omega) \hat{a}^+(\omega) - HC\right) |0\rangle \quad (1.58)$$

que, como pode ser observado, obedece a [Ref. 1.1, 1.2]:

$$\hat{a}(\omega) |\alpha(\omega)\rangle = \alpha(\omega) |\alpha(\omega)\rangle, \quad (1.59)$$

como era esperado. Portanto, quando cada oscilador individual estiver num estado coerente, Eq. (1.49), o estado como um todo também estará, Eq. (1.59). O número médio de fótons e a variância, que são iguais para estados coerentes, são dados por [Ref. 1.2]:

$$\langle \hat{N} \rangle = \langle \Delta \hat{N} \rangle^2 = \sum_i |\alpha_i|^2 = \int_0^\infty |\alpha(\omega)|^2 d\omega, \quad (1.60)$$

enquanto que o valor esperado e a variância da energia são dadas por [Ref. 1.2]:

$$\langle \hat{H} \rangle = \int_0^\infty \hbar \omega |\alpha(\omega)|^2 d\omega \quad (1.61)$$

$$\langle \Delta \hat{H} \rangle^2 = \int_0^\infty (\hbar \omega)^2 |\alpha(\omega)|^2 d\omega. \quad (1.62)$$

Por fim, a projeção do estado coerente total sobre o estado de número do i -ésimo oscilador é:

$$\langle n_i | \alpha \rangle = \prod_j \langle n_i | \alpha_j \rangle = \prod_j \langle n_i | \exp\left(\frac{-|\alpha_j|^2}{2}\right) \sum_{n_k} \frac{\alpha_j^{n_k}}{\sqrt{n_k!}} |n_k\rangle = \quad (1.63)$$

$$\prod_j \exp\left(\frac{-|\alpha_j|^2}{2}\right) \sum_{n_k} \frac{\alpha_j^{n_k}}{\sqrt{n_k!}} \langle n_i | n_k \rangle = \prod_j \exp\left(\frac{-|\alpha_j|^2}{2}\right) \frac{\alpha_j^{n_i}}{\sqrt{n_i!}} \Rightarrow \quad (1.64)$$

$$|\langle n_i | \alpha \rangle|^2 = \exp\left(-\sum_j |\alpha_j|^2\right) \frac{\left|\prod_j \alpha_j\right|^{2n_i}}{n_i!}, \quad (1.65)$$

onde a Eq. (1.51) foi usada em (1.63). Devido à Eq. (1.43), a distribuição de probabilidade do número de fótons no estado contínuo coerente $|\alpha\rangle$, é a distribuição da soma das variáveis aleatórias correspondentes ao número de fótons de cada oscilador individual, com distribuições de probabilidades dadas por $|\langle n_i | \alpha_i \rangle|^2$. Neste ponto, com as Eqs. (1.13), (1.14), (1.43), (1.51) e (1.57) podemos determinar a função densidade de probabilidade, FDP, do número de fótons de um pulso, com envoltória dada por $\alpha(\omega)$, num estado coerente contínuo. Agora, falta-nos determinar a FDP da fase. Este problema é mais complexo pois não há um operador fase Hermiteano no espaço de Hilbert de dimensão infinita. Iniciaremos o tratamento da fase definindo o operador fase de Pegg-Barnett [Apêndice A] e o aplicaremos em cada oscilador individual da representação discreta do contínuo. Depois tentaremos obter a FDP da fase do contínuo a partir da FDP da fase dos osciladores individuais.

Observando a Eq. (1.51) vemos que, se $|\alpha_i|^2$ for pequeno o somatório infinito pode ser truncado e os estados $|\alpha_i\rangle$ podem, com boa aproximação, ser expandidos em um número finito de estados de número (base finita). Isto e a possibilidade de definir um operador fase Hermiteano em um espaço de dimensão finita foram as motivações para o desenvolvimento dos estados quânticos da luz num espaço de dimensão finita [Ref. 1.5]. Daqui em diante todos os cálculos são referidos a um único oscilador discreto. Neste espaço finito de dimensão $s+1$, onde $\{|0\rangle, \dots, |n\rangle, \dots, |s\rangle\}$ é uma base para o mesmo, temos [Ref 1.5]:

$$\sum_{n=0}^s |n\rangle \langle n| = 1 \quad (1.66)$$

$$\langle n | m \rangle = \delta_{nm} . \quad (1.67)$$

Os operadores aniquilação e criação são redefinidos neste novo espaço de dimensão finita como sendo [Ref 1.5]:

$$\hat{a} = \sum_{n=1}^s \sqrt{n} |n-1\rangle \langle n| \quad (1.68)$$

$$\hat{a}^+ = \sum_{n=1}^s \sqrt{n} |n\rangle \langle n-1| . \quad (1.69)$$

com os estados limites inferior e superior obedecendo a [Ref 1.5]:

$$\hat{a}|0\rangle = 0 \quad (1.70)$$

$$\hat{a}^+|s\rangle = 0 \quad (1.71)$$

e com a relação de comutação para os operadores criação e aniquilação da forma [Ref 1.5]:

$$[\hat{a}, \hat{a}^+] = 1 - (s+1)|s\rangle\langle s| \quad (1.72)$$

Por fim, o operador número é definido, da forma usual, como sendo [Apêndice A]:

$$\hat{N} = \sum_{n=1}^s n|n\rangle\langle n| = \hat{a}^+ \hat{a} \quad (1.73)$$

Pode-se, neste espaço de dimensão finita, definir-se estados fases (estados com fase precisamente conhecida) [Ref. 1.5, 1.6]:

$$|\theta_m\rangle = \frac{\sum_{n=0}^s \exp(i\theta_m n)|n\rangle}{\sqrt{s+1}}, \quad (1.74)$$

com as propriedades de completeza e ortonormalidade [Ref. 1.5]:

$$\sum_{m=0}^s |\theta_m\rangle\langle\theta_m| = 1 \quad (1.75)$$

$$\langle\theta_m|\theta_n\rangle = \delta_{nm} \quad (1.76)$$

Cada fase é definida por [Refs. 1.5, 1.6]:

$$\theta_m = \theta_0 + \frac{2\pi m}{s+1}, \quad m = 0, 1, 2, \dots, s \quad (1.77)$$

sendo θ_0 a fase inicial de referência. O operador fase Hermiteano, conhecido como operador de Pegg-Barnett, é definido como sendo:

$$\hat{\Phi} = \sum_{m=0}^s \theta_m |\theta_m\rangle\langle\theta_m| \quad (1.78)$$

$$\hat{\Phi}|\theta_m\rangle = \theta_m |\theta_m\rangle \quad (1.79)$$

Como os estados de número e fases formam bases para o mesmo espaço, todas as funções do operador fase podem ser escritas como função dos estados de número e vice-versa. O operador fase em função dos estados de número fica [Ref. 1.5]:

$$\hat{\Phi} = \theta_0 + \frac{2\pi s}{s+1} + \frac{2\pi}{s+1} \sum_{\substack{k,n=0 \\ k \neq n}}^s \frac{\exp[-i(k-n)\theta_0]}{\exp\left[-i(k-n)\frac{2\pi}{s+1}\right] - 1} |n\rangle\langle k| . \quad (1.80)$$

Apesar dos estados coerentes truncados terem sido a motivação do uso do espaço de dimensão finita, a definição dos mesmos neste espaço não é trivial. Os estados coerentes não podem ser considerados como autoestados do operador aniquilação uma vez que, o único autoestado deste operador no espaço de dimensão finita, é o vácuo. De qualquer forma, o estado coerente ainda é uma superposição dos estados de número [Apêndice A]:

$$|\alpha\rangle = \sum_{n=0}^s c_n^s |n\rangle \quad (1.81)$$

e pode ser obtido usando-se o operador deslocamento:

$$|\alpha\rangle = \exp(\alpha \hat{a}^+ - \alpha^* \hat{a}) |0\rangle = \sum_{k=0}^{\infty} \frac{(\alpha \hat{a}^+ - \alpha^* \hat{a})^k}{k!} |0\rangle . \quad (1.82)$$

Determinamos os coeficientes c_n^s da Eq. (1.81) numericamente usando a forma matricial dos estados e operadores. A representação matricial do estado de número, no espaço de dimensão $s+1$, é dada por:

$$|n\rangle = (1 \quad \dots \quad n+1 \quad \dots \quad s)^T = (0 \quad \dots \quad 1 \quad \dots \quad 0)^T \quad (1.83)$$

$$\langle n| = (1 \quad \dots \quad n+1 \quad \dots \quad s) = (0 \quad \dots \quad 1 \quad \dots \quad 0) , \quad (1.84)$$

ou seja, o estado $|n\rangle$ é representado por um vetor coluna com 1 na $(n+1)$ -ésima posição e zero nas demais. Usando as Eqs. (1.83) e (1.84) em (1.68) e (1.69), obtemos a forma matricial dos operadores aniquilação e criação:

$$\hat{a} = \begin{pmatrix} 0 & \sqrt{1} & 0 & \dots & 0 \\ 0 & 0 & \sqrt{2} & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \dots & 0 & \sqrt{s} \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix} , \quad \hat{a}^+ = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ \sqrt{1} & 0 & 0 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & \dots & \sqrt{s-1} & 0 & 0 \\ 0 & \dots & 0 & \sqrt{s} & 0 \end{pmatrix} \quad (1.85)$$

e o argumento da função exponencial da Eq. (1.82) fica da forma:

$$\hat{T} = (\alpha \hat{a}^\dagger - \alpha^* \hat{a}) = \begin{pmatrix} 0 & -\alpha^* \sqrt{1} & 0 & \dots & 0 \\ \alpha \sqrt{1} & 0 & -\alpha^* \sqrt{2} & & 0 \\ \vdots & & & & \vdots \\ 0 & \dots & \alpha \sqrt{s-1} & 0 & -\alpha^* \sqrt{s} \\ 0 & \dots & 0 & \alpha \sqrt{s} & 0 \end{pmatrix}. \quad (1.86)$$

Logo, os coeficientes da expansão (1.81) são obtidos por:

$$c_n^s = \langle n | \alpha \rangle = \langle n | D(\alpha) | 0 \rangle = \langle n | \exp(\hat{T}) | 0 \rangle = \begin{pmatrix} 0 & \dots & 1 & \dots & 0 \end{pmatrix} \left(\sum_{k=0}^{\infty} \frac{(\hat{T})^k}{k!} \right) \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \quad (1.87)$$

Uma vez calculado os coeficientes, a distribuição do número de fótons, no espaço de dimensão s , é dada por:

$$p_n = |\langle n | \alpha \rangle|^2 = |c_n^s|^2. \quad (1.88)$$

Pode-se mostrar numericamente que (1.88) se aproxima da distribuição Poissoniana quando $s \rightarrow \infty$ [Ref 1.5]. O número médio de fótons do estado coerente $|\alpha\rangle$ é dado por:

$$\langle n \rangle = \sum_{n=0}^s n p_n = \sum_{n=0}^s n |c_n^s|^2. \quad (1.89)$$

Por sua vez, a distribuição de probabilidade da fase é:

$$p(\theta_m) = |\langle \theta_m | \alpha \rangle|^2. \quad (1.90)$$

Usando as Eqs. (1.74) e (1.81) em (1.90) obtemos [Ref 1.5]:

$$p(\theta_m) = \frac{1}{s+1} \left| \sum_{k=0}^s c_k^s \exp(-ik\theta_m) \right|^2. \quad (1.91)$$

O valor médio da fase é o valor da fase de α , isto é, se $\alpha = |\alpha| \exp(i\phi)$, então:

$$\langle \theta \rangle = \sum_m p_m \theta_m = \phi \quad [\text{rad}]. \quad (1.92)$$

A variância depende da fase de referência θ_0 , sendo mínima quando $\theta_0 = \phi - \pi$ e máxima quando $\theta_0 = \phi$ [Ref. 1.5]. Consideremos, por exemplo, um estado coerente com $\alpha =$

$4\exp(i\pi/4)$. As Figs. 1.1 e 1.2 mostram, respectivamente, as distribuições de probabilidade do número de fótons e da fase, $p(n)$ e $p(\theta)$, para o referido estado coerente, num espaço de dimensão 21.

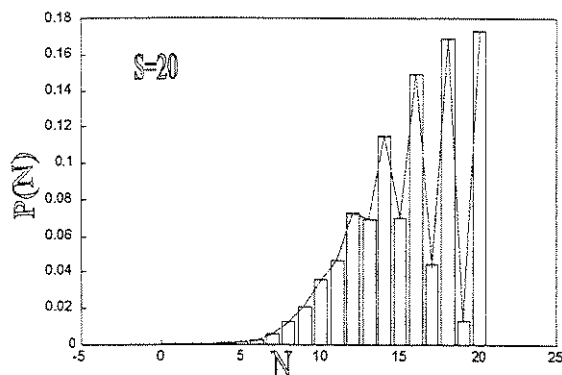


Fig. 1.1 - Distribuição do número de fótons.
 $\alpha = 4\exp(i\pi/4)$ e $s = 20$. $\langle n \rangle = 15,5282$.

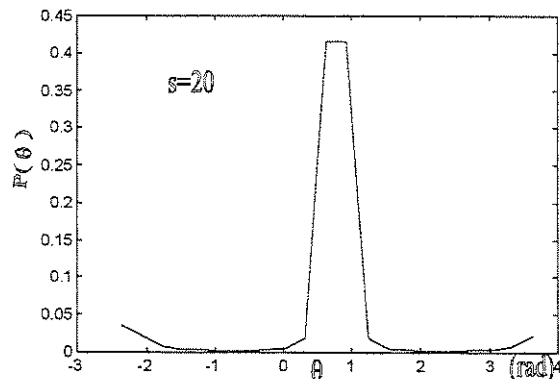


Fig. 1.2 - Distribuição da fase.
 $\alpha = 4\exp(i\pi/4)$ e $s = 20$. $\langle \theta \rangle = 38,5796^\circ$

Para as distribuições das Figs. 1.1 e 1.2, o número médio de fótons e da fase são, respectivamente, $\langle n \rangle = 15,5282$ e $\langle \theta \rangle = 38,5796^\circ$. As Figs. 1.3 e 1.4 mostram, respectivamente, as distribuições de probabilidade do número de fótons e da fase, $p(n)$ e $p(\theta)$, para o mesmo estado coerente, num espaço de dimensão 101.

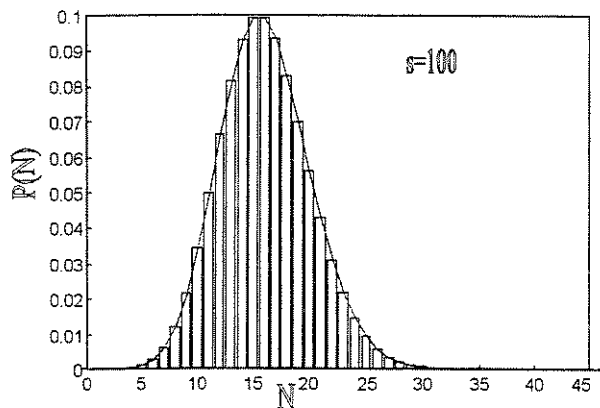


Fig. 1.3 - Distribuição do número de fótons.
 $\alpha = 4\exp(i\pi/4)$ e $s = 100$. $\langle n \rangle = 16$.

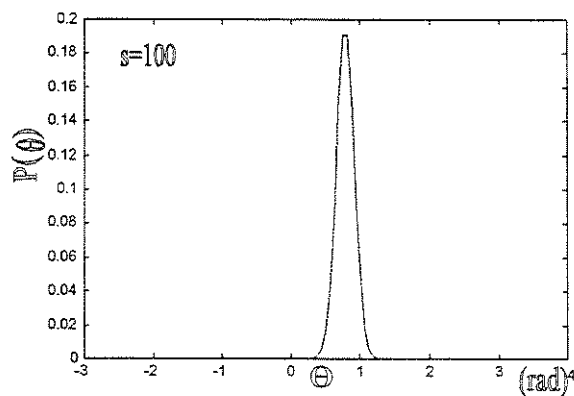


Fig. 1.4 - Distribuição da fase.
 $\alpha = 4\exp(i\pi/4)$ e $s = 100$. $\langle \theta \rangle = 45^\circ$.

Para as distribuições das Figs. 1.3 e 1.4 os valores médios do número de fótons e da fase são, respectivamente, $\langle n \rangle = 16$ e $\langle \theta \rangle = 45^\circ$, que são os valores corretos esperados. Portanto, quanto maior a razão $s/|\alpha|^2$ mais os estados da Eq. (1.81) se aproximam dos estados coerentes de Glauber. Os resultados das Figs. 1.1 -1.4 estão de acordo com os resultados mostrados na Referência 1.5.

Consideraremos agora, usando as informações já expostas, a propagação de um pulso coerente através da fibra óptica. O pulso de entrada na fibra é suposto coerente e, portanto, representado pela Eq. (1.48), aqui repetida:

$$|\alpha(\omega)\rangle = |\alpha_1\rangle \otimes \dots \otimes |\alpha_i\rangle \otimes \dots \otimes |\alpha_k\rangle = \prod_{i=1}^k |\alpha_i\rangle . \quad (1.93)$$

O produtório da Eq. (1.93) foi feito finito para fins de simulação computacional. Cada oscilador discreto, no estado coerente $|\alpha_i\rangle$, pertence ao espaço de dimensão finita anteriormente descrito, com as distribuições de número de fótons e de fase dadas pelas Eqs. (1.88) e (1.91), respectivamente. A envoltória do pulso de entrada na fibra é considerado Gaussiano com equações no tempo e na frequência da forma:

$$\alpha(t) = A \exp\left(\frac{-t^2}{2T_0^2}\right) \exp(i\phi) \quad (1.94)$$

$$\alpha(\omega) = \frac{A}{b} \exp\left(\frac{-(\omega - \omega_0)^2}{4\pi b^2}\right) \exp(i\phi) \quad (1.95)$$

$$b = \left(\sqrt{2\pi T_0^2}\right)^{-1} \quad (1.96)$$

$$A = \sqrt{\frac{\langle n \rangle b}{\pi\sqrt{2}}} , \quad (1.97)$$

onde ω_0 é a frequência da portadora, T_0 é a largura do pulso, ϕ é a fase inicial e A é a amplitude, dependente do número médio de fótons, obtida a partir da Eq. (1.60). Devemos, agora, usar a Eq. (1.57) para determinar as variáveis α_i a partir $\alpha(\omega)$. Para isso, devemos inicialmente escolher as funções de expansão $\xi_i(\omega)$ que obedçam as Eqs. (1.13) e (1.14) (condições de ortonormalidade e completicidade). Aqui, optamos pelo uso da função *sinc*, que é destinada comumente à reconstrução de sinais amostrados [Refs. 1.4, 1.7], como função de expansão. A função *sinc* e a expansão de $\alpha(\omega)$ com o uso da mesma, são dadas por [Refs. 1.4, 1.7]:

$$\text{sinc}(\omega) = \frac{\text{sen}(\pi\omega)}{\pi\omega} \quad (1.98)$$

$$\alpha(\omega) = 2B\omega_s \sum_{k=-\infty}^{\infty} \alpha(k\omega_s) \text{sinc}[2B(\omega - k\omega_s)] , \quad (1.99)$$

onde ω_s é o período de amostragem e B é a largura de banda do filtro passa-baixa destinado a integrar a função amostrada. Se W é a largura de banda do sinal amostrado, então:

$$W \leq B \leq T_s - W \quad (1.100)$$

$$T_s = \frac{2\pi}{\omega_s} \geq 2W \quad (1.101)$$

A Eq. (1.101) é o critério de Nyquist para a amostragem de um sinal. Usando a Eq. (1.99), o número médio de fótons fica dado por:

$$\begin{aligned} \int_0^\infty |\alpha(\omega)|^2 d\omega &= \sum_{k=-\infty}^\infty |\alpha(k\omega_s)|^2 \omega_s + \\ &+ (2B\omega_s)^2 \sum_{n=-\infty}^\infty \sum_{\substack{m=-\infty \\ m \neq n}}^\infty \alpha(n\omega_s) \alpha^*(m\omega_s) \int_0^\infty \text{sinc}[2B(\omega - n\omega_s)] \text{sinc}[2B(\omega - m\omega_s)] d\omega \end{aligned} \quad (1.102)$$

O último termo de (1.102) é devido à função *sinc* não obedecer a condição de ortonormalidade (Eq. (1.14)) mas esta pode ser bem aproximada se a função *sinc* for suficientemente estreita, isto é, se B for suficientemente grande. Com esta condição sobre B satisfeita, a Eq. (1.102) se resume a:

$$\int_0^\infty |\alpha(\omega)|^2 d\omega \cong \sum_{k=-\infty}^\infty |\alpha(k\omega_s)|^2 \omega_s \quad (1.103)$$

Comparando a Eq. (1.103) com o somatório da Eq. (1.60) temos que:

$$\alpha_i = \alpha(i\omega_s) \sqrt{\omega_s} \quad (1.104)$$

A Eq. (1.104) nos diz que o número de osciladores discretos a ser considerado no campo contínuo é igual ao número de amostras tomadas da envoltória. Agora que determinamos os α_i podemos encontrar as estatísticas de número de fótons e da fase do estado contínuo, a partir das estatísticas de cada oscilador individual, Eqs. (1.88) e (1.91). Se temos k amostras da envoltória do pulso, então a função densidade de probabilidade (FDP) do número de fótons do campo contínuo é dado por :

$$FDP(N) = FDP\left(\sum_{i=1}^k n_i\right) \quad (1.105)$$

onde, mais uma vez, n_i é o número de fótons do i -ésimo oscilador discreto que tem FDP, dependente de α_i , dada pela Eq. (1.88). A FDP da fase do campo contínuo é mais complicada; optamos por escolher um modelo analítico onde, se todos os osciladores individuais têm a mesma fase média, $\arg(\alpha_i) = \arg(\alpha_j)$ para todo i e j , então a fase média do contínuo será a mesma, $\arg(\alpha_i)$. Com esta condição, a FDP escolhida para a fase do campo contínuo é:

$$FDP(\theta) = \sum_{i=1}^k \frac{|\alpha_i|^2}{\langle N \rangle} FDP(\theta_i) , \quad (1.106)$$

ou seja, uma soma ponderada das FDP's individuais onde o oscilador individual que tiver maior número médio de fótons terá maior peso na soma. Faremos, agora, uma simulação das FDP's para a envoltória dada pelas Eqs. (1.95) - (1.97) com $\langle N \rangle = 16$, $\phi = 60^\circ$, $T_0 = 5$ ps e $\omega_0 = 2\pi(1,58061e14)$ rad/s. A Fig. 1.5 mostra a forma do pulso no domínio da frequência.

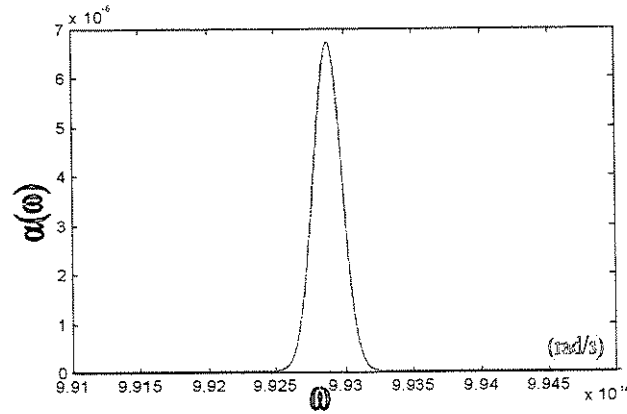


Fig. 1.5 - Pulso inicial no domínio da frequência.

Serão usados 100 osciladores individuais, implicando que foram tomadas 100 amostras da envoltória. O período de amostragem é dado por:

$$\omega_s = \frac{(\omega_{max} - \omega_{min})}{N_{osc} - 1} , \quad (1.107)$$

sendo N_{osc} o número de osciladores individuais, ω_{max} e ω_{min} são os limites superior e inferior da janela espectral. As Figs. 1.6 e 1.7 mostram as FDP's do número de fótons e da fase para o campo contínuo mostrado na Fig. 1.5.

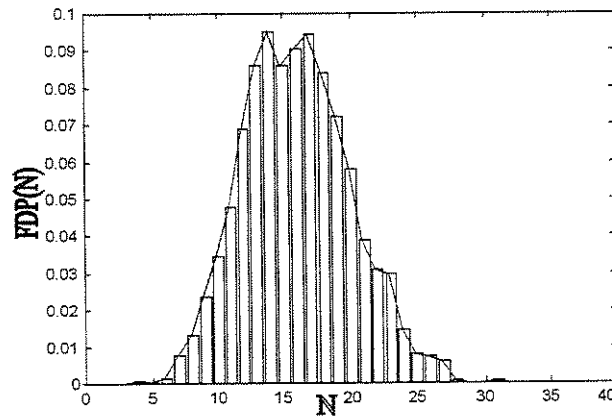


Fig. 1.6 - FDP do número de fótons.

A curva da Fig. 1.6 foi obtida numericamente [Eq.(1.105)] usando a frequência relativa dos resultados da soma do número de fótons de cada oscilador (2500 resultados). O número médio de fótons obtido com a Fig. 1.6 é $\langle N \rangle = 16,0240$, enquanto que a variância é $(\Delta N)^2 = 16,5162$. Estes valores estão de acordo com o esperado para um estado coerente com $\langle N \rangle = 16$.

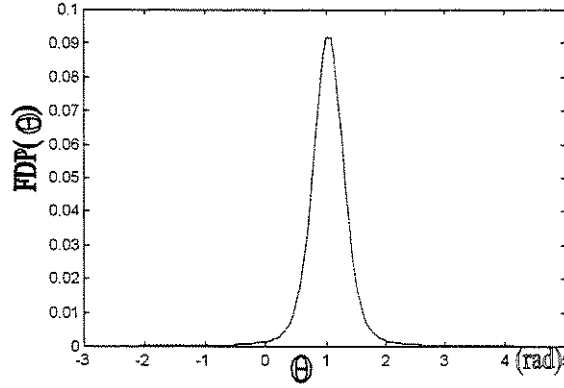


Fig. 1.7 - FDP da fase.

Com a distribuição da Fig. 1.7 [Eq. (1.106)] temos que o valor médio da fase é $\langle \theta \rangle = 59,9658^\circ$, muito próximo ao valor de 60° esperado, e o desvio padrão $\Delta\theta = 23.6930^\circ$. A fase de referência tomada para todos os osciladores individuais foi $\theta_0 = -120^\circ$, referente à mínima variância. Neste ponto estamos aptos a determinar as estatísticas de número de fótons e da fase do campo contínuo a partir da forma do pulso. Assim, propagaremos o pulso através da fibra óptica segundo as equações clássicas de propagação e determinaremos as estatísticas do número de fótons e da fase do pulso de saída através do método acima exposto. A propagação do pulso na fibra óptica em regime linear é regida por [Ref. 1.1]:

$$i \frac{\partial \alpha(z, t)}{\partial z} + \beta \frac{\partial \alpha(z, t)}{\partial t} + \frac{\beta_2}{2} \frac{\partial^2 \alpha(z, t)}{\partial t^2} - \frac{\beta_3}{6} \frac{\partial^3 \alpha(z, t)}{\partial t^3} + i \sigma \alpha(z, t) = 0 \quad , \quad (1.107)$$

onde β_2 é a dispersão de velocidade de grupo, β_3 a dispersão de terceira ordem e σ representa a perda. A solução, no domínio da frequência, da Eq. (1.107) é:

$$\alpha(z, \omega) = \alpha(z = 0, \omega) \exp \left(i \beta z + \frac{i \beta_2 \omega^2 z}{2} - \frac{i \beta_3 \omega^3 z}{6} \right) \exp \left(\frac{-\sigma z}{2} \right) . \quad (1.108)$$

Usando a Eq. (1.108) podemos determinar as estatísticas de número de fótons e da fase em qualquer posição da fibra. Como a amplitude do campo decai exponencialmente, também é esperado um decréscimo exponencial do número médio de fótons ao longo da propagação. Além disso, o campo sofre um deslocamento linear de fase, βL , onde L é a distância percorrida na fibra, que não será considerado nas simulações por representar apenas uma adição à fase média, e um gorjeio que deve atuar fortemente na FDP da fase. A seguir, mostramos as simulações para uma fibra de 10 km com o pulso de entrada mostrado na Fig. 1.5. Os parâmetros das simulações, bem como os valores médios e variâncias do número de fótons e os valores médios e desvios padrões da fase, são apresentados na Tabela 1.1.

SIM	β_2 [ps ² /km]	β_3 [ps ³ /km]	σ [dB/km]	$\langle N \rangle$	$(\Delta N)^2$	$\langle \theta \rangle$	$\Delta \theta$
1	20	0	0	15,9336	16,0364	-27,2019°	68,7930°
2	0	0,1	0	(-)	(-)	-5,7883°	75,1142°
3	0	0	0,3	8,0728	8,0771	59,9229°	34,1614°
4	20	0	0,3	7,9784	7,7371	27,0983°	71,5626°
$L=10$ km, $\langle N \rangle = 16$, $\phi = 60^\circ$, $T_0 = 5$ ps, $\omega_0 = 2\pi(1,58061e14)$ rad/s. (-) não realizada							

Tabela 1.1 - Parâmetros usados nas simulações das FDPs de número de fótons e da fase.

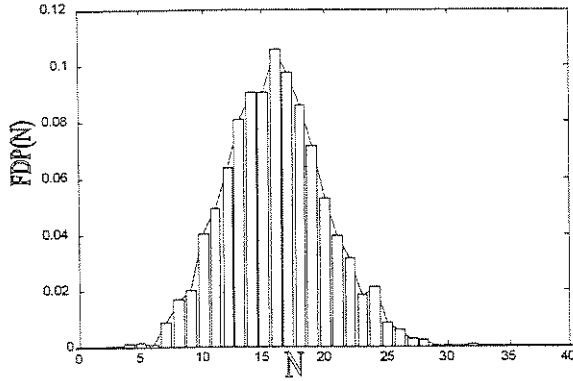


Fig. 1.8 - FDP do número de fótons. (SIM-1)

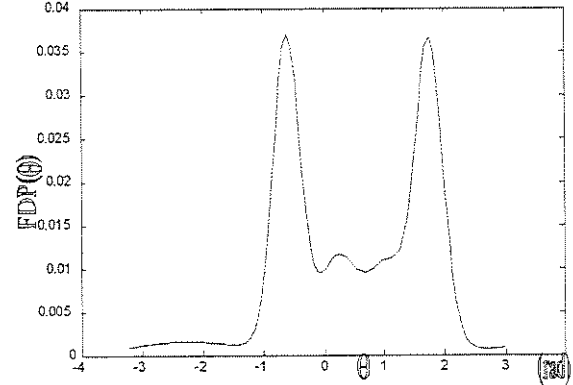


Fig. 1.9 - FDP da fase. (SIM-1)

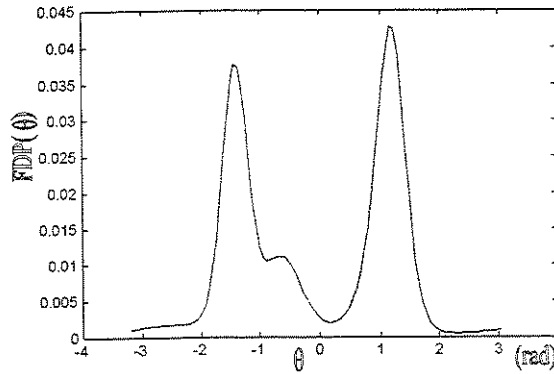


Fig. 1.10 - FDP da fase. (SIM-2)

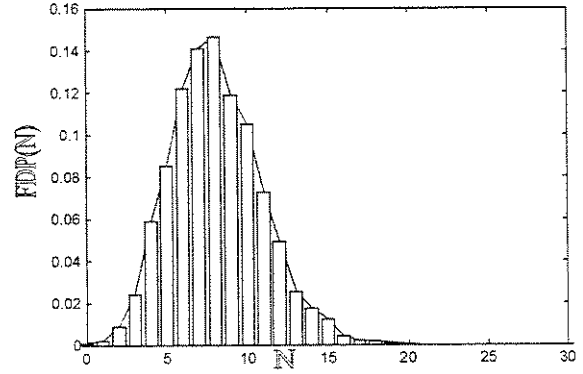


Fig. 1.11 - FDP do número de fótons. (SIM-3)

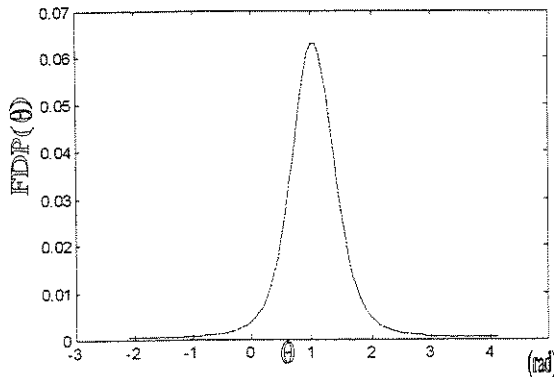


Fig. 1.12 - FDP da fase. (SIM-3)

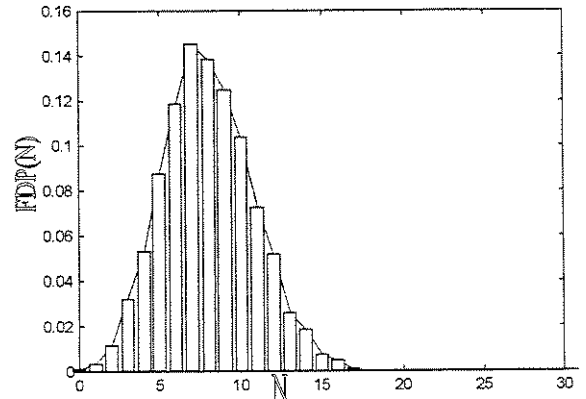


Fig. 1.13- FDP do número de fótons. (SIM-4)

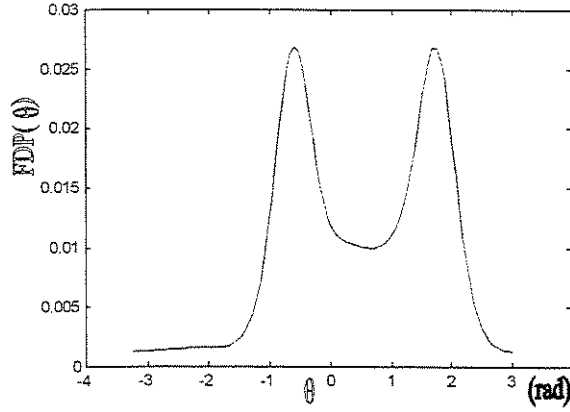


Fig. 1.14 - FDP da fase. (SIM-4)

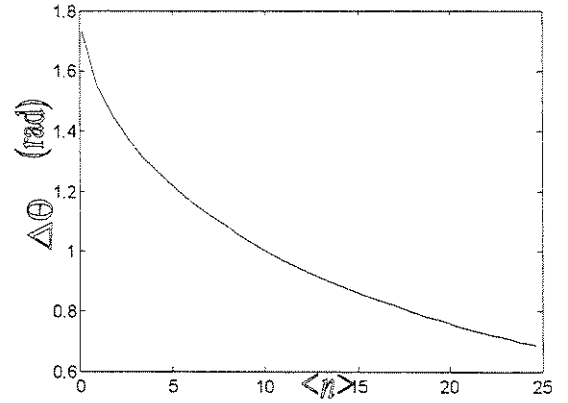


Fig. 1.15 Desvio padrão da fase.

Observando os resultados na Tabela 1.1 e as Figs. 1.8 - 1.14, podemos ver que a dispersão não afeta a distribuição do número de fótons, embora ela tenha forte influencia na distribuição da fase. Isto é devido ao gorjeio sofrido pelo pulso ao se propagar pela fibra. Em particular, vemos, na Figs. 1.9, 1.10 e 1.14, que a dispersão causou uma divisão na forma da curva da distribuição de fase provocando o aparecimento de picos. Na Fig. 1.9, os picos ocorrem em $\theta = -34,5734^\circ$ e $\theta = 100,8722^\circ$, e na Fig. 1.10 eles ocorrem em $\theta = 67,0917^\circ$ e $\theta = -82,6113^\circ$. Por outro lado, a perda causa um decaimento exponencial do número médio de fótons do pulso. Além disso, ela também provoca um aumento da variância da fase, como é esperado, uma vez que a variância do número de fótons diminui a medida que o número médio de fótons diminui. Isto pode ser observado na Fig. 1.15, que mostra o desvio padrão da fase pelo número médio de fótons, usando $T_0 = 30$ ps.

Como anteriormente afirmado, após o pulso se propagar pela fibra com perda é esperado que o número médio de fótons do estado coerente decaia exponencialmente. De fato, temos que:

$$\langle N \rangle_{z=L} = \langle N \rangle_{z=0} \exp(-\sigma L) = 16 \exp(-0.069 \cdot 10) = 8,0252 \quad , \quad (1.109)$$

o que está de acordo com o valor obtido com a FDP da Fig. 1.11. Consideraremos, agora, os efeitos da perda através de um modelo estatístico. Neste modelo, a probabilidade de um fóton sobreviver durante um intervalo de tempo τ é dada por [Ref. 1.3]:

$$p(\tau) = \exp\left(\frac{-\tau}{T_R}\right) \quad , \quad (1.110)$$

onde T_R é o tempo de relaxação. Obviamente, a probabilidade do fóton ser absorvido no mesmo intervalo de tempo é $q(\tau) = 1 - p(\tau)$. A probabilidade de, tendo começado com n fótons, após o intervalo τ restarem n_1 fótons, é dada pela distribuição binomial [Ref 1.3]:

$$p_c(n_1|n) = \frac{n! [p(\tau)]^{n_1} [1 - p(\tau)]^{n-n_1}}{n_1! (n - n_1)!} \quad . \quad (1.111)$$

Se um estado coerente é enviado por uma fibra óptica, de comprimento L , com perda, então a probabilidade de haver n_1 fótons no estado que chega ao final da fibra é:

$$p_L(n_1) = \sum_{n=n_1}^{\infty} p_c(n_1|n) p_\alpha(n) \quad , \quad (1.112)$$

onde $p_\alpha(n)$ é a probabilidade do estado coerente no início da fibra ter n fótons. Para que o número médio de fótons decaia exponencialmente, devemos ter no final da fibra:

$$\sum_{m=0}^{\infty} m \left(\sum_{n=m}^{\infty} p_c(m|n) p_\alpha(n) \right) = \sum_{m=0}^{\infty} m p_\alpha(m) \exp(-\sigma L) \quad . \quad (1.113)$$

Usando as Eqs. (1.110) e (1.111) na Eq. (1.113), obtemos:

$$\sum_{m=0}^{\infty} m \left\{ \sum_{n=m}^{\infty} \left\{ \frac{n!}{m!(n-m)!} \left[\exp\left(\frac{-\tau}{T_R}\right) \right]^m \left[1 - \exp\left(\frac{-\tau}{T_R}\right) \right]^{n-m} p_\alpha(n) \right\} - p_\alpha(m) \exp(-\sigma L) \right\} = 0 \quad . (1.114)$$

Trabalhando com (1.114) encontramos a condição:

$$\frac{\tau}{T_R} = \sigma L \Rightarrow T_R = \frac{1}{V_g \sigma} \quad , \quad (1.115)$$

onde a relação $\tau = L/V_g$, sendo V_g a velocidade de grupo, foi usada na obtenção da Eq. (1.115). A Fig. 1.16, a seguir, mostra as FDPs do número de fótons, para uma simulação com perdas, usando os modelos estatístico e o da exponencial decrescente.

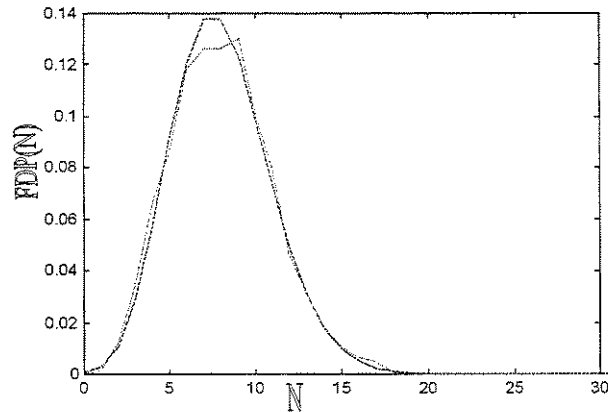


Fig. 1.16 - FDPs do número de fótons. Modelo estatístico linha contínua e modelo da exponencial decrescente linha tracejada. (SIM-3)

A Fig. 1.16 mostra uma boa concordância entre os dois modelos; entretanto, quando o número médio de fótons se torna muito pequeno, $\langle N \rangle \ll 1$, as diferenças são mais

pronunciadas. Os números médios de fótons são 8,0595 para o modelo da exponencial decrescente e 8,0373 para o modelo estatístico.

Por fim, em uma simulação não apresentada, um pulso com $\langle N \rangle = 0,1$ e $T_0 = 30$ ps, após se propagar por uma fibra de 30 km, com perda de 0,3 dB/km, apresentou, na saída da fibra, $\langle N \rangle = 0,012$. Assim, a aproximadamente cada 100 intervalos de pulsos, 1 contém um fóton e, portanto, uma taxa de 1 MHz, por exemplo, é transformada numa taxa de 10 kHz. Este fato parece ser desanimador, pois ele indica que a taxa de transmissão de bits em criptografia quântica é muito baixa. Vale ressaltar, no entanto, que a comunicação quântica só se dá durante a troca dos bits da chave. Após isso, a comunicação volta a se utilizar de pulsos "normais". Esta baixa taxa de transmissão é devida, por exemplo, a fonte utilizada para gerar luz de um fóton: um laser fortemente atenuado. Com o desenvolvimento de fontes que gerem luz realmente no estado de número, esta situação tende a melhorar.

Analisaremos, agora, o interferômetro a fibra que é o dispositivo responsável pela transmissão da informação quântica do transmissor ao receptor em sistemas de criptografia quântica. A Fig. 1.17 mostra o diagrama de um interferômetro a fibra [Refs. 1.8, 1.9]. O funcionamento deste interferômetro é descrito no Apêndice C. Ele é dividido em duas partes, uma pertencente ao transmissor e a outra pertencente ao receptor. Cada parte possui um modulador de fase em um dos braços. Os tempos de propagação, t_1 e t_2 , devem ser iguais nas duas partes do interferômetro. Todos os divisores de feixe são iguais e possuem coeficientes de transmissão $T = 1/\sqrt{2}$ e de reflexão $R = i/\sqrt{2}$.

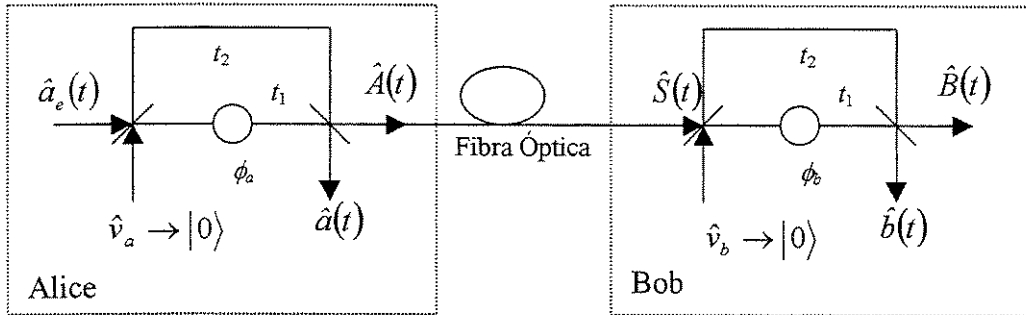


Fig. 1.17 - Interferômetro a fibra para criptografia quântica

O operador aniquilação, na saída de Alice, é dado por [Ref 1.8]:

$$\hat{A}(t) = T^2 \exp(i\phi_a) \hat{a}_e(t - t_1) + R^2 \hat{a}_e(t - t_2) + RT [\exp(i\phi_a) \hat{v}_a(t - t_1) + \hat{v}_a(t - t_2)] . \quad (1.116)$$

O estado coerente na saída de Alice, no domínio da frequência e com o estado vácuo na entrada $\hat{v}_a$, é:

$$|\alpha_A(\omega)\rangle = \exp \left(\int [\alpha_A(\omega) \hat{A}^\dagger(\omega) - \alpha_A^*(\omega) \hat{A}(\omega)] d\omega \right) |0\rangle \quad (1.117)$$

$$\alpha_A(\omega) = [T^2 \exp(i\phi_a) \exp(-i\omega t_1) + R^2 \exp(-i\omega t_2)] \alpha_e(\omega) . \quad (1.118)$$

Trabalhando com a Eq. (1.118), chegamos a:

$$\alpha_A(\omega) = \text{sen}\left[\frac{\phi_a - \omega(t_1 - t_2)}{2}\right] \exp\left(i\frac{\phi_a - \omega(t_1 + t_2) + \pi}{2}\right) \alpha_e(\omega) . \quad (1.119)$$

A Eq. (1.119) é a envoltória do sinal na entrada da fibra. Na saída da fibra de comprimento L , temos:

$$\alpha_s(\omega) = \alpha_A(\omega) \exp\left[i\left(\beta L + \frac{\beta_2 \omega^2 L}{2} - \frac{\beta_3 \omega^3 L}{6}\right)\right] \exp\left(\frac{-\sigma L}{2}\right) . \quad (1.120)$$

Este é o sinal que chega em Bob. O operador aniquilação na saída B de Bob é dado por:

$$\hat{B}(t) = T^2 \exp(i\phi_b) \hat{S}(t - t_1) + R^2 \hat{S}(t - t_2) + RT[\exp(i\phi_b) \hat{v}_b(t - t_1) + \hat{v}_b(t - t_2)] . \quad (1.121)$$

O estado coerente na saída B de Bob, no domínio da frequência e com o estado vácuo na entrada $\hat{v}_b$, é:

$$|\alpha_B(\omega)\rangle = \exp\left(\int [\alpha_B(\omega) \hat{B}^+(\omega) - \alpha_B^*(\omega) \hat{B}(\omega)] d\omega\right) |0\rangle , \quad (1.122)$$

onde

$$\alpha_B(\omega) = \text{sen}\left[\frac{\phi_b - \omega(t_1 - t_2)}{2}\right] \exp\left(i\frac{\phi_b - \omega(t_1 + t_2) + \pi}{2}\right) \alpha_s(\omega) . \quad (1.123)$$

Substituindo (1.119) em (1.120), e esta em (1.123), obtemos:

$$\begin{aligned} \alpha_B(\omega) = & \left\{ \frac{1}{2} \cos\left[\frac{(\phi_b - \phi_a)}{2}\right] - \frac{1}{2} \cos\left[\frac{\phi_b + \phi_a - 2\omega(t_1 - t_2)}{2}\right] \right\} \exp\left(-\frac{\sigma}{2} L\right) \\ & \exp\left[i\left(\frac{\phi_a - \omega(t_1 + t_2) + \pi}{2} + \frac{\phi_b - \omega(t_1 + t_2) + \pi}{2} + \beta L + \frac{\beta_2 \omega^2 L}{2} - \frac{\beta_3 \omega^3 L}{6}\right)\right] \alpha_e(\omega) \end{aligned} \quad (1.124)$$

que expandida dá:

$$\begin{aligned} \alpha_B(\omega) = & \frac{1}{2} \cos\left[\frac{(\phi_b - \phi_a)}{2}\right] \exp[\Psi(\omega)] \alpha_e(\omega) + \\ & \frac{1}{2} \exp\left(\Psi(\omega) + \frac{-i(\phi_a + \phi_b)}{2}\right) \alpha_e(\omega) \exp[i\omega(t_1 - t_2)] + \\ & \frac{1}{2} \exp\left(\Psi(\omega) + \frac{i(\phi_a + \phi_b)}{2}\right) \alpha_e(\omega) \exp[-i\omega(t_1 - t_2)] , \end{aligned} \quad (1.125)$$

onde

$$\Psi(\omega) = -\frac{\sigma}{2}L + i \left(\frac{\phi_a - \omega(t_1 + t_2) + \pi}{2} + \frac{\phi_b - \omega(t_1 + t_2) + \pi}{2} + \beta L + \frac{\beta_2 \omega^2 L}{2} - \frac{\beta_3 \omega^3 L}{6} \right). \quad (1.126)$$

Tomando a transformada de Fourier inversa da Eq. (1.125), observamos a presença de 3 pulsos. O primeiro termo, correspondendo ao pulso central, ocorre em t e é onde se dá a interferência. O segundo termo é referente ao pulso que chega em Bob no tempo $t+(t_1-t_2)$ e o terceiro termo referente ao pulso que aparece em Bob em $t-(t_1-t_2)$. Estes dois pulsos não têm importância no protocolo de obtenção da chave e podem ser evitados fazendo-se uso da polarização, como mostrado na Fig. E5 do Apêndice C. Trabalhando de forma semelhante, encontramos que a segunda saída de Bob é:

$$\alpha_b(\omega) = \left\{ \frac{1}{2} \sin \left[\frac{(\phi_a - \phi_b)}{2} \right] + \frac{1}{2} \sin \left[\frac{\phi_b + \phi_a - 2\omega(t_1 - t_2)}{2} \right] \right\} \exp \left(-\frac{\sigma}{2} \right) \exp \left[i \left(\frac{\pi}{2} + \frac{\phi_a - \omega(t_1 + t_2) + \pi}{2} + \frac{\phi_b - \omega(t_1 + t_2) - \pi}{2} + \beta L + \frac{\beta_2 \omega^2 L}{2} - \frac{\beta_3 \omega^3 L}{6} \right) \right] \alpha_e(\omega). \quad (1.127)$$

Uma simulação numérica do interferômetro foi realizada. Injetamos 500 pulsos de largura $T_0 = 30$ ps e $\langle N \rangle = 0,1$ na entrada de um interferômetro de 30 km, com perdas de 0,3 dB/km, e calculamos o número médio de fótons nas saídas de Bob, $\langle N_b \rangle$ e $\langle N_B \rangle$, para cada pulso injetado. Os moduladores ϕ_a e ϕ_b receberam, aleatoriamente, os valores $0, \pi, \pi/2$ e $3\pi/2$, os dois primeiros correspondendo à primeira base e os dois últimos correspondendo à segunda base do protocolo BB84, descrito no Apêndice C. A Fig. 1.18 mostra a escolha aleatória das fases.

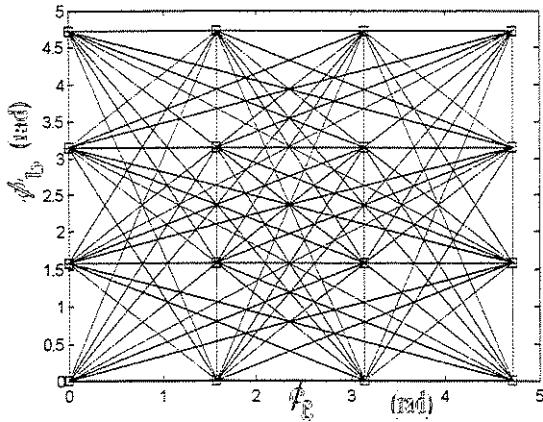


Fig. 1.18 - Escolha aleatória das fases para simulação do interferômetro da Fig. 1.16.

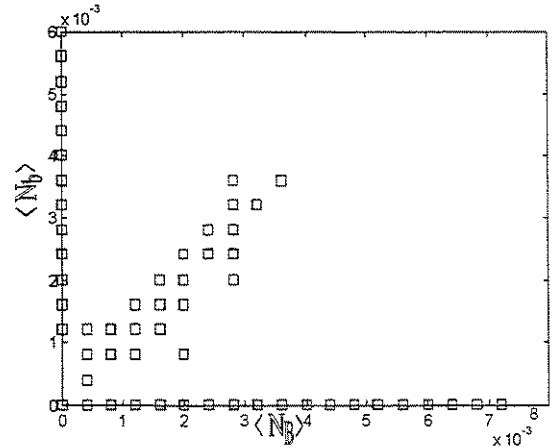


Fig. 1.19 - Valores médios do número de fótons nas saídas de Bob.

A Fig. 1.19 apresenta os valores médios do número de fótons nas saídas de Bob. As marcações sobre os eixos são referentes aos instantes em que Alice e Bob escolheram a mesma base, tornando nulo o número médio de fótons em uma das saídas de Bob. As

demais marcações são referentes aos instantes em que Alice e Bob escolheram bases diferentes. O número médio de fótons em ambas as saídas de Bob, para os 500 pulsos, é $\langle N_B \rangle = \langle N_b \rangle = 0,0016$. Calculando analiticamente o número médio de fótons em ambas as saídas de Bob, temos: Para um pulso entrando em Alice com $\langle N \rangle = 0,1$, aparecerão, na saída de Alice, dois pulsos espacialmente separados, com $\langle N_A \rangle = 0,025$. Após a propagação na fibra, cada pulso alcança Bob com $\langle N_f \rangle = 0,0032$. Quando Bob usar a mesma base que Alice ele obterá, para o número médio de fótons em suas saídas, os valores 0,0032 e 0. Quando Bob usar uma base diferente da usada por Alice ele obterá, para o número médio de fótons em suas saídas, o valor 0,0016 em ambas as saídas. Desta forma, o número médio de fótons nas saídas de Bob, para 500 pulsos injetados em Alice e escolha equiprovável das bases, é:

$$\langle N_B \rangle = \langle N_b \rangle = \frac{125(0) + 125(0,0032) + 250(0,0016)}{500} = 0,0016 \quad , \quad (1.128)$$

que é o mesmo valor obtido pela simulação numérica apresentada na Fig. 1.19. A probabilidade de Bob obter uma contagem em seus detetores é:

$$p_B = 1 - \exp(-\eta \langle N_B \rangle) = p_b = 1 - \exp(-\eta \langle N_b \rangle) = 5,5984e-4 \quad , \quad (1.129)$$

onde η é a eficiência quântica do detetor, suposta igual a 0,35. Portanto, a probabilidade de Alice e Bob obterem um bit da chave, em 500 pulsos, é $0,5[p_B(1-p_b) + p_b(1-p_B)] = 5,5953e-4$. Uma contagem em ambas as saídas de Bob, que é uma das fontes de erros em criptografia quântica, para os 500 pulsos, ocorre com probabilidade $p_B p_b = 3,1342e-7$. Ainda na Fig. 1.19, podemos observar a variação do número médio de fótons na saída de Bob. Na prática, esta flutuação realmente acontece, pois o número médio de fótons, dos pulsos que saem de Alice, variam devido ao caráter estatístico da absorção realizada para aproximar o estado coerente do estado de número de um fóton. Uma análise mais acurada do desempenho de sistemas de criptografia quântica deve considerar estas flutuações. Por fim, usando o valor médio do número de fótons encontrado nas saídas de Bob, por pulso enviado por Alice, encontramos que, para obter um bit da chave com probabilidade 1, Alice deve enviar para Bob aproximadamente 1780 pulsos. Se Alice os envia em uma taxa de 1 MHz, então, Alice e Bob obterão os bits da chave em uma taxa de aproximadamente 562 bps.

CONCLUSÕES DO CAPÍTULO I

Utilizando os já conhecidos conceitos de discretização de modos contínuos e a definição de um operador fase Hermitiano em um espaço de dimensão finita (operador de Pegg-Barnnet), descrevemos um método para o cálculo das funções densidade de probabilidade do número de fótons e da fase, a partir da envoltória de um pulso de luz coerente. Com este método determinamos as estatísticas de número de fótons e da fase na saída de dispositivos ópticos passivos e lineares, como fibras ópticas, atenuadores e divisores de feixes, usando a envoltória do pulso incidente no dispositivo e as equações clássicas de propagação através dos mesmos. O método consiste em:

1 - Aproximar o estado coerente contínuo por um produto tensorial finito de osciladores individuais no estado coerente.

2 - Amostrar a envoltória do pulso coerente tal que o número de amostras seja igual ao número de osciladores individuais. A cada amostra corresponde um oscilador individual com amplitude igual ao produto do valor da amostra pela raiz quadrada do período de amostragem:

$$|\alpha(\omega)\rangle = |\alpha(\omega_s)\sqrt{\omega_s}\rangle |\alpha(2\omega_s)\sqrt{\omega_s}\rangle \cdots |\alpha(i\omega_s)\sqrt{\omega_s}\rangle \cdots |\alpha(k\omega_s)\sqrt{\omega_s}\rangle \quad (1.130)$$

onde k é o número de amostras tiradas de $\alpha(\omega)$ e ω_s é o período de amostragem.

3 - A função densidade de probabilidade, FDP, do número de fótons do pulso no estado coerente contínuo é igual à distribuição de probabilidade da soma do número de fótons de cada oscilador individual:

$$FDP(N) = FDP\left(\sum_{i=1}^k n_i\right) \quad (1.131)$$

sendo n_i é o número de fótons do i -ésimo oscilador individual.

4 - A função densidade de probabilidade da fase do pulso no estado coerente contínuo é dada por:

$$FDP(\theta) = \sum_{i=1}^k \frac{|\alpha(i\omega_s)|^2 \omega_s}{\langle N \rangle} FDP(\theta_i) \quad (1.132)$$

sendo $FDP(\theta_i)$ a distribuição da fase do i -ésimo oscilador individual.

Nas simulações realizadas, os resultados das FDPs do número de fótons se mostraram coerentes e confiáveis. Quando da consideração de perdas, pelo método da exponencial decrescente e pelo modelo estatístico, as FDPs do número de fótons foram bem semelhantes e, como esperado, o número médio de fótons, em ambos os métodos, decaiu exponencialmente. Por outro lado, os resultados das FDPs da fase foram de difícil conceituação. Observamos, como pontos positivos, que: 1) Quando todos os osciladores individuais têm a mesma fase média, a fase média do pulso coerente é igual à fase média dos osciladores individuais; 2) - Quando o número médio de fótons do estado coerente diminui (e portanto a incerteza do número de fótons diminui) a variância (incerteza) da fase aumenta.

Portanto, podemos afirmar que a Eq. (1.131) representa bem o número de fótons do pulso coerente. Por outro lado, quando o pulso sofre um gorjeio devido, por exemplo, à propagação do pulso numa fibra óptica com dispersão, a distribuição de probabilidade da fase assume formas complexas e nada podemos inferir. Portanto, não podemos afirmar que a Eq. (1.132) represente bem a fase do pulso coerente.

Uma simulação numérica do protocolo BB84, num interferômetro a fibra, foi realizada. Os resultados numéricos para os valores médios do número de fótons, nas saídas de Bob, concordaram com os valores analíticos calculados para as mesmas condições, mostrando a confiabilidade do método empregado. Em particular, a simulação numérica fornece, devido a caráter estatístico da mesma, uma flutuação no número médio de fótons nas saídas de Bob. Esta flutuação pode ser usada na determinação mais acurada do desempenho de sistemas de criptografia quântica.

CAPÍTULO II

MATRIZ DENSIDADE E MATRIZ COERÊNCIA EM COMUNICAÇÃO QUÂNTICA

2.1 Introdução

A matriz coerência, J , representa as autocorrelações e correlações cruzadas das componentes transversais do campo eletromagnético. A polarização da luz, e suas variações ao atravessar dispositivos ópticos, pode ser completamente caracterizada através de J [Apêndice E]. Por outro lado, a matriz densidade, ρ , contém toda a informação disponível sobre um determinado estado quântico [Apêndices A e F]. As semelhanças entre J e ρ são grandes, em particular, quando o estado quântico em questão é a polarização, as duas são iguais. Estas semelhanças estimulam a aplicação de conceitos comuns de uma na outra. Assim, na primeira parte deste capítulo, usando a matriz coerência para tratar um sistema quântico polarimétrico, apresentamos as probabilidades dos resultados das medidas, as medidas de distâncias e a correção da variação da polarização através do uso de um equalizador óptico. Na segunda parte, realizamos a separação da matriz densidade (2x2) na soma de duas outras, uma representando um estado maximamente misto e a outra representando um estado puro, tal como é feito com a matriz coerência. Definimos, então, o grau de pureza, g_p , da matriz densidade, equivalente ao grau de polarização para luz parcialmente polarizada. Verificamos, então, a dependência da entropia, distância de Kolmogorov, informação mútua, fidelidade e estados entrelaçados, com g_p .

2.2 Matrizes Densidade e Coerência em Comunicação Polarimétrica

A polarização da luz tem sido usada como portadora de informação em comunicações quânticas. Ela tem como vantagem não ser uma variável dependente do número de fótons e, por isso, não é influenciada pelas perdas na fibra óptica. Por outro lado, é dependente de diversos fatores, como forma e composição do núcleo, emendas, tensões mecânicas (curvaturas e vibrações) e temperatura, dentre outros. Como resultado, para que o processo de comunicação seja eficiente, um controle rigoroso da polarização deve ser feito, inclusive com o uso de fibras especiais que mantêm a polarização fixa [Ref. 2.1]. Visando dispensar o uso destas fibras especiais, que são de custo elevado, analisaremos a viabilidade do desenvolvimento e uso de um equalizador óptico, capaz de compensar as variações da polarização do sinal ao longo do percurso percorrido pelo mesmo até a sua chegada no receptor, segundo os modelos estatísticos adotados para a variação da polarização na fibra óptica [Refs. 2.1, 2.2]. Para isso, usaremos as ferramentas clássicas descritas no Apêndice E para caracterizar e processar os estados quânticos de polarização. O uso de ferramentas clássicas, para tratar estados quânticos de polarização, é possível devido à grande semelhança entre as matrizes coerência, J , e densidade de estados, ρ [Ref. 2.3]. O pulso de luz a ser considerado é suposto ter apenas um fóton e, por isso, para que os resultados clássicos tenham a interpretação probabilística da mecânica quântica, a seguinte condição deve ser obedecida:

$$S_0 = \text{Tr}(J) = 1 . \quad (2.1)$$

2.2.1 Probabilidades dos Resultados de Medições de Polarização com Matriz Coerência (J) e Vetor de Stokes (S)

O estado quântico $|\theta\rangle$, representando uma luz linearmente polarizada, de ângulo θ com o eixo horizontal, é representado pelo vetor de Stokes $S(\theta)$ e/ou matriz coerência $J(\theta)$. O estado $|\theta\rangle$ é obtido através da rotação do estado horizontal, $|0^\circ\rangle$ ou $|H\rangle$, de θ . A matriz coerência, referente ao estado $|\theta\rangle$, é [Apêndice E]:

$$J(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} = \begin{bmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & \sin^2(\theta) \end{bmatrix} . \quad (2.2)$$

O vetor de Stokes, para este mesmo estado, é [Apêndice E]:

$$S(\theta) = [1 \quad \cos(2\theta) \quad \sin(2\theta) \quad 0]^T . \quad (2.3)$$

Obviamente, para polarização linear, temos $S_3 = 0$. É fácil verificar que o produto escalar de dois vetores de Stokes, representando estados de polarização linear, é dado por:

$$S'(\theta) \cdot S'(\varphi) = \cos[2(\theta - \varphi)] , \quad (2.4)$$

onde S' é o vetor de Stokes sem o primeiro elemento, S_0 . Observando a Eq. (2.3) vemos que os estados separados de ϕ são representados, na esfera de Poincaré, por vetores de Stokes separados por 2ϕ , portanto, estados ortogonais são representados por vetores diametralmente opostos na esfera de Poincaré.

Medir o estado de polarização de um feixe, representado por $J(\theta)$, usando um polarizador representado pela matriz transferência $P(\varphi)$, equivale a decompor o estado da luz incidente nos autoestados V_1 e V_2 de $P(\varphi)$, os quais possuem autovalores 1 e 0, respectivamente [Ref. 2.4]. Desta forma, expandindo o estado polarizado $|\theta\rangle$, temos:

$$\begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix} = aV_1(\varphi) + bV_2(\varphi) = a \begin{bmatrix} \cos(\varphi) \\ \sin(\varphi) \end{bmatrix} + b \begin{bmatrix} -\sin(\varphi) \\ \cos(\varphi) \end{bmatrix} , \quad (2.5)$$

onde a e b são reais, pois só usaremos polarização linear. Igualando a matriz coerência do estado da Eq. (2.5) com $J(\theta)$, encontramos que:

$$a^2 + b^2 = 1 \quad (2.6)$$

$$a^2 = \frac{1}{2} \{1 + \cos[2(\varphi - \theta)]\} = \frac{1}{2} [1 + S'(\varphi) \cdot S'(\theta)] . \quad (2.7)$$

Como o pulso de luz é de um fóton, a^2 é a probabilidade do fóton emergir do polarizador no autoestado V_1 e b^2 é a probabilidade do fóton emergir do polarizador no autoestado V_2 .

Quando o feixe de luz é parcialmente polarizado, o estado quântico correspondente é uma mistura de estados representada pela matriz densidade ρ [Apêndice A]. Esta mistura é representada por uma matriz coerência da forma:

$$J = \sum_n p_n J(\theta_n) \quad (2.8)$$

$$\sum_n p_n = 1, \quad (2.9)$$

sendo p_n a probabilidade da luz estar com ângulo de polarização θ_n . Medindo esta mistura de estados com o polarizador $P(\varphi)$, obtemos as probabilidades:

$$a^2 + b^2 = 1 \quad (2.10)$$

$$a^2 = \frac{1}{2} [1 + \langle \sin(2\varphi) \rangle \langle \sin(2\theta) \rangle + \langle \cos(2\varphi) \rangle \langle \cos(2\theta) \rangle] \quad (2.11)$$

$$\langle \sin(2\theta) \rangle = \sum_n p_n \sin(2\theta_n) \quad (2.12)$$

$$\langle \cos(2\theta) \rangle = \sqrt{1 - \langle \sin(2\theta) \rangle^2}. \quad (2.13)$$

Se, por exemplo, a polarização é uniformemente distribuída, isto é, todos os ângulos de polarização são equiprováveis, temos:

$$\langle \sin(2\theta) \rangle = \langle \cos(2\theta) \rangle = 0 \Rightarrow a^2 = \frac{1}{2} \quad (2.14)$$

como deve ser, para a luz totalmente despolarizada. Se medirmos, por exemplo, o estado misto:

$$\rho = \frac{1}{4} |0^\circ\rangle\langle 0^\circ| + \frac{3}{4} |45^\circ\rangle\langle 45^\circ| \quad (2.15)$$

com um polarizador $P(\varphi=0)$, a probabilidade do fóton emergir com polarização horizontal, segundo as Eqs. (2.11)-(2.13), é:

$$a^2 = \frac{1}{2} [1 + \langle \cos(2\theta) \rangle] = \frac{1}{2} \left[1 + \frac{1}{4} \cos(0^\circ) + \frac{3}{4} \cos(90^\circ) \right] = \frac{5}{8}. \quad (2.16)$$

Resolvendo pela mecânica quântica, temos:

$$\langle 0^\circ | \rho | 0^\circ \rangle = \langle 0^\circ | \frac{1}{4} |0^\circ\rangle\langle 0^\circ| + \frac{3}{4} |45^\circ\rangle\langle 45^\circ| | 0^\circ \rangle = \frac{1}{4} + \frac{3}{4} |\langle 0^\circ | 45^\circ \rangle|^2 = \frac{5}{8} \quad (2.17)$$

estando, portanto, os resultados em concordância. As probabilidades, dadas pelas Eqs. (2.10)-(2.11) em termos dos elementos de J e S , são:

$$a^2 = \frac{1}{2} \frac{\text{Tr}(J_{np})}{\text{Tr}(J)} + \frac{1}{2} \left[1 + \frac{1}{S_0^p} S_p' \cdot S_m' \right] \frac{\text{Tr}(J_p)}{\text{Tr}(J)} \quad (2.18)$$

$$b^2 = 1 - a^2, \quad (2.19)$$

onde a matriz coerência da luz parcialmente polarizada, J , foi dividida nas matrizes referentes às partes totalmente polarizada, J_p , e totalmente despolarizada, J_{np} [Apêndice E]. S_p' é o vetor de Stokes referente à J_p , sem o primeiro elemento, e S_m' é o vetor de Stokes do medidor de polarização, também sem o primeiro elemento. Trabalhando a Eq. (2.18) obtemos:

$$a^2 = \frac{1}{2} [1 + S_p' \cdot S_m'] = \frac{1}{2} [1 + S' \cdot S_m'] \quad (2.20)$$

Comparando as Eqs. (2.7) e (2.20), vemos que, a probabilidade de um resultado de uma medição depende apenas das componentes da parte polarizada da luz. J_p e S_p não representam estados físicos reais pois, para eles, a condição (2.1) não é satisfeita. Além disso, como $|S_p| < 1$, o produto escalar na Eq. (2.20) estará no intervalo aberto $(-1, 1)$ e, portanto, a^2 nunca assumirá os valores 1 e 0, para qualquer que seja S_m (medidor); ou seja, se a luz é parcialmente polarizada (estado misto), independentemente da medição utilizada, nunca poderemos ter certeza de sua polarização, uma vez que as probabilidades 1 e 0 são proibidas.

2.2.2 Medidas de Distância entre Estados Quânticos de Polarização usando J e S .

É interessante, neste momento, encontrarmos medidas de distância entre matrizes coerências de forma a poder distingui-las. Para isso, usaremos as medidas de distância entre matrizes densidades apresentadas no Apêndice F. Sejam dois estados diferentes representados pelas matrizes coerências (vetores de Stokes) J_0 (S_0) e J_1 (S_1), ocorrendo com probabilidades *a priori* π_0 e π_1 , respectivamente. Seja também um polarizador, $P(\varphi)$, representado por J_m e S_m , e com autoestados dados na Eq. (2.5). Os resultados da medição dos estados J_0 e J_1 , pelo polarizador S_m , são mostrados na Tabela 2.1.

Estados Enviados	Estados Medidos: $E_1 = [\cos(\varphi) \sin(\varphi)]^T$ e $E_2 = [-\sin(\varphi) \cos(\varphi)]^T$	
	$p(E_1)$	$p(E_2)$
J_0 (π_0)	$p(E_1 J_0) = \frac{1}{2} [1 + S_0' \cdot S_m']$	$p(E_2 J_0) = \frac{1}{2} [1 - S_0' \cdot S_m']$
J_1 (π_1)	$p(E_1 J_1) = \frac{1}{2} [1 + S_1' \cdot S_m']$	$p(E_2 J_1) = \frac{1}{2} [1 - S_1' \cdot S_m']$

Tabela 2.1 - Probabilidades de obtenção dos possíveis resultados de uma medição para dois estados diferentes.

Para sermos capazes de distinguir entre J_0 e J_1 , usando o polarizador S_m , devemos responder à seguinte pergunta: Dado que o estado E_i , $i = 1, 2$, foi obtido como resultado de uma medição, então qual estado foi medido, J_0 ou J_1 ? A estratégia ótima é observar as

probabilidades *a posteriori*, as quais podem ser obtidas fazendo-se uso do teorema de Bayes [Apêndice E]:

$$p(J_0|E_i) = \frac{\pi_0 p(E_i|J_0)}{p(E_i)} \quad (2.21)$$

$$p(J_1|E_i) = \frac{\pi_1 p(E_i|J_1)}{p(E_i)} . \quad (2.22)$$

Portanto, para acertar ao máximo a identidade do estado medido, dado o resultado obtido da medição, devemos apostar no estado que tiver maior probabilidade *a posteriori*. Por outro lado, a probabilidade média de erro, que acontece quando apostamos na menor probabilidade *a posteriori*, é dada por:

$$PE(J_0, J_1) = \sum_i p(E_i) \min[p(J_0|E_i), p(J_1|E_i)] \Rightarrow \quad (2.23)$$

$$PE(J_0, J_1) = p(E_1) \min[p(J_0|E_1), p(J_1|E_1)] + p(E_2) \min[p(J_0|E_2), p(J_1|E_2)] . \quad (2.24)$$

Usando as Eqs. (2.21) e (2.22), temos:

$$\min[p(J_0|E_i), p(J_1|E_i)] = \frac{1}{2p(E_i)} \min[p(E_i|J_0), p(E_i|J_1)] , \quad (2.25)$$

onde foi feita a consideração $\pi_0 = \pi_1 = 0,5$. Substituindo as equações da Tabela 2.1 na Eq. (2.25), obtemos:

$$\min[p(E_1|J_0), p(E_1|J_1)] = \min\left[\frac{1}{2}(1 + S'_0 \cdot S'_m), \frac{1}{2}(1 + S'_1 \cdot S'_m)\right] = \frac{1}{2} \{1 + \min[S'_0 \cdot S'_m, S'_1 \cdot S'_m]\} \quad (2.26)$$

$$\min[p(E_2|J_0), p(E_2|J_1)] = \min\left[\frac{1}{2}(1 - S'_0 \cdot S'_m), \frac{1}{2}(1 - S'_1 \cdot S'_m)\right] = \frac{1}{2} \{1 - \max[S'_0 \cdot S'_m, S'_1 \cdot S'_m]\} \quad (2.27)$$

Expandindo as funções min e max, temos:

$$\left. \begin{matrix} \min(A, B) \\ \max(A, B) \end{matrix} \right\} = \frac{1}{2} [(A+B) \mp (A-B) \operatorname{sgn}(A-B)] = \frac{1}{2} \left[(A+B) \mp \frac{(A-B)^2}{|A-B|} \right] \Rightarrow \quad (2.28)$$

$$\left. \begin{matrix} \min(A, B) \\ \max(A, B) \end{matrix} \right\} = \frac{1}{2} [(A+B) \mp |A-B|] . \quad (2.29)$$

Substituindo (2.28) e (2.29) em (2.26) e (2.27) e a resultante em (2.25) e (2.24), obtemos:

$$PE(J_0, J_1) = \frac{1}{2} - \frac{1}{4} |(S'_0 - S'_1) \cdot S'_m| . \quad (2.30)$$

A Eq. (2.30) é muito sugestiva, pois ela nos dá uma interpretação física da probabilidade de erro. Se os dois feixes, representados por S_0 e S_1 , têm a mesma potência nas polarizações de referência do vetor de Stokes, então eles são indistinguíveis perante qualquer medição de polarização. Neste caso $(S'_0 - S'_1) = [0]$ e $PE = 0,5$. Isto também ocorre quando o vetor de Stokes do aparelho de medição é ortogonal a ambos os vetores de Stokes dos estados. Neste caso, devemos trocar a base de medição para sermos capazes de fazer alguma distinção entre os estados. Usando, agora, a relação entre parâmetros de Stokes e matriz coerência através das matrizes sigmas [Apêndice E]:

$$s_i^k = \text{Tr}(J_k \sigma_i), \quad k = 0, 1, \quad (2.31)$$

no produto escalar da Eq. (2.30), obtemos:

$$PE(J_0, J_1) = \frac{1}{2} - \frac{1}{4} \left| \sum_{i=1}^3 \text{Tr}[(J_0 - J_1) \sigma_i] s_i^m \right|. \quad (2.32)$$

Se o polarizador mede as polarizações vertical e horizontal, então $S_m = [1 \ 1 \ 0 \ 0]^T$, o que leva a Eq. (2.32) a:

$$PE(J_0, J_1) = \frac{1}{2} - \frac{1}{4} \left| \text{Tr}[(J_0 - J_1) \sigma_1] \right|. \quad (2.33)$$

Usando $\text{Tr}(J_0) = \text{Tr}(J_1) = 1$, em (2.33), mostra-se que a operação módulo e traço podem ter a ordem de atuação trocada, o que nos dá:

$$PE(J_0, J_1) = \frac{1}{2} - \frac{1}{4} \text{Tr} \left[(J_0 - J_1) \sigma_1 \right]. \quad (2.34)$$

A Eq. (2.34) é bem similar à probabilidade de erro entre duas matrizes densidade de estados, $PE(\rho_0, \rho_1)$, apresentada na Apêndice F, exceção feita apenas à presença da matriz sigma na Eq. (2.34). Na situação geral de um polarizador sem base definida, podemos trabalhar com (2.32) de forma a obter uma equação mais simples. Trabalhando o somatório da Eq. (2.32), temos:

$$\sum_{i=1}^3 \text{Tr}[(J_0 - J_1) \sigma_i] s_i^m = \text{Tr} \left[(J_0 - J_1) \sum_{i=1}^3 s_i^m \sigma_i \right]. \quad (2.35)$$

Do Apêndice E, temos que:

$$J_m = \frac{1}{2} \sum_{i=0}^3 s_i^m \sigma_i \Rightarrow \sum_{i=1}^3 s_i^m \sigma_i = 2J_m - s_0^m I, \quad (2.36)$$

onde I é a matriz identidade. Substituindo (2.36) em (2.35) e a resultante em (2.32), obtemos:

$$PE(J_0, J_1) = \frac{1}{2} - \frac{1}{2} |Tr[(J_0 - J_1)J_m]|, \quad (2.37)$$

onde $s_0^m=1$ e $Tr(J_0-J_1)=0$ foram usados na obtenção de (2.37). Embora a PE seja uma medida de distinção entre J_0 e J_1 , ela não é uma medida de distância entre J_0 e J_1 . Uma medida de distância deve valer 0 quando as matrizes coerência são iguais (indistinguíveis) e 1 quando forem ortogonais (maximamente distinguíveis). Uma conhecida medida de distância é a distância de Kolmogorov, K , a qual é relacionada a PE por [Apêndice F]:

$$K(J_0, J_1) = 1 - 2PE(J_0, J_1) = |Tr[(J_0 - J_1)J_m]| = \frac{1}{2} |(S'_0 - S'_1) \cdot S'_m|. \quad (2.38)$$

Como pode-se observar na Eq. (2.20), a distribuição de probabilidade dos possíveis resultados de uma medida é a mesma para o estado de polarização parcial (misto), $J(S)$, e para o *quase-estado* ($Tr(J_p) < 1$) completamente polarizado (puro), $J_p(S_p)$. Nestas condições eles são indistinguíveis e chamaremos o *quase-estado* puro S_p de uma purificação do estado misto S . Esta purificação é diferente da exposta no Apêndice F, onde a purificação para a matriz densidade de um estado misto também é um estado. Qualquer medida de distância que só tenha sentido físico para estados puros, também pode ser usada em estados mistos fazendo-se uso da purificação. Um bom exemplo disso é a seguinte medida de distância:

$$D = \frac{1}{2} - \frac{1}{2} S'_0 \cdot S'_1. \quad (2.39)$$

A distância entre os estados puros $S(\theta)$ e $S(\varphi)$, usando as Eqs. (2.39) e (2.4), é da forma:

$$D = \frac{1}{2} - \frac{1}{2} \cos[2(\theta - \varphi)] = \sin^2(\theta - \varphi). \quad (2.40)$$

A interpretação física desta medida é óbvia: ela é baseada na diferença dos ângulos de polarização e, por isso, é adequada a estados puros. Entretanto, se for usada em estados mistos, ela fornecerá um resultado correto porém de difícil interpretação física, caso a mesma exista. As Eqs. (2.38) e (2.39) mostram que a distância entre dois estados mistos é, na verdade, a distância entre as purificações dos mesmos.

2.2.3 Correção da Variação da Polarização em um Sistema Quântico Polarimétrico

Até o presente momento, os conceitos de probabilidade de resultados de medidas e de distâncias (distinções) entre estados, comumente conhecidos para a matriz densidade de estados ρ , foram estendidos à matriz coerência e vetor de Stokes. Isto foi importante porque simularemos a evolução da polarização em um sistema quântico de comunicações ópticas através da matriz coerência e do vetor de Stokes. Trataremos de um sistema de comunicações quânticas no qual os fótons polarizados são enviados do transmissor ao receptor através de uma fibra óptica. Diversos experimentos de criptografia quântica polarimétrica em fibras ópticas já foram realizados [Refs. 2.7-2.10]. Ao se propagar na

fibra, a polarização do fóton sofre mudanças devido à variação aleatória da birrefringência ao longo da fibra; por isso, todos os experimentos polarimétricos fazem algum tipo de controle de polarização, em particular, o uso de um pré-equalizador foi proposto na Referência 2.7. Devido à birrefringência, o estado de polarização incidente na fibra se decompõe em dois estados ortogonais entre si, chamados estados principais de polarização. Como a birrefringência em uma fibra normal varia aleatoriamente ao longo da fibra, usaremos um modelo discreto no qual a fibra é dividida em trechos de birrefringência constante [Refs. 2.1, 2.2], Fig. 2.1. O número de trechos e os estados principais de cada trecho devem obedecer a um critério estatístico.



Fig. 2.1 - Modelo estatístico discreto da variação aleatória da birrefringência ao longo da fibra óptica.

Cada trecho de fibra é representado por uma matriz transferência da forma [Refs. 2.2, 2.5, 2.6]:

$$T_h = \exp(-\alpha L_h + i\beta L_h) \begin{bmatrix} \cos(\psi_h) & \sin(\psi_h) \exp(i\Phi_h) \\ -\sin(\psi_h) \exp(-i\Phi_h) & \cos(\psi_h) \end{bmatrix}, \quad (2.41)$$

onde L_h é o comprimento do h -ésimo trecho de fibra, α é responsável pela perda e β é a constante de propagação linear. Abandonaremos, neste momento, o sub-índice h para facilitar a nomenclatura. O ângulo ψ é uniformemente distribuído no intervalo $[0, 2\pi]$ e o atraso de fase entre as componentes do campo, Φ , é devido à diferença de índices de refração para as duas componentes, Δn [Ref. 2.2]:

$$\Phi = \frac{2\pi L_h}{\lambda} \Delta n, \quad (2.42)$$

onde λ é o comprimento de onda da luz. Δn provoca também um atraso temporal entre as componentes do campo, chamado dispersão de polarização [Refs. 2.1, 2.2]:

$$\Delta\tau = D_p \sqrt{L} \quad (2.43)$$

$$D_p = \sqrt{\frac{8}{3\pi}} \frac{\Delta n}{c} \sqrt{L}, \quad (2.44)$$

onde D_p é o parâmetro de dispersão de polarização e c a velocidade da luz no vácuo. Usando as Eqs. (2.42) a (2.44), obtemos:

$$\Phi = \sqrt{\frac{3\pi}{8}} \frac{2\pi c}{\lambda} \Delta\tau. \quad (2.45)$$

É importante colocar Φ em função de $\Delta\tau$ pois é sabido que este último segue uma distribuição de probabilidade Maxwelliana [Ref. 2.1]. Por fim, voltando a usar o sub-índice h , a matriz transferência da fibra inteira é dada por:

$$T_f = \prod_{h=1}^n T_h = \exp(-\alpha L + i\beta L) \prod_{h=1}^n \begin{bmatrix} \cos(\psi_h) & \sin(\psi_h) \exp(i\Phi_h) \\ -\sin(\psi_h) \exp(-i\Phi_h) & \cos(\psi_h) \end{bmatrix}, \quad (2.46)$$

onde n é o número de trechos em que a fibra foi dividida. Após a multiplicação, a Eq. (2.46) pode ser posta na forma mostrada no Apêndice E:

$$T_f = \exp(-\alpha L + i\beta L) \begin{pmatrix} \varepsilon \exp(i\xi_1) & \sqrt{1-\varepsilon^2} \exp(i\xi_2) \\ -\sqrt{1-\varepsilon^2} \exp(-i\xi_2) & \varepsilon \exp(-i\xi_1) \end{pmatrix}. \quad (2.47)$$

Portanto, um estado de polarização incidente na fibra será modificado segundo a matriz transferência da Eq. (2.47). A variação da polarização, causada pela Eq. (2.47), varia com o tempo e é muito severa, devendo ser compensada para que a comunicação seja viável. Para isso propomos um equalizador óptico a ser colocado na entrada do receptor. O equalizador é formado pelo conjunto compensador-rotacionador-compensador cujas matrizes transferências individuais e do conjunto são [Refs. 2.4, 2.11]:

$$R(\phi) = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix} \quad (2.48)$$

$$C(\delta) = \begin{bmatrix} e^{i\frac{\delta}{2}} & 0 \\ 0 & e^{-i\frac{\delta}{2}} \end{bmatrix} \quad C(\sigma) = \begin{bmatrix} e^{i\frac{\sigma}{2}} & 0 \\ 0 & e^{-i\frac{\sigma}{2}} \end{bmatrix} \quad (2.49)$$

$$E = C(\delta)R(\phi)C(\sigma) = \begin{pmatrix} \cos(\phi) \exp[i0,5(\delta + \sigma)] & \sin(\phi) \exp[i0,5(\delta - \sigma)] \\ -\sin(\phi) \exp[-i0,5(\delta - \sigma)] & \cos(\phi) \exp[-i0,5(\delta + \sigma)] \end{pmatrix}. \quad (2.50)$$

A matriz transferência do conjunto fibra-equalizador é:

$$T = T_f E. \quad (2.51)$$

Para que não haja variação na polarização devemos ter:

$$T = I \Rightarrow C(\delta)R(\phi)C(\sigma) = T_f^{-1}, \quad (2.52)$$

ou seja, para que a polarização do estado incidente seja preservada ao longo do percurso do transmissor ao receptor, a matriz transferência do conjunto canal-equalizador deve ser igual à matriz identidade. Substituindo as Eqs. (2.47) e (2.50) na Eq. (2.52), desconsiderando os termos de perdas e fase linear, encontramos as seguintes condições a serem satisfeitas:

$$\cos(\phi) = \varepsilon \quad (2.53)$$

$$\delta = \xi_2 - \xi_1 \quad (2.54)$$

$$\sigma = -(\xi_2 + \xi_1) \quad (2.55)$$

Portanto, para atuarmos no equalizador de forma a compensar os efeitos da fibra óptica devemos estimar os parâmetros da matriz transferência da fibra. Para isso, adotamos o procedimento da Referência 2.1, descrito no Apêndice E. Assim, o protocolo de comunicação usado no sistema deverá incluir a transmissão de seqüências de pulsos, no mínimo três, de intensidades normais e polarizações iniciais conhecidas, que serão usados no receptor para a estimação da matriz transferência da fibra. O envio destes pulsos deverá ocorrer a cada metade do tempo que a fibra leva para mudar seu estado (mudar sua matriz transferência).

Neste momento, estamos aptos à realizar simulações de um sistema quântico de comunicações usando o formalismo clássico da matriz coerência e vetor de Stokes. Seja o sistema de comunicação binário mostrado na Fig. 2.2. O transmissor usa como codificação de suas mensagens, bits 0 e 1, os estados de polarizações lineares $|\theta\rangle$ e $|\varphi\rangle$, e os envia ao receptor com probabilidades *a priori* π_0 e π_1 , respectivamente. Ao trafegar pelo canal quântico, a polarização sofrerá perturbações modelada pela matriz transferência da fibra T_f . Na entrada do receptor o estimador, usando os pulsos de intensidade normal que serão enviados periodicamente durante a comunicação, configurará os parâmetros do equalizador de forma a compensar as variações da polarização. O equalizador, por sua vez, entregará o sinal óptico ao polarizador, caracterizado pelo vetor de Stokes $S_m = [1 \ 1 \ 0 \ 0]^T$.

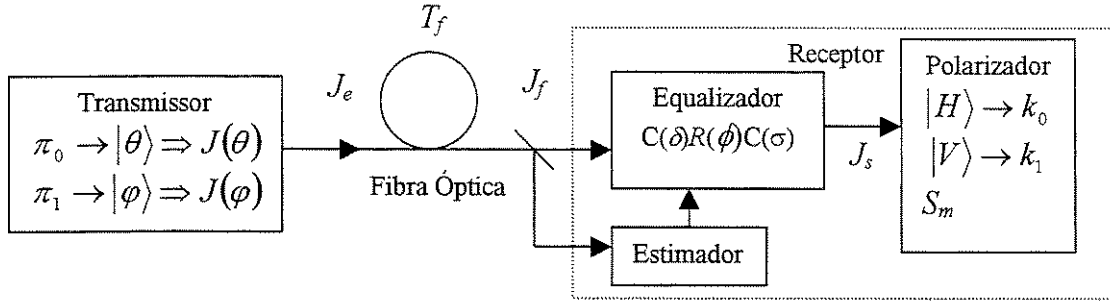


Fig. 2.2 - Sistema de comunicação quântica polarimétrica com equalizador óptico.

k_0 e k_1 são as frequências relativas dos resultados da medição da polarização feitas no receptor. Para a simulação do sistema de comunicação, usamos estados de polarização representados por vetores da forma:

$$E = \begin{bmatrix} \cos(\theta)\exp(i\phi) \\ \sin(\theta)\exp(i\xi) \end{bmatrix} \quad (2.56)$$

O estado de polarização horizontal, por exemplo, é representado pelo vetor $E = [1 \ 0]^T$. Seguindo a Referência 2.2, cada trecho de fibra, com birrefringência constante, tem comprimento de 250 m e o comprimento de onda usado é $1,3\mu\text{m}$. Os parâmetros da matriz transferência de cada trecho de fibra, Eq.(2.41), aqui repetida,

$$T_h = \begin{bmatrix} \cos(\psi_h) & \sin(\psi_h)\exp(i\Phi_h) \\ -\sin(\psi_h)\exp(-i\Phi_h) & \cos(\psi_h) \end{bmatrix}, \quad (2.57)$$

são obtidos através das funções distribuições de probabilidades (FDP), sendo uma FDP constante em $[0, 2\pi]$ para a variável aleatória ψ_h . Para a dispersão de polarização, Eq. (2.43), usamos a distribuição [Ref. 2.1]:

$$FDP(\Delta\tau) = \frac{1}{N} \frac{1}{\sqrt{(2\pi\eta^2)^3}} \exp\left(-5 \frac{(\Delta\tau - 0,5)^2}{2\eta^2}\right) \quad (2.58)$$

$$\eta = \frac{1}{2} \sqrt{\frac{\pi}{8}}. \quad (2.59)$$

N é uma constante de normalização de forma a fazer a probabilidade total (integral da Eq.(2.58)) unitária. A Eq. (2.58) pode ser vista na Fig. 2.3.

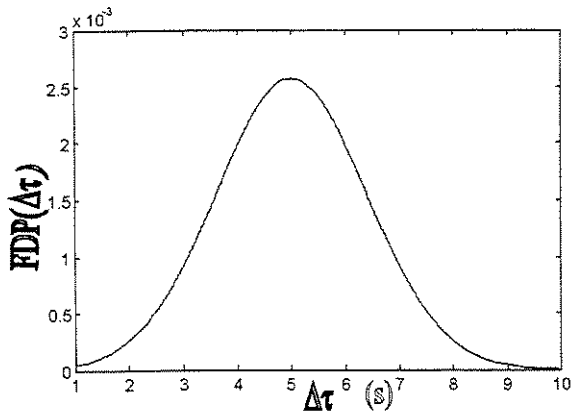


Fig. 2.3 - FDP da dispersão de polarização.

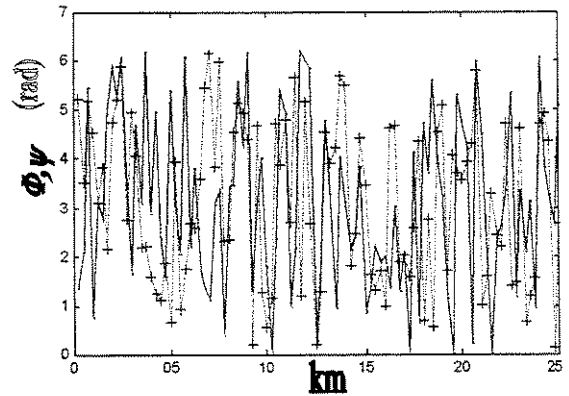


Fig. 2.4 - ψ (+) e Φ (linha contínua) para uma fibra de 25 km.

A fase relativa entre as componentes do campo, Φ , é obtida usando-se a Eq.(2.42), aqui repetida:

$$\Phi = \sqrt{\frac{3\pi}{8}} \frac{2\pi c}{\lambda} \Delta\tau \quad (2.60)$$

Na Fig. 2.4 vemos o resultado de ψ e Φ para uma simulação de uma fibra com 25 km. Os bits transmitidos são equiprováveis, isto é, $\pi_0 = \pi_1 = 0,5$. Para analisar o desempenho do sistema, com e sem o equalizador, os estados a serem transmitidos são $|H\rangle$ e $|V\rangle$; neste caso, para um canal que não introduza ruído, os resultados na recepção são determinísticos pois os estados a serem transmitidos também formam a base de medição do polarizador, $S_m = [1 \ 1 \ 0 \ 0]^T$. Assim, se por exemplo, o estado $|V\rangle$ for enviado, deveremos obter como resultado da medição, no receptor, o estado $|V\rangle$ com 100% de certeza. Os resultados das simulações

são expostos na Tabela 2.2, sendo t_f o tempo, em número de bits, em que a fibra permanece com suas características fixas e t_e o período, em número de bits, em que o estimador tem que atuar, ou seja, o transmissor deve enviar a sequência de pulsos de intensidade normal e polarização conhecida a cada t_e (unidades de tempo).

Número de bits	t_f	t_e	Erro (%)
20000	200	∞	50,36
20000	200	250	25,32
20000	200	200	0,72
20000	200	150	12,32
20000	200	100	0,26

Tabela 2.2 - Resultados das simulações da configuração da Fig. 2.2.

O uso do sistema com equalizador em criptografia quântica é direta. A Fig. 2.5 mostra a configuração.

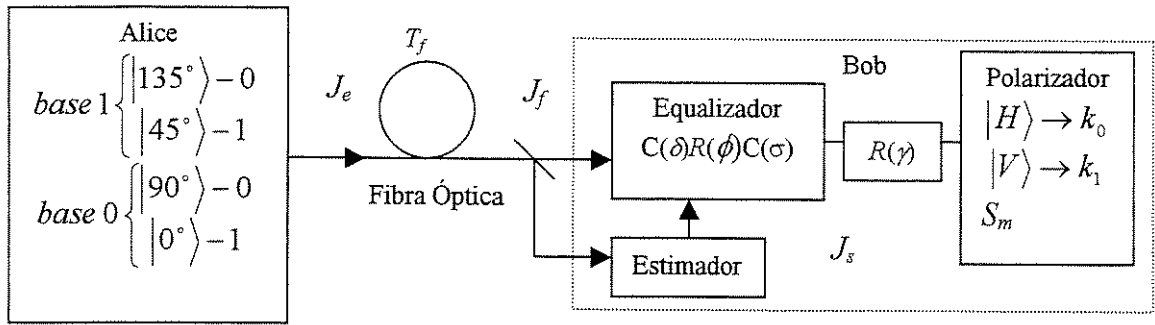


Fig. 2.5 - Sistema de criptografia quântica polarimétrica com equalizador óptico.

O funcionamento é o seguinte: Alice escolhe aleatoriamente a base e o bit, selecionando um dos quatro estados mostrado na Fig. 2.5, e o envia a Bob. Se Bob escolher para sua medição a base 1, ele fará $\gamma = -45^\circ$; caso contrário fará $\gamma = 0^\circ$. O protocolo usado é o BB84, descrito no Apêndice C. A Tabela 2.3 mostra os resultados das simulações.

Número de bits	t_f	t_e	Erro (%)
20000	200	∞	51,71
20000	200	150	11,64
20000	200	100	0,1314

Tabela 2.3 - Resultados das simulações da configuração da Fig. 2.5.

Os resultados das Tabelas 2.2 e 2.3 mostram a eficiência do equalizador, o qual leva a probabilidade de erro a próxima de 50%, na sua ausência, e a menor de 0,5%, quando $t_e = 0,5t_f$, sendo este último valor devido aos primeiros 200 bits, durante os quais o equalizador ainda não foi inicializado.

2.3 Grau de Pureza para Matrizes Densidade, g_p

Uma luz parcialmente polarizada pode ser decomposta em uma soma incoerente de um feixe totalmente polarizado e um feixe totalmente despolarizado, $J = J_{np} + J_p$ [Apêndice E]. De forma semelhante, vamos separar a matriz densidade, 2×2 , na soma de uma matriz correspondendo a um estado maximamente misto, ρ_m , e outra correspondendo a um estado puro, ρ_p . Iniciamos aplicando a ρ a mesma transformação usada para dividir J :

$$\rho = \rho_0 + \rho_1 = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} + \begin{pmatrix} B & D \\ D^* & C \end{pmatrix}, \quad (2.61)$$

onde os elementos das matrizes em (2.61) são dados por:

$$A = \frac{1}{2} [1 - \sqrt{1 - 4 \det(\rho)}] \quad (2.62)$$

$$B = \frac{1}{2} (\rho_{11} - \rho_{22}) + \frac{1}{2} \sqrt{1 - 4 \det(\rho)} \quad (2.63)$$

$$C = \frac{1}{2} (\rho_{22} - \rho_{11}) + \frac{1}{2} \sqrt{1 - 4 \det(\rho)} \quad (2.64)$$

$$D = \rho_{12}, \quad (2.65)$$

sendo ρ_{ij} os elementos de ρ . Para que a separação (2.61) seja única, a condição $\det(\rho_1) = 0$ deve ser satisfeita. Definimos, então, o grau de pureza, g_p , de forma semelhante ao grau de polarização, por:

$$g_p = \text{Tr}(\rho_1) = \sqrt{1 - 4 \det(\rho)}. \quad (2.66)$$

g_p é uma medida de pureza do estado quântico representado pela matriz densidade ρ . Esta medida é geralmente feita pela entropia de von Neumann, $S(\rho) = -\text{Tr}(\rho \log \rho)$ [Apêndice F] e, por isso, é interessante relacioná-las. Assim, seja a matriz densidade ρ com autovalores λ_1 e λ_2 . O grau de pureza, g_p , e os autovalores de ρ são ligados pelas relações:

$$\lambda_1 = \frac{1}{2} (1 + g_p) \quad (2.67)$$

$$\lambda_2 = \frac{1}{2} (1 - g_p). \quad (2.68)$$

Por outro lado, a entropia de von Neumann, S , é dada também por [Apêndice F]:

$$S = -\lambda_1 \log \lambda_1 - \lambda_2 \log \lambda_2. \quad (2.69)$$

Trabalhando com as Eqs. (2.67)-(2.69), obtemos:

$$S = -\frac{1}{2} \log \left\{ \frac{(1-g_p^2)}{4} \left[\frac{(1+g_p)}{(1-g_p)} \right]^{g_p} \right\} = -\frac{1}{2} \log \left\{ \frac{1}{4} (1+g_p)^{(1+g_p)} (1-g_p)^{(1-g_p)} \right\}. \quad (2.70)$$

Quando um estado é puro temos $S = 0$ e $g_p = 1$. Por outro lado, para um estado maximamente misto, isto é, todos os resultados de uma medição têm a mesma probabilidade de ocorrer, $S = 1$ [bit] (entropia máxima) e $g_p = 0$. A Fig. 2.6 mostra a curva referente à Eq. (2.70).

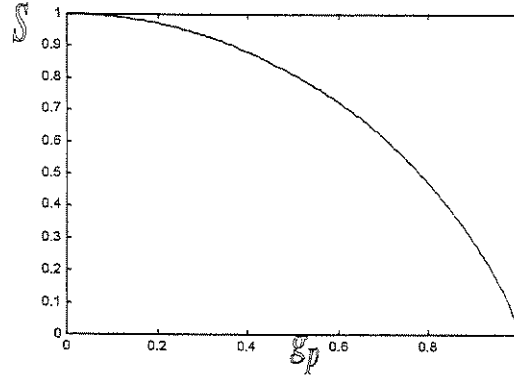


Fig. 2.6 - Entropia x Grau de Pureza

O grau de pureza é interessante, pois troca a operação logaritmo de uma matriz pelo cálculo do determinante da matriz densidade. É importante salientar que, as condições para um estado ser puro, $S(\rho) = 0$ e $\det(\rho) = 0$, representam na verdade apenas uma condição, senão vejamos: A entropia, dada pela Eq. (2.69), só se anula se $\lambda_i = 1$ ou 0 , $i=1,2$, pois os autovalores da matriz densidade são sempre positivos e reais (Hermitiana e definida positiva). Como $\text{Tr}(\rho) = \lambda_1 + \lambda_2 = 1$, apenas um autovalor é unitário, sendo o outro nulo. Agora, como $\det(\rho) = \lambda_1 \lambda_2$, se um dos autovalores é nulo, então o determinante também o é. Portanto, $S(\rho) = 0 \Rightarrow \det(\rho) = 0$. O contrário nem sempre é verdadeiro.

A Eq. (2.61) não nos serve muito pois as matrizes densidades ρ_0 e ρ_1 possuem traço inferior à unidade ($\text{Tr}(\rho_0) + \text{Tr}(\rho_1) = 1$). Resolvemos este problema usando a Eq. (2.66) nas Eqs. (2.61)-(2.65) e reescrevendo a matriz densidade como:

$$\rho = (1-g_p) \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} + g_p \begin{pmatrix} B/g_p & D/g_p \\ D^*/g_p & C/g_p \end{pmatrix} = (1-g_p) \rho_m + g_p \rho_p. \quad (2.71)$$

Agora, vemos a matriz densidade ρ como uma mistura clássica das matrizes ρ_m (maximamente mista) e ρ_p (puro), ambas com traço unitário, a primeira ocorrendo com probabilidade $(1-g_p)$ e, a segunda, ocorrendo com probabilidade g_p .

2.3.1 Medida de Distância Entre Estados Quânticos Utilizando g_p

Como visto na Seção 2.2.2 e no Apêndice F, usamos as medidas de distância para distinguir os estados quânticos. Nesta seção vamos analisar a variação da distância de Kolmogorov, K , com a variação do grau de pureza dos estados em sistemas bidimensionais.

Sejam as matrizes densidades:

$$\rho_a = (1 - g_p^a) \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} + g_p^a \begin{pmatrix} B_a/g_p^a & D_a/g_p^a \\ D_a^*/g_p^a & C_a/g_p^a \end{pmatrix} = (1 - g_p^a) \rho_m + g_p^a \rho_p^a \quad (2.72)$$

$$\rho_b = (1 - g_p^b) \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} + g_p^b \begin{pmatrix} B_b/g_p^b & D_b/g_p^b \\ D_b^*/g_p^b & C_b/g_p^b \end{pmatrix} = (1 - g_p^b) \rho_m + g_p^b \rho_p^b \quad (2.73)$$

A distância de Kolmogorov é dada por [Apêndice F]:

$$K(\rho_a, \rho_b) = \frac{1}{2} \text{Tr}(|\rho_a - \rho_b|) = \frac{1}{2} (|\mu_1| + |\mu_2|), \quad (2.74)$$

onde μ_1 e μ_2 são os autovalores da matriz $\Gamma = \rho_a - \rho_b$. Trabalhando com a Eq. (2.74), obtemos:

$$K = |\sqrt{\det(\Gamma)}| \quad (2.75)$$

$$\det(\Gamma) = -0,25(g_p^b - g_p^a)^2 + g_p^b g_p^a \sigma \quad (2.76)$$

$$\sigma = (D_a D_b^* + D_b D_a^* - B_a C_b - B_b C_a) / g_p^b g_p^a, \quad (2.77)$$

onde $|\sigma|^{1/2}$ é a distância de Kolmogorov, quando os estados ρ_a e ρ_b são puros. Como $K_{max} = 1$ (distância entre dois estados puros ortogonais), $\sigma_{max} = 1$. Pelas Eqs. (2.75)-(2.77), temos que, a distância entre um estado puro ($g_p^b = 1$), qualquer que seja ele, e um estado maximamente misto ($g_p^a = 0$) é sempre $K = 0,5$; bem como a distância entre um estado misto qualquer ($0 < g_p^a < 1$) e um maximamente misto ($g_p^b = 0$), é sempre $K < 0,5$. Escrevemos, agora, as matrizes densidades como sendo da forma:

$$\rho_a = (1 - g_p^a) \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} + g_p^a \begin{pmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & \sin^2(\theta) \end{pmatrix} \quad (2.78)$$

$$\rho_b = (1 - g_p^b) \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} + g_p^b \begin{pmatrix} \cos^2(\phi) & \cos(\phi)\sin(\phi) \\ \cos(\phi)\sin(\phi) & \sin^2(\phi) \end{pmatrix}. \quad (2.79)$$

Com isto, obtemos para a distância de Kolmogorov, a seguinte equação:

$$K = \sqrt{0,25(g_p^b - g_p^a)^2 + g_p^b g_p^a \sin^2(\phi - \theta)}. \quad (2.80)$$

Podemos, então, parametrizar a matriz densidade pelo par (g_p, ϕ) e, assim, representar qualquer estado, com matriz densidade da forma (2.78), por um ponto de coordenadas (raio = g_p , ângulo = ϕ), dentro de um círculo de raio unitário, Fig. 2.7.

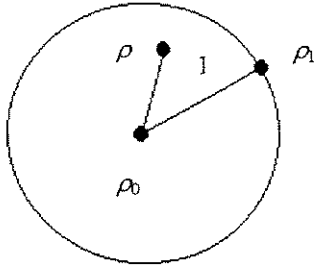


Fig. 2.7 - Representação de ρ na circunferência de raio unitário.

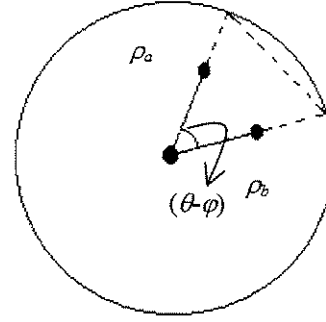


Fig. 2.8 - Representação geométrica da distância entre os estados ρ_a e ρ_b

No centro da circunferência se localiza o estado maximamente misto e na fronteira os estados puros. No interior do círculo, com exceção do centro, estão os estados mistos. Podemos, baseado na Fig. 2.7, dar uma interpretação geométrica à distância de Kolmogorov:

$$K = \sqrt{0,25d^2 + g_p^a g_p^b 4s^2}, \quad (2.81)$$

onde d é a distância entre os pontos que representam ρ_a e ρ_b no círculo, caso eles fossem colineares ($\theta = \varphi$), e s é a área do triângulo na Fig. 2.8. Se tivéssemos usado uma exponencial complexa nos elementos fora da diagonal das segundas matrizes no lado direito das Eqs. (2.78) e (2.79), o círculo da Fig. 2.7 se transformaria numa esfera.

A seguir, usando as matrizes densidades das Eqs. (2.78) e (2.79), mostramos, nas Figs. 2.9-2.17, as curvas da variação de $K(\rho_a, \rho_b)$ quando as matrizes densidades vão de estados puros a maximamente mistos. Os dados das simulações são expostos na Tabela 2.4.

SIM	θ	φ	g_p^a	g_p^b
1	0	0	0-1	0
2			0-1	1
3			0-1	0-1
4	0	$\pi/2$	0-1	0
5			0-1	1
6			0-1	0-1
7	$\pi/4$	$\pi/3$	0-1	0
8			0-1	1
9			0-1	0-1

Tabela 2.4 - Dados para as simulações das distâncias de Kolmogorov.

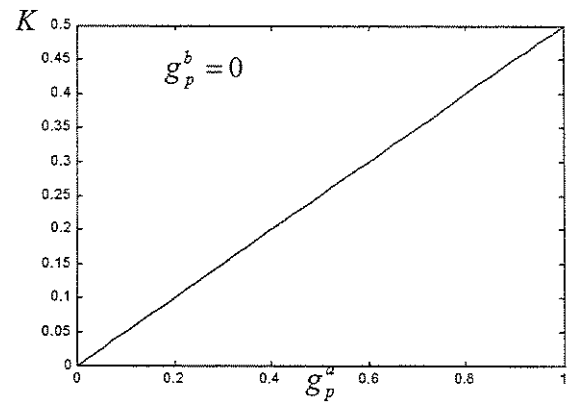


Fig. 2.9 - $K(g_p^a, g_p^b = 0)$. (SIM-1)

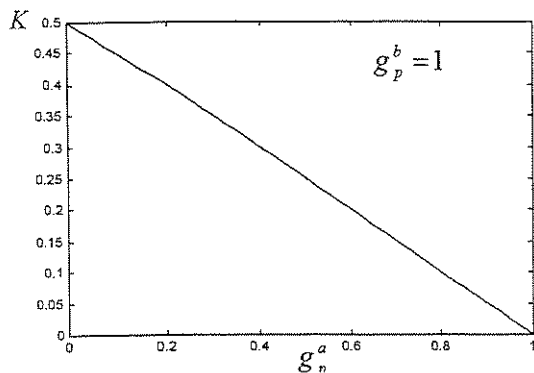


Fig. 2.10 - $K(g_p^a, g_p^b = 1)$. (SIM-2)

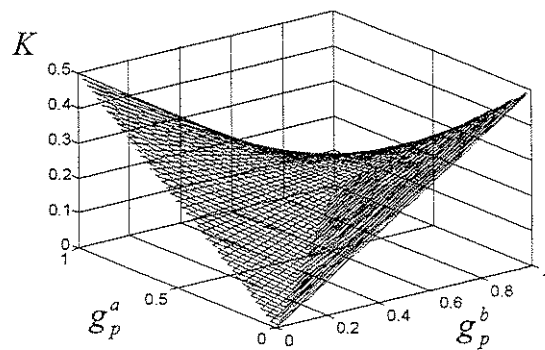


Fig. 2.11 - $K(g_p^a, g_p^b)$. (SIM-3)

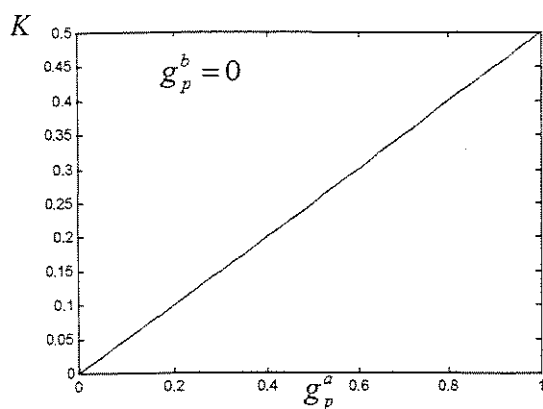


Fig. 2.12 - $K(g_p^a, g_p^b = 0)$. (SIM-4)

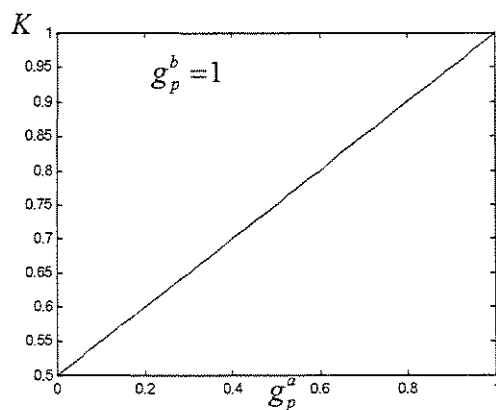


Fig. 2.13 - $K(g_p^a, g_p^b = 1)$. (SIM-5)

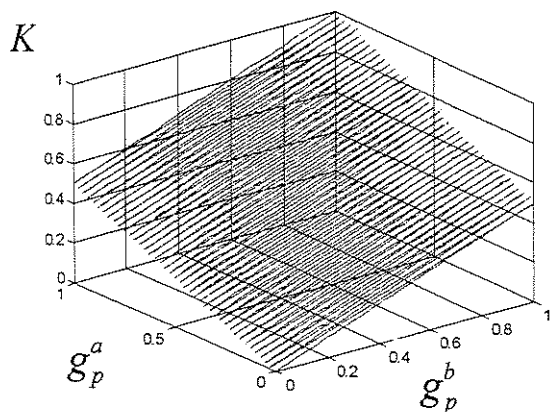


Fig. 2.14 - $K(g_p^a, g_p^b)$. (SIM-6)

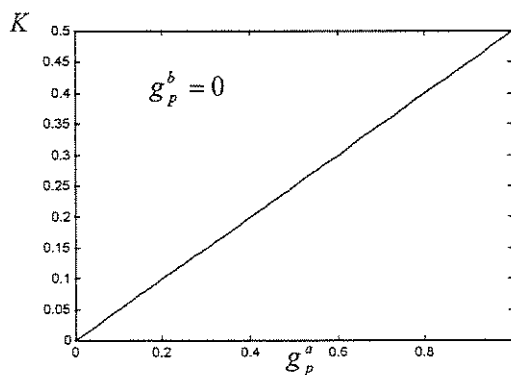


Fig. 2.15 - $K(g_p^a, g_p^b = 0)$. (SIM-7)

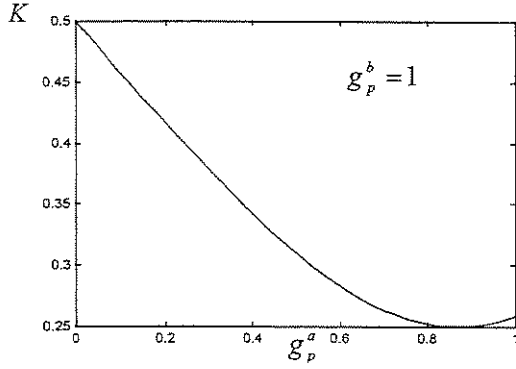


Fig. 2.16 - $K(g_p^a, g_p^b = 1)$. (SIM-8)

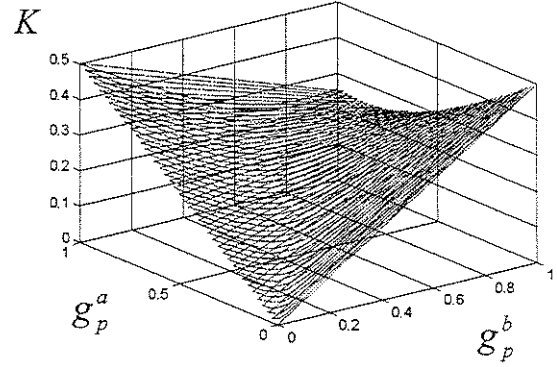


Fig. 2.17 - $K(g_p^a, g_p^b)$. (SIM-9)

2.3.2 Canal Ruidoso e Informação Mútua Utilizando g_p

A informação, em comunicações quânticas, é transmitida na coerência e/ou no entrelaçamento (correlação) de estados quânticos e, portanto, um bom canal quântico deve preservar estas características. Um canal ruidoso provoca a descoerência e a descorrelação dos estados quânticos, em maior ou menor grau segundo a quantidade ruído presente, transformando o canal quântico em um canal clássico. O processo de descoerência transforma um estado puro em um misto. Analisemos, agora, um sistema de comunicação quântica com canal ruidoso. Seja uma fonte de estados puros transmitindo os estados $|\alpha_i\rangle$ com probabilidade p_i . Após passar pelo canal ruidoso, o estado $|\alpha_i\rangle$ se transforma em um dos estados do conjunto $\{|\beta_j^i\rangle\}_{j=1}^N$ com probabilidades $\{p_j^i\}_{j=1}^N$, respectivamente [Ref. 2.12]. Equivalentemente, podemos dizer que o estado puro $|\alpha_i\rangle$ evoluiu para o estado misto:

$$\rho_i = \sum_{j=1}^N p_j^i |\beta_j^i\rangle \langle \beta_j^i| = (1 - g_p^i) \rho_m + g_p^i \rho_p^i = (1 - g_p^i) \rho_m + g_p^i |\Phi_i\rangle \langle \Phi_i|. \quad (2.82)$$

O estado puro $|\Phi_i\rangle$ é ortonormalizado. Para encontrarmos o valor de g_p^i , a partir dos p_j^i , calculamos $\langle \Phi_i | \rho_i | \Phi_i \rangle$ em ambos os lados de (2.82), obtendo:

$$g_p^i = 2 \sum_{j=1}^N p_j^i \left| \langle \Phi_i | \beta_j^i \rangle \right|^2 - 1. \quad (2.83)$$

Se $|\Phi_i\rangle \in \{|\beta_j^i\rangle\}_{j=1}^N$, a Eq. (2.83) se resume a:

$$g_p^i = 2p_n^i - 1, \quad (2.84)$$

na qual foi suposto $|\Phi_i\rangle = |\beta_n^i\rangle$. Nas Eqs. (2.82)-(2.84) o processo de ruído é suposto não provocar o aparecimento de variáveis complexas. Para identificar o estado enviado, o

receptor deverá realizar uma medida no mesmo. Suponhamos que, para isso, ele se utilize do operador $\hat{A}$ cujos autoestados são $|\varepsilon_k\rangle_{k=1}^M$. Então, a informação (clássica) mútua, que mede o grau de certeza que temos nos resultados das medições, é [Apêndice F]:

$$I = H(\rho) - H(\rho | \varepsilon) \quad (2.85)$$

$$H(\rho) = -\sum_{k=1}^M p(\varepsilon_k | \rho) \log_2 [p(\varepsilon_k | \rho)] = -\sum_{k=1}^M \langle \varepsilon_k | \rho | \varepsilon_k \rangle \log_2 (\langle \varepsilon_k | \rho | \varepsilon_k \rangle), \quad (2.86)$$

onde H é a entropia clássica. Para $\rho = \pi_0 \rho_m + \pi_1 \rho_p$, o segundo termo da Eq. (2.85) é dado por [Apêndice F]:

$$H(\rho | \varepsilon) = \pi_0 H(\rho_m) + \pi_1 H(\rho_p). \quad (2.87)$$

Para o canal ruidoso descrito, a informação mútua para cada símbolo é encontrada substituindo a Eq. (2.82) em (2.85)-(2.87):

$$I_i = -\sum_{k=1}^M \left[\frac{(1 - g_p^i)}{2} + g_p^i \langle \varepsilon_k | \Phi_i \rangle^2 \right] \log_2 \left[\frac{(1 - g_p^i)}{2} + g_p^i \langle \varepsilon_k | \Phi_i \rangle^2 \right] - \frac{(1 - g_p^i)M}{2} + g_p^i \sum_{k=1}^M \langle \varepsilon_k | \Phi_i \rangle^2 \log_2 (\langle \varepsilon_k | \Phi_i \rangle^2). \quad (2.88)$$

A informação mútua média é:

$$I = \sum_{i=1}^N p_i I_i. \quad (2.89)$$

A máxima quantidade de informação clássica que se pode obter de um estado quântico, através de uma medição, é limitada pelo teorema de Kholevo [Apêndice F]:

$$I \leq S\left(\sum_i \pi_i \rho_i\right) - \sum_i \pi_i S(\rho_i). \quad (2.90)$$

Substituindo as Eqs. (2.70) e (2.82) em (2.90), obtemos o limite superior de Kholevo em função do grau de pureza, para cada símbolo:

$$I_i \leq -\frac{1}{2} \log_2 \left\{ \frac{(1 + g_p^i)^{(1+g_p^i)} (1 - g_p^i)^{(1-g_p^i)}}{4} \right\} - (1 - g_p^i). \quad (2.91)$$

Como ilustração, consideremos o sistema de comunicação quântica da Fig. 2.18.

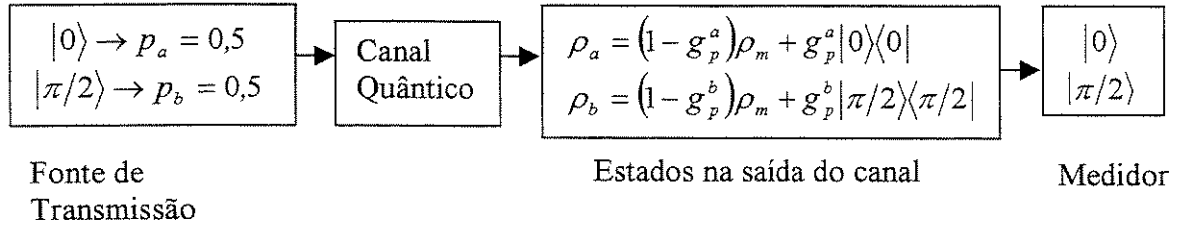


Fig. 2.18 - Sistema de comunicação quântica binário.

Na Fig. 2.18, o transmissor envia os estados $|0\rangle$ e $|\pi/2\rangle$, com probabilidades $p_a = p_b = 0,5$, respectivamente. Ao passarem pelo canal, $|0\rangle$ e $|\pi/2\rangle$ se transformam nos estados mistos ρ_a e ρ_b , respectivamente. Os estados mistos na saída do canal são entregues a um medidor cujo operador, que o representa, tem como autoestados $|0\rangle$ e $|\pi/2\rangle$. Aplicando estes dados na Eq. (2.88), encontramos para a informação mútua de cada símbolo:

$$I_a = -\frac{1}{2} \log_2 \left[\frac{(1 + g_p^a)^{(1+g_p^a)} (1 - g_p^a)^{(1-g_p^a)}}{4} \right] - (1 - g_p^a) \quad (2.92)$$

$$I_b = -\frac{1}{2} \log_2 \left[\frac{(1 + g_p^b)^{(1+g_p^b)} (1 - g_p^b)^{(1-g_p^b)}}{4} \right] - (1 - g_p^b) \quad (2.93)$$

$$I = \frac{1}{2} (I_a + I_b) . \quad (2.94)$$

Nas Eqs. (2.92)-(2.94) temos as informações mútuas dependendo apenas dos graus de pureza. Comparando as Eqs. (2.92) e (2.93) com a Eq. (2.91), vemos que o limite superior de Kholevo para a informação mútua é alcançado, implicando que a base de medição escolhida pelo receptor é ótima. A Fig. 2.19, a seguir, apresenta a variação da informação mútua (igual ao limite superior de Kholevo) com o grau de pureza, enquanto que a Fig. 2.20 mostra a informação mútua média, Eq. (2.94), do sistema da Fig. 2.18.

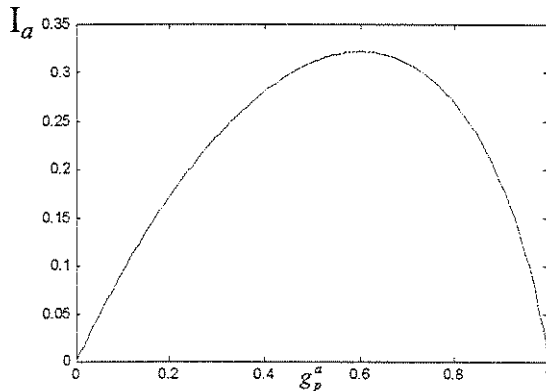


Fig. 2.19 - Variação da Informação mútua com o grau de pureza, $I_a(g_p^a)$.

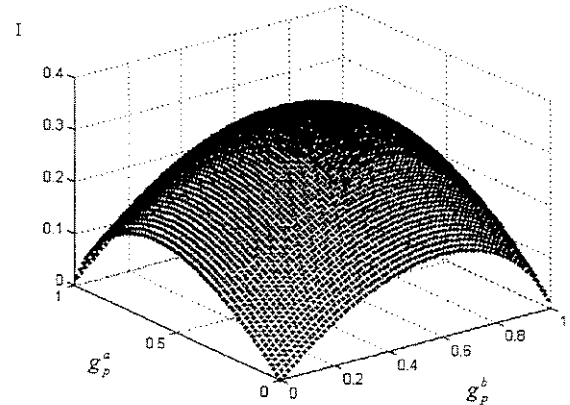


Fig. 2.20 - Variação da Informação mútua com os graus de pureza, $I(g_p^a, g_p^b)$.

O conceito de fidelidade mede a qualidade do canal para transmitir os estados quânticos. Seja uma fonte transmitindo os estados quânticos puros $|\theta_i\rangle$ com probabilidades p_i . Além disso, cada estado puro $|\theta_i\rangle$, ao se propagar pelo canal, evolui para o estado misto ρ_i . Então, a fidelidade é dada por [Apêndice F]:

$$F = \sum_i p_i \langle \theta_i | \rho_i | \theta_i \rangle . \quad (2.95)$$

Para o sistema da Fig. 2.18, temos:

$$F = \frac{1}{2} \langle 0 | \rho_a | 0 \rangle + \frac{1}{2} \langle \pi/2 | \rho_b | \pi/2 \rangle \Rightarrow \quad (2.96)$$

$$F = \frac{1}{2} \left[(1 - g_p^a) \langle 0 | \rho_m | 0 \rangle + g_p^a \langle 0 | \rho_p^a | 0 \rangle + (1 - g_p^b) \langle \pi/2 | \rho_m | \pi/2 \rangle + g_p^b \langle \pi/2 | \rho_p^b | \pi/2 \rangle \right] \Rightarrow \quad (2.97)$$

$$F = \frac{1}{2} + \frac{g_p^a + g_p^b}{4} , \quad (2.98)$$

pois $\langle 0 | \rho_m | 0 \rangle = \langle \pi/2 | \rho_m | \pi/2 \rangle = 0,5$ e $\langle 0 | \rho_p^a | 0 \rangle = \langle \pi/2 | \rho_p^b | \pi/2 \rangle = 1$, sendo esta última igualdade devida à escolha apropriada das partes puras de ρ_a e ρ_b na Fig. 2.18. O valor máximo da fidelidade é 1 ($g_p^a = g_p^b = 1$, portanto sem distorção) e o mínimo 0,5 ($g_p^a = g_p^b = 0$).

Como visto, um estado puro, ao ser enviado pelo canal, sofre descoerência e se torna misto. Podemos pensar em colocar um dispositivo, representado pelo operador $\hat{U}$, na saída do canal, de forma a fazer com que o estado misto na saída se aproxime ao máximo do estado inicial. Suponhamos que, ao enviar o estado puro ρ_i pelo canal este evolua para o estado misto ρ_s , e este, por sua vez, ao passar pelo dispositivo corretor, evolua para o estado ρ_f . Queremos que operador $\hat{U}$ seja tal que a condição $K(\rho_i, \rho_f) < K(\rho_i, \rho_s)$ seja satisfeita. A ação do operador $\hat{U}$, no estado misto ρ_s , é dada por:

$$\rho_f = \hat{U} \rho_s \hat{U}^\dagger = (1 - g_p^s) \hat{U} \rho_m \hat{U}^\dagger + g_p^s \hat{U} \rho_p^s \hat{U}^\dagger = (1 - g_p^s) \rho_m + g_p^s \hat{U} \rho_p^s \hat{U}^\dagger . \quad (2.99)$$

Portanto, a ação do dispositivo corretor não altera o grau de pureza do estado quântico, mas altera a parte pura do mesmo. Se os estados considerados são do tipo mostrado nas Eqs. (2.78) e (2.79), então a ação de $\hat{U}$ deve ser no sentido de aproximar os ângulos das partes puras. Para o sistema da Fig. 2.18 nada mais pode ser feito, pois os estados puros iniciais e os mistos finais já têm os mesmos ângulos, situação em que a máxima informação acessível também já é alcançada, Fig 2.19.

2.4 Considerações Sobre Estados Quânticos Entrelaçados

Estados quânticos entrelaçados (correlação quântica) [Apêndice A] são usados em criptografia quântica [Apêndice C] e teleportação de qubits [Apêndice F], bem como

modelam o processo de medição de um observável [Apêndice F]. Por isso, há grande interesse na compreensão destes estados. Um processo de medição é mostrado na Fig. 2.21. Nela, ρ_a é o estado quântico a ser medido, σ é o estado inicial do aparelho de medida, ρ_b é o estado final para o qual ρ_a evoluiu e ρ_e é o estado final do aparelho de medida.

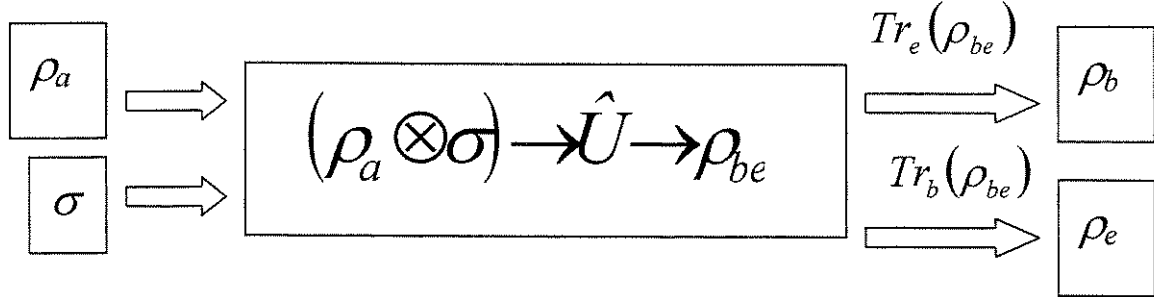


Fig. 2.21 - Processo de medição.

$\hat{U}$ é o operador unitário que representa a medição. A aplicação de $\hat{U}$ no estado produto $(\rho_a \otimes \sigma)$ gera um estado entrelaçado ρ_{be} . Cada parte individual do estado entrelaçado é obtido através do traço parcial em relação à outra parte, ou seja, os graus quânticos de liberdade da outra parte são desconsiderados. Portanto, os estados finais, após a medição, são dados por [Apêndice F]:

$$\rho_b = Tr_e [\hat{U}(\rho_a \otimes \sigma) \hat{U}^\dagger] \quad (2.100)$$

$$\rho_e = Tr_b [\hat{U}(\rho_a \otimes \sigma) \hat{U}^\dagger]. \quad (2.101)$$

Da Fig. 2.21 temos que, ρ_b é o estado na saída do processo em que ρ_a é a entrada. Por isso, quanto mais próximo ρ_b estiver de ρ_a , menor o grau de distúrbio que o operador $\hat{U}$ causou. Entretanto, quando isso acontece, ρ_e e σ também são próximos e, portanto, pouca informação é ganha no processo. O contrário também é verdade, quanto maior a distância entre ρ_e e σ maior a quantidade de informação ganha e maior, também, o distúrbio causado por $\hat{U}$. O resultado da medição é obtido fazendo-se uma medida de von Neumann em ρ_e . Como ρ_e e ρ_b são entrelaçados, o resultado arbitrário $|\phi_e\rangle$, de uma medida em ρ_e , implica univocamente que $\rho_b = |\phi_b\rangle\langle\phi_b|$, onde $|\phi_b\rangle$ é o estado conjugado a $|\phi_e\rangle$. Uma forma geral do operador $\hat{U}$, com elementos reais, é:

$$\hat{U}(\Omega, \Psi) = \begin{bmatrix} \cos(\Omega)\cos(\Psi) & -\cos(\Omega)\sin(\Psi) & -\sin(\Omega)\cos(\Psi) & \sin(\Omega)\sin(\Psi) \\ \cos(\Omega)\sin(\Psi) & \cos(\Omega)\cos(\Psi) & -\sin(\Omega)\sin(\Psi) & -\sin(\Omega)\cos(\Psi) \\ \sin(\Omega)\sin(\Psi) & \sin(\Omega)\cos(\Psi) & \cos(\Omega)\sin(\Psi) & \cos(\Omega)\cos(\Psi) \\ \sin(\Omega)\cos(\Psi) & -\sin(\Omega)\sin(\Psi) & \cos(\Omega)\cos(\Psi) & -\cos(\Omega)\sin(\Psi) \end{bmatrix}. \quad (2.102)$$

Para uma medição padrão de von Neumann temos $\Omega = \Psi = 0$ [Ref. 2.13]. A Tabela 2.5 apresenta os resultados de uma medição de von Neumann com o esquema da Fig. 2.21.

Nela, percebemos que os estados finais são diretamente correlacionados, ou seja, medições em ρ_e e ρ_b resultam ambas no mesmo estado.

σ	ρ_a	ρ_b	ρ_e	Evolução
$ 0\rangle\langle 0 $	$ 0\rangle\langle 0 $	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	$ 0\rangle\langle 0 \xrightarrow{\hat{U}} 0\rangle\langle 0 $
$ 0\rangle\langle 0 $	$ \pi/2\rangle\langle \pi/2 $	$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$	$ \pi/2\rangle\langle 0 \xrightarrow{\hat{U}} \pi/2\rangle\langle \pi/2 $
$ 0\rangle\langle 0 $	$ \pi/4\rangle\langle \pi/4 $	$\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$	$\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$	$ \pi/4\rangle\langle 0 \xrightarrow{\hat{U}} \sqrt{2}^{-1} (0\rangle\langle 0 + \pi/2\rangle\langle \pi/2)$

Tabela 2.5 - Medição de von Neumann.

Se o estado inicial do aparelho de medição for $\sigma = |\pi/2\rangle\langle \pi/2|$, os estados finais são anticorrelacionados, ou seja, medidas em ρ_e e ρ_b resultam em estados ortogonais:

$$(\alpha|0\rangle + \beta|\pi/2\rangle) |\pi/2\rangle \xrightarrow{\hat{U}} \alpha|0\rangle|\pi/2\rangle + \beta|\pi/2\rangle|0\rangle. \quad (2.103)$$

Em uma situação mais geral, vamos analisar o comportamento da configuração mostrada na Fig. 2.21, quando os estados iniciais são mistos:

$$\rho_a \otimes \sigma = p_{00}(\rho_m \otimes \rho_m) + p_{01}(\rho_m \otimes \rho_p^\sigma) + p_{10}(\rho_p^a \otimes \rho_m) + p_{11}(\rho_p^a \otimes \rho_p^\sigma). \quad (2.104)$$

onde $p_{00} = (1 - g_p^a)(1 - g_p^\sigma)$, $p_{01} = (1 - g_p^a)g_p^\sigma$, $p_{10} = (1 - g_p^\sigma)g_p^a$, $p_{11} = g_p^a g_p^\sigma$. Usando as formas dadas nas Eqs. (2.78) e (2.79), com $\rho_a(g_p^a, \theta)$ e $\sigma(g_p^\sigma, \varphi)$, temos:

$$\rho_m \otimes \rho_m = \frac{1}{4} I \quad (2.105)$$

$$\rho_m \otimes \rho_p^\sigma = \frac{1}{2} \begin{pmatrix} \cos^2(\varphi) & \cos(\varphi)\sin(\varphi) & 0 & 0 \\ \cos(\varphi)\sin(\varphi) & \sin^2(\varphi) & 0 & 0 \\ 0 & 0 & \cos^2(\varphi) & \cos(\varphi)\sin(\varphi) \\ 0 & 0 & \cos(\varphi)\sin(\varphi) & \sin^2(\varphi) \end{pmatrix} \quad (2.106)$$

$$\rho_p^a \otimes \rho_m = \frac{1}{2} \begin{pmatrix} \cos^2(\theta) & 0 & \cos(\theta)\sin(\theta) & 0 \\ 0 & \cos^2(\theta) & 0 & \cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & 0 & \sin^2(\theta) & 0 \\ 0 & \cos(\theta)\sin(\theta) & 0 & \sin^2(\theta) \end{pmatrix} \quad (2.107)$$

$$\rho_p^a \otimes \rho_p^\sigma = \begin{pmatrix} c^2(\theta)c^2(\varphi) & c^2(\theta)c(\varphi)s(\varphi) & c(\theta)s(\theta)c^2(\varphi) & c(\theta)s(\theta)c(\varphi)s(\varphi) \\ c^2(\theta)c(\varphi)s(\varphi) & c^2(\theta)s^2(\varphi) & c(\theta)s(\theta)c(\varphi)s(\varphi) & c(\theta)s(\theta)s^2(\varphi) \\ c(\theta)s(\theta)c^2(\varphi) & c(\theta)s(\theta)c(\varphi)s(\varphi) & s^2(\theta)c^2(\varphi) & s^2(\theta)c(\varphi)s(\varphi) \\ c(\theta)s(\theta)c(\varphi)s(\varphi) & c(\theta)s(\theta)s^2(\varphi) & s^2(\theta)c(\varphi)s(\varphi) & s^2(\theta)s^2(\varphi) \end{pmatrix} \quad (2.108)$$

onde I é a matriz identidade (4x4), c é a simplificação de cosseno e s a de seno. As matrizes densidades dos sistemas individuais são obtidas por:

$$\rho_b = p_{00}Tr_e(\hat{U}\rho_m \otimes \rho_m \hat{U}^+) + p_{01}Tr_e(\hat{U}\rho_m \otimes \rho_p^\sigma \hat{U}^+) + p_{10}Tr_e(\hat{U}\rho_p^a \otimes \rho_m \hat{U}^+) + p_{11}Tr_e(\hat{U}\rho_p^a \otimes \rho_p^\sigma \hat{U}^+) \quad (2.109)$$

$$\rho_e = p_{00}Tr_b(\hat{U}\rho_m \otimes \rho_m \hat{U}^+) + p_{01}Tr_b(\hat{U}\rho_m \otimes \rho_p^\sigma \hat{U}^+) + p_{10}Tr_b(\hat{U}\rho_p^a \otimes \rho_m \hat{U}^+) + p_{11}Tr_b(\hat{U}\rho_p^a \otimes \rho_p^\sigma \hat{U}^+). \quad (2.110)$$

Neste momento, para simplificação, optamos por um operador $\hat{U}$ com $\Omega = 0$:

$$\hat{U}(\Psi) = \begin{pmatrix} \cos(\Psi) & -\sin(\Psi) & 0 & 0 \\ \sin(\Psi) & \cos(\Psi) & 0 & 0 \\ 0 & 0 & \sin(\Psi) & \cos(\Psi) \\ 0 & 0 & \cos(\Psi) & -\sin(\Psi) \end{pmatrix}. \quad (2.111)$$

Substituindo as Eqs. (2.105)-(2.108) e (2.111) em (2.109) e (2.110) obtemos:

$$\rho_b = (1 - g_p^a)\rho_m + g_p^a \begin{pmatrix} \cos^2(\theta) & g_p^\sigma \sin[2(\varphi + \Psi)]\cos(\theta)\sin(\theta) \\ g_p^\sigma \sin[2(\varphi + \Psi)]\cos(\theta)\sin(\theta) & \sin^2(\theta) \end{pmatrix} \quad (2.112)$$

$$\rho_e = (1 - g_p^\sigma)\rho_m + g_p^\sigma \begin{pmatrix} \{1 + g_p^a \cos(2\theta)\cos[2(\varphi + \Psi)]\}/2 & \sin[2(\varphi + \Psi)]/2 \\ \sin[2(\varphi + \Psi)]/2 & \{1 - g_p^a \cos(2\theta)\cos[2(\varphi + \Psi)]\}/2 \end{pmatrix}. \quad (2.113)$$

Na equação de ρ_b podemos perceber claramente a influência do processo de medição em ρ_a . Trabalhando com as Eqs. (2.112) e (2.113), encontramos os graus de pureza de ρ_b e ρ_e :

$$g_p^b = g_p^a \sqrt{1 - \{1 - (g_p^\sigma)^2 \sin^2[2(\varphi + \Psi)]\} \sin^2(2\theta)} \quad (2.114)$$

$$g_p^e = g_p^\sigma \sqrt{1 - [1 - (g_p^a)^2 \cos^2(2\theta)] \cos^2[2(\varphi + \Psi)]}. \quad (2.115)$$

Como podemos observar na Eq. (2.114), $g_p^b \leq g_p^a$, ou seja, o processo aumenta a entropia (incerteza) do sistema. Agora, é importante verificarmos a intensidade da correlação entre os estados finais, ρ_b e ρ_e , através de uma medição de entrelaçamento. As medições de

entrelaçamento são complexas e, em alguns casos, não há uma forma definida de calculá-las [Refs. 2.14, 2.15]. Por isso, optamos pelo uso do índice de correlação I_c como medida. É importante frisar que este índice não distingue a correlação quântica da correlação clássica. Ele é dado por [Apêndice F, Refs. 2.16, 2.17]:

$$I_c = S_b + S_e - S_{be} , \quad (2.116)$$

onde S_b e S_e são as entropias de von Neumann das partes individuais e S_{be} é a entropia do estado conjunto. O valor mínimo do índice de correlação é $I_c = 0$ e acontece quando os estados individuais não são entrelaçados. Por outro lado, o valor máximo do índice de correlação é $I_c = 2S_b$ e acontece quando o estado conjunto entrelaçado é um estado puro, $S_{be} = 0$. Nesta situação $S_b = S_e$. Temos ainda que, quando os estados finais ρ_b e ρ_e são puros, $S_b = S_e = 0$, e o índice de correlação se anula devido a desigualdade de Araki e Lieb: $|S_b - S_e| \leq S_{be} \leq S_b + S_e$ [Apêndice F, Refs. 2.16, 2.17]. A Fig. 2.22 mostra a variação do índice de correlação de ρ_{be} com os graus de pureza dos estados iniciais $\rho_a(g_p^a, \theta = \pi/2)$ e $\sigma(g_p^\sigma, \varphi = 0)$, usando o operador $\hat{U}(\Psi = \pi/2)$.

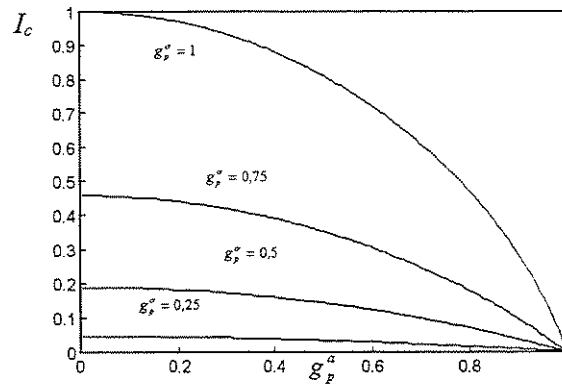


Fig. 2.22 - $I_c \times g_p^a$

É interessante observar que, para os valores usados, só há correlação enquanto ρ_a e σ forem estados mistos. Até o presente momento temos visto o esquema da Fig. 2.21 apenas como um processo de medição. Consideremos, agora, a Fig. 2.21 como parte de um sistema de comunicações quânticas usando estados entrelaçados. Cada parte individual do sistema é enviada a um usuário diferente através de um canal. Suponhamos, inicialmente, que os canais sejam sem ruído e representados pelos operadores unitários $\hat{U}_1$ e $\hat{U}_2$. A Fig. 2.23 mostra a configuração.

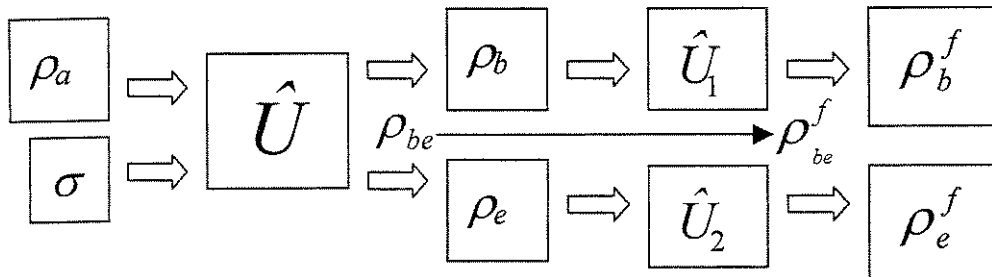


Fig. 2.23 - Transmissão de estados entrelaçados.

Da Fig. 2.23 vemos que cada parte individual evolui segundo o operador que representa o seu canal:

$$\rho_b^f = \hat{U}_1 \rho_b \hat{U}_1^+ \quad (2.117)$$

$$\rho_e^f = \hat{U}_2 \rho_e \hat{U}_2^+ , \quad (2.118)$$

enquanto que o estado conjunto evolui segundo a equação:

$$\rho_{be}^f = (\hat{U}_1 \otimes \hat{U}_2) \rho_{be} (\hat{U}_1 \otimes \hat{U}_2)^+ . \quad (2.119)$$

Usando (2.119) temos também que:

$$\rho_b^f = \text{Tr}_e(\rho_{be}^f) \quad (2.120)$$

$$\rho_e^f = \text{Tr}_b(\rho_{be}^f) . \quad (2.121)$$

Como os canais foram representados por operadores unitários, o grau de pureza, e portanto também a entropia, não se alteram. Logo, o índice de correlação também permanece constante $I_c(\rho_{be}^f) = I_c(\rho_{be})$. Por outro lado, se os canais 1 e 2 são ruidosos, podemos representá-los por uma mistura de operadores unitários, $\{\hat{U}_{1i}, p_i\}$ para o canal 1 e $\{\hat{U}_{2j}, q_j\}$ para o canal 2, onde p_i e q_j são as probabilidades associadas a $\hat{U}_1$ e $\hat{U}_2$, respectivamente. Com isto, o estado conjunto final passa a ser dado por:

$$\rho_{be}^f = \sum_i \sum_j p_i q_j (\hat{U}_{1i} \otimes \hat{U}_{2j}) \rho_{be} (\hat{U}_{1i} \otimes \hat{U}_{2j})^+ . \quad (2.122)$$

Desta forma, se as partes individuais de um estado entrelaçado inicialmente puro, são enviadas através de canais ruidosos, o estado entrelaçado puro evolui para um estado entrelaçado misto, Fig. 2.24.

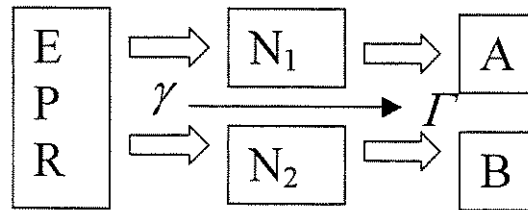


Fig. 2.24 - Transmissão de um estado entrelaçado por um canal ruidoso. γ (puro) $\rightarrow \Gamma$ (misto).

Na Fig. 2.24, uma fonte (EPR) gera um par de fótons entrelaçados num estado puro γ e envia um fóton do par para Alice (A) e o outro para Bob (B), através dos canais ruidosos N_1 e N_2 . O estado entrelaçado que Alice e Bob compartilharão é o estado misto Γ . O entendimento de um estado misto entrelaçado é realmente complicado. Entretanto, antes de comentarmos um pouco mais sobre estados mistos entrelaçados, vejamos uma outra medida

de entrelaçamento, chamada *entrelaçamento* E . Assim, se o estado entrelaçado γ , compreendendo os subsistemas ρ_a e ρ_b , é puro, então uma medida do entrelaçamento é [Refs. 2.14, 2.15]:

$$E(\gamma) = S(\rho_a) = S(\rho_b) , \quad (2.122)$$

ou seja, o entrelaçamento é igual à entropia dos sistemas individuais. Agora, um estado misto Γ é considerado entrelaçado ou não-local se ele não pode ser escrito como uma mistura de produto de estados [Ref. 2.14]:

$$\Gamma \neq \sum_i p_i (\rho_a^i \otimes \rho_b^i) . \quad (2.123)$$

Além disso, um estado entrelaçado misto é uma mistura de estados entrelaçados puros, γ_i [Ref. 2.14]:

$$\Gamma = \sum_i p_i \gamma_i . \quad (2.124)$$

Uma medida do entrelaçamento de um estado entrelaçado misto Γ , chamada *entrelaçamento de formação*, é dada pelo menor entrelaçamento médio de todas as possíveis expansões da forma (2.124) que resultem no mesmo Γ [Refs. 2.14, 2.15]:

$$E(\Gamma) = \min \left\{ \sum_i p_i E(\gamma_i) \middle| \sum_i p_i \gamma_i = \Gamma \right\} . \quad (2.125)$$

Apresentaremos, agora, uma medida de entrelaçamento mais direta. Suponhamos, inicialmente, que as partes individuais do estado conjunto puro γ , pertencente ao espaço $H_A \otimes H_B$, sejam dadas pela matrizes densidades ρ_a e ρ_b . Então, se γ é um estado entrelaçado, temos necessariamente que: 1) $\gamma \neq \rho_a \otimes \rho_b$, 2) $\rho_a = Tr_b(\gamma)$ e $\rho_b = Tr_a(\gamma)$. É fácil verificar que qualquer estado da forma:

$$\gamma = \rho_a \otimes \rho_b + R \quad (2.126)$$

com a matriz R (4x4) dada por:

$$R = \begin{pmatrix} k & q & p & y \\ q & -k & w & -p \\ p & z & -k & -q \\ x & -p & -q & k \end{pmatrix} \quad (2.127)$$

obedece às condições 1 e 2. Os valores dos elementos de R são determinados pelo processo físico que gera o entrelaçamento. Se supusermos que o estado entrelaçado γ resulta da aplicação do operador $\hat{U}$ no estado conjunto não entrelaçado ($\rho \otimes \sigma$), temos:

$$R = \hat{U}(\rho \otimes \sigma)\hat{U}^+ - (\rho_a \otimes \rho_b) = \hat{U}(\rho \otimes \sigma)\hat{U}^+ - \text{Tr}_b[\hat{U}(\rho \otimes \sigma)\hat{U}^+] \otimes \text{Tr}_a[\hat{U}(\rho \otimes \sigma)\hat{U}^+] \quad (2.128)$$

Observando a Eq. (2.126) vemos que uma medida de entrelaçamento deve depender apenas de R . Em particular, quando $R = [0]$ o entrelaçamento deve ser nulo. Tomamos então, como medida de entrelaçamento, a distância de Kolmogorov entre o estado entrelaçado e o estado produto das matrizes densidades individuais:

$$E_R = K(\gamma, \rho_a \otimes \rho_b) = \frac{1}{2} \text{Tr}(|\gamma - \rho_a \otimes \rho_b|) = \frac{1}{2} \text{Tr}(|R|) \quad (2.129)$$

Em outras palavras, E_R é uma medida de distância entre o estado entrelaçado, γ , e o estado não entrelaçado, $(\rho_a \otimes \rho_b)$, os quais geram as mesmas matrizes densidades individuais, ρ_a e ρ_b . Agora, se o estado entrelaçado, Γ , é misto, temos:

$$\Gamma = \sum_i p_i \gamma_i = \sum_i p_i (\rho_a^i \otimes \rho_b^i + R_i) \quad (2.130)$$

e a medida de entrelaçamento fica da forma:

$$E_R = \frac{1}{2} \text{Tr} \left(\left| \sum_i p_i R_i \right| \right) \leq \sum_i \frac{1}{2} p_i \text{Tr}(|R_i|) = \sum_i p_i E_R^i \quad (2.131)$$

A medida de entrelaçamento E , dada na Eq. (2.122), usa as matrizes individuais, enquanto que a medida da Eq. (2.129) usa a matriz do estado conjunto. Para ilustrar a medida de entrelaçamento proposta, aplicamos o operador $\hat{U}(\Psi)$, Eq. (2.111), com Ψ variando no intervalo $[-\pi, \pi]$, ao estado conjunto não entrelaçado $[\rho(g_p^\rho = 1, \theta = \pi/4) \otimes \sigma(g_p^\sigma = 1, \varphi = 0)]$, e medimos o entrelaçamento dos estados na saída usando as Eqs. (2.122) (entropia) e (2.129) (distância de Kolmogorov). Substituindo os valores dos parâmetros adotados nas Eqs. (2.114) e (2.115), encontramos que os graus de pureza dos estados na saída, ρ_a e ρ_b , são dados por $g_p^a = g_p^b = \sin(2\Psi)$. Sendo estes últimos iguais, temos também que $S_a = S_b$ e, portanto, o estado final entrelaçado é puro, o que justifica o uso da Eq. (2.122). O resultado pode ser visto na Fig. 2.25.

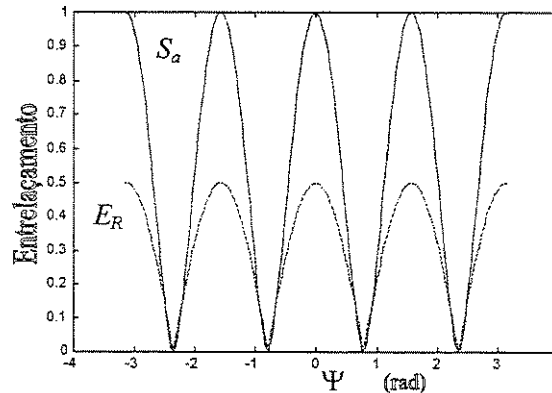


Fig. 2.25 - Medida de entrelaçamento com S_a e E_R para estados puros.

Na Fig. 2.25 vemos que, como medida de entrelaçamento, a medida de distância é equivalente à medida usando a entropia das partes individuais. As duas possuem o mesmo comportamento e alcançam seus valores de pico e de mínimo para os mesmos valores de Ψ . Agora, suponhamos que os estados iniciais sejam $\rho(g_p^\rho = 0,75, \theta = \pi/4) \otimes \sigma(g_p^\sigma = 1, \varphi = 0)$. Com estes valores os graus de pureza dos estados na saída são $g_p^a = 0,75 \sin(2\Psi)$ e $g_p^b = \sin(2\Psi)$; portanto, o estado entrelaçado final é um estado misto. Por isso, usaremos o índice de correlação I_c , Eq. (2.116), como referência. A Fig. 2.26 mostra as formas de I_c e E_R quando Ψ varia no intervalo $[-\pi, \pi]$.

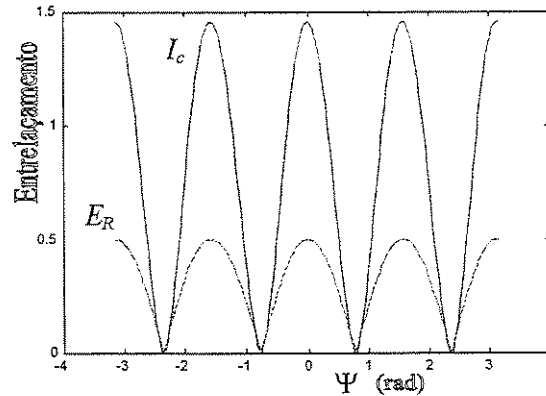


Fig. 2.26 - Medida de entrelaçamento usando I_c e E_R , para estados mistos.

Na Fig. 2.26 podemos observar que o índice de correlação e a medida de entrelaçamento usando distância de Kolmogorov são equivalentes, pois possuem a mesma forma e crescem e decrescem simultaneamente. Comparando, ainda, as Figs. 2.25 e 2.26 vemos que E_R aplica-se indistintamente a estados puros e mistos. É importante frisar que a medida E_R é baseada em conceitos simples e por isso sofre de algumas deficiências que a torna de uso limitado.

CONCLUSÕES DO CAPÍTULO II

Neste capítulo, enfatizamos as já conhecidas semelhanças entre as matrizes densidade de estados, ρ , e coerência, J . Iniciamos aplicando os conceitos de probabilidade dos resultados de medições e distinção entre matrizes densidades, probabilidade de erro e distância de Kolmogorov, às matrizes coerências. Com estas semelhanças pudemos tratar um sistema quântico de comunicação polarimétrico, através do uso das matrizes transferência, coerência e parâmetros de Stokes. Assim, com argumentos puramente clássicos, propusemos o uso de um equalizador óptico, tendo como estrutura física a seqüência compensador-rotacionador-compensador, $C(\delta)R(\phi)C(\sigma)$, e o algoritmo de equalização, o qual se utiliza de uma estimativa do comportamento do canal para dar valores corretos às variáveis do equalizador, de forma a tentar recuperar a polarização original em sistemas quânticos polarimétricos a fibra. É importante frisarmos que o equalizador corrige uma fonte de ruído clássica que é a variação da polarização devido à propagação na fibra óptica. Analisamos o comportamento do equalizador através de simulações numéricas, tendo sido adotado um modelo estatístico para as variáveis que modelam o canal (fibra). Dois pontos importantes para o sucesso da equalização do canal são: 1) As variáveis que modelam o canal são supostas variarem lentamente de tal forma que, durante um determinado intervalo de tempo, o canal é invariante constante. 2) O intervalo de tempo entre duas estimativas sucessivas do canal, t_e , deve ser casado com o período de variação do canal, t_f . No caso ótimo temos $t_e = 0,5t_f$. Em particular, notamos, nas simulações, que a probabilidade de erro cai de aproximadamente 50 %, na ausência do equalizador, para próximo de 0,15 % no caso ótimo.

Dando seqüência às semelhanças entre ρ e J , dividimos a matriz densidade na soma de duas outras, uma correspondendo a um estado puro e a outra a um estado maximamente misto. Definimos, então, o grau de pureza, g_p , semelhante ao grau de polarização, que mede o quanto um estado é puro. Verificamos que o grau de pureza é relacionado à entropia do estado. Com isto, pusemos a informação mútua, a fidelidade e a distância de Kolmogorov como funções do grau de pureza. Em particular, demos uma visão geométrica da distância de Kolmogorov entre os estados quânticos, no espaço bidimensional, que não possuem valores complexos nas componentes fora diagonal principal de ρ .

Por fim, demos uma rápida passagem pelos estados quânticos entrelaçados. Descrevemos a obtenção de estados entrelaçados a partir da aplicação de um operador unitário a um estado conjunto não-entrelaçado e, também, algumas medidas de entrelaçamento para estados entrelaçados puros e mistos. Mostramos, através de uma simulação, a variação do índice de correlação de um estado entrelaçado com os graus de pureza dos estados iniciais que o gera. Finalmente, propusemos a distância de Kolmogorov entre um estado entrelaçado e o estado não-entrelaçado que fornecem as mesmas matrizes densidades parciais, como uma medida de entrelaçamento, E_R . Verificamos que, nas condições especificadas, E_R é equivalente ao índice de correlação, I_c , e ao entrelaçamento medido pela entropia de um dos sistemas parciais, quando o estado entrelaçado é puro, E .

CAPÍTULO III

DISPOSITIVOS ÓPTICOS NÃO-LINEARES EM SISTEMAS DE COMUNICAÇÕES QUÂNTICAS

3.1 Introdução

Neste capítulo consideraremos o comportamento não-linear na propagação de pulsos de alta intensidade em fibras ópticas, segundo as aplicações de interesse desta tese. O comportamento não-linear é devido à variação do índice de refração da fibra com a intensidade do pulso, o chamado efeito Kerr. Em particular, apresentaremos, de forma sucinta, uma vez que há vasta bibliografia sobre efeitos não-lineares em fibras [Refs. 3.1, 3.2], o ressonador não-linear a fibra, RNL, o acoplador não-linear a fibra, ANL, e efeitos de birrefringência na propagação. Após a caracterização numérica dos dispositivos não-lineares, apresentaremos a utilização dos mesmos como parte integrante de um sistema de comunicações quânticas.

3.2 Ressonador Não-linear a Fibra - RNL

O RNL é mostrado na Fig. 3.1. Ele é basicamente um sistema não-linear (fibra com efeito Kerr) realimentado (via acoplador) e, portanto, apresenta toda a rica dinâmica característica desta configuração, como a duplicação de períodos e caos [Refs. 3.3 - 3.6], segundo a variação de um parâmetro do sistema que, em geral, pela facilidade de atuação, é a intensidade dos pulsos incidentes no RNL.

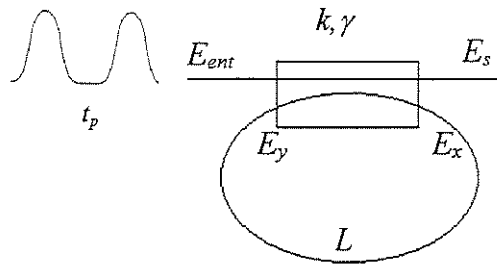


Fig. 3.1 - Ressonador não-linear a fibra, RNL.

A fibra do ressonador, de comprimento L , é monomodo e do tipo que preserva a polarização. A luz incidente do laser é suposta ser linearmente polarizada. O acoplador é considerado pontual (sem dimensões físicas), k é o coeficiente de acoplamento e γ representa a perda intrínseca do acoplador, ambos referentes à intensidade. A evolução da envoltória do campo no ressonador, em regime estacionário, é dada por [Refs. 3.3, 3.4]:

$$E_s(n, t) = (1 - \gamma)^{\frac{1}{2}} \left[(1 - k)^{\frac{1}{2}} E_{ent}(n, t) + ik^{\frac{1}{2}} E_y(n, t) \exp(i\beta L) \right] \quad (3.1)$$

$$E_x(n, t) = (1 - \gamma)^{\frac{1}{2}} \left[ik^{\frac{1}{2}} E_{ent}(n, t) + (1 - k)^{\frac{1}{2}} E_y(n, t) \exp(i\beta L) \right] \quad (3.2)$$

$$E_y(n, t) = G[E_x(n - 1, t)] , \quad (3.3)$$

onde n é o número da volta no ressonador. O operador G , na Eq. (3.3), é obtido via integração da equação não-linear de Schrödinger, ENLS [Refs. 3.1, 3.2]:

$$\frac{\partial E}{\partial z} = -\frac{i}{2} \beta_2 \frac{\partial^2 E}{\partial \tau^2} + \frac{1}{6} \beta_3 \frac{\partial^3 E}{\partial \tau^3} + iR|E|^2 E - \frac{\alpha}{2} E . \quad (3.4)$$

onde τ é o tempo normalizado, dado por $\tau = t - \beta_1 z$ [Ref. 3.1] e o coeficiente de não-linearidade, R , é dado por [Ref. 3.1]:

$$R = \frac{n_2 k_0 \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} |f(x, y)|^4 dx dy}{\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} |f(x, y)|^2 dx dy} , \quad (3.5)$$

onde n_2 é o coeficiente não-linear do índice de refração [Ref. 3.1], k_0 é a constante de propagação no vácuo e $f(x, y)$ é a distribuição transversal (modo) do campo na fibra. β_1 é o inverso da velocidade de grupo V_g , β_2 é a dispersão da velocidade de grupo, α é o coeficiente de atenuação da fibra, β é a constante de propagação do modo na fibra e, portanto, βL é o deslocamento linear de fase devido à propagação na fibra. Para as simulações, o RNL é alimentado por um trem de pulsos, de período t_p , da forma secante hiperbólica. Assumimos que existe um perfeito sincronismo entre o tempo de uma volta no RNL, $t_r = V_g/L$, e o período dos pulsos, isto é, o comprimento da fibra é tal que permite a perfeita sobreposição temporal do próximo pulso incidente no ressonador com o precedente dele e, portanto, $t_r = t_p$. Os pulsos de entrada no RNL são dados por:

$$E_{ent} = N \sqrt{\frac{|\beta_2|}{RT_1^2}} \operatorname{sech} \left(\frac{\tau}{T_1} \right) \quad (3.6)$$

$$T_1 = \frac{T_0}{1,6574544} \quad (3.7)$$

sendo T_0 a largura do pulso e N um número real que controla a intensidade do pulso. Para analisar o comportamento do RNL usamos, como variável de observação, a energia dos pulsos na saída do mesmo:

$$S(n) = \int_{-\infty}^{\infty} |E_s(n, \tau)|^2 d\tau . \quad (3.8)$$

As Figs. 3.1 - 3.5, a seguir, apresentam os resultados das simulações cujos parâmetros são apresentados na Tabela 3.1.

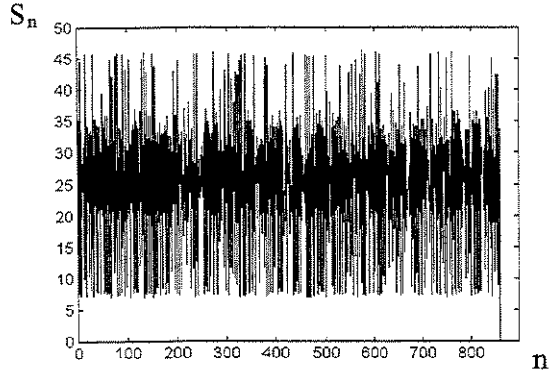


Fig. 3.1 - Energia dos pulsos na saída do RNL. (SIM-1)

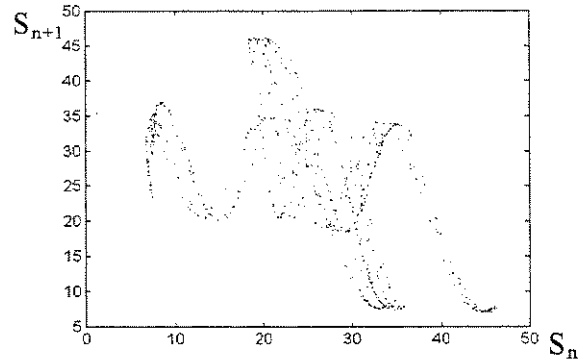


Fig. 3.2 - Plano de fase: $S_{n+1} \times S_n$. (SIM-1)

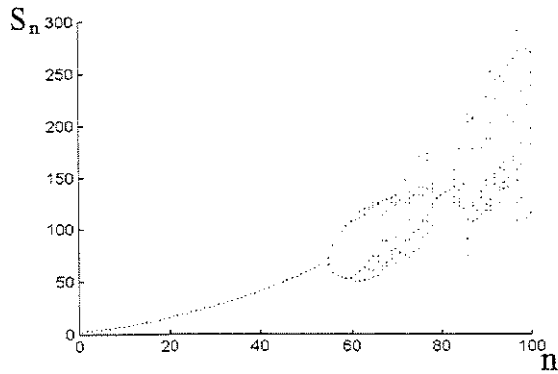


Fig. 3.3 - Diagrama de bifurcação. (SIM-2)

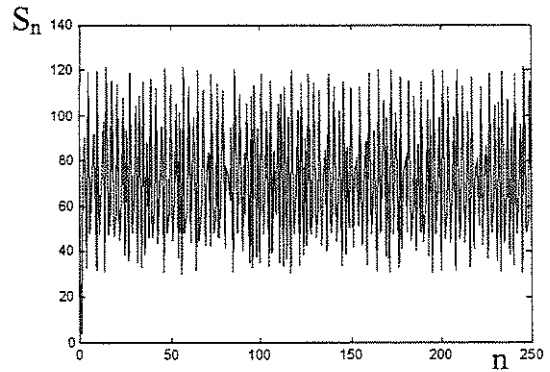


Fig. 3.4 - Energia dos pulsos na saída do RNL. (SIM-3)

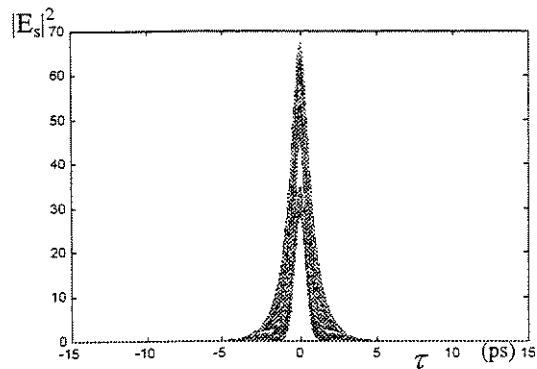


Fig. 3.5 - Pulsos na saída do RNL. (SIM-3)

SIM	N	βL [rad]
1	1,5	$(0,9+15.10^8)\pi$
2	[0,25 , 2,5]	$(1,54+10^8)\pi$
3	1,75	$(0,9+15.10^7)\pi$
$\lambda = 1,55 \mu\text{m}$, $\beta_2 = -20,4 \text{ ps}^2/\text{km}$, $\beta_3 = 0,1 \text{ ps}^3/\text{km}$, $\alpha = 0,3 \text{ dB/km}$, $R = 1,3 \text{ W}^{-1}\text{km}^{-1}$, $T_0 = 2 \text{ ps}$, $k=0,95$ e $\gamma=0,05$		

Tabela 3.1 - Valores dos parâmetros do RNL usados nas simulações.

Na Fig. 3.1 vemos que a energia dos pulsos na saída do RNL varia de forma aperiódica (pelo ao menos nas voltas apresentadas) indicando que o RNL está operando em regime caótico. Na Fig. 3.2, usando os dados mostrados na Fig. 3.1, traçamos o plano de fase do sistema e nele podemos observar um desenho que lembra um atrator estranho. Apesar de não termos usado métodos matemáticos rigorosos, como cálculo dos expoentes de Lyapunov e da informação de Kolmogorov [Ref. 3.7], para afirmar que a energia na saída do RNL esta realmente variando caoticamente, as Figs. 3.1 e 3.2 deixam poucas dúvidas sobre isso. Na Fig. 3.3 vemos um diagrama de bifurcação mostrando a duplicação de períodos, antes de se chegar ao regime caótico, à medida que o parâmetro N cresce. A Fig. 3.4 mostra novamente, a variação caótica, em 250 voltas, da energia dos pulsos na saída do RNL usando um menor comprimento de fibra e maior intensidade de entrada que os usados na SIM-1. Na Fig. 3.5 temos que, apesar da variação de energia apresentada na Fig 3.4, a forma dos pulsos nas saída do RNL não sofre mudanças fortes ou drásticas.

3.2.1 - Controle e Sincronização de RNLs

Tradicionalmente, o comportamento caótico, em engenharia, é visto como um problema a ser evitado. Uma das poucas utilizações seria como gerador de uma variável pseudo-aleatória. Entretanto, com o desenvolvimento de técnicas de controle e sincronização de sistemas caóticos, surgiram aplicações potenciais, como oscilador de período programável e criptografia caótica [Refs. 3.8-3.10].

Quando um sistema está operando em regime caótico, o plano de fase do mesmo apresenta um atrator estranho [Ref. 3.7]. Neste atrator estão mergulhadas inúmeras órbitas periódicas de períodos diversos. O controle de um sistema caótico consiste, basicamente, em forçar o sistema a entrar e permanecer em uma das órbitas, de forma a tornar o sistema periódico. Mudando-se a órbita selecionada muda-se o período de oscilação do sistema. As técnicas de controle desenvolvidas são baseadas na variação temporal, em alguns casos periódica, de um dos parâmetros do sistema [Refs. 3.8, 3.11]. Estas técnicas geralmente fazem uso das equações diferenciais que modelam o sistema físico. Sendo assim, as mesmas não se aplicam no RNL pois, devido à complexidade da ENLS, não dispomos de um modelo fechado para o RNL, isto é, não dispomos de uma forma analítica para o operador G . Para solucionarmos este problema, optamos pelo uso da técnica de inteligência numérica conhecida por lógica nebulosa (*fuzzy*) [Refs. 3.12, 3.13]. A melhor forma de explicar a lógica nebulosa é através de um exemplo. Suponhamos que temos um controlador que, baseado nos valores de duas variáveis de entrada, e_g e e_l , fornece um valor em sua saída, sendo esta representada pela variável cf . As variáveis e_g e e_l assumem valores dentro dos intervalos $[e_g^{min}, e_g^{max}]$ e $[e_l^{min}, e_l^{max}]$, respectivamente, enquanto cf só assume valores no intervalo $[y_{min}, y_{max}]$. Agora, definimos conjuntos dentro dos intervalos segundo expressões lingüísticas. Como todas as variáveis citadas podem assumir valores positivos e negativos, optamos por definir os seguintes conjuntos para todas elas: **negativo alto** (NA), **negativo baixo** (NB), **zero** (Z), **positivo baixo** (PB) e **positivo alto** (PA). Precisamos, agora, de funções, uma para cada conjunto, de valor máximo unitário e com o domínio igual ao intervalo ao qual os conjuntos pertencem, que darão a *possibilidade* do valor da variável em questão pertencer ao referido conjunto. Por exemplo, para a variável e_l o valor e_l^{min} tem possibilidade 1 de pertencer ao conjunto NA , enquanto que o mesmo valor deve ter

possibilidade 0, ou próxima, de pertencer ao conjunto *PA*. Estas funções que dão a possibilidade do valor pertencer a um determinado conjunto são chamadas funções de pertinência (funções *membership*). As Figs. 3.6, 3.7 e 3.8 mostram as funções de pertinência das variáveis de entrada e de saída, respectivamente, para os intervalos $e_g \in [-120, 120]$, $e_l \in [-10, 10]$ e $cf \in [-0,2512, 0,2512]$.

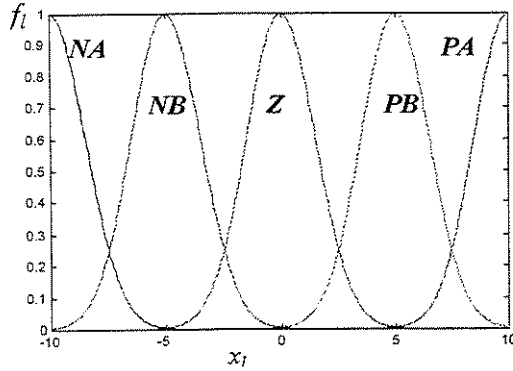


Fig. 3.6 - Funções de pertinência da variável e_l .

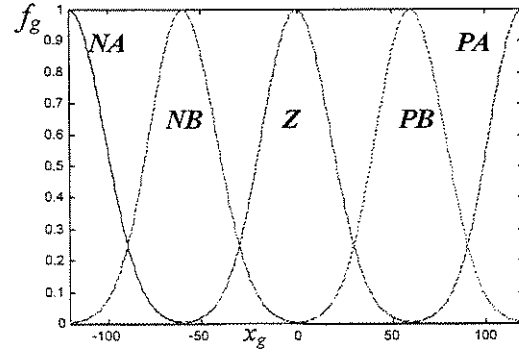


Fig. 3.7 - Funções de pertinência da variável e_g .

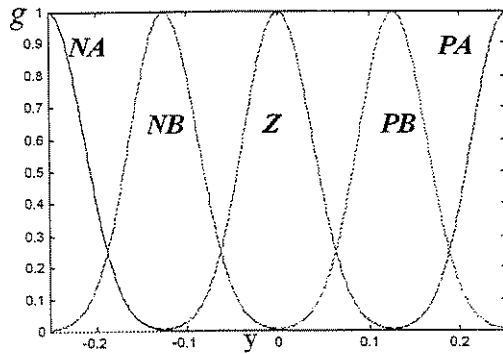


Fig. 3.8 - Funções de pertinência da variável cf .

As funções de pertinência usadas nas Figs. 3.6 - 3.8 são dadas por:

$$f_l^i = \exp \left\{ -88,7228 \left[(x_l - x_l^i) / \Delta e_l \right]^2 \right\} \quad (3.9)$$

$$f_g^i = \exp \left\{ -88,7228 \left[(x_g - x_g^i) / \Delta e_g \right]^2 \right\} \quad (3.10)$$

$$g_i = \exp \left\{ -88,7228 \left[(y - y_i) / \Delta y \right]^2 \right\} \quad (3.11)$$

$$\Delta e_l = e_l^{\max} - e_l^{\min}, \quad \Delta e_g = e_g^{\max} - e_g^{\min}, \quad \Delta y = y_{\max} - y_{\min} \quad (3.12)$$

onde, $i = 1, 2, 3, 4$ e 5 faz correspondência com $[NA \ NB \ Z \ PB \ PA]$, bem como indica a posição nos vetores que contém as coordenadas dos centros das gaussianas:

$$\left[\begin{array}{ccccc} x_l^1 = x_l^{\min} & x_l^2 = x_l^{\min} + \frac{\Delta e_l}{4} & x_l^3 = x_l^{\min} + \frac{\Delta e_l}{2} & x_l^4 = x_l^{\min} + \frac{3\Delta e_l}{4} & x_l^5 = x_l^{\max} \end{array} \right] \quad (3.13)$$

$$\left[\begin{array}{ccccc} x_g^1 = x_g^{\min} & x_g^2 = x_g^{\min} + \frac{\Delta e_g}{4} & x_g^3 = x_g^{\min} + \frac{\Delta e_g}{2} & x_g^4 = x_g^{\min} + \frac{3\Delta e_g}{4} & x_g^5 = x_g^{\max} \end{array} \right] \quad (3.14)$$

$$\left[\begin{array}{ccccc} y_1 = y_{\min} & y_2 = y_{\min} + \frac{\Delta y}{4} & y_3 = y_{\min} + \frac{\Delta y}{2} & y_4 = y_{\min} + \frac{3\Delta y}{4} & y_5 = y_{\max} \end{array} \right] \quad (3.15)$$

Optamos por funções de pertinência na forma de gaussianas, embora pudéssemos usar funções triangulares ou trapezoidais, dentre outras. Tanto a forma como a largura das funções influenciam no comportamento do controlador nebuloso [Refs. 3.12, 3.13].

A ação do controlador é programada através de regras que ligam as variáveis de entrada à variável de saída. As regras são, por exemplo, do tipo:

1 - Se e_g é Negativo Alto e e_l é Zero então cf é Positivo Alto.

ou

2 - Se e_g é Negativo Baixo e e_l é Positivo Alto então cf é Positivo Alto.

ou

3 - Se e_g é Positivo Alto e e_l é Positivo Alto então cf é Negativo Alto

⋮

Portanto, cada regra pergunta a possibilidade dos valores das variáveis de entrada pertencerem a determinados conjuntos, e indica qual o conjunto da variável de saída que deve ser acionado. As diversas regras são ligadas através do operador **ou**. As operações **e** e **ou** são, respectivamente, operações de mínimo e máximo. Na forma de tabela ou matriz temos:

$e_l \backslash e_g$	NA	NB	Z	PB	PA
NA	PA	PA	PA	PA	PA
NB	PA	PB	PB	PB	PA
Z	Z	Z	Z	Z	Z
PB	NA	NB	NB	NB	NA
PA	NA	NA	NA	NA	NA

Tabela 3.2 - Formulação lingüística das regras do controlador nebuloso.

$e_l \backslash e_g$	f_l^1	f_l^2	f_l^3	f_l^4	f_l^5
f_g^1	g_5	g_5	g_5	g_5	g_5
f_g^2	g_5	g_4	g_4	g_4	g_5
f_g^3	g_3	g_3	g_3	g_3	g_3
f_g^4	g_1	g_2	g_2	g_2	g_1
f_g^5	g_1	g_1	g_1	g_1	g_1

Tabela 3.3 - Formulação matemática das regras do controlador nebuloso

O algoritmo de execução das regras é melhor entendido com a formulação matemática das regras mostrada na Tabela 3.3. Assim, dada uma entrada de valores no controlador (e_g, e_l) cada regra é testada. Por exemplo, para a primeira regra temos:

Se e_g é Negativo Alto e e_l é Negativo Alto então cf é Positivo Alto.

Para executá-la, fazemos:

$$s_1 = \min\left(\min\left(f_g^1(e_g), f_l^1(e_l)\right), g_5\right), \quad (3.16)$$

onde a operação min interna é entre dois valores (cálculo da função f_g^1 no ponto $x_g = e_g$ e cálculo da função f_l^1 no ponto $x_l = e_l$), enquanto que a operação min externa é entre um valor, (resultante da operação min interna) e a função, g_5 , tendo como resultado final, a variável s_1 , uma função. Como todas as regras são ligadas pelo operador **ou**, o resultado final da aplicação de todas as regras é:

$$s = \max(s_1, s_2, \dots, s_{25}) , \quad (3.17)$$

que ainda é uma função. De forma resumida, o algoritmo é:

$$s = \max\left(s, \min\left(\min\left(f_g^i(e_g), f_l^j(e_l)\right), Rg(i, j)\right)\right), \quad (3.18)$$

onde $i, j = 1, 2, 3, 4$ e 5 , para que toda a tabela seja percorrida. Rg é a matriz de funções g 's inscrita na Tabela 3.3. A variável s ainda não é a saída do controlador pois ela é conjunto de valores. Para reduzi-la a um valor, empregamos as técnicas de "desnebulização", sendo a mais comumente usada o cálculo do centro de massa [Refs. 3.12, 3.13]; assim, a saída do controlador é:

$$cf = CM(s) = \sum sy / \sum s , \quad (3.19)$$

onde o somatório indica que o sistema considerado é discreto. Agora, usaremos o controlador nebuloso, acima descrito, para controlar o comportamento caótico do RNL [Ref. 3.14]. O diagrama é mostrado na Fig. 3.9.

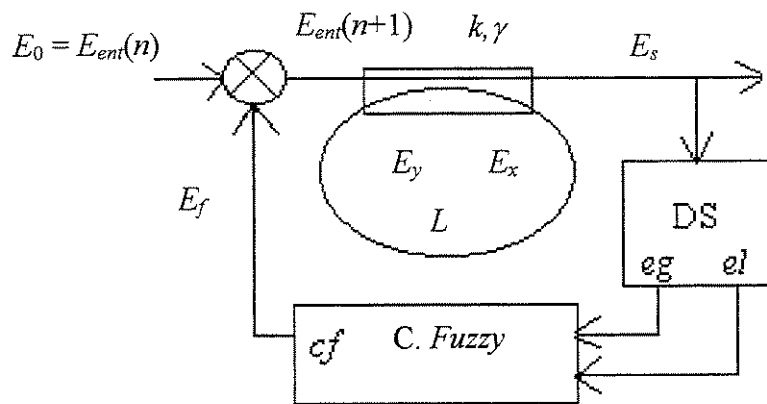


Fig. 3.9 - RNL com controlador nebuloso.

O bloco DS é responsável pela obtenção das variáveis de entrada do controlador a partir do campo de saída do RNL, E_s . As variáveis e_g e e_l são dadas por:

$$e_g = S_n - S_{n-k} \quad (3.20)$$

$$e_l = H_n - H_{n-k} \quad , \quad (3.21)$$

onde

$$S_n = \int_{-\infty}^{\infty} |E_s(n, \tau)|^2 d\tau \quad (3.22)$$

$$H_n = |E_s(n, \tau = 0)|^2 \quad . \quad (3.23)$$

Ou seja, e_g e e_l são, respectivamente, os erros resultantes da comparação da energia e do quadrado do módulo do valor central de E_s , da volta atual com os da k -ésima volta anterior. Estes valores são entregues ao controlador que, segundo as Eqs. (3.9) - (3.19) e as regras das Tabelas 3.2 e 3.3, fornece uma saída que vai atuar diretamente na amplitude do campo incidente no RNL. Antes do controlador ser ligado temos na entrada do RNL:

$$E_{ent}(n, \tau) = E_0 = N \sqrt{|\beta_2|/RT_1^2} \operatorname{sech}(\tau/T_1) \quad , \quad (3.24)$$

onde T_1 é dado em (3.7). Ligando o controlador, os pulsos na entrada do RNL serão:

$$E_{ent}(n+1, \tau) = E_{ent}(n, \tau) + E_f = E_{ent}(n, \tau) + cf \sqrt{|\beta_2|/RT_1^2} \operatorname{sech}(\tau/T_1) \quad . \quad (3.25)$$

Para a simulação da configuração mostrada na Fig. 3.9 usamos, para o RNL, os parâmetros da SIM-3 da Tabela 3.1 (situação de comportamento caótico do RNL) enquanto que, os parâmetros do controlador, bem como os períodos em que o RNL ficou amarrado, são apresentados na Tabela 3.4. Por fim, o controlador nebuloso é ligado apenas na 14ª volta após iniciada a entrada de pulsos. As Figs. 3.10 - 3.17 mostram os resultados das simulações.

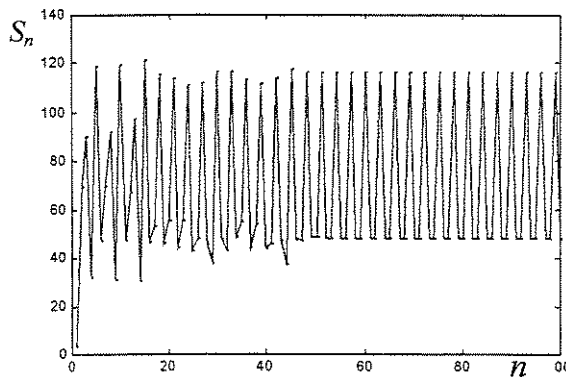


Fig. 3.10 - $S(n) \times n$. (SIM-4)

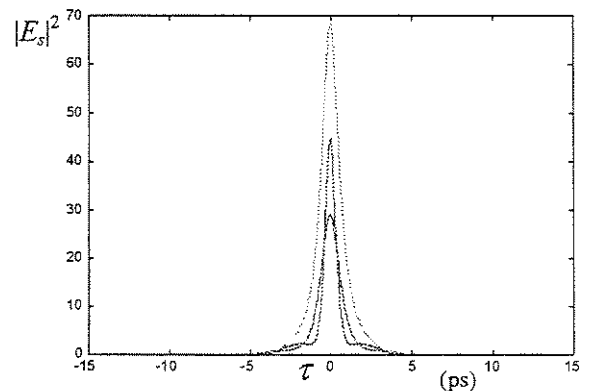


Fig. 3.11 - Pulsos na saída do RNL com controlador. (SIM-4)

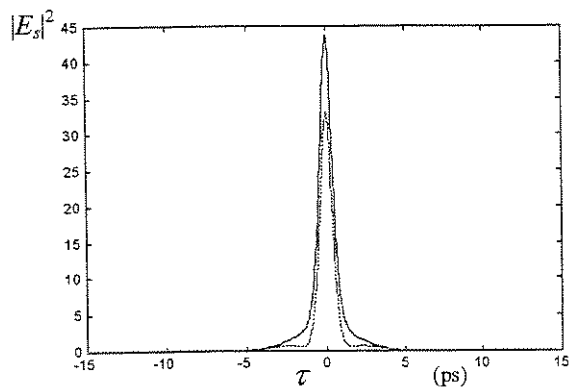


Fig. 3.13 - Pulsos na saída do RNL com controlador. (SIM-5)

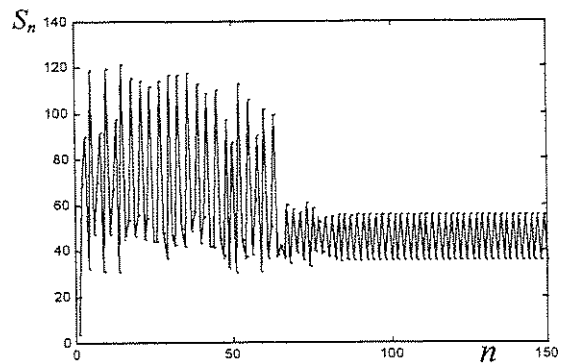


Fig. 3.12 - $S(n) \times n$. (SIM-5)

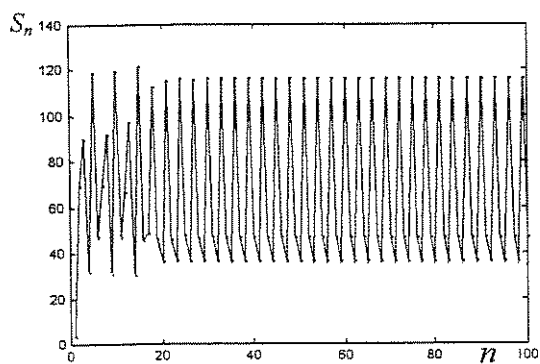


Fig. 3.14 - $S(n) \times n$. (SIM-6)

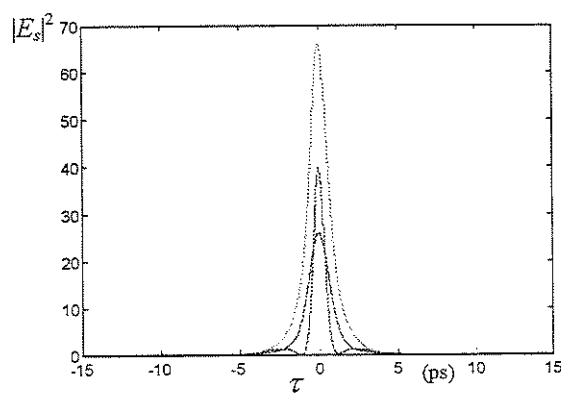


Fig. 3.15 - Pulsos na saída do RNL com controlador. (SIM-6)

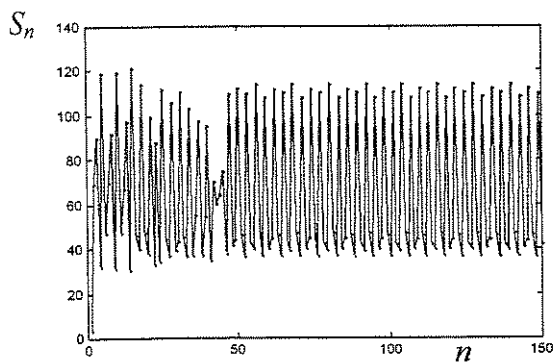


Fig. 3.16 - $S_n \times n$. (SIM-7)

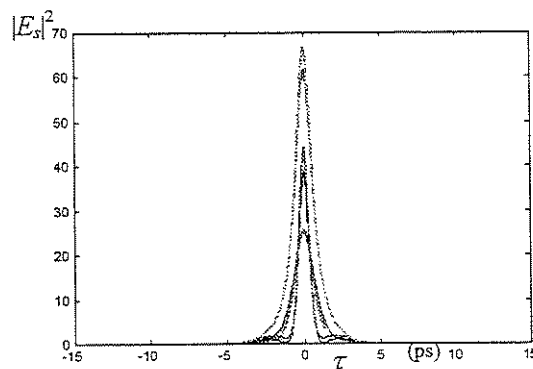


Fig. 3.17 - Pulsos na saída do RNL com controlador. (SIM-7)

SIM	y_{min}^{max}	k	período
4	$\pm 0,2$	1	3
5	$\pm 0,2512$	1	2
6	$\pm 0,2512$	3	3
7	$\pm 0,3$	3	12
N=1,75 $e_{g_{min}}^{max} = \pm 120$ $e_{l_{min}}^{max} = \pm 10$			

Tabela 3.4 - Parâmetros do controlador nebuloso utilizados nas simulações.

Como observado nas Figs. 3.10 - 3.17, em todos os casos o controlador obteve sucesso na tarefa de controlar o comportamento caótico do RNL, embora a duração do transiente seja maior ou menor, dependendo da escolha de parâmetros. Além disso, a forma dos pulsos na saída não sofreram fortes mudanças. Observando os dados da Tabela 3.4 vemos ainda que a escolha da órbita periódica em que o RNL permanece preso depende dos valores de $y_{\min}$ e $y_{\max}$, bem como do atraso k . Portanto, podemos variar o período de oscilação do RNL atuando no *software* do controlador.

A sincronização de sistemas caóticos é uma tarefa mais complicada que o controle dos mesmos. Os sistemas caóticos a serem sincronizados são sistemas idênticos iniciados em tempos diferentes e/ou com condições iniciais diferentes. Desta forma, cada sistema estará percorrendo uma trajetória diferente em seus atratores. O objetivo da sincronização é, mantendo o comportamento caótico, fazer com que os diferentes sistemas percorram a mesma trajetória em seus atratores. Os fundamentos da sincronização de sistemas caóticos podem ser encontrados nas Referências. 3.8, 3.15 e 3.16. Aqui nos limitaremos a uma rápida explanação sobre o assunto e algumas considerações sobre a sincronização de RNLs.

Para obter-se a sincronização é necessário o envio de um sinal (ou informação) de um dos sistemas caóticos, conhecido como mestre, para o segundo, conhecido com escravo. A Fig. 3.18 mostra o diagrama de blocos para a sincronização de dois sistemas baseados nas equações de Lorenz, estando estas ao lado da figura [Ref. 3.16].

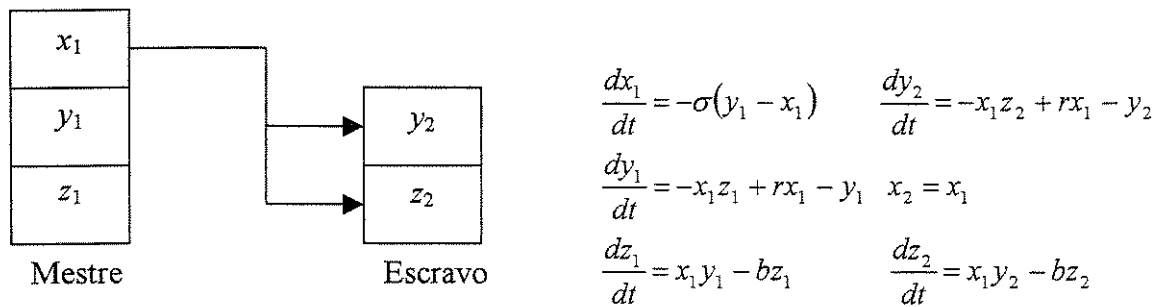


Fig. 3.18 - Sincronização de 2 sistemas de Lorenz.

Como observa-se nas equações diferenciais ao lado da Fig. 3.18, a variável x_2 é trocada por x_1 e, com a evolução temporal, ocorre que $y_2 \rightarrow y_1$ e $z_2 \rightarrow z_1$ e, portanto, os sistemas tornam-se sincronizados. Os demais métodos de sincronização propostos, pouco diferem do exposto na Fig. 3.18. Por exemplo, alguns envolvem também o envio de um sinal do Sistema 2 (escravo) para o Sistema 1 (mestre) [Refs. 3.8, 3.16]. Quando os sistemas a serem sincronizados estão em locais afastados, a transmissão do sinal de sincronismo, de uma ponta a outra, deve ser de alta fidelidade, isto é, o canal não deve distorcer a informação de sincronismo. Para a sincronização de RNLs este problema se torna crítico. A única variável óptica disponível para ser enviada, pelo RNL local ao RNL remoto, é o próprio campo na saída do RNL. Com a falta de um modelo analítico fechado para o RNL, a situação fica ainda mais complicada pois não há como verificar se informações, como a energia e outros momentos do pulso de saída do RNL local, possam ser usadas pelo RNL remoto, via algum algoritmo, para obter-se a sincronização. A utilização dos RNLs controlados traz uma luz ao problema. Embora trabalhando em regime periódico, RNLs espacialmente afastados podem ser sincronizados através da troca de informações usadas pelos controladores. Os RNLs são iniciados simultaneamente mas com condições iniciais

diferentes. Os controladores de ambos, assumidos idênticos, são ligados apenas na 15ª volta. O RNL mestre (1) assim permanece indefinidamente. Para o RNL escravo (2), temos:

$$E_{ent}^{(2)}(n+1, \tau) = E_{ent}^{(2)}(n, \tau) + cf^{(2)} \sqrt{|\beta_2|/RT_1^2} \operatorname{sech}(\tau/T_1) \quad 15 \leq n < 50 \quad (3.26)$$

$$E_{ent}^{(2)}(n+1, \tau) = E_{ent}^{(2)}(n, \tau) + (cf^{(1)} - cf^{(2)}) \sqrt{|\beta_2|/RT_1^2} \operatorname{sech}(\tau/T_1) \quad 50 \leq n < 160 \quad (3.27)$$

Da Eq. (3.27), vemos que o valor da saída do controlador do RNL mestre deve ser enviado ao controlador do RNL escravo. A partir da 160ª volta a variável $e_g^{(2)}$ do controlador do RNL escravo passa a ser dada por:

$$e_g^{(2)} = S_n^{(2)} - S_n^{(1)} \quad (3.28)$$

e a Eq. (3.26) volta a ser usada para o controle. Os resultados das simulações são mostrados nas Figs. 3.19 - 3.25 e os valores dos parâmetros na Tabela 3.5. Todos os parâmetros do RNL são os mesmos dados na Tabela 3.1. Os pulsos de entrada do RNL mestre e escravo, antes dos controladores serem ligados, são da forma mostrada na Eq. (3.24).

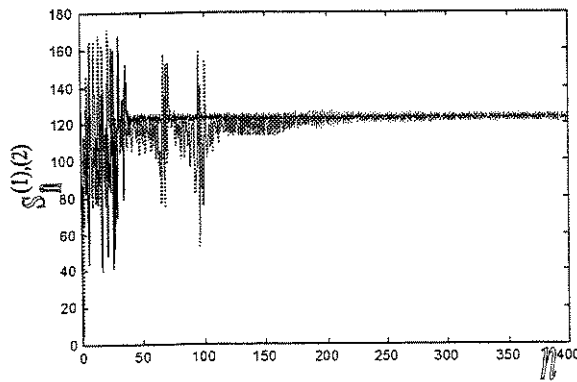


Fig. 3.19 - $S_n^{(1)}, S_n^{(2)} \times n$. (SIM-1)

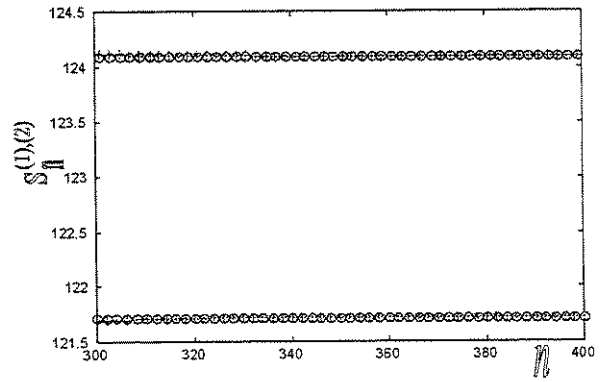


Fig. 3.20 - $S_n^{(1)}(\circ), S_n^{(2)}(+)\times n$. (SIM-1)

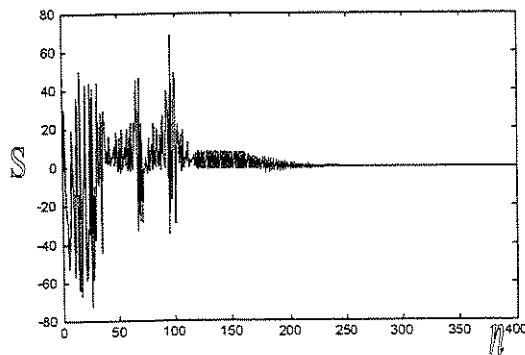


Fig. 3.21 - $[S = S_n^{(1)} - S_n^{(2)}] \times n$. (SIM-1)

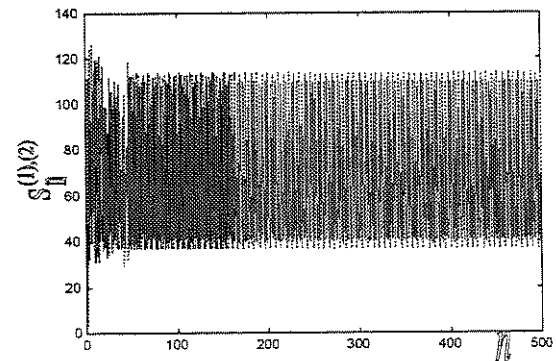


Fig. 3.22 - $S_n^{(1)}, S_n^{(2)} \times n$. (SIM-2)

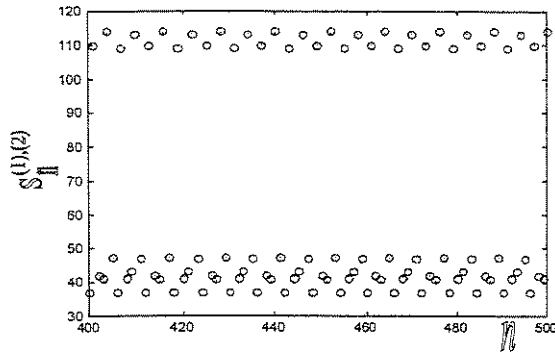


Fig. 3.23 - $S_n^{(1)}(o), S_n^{(2)}(\bullet) \times n$. (SIM-2)

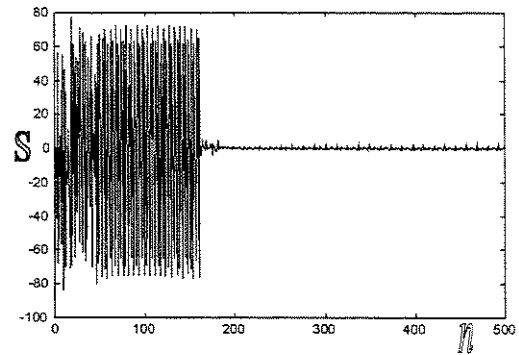


Fig. 3.24 - $|S = S_n^{(1)} - S_n^{(2)}| \times n$. (SIM-2)

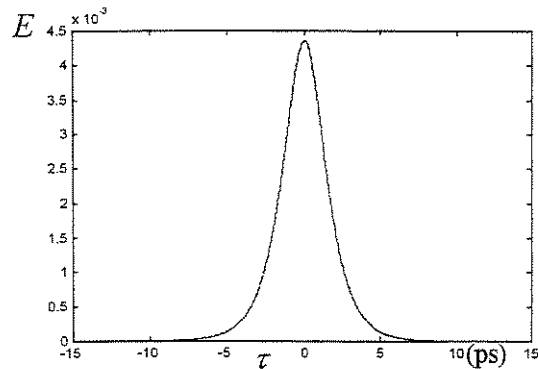


Fig. 3.25 - $(E = E_{ent}^{(1)} - E_{ent}^{(2)}) \times \tau$. (SIM-2)

SIM	N ₁	N ₂	T ₀ [ps]	y _{min} ^{max}
1	1,75	1,9	3	±0,2512
2	1,75	1,9	4	±0,3
k = 3 e _{g min} ^{max} = ±120 e _{i min} ^{max} = ±10				

Tabela 3.5 - Parâmetros da sincronização de RNLs.

Observando as Figs. 3.19 - 3.24 vemos que a sincronização realmente acontece estando, portanto, o RNL escravo percorrendo a mesma órbita periódica na qual o RNL mestre foi aprisionado por seu controlador. Na Fig. 3.25 vemos que, após a sincronização, os pulsos nas entradas dos RNLs mestre e escravo são quase idênticos.

3.3 Acoplador Não-linear a Fibra - ANL

Os acopladores ópticos não-lineares a fibra consistem de duas fibras ópticas com núcleos fundidos ou bastante próximos um do outro, de modo a permitir que modos evanescentes se acoplem entre os núcleos, Fig. 3.26. Este acoplamento provoca a transferência da energia luminosa de um núcleo para o outro. Por isso, os ANLs são candidatos naturais a desempenharem a função de chaveadores ópticos de alta velocidade [Refs. 3.17-3.19]. A característica interessante destes acopladores é que, para um dado comprimento do acoplador, a transmissividade, isto é, a razão entre a energia na saída e na entrada de uma das fibras, depende da intensidade ou da energia do pulso incidente na mesma. Quando a largura do pulso incidente é grande comparada ao tempo de relaxação da não-linearidade, o ANL tende a "enxergar" cada parte individual do pulso como um feixe CW com intensidade igual à intensidade instantânea da referida parte do pulso incidente e, portanto, acoplará cada parte do pulso segundo a transmissividade CW do ANL. Este efeito leva à quebra do pulso incidente [Ref. 3.17]. Entretanto, quando os pulsos incidentes no ANL são sólitons, a quebra do pulso não ocorre [Refs. 3.17-3.19]; além disso, a eficiência

de acoplamento é duas vezes maior que para o caso CW, bem como a curva de transmissividade é mais aguda [Ref. 3.17]. As referências citadas apresentam o estudo numérico e analítico, este último via formulação variacional, do ANL. Aqui, nos limitamos à percepção, via simulações numéricas, da variação da curva de transmissividade do ANL através da variação do perfil do coeficiente de acoplamento, sem entrar em detalhes na quantificação das variações do perfil e seus efeitos na curva de transmissividade.

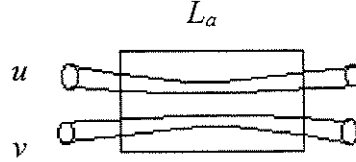


Fig. 3.26 - Acoplador não-linear a fibra.

As equações de propagação das envoltórias, u e v , nas fibras do ANL são [Refs. 3.17-3.19]:

$$i \frac{\partial u}{\partial z} + \beta_{1u} \frac{\partial u}{\partial t} + \frac{\beta_{2u}(z)}{2} \frac{\partial^2 u}{\partial t^2} + R(z)|u|^2 u + i\Gamma(z)u + K(z)v = 0 \quad (3.29)$$

$$i \frac{\partial v}{\partial z} + \beta_{1v} \frac{\partial v}{\partial t} + \frac{\beta_{2v}(z)}{2} \frac{\partial^2 v}{\partial t^2} + R(z)|v|^2 v + i\Gamma(z)v + K(z)u = 0 . \quad (3.30)$$

Nas Eqs. (3.29) e (3.30) levamos em conta a situação mais geral em que os coeficientes podem variar ao longo do comprimento da fibra. Consideraremos apenas o caso em que só há pulsos em uma das entradas do ANL; assim, tomaremos $\beta_{1u} = \beta_{1v} = \beta_1$ e $\beta_{2u} = \beta_{2v} = \beta_2$. Γ representa a perda na fibra e K é o coeficiente de acoplamento linear, dependente da distância entre os dois núcleos; todos os demais símbolos têm o mesmo significado exposto na Seção 3.2. Aplicando, agora, as conhecidas transformações [Ref. 3.1]:

$$\tau = t - \beta_1 z \Rightarrow \begin{cases} \frac{\partial}{\partial z} = \frac{\partial}{\partial z'} \frac{\partial z'}{\partial z} + \frac{\partial}{\partial \tau} \frac{\partial \tau}{\partial z} = \frac{\partial}{\partial z'} - \beta_1 \frac{\partial}{\partial \tau} \end{cases} \quad (3.31)$$

$$z' = z \Rightarrow \begin{cases} \frac{\partial}{\partial t} = \frac{\partial}{\partial z'} \frac{\partial z'}{\partial t} + \frac{\partial}{\partial \tau} \frac{\partial \tau}{\partial t} = \frac{\partial}{\partial \tau} \end{cases} \quad (3.32)$$

$$\frac{\partial^2}{\partial t^2} = \frac{\partial^2}{\partial \tau^2} \quad (3.33)$$

juntamente com as substituições

$$u = A \exp\left(\int_0^z \Gamma(\varepsilon) d\varepsilon\right) \quad (3.34)$$

$$v = B \exp\left(\int_0^z \Gamma(\varepsilon) d\varepsilon\right) \quad (3.35)$$

em (3.29) e (3.30), obtemos:

$$i \frac{\partial A}{\partial z'} + \frac{\beta_2(z')}{2} \frac{\partial^2 A}{\partial \tau^2} + R(z') \exp\left(-2 \int_0^{z'} \Gamma(\varepsilon) d\varepsilon\right) |A|^2 A + K(z') B = 0 \quad (3.36)$$

$$i \frac{\partial B}{\partial z'} + \frac{\beta_2(z')}{2} \frac{\partial^2 B}{\partial \tau^2} + R(z') \exp\left(-2 \int_0^{z'} \Gamma(\varepsilon) d\varepsilon\right) |B|^2 B + K(z') A = 0 . \quad (3.37)$$

Se desejarmos, podemos ainda fazer a transformação:

$$\xi = \int_0^{z'} \beta_2(\varepsilon) d\varepsilon \quad (3.38)$$

que, substituída em (3.36) e (3.37), dá:

$$i \frac{\partial A}{\partial \xi} + \frac{1}{2} \frac{\partial^2 A}{\partial \tau^2} + \frac{R(\xi)}{\beta_2(\xi)} \exp\left(-2 \int_0^\xi \Gamma(\varepsilon) d\varepsilon\right) |A|^2 A + \frac{K(\xi)}{\beta_2(\xi)} B = 0 \quad (3.39)$$

$$i \frac{\partial B}{\partial \xi} + \frac{1}{2} \frac{\partial^2 B}{\partial \tau^2} + \frac{R(\xi)}{\beta_2(\xi)} \exp\left(-2 \int_0^\xi \Gamma(\varepsilon) d\varepsilon\right) |B|^2 B + \frac{K(\xi)}{\beta_2(\xi)} A = 0 . \quad (3.40)$$

Obviamente β_2 é suposto nunca se anular; se isto acontecesse, termos de dispersão de ordens mais elevadas teriam de ser considerados. A primeira conclusão, observando as Eqs. (3.39) e (3.40), é que o termo de perdas aparece no coeficiente do termo não-linear e, por isso, uma escolha apropriada de variação de R e/ou β_2 , ao longo da fibra, pode minimizar o efeito das perdas, muito embora variações de R ao longo da fibra sejam de difícil implementação. Para as simulações das Eqs. (3.39) e (3.40), com exceção de K , todos os demais termos foram considerados constantes e a perda nula. Os valores dos parâmetros utilizados nas simulações estão na Tabela 3.6. Os pulsos nas entradas do acoplador são da forma:

$$A = N \sqrt{\frac{|\beta_2|}{RT_1^2}} \operatorname{sech}\left(\frac{\tau}{T_1}\right) \quad (3.41)$$

$$B = 0 . \quad (3.42)$$

Os resultados são mostrados nas Figs. 3.27 - 3.31.

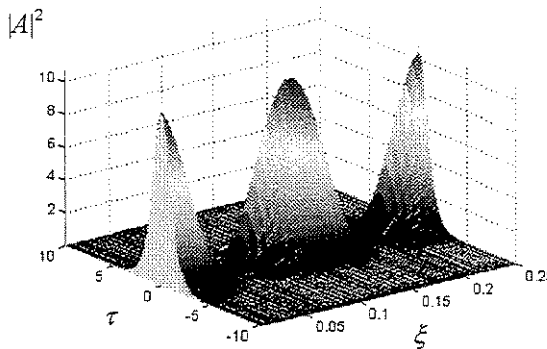


Fig. 3.27 - $A(\xi, \tau)$. (SIM-1)

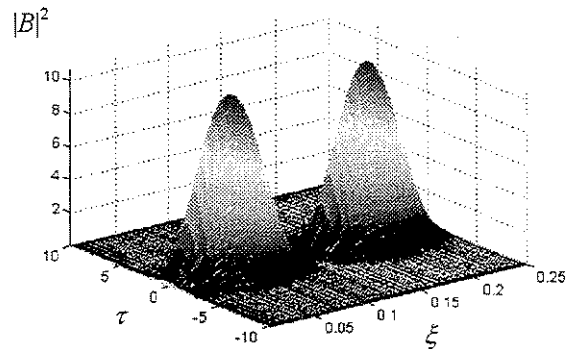


Fig. 3.28 - $B(\xi, \tau)$. (SIM-1)

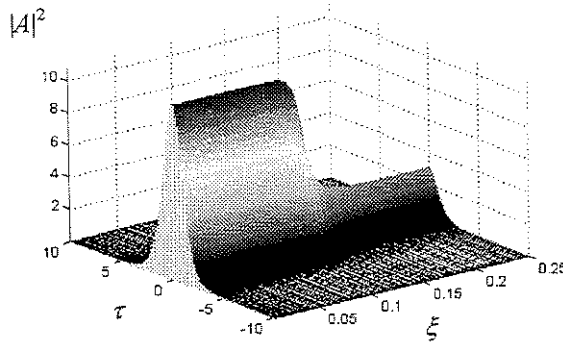


Fig. 3.29 - $A(\xi, \tau)$. (SIM-2)

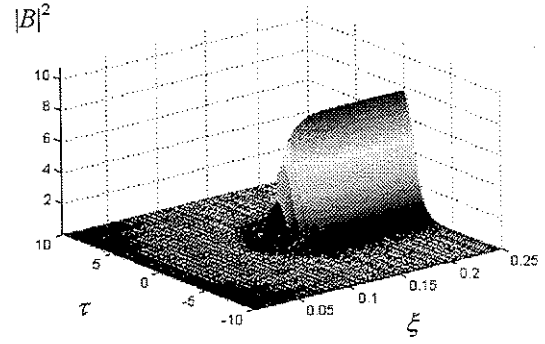


Fig. 3.30 - $B(\xi, \tau)$. (SIM-2)

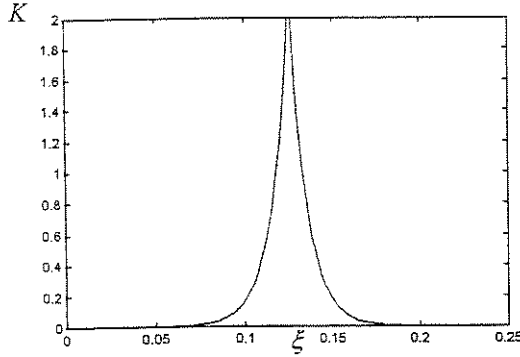


Fig. 3.31 - $K(\xi)$. (SIM-2)

SIM	N	K	L_a
1	1	1	0,25
2	1	$2\exp[-100(\xi-L_a/2)] * +2\exp[-100(L_a/2-\xi)] **$	0,25
$\lambda = 1,55 \mu\text{m}$, $\beta_2 = -20,4 \text{ ps}^2/\text{km}$, $R = 1,3 \text{ W}^{-1} \text{ km}^{-1}$, $T_0 = 2 \text{ ps}$. * $\xi > L_a/2$. ** $\xi \leq L_a/2$.			

Tabela 3.6 - Parâmetros de simulação da propagação de pulsos no ANL.

As Figs. 3.27 e 3.28 mostram, para o coeficiente de acoplamento constante, a transferência periódica da energia luminosa entre os dois núcleos, havendo, em determinadas posições, a transferência total de energia. As Figs. 3.29 e 3.30 mostram, para o coeficiente de acoplamento mostrado na Fig. 3.31, que a troca de energia só acontece na região em que o perfil exponencial assume valores consideráveis. Portanto, apenas uma parcela da energia de A é capturada e não mais devolvida ao núcleo de origem. Para a normalização completa das Eqs. (3.39) e (3.40), com R e β_2 constantes e perdas nulas, podemos fazer:

$$a = A \sqrt{\frac{R}{\beta_2}}, \quad b = B \sqrt{\frac{R}{\beta_2}} \quad (3.43)$$

$$k = \frac{K(\xi)}{\beta_2}, \quad (3.44)$$

o que nos leva a [Ref. 3.19]:

$$i \frac{\partial a}{\partial \xi} + \frac{1}{2} \frac{\partial^2 a}{\partial \tau^2} + |a|^2 a + k(\xi) b = 0 \quad (3.45)$$

$$i \frac{\partial b}{\partial \xi} + \frac{1}{2} \frac{\partial^2 b}{\partial \tau^2} + |b|^2 b + k(\xi) a = 0 \quad (3.46)$$

Para a simulação das Eqs. (3.45) e (3.46) só precisamos nos preocupar com o perfil $k(\xi)$. Usamo-las para o cálculo da curva de transmissividade, T . Esta curva é obtida achando-se [Ref. 3.18]:

$$T = \int_{-\infty}^{\infty} |a(L_a, \tau)|^2 d\tau \bigg/ \int_{-\infty}^{\infty} |a(0, \tau)|^2 d\tau = I_{La} / I_0 \quad (3.47)$$

para diversos valores de energia dos pulsos de entrada. Estes pulsos são da forma:

$$a(0, \tau) = N \operatorname{sech}(N\tau) \quad (3.48)$$

$$b(0, \tau) = 0 \quad (3.49)$$

onde o parâmetro N controla a energia do pulso de entrada. As Figs. 3.32 - 3.36 mostram as simulações do ANL para diferentes perfis da constante de acoplamento. Os dados das simulações estão na Tabela 3.7.

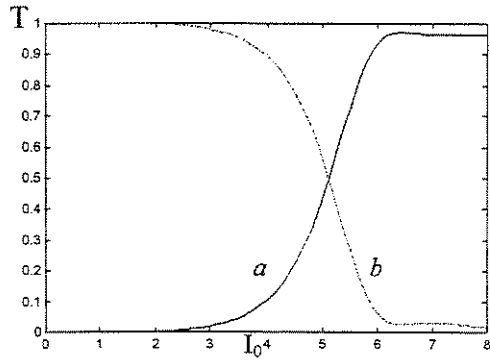


Fig. 3.32 - Transmissividade, $T \times I_0$. (SIM-1)

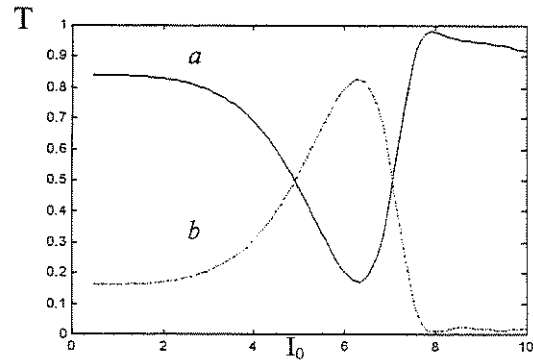


Fig. 3.33 - Transmissividade, $T \times I_0$. (SIM-2)

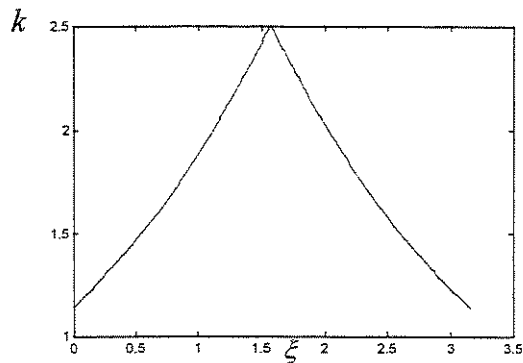


Fig. 3.34 - Perfil da constante de acoplamento, $k(\xi)$. (SIM-2)

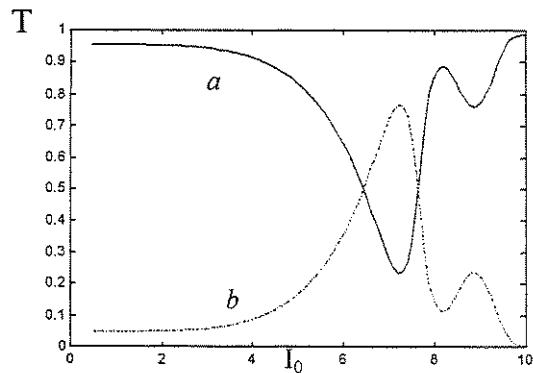


Fig. 3.35 - Transmissividade, $T \times I_0$. (SIM-3)

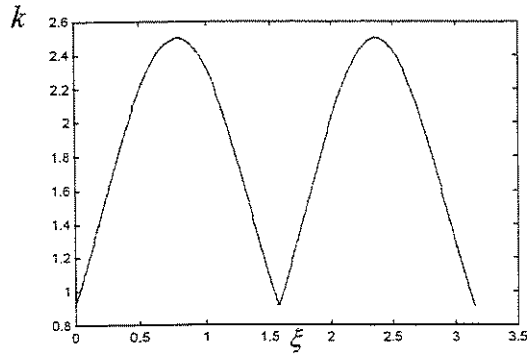


Fig. 3.36 - Perfil da constante de acoplamento, $k(\xi)$. (SIM-3)

SIM	N	k
1	$[v^+, 5]$	1
2	$[v^+, 7, 5]$	$2,5 \exp[-0,5(\xi - L_a/2)] * + 2,5 \exp[-0,5(L_a/2 - \xi)] **$
3	$[v^+, 7, 5]$	$2,5 \exp[-(L_a/4)^2 (\xi - L_a/4)^2] + 2,5 \exp[-(L_a/4)^2 (\xi - 3L_a/4)^2]$
$L_a = \pi, v^+ = 0,5, * \xi \geq L_a/2, ** \xi \leq L_a/2$		

Tabela 3.7 - Parâmetros de Simulação do ANL.

A Fig. 3.32 mostra a curva tradicionalmente encontrada nas referências. As Figs. 3.33, com o perfil mostrado em 3.34, e 3.35, com o perfil mostrado em 3.36, indicam que, variando-se o perfil da constante de acoplamento, podemos moldar a curva de transmissividade. Observamos que os ANLs se comportam como filtros de energia, selecionando, em uma de suas saídas, apenas os pulsos com energia situada dentro da janela de transmissão (comportamento ideal), enquanto que os demais pulsos são dirigidos à outra saída. Para os casos em que os pulsos de entrada não são da forma (3.48) as curvas das Figs. 3.32 a 3.36 não se aplicam pois, se a forma do pulso de entrada muda, a forma da curva de transmissividade também muda. Voltando às Eqs. (3.39) e (3.40), para o caso em que os pulsos de entrada são da forma (não solitônica):

$$A(0, \tau) = N \sqrt{\frac{|\beta_2|}{RT_1^2}} \operatorname{sech}\left(\frac{\tau}{T_1}\right) \quad (3.50)$$

$$B(0, \tau) = 0 \quad (3.51)$$

$$T_1 = \frac{T_0}{1,6574544} \quad (3.52)$$

com $N \in [0,75, 5]$, $T_0 = 2$ ps, $L_a = 2$, $K = \exp[-(\xi - L_a/2)] + \exp[-(L_a/2 - \xi)]$, $R = 1,3 \text{ W}^{-1} \text{ km}^{-1}$ e $\beta_2 = -20,4 \text{ ps}^2 \text{ km}^{-1}$, obtemos, para o perfil mostrado na Fig. 3.38, a curva de transmissividade mostrada na Fig. 3.37.

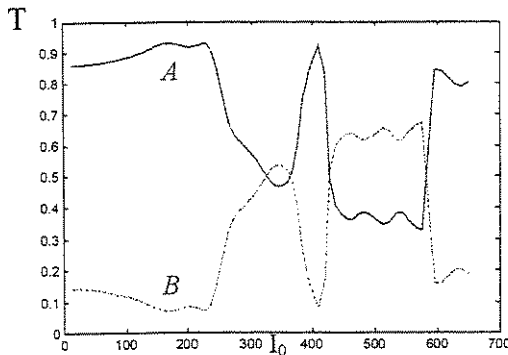


Fig. 3.37 - Transmissividade, $T \times I_0$.

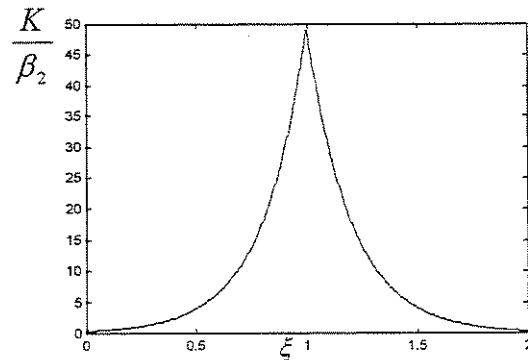


Fig. 3.38 - Perfil da constante de acoplamento.

A Fig. 3.37 nos apresenta uma curva bem mais complexa que as demais, sendo a transmissividade mínima próxima de 0,4 indicando que os pulsos não são bem selecionados.

3.4. Birrefringência

Do exposto no Capítulo 2, sabemos que a fibra óptica têm dois eixos principais de propagação, o eixo rápido e o eixo lento, nos quais qualquer campo incidente se decompõe. Assim, se o pulso incidente não for linearmente polarizado, com a direção de polarização coincidente com a direção de um dos eixos principais, teremos a propagação de dois modos na fibra. Desta forma, quando do uso de efeitos não-lineares, devemos levar em consideração, além da variação do índice de refração devido à própria intensidade do modo (automodulação de fase), a variação do índice de refração devido à intensidade do outro modo (modulação de fase cruzada). As equações de propagação dos modos são [Refs. 3.1, 3.20, 3.21]:

$$i \frac{\partial u}{\partial z} + i\delta \frac{\partial u}{\partial \tau} + \frac{\beta_{2u}}{2} \frac{\partial^2 u}{\partial \tau^2} + R(|u|^2 + \varepsilon|v|^2)u + i\Gamma u = 0 \quad (3.53)$$

$$i \frac{\partial v}{\partial z} - i\delta \frac{\partial v}{\partial \tau} + \frac{\beta_{2v}}{2} \frac{\partial^2 v}{\partial \tau^2} + R(|v|^2 + \varepsilon|u|^2)v + i\Gamma v = 0 \quad (3.54)$$

$$\delta = \frac{\beta_{1u}(\omega_0) - \beta_{1v}(\omega_0)}{2} \quad (3.55)$$

onde os pulsos u e v , que se propagam nos eixos principais da fibra, estão montados em portadoras de mesma frequência, ω_0 , o que leva a $\beta_{2u} = \beta_{2v} = \beta_2$. Fazendo, novamente, as transformações (3.31) - (3.35), com perda nula e coeficientes constantes, obtemos:

$$i \frac{\partial u}{\partial \xi} + i\delta \frac{\partial u}{\partial \tau} + \frac{1}{2} \frac{\partial^2 u}{\partial \tau^2} + \frac{R}{\beta_2} (|u|^2 + \varepsilon|v|^2)u = 0 \quad (3.56)$$

$$i \frac{\partial v}{\partial \xi} - i\delta \frac{\partial v}{\partial \tau} + \frac{1}{2} \frac{\partial^2 v}{\partial \tau^2} + \frac{R}{\beta_2} (|v|^2 + \varepsilon|u|^2)v = 0 \quad (3.57)$$

$$\delta = [\beta_{1u}(\omega_0) - \beta_{1v}(\omega_0)]/2\beta_2 \quad (3.58)$$

Aplicando, agora, as substituições [Ref. 3.20]:

$$u(\xi, \tau) = A(\xi, \tau) \exp[i(-\delta\tau + 0,5\delta^2\xi)] \quad (3.59)$$

$$v(\xi, \tau) = B(\xi, \tau) \exp[i(\delta\tau + 0,5\delta^2\xi)] \quad (3.60)$$

seguida da Eq. (3.43), $a(b) = A(B)(R/\beta_2)^{1/2}$, em (3.56) e (3.57), resulta em:

$$i \frac{\partial a}{\partial \xi} + \frac{1}{2} \frac{\partial^2 a}{\partial \tau^2} + (|a|^2 + \varepsilon |b|^2) a = 0 \quad (3.61)$$

$$i \frac{\partial b}{\partial \xi} + \frac{1}{2} \frac{\partial^2 b}{\partial \tau^2} + (|b|^2 + \varepsilon |a|^2) b = 0 \quad (3.62)$$

As Eqs. (3.61) e (3.62) foram extensivamente estudadas nas Referências 3.1, 3.20 e 3.21. Aqui, consideraremos apenas o caso em que o pulso b é de intensidade suficientemente baixa para que todos os efeitos não-lineares, devidos ao mesmo possam ser desprezados. Além disso, consideramos que o comprimento da fibra é muito menor que o comprimento de dispersão, $L_D = T_0^2 / |\beta_2|$, tal que os efeitos de dispersão também possam ser desprezados. Nestes limites, os dois pulsos não variam suas amplitudes, mas sofrem uma variação na fase proporcional à intensidade do pulso mais forte, ou seja, ambos os pulsos sofrem uma modulação de fase ficando com um gorjeio. As Figs. 3.39 e 3.40 mostram a simulação das Eqs. (3.61) e (3.62) para o comprimento de fibra $L_f = \pi/30$ e coeficiente de birrefringência $\varepsilon = 2/3$. Os pulsos na entrada da fibra são:

$$a(\xi, \tau) = 4 \operatorname{sech}(1,6575\tau) \exp(i0,25\pi + i0,5\tau^2) \quad (3.63)$$

$$b(\xi, \tau) = 0,1 \operatorname{sech}(1,6575\tau) \quad (3.64)$$

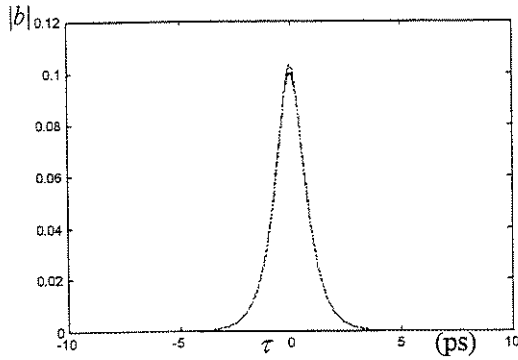


Fig. 3.39 - Módulo de $b(0, \tau)$ e $b(L_f, \tau)$.

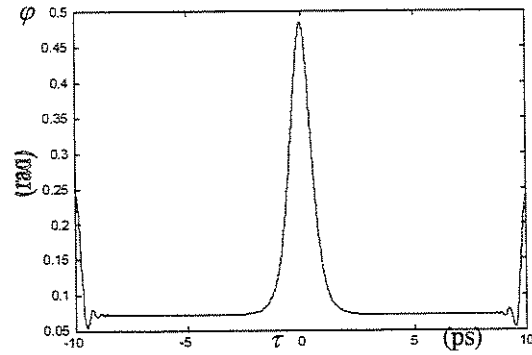


Fig. 3.40 - Fase de $b(L_f, \tau)$. $\varphi = \arg[b(L_f, \tau)]$.

As Figs. 3.39 e 3.40 mostram, respectivamente, a conservação da forma do pulso de baixa intensidade e a modulação de fase que o mesmo sofre, ficando com um gorjeio proporcional à intensidade do pulso mais intenso e com a forma do mesmo. É interessante apontar que este gorjeio pode mascarar a fase do pulso.

3.5 Aplicação dos Dispositivos Não-lineares em Comunicações Quânticas

Os dispositivos ópticos não-lineares podem desempenhar funções variadas em um sistema de comunicação quântica. Uma das mais simples é mostrada, em diagrama de blocos, na Fig 3.41. Nela, um sistema caótico substitui o processo de escolha aleatória do bit da chave, feita por Alice, em um sistema de criptografia quântica .

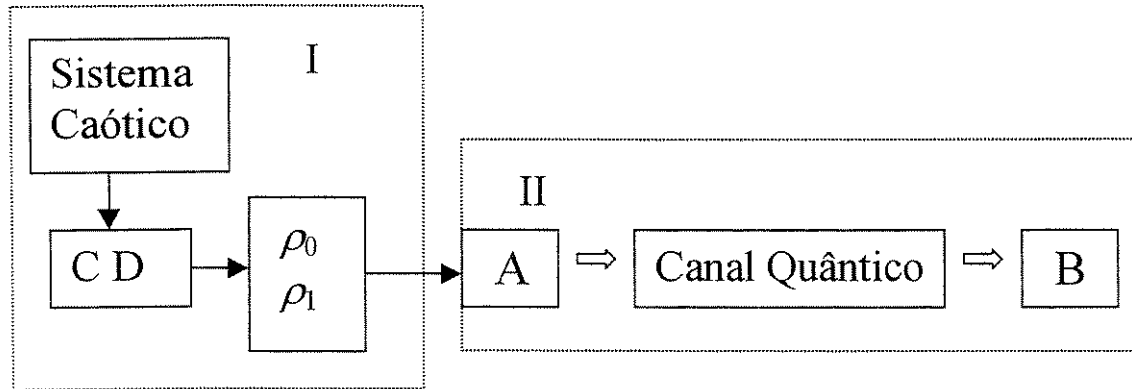


Fig. 3.41 - Criptografia quântica com chave produzida caoticamente.

O funcionamento do diagrama da Fig. 3.41 é simples. A variável caótica é entregue ao bloco CD, Compara-Decide; este compara o valor da variável caótica a um valor de referência e, caso o valor da variável caótica seja maior ou menor que o valor de referência, decide-se qual dos estados vai ser entregue a Alice, se ρ_0 ou ρ_1 . Estes estados são ortogonais, para que Alice possa identificá-los através uma medição. Assim, Alice escolhe a base, repete o resultado de sua medição como sendo o bit da chave e o envia a Bob. O resto da comunicação segue o protocolo BB84 apresentado no Apêndice C. O Bloco I da Fig. 3.41 pode ser construído com o uso combinado do RNL com o ANL. A Fig. 3.42 mostra essa configuração e sua ligação com Alice, em um esquema polarimétrico [Ref. 3.22].

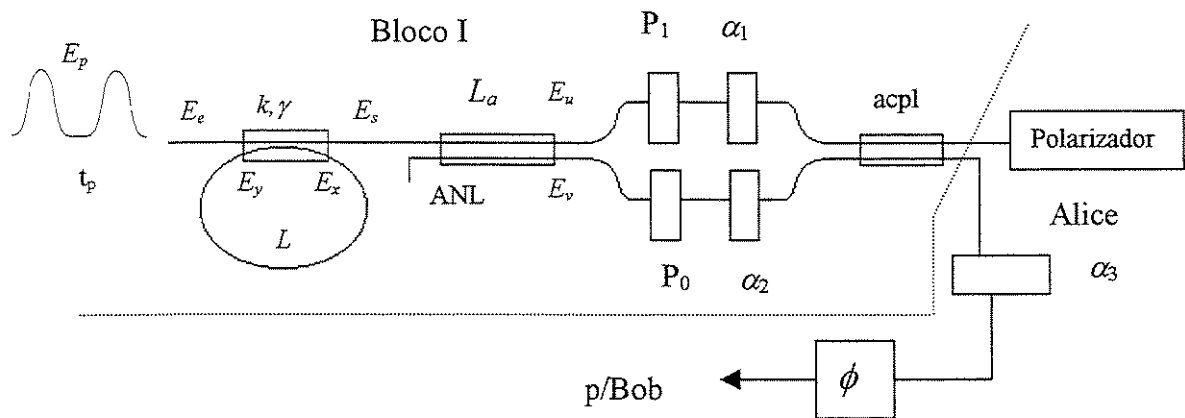


Fig. 3.42 - Gerador de pulsos, com polarização binária caótica, para produção da chave de um sistema polarimétrico de criptografia quântica.

O funcionamento do diagrama da Fig. 3.42 é o seguinte: O RNL fornece pulsos, com a intensidade variando caoticamente, ao ANL. Este, segundo os valores de seus parâmetros, vai chavear os pulsos entre as duas saídas. Espera-se que, na maioria das vezes, a razão entre as potências nas saídas do ANL seja muito pequena ou muito grande, ou seja, que a potência em uma das saídas seja bem próxima à potência incidente no acoplador e que, a outra, seja bem próxima de zero. Os pulsos emergentes na saída u passarão pelo polarizador

P_1 , de 90° , enquanto que os pulsos na saída v passarão pelo polarizador P_0 , de 0° . Os atenuadores α_1 e α_2 têm a finalidade de eliminar o pulso de menor potência, oriundo da não idealidade do chaveamento do ANL, ou seja, eles eliminam os pulsos de baixa intensidade que emergirem na saída que não foi selecionada. O pulso mais brilhante, aquele na saída selecionada, sofre uma atenuação mas não deixa de existir. Ele é, então, dividido por um acoplador linear. Uma parte dele vai para um polarizador em Alice, uma vez que ela precisa saber qual polarização está sendo enviada para Bob, se 90° ou 0° . A outra parte passa pelo atenuador α_3 , cuja função é aproximar o estado coerente do estado de número de 1 fóton. Finalmente, o rotacionador ϕ , controlado por Alice, dá um acréscimo de 0° ou 45° na polarização, segundo a base escolhida aleatoriamente para a comunicação. Portanto, na saída de Alice temos 90° ou 0° , escolhidos segundo o comportamento caótico do RNL, somados a 0° ou 45° , segundo a escolha aleatória de Alice para a base, proporcionando na saída, um dos 4 possíveis estados $|0^\circ\rangle$, $|90^\circ\rangle$, $|45^\circ\rangle$ e $|135^\circ\rangle$. Poderá acontecer, devido à variação caótica da intensidade na saída do RNL, que surja um pulso na entrada do ANL que seja dividido em razões próximas à 0,5, provocando o aparecimento de pulsos com polarização 90° e 0° , nas saídas do acpl, acoplador linear. Quando isto ocorrer, Alice será capaz de perceber pois ela receberá fótons nas duas saídas de seu polarizador. Posteriormente, Alice deve combinar com Bob a desconsideração dos bits nos "slots" de tempo em que esta situação ocorrer.

Uma situação bem mais complicada é a mostrada na Fig. 3.43. Nela percebemos que a comunicação quântica é controlada por dois sistemas caóticos sincronizados.

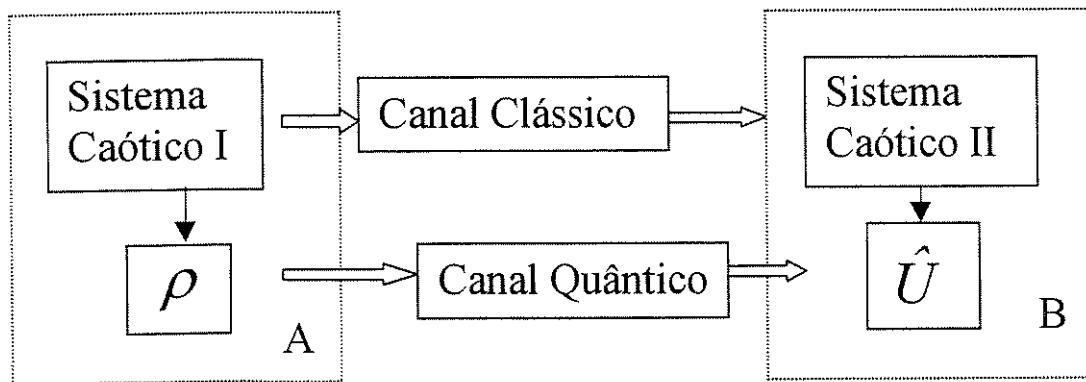


Fig. 3.43 - Comunicação quântica controlada por sistemas caóticos sincronizados.

O sincronismo é feito através de informações clássicas enviadas do Sistema Caótico I, mestre, para o Sistema Caótico II, escravo, através de um canal clássico. Na Fig. 3.43 temos que o Sistema Caótico I atua no estado a ser enviado por Alice; ao passo que o Sistema Caótico II atua no operador ($\hat{U}$) que representa a medição que Bob fará para reconhecer o estado enviado por Alice. Se os dois sistemas caóticos estão em sincronismo, a informação enviada por Alice é casada com a base de medição escolhida por Bob, de forma que não haja dúvida no resultado obtido por Bob. Quando não há sincronismo, Bob não pode ter certeza se a informação que ele obteve foi a mesma que Alice enviou. Uma situação interessante do sistema proposto na Fig. 3.43 é que o Sistema Caótico I pode servir para embaralhar o estado quântico enviado por Alice e o Sistema Caótico II desembaralhá-

lo para que Bob possa fazer uma medição, ou seja, temos um sistema de comunicações quânticas protegido por um sistema de criptografia caótica. A Fig. 3.44 mostra a configuração para um sistema de comunicação quântico protegido por criptografia caótica. O funcionamento do sistema mostrado na Fig. 3.44 é quase idêntico ao descrito no Apêndice C. Na saída de Alice, o pulso que sofreu a modulação de fase ϕ_a também sofreu um gorjeio devido à propagação conjunta com um pulso proveniente do RNL na fibra birrefringente, L_f . Os polarizadores $P_{a(b)}$ são responsáveis pela junção e separação destes pulsos na fibra birrefringente. O gorjeio mascara ϕ_a . O pulso que não sofre modulação de fase em Alice é o que vai passar pela fibra birrefringente em Bob. Se os RNLs I e II estão em sincronismo então o gorjeio sofrido pelo pulso em Bob será igual ao gorjeio sofrido pelo outro pulso em Alice, de forma que a diferença de fase entre os dois pulsos na saída

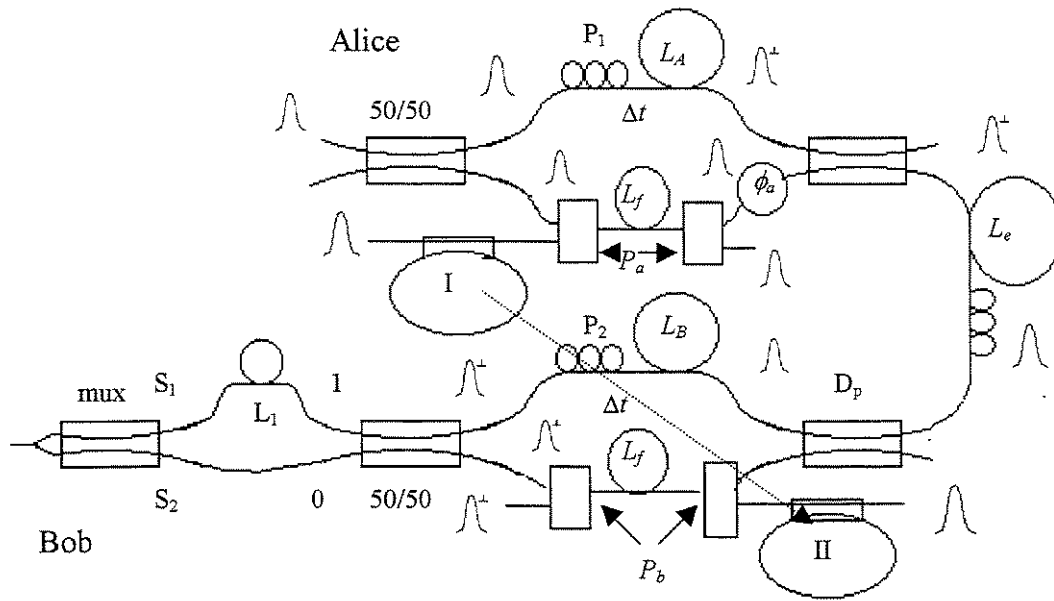


Fig. 3.44 - Sistema de comunicação quântica com criptografia caótica.

do interferômetro seja ϕ_a e, portanto, Alice pode controlar em que saída de Bob o pulso emergirá do interferômetro através do controle do valor de ϕ_a . Por outro lado, se os RNLs não estão em sincronismo, a diferença de fase entre os dois pulsos na saída do interferômetro será $\phi_a + [f(t)-g(t)]$ onde f e g representam os gorjeios causados em Alice e Bob, respectivamente. Desta forma, o pulso emergirá em qualquer uma das saídas de Bob. Se um espião quiser obter o valor de ϕ_a , a partir do pulso enviado por Alice, ele terá que ser capaz de separar ϕ_a do gorjeio; para isso, terá que ter um RNL igual e sincronizado com o de Alice. Para evitar esta possibilidade, Alice e Bob podem, antes de iniciar a comunicação, ajustar um dos parâmetros do RNL a partir de um algoritmo que use uma semente (valor inicial). A semente poderia ser a chave obtida em um processo de criptografia quântica tradicional a ser realizado logo no início da comunicação.

Da explicação acima exposta duas questões importantes surgem: 1) Como saber se os RNLs já estão sincronizados? 2) Como diferenciar a falta de sincronismo entre os RNLs do envio de dados por Alice, uma vez que ambos permitem pulsos em ambas as saídas de Bob? A resposta da primeira questão é mais simples. Durante o processo de sincronismo

Alice faz, por exemplo, $\phi_a = 0$. Assim, no perfeito sincronismo, Bob só receberá pulsos em uma única saída; enquanto isso não ocorrer o sincronismo não foi alcançado. A resposta da segunda questão é mais elaborada, exige que, de tempo em tempo, Alice e Bob testem o sincronismo, ou seja, a cada R bits enviados, Alice envia uma sequência de P bits com $\phi_a = 0$; para ver se Bob os receberá todos em uma única saída. Alice e Bob podem ainda, ao final da comunicação, empregar técnicas de checagem e correção de erros.

CONCLUSÕES DO CAPÍTULO III

Neste capítulo, tratamos do aproveitamento de dispositivos e efeitos ópticos não-lineares em sistemas de comunicações quânticas. Iniciamos trabalhando com o ressonador não-linear a fibra, RNL:

1. Apresentamos, através de uma simulação, o comportamento caótico do RNL.
2. Descrevemos, detalhadamente, um controlador baseado na técnica de inteligência numérica lógica nebulosa (*fuzzy*).
3. Introduzimos uma malha de realimentação, com o controlador nebuloso, no RNL, objetivando controlar o comportamento caótico deste.
4. Implementamos a sincronização de dois RNLs controlados através da troca de informações entre seus controladores nebulosos.

Através de simulações, mostramos que o comportamento caótico do RNL é controlado com sucesso pelo controlador nebuloso. Mostramos, também usando simulações computacionais, que o sincronismo entre dois RNLs, operando em regime periódico, é possível.

Em seguida, descrevemos o acoplador não-linear a fibra, ANL. Mostramos que a variação do perfil do coeficiente de acoplamento causa uma variação na forma da curva de transmissividade do acoplador permitindo, com isto, produzirmos "filtros ópticos de potência (intensidade)" tipo passa-banda. Por fim, descrevemos o efeito de birrefringência em fibra óptica não-linear, explorando a modulação cruzada de fase entre um pulso de alta intensidade e outro de baixa intensidade.

Uma vez apresentados os dispositivos não-lineares, foram propostas algumas utilizações dos mesmos em sistemas de comunicações quânticas. Inicialmente, propusemos o uso conjunto do RNL com o ANL para a produção dos bits da chave em um sistema de criptografia quântica polarimétrico. Aqui, o RNL gera pulsos de intensidade caótica e os entrega ao ANL que tem a função de selecioná-los, em suas saídas, segundo sua curva de transmissividade. Em cada saída do ANL é colocado um polarizador e, assim transformamos uma sequência de pulsos, vinda do RNL, com intensidades pseudo-aleatórias, em uma sequência de pulsos com polarização binária pseudo-aleatória, a ser usada no protocolo de criptografia quântica.

Propusemos, também, o uso de RNLs sincronizados para, através da propagação em fibra birrefringente, mascarar a fase de um sistema quântico interferométrico. Aqui, um pulso de intensidade muito baixa, proveniente do transmissor, é posto a se propagar conjuntamente com um pulso de alta intensidade em um pedaço de fibra birrefringente. Assim, o pulso de baixa intensidade sofre uma modulação de fase proporcional à intensidade do pulso mais intenso. Como este último provém da saída de um RNL, temos uma modulação caótica da fase dos pulsos que são enviados para o receptor. Sendo o sistema total um interferômetro, o receptor deve ser capaz de produzir a mesma fase caótica que o transmissor, para poder recuperar a informação; para isso, ele se utiliza de um RNL sincronizado com o do transmissor. Em ambos os casos acima expostos, alguns detalhes do protocolo de comunicação para os mesmos foram devidamente abordados.

CAPÍTULO IV

CONCLUSÕES E PERSPECTIVAS

4.1 Conclusões

Nesta tese procuramos abordar a comunicação quântica segundo três aspectos:

1. Aspectos físicos da comunicação quântica: Procuramos dar, no Capítulo I, uma introdução dos estados quânticos da luz em comunicações, descrevendo os estados de número e coerentes do contínuo. Utilizando os já conhecidos conceitos de discretização de modos contínuos e de definição de um operador fase Hermitiano (operador de Pegg-Barnnet), em um espaço de dimensão finita, descrevemos um método para o cálculo das funções densidade de probabilidade do número de fótons e da fase, a partir da envoltória de um pulso de luz coerente. Com este método, determinamos as estatísticas de número de fótons e da fase na saída de dispositivos ópticos passivos e lineares, como fibras ópticas, atenuadores e divisores de feixes, usando a envoltória do pulso incidente no dispositivo e as equações clássicas de propagação através do mesmo. Os resultados das FDPs do número de fótons se mostraram coerentes e confiáveis, enquanto que os resultados das FDPs da fase precisam de uma maior reflexão teórica, exceção feita às simulações em que a fase não sofreu gorjeio ao longo da propagação. Finalmente, mostramos a utilização do método num sistema óptico de criptografia quântica, simulando o protocolo BB84 num interferômetro a fibra. Os resultados numéricos obtidos concordam, com boa precisão, com os resultados analíticos, mostrando a confiabilidade do método. Mais ainda, devido à natureza aleatória da simulação, podemos simular a variação aleatória do número médio de fótons que acontece em sistemas reais e obter resultados sobre características de desempenho que sejam dependentes do número médio de fótons, como segurança e taxa de transmissão.
2. Aspectos matemáticos da comunicação quântica: No Capítulo II apresentamos aspectos da teoria quântica da informação. Enfatizamos as já conhecidas semelhanças entre as matrizes densidade de estados e coerência. Aplicamos os conceitos de probabilidade de resultados de medição e distinção entre matrizes densidade às matrizes coerência. Utilizando estas semelhanças, tratamos um sistema quântico polarimétrico através do uso das matrizes transferência e coerência, e dos parâmetros de Stokes. Assim, com argumentos puramente clássicos, propusemos o uso de um equalizador óptico, estrutura física e algoritmo de equalização, para recuperar a polarização, que varia devido à variação aleatória da birrefringência, sendo portanto um ruído clássico, em sistemas quânticos polarimétricos a fibra. Os resultados das simulações foram bastante satisfatórios, mostrando que o equalizador pode desempenhar bem a sua função. Em seguida, definimos o grau de pureza de estados quânticos e sua relação com a entropia dos mesmos. Calculamos, então, a distinção entre estados quânticos (distância de

Kolmogorov), a informação mútua e a fidelidade, como funções do grau de pureza. Terminamos o capítulo comentando sobre estados quânticos entrelaçados, puros e mistos, e medidas de entrelaçamento. Em particular, propusemos uma medida de entrelaçamento, usando a distância de Kolmogorov, e verificamos que a mesma é equivalente às já conhecidas entropia e índice de correlação.

3. Aspectos sistêmicos da comunicação quântica: No Capítulo III abordamos, de forma simplificada, o problema da geração, transmissão e recepção da informação quântica baseado nos sistemas já existentes. Propusemos, então, topologias de sistemas ópticos, usando dispositivos e efeitos não-lineares, capazes de realizar a comunicação quântica. Iniciamos o capítulo descrevendo, sucintamente, o ressonador não-linear a fibra, RNL, o acoplador não-linear a fibra, ANL, e o efeito da birrefringência em fibra óptica não-linear. Em particular, demonstramos a possibilidade de controle e de sincronização de RNLs através do uso de controladores nebulosos, e da variação da curva de transmissividade de um ANL, devido à variação do perfil do coeficiente de acoplamento. Aproveitando os dispositivos não-lineares expostos, foi proposto o uso conjunto do RNL com o ANL para a produção dos bits da chave em um sistema de criptografia quântica polarimétrico. Em um segundo desenvolvimento foi proposto o uso de RNLs sincronizados para, através da propagação em fibra altamente birrefringente, mascarar a fase de um sistema quântico interferométrico.

4.2 Perspectivas

A área de comunicações quânticas ainda é nova e há muitos desafios a serem enfrentados. A seguir, apontamos alguns dos quais podem tomar esta tese como ponto de partida:

1. Dar um maior aprofundamento teórico na geração da FDP da fase para estados coerentes a partir dos conceitos introduzidos no Capítulo I.
2. Dar um maior aprofundamento nos sistemas quânticos de comunicações, usando dispositivos ópticos não-lineares, como propostos no Capítulo III.
3. Desenvolver um protocolo de criptografia quântica a partir de estado mistos.
4. Considerar efeitos quânticos em sistemas não-lineares, como sólitons quânticos.

REFERÊNCIAS BIBLIOGRÁFICAS

CAPÍTULO I

- 1.1 K. J. Blow, Rodney Loudon e Simon J. D. Phoenix, "Continuum fields in quantum optics", *Physical Review A*, vol. 42, N° 7, pp. 4102-4114, October 1990.
- 1.2 David J. Santos, Rodney Loudon e Francisco J. Fraile-Peláez, "Continuum states and fields in quantum optics", *American Journal of Physics*, vol. 65, N° 2, pp. 126-132, February 1997.
- 1.3 Vladimir B. Braginsky e Farid Y.A. Khalili, *Quantum measurement*, Cambridge University Press, 1992.
- 1.4 A. Bruce Carlson, *Communication Systems*, 3rd edition, McGraw-Hill.
- 1.5 V. Buzek, A. D. Wilson-Gordon, P. L. Knight e W. K. Lai, "Coherent states in a finite-dimensional basis: Their phase properties and relationship to coherent states of light", *Physical Review A*, Vol. 45, N° 11, pp. 8079-8094, June 1992.
- 1.6 D. F. Walls e G. J. Milburn, *Quantum Optics*, Springer-Verlag, 1994.
- 1.7 Jonas Gomes e Luiz Velho, *Computação Gráfica: Imagem*, Série de Computação e Matemática, IMPA, SBM, 1994.
- 1.8 Stephen M. Barnett, Rodney Loudon, David Pegg e Simon J. D. Phoenix, "Communication using quantum states", *Journal of Modern Optics*, Vol. 41, N° 12, pp. 2351-2373, 1994.
- 1.9 Richard J. Hughes, George L. Morgan e C. Glen Peterson, "Practical quantum key over a 48-km optical fiber network", Los Alamos report LA-UR-99-1593, 1999.

CAPÍTULO II

- 2.1 Dennis Derickson (Editor), *Fiber Optic Test and Measurement*, Hewlett-Packard Professional Books, Prentice Hall, 1998.
- 2.2 Costas A. Eleftherianos, Dimitris Syvridis, Thomas Sphicopoulos e Costas Caroubalos, "Influence of polarisation mode dispersion on the transmission of parallel and orthogonally polarised solitons at 40 Gb/s", *Optics Communications*, N° 154, pp. 14-18, August 1998.

- 2.3 Joseph W. Simmons e Mark J. Guttman, *States, Waves and Photons: A Modern Introduction to Light*, Addison-Wesley, 1970.
- 2.4 Edward L. O'Neill, *Introduction To Statistical Optics*, Dover Publications, 1992.
- 2.5 G. Marchis, "Coherent Communications", *Fiber and Integrated Optics*, Vol. 11, pp. 277-317, 1992.
- 2.6 S. Betti, F. Curti, G. Marchis e E. Iannone, "Polarization Modulated Coherent Optical Communication Systems", *Fiber and Integrated Optics*, Vol. 10, pp. 291-307, 1991.
- 2.7 J. D. Frasson e H. Ilves, "Quantum Cryptography using polarization feedback", *Journal of Modern Optics*, Vol. 41, N° 12, pp. 2391-2396, 1994.
- 2.8 J. D. Frasson e H. Ilves, "Quantum cryptography using optical fibers", *Applied Optics*, Vol. 33, N° 14, pp. 2949-2954, May 1994.
- 2.9 J. Breguet, A. Muller e N. Gisin, "Quantum cryptography with polarized photons in optical fibres: Experimental and Practical limits", *Journal of Modern Optics*, Vol. 41, N° 12, pp. 2405-2412, 1994.
- 2.10 J. Breguet, A. Muller e N. Gisin, "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km", *Europhysics Letters*, N° 23, pp. 383-388, 1993.
- 2.11 Leonard Mandel e Emil Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995.
- 2.12 Seth Lloyd, "Capacity of the noise quantum channel", *Physical Review A*, Vol. 55, N° 3, pp. 1613-1622, March 1997.
- 2.13 N. Gisin e B. Huttner, "Quantum cloning, eavesdropping and Bell's inequality", *Physics Letters A*, Vol. 228, pp. 13-21, March 1997.
- 2.14 John Aaron Smolin, *Quantum Gates, Mixed-States Entanglement and Error-Correcting Codes*, Tese de Doutorado, University of California, 1996.
- 2.15 Charles H. Bennet, "Quantum Information", *Physica Scripta*, Vol. T76, pp. 210-217, 1998.
- 2.16 S. M. Barnett e S. J. D. Phoenix, "Entropy as a measurement of quantum optical correlation", *Physical Review A*, Vol. 40, N° 5, pp. 2404-2409, September 1989.
- 2.17 Stephen M. Barnett e Simon J. D. Phoenix, "Information theory, squeezing, and quantum correlations", *Physical Review A*, Vol. 44, N° 1, pp. 535-545, July 1991.

CAPÍTULO III

- 3.1 Govind P. Agrawal, *Nonlinear Fiber Optics*, Academic Press, New York, 1990.
- 3.2 Bruno Crosignani, "Nonlinear Effects in Optical Fibers", *Fiber and Integrated Optics*, Vol. 11, pp. 235-252, 1992.
- 3.3 Rubens Viana Ramos, *Estudo de Ressonadores Não-Lineares a Fibra e suas Aplicações em Processamento Óptico de Sinais para Comunicações*, Dissertação de Mestrado, Departamento de Microonda e Óptica, FEEC, UNICAMP, Março 1998.
- 3.4 B. Crosignani, B. Daino, P. Di Porto e S. Wabnitz, "Optical multistability in a fiber optic passive loop resonator", *Optics Communications*, Vol. 59, N° 4, pp. 309-312, September 1986.
- 3.5 M. Haelterman, S. Trillo e S. Wabnitz, "Dissipative modulation instability in a nonlinear dispersive ring cavity", *Optics Communications*, Vol. 91, N° 5, pp. 401-407, August 1992.
- 3.6 G. Steinmeyer, A. Buchholz, M. Hänsel, M. Heuer, A. Schwanche e F. Mitschke, "Dynamical pulse shaping in a nonlinear resonator", *Physical Review A*, Vol. 52, N° 1, July 1995.
- 3.7 Nelson Fielder-Ferrara e Carmen P. Cintra, *Caos uma introdução*, Edgard Blücher LTDA, 1994.
- 3.8 F. T. Arecchi e S. Boccaletti, "Adaptive strategies for recognition, noise filtering, control, synchronization and targeting of chaos", *Chaos*, Vol. 7, N° 4, pp. 621-634, 1997.
- 3.9 W. Martienssen, B. Hübinger e R. Doerner, "Chaotic cryptology", *Annalen der Physik*, Vol. 4, pp. 35-42, 1995.
- 3.10 Ron Daisy e Baruch Fischer, "Synchronization of chaotic nonlinear optical ring oscillators", *Optics Communications*, Vol. 133, pp. 282-286, January 1997.
- 3.11 Edward Ott, Celso Grebogi, e James A. Yorke, "Controlling Chaos", *Physical Review Letters*, Vol. 64, N° 11, pp. 1196-1199, March 1990.
- 3.12 Ian S. Shaw, e Marcelo Godoy Simões, *Controle e Modelagem Fuzzy*, 1ª edição, Edgard Blücher LTDA, 1999.
- 3.13 Timothy J. Ross, *Fuzzy Logic with Engineering Applications*, McGraw-Hill, 1997.

- 3.14 Rubens V. Ramos e Rui F. Souza, "Controlling Chaos in a Nonlinear Fiber Ring Resonator Using Fuzzy Logic", *Microwave and Optical Technology Letters*, Vol. 21, N° 5, pp. 378-380, June 1999.
- 3.15 Louis M. Pecora e Thomas L. Carrol, "Synchronization in Chaotic Systems", *Physical Review Letters*, Vol. 64, N° 8, pp. 821, February 1990.
- 3.16 Louis M. Pecora, Thomas L. Carrol, Greg A. Johnson, e Douglas J. Mar, "Fundamentals of synchronization in chaotic systems, concepts, and applications", *Chaos*, Vol. 7, N° 4, pp. 520-542, 1997.
- 3.17 S. Trillo, S. Wabnitz, E. M. Wright e G. I. Stegeman, "Soliton switching in fiber nonlinear directional couplers", *Optics Letters*, Vol. 13, N° 8, pp. 672-674, August 1988.
- 3.18 P. L. Chu, B. A. Malomed e G. D. Peng, "Soliton switching and propagation in nonlinear fiber couplers: analytical results", *J. Opt. Soc. Am. B*, Vol. 10, N° 8, pp. 1379-1385, August 1993.
- 3.19 P. L. Chu, Yuri S. Kivshar, Boris Malomed, Manuel L. Quiroga e Gang-Ding Peng, "Soliton controlling, switching, and splitting in nonlinear fused-fiber couplers", *J. Opt. Soc. Am. B*, Vol. 12, N° 5, pp. 898-903, May 1995.
- 3.20 D. J. Kaup, Boris A. Malomed e Richard S. Tasgal, "Internal dynamics of a vector soliton in a nonlinear optical fiber", *Physical Review E*, Vol. 48, N° 4, pp. 3049-3053, October 1993.
- 3.21 Curtis R. Menyuk, "Stability of solitons in birefringent optical fibers. II. Arbitrary amplitudes", *J. opt. Soc. Am. B*, Vol. 5, N° 2, pp. 392-402, February 1988.
- 3.22 Rubens V. Ramos e Rui F. Souza, "A Setup for Quantum Cryptography Using an All-Optical Chaotically Produced Key", *Microwave and Optical Technology Letters*, Vol. 24, N° 2, pp. 79-81, January 2000.

APÊNDICE A

- A1 Claude Cohen-Tannoudji, Bernard Diu e Franck Laloe, *Quantum Mechanics*, Vol. 1, John Wiley and Sons, 1997.
- A2 Bas C. Van Fraassen, *Quantum Mechanics: an Empiricist View*, Claredon Press Oxford, 1991.
- A3 Jean-Fançois Riendeau, *Simulation de Protocoles de Cryptographie Quantique*, Dissertação de Mestrado, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, Décembre 1995.

- A4** Vladimir B. Braginsky e Farid Ya. Khalili, *Quantum Measurement*, Cambridge University Press, 1992.
- A5** Jeroen Van Graaf, *Towards a Formal Definition of Security for Quantum Protocols*, Tese de Doutorado, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, Décembre 1997.
- A6** Christopher A. Fuchs, *Distinguishability and Accessible Information in Quantum Theory*, Tese de Doutorado, Department of Physics and Astronomy, University of New Mexico, December, 1995. URL: <http://xxx.lanl.gov>, quant-ph/9601020.
- A7** John Aaron Smolin, *Quantum Gates, Mixed-States Entanglement and Error-Correcting Codes*, Tese de Doutorado, University of California, 1996.
- A8** D. F. Walls e G. J. Milburn, *Quantum Optics*, Springer-Verlag, 1994.
- A9** Leonard Mandel e Emil Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995.
- A10** Rodney Loudon, *The Quantum Theory of Light*, Oxford Science Publications, 2nd Ed., 1995.

APÊNDICE B

- B1** Walter Greiner e Joachim Reinhardt, *Field Quantization*, Springer-Verlag, 1996.
- B2** Rodney Loudon, *The Quantum Theory of Light*, Oxford Science Publications, 2nd Ed., 1995.

APÊNDICE C

- C1** Simon J. D. Phoenix e Paul D. Townsend, "Quantum Cryptography: how to beat the code breakers using quantum mechanics", *Contemporary Physics*, Vol. 36, N° 3, pp. 165-195, 1995.
- C2** Charles H. Bennet, "Quantum Cryptography Using Any Two Nonorthogonal States", *Physical Review Letters*, Vol. 68, N° 21, pp. 3121-3124, May 1992.
- C3** K. J. Blow e Simon J. D. Phoenix, "On a fundamental theorem of quantum cryptography", *Journal of Modern Optics*, Vol. 40, N° 1, pp. 33-36, 1993.
- C4** J. D. Frasson e H. Ilves, "Quantum Cryptography using polarization feedback", *Jornal of Modern Optics*, Vol. 41, N° 12, pp. 2391-2396, 1994.
- C5** J. D. Frasson e H. Ilves, "Quantum cryptography using optical fibers", *Applied Optics*, Vol. 33, N° 14, pp. 2949-2954, May 1994.

- C6 J. Breguet, A. Muller e N. Gisin, "Quantum cryptography with polarized photons in optical fibres: Experimental and Practical Limits", *Journal of Modern Optics*, Vol. 41, N° 12, pp. 2405-2412, 1994.
- C7 J. Breguet, A. Muller e N. Gisin, "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km", *Europhysics Letters*, N° 23, pp. 383-388, 1993.
- C8 P. D. Townsend, J. G. Rarity e P. R. Tapster, "Single Photon Interference in 10 km Long Optical Fibre Interferometer", *Electronics Letters*, Vol. 29, N° 7, pp. 634-635, April 1993.
- C9 P. D. Townsend, J. G. Rarity e P. R. Tapster, "Enhanced Single Photon Fringe Visibility in a 10 km-Long Prototype Quantum Cryptography Channel", *Electronics Letters*, Vol. 29, N° 14, pp. 1291-1293, July 1993.
- C10 Paul D. Townsend e I. Thompson, "A quantum key distribution channel based on optical fibre", *Journal of Modern Optics*, Vol. 41, N° 12, pp. 2425-2433, 1994.
- C11 Paul D. Townsend, C. Marand, S. J. D. Phoenix, K. J. Blow e S. M. Barnett, "Secure optical communications systems using quantum cryptography", *Phil. Trans. R. Soc. Lond. A*, N° 354, pp. 805-817, 1996.
- C12 Anton Zeilinger, "Quantum Entanglement: A Fundamental Concept Finding its Applications" *Physica Scripta*, Vol. T76, pp. 203-209, 1998.
- C13 G. A. Barbosa, "Parametric Down-Conversion Luminescence: A Fertile Ground in Quantum Optics", *Brazilian Journal of Physics*, Vol. 25, N° 4, pp. 335-375, December 1995.
- C14 Artur K. Ekert, "Quantum Cryptography Based on Bell's Theorem", *Physical Review Letters*, Vol. 67, N° 6, pp. 661 August 1991.
- C15 Artur K. Ekert, John G. Rarity, Paul R. Tapster e G. Massimo Palma, "Practical Quantum Cryptography Based on Two-Photon Interferometry", *Physical Review Letters*, Vol. 69, N° 9, pp. 1293 August 1992.
- C16 P. R. Tapster, J. G. Rarity, e P.C.M. Owens, "Violation of Bell's Inequality over 4 km of Optical Fiber", *Physical Review Letters*, Vol. 73, N° 14, pp. 1923, October 1994.
- C17 Artur K. Ekert e G. Massimo Palma, "Quantum cryptography with interferometric quantum entanglement", *Journal of Modern Optics*, Vol. 41, N° 12, pp. 2413-2423, 1994.

APÊNDICE D

- D1** Peyton Z. Peebles, Jr. *Probability, Random Variables, and Random Signal Principles*, 3rd Ed., McGraw-Hill, 1993.
- D2** A. Bruce Carlson, *Communication Systems*, 3^a edition, McGraw-Hill.

APÊNDICE E

- E1** Dennis Derickson (Editor), *Fiber Optic Test and Measurement*, Hewlett-Packard Professional Books, Prentice Hall, 1998.
- E2** Leonard Mandel e Emil Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995.
- E3** Edward L. O'Neill, *Introduction To Statistical Optics*, Dover Publications, 1992.
- E4** G. Marchis, "Coherent Communications", *Fiber and Integrated Optics*, Vol. 11, pp. 277-317, 1992.
- E5** S. Betti, F. Curti, G. Marchis e E. Iannone, "Polarization Modulated Coherent Optical Communication Systems", *Fiber and Integrated Optics*, Vol. 10, pp. 291-307, 1991.

APÊNDICE F

- F1** Simon J. D. Phoenix, "Quantum cryptography without conjugate coding", *Physical Review A*, Vol. 48, N° 1, pp. 96-102, July 1993.
- F2** Stephen M. Barnett e Simon J. D. Phoenix, "Information-Theoretic limits to quantum cryptography", *Physical Review A*, Vol. 48, N° 1, pp. R5-R8, July 1993.
- F3** Christopher A. Fuchs, *Distinguishability and Accessible Information in Quantum Theory*, Tese de Doutorado, Department of Physics and Astronomy, University of New Mexico, December 1995. URL: <http://xxx.lanl.gov>, quant-ph/9601020.
- F4** Jeroen Van Graaf, *Towards a Formal Definition of Security for Quantum Protocols*, Tese de Doutorado, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, Décembre, 1997.
- F5** John Aaron Smolin, *Quantum Gates, Mixed-States Entanglement and Error-Correcting Codes*, Tese de Doutorado, University of California, 1996.
- F6** Charles H. Bennet, "Quantum Information", *Physica Scripta*, Vol. T76, pp. 210-217, 1998.

- F7** Benjamin Schumacher, "Information from Quantum Measurements", Complexity, Entropy, and the Physics of Information, *SFI Studies in the Sciences of Complexity*, Vol. VIII, Ed. W. H. Zurek, Addison-Wesley.
- F8** Richard Jozsa, Daniel Robb, e William K. Wootters, "Lower bound for accesible information in quantum mechanics", *Physical Review A*, Vol. 49, N° 2, pp. 668-677, February 1994.
- F9** Benjamin Schumacher, "Quantum coding", *Physical Review A*, Vol. 51, N° 4, pp. 2738-2747, April 1995.
- F10** Bas C. Van Fraassen, *Quantum Mechanics an Empiricist View*, Claredon Press Oxford, 1991.
- F11** S. M. Barnett e S. J. D. Phoenix, "Entropy as a measurement of quantum optical correlation", *Physical Review A*, Vol. 40, N° 5, pp. 2404-2409, September 1989.
- F12** Stephen M. Barnett e Simon J. D. Phoenix, "Information theory, squeezing, and quantum correlations", *Physical Review A*, Vol. 44, N° 1, pp. 535-545, July 1991.
- F13** Anton Zeilinger, "Quantum Entanglement: A Fundamental Concept Finding its Applications" *Physica Scripta*, Vol. T76, pp. 203, 1998.

APÊNDICE A

PRINCÍPIOS BÁSICOS DE MECÂNICA QUÂNTICA E ESTADOS QUÂNTICOS DA LUZ

A1. Introdução

Neste apêndice apresentamos, de forma reduzida e simplificada, os principais conceitos de mecânica e óptica quântica, utilizados ao longo da presente tese.

A2. Estados Quânticos, Operadores e Notação de Dirac

O estado quântico particular de um sistema físico pode ser representado por um vetor de estado, pertencente ao espaço de Hilbert que representa o sistema completo. Dirac introduziu uma notação simples para este vetor, conhecida como *ket* e seu complexo conjugado transposto, *bra*, cujas representações são, respectivamente [Refs. A1, A2]:

$$|\alpha\rangle = [\alpha_1 \quad \alpha_2 \quad \dots \quad \alpha_n]^T \quad (A1)$$

$$\langle\alpha| = [\alpha_1^* \quad \alpha_2^* \quad \dots \quad \alpha_n^*]. \quad (A2)$$

Sendo α uma variável associada ao estado que se quer representar (número de fótons, fase, polarização, etc...) e n a dimensão do espaço de Hilbert ao qual o sistema pertence, no caso presente, considerado finito. As ações sobre os estados quânticos (rotação do ângulo de polarização de um fóton, medição de um observável, etc...) são realizadas através da aplicação de um operador linear sobre o estado quântico que se quer atuar:

$$\hat{A}|\alpha\rangle = |\beta\rangle. \quad (A3)$$

Portanto, um operador linear faz um mapeamento, transformando um estado em outro (ou no mesmo, no caso de ser um autoestado do operador). Os operadores são normalmente representados por matrizes quadradas, com o número de linhas igual à dimensão do espaço de Hilbert do sistema. Os vetores *bra* e *ket* estão sujeitos às seguintes regras de utilização [Refs. A1, A2]:

I - Produto Escalar

$$\langle\alpha|\beta\rangle = (\langle\beta|\alpha\rangle)^* = \sum_{i=1}^n \alpha_i^* \beta_i \quad (A4)$$

II - Hermiticidade

Seja o operador $\hat{A}$ e as seguintes relações:

$$\hat{A}|\alpha\rangle = |c\rangle \quad (\text{A5})$$

$$\langle\alpha|\hat{A}^+ = \langle c| \quad (\text{A6})$$

$$\langle\alpha|\hat{A} = \langle d| , \quad (\text{A7})$$

onde o índice superior "+" indica o operador adjunto. Este, em termos matriciais, é o conjugado da transposta da matriz que representa o operador. Se $\hat{A}$ for Hermiteano, isto é, $\hat{A} = \hat{A}^+$, então:

$$\langle d| = \langle c| = (|c\rangle)^* . \quad (\text{A8})$$

Para um estado arbitrário $|b\rangle$, usando as Eqs. (A5) e (A6) temos:

$$\langle b|c\rangle = \langle b|\hat{A}|\alpha\rangle \quad (\text{A9})$$

$$\langle c|b\rangle = \langle\alpha|\hat{A}^+|b\rangle . \quad (\text{A10})$$

Portanto:

$$(\langle b|\hat{A}|\alpha\rangle)^* = \langle\alpha|\hat{A}^+|b\rangle . \quad (\text{A11})$$

Com $\hat{A}$ Hermiteano e usando a Eq. (A11), temos que:

$$\langle\alpha|\hat{A}|\alpha\rangle \in \mathfrak{R} . \quad (\text{A12})$$

III - Propriedades dos operadores lineares:

$$(\hat{A} + \hat{B})|\alpha\rangle = \hat{A}|\alpha\rangle + \hat{B}|\alpha\rangle \quad (\text{A13})$$

$$\hat{A}(|\alpha\rangle + |\beta\rangle) = \hat{A}|\alpha\rangle + \hat{A}|\beta\rangle . \quad (\text{A14})$$

Seja, agora, o operador $\hat{C} = \hat{A}\hat{B}$ e os vetores:

$$|\psi\rangle = \hat{A}|b\rangle \quad (\text{A15})$$

$$|b\rangle = \hat{B}|\alpha\rangle \quad (\text{A16})$$

$$|\psi\rangle = \hat{C}|\alpha\rangle = \hat{A}|b\rangle = \hat{A}\hat{B}|\alpha\rangle . \quad (\text{A17})$$

Então, temos:

$$\langle \psi | = \langle \alpha | \hat{C}^+ = \langle b | \hat{A}^+ = \langle \alpha | \hat{B}^+ \hat{A}^+ \quad (\text{A18})$$

e, portanto:

$$\hat{C}^+ = (\hat{A}\hat{B})^+ = \hat{B}^+ \hat{A}^+ . \quad (\text{A19})$$

A3. Autoestados e Autovalores

Pode acontecer que a aplicação de um operador a um vetor de estado leve ao mesmo vetor de estado multiplicado por uma constante. Neste caso, este vetor é chamado de autoestado, do referido operador, e a constante multiplicativa de autovalor:

$$\hat{A}|\alpha_n\rangle = \alpha_n|\alpha_n\rangle . \quad (\text{A20})$$

Os autovalores de operadores Hermiteanos são reais e os autoestados deste operadores são ortogonais entre si [Refs. A1, A2]:

$$\langle \alpha_n | \alpha_k \rangle = 0 . \quad (\text{A21})$$

Os autoestados de um operador Hermiteano formam um conjunto completo, isto é, formam uma base para o espaço ao qual pertencem; portanto, qualquer vetor de estado $|\psi\rangle$, pertencente ao mesmo espaço, pode ser escrito como uma combinação linear dos estados da base (autovalores discretos):

$$|\psi\rangle = \sum_n C_n |\alpha_n\rangle , \quad (\text{A22})$$

onde o valor máximo de n é a dimensão do espaço. Um coeficiente particular é dado por:

$$C_k = \frac{\langle \alpha_k | \psi \rangle}{\langle \alpha_k | \alpha_k \rangle} . \quad (\text{A23})$$

Sejam, agora, as operações de comutatividade:

$$(|a\rangle\langle b|)|c\rangle = |a\rangle(\langle b|c\rangle) \quad (\text{A24})$$

$$\langle c|(|a\rangle\langle b|) = (\langle c|a\rangle)\langle b| . \quad (\text{A25})$$

Usando as Eqs. (A22) - (A25) e considerando a base de autoestados ortonormal (vetores de módulo unitário), podemos escrever:

$$|\psi\rangle = \sum_n |\alpha_n\rangle \langle \alpha_n | \psi \rangle = \left(\sum_n |\alpha_n\rangle \langle \alpha_n| \right) |\psi\rangle \quad (\text{A26})$$

Observando a Eq. (A26), vemos que o termo entre parêntese define o operador identidade:

$$\hat{I} = \left(\sum_n |\alpha_n\rangle\langle\alpha_n| \right). \quad (\text{A27})$$

Por fim, qualquer operador pode ser definido através de seus autovalores e autoestados [Ref. A1]:

$$\hat{A} = \sum_n \alpha_n |\alpha_n\rangle\langle\alpha_n|. \quad (\text{A28})$$

Através das Eqs. (A28), (A1) e (A2) podemos obter a representação matricial do operador.

A4. Espaço Definido por Produto Tensorial

Sejam dois espaços de Hilbert, $\mathbf{H}_1$ e $\mathbf{H}_2$, de dimensões m e n , respectivamente. Então, para cada par de estados, representados pelos vetores $|\varepsilon\rangle \in \mathbf{H}_1$ e $|\lambda\rangle \in \mathbf{H}_2$, está associado um vetor pertencente ao espaço $\mathbf{H} = \mathbf{H}_1 \otimes \mathbf{H}_2$, denotado por $|\varepsilon\rangle \otimes |\lambda\rangle$ ou $|\varepsilon, \lambda\rangle$. Algumas propriedades deste espaço são [Ref. A1]:

$$(k|\varepsilon\rangle) \otimes |\lambda\rangle = |\varepsilon\rangle \otimes (k|\lambda\rangle) = k(|\varepsilon\rangle \otimes |\lambda\rangle) \quad (\text{A29})$$

$$|\varphi\rangle \otimes (|\varepsilon\rangle + |\lambda\rangle) = |\varphi\rangle \otimes |\varepsilon\rangle + |\varphi\rangle \otimes |\lambda\rangle. \quad (\text{A30})$$

Se $\{|u_i\rangle\}$ $i=1\dots m$ é uma base do espaço $\mathbf{H}_1$ e $\{|v_j\rangle\}$ $j=1\dots n$ é uma base do espaço $\mathbf{H}_2$, então o conjunto de vetores $|u_i\rangle \otimes |v_j\rangle$ formam uma base para o espaço $\mathbf{H}$ cuja dimensão é mn . Desta forma, se:

$$|\varepsilon\rangle = \sum_i a_i |u_i\rangle \quad (\text{A31})$$

$$|\lambda\rangle = \sum_j b_j |v_j\rangle \quad (\text{A32})$$

então:

$$|\varepsilon\rangle \otimes |\lambda\rangle = \sum_{i,j} a_i b_j |u_i\rangle \otimes |v_j\rangle. \quad (\text{A33})$$

O produto escalar, no espaço $\mathbf{H} = \mathbf{H}_1 \otimes \mathbf{H}_2$, é dado por:

$$\langle \varepsilon, \lambda | \eta, \varphi \rangle = \langle \varepsilon | \eta \rangle \langle \lambda | \varphi \rangle, \quad (\text{A34})$$

onde os estados $\{|\varepsilon\rangle, |\eta\rangle\} \in \mathbf{H}_1$ e $\{|\lambda\rangle, |\varphi\rangle\} \in \mathbf{H}_2$. Por fim, se $\hat{A}$ é um operador do espaço $\mathbf{H}_1$ e $\hat{B}$ um operador do espaço $\mathbf{H}_2$, então $\hat{A} \otimes \hat{B}$ é um operador linear no espaço $\mathbf{H} = \mathbf{H}_1 \otimes \mathbf{H}_2$, tal que:

$$[A \otimes B](|\varepsilon\rangle \otimes |\lambda\rangle) = (A|\varepsilon\rangle) \otimes (B|\lambda\rangle). \quad (\text{A35})$$

Por exemplo, qualquer estado de polarização de um fóton pode ser representado por uma combinação linear das polarizações $|H\rangle$ (horizontal) e $|V\rangle$ (vertical); estes dois estados formam uma base para um espaço de Hilbert de dimensão 2. O vetor de estado de polarização é representado por um vetor coluna cujos elementos são os coeficientes da expansão do estado na base de referência ($|H\rangle, |V\rangle$). Assim, se $|P_1\rangle$ e $|P_2\rangle$ são dois estados de polarização, temos:

$$|P_1\rangle = a|H\rangle + b|V\rangle \rightarrow \begin{pmatrix} a \\ b \end{pmatrix} \quad (\text{A36})$$

$$|P_2\rangle = c|H\rangle + d|V\rangle \rightarrow \begin{pmatrix} c \\ d \end{pmatrix}. \quad (\text{A37})$$

Se o sistema em consideração é composto por dois fótons com, por exemplo, um de polarização P_1 e outro com polarização P_2 , então o estado (não entrelaçado) do sistema é dado pelo produto tensorial das partes, ficando, então, representado por [Ref. A3]:

$$|P_1\rangle \otimes |P_2\rangle \equiv |P_1, P_2\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}. \quad (\text{A38})$$

Por sua vez, o produto tensorial de operadores é feito através do produto tensorial das matrizes que os representam. Para matrizes quadradas 2x2 temos [Ref. A3]:

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 & b_1 a_2 & b_1 b_2 \\ a_1 c_2 & a_1 d_2 & b_1 c_2 & b_1 d_2 \\ c_1 a_2 & c_1 b_2 & d_1 a_2 & d_1 b_2 \\ c_1 c_2 & c_1 d_2 & d_1 c_2 & d_1 d_2 \end{bmatrix} \quad (\text{A39})$$

No caso mais geral do produto tensorial de uma matriz $m \times n$ por outra $p \times q$, a matriz resultante será $mp \times nq$.

A5. Operador Densidade de Estados - ρ

Os estados quânticos mais simples são os estados puros. Tais estados podem ser completamente caracterizados por uma medição, isto é, se o estado é puro então existe uma medição que o identifica com 100% de acerto. Muitas vezes o estado quântico de uma entidade física não é conhecido com certeza, apenas as probabilidades de estar em um ou outro estado é que são conhecidas. Nesta situação, é dito que a entidade física está em uma mistura de estados. Esta mistura é completamente caracterizada pelo operador ou matriz

densidade de estados, ρ . Assim, se p_i é a probabilidade da entidade física estar no estado quântico puro $|u_i\rangle$, o operador densidade é dado por:

$$\rho = \sum_i p_i |u_i\rangle\langle u_i| = \sum_i p_i \rho_i . \quad (\text{A40})$$

A forma matricial de ρ , usando as Eqs. (A1) e (A2), para um espaço bidimensional, é:

$$|u_i\rangle = [a_i \quad b_i] \Rightarrow \rho = \sum_i p_i \begin{pmatrix} |a_i|^2 & a_i b_i^* \\ b_i a_i & |b_i|^2 \end{pmatrix} . \quad (\text{A41})$$

Se o estado é puro, então um dos p_i vale 1 e os demais são nulos. A matriz densidade sempre é Hermiteana, positiva definida e possui traço unitário. Uma das mais importantes características da matriz densidade é que o valor médio de um observável, representado pelo operador $\hat{A}$, é dado por:

$$\langle \hat{A} \rangle = \text{Tr}(\rho \hat{A}) , \quad (\text{A42})$$

onde Tr é o traço da matriz. O operador densidade representa a nossa ignorância sobre o valor de um observável. Vejamos o seguinte exemplo: Um transmissor vai enviar fótons polarizados, entre dois possíveis valores de polarização, para o receptor e este, através de uma medição de polarização, tentará identificar o estado que foi enviado. A Fig A1 mostra o diagrama esquemático.

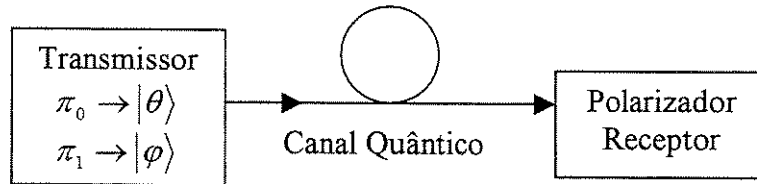


Fig. A1 - Sistema de comunicação quântica, usando fótons polarizados.

Na Fig. A1, π_0 é a probabilidade *a priori* do transmissor enviar o estado puro $\rho_0 = |\theta\rangle\langle\theta|$ e π_1 é a probabilidade *a priori* do transmissor enviar o estado puro $\rho_1 = |\phi\rangle\langle\phi|$. Como o receptor não sabe qual estado vai ser enviado, a matriz densidade que ele "enxerga" é o estado misto:

$$\rho = \pi_0 \rho_0 + \pi_1 \rho_1 . \quad (\text{A43})$$

Portanto, uma probabilidade clássica misturou os dois estados puros. Por vezes, acontece de um estado ser puro quando é produzido e, devido a interações com o meio externo, se torna misto. Este processo de um estado puro se tornar misto é conhecido como descoerência. Um exemplo comum disto é um fóton polarizado que, ao se propagar ao longo de uma fibra óptica comum, varia sua polarização. Como não sabemos para qual polarização o fóton

passou, podemos descrevê-la apenas estatisticamente, dentre os possíveis valores de polarização e, portanto, temos agora um estado misto.

A6. Medições de Observáveis Físicos

As variáveis de um sistema físico, passíveis de serem medidas, são conhecidas como *observáveis*. Todo observável físico é matematicamente representado por um operador Hermiteano e toda medição precisa deste observável resultará em um dos autovalores do correspondente operador. Se temos um conjunto de sistemas onde todos estão no estado $|\psi\rangle$ e realizamos a medição do observável representado pelo operador $\hat{H}$, em todos eles, então o valor médio deste observável, com o sistema no referido estado é dado pela quantidade [Ref. A1, A2]:

$$\langle \hat{H} \rangle = \langle \psi | \hat{H} | \psi \rangle . \quad (\text{A44})$$

Se E_n são os autovalores de $\hat{H}$ com autoestados $|E_n\rangle$, então, usando (A26), temos que:

$$\langle \psi | \hat{H} | \psi \rangle = \sum_k \langle \psi | E_k \rangle \langle E_k | \hat{H} | \sum_n \langle E_n | \psi \rangle | E_n \rangle = \sum_k \sum_n \langle E_k | \hat{H} | E_n \rangle \langle E_n | \psi \rangle \langle \psi | E_k \rangle . \quad (\text{A45})$$

Usando a Eq. (A20) e a condição de ortonormalidade, no primeiro termo da equação mais a direita de (A45), obtemos:

$$\langle E_k | \hat{H} | E_n \rangle = E_n \langle E_k | E_n \rangle = E_n \delta_{nk} \quad (\text{A46})$$

e, portanto, substituindo a Eq. (A46) em (A45), esta última fica reduzida a:

$$\langle \psi | \hat{H} | \psi \rangle = \sum_n |\langle E_n | \psi \rangle|^2 E_n = \sum_n p_n E_n . \quad (\text{A47})$$

Sendo p_n a probabilidade de encontrar o valor E_n como resultado da medição. Este tipo de medição é conhecida como medição de valor projetado, PVM [Refs. A1, A4]. Uma vez que uma medição foi realizada, a função de onda colapsa para o estado do resultado da medição. Se uma nova medição é realizada, ela apenas repete, com probabilidade 1, o resultado da medição anterior. Um tipo mais complexo de medição, chamada medição de operador de valor positivo, POM ou POVM, envolve uma evolução unitária entre o estado da entidade física a ser medida e o estado do aparelho de medição [Refs. A4-A7]. Neste tipo de medição, a repetição da medição não implica na repetição do resultado anterior com probabilidade 1. Aqui, a cada possível resultado da medição está associado um operador. Assim, os possíveis resultados (discretos) de uma medição $\{r_1, \dots, r_i, \dots, r_m\}$ correspondem aos operadores no conjunto $\hat{E} = \{\hat{E}_1, \dots, \hat{E}_i, \dots, \hat{E}_m\}$, onde todos os operadores $\hat{E}_i$ devem ser positivos semi-definidos e a condição:

$$\sum_i \hat{E}_i = I \quad (\text{A48})$$

deve ser satisfeita. A aplicação deste POVM a um sistema descrito pela matriz densidade ρ , resulta em uma distribuição de probabilidade dos possíveis resultados da medição, dada por [Refs. A5-A7]:

$$p(r_i | \rho) = \text{Tr}(\rho \hat{E}_i), \quad (\text{A49})$$

onde $p(r_i|\rho)$ é a probabilidade do resultado r_i ser obtido, dado que o estado do sistema é representado por ρ . Um PVM é um caso particular de um POVM. Por exemplo, se queremos medir a polarização de um fóton, usando um aparelho de medição que fornece dois possíveis resultados de saída, $\{\theta, \theta + \pi/2\}$, os operadores do POVM são [Ref. A5]:

$$\{\hat{E}_1, \hat{E}_2\} = \left\{ \begin{pmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & \sin^2(\theta) \end{pmatrix}, \begin{pmatrix} \sin^2(\theta) & -\cos(\theta)\sin(\theta) \\ -\cos(\theta)\sin(\theta) & \cos^2(\theta) \end{pmatrix} \right\}. \quad (\text{A50})$$

Este POVM é um PVM. Quando ele é aplicado a um fóton conhecido no estado $|H\rangle$ ($\theta = 0$ rad), a distribuição de probabilidade usando, a Eq. (A49), é $\langle \cos^2(\theta), \sin^2(\theta) \rangle = \langle 1, 0 \rangle$. Por outro lado, se o aparelho de medição decompõe a polarização em três possíveis resultados: $\{0, \pi/3, 2\pi/3\}$, o POVM é [Ref. A5]:

$$\left\{ \frac{2}{3} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \frac{2}{3} \begin{pmatrix} \varepsilon^2 & \varepsilon\sigma \\ \varepsilon\sigma & \sigma^2 \end{pmatrix}, \frac{2}{3} \begin{pmatrix} \varepsilon^2 & \varepsilon\sigma \\ \varepsilon\sigma & \sigma^2 \end{pmatrix} \right\}, \quad (\text{A51})$$

onde $\varepsilon = \cos(\pi/3) = -\cos(2\pi/3) = 1/2$ e $\sigma = \sin(\pi/3) = \sin(2\pi/3) = \sqrt{3}/2$, o que leva a Eq. (A51) para:

$$\{\hat{E}_1, \hat{E}_2, \hat{E}_3\} = \left\{ \begin{pmatrix} \frac{2}{3} & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{6} & \frac{\sqrt{3}}{6} \\ \frac{\sqrt{3}}{6} & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{6} & -\frac{\sqrt{3}}{6} \\ -\frac{\sqrt{3}}{6} & \frac{1}{2} \end{pmatrix} \right\}. \quad (\text{A52})$$

Aplicando este POVM a um fóton que está conhecido no estado $|V\rangle$ resulta, usando a Eq. (A49), na distribuição de probabilidade $\langle 0, 1/2, 1/2 \rangle$. Portanto, a polarização 0 (rad) nunca será obtida, enquanto que as polarizações $\pi/3$ e $2\pi/3$ (rad) ocorrerão com probabilidade 0,5.

A7. Princípio da Incerteza

Sejam os valores esperados dos observáveis relacionados aos operadores $\hat{A}$ e $\hat{B}$, para o sistema físico no estado $|\psi\rangle$ (Eq. A44):

$$\langle \hat{A} \rangle = \langle \psi | \hat{A} | \psi \rangle \quad (\text{A53})$$

$$\langle \hat{B} \rangle = \langle \psi | \hat{B} | \psi \rangle . \quad (\text{A54})$$

Sejam, também, suas variâncias:

$$(\Delta A)^2 = \langle \psi | (\hat{A} - \langle \hat{A} \rangle) (\hat{A} - \langle \hat{A} \rangle) | \psi \rangle = \langle \psi | \hat{A}^2 | \psi \rangle - \langle \psi | \hat{A} | \psi \rangle^2 \quad (\text{A55})$$

$$(\Delta B)^2 = \langle \psi | (\hat{B} - \langle \hat{B} \rangle) (\hat{B} - \langle \hat{B} \rangle) | \psi \rangle = \langle \psi | \hat{B}^2 | \psi \rangle - \langle \psi | \hat{B} | \psi \rangle^2 . \quad (\text{A56})$$

Se os operadores $\hat{A}$ e $\hat{B}$ são Hermiteanos e a relação de comutação entre eles é $[\hat{A}, \hat{B}] = i\hat{C}$, onde $\hat{C}$ pode ser outro operador Hermiteano, ou um número real, então mostra-se que [Ref. A1]:

$$(\Delta A)(\Delta B) \geq \frac{1}{2} \langle \psi | \hat{C} | \psi \rangle , \quad (\text{A57})$$

ou seja, dois observáveis conjugados, representados por operadores que não comutam, não podem ser precisamente conhecidos simultaneamente. No campo eletromagnético a fase e o número de fótons são observáveis conjugados representados por operadores que não comutam e, por isso, estão sujeitos à relação de incerteza. Portanto, se é conhecido que um campo eletromagnético tem precisamente n fótons, então nada se sabe sobre a sua fase.

A8. Representação de Schrödinger e Representação de Heisenberg

As representações de Schrödinger e Heisenberg provêm a evolução temporal dos sistemas quânticos de formas diferentes, porém com o mesmo resultado final. Na primeira, os operadores são independentes do tempo e toda a dependência temporal está nos estados quânticos. A evolução temporal é dada, então, pela equação de Schrödinger [Ref. A1]:

$$\frac{\partial |\alpha\rangle}{\partial t} = -\frac{i}{\hbar} \hat{H} |\alpha\rangle , \quad (\text{A58})$$

sendo $\hat{H}$ o operador Hamiltoniano (energia) do sistema. A solução de (A58) é [Ref. A1]:

$$|\alpha(r, t)\rangle = \exp\left(-\frac{i\hat{H}t}{\hbar}\right) |\alpha(r, 0)\rangle . \quad (\text{A59})$$

No quadro de Heisenberg, os estados são considerados fixos no tempo e toda a evolução temporal está nos operadores. Podemos obter a representação de Heisenberg a

partir da representação de Schrödinger da seguinte maneira: Seja o valor esperado do observável O , representado pelo operador $\hat{O}$, com o sistema no estado quântico $|\alpha\rangle$:

$$\langle \hat{O} \rangle = \langle \alpha(r, t) | \hat{O} | \alpha(r, t) \rangle. \quad (\text{A60})$$

Usando a Eq. (A59) em (A60), temos:

$$\langle \hat{O} \rangle = \langle \alpha(r, 0) | \hat{O}_H | \alpha(r, 0) \rangle \quad (\text{A61})$$

$$\hat{O}_H(t) = \exp\left(\frac{i\hat{H}t}{\hbar}\right) \hat{O} \exp\left(-\frac{i\hat{H}t}{\hbar}\right). \quad (\text{A62})$$

A Eq. (A62) é o operador $\hat{O}$ na representação de Heisenberg, isto é, variando no tempo. A lei de variação pode ser obtida derivando-se a Eq. (A62) em relação ao tempo. O resultado é [Ref. A1]:

$$\frac{d\hat{O}_H(t)}{dt} = \frac{i}{\hbar} [\hat{H}, \hat{O}_H(t)] + \left(\frac{\partial \hat{O}}{\partial t} \right)_H. \quad (\text{A63})$$

A Eq. (A63) tem a mesma forma da equação de evolução temporal de variáveis clássicas, sendo que, nesta última, não há a constante de Planck e usam-se os parênteses de Poisson no lugar da relação de comutação.

A9. Correlação Quântica - EPR (Einstein-Podolsky-Rosen)

Em alguns experimentos é possível a emissão de fótons com características físicas correlacionadas. Desta maneira, dois fótons podem ser gerados em um estado conjunto tal que, a medição de uma variável escolhida do fóton 1 determina completamente o resultado de uma medição da variável correspondente do fóton 2, mesmo estando ambos suficientemente separados, de tal forma que uma medição em um dos fótons não perturbe o outro. Esta situação ocorre, por exemplo, quando ambos os fótons são emitidos de uma mesma fonte em algum estado quântico entrelaçado, isto é, não fatorável, ou seja, não pode ser decomposto na forma da Eq. (A33). Seja, por exemplo, o estado entrelaçado de dois fótons com polarizações ortogonais:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}} (|90^\circ, 0^\circ\rangle - |0^\circ, 90^\circ\rangle) = \\ &= \frac{1}{\sqrt{2}} (|90^\circ\rangle_1 |0^\circ\rangle_2 - |0^\circ\rangle_1 |90^\circ\rangle_2) = \frac{1}{\sqrt{2}} (|90^\circ\rangle_1 \otimes |0^\circ\rangle_2 - |0^\circ\rangle_1 \otimes |90^\circ\rangle_2). \end{aligned} \quad (\text{A64})$$

O estado da Eq. (A64) afirma que, ou o fóton 1 tem polarização de 90° e o fóton 2 de 0° ou o contrário, o fóton 1 tem polarização de 0° e o fóton 2 de 90° . As polarizações só se

definirão no ato da medição. Se, por exemplo, a polarização do fóton 1 for medida e o resultado for 90° então, com probabilidade igual a 1, a polarização do fóton 2 será 0° , mesmo que o fóton 2 esteja distante o suficiente do fóton 1 para que não haja nenhuma interação entre eles. Devido à independência da distância entre as partes, esta correlação é dita ser não local. Devido à estas condições estranhas de ação à distância e definição do realismo físico só no momento da medição, postulou-se a existência de variáveis escondidas, ou seja, variáveis que não temos acesso para completar a mecânica quântica e explicar tais efeitos. Entretanto, mostra-se que, levando em consideração as variáveis escondidas, forma-se uma desigualdade, conhecida por desigualdade de Bell, na qual apenas estados quânticos entrelaçados a viola [Refs. A8, A9].

A10. Estados Quânticos da Luz - Número e Coerente

Para termos um completo entendimento das propriedades quânticas da luz, precisamos quantizar o campo eletromagnético. Como será mostrado no Apêndice B, isto geralmente é feito reconhecendo cada modo individual de uma cavidade como um oscilador harmônico quântico [Refs. A8-A10], fazendo a troca das variáveis dinâmicas por operadores e os clássicos parênteses de Poisson por relações de comutação adequadas. O Hamiltoniano (energia total) do campo eletromagnético, após a quantização, é igual à soma dos Hamiltonianos dos modos individuais (osciladores harmônicos quânticos) [Refs. A8-A10]:

$$\hat{H} = \sum_k \hbar \omega_k \left(\hat{a}_k^+ \hat{a}_k + \frac{1}{2} \right) = \sum_k \hbar \omega_k \hat{a}_k^+ \hat{a}_k + E_0^k = \sum_k \hbar \omega_k \hat{N}_k + E_0^k, \quad (\text{A65})$$

onde $\hat{a}_k^+$ e $\hat{a}_k$ são, respectivamente, os operadores criação e aniquilação dos quanta do k -ésimo modo, respectivamente, enquanto que ω_k é a frequência angular do referido modo. O termo $E_0^k = 0,5\hbar\omega_k$ é a energia do ponto zero, a flutuação do vácuo de cada modo. O termo $\hbar\omega_k$ é o quantum do modo k . O operador $\hat{N}_k$ é o operador número de quanta (fótons). Quando aplicado ao estado do campo eletromagnético, ele dá o número de fótons do modo. Agora, o significado da Eq. (A65) fica óbvio: a energia do k -ésimo modo é igual ao número de quanta do modo vezes o quantum de energia do modo mais a energia do vácuo (nenhum quanta) ou ponto zero. O princípio da incerteza de Heisenberg também aparece no campo eletromagnético, só que da seguinte forma [Ref. A4]:

$$\Delta n \Delta \varphi \geq K, \quad (\text{A66})$$

onde K é uma constante. A Eq. (A66) é o princípio da incerteza para o número de fótons (amplitude) e fase do campo eletromagnético. Ou seja, não podemos conhecer, com precisão perfeita e simultaneamente, a fase e a amplitude do campo. A Eq. (A66) facilita a compreensão e distinção dos principais estados quânticos da luz. Apesar de existirem diversos estados quânticos do campo eletromagnético, nos limitaremos a apresentação do estado de número, que é autoestado do operador número, e do estado coerente, que é autoestado do operador aniquilação.

A10.1 Estado de número

O estado de número, $|n\rangle$, é o estado do campo eletromagnético que possui exatos n fótons; em compensação, pelo princípio da incerteza, sua fase é completamente desconhecida. Os estados número formam uma base ortonormal para o espaço de Hilbert do qual fazem parte [Refs. A8-A10]:

$$\langle n|m\rangle = \delta_{nm} \quad (\text{A67})$$

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = 1 . \quad (\text{A68})$$

Os operadores aniquilação e criação, atuando no estado de número, resultam em [Refs. A8-A10]:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \quad (\text{A69})$$

$$\hat{a}^+|n\rangle = \sqrt{n+1}|n+1\rangle \quad (\text{A70})$$

$$\hat{N}|n\rangle = \hat{a}^+ \hat{a}|n\rangle = n|n\rangle . \quad (\text{A71})$$

Na Eq. (A71) vemos que o estado de número é um autoestado do operador número com autovalor igual ao número de quanta no modo. Um modo com n quanta pode ser obtido através da aplicação sucessiva do operador criação sobre o estado vácuo (nenhum fóton) [Refs. A8-A10]:

$$|n\rangle = \frac{(\hat{a}^+)^n}{\sqrt{n!}}|0\rangle . \quad (\text{A72})$$

Um campo multimodo com n_k fótons no k -ésimo modo é representado por [Refs. A8-A10]:

$$|n_1, n_2, \dots, n_k, \dots, n_m\rangle = |\{n\}_1^m\rangle . \quad (\text{A73})$$

onde m é o número de modos. O operador número total do campo é obtido somando os operadores números de cada modo individual [Refs. A8-A10]:

$$\hat{N} = \sum_k \hat{N}_k . \quad (\text{A74})$$

Portanto, o número total de quanta de um campo multimodo é obtido a partir de [Refs. A8-A10]:

$$\hat{N}|\{n\}\rangle = \sum_k n_k |\{n\}\rangle = n|\{n\}\rangle . \quad (\text{A75})$$

Ou seja, o número de fótons do campo é igual a soma do número de fótons de cada modo individual. Um fóton de frequência única ω_0 não tem localização, isto é, ele se estende por todo espaço-tempo (transformada de Fourier da função $\delta(\omega-\omega_0)$); entretanto, podemos obter estados de um fóton aproximadamente localizados, como um pacote de onda, se uma superposição de estados de um fóton em diferentes frequências é construída [Refs. A4, A9]:

$$|\psi\rangle = B \sum_k \exp\left(\frac{(\vec{k} - \vec{k}_0)^2}{2\sigma^2}\right) \exp(-i\vec{k} \cdot \vec{r}) |1_k, \{0\}\rangle . \quad (\text{A76})$$

A Eq. (A76) é uma superposição linear de estados de um fóton com diferentes vetores de onda, os quais seguem uma distribuição gaussiana normalizada pela constante B . A Eq. (A76) é um estado de um fóton porque é um autoestado do operador número, Eq. (A75), com autovalor unitário.

Embora tenhamos descrito apenas modos discretos nos quais o índice k enumerava as frequências, podemos também quantizar o campo eletromagnético em estados contínuos. Desta forma, o estado de número do contínuo pode ser representado por [Refs. A4]:

$$|n\rangle = \frac{1}{\sqrt{n!}} \int \mathcal{W}(\omega_1 \dots \omega_n) \hat{a}^\dagger(\omega_1) \dots \hat{a}^\dagger(\omega_n) d\omega_1 \dots d\omega_n |0\rangle \quad (\text{A77})$$

com

$$\int_0^\infty |\mathcal{W}(\omega_1, \dots, \omega_n)|^2 d\omega_1 \dots d\omega_n = 1 , \quad (\text{A78})$$

onde $|\mathcal{W}(\omega_1, \dots, \omega_n)|^2 d\omega_1 \dots d\omega_n$ dá a probabilidade de existir um fóton em cada intervalo $\omega_i + d\omega_i$, com $i=1, 2, \dots, n$. O Hamiltoniano do contínuo, por exemplo, é dado por:

$$\hat{H} = \int_0^\infty \hbar \omega \hat{a}^\dagger(\omega) \hat{a}(\omega) d\omega , \quad (\text{A79})$$

onde, em (A79), a energia do vácuo foi desconsiderada. Os estados do contínuo são trabalhados no Capítulo 1.

A10.2 Estado Coerente

O estado coerente é um estado quântico de mínima incerteza, com igualdade nas incertezas das quadraturas. As quadraturas são as partes real e imaginária do operador aniquilação. Ele é o estado quântico mais próximo de uma onda eletromagnética clássica. Um laser monomodo, operando bem acima do limiar, gera luz no estado coerente. Um estado coerente, representado por $|\alpha\rangle$, pode ser definido como uma superposição linear de estados número $|n\rangle$ [Refs. A8-A10]:

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_n \frac{\alpha^n}{(n!)^{\frac{1}{2}}} |n\rangle \quad (\text{A80})$$

com a normalização:

$$|\langle\alpha|\alpha\rangle|^2 = \exp(-|\alpha|^2) \sum_n \frac{(|\alpha|^2)^n}{n!} = 1, \quad (\text{A81})$$

onde α é um número complexo arbitrário que representa a amplitude do campo. Dois estados coerentes diferentes não são ortogonais [Refs. A8-A10]:

$$\langle\alpha|\beta\rangle = \exp\left(-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2\right) \sum_n \frac{(\alpha^*\beta)^n}{n!} = \exp\left(-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2 + \alpha^*\beta\right) \quad (\text{A82})$$

$$|\langle\alpha|\beta\rangle|^2 = \exp(-|\alpha - \beta|^2). \quad (\text{A83})$$

Os estados coerentes formam um conjunto mais que completo (*overcomplete*) de estados para o oscilador harmônico e, por isso, diferentes estados coerentes não são ortogonais. Os estados coerentes são autoestados do operador aniquilação [Refs. A8-A10]:

$$\hat{a}|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_n \frac{\alpha^n}{(n!)^{\frac{1}{2}}} \sqrt{n} |n-1\rangle = \alpha|\alpha\rangle. \quad (\text{A83})$$

O valor médio e a variância do número de fótons em um estado coerente são dados por [Refs. A8-A10]:

$$\langle\alpha|\hat{n}|\alpha\rangle = \exp(-|\alpha|^2) \sum_n \frac{|\alpha|^{2n} n}{(n!)} = |\alpha|^2 \quad (\text{A84})$$

$$\langle\alpha|\hat{n}^2|\alpha\rangle = \exp(-|\alpha|^2) \sum_n \frac{|\alpha|^{2n} n^2}{(n!)} = |\alpha|^4 + |\alpha|^2 \quad (\text{A85})$$

$$(\Delta n) = \langle\alpha|\hat{n}^2|\alpha\rangle - (\langle\alpha|\hat{n}|\alpha\rangle)^2 = |\alpha|^2. \quad (\text{A86})$$

Da expansão do estado coerente em estados de número, Eq. (A80), temos que a probabilidade do estado coerente ter n fótons é [Refs. A8-A10]:

$$|\langle n|\alpha\rangle|^2 = \exp(-|\alpha|^2) \sum_n \frac{|\alpha|^{2n}}{(n!)}, \quad (\text{A87})$$

que é uma distribuição Poissoniana com média $|\alpha|^2$ e desvio padrão $|\alpha|$. Pode-se criar estados coerentes a partir do estado vácuo através do operador deslocamento de Glauber,

$D(\alpha)$ [Refs. A8-A10]:

$$|\alpha\rangle = D(\alpha)|0\rangle, \quad (\text{A88})$$

onde o operador deslocamento é dado por [Refs. A8-A10]:

$$D(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}). \quad (\text{A89})$$

Devido às dificuldades práticas de construir fontes de luz de um fóton, estas têm sido, na prática, aproximadas por estados coerentes, produzidos por lasers semicondutores pulsados, fortemente atenuados, de forma que cada pulso tenha em média 0,1 fótons ($|\alpha|^2 = 0,1$), isto é, em média somente um pulso, em cada dez, tem um fóton. A Eq. (A80), com termos da ordem $O(|\alpha|^3)$ desprezados, dá:

$$|\alpha\rangle \approx \left(1 - \frac{|\alpha|^2}{2}\right) \left[|0\rangle + \alpha|1\rangle + \frac{\alpha^2}{\sqrt{2}}|2\rangle\right]. \quad (\text{A90})$$

Na maioria das vezes que este estado incidir num fotodiodo ele não causará uma contagem, devido à grande amplitude da componente vácuo (nenhum fóton); entretanto, quando ela ocorrer, será muito mais provável ser devido a um estado de um fóton do que a estados de mais de um fóton. Suponhamos, agora, que um pulso proveniente de um diodo laser, tendo largura τ , seja atenuado por um filtro com largura de banda suficiente, tal que a energia do pulso, após passar pelo filtro, seja aproximadamente $\hbar\bar{\omega}$, onde a barra indica a frequência angular central do pulso. Então, usando $E = \hbar\omega$ e $\Delta\omega\tau \geq 1$ obtemos $\Delta E \geq \hbar/\tau$; portanto, a energia do fóton deve estar no intervalo [Ref. A4]:

$$E = \hbar\bar{\omega} \pm \frac{\Delta E}{2} = \hbar\bar{\omega} \pm \frac{\hbar}{2\tau}. \quad (\text{A91})$$

De (A91) podemos inferir que, quanto mais $\hbar\bar{\omega} \gg \hbar/2\tau$ (o valor médio muito maior que o desvio) for verdadeiro, melhor o pacote de onda atenuado aproxima o estado de um fóton [Ref. A4]. Embora o estado coerente atenuado seja uma boa aproximação para o estado de número de um fóton, eles se comportam diferentemente e estas diferenças precisam ser levadas em conta quando do projeto de sistemas de comunicações quânticas.

A11. Operador de Fase

Assim como precisamos do operador Hermiteano número para determinar o número de fótons e suas médias estatísticas, também precisamos de um operador Hermiteano fase para determinar a fase do campo e as suas médias estatísticas. Para entendermos o operador fase, inicialmente dividimos os operadores criação e aniquilação em amplitude e fase [Refs. A8-A10]:

$$\hat{a} = (\hat{n} + 1)^{\frac{1}{2}} \hat{\exp}(i\varphi) \quad (\text{A92})$$

$$\hat{a}^+ = \hat{\exp}(-i\varphi) (\hat{n} + 1)^{\frac{1}{2}} . \quad (\text{A93})$$

As relações inversas de (A92) e (A93) são:

$$\hat{\exp}(i\varphi) = (\hat{n} + 1)^{-\frac{1}{2}} \hat{a} \quad (\text{A94})$$

$$\hat{\exp}(-i\varphi) = \hat{a}^+ (\hat{n} + 1)^{-\frac{1}{2}} . \quad (\text{A95})$$

A Eq. (A94) pode ser decomposta em estados de número [Refs. A8-A10]:

$$\hat{\exp}(i\varphi) = \sum_{n=0}^{\infty} |n\rangle \langle n+1| . \quad (\text{A96})$$

Temos, ainda, as propriedades [Refs. A8-A10]:

$$\hat{\exp}(i\varphi) \hat{\exp}(-i\varphi) = 1 \quad (\text{A97})$$

$$\hat{\exp}(-i\varphi) \hat{\exp}(i\varphi) \neq 1 . \quad (\text{A98})$$

Usando (A94) e (A95) é fácil verificar que [Refs. A8-A10]:

$$\hat{\exp}(i\varphi) |n\rangle = (\hat{n} + 1)^{-\frac{1}{2}} \sqrt{n} |n-1\rangle = \begin{cases} |n-1\rangle & \text{para } n \neq 0 \\ 0 & \text{para } n = 0 \end{cases} \quad (\text{A99})$$

$$\hat{\exp}(-i\varphi) |n\rangle = \hat{a}^+ \sqrt{n+1} |n\rangle = |n+1\rangle . \quad (\text{A100})$$

Os autoestados do operador $\hat{\exp}(i\varphi)$ são os estados:

$$|\exp(i\varphi)\rangle = \sum_{n=0}^{\infty} \exp(in\varphi) |n\rangle, \quad -\pi < \varphi \leq \pi . \quad (\text{A101})$$

Estes autoestados não são ortogonais entre si, mas são normalizados por:

$$\int_{-\pi}^{\pi} |\exp(i\varphi)\rangle \langle \exp(i\varphi)| d\varphi = 2\pi . \quad (\text{A102})$$

Os operadores $\hat{\exp}(i\varphi)$ e $\hat{\exp}(-i\varphi)$ são chamados operadores fase de Susskind-Glogower (SG). Os operadores SG não são Hermiteanos e, por isso, não representam quantidades observáveis do campo eletromagnético. Entretanto, as seguintes combinações destes operadores são Hermiteanas [Refs. A8-A10]:

$$\hat{\cos}(\varphi) = \frac{1}{2} \{ \hat{\exp}(i\varphi) + \hat{\exp}(-i\varphi) \} \quad (\text{A103})$$

$$\hat{\sin}(\varphi) = \frac{1}{2i} \{ \hat{\exp}(i\varphi) - \hat{\exp}(-i\varphi) \} . \quad (\text{A104})$$

Pode-se, ainda, observar que o operador número não comuta com os operadores das Eqs. (A103) e (A104) [Refs. A8-A10].

$$[\hat{n}, \hat{\cos}(\varphi)] = -i \hat{\sin}(\varphi) \quad (\text{A105})$$

$$[\hat{n}, \hat{\sin}(\varphi)] = i \hat{\cos}(\varphi) . \quad (\text{A106})$$

Portanto, a amplitude e as funções cosseno e seno da fase do campo eletromagnético não podem ser precisamente especificadas simultaneamente. As relações de incerteza são [Refs. A8-A10]:

$$(\Delta n)(\Delta \cos(\varphi)) \geq \frac{1}{2} |\langle \hat{\sin}(\varphi) \rangle| \quad (\text{A107})$$

$$(\Delta n)(\Delta \sin(\varphi)) \geq \frac{1}{2} |\langle \hat{\cos}(\varphi) \rangle| . \quad (\text{A108})$$

Por fim, o valor médio e a variância dos operadores seno e cosseno, no estado de número, são [Refs. A8-A10]:

$$\langle n | \hat{\cos}(\varphi) | n \rangle = \langle n | \hat{\sin}(\varphi) | n \rangle = 0 \quad (\text{A109})$$

$$\langle n | \hat{\cos}^2(\varphi) | n \rangle = \langle n | \hat{\sin}^2(\varphi) | n \rangle = \begin{cases} \frac{1}{2} & \text{para } n \neq 0 \\ \frac{1}{4} & \text{para } n = 0 \end{cases} . \quad (\text{A110})$$

Realmente, no estado de número a fase é uniformemente distribuída e o valor médio do seno ou cosseno de uma variável uniformemente distribuída no intervalo $[-\pi, \pi]$ é nulo. A distribuição de probabilidade dos resultados da medição de fase, no intervalo $[-\pi, \pi]$, realizada no estado genérico $|\beta\rangle$, é dada por:

$$p(\beta) = \frac{1}{2\pi} |\langle \exp(i\varphi) | \beta \rangle|^2 \quad (\text{A111})$$

$$\int_{-\pi}^{\pi} p(\beta) d\beta = 1 . \quad (\text{A112})$$

Como visto, os operadores de SG não são Hermiteanos. Visando desenvolver um operador fase Hermiteano, Pegg e Barnett propuseram estados de fase bem definidos e um operador

fase pertencentes a um espaço finito. Seja o estado $|\theta_0\rangle$, definido em um sub-espaço finito, de dimensão $s+1$, dado por [Ref. A8]:

$$|\theta_0\rangle = (s+1)^{-1/2} \sum_{n=0}^s \exp(in\theta_0) |n\rangle, \quad (\text{A113})$$

onde θ_0 é a fase inicial de referência. Sejam, agora, os estados $|\theta_m\rangle$ definidos por [Ref. A8]:

$$|\theta_m\rangle = \exp\left(\frac{i\hat{a}^+ \hat{a} m 2\pi}{s+1}\right) |\theta_0\rangle \quad (\text{A114})$$

com

$$\theta_m = \theta_0 + \frac{2\pi m}{s+1}, \quad (\text{A115})$$

$m = 0, 1, 2, \dots, s$, sendo θ_m pertencente ao intervalo $[\theta_0, \theta_0 + 2\pi)$. Os estados $|\theta_m\rangle$ são ortogonais entre si e formam uma base para o espaço de Hilbert truncado, de dimensão $s+1$. O operador Hermiteano fase para o espaço de dimensão $s+1$ é definido usando a Eq. (A28) [Ref. A8]:

$$\hat{\theta} = \sum_{m=0}^s \theta_m |\theta_m\rangle \langle \theta_m|. \quad (\text{A116})$$

As distribuições estatísticas de medições da fase para o estado puro $|\beta\rangle$ e para o estado misto ρ , são dadas por [Ref. A8]:

$$p(\theta) = |\langle \theta_m | \beta \rangle|^2 \quad (\text{A117})$$

$$p(\theta) = \frac{s+1}{2\pi} \langle \theta | \rho | \theta \rangle = \frac{1}{2\pi} \sum_{n,m} \exp[i(m-n)\theta] \langle n | \rho | m \rangle \quad (\text{A118})$$

APÊNDICE B

QUANTIZAÇÃO DO CAMPO ELETROMAGNÉTICO

B1. Quantização do Campo Eletromagnético no Vácuo

A quantização do campo eletromagnético geralmente é feita por um procedimento conhecido como segunda quantização [Refs. B1, B2]. O conceito de fóton surge naturalmente neste processo. Mostramos, agora, a quantização do campo eletromagnético no vácuo, seguindo de perto a Referência B2. Sejam as equações de Maxwell:

$$\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t} \quad (\text{B1})$$

$$\nabla \times \vec{H} = \vec{J} + \frac{\partial \vec{D}}{\partial t} \quad (\text{B2})$$

$$\nabla \cdot \vec{D} = \rho \quad (\text{B3})$$

$$\nabla \cdot \vec{B} = 0 \quad (\text{B4})$$

Usando a identidade vetorial I $\nabla \cdot (\nabla \times) = 0$, em (B4), obtemos:

$$\vec{B} = \nabla \times \vec{A} \quad (\text{B5})$$

sendo $\vec{A}$ o vetor potencial. Substituindo (B5) em (B1), chegamos a:

$$\nabla \times \vec{E} - \frac{\partial \vec{B}}{\partial t} = \nabla \times \vec{E} - \frac{\partial (\nabla \times \vec{A})}{\partial t} = \nabla \times \left(\vec{E} + \frac{\partial \vec{A}}{\partial t} \right) = 0 \quad (\text{B6})$$

Usando, agora, a identidade vetorial II $\nabla \times (\nabla \cdot) = 0$, em (B6), obtemos:

$$\vec{E} = -\nabla \phi - \frac{\partial \vec{A}}{\partial t} \quad (\text{B7})$$

sendo ϕ o potencial escalar. Portanto, com as Eqs. (B5) e (B7), podemos obter os campos elétrico e indução magnética através dos potenciais escalar e vetor. Substituindo (B5) e (B7) em (B2), ficamos com:

$$\nabla \times \nabla \times \vec{A} = \mu \vec{J} - \mu \varepsilon_0 \frac{\partial \nabla \phi}{\partial t} - \mu \varepsilon_0 \frac{\partial^2 \vec{A}}{\partial t^2} . \quad (\text{B8})$$

Usando, agora, a identidade vetorial III $\nabla \times \nabla \times = \nabla(\nabla \cdot) - \nabla^2$, em (B8), obtemos:

$$\nabla(\nabla \cdot \vec{A}) - \nabla^2 \vec{A} = \mu \vec{J} - \mu \varepsilon_0 \frac{\partial \nabla \phi}{\partial t} - \mu \varepsilon_0 \frac{\partial^2 \vec{A}}{\partial t^2} . \quad (\text{B9})$$

Substituindo, agora, (B7) em (B3), obtemos:

$$\nabla \cdot \vec{D} = \varepsilon_0 \nabla \cdot \vec{E} = \varepsilon_0 \nabla \cdot \left(-\nabla \phi - \frac{\partial \vec{A}}{\partial t} \right) = -\varepsilon_0 \nabla^2 \phi - \varepsilon_0 \nabla \cdot \frac{\partial \vec{A}}{\partial t} = \rho . \quad (\text{B10})$$

As Eqs. (B9) e (B10) são as equações de evolução dos potenciais [Ref. B2]. Percebemos que, se A_0 e ϕ_0 são soluções de (B9) e (B10), então

$$\vec{A} = \vec{A}_0 - \nabla \Psi \quad (\text{B11})$$

$$\phi = \phi_0 + \frac{\partial \Psi}{\partial t} \quad (\text{B12})$$

também satisfazem as Eqs. (B9) e (B10), sendo Ψ uma função arbitrária de r e t obedecendo a $\nabla \times \nabla \Psi = 0$. Portanto, $\vec{E}$ e $\vec{B}$ são invariantes segundo as transformações acima, conhecida como transformação de calibre. O calibre de Coulomb é definido como [Ref. B2]:

$$\nabla \cdot \vec{A} = 0 . \quad (\text{B13})$$

Usando o calibre de Coulomb nas equações (B9) e (B10) temos:

$$-\nabla^2 \vec{A} + \mu \varepsilon_0 \frac{\partial \nabla \phi}{\partial t} + \mu \varepsilon_0 \frac{\partial^2 \vec{A}}{\partial t^2} = \mu \vec{J} \quad (\text{B14})$$

$$\nabla^2 \phi = -\frac{\rho}{\varepsilon_0} . \quad (\text{B15})$$

Na Eq. (B15), percebemos que o potencial escalar ϕ satisfaz à equação de Poisson da eletrostática, cuja solução é [Ref. B2]:

$$\phi(\vec{r}, t) = \frac{1}{4\pi\varepsilon_0} \int \frac{\rho(\vec{r}', t)}{|\vec{r} - \vec{r}'|} d\vec{r}' . \quad (\text{B16})$$

Usando, agora, o teorema de Helmholtz, representamos a densidade de corrente, que é a fonte para o potencial vetor, na soma de uma componente solenoidal (transversal) e outra

irrotacional (longitudinal) [Ref. B2]:

$$\vec{J} = \vec{J}_T + \vec{J}_L , \quad (\text{B17})$$

onde

$$\nabla \cdot \vec{J}_T = 0 \quad (\text{B18})$$

$$\nabla \times \vec{J}_L = 0 . \quad (\text{B19})$$

Aplicando (B17) e (B18) na equação da continuidade, temos:

$$\nabla \cdot \vec{J} + \frac{\partial \rho}{\partial t} = \nabla \cdot (\vec{J}_T + \vec{J}_L) + \frac{\partial \rho}{\partial t} = 0 \Rightarrow \quad (\text{B20})$$

$$\nabla \cdot \vec{J}_L = -\frac{\partial \rho}{\partial t} . \quad (\text{B21})$$

Fazendo uso da identidade vetorial II em (B19), obtemos:

$$\vec{J}_L = \nabla \Omega . \quad (\text{B22})$$

Logo, usando (B21) e (B22), temos:

$$\nabla \cdot \vec{J}_L = \nabla \cdot (\nabla \Omega) = \nabla^2 \Omega = -\frac{\partial \rho}{\partial t} . \quad (\text{B23})$$

Obtendo o valor de ρ , em (B15), e substituindo em (B23), chegamos a:

$$\Omega = \varepsilon_0 \frac{\partial \phi}{\partial t} . \quad (\text{B24})$$

Portanto:

$$\vec{J}_L = \varepsilon_0 \nabla \left(\frac{\partial \phi}{\partial t} \right) . \quad (\text{B25})$$

Utilizando (B25) e (B17) em (B14), resulta na equação:

$$-\nabla^2 \vec{A} + \mu \varepsilon_0 \frac{\partial^2 \vec{A}}{\partial t^2} = \mu \vec{J}_T . \quad (\text{B26})$$

A Eq. (B26) afirma que só a componente transversal da densidade de corrente é a fonte do potencial vetor. Seja, agora, o teorema de Helmholtz aplicado ao campo elétrico, $\vec{E} = \vec{E}_L + \vec{E}_T$. De (B7), (B13) e da identidade vetorial II, verifica-se que:

$$\vec{E}_T = -\frac{\partial \vec{A}}{\partial t} \quad (\text{B27})$$

$$\vec{E}_L = -\nabla \phi . \quad (\text{B28})$$

Como $\nabla \cdot \vec{B} = 0$, isto é, a indução magnética é puramente solenoidal, temos que:

$$\vec{B}_T = \vec{B} \quad (\text{B29})$$

$$\vec{B}_L = 0 . \quad (\text{B30})$$

Portanto, no calibre de Coulomb, pelas Eqs. (B16) e (B28), vemos que a densidade de cargas é responsável pela componente longitudinal do campo elétrico enquanto que, pelas Eqs. (B26) e (B27), vemos que a componente transversal da densidade de corrente é responsável pela componente transversal do campo elétrico.

Na propagação de uma onda eletromagnética no vácuo, temos $\vec{J} = 0$. O campo é suposto estar confinado em uma cavidade cúbica imaginária de lado L , volume $v=L^3$, com condições de contorno periódicas. A Eq. (B26) fica da forma:

$$-\nabla^2 \vec{A} + \mu\epsilon_0 \frac{\partial^2 \vec{A}}{\partial t^2} = 0 . \quad (\text{B31})$$

A Eq. (B31) tem solução do tipo [Ref. B2]:

$$\vec{A} = \sum_n \left\{ \vec{A}_n(t) \exp(i\vec{k} \cdot \vec{r}) + \vec{A}_n^*(t) \exp(-i\vec{k} \cdot \vec{r}) \right\} , \quad (\text{B32})$$

$$\vec{k} = k_x \hat{i} + k_y \hat{j} + k_z \hat{k} , \quad (\text{B33})$$

sendo

$$k_m = \frac{2\pi n_m}{L}; \quad m = x, y, z \quad (\text{B34})$$

$$n_m = 0, \pm 1, \pm 2, \pm 3, \dots \quad (\text{B35})$$

Para que o calibre de Coulomb (Eq. B13) seja satisfeito, devemos ter:

$$\vec{k} \cdot \vec{A}_n(t) = \vec{k} \cdot \vec{A}_n^*(t) = 0 . \quad (\text{B36})$$

Existem duas direções (polarizações) de $A_n(t)$, para cada k . Substituindo (B32) em (B31) encontramos que os A_n devem obedecer à equação [Ref. B2]:

$$\frac{\partial^2 \vec{A}_n(t)}{\partial t^2} + \omega_n^2 \vec{A}_n(t) = 0 \quad (\text{B37})$$

$$\omega_n = \mu \varepsilon_0 k , \quad (\text{B38})$$

cuja solução é:

$$\vec{A}_n(t) = \vec{A}_n \exp(-i\omega_n t) . \quad (\text{B39})$$

Portanto, a solução completa do vetor potencial é [Ref. B2]:

$$\vec{A} = \sum_n \left\{ \vec{A}_n \exp(-i\omega_n t + i\vec{k} \cdot \vec{r}) + \vec{A}_n^* \exp(i\omega_n t - i\vec{k} \cdot \vec{r}) \right\} . \quad (\text{B40})$$

Substituindo a Eq. (B40) nas Eqs. (B5) e (B27), obtemos:

$$\vec{B}_n = i\vec{k} \times \left\{ \vec{A}_n \exp(-i\omega_n t + i\vec{k} \cdot \vec{r}) - \vec{A}_n^* \exp(i\omega_n t - i\vec{k} \cdot \vec{r}) \right\} \quad (\text{B41})$$

$$\vec{E}_{Tn} = i\omega_n \left\{ \vec{A}_n \exp(-i\omega_n t + i\vec{k} \cdot \vec{r}) - \vec{A}_n^* \exp(i\omega_n t - i\vec{k} \cdot \vec{r}) \right\} . \quad (\text{B42})$$

A energia média em um ciclo, do modo n na cavidade, é dada por [Ref. B2]:

$$\bar{E}_n = \frac{1}{2} \int_0^{2\pi} \int_v \left(\varepsilon_0 |\vec{E}_n|^2 + \mu^{-1} |\vec{B}_n|^2 \right) dv d(\omega_n t) . \quad (\text{B43})$$

Substituindo (B41) e (B42) em (B43), obtemos:

$$\bar{E}_n = 2\varepsilon_0 v \omega_n^2 \vec{A}_n \cdot \vec{A}_n^* . \quad (\text{B44})$$

Até o presente momento, apenas fórmulas clássicas foram envolvidas. Para realizar a quantização faremos, agora, algumas transformações de variáveis para igualar a energia em cada modo do campo eletromagnético à energia de um oscilador harmônico e este será identificado com o oscilador harmônico quântico, finalizando a quantização. Sejam as transformações [Ref. B2]:

$$\vec{A}_n = \left(4\varepsilon_0 v \omega_n^2 \right)^{-\frac{1}{2}} (\omega_n Q_n + iP_n) \vec{\varepsilon}_n \quad (\text{B45})$$

$$\vec{A}_n^* = \left(4\varepsilon_0 v \omega_n^2 \right)^{-\frac{1}{2}} (\omega_n Q_n - iP_n) \vec{\varepsilon}_n , \quad (\text{B46})$$

nas quais, as quantidades escalares Q_n e P_n representam a posição e o momento do oscilador harmônico. $\vec{\varepsilon}_n$ é o vetor unitário de polarização para o modo n . Assim, a Eq. (B44) fica da forma:

$$\bar{E}_n = \frac{1}{2} (P_n^2 + \omega_n^2 Q_n^2) , \quad (\text{B47})$$

que é a forma da energia média do oscilador harmônico clássico. O Hamiltoniano clássico total é formado pela soma sobre todos os n modos e nas duas direções independentes de $\vec{\varepsilon}_n$. Por sua vez, o Hamiltoniano do oscilador harmônico quântico unidimensional, com massa unitária, é [Refs. B1, B2]:

$$\hat{H} = \frac{1}{2}(\hat{p}^2 + \omega\hat{q}^2), \quad (\text{B48})$$

onde os operadores posição e momento, $\hat{q}$ e $\hat{p}$, obedecem à relação de comutação [Refs. B1, B2]:

$$[\hat{q}, \hat{p}] = i\hbar. \quad (\text{B49})$$

Define-se, agora, os operadores criação $\hat{a}^+$ e aniquilação $\hat{a}$, a partir dos operadores $\hat{q}$ e $\hat{p}$ [Refs. B1, B2]:

$$\hat{a} = (2\hbar\omega)^{-\frac{1}{2}}(\omega\hat{q} + i\hat{p}) \quad (\text{B50})$$

$$\hat{a}^+ = (2\hbar\omega)^{-\frac{1}{2}}(\omega\hat{q} - i\hat{p}). \quad (\text{B51})$$

As relações inversas de (B50) e (B51) são:

$$\hat{q} = \left(\frac{\hbar}{2\omega}\right)^{-\frac{1}{2}}(\hat{a} + \hat{a}^+) \quad (\text{B52})$$

$$\hat{p} = -i\left(\frac{\hbar\omega}{2}\right)^{-\frac{1}{2}}(\hat{a} - \hat{a}^+). \quad (\text{B53})$$

Usando (B52), (B53) e (B49), vemos que os operadores $\hat{a}^+$ e $\hat{a}$ obedecem à relação de comutação de bósons [Refs. B1, B2]:

$$[\hat{a}, \hat{a}^+] = 1. \quad (\text{B54})$$

Com isto, o Hamiltoniano (B48) fica sendo [Ref. B1, B2]:

$$\hat{H} = \hbar\omega\left(\hat{a}^+\hat{a} + \frac{1}{2}\right). \quad (\text{B55})$$

Por fim, a quantização é feita associando um oscilador quanto-mecânico a cada modo k do campo. Sejam $\hat{a}_k^+$ e $\hat{a}_k$ os operadores criação e aniquilação que criam e destroem um quantum de energia, $\hbar\omega_k$, no modo do campo eletromagnético da cavidade, com número de onda k . O número de fótons, pertencente ao referido modo, é dado pelo autovalor n_k do

operador número $\hat{N}_k = \hat{a}_k^\dagger \hat{a}_k$, definido na Seção A10 do Apêndice A. O estado do campo eletromagnético total na cavidade pode ser especificado pelo número de fótons $n_{k1}, n_{k2}, n_{k3} \dots$ excitados no conjunto completo dos modos da cavidade $k_1, k_2, k_3 \dots$. Novamente, para cada número de onda k existem duas direções (polarizações) possíveis do modo. O estado total do campo pode ser escrito como [Refs. B1, B2]:

$$|n_{k1}, n_{k2}, n_{k3} \dots\rangle = |n_{k1}\rangle |n_{k2}\rangle |n_{k3}\rangle \dots \quad (\text{B56})$$

Uma vez que os diferentes modos da cavidade são independentes, o estado do campo total pode ser escrito como o produto dos modos individuais. Um operador, que se refira a um modo particular, afeta apenas os fótons naquele modo particular [Refs. B1, B2]:

$$\hat{a}_{ki}^\dagger |n_{k1}, n_{k2}, n_{k3} \dots n_{ki} \dots\rangle = \sqrt{n_{ki} + 1} |n_{k1}, n_{k2}, n_{k3} \dots n_{ki+1} \dots\rangle. \quad (\text{B57})$$

Para simplificar a notação é usual a simbologia [Ref. B1, B2]:

$$|\{n_k\}\rangle = |n_{k1}\rangle |n_{k2}\rangle |n_{k3}\rangle \dots \quad (\text{B58})$$

Por fim, o operador vetor potencial para o modo k é obtido colocando os coeficientes da Eq. (B40) em função dos operadores criação e aniquilação, através das Eqs. (B45), (B46), (B52) e (B53), trocando os escalares Q e P pelos operadores $\hat{q}$ e $\hat{p}$. Assim, obtemos [Refs. B1, B2]:

$$\vec{A}_k = \left(\frac{\hbar V \omega_k}{2 \varepsilon_0} \right)^{\frac{1}{2}} \hat{a}_k \vec{\varepsilon}_k \quad (\text{B59})$$

$$\vec{A}_k^* = \left(\frac{\hbar V \omega_k}{2 \varepsilon_0} \right)^{\frac{1}{2}} \hat{a}_k^\dagger \vec{\varepsilon}_k. \quad (\text{B60})$$

Logo

$$\hat{A} = \sum_k \left(\frac{\hbar V \omega_k}{2 \varepsilon_0} \right)^{\frac{1}{2}} \vec{\varepsilon}_k \left[\hat{a}_k \exp(-i \omega_k t + i \vec{k} \cdot \vec{r}) + \hat{a}_k^\dagger \exp(i \omega_k t - i \vec{k} \cdot \vec{r}) \right]. \quad (\text{B61})$$

O vetor potencial é, agora, um operador. Substituindo a Eq. (B61), em (B41) e (B42), obtemos os operadores para os campos elétrico e magnético, para o modo k [Ref. B2]:

$$\hat{E}_k = i \left(\frac{\hbar V \omega_k}{2 \varepsilon_0} \right)^{\frac{1}{2}} \vec{\varepsilon}_k \left[\hat{a}_k \exp(-i \omega_k t + i \vec{k} \cdot \vec{r}) - \hat{a}_k^\dagger \exp(i \omega_k t - i \vec{k} \cdot \vec{r}) \right] \quad (\text{B62})$$

$$\hat{B}_k = i \left(\frac{\hbar V \omega_k}{2 \varepsilon_0} \right)^{\frac{1}{2}} \vec{k} \times \vec{\varepsilon}_k \left[\hat{a}_k \exp(-i \omega_k t + i \vec{k} \cdot \vec{r}) - \hat{a}_k^\dagger \exp(i \omega_k t - i \vec{k} \cdot \vec{r}) \right]. \quad (\text{B63})$$

Os campos totais são dados pela soma dos modos:

$$\hat{E}_T = \sum_k \hat{E}_k \quad (B64)$$

$$\hat{B} = \sum_k \hat{B}_k . \quad (B65)$$

A energia eletromagnética contida no modo k , para um estado de n_k fótons excitados, é dada por [Ref. B2]:

$$\bar{E}_k = \frac{1}{2} \int_v (\varepsilon_0 \bar{E}_k^2 + \mu^{-1} \bar{B}_k^2) dv = \frac{1}{2} \int_v \overline{\langle n_k | \varepsilon_0 \hat{E}_k \cdot \hat{E}_k + \mu^{-1} \hat{B}_k \cdot \hat{B}_k | n_k \rangle} dv . \quad (B66)$$

Substituindo as equações para os operadores dos campos elétrico e magnético, encontramos [Ref. B2]:

$$\bar{E}_k = \left(n_k + \frac{1}{2} \right) \hbar \omega_k . \quad (B67)$$

Portanto, o Hamiltoniano quântico, para o campo eletromagnético total na cavidade, vale [Ref. B2]:

$$\hat{H}_T = \sum_k \hbar \omega \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right) . \quad (B68)$$

APÊNDICE C

CRİPTOGRAFIA QUÂNTICA

C1. Introdução

Para a segurança das transmissões de dados, isto é, para tornar a mensagem distribuída em um canal de comunicação público não inteligível aos usuários para os quais a referida mensagem não foi endereçada ou autorizada, técnicas de criptografia devem ser empregadas. Neste caso, o transmissor, responsável pela encriptação, deve gerar uma palavra (conjunto de bits) secreta, conhecida como chave. Através de um algoritmo de encriptação, a chave é usada para embaralhar o texto a ser enviado, sendo a mensagem criptografada resultante conhecida como criptograma. Para a recuperação da mensagem original, no receptor, faz-se necessária a utilização da mesma chave, sendo a mensagem praticamente inviolável para quem não possui-la. Portanto, uma vez que a chave tenha sido escolhida no transmissor, ela deve ser transmitida ao receptor. Nesta etapa, se um terceiro usuário, não autorizado, tiver acesso ao canal de transmissão, ele poderá obter a chave e decodificar os dados que ele obtiver posteriormente. Um sistema de comunicação, fazendo uso de técnicas de criptografia, é dito exibir perfeita segurança se um criptanalista, interessado em decifrar o criptograma, não ganha informação extra sobre a mensagem a partir do criptograma obtido, isto é, $P(m|c) = P(m)$, a probabilidade de obter a mensagem m dado que o criptograma c foi obtido *a priori* deve ser igual à probabilidade de obter a mensagem m . Outro requerimento esperado é que $P(c|m) = P(c)$, a probabilidade de se obter um criptograma particular independe da mensagem enviada. Isto implica que a probabilidade total de todas as chaves que transformam a mensagem m no criptograma c é a mesma que a probabilidade de todas as chaves que transformam outra mensagem no mesmo criptograma. Por fim, diferentes mensagens, criptografadas pela mesma chave, devem produzir diferentes criptogramas. A perfeita segurança implica que o número de chaves possíveis deve ser tão grande quanto o número de mensagens existentes [Ref. C1].

O ponto crítico da criptografia tradicional é a transmissão da chave do transmissor ao receptor. Visando impossibilitar usuários não autorizados de obterem a chave durante a transmissão da mesma, foi desenvolvido um protocolo de distribuição de chave usando dados quânticos (estados quântico da luz). Dados quânticos estão sujeitos a princípios físicos fundamentais como o da incerteza de Heisenberg e o da correlação quântica. Quando estes dados são violados, pode-se medir uma alta taxa de erros de bits na recepção, indicando a presença de um intruso no canal de comunicação. O primeiro protocolo de criptografia quântica fez uso dos estados de polarização de fótons (polarimétrico), sendo conhecido como BB84 [Refs. C1, C4-C7]. Posteriormente, o mesmo protocolo, usando a fase dos fótons (interferométrico), foi proposto [Refs. C1, C8-C11]. Em 1992, foi proposto o segundo protocolo, conhecido como B92, também em versão interferométrica [Ref. C2]. Estes protocolos são baseados na complementaridade de entidades quânticas [Apêndice A]. Em 1991, foi proposto uma outra forma de implementar a criptografia quântica, através da correlação não local de estados quânticos [Apêndice A, Ref. C14]. Neste tipo de protocolo,

faz-se uso da correlação entre dois fótons preparados, por exemplo, através de conversão paramétrica descendente [Ref. C13]. Todos estes protocolos foram implementados sobre sistemas ópticos a fibra e muitos foram os experimentos, polarimétricos e interferométricos, já realizados com sucesso [Refs. C4-C11].

C2. Protocolos Baseados em Complementaridade

Os primeiros protocolos foram baseados na complementaridade ou princípio da incerteza de Heisenberg. Serão descritos os protocolos BB84, polarimétrico e interferométrico, que fazem uso de 4 estados quânticos, e o protocolo B92 interferométrico com dois estados quânticos não ortogonais.

C2.1 Protocolo BB84 Polarimétrico

O BB84 polarimétrico faz uso de 4 estados de polarização, por exemplo: circular à direita, $|C_D\rangle$, circular à esquerda, $|C_E\rangle$, linear vertical, $|L_V\rangle$, e linear horizontal, $|L_H\rangle$. Os dois primeiros estados formam a base B_1 , para um espaço de Hilbert de dimensão 2 e os dois últimos formam a base B_2 , para o mesmo espaço. Os estados de uma base podem ser relacionados aos estados da outra base através das seguintes relações [Ref. C1]:

$$|C_D\rangle = \frac{1}{\sqrt{2}}(|L_H\rangle + i|L_V\rangle) \quad (C1)$$

$$|C_E\rangle = \frac{1}{\sqrt{2}}(|L_H\rangle - i|L_V\rangle) \quad (C2)$$

$$|L_V\rangle = \frac{i}{\sqrt{2}}(|C_D\rangle - |C_E\rangle) \quad (C.3)$$

$$|L_H\rangle = \frac{1}{\sqrt{2}}(|C_D\rangle + |C_E\rangle) . \quad (C4)$$

Definimos, na Tabela C1, a representação dos bits pelos estados de polarização em cada base.

BASE	ESTADO	SÍMBOLO
B₁	$ C_D\rangle$	1
	$ C_E\rangle$	0
B₂	$ L_V\rangle$	1
	$ L_H\rangle$	0

Tabela C1 - Representação dos bits pelos estados de polarização.

Se Alice (transmissor) prepara e envia um fóton na base B_i e Bob (receptor) mede a polarização deste fóton usando a base B_j então, através das Eqs. (C1) - (C4), a probabilidade do resultado da medição de Bob ser o mesmo bit representado pelo estado

que Alice enviou é :

50% se $i \neq j$ (C5)

100% se $i = j$. (C6)

Por exemplo, suponhamos que Alice envie um bit 0 na base B_2 ($|L_H\rangle$) e que Bob escolha a base B_1 para medir a polarização; então, a probabilidade de Bob obter, como resultado da medida, o bit 1, é dada pelo quadrado do módulo do coeficiente que multiplica $|C_D\rangle$ na expansão de $|L_H\rangle$ na base B_1 . Da mesma forma, a probabilidade de Bob obter, como resultado, o bit 0, é dada pelo quadrado do módulo do coeficiente que multiplica $|C_E\rangle$ na expansão de $|L_H\rangle$ na base B_1 . Nesses dois casos, a probabilidade é de 50%. Em outras palavras, Bob tem 50% de chance de acertar o bit que Alice enviou. Quando Bob escolhe a mesma base que Alice, a probabilidade de Bob acertar o bit que Alice enviou é de 100% pois, obviamente, o coeficiente na expansão vale 1. Abaixo descrevemos a sequência de passos que compõem o protocolo BB84 [Refs. C1, C10]:

PROTÓCOLO BB84

1. Alice escolhe uma sequência aleatória de bits.
2. Alice escolhe aleatoriamente a base, B_1 ou B_2 , para cada bit da sequência, e envia um fóton por bit a Bob.
3. Bob escolhe aleatoriamente a base, B_1 ou B_2 , para medir a polarização do fóton e vai armazenando os valores dos bits que ele obteve como resultado das medições.
4. Durante uma discussão pública, sem preocupações com segurança, Alice e Bob informam, um ao outro, quais bases eles usaram. Os bits para os quais Alice e Bob escolheram a mesma base, e, portanto, Bob os leu com 100% de acerto, são guardados e formarão a chave; os demais bits são descartados.

A discussão aberta de quais bases foram escolhidas não revela nenhuma informação útil a um usuário não autorizado. Este, daqui por diante, será chamado de Eva. Devemos, agora, determinar a influência da presença de Eva no canal de comunicação. Suponhamos que Eva leia os bits enviados por Alice e envie os resultados de sua mensuração a Bob. Podemos, então, considerar três situações possíveis [Ref. C3]:

- 1 - Eva e Alice escolhem a mesma base e Bob escolhe uma base diferente, Fig. C1.

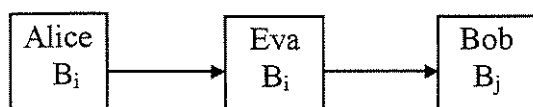


Fig. C1 - Alice = Eva $\neq$ Bob

UNICAMP
BIBLIOTECA CENTRAL
SEÇÃO CIRCULANTE

Nesta situação, Eva lê corretamente o bit enviado por Alice com 100% de certeza e o repassa a Bob. Como não há incerteza no resultado obtido por Eva, ela se torna transparente e não tem como ser detectada.

2 - Eva e Bob escolhem a mesma base e Alice escolhe uma base diferente, Fig. C2.

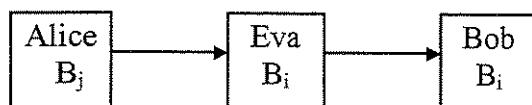


Fig. C2 - Alice $\neq$ Eva = Bob

Nesta situação, Eva lê o bit enviado por Alice com 50% de certeza e o repassa a Bob. Como Bob usa a mesma base que Eva, ele simplesmente obterá o mesmo resultado que esta. Portanto, Eva outra vez é transparente e não pode ser detectada.

3 - Bob e Alice escolhem a mesma base e Eva escolhe uma base diferente, Fig. C3.

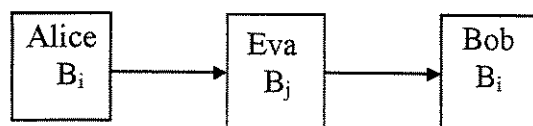


Fig. C3 - Alice = Bob $\neq$ Eva

Nesta situação, Eva lê o bit enviado por Alice com 50% de certeza e o repassa a Bob. Este, por sua vez, lê o bit enviado por Eva com 50% de certeza. Com isto, apesar de Alice e Bob usarem mesma base, o bit lido por Bob poderá ser diferente do enviado por Alice. Como este bit fará parte da chave, Alice e Bob conterão chaves diferentes. Caso usem um algoritmo de detecção de erro, como teste de paridade, o erro poderá ser detectado e, portanto, a presença de Eva também o será.

Do exposto acima, é fácil verificar que Eva tem uma probabilidade de 25% por bit de ser descoberta. Portanto, para uma chave de N bits, a probabilidade de não haver erros, na presença de Eva, é $0,75^N$. Alice e Bob podem escolher M , dos N bits da chave, compará-los publicamente, para ver se há erros, e depois descartá-los. Em todas as situações acima foram supostos detectores perfeitos e a ausência de ruídos. Na situação real não há como distinguir a presença de Eva e um erro causado por ruído. Se Alice e Bob acreditam que o erro na chave é devido ao ruído ou imperfeição de detectores, então pode-se usar um algoritmo de reconciliação para igualar as chaves de Bob e Alice, sendo os bits errados descartados.

C2.2 Protocolo BB84 Interferométrico

O protocolo BB84 pode ser implementado com um esquema de codificação de fase. Para isso, usa-se o interferômetro de Mach-Zehnder mostrado na Fig. C4 [Refs. C1. C8-C11].

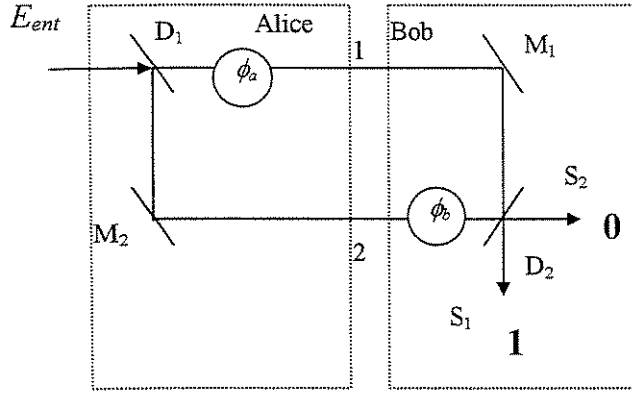


Fig. C4 - Interferômetro para criptografia quântica

Na Fig. C4, M_1 e M_2 são espelhos, D_1 e D_2 são divisores de feixe, aqui considerados iguais, com coeficientes de reflexão e transmissão dados por R e T , respectivamente. ϕ_a e ϕ_b são moduladores de fase controlados por Alice e Bob, respectivamente. S_1 e S_2 são as saídas do interferômetro. Da óptica clássica, temos as conhecidas relações para as intensidades luminosas nas saídas S_1 e S_2 :

$$I_1 = |E_{ent}|^2 \left[1 - 4|R|^2|T|^2 \cos^2\left(\frac{\phi_a - \phi_b}{2}\right) \right] \quad (C7)$$

$$I_2 = 4|E_{ent}|^2 |R|^2|T|^2 \cos^2\left(\frac{\phi_a - \phi_b}{2}\right). \quad (C8)$$

A diferença relativa de fase, $\Delta\phi = \phi_a - \phi_b$, controla a fração de intensidade luminosa nas saídas. Para um interferômetro balanceado temos $|R|^2 = |T|^2 = 0,5$. Existe um deslocamento de fase de 90° , entre a luz refletida e a transmitida no divisor de feixe, que é observado na reflexão em interfaces dielétricas. Iremos supor que ϕ_a e ϕ_b podem assumir apenas os valores 0° , 180° , 90° e 270° , onde os dois primeiros formam a base B_1 e os dois últimos formam a base B_2 . Aplicando estes valores nas Eqs. (C7) e (C8), temos os resultados da Tabela C2.

$\phi_a - \phi_b$	$I_1 E_{ent} ^{-2}$	$I_2 E_{ent} ^{-2}$
$\pm 90^\circ$	0,5	0,5
$\pm 270^\circ$	0,5	0,5
$\pm 0^\circ$	0	1
$\pm 180^\circ$	1	0

Tabela C2 - Fração da intensidade luminosa nas saídas S_1 e S_2 , para os possíveis valores de $\phi_a - \phi_b$.

Quando um fóton incide no interferômetro balanceado, este fóton emergirá do interferômetro pelas saídas, S_1 ou S_2 , com probabilidades dadas pelos valores da Tabela C2,

de acordo com o respectivo valor de diferença de fase $\Delta\phi$. Desta forma, quando Alice e Bob escolherem a mesma base, o fóton se comportará de maneira determinística, pois as probabilidades do fóton sair em S_1 ou S_2 serão 100% e 0%. Quando Alice e Bob usarem bases diferentes, o fóton se comportará de maneira aleatória e as probabilidades serão de 50%. Quando Bob detectar um pulso em S_1 , ele o interpretará como bit 1 e, quando detectar um pulso em S_2 , ele o interpretará como bit 0. Do ponto de vista da mecânica quântica, o interferômetro trabalha da seguinte maneira: A saída de Alice é dada por [Ref. C1]:

$$|\Psi(\phi_a)\rangle = \frac{1}{\sqrt{2}}[|1,0\rangle + i \exp(i\phi_a)|0,1\rangle] , \quad (C9)$$

onde $|n,m\rangle$ indica que há m fótons no ramo 1 do interferômetro e n fótons no ramo 2. O coeficiente $1/\sqrt{2}$ é devido ao fato dos divisores de feixe terem igual probabilidade de transmitir ou refletir o fóton ($|R|^2 = |T|^2 = 0,5$), o fator i é devido ao deslocamento de fase de 90° entre o fóton transmitido e o refletido e, por fim, o fóton que passar pelo ramo 1 deve sofrer um deslocamento de fase de ϕ_a . A Eq. (C9) é uma superposição de dois estados quânticos, pois não há como saber se o fóton passou pelo caminho 1 ou 2. O estado quântico na saída de Alice é a entrada de Bob. Após o modulador de Bob e antes de seu divisor de feixe, o estado quântico é [Ref. C1]:

$$|\Psi(\phi_a, \phi_b)\rangle = \frac{1}{\sqrt{2}}[|1,0\rangle \exp(i\phi_b) + i \exp(i\phi_a)|0,1\rangle] . \quad (C10)$$

Em (C10), o fóton que passou pelo ramo 2 sofreu um deslocamento de fase de ϕ_b . Na saída de Bob, isto é, após o divisor de feixe de Bob, temos [Ref. C1]:

$$\frac{1}{2}(\exp(i\phi_b) - \exp(i\phi_a))|1,0\rangle_b + \frac{i}{2}(\exp(i\phi_b) + \exp(i\phi_a))|0,1\rangle_b . \quad (C11)$$

onde $|n,m\rangle_b$ implica n fótons na saída S_1 e m na saída S_2 . Suponhamos que Alice faça $\phi_a = 90^\circ$ e Bob faça $\phi_b = 0^\circ$ (bases diferentes). Substituindo estes valores na Eq. (C11), temos:

$$\frac{1}{2}(1 - i)|1,0\rangle_b - \frac{1}{2}(1 - i)|0,1\rangle_b \quad (C12)$$

e, portanto, o fóton tem 50% de chance de aparecer em S_1 e 50% de aparecer em S_2 . Suponhamos, agora, que Alice faça $\phi_a = 90^\circ$ e Bob faça $\phi_b = 270^\circ$ (bases iguais). Substituindo estes valores na Eq. (C11), temos:

$$-i|1,0\rangle_b + 0|0,1\rangle_b \quad (C13)$$

e, portanto, o fóton tem 100% de chance de aparecer em S_2 e 0% de chance de aparecer em S_1 . A implementação do protocolo BB84 interferométrico é análoga à do polarimétrico. Definimos a codificação dos bits 1 e 0, segundo as fases, nas Tabelas C3 e C4.

ALICE	
FASE	BIT
0°	0
180°	1
90°	0
270°	1

Tabela C3 - Codificação de bits para Alice.

BOB	
FASE	BIT
0°	0 (s_2)
	1 (s_1)
90°	0 (s_2)
	1 (s_1)

Tabela C4 - Codificação de bits para Bob.

Para implementar o BB84 com fase é só aplicar os passos 1 a 4, descritos na Seção C2.1, com o item 3 levemente modificado, como mostrado abaixo:

3 - Bob escolhe aleatoriamente a base, B_1 ou B_2 , para modular a fase do fóton que recebeu de Alice e vai armazenando os valores dos bits que ele obteve, de acordo com a saída em que o pulso emergiu, se em S_1 ou em S_2 .

O interferômetro da Fig. C4 pode ser implementado com fibras ópticas [Refs. C1, C8-C11]. O diagrama é mostrado na Fig. C5.

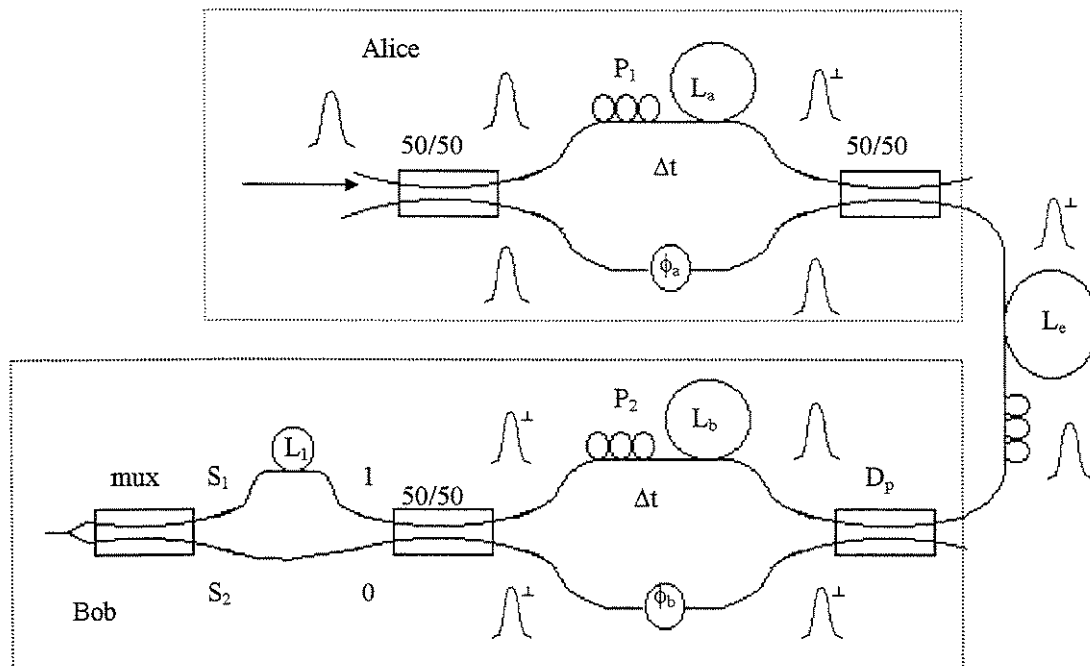


Fig. C5 - Interferômetro a fibra para criptografia quântica

A operação do interferômetro a fibra da Fig. C5 é completamente análogo ao da Fig. C4 e pode ser explicado da seguinte maneira [Refs. C1, C10]: Um pulso luminoso de baixíssima intensidade incide no interferômetro, em Alice, e é dividido em dois, de intensidades iguais. Um passará pelo modulador ϕ_a e o outro pelo conjunto polarizador P_1 e

laço de fibra L_a . O primeiro rotacionará a polarização de 90° e o segundo ocasionará um atraso adicional no pulso, de Δt , devido ao comprimento da fibra neste ramo. Os dois pulsos são, então, enviados a Bob através do enlace de fibra, sendo que o pulso de polarização rotacionada por Alice chegará em um instante de tempo Δt posterior à chegada do pulso modulado. Na entrada de Bob, temos um divisor de feixe controlado por polarização que enviará o pulso modulado em Alice para o polarizador P_2 . Este pulso terá sua polarização rotacionada de 90° e sofrerá um atraso de Δt ao se propagar por L_b . O pulso que passou por P_1 , em Alice, agora passará pelo modulador ϕ_b de Bob. Ambos os pulsos chegarão na saída de Bob ao mesmo tempo, com mesma polarização e sofrerão interferência. Dependendo dos valores de ϕ_a e ϕ_b o pulso emergirá de Bob por S_1 ou S_2 ou ainda, em raras vezes, por ambas (quando o pulso luminoso for um estado coerente atenuado). Como a saída S_1 , representando o bit 1, possui um comprimento maior que a saída S_2 , que representa o bit 0, existirá uma separação temporal entre os bits 1 e 0, permitindo, assim, a utilização de apenas um fotodetector. Para isso Bob deve manter uma base de tempo sincronizada com Alice.

C2.3 Protocolo B92 Interferométrico

O protocolo BB84 usa 4 estados, dois para cada base conjugada. Em 1992 mostrou-se que a distribuição quântica da chave pode ser realizada com apenas 2 estados não ortogonais e o protocolo B92 foi proposto [Ref. C2]. Para começar a descrição deste protocolo, definamos dois estados distintos não ortogonais, $|a_0\rangle$ e $|b_0\rangle$, autoestados dos operadores $\hat{A}$ e $\hat{B}$, respectivamente, e as seguintes relações de autoestados:

$$\hat{A}|a_i\rangle = \eta_i|a_i\rangle \quad (C14)$$

$$\hat{B}|b_i\rangle = \lambda_i|b_i\rangle, \quad (C15)$$

onde os autoestados são ortonormalizados, isto é :

$$\langle a_i | a_j \rangle = \delta_{ij} \quad (C16)$$

$$\langle b_i | b_j \rangle = \delta_{ij}. \quad (C17)$$

Definamos, também, dois operadores que não comutam, $\hat{P}=1-|a_0\rangle\langle a_0|$ e $\hat{Q}=1-|b_0\rangle\langle b_0|$, conhecidos como operadores projeção. Então, usando (C16) e (C17), é fácil verificar que:

$$\hat{P}|a_j\rangle = |a_j\rangle - |a_0\rangle\langle a_0|a_j\rangle = \begin{cases} 0 & \text{se } j = 0 \\ |a_j\rangle & \text{se } j \neq 0 \end{cases} \quad (C18)$$

$$\hat{Q}|b_j\rangle = |b_j\rangle - |b_0\rangle\langle b_0|b_j\rangle = \begin{cases} 0 & \text{se } j = 0 \\ |b_j\rangle & \text{se } j \neq 0 \end{cases}. \quad (C19)$$

No protocolo B92 os estados $|a_0\rangle$ e $|b_0\rangle$ representam os bits 1 e 0, respectivamente. Bob utiliza os operadores $\hat{P}$ e $\hat{Q}$ para realizar uma medição no fóton emitido por Alice. Verifiquemos, então, os casos possíveis:

1 - Alice envia um fóton no estado $|a_0\rangle$

1.1 - Bob usa o operador $\hat{P}$ para realizar uma medição.

Nesta situação, de (2.18) vemos que Bob obterá o valor 0 como resultado.

1.2 - Bob usa o operador $\hat{Q}$ para realizar uma medição.

Inicialmente, expandimos o estado $|a_0\rangle$ na base de autoestados $|b_k\rangle$, obtendo assim a Eq. (C20).

$$|a_0\rangle = \sum_{k=0} |b_k\rangle \langle b_k | a_0 \rangle . \quad (C20)$$

Agora, aplicando o operador $\hat{Q}$ à Eq. (C20), obtemos:

$$\hat{Q}|a_0\rangle = \hat{Q} \sum_{k=0} |b_k\rangle \langle b_k | a_0 \rangle = \sum_{k=0} \langle b_k | a_0 \rangle \hat{Q}|b_k\rangle . \quad (C21)$$

A Eq. (C21) dá um resultado nulo, com probabilidade $|\langle b_0 | a_0 \rangle|^2$, que é a probabilidade de $|a_0\rangle$ colapsar para o estado $|b_0\rangle$ durante a medição. Portanto, a Eq. (C21) dá um resultado positivo, com probabilidade igual a $1 - |\langle b_0 | a_0 \rangle|^2$.

2 - Alice envia um fóton no estado $|b_0\rangle$

2.1 - Bob usa o operador $\hat{Q}$ para realizar uma medição:

Nesta situação, de (C19) vemos que Bob obterá o valor 0 como resultado.

2.2 - Bob usa o operador $\hat{P}$ para realizar uma medição:

Inicialmente expandimos o estado $|b_0\rangle$ usando a base de autoestados $|a_k\rangle$, obtendo assim a Eq. (C22).

$$|b_0\rangle = \sum_{k=0} |a_k\rangle \langle a_k | b_0 \rangle . \quad (C22)$$

Agora, aplicando o operador $\hat{P}$ à Eq. (C22), obtemos:

$$\hat{P}|b_0\rangle = \hat{P} \sum_{k=0} |a_k\rangle \langle a_k|b_0\rangle = \sum_{k=0} \langle a_k|b_0\rangle \hat{P}|a_k\rangle, \quad (C23)$$

que dá um resultado nulo com probabilidade $|\langle b_0|a_0\rangle|^2$, que é a probabilidade do estado $|b_0\rangle$ colapsar para o estado $|a_0\rangle$ durante a medição. Portanto, a Eq. (C23) dá um resultado positivo com probabilidade igual a $1-|\langle b_0|a_0\rangle|^2$. A Tabela C5 resume as possíveis ações de Alice e Bob, e os resultados obtidos por Bob, com suas respectivas probabilidades.

Alice	Bob		
	Operador	Resultado	Probabilidade
0 $ a_0\rangle$	$\hat{P}$	0	1
	$\hat{Q}$	> 0	$1- \langle b_0 a_0\rangle ^2$
1 $ b_0\rangle$	$\hat{P}$	> 0	$1- \langle b_0 a_0\rangle ^2$
	$\hat{Q}$	0	1

Tabela C5 – Ações possíveis de Alice e Bob e os resultados obtidos por Bob, com suas respectivas probabilidades.

A implementação do protocolo B92, a partir da Tabela C5, é direta. Os passos são descritos a seguir.

PROTÓCOLO B92

1. Alice escolhe uma sequência aleatória de bits e envia fótons, nos estados quânticos correspondentes a estes bits, para Bob, um por vez, segundo uma sincronização temporal.
2. Bob escolhe aleatoriamente e independentemente de Alice, para cada fóton que nele chegue, o operador com o qual fará a medida, se $\hat{P}$ ou $\hat{Q}$.
3. Os bits nas fatias (*slots*) de tempo em que o resultado da medição de Bob foram nulos são descartados.
4. Ao final, Bob informa à Alice quais fatias temporais ele mediu um resultado positivo. Os bits nestas fatias de tempo formarão a chave.

O teste de presença de Eva pode ser realizado comparando-se publicamente alguns bits da chave que, depois do teste, serão descartados. Se Eva não está presente então, para transmissão equiprovável de uns e zeros, aproximadamente $0,5(1-|\langle b_0|a_0\rangle|^2)$ dos eventos resultará em uma medição positiva, correspondendo aos casos onde Alice enviou $|a_0\rangle$ e Bob mediu com $\hat{Q}$, ou aos casos onde Alice enviou $|b_0\rangle$ e Bob mediu com $\hat{P}$. A presença de Eva pode fazer com que a medição de Bob dê um resultado positivo nos outros casos. A Tabela C6 mostra estes casos.

Alice	Eva				Bob		
	o	r	p	e	o	r	p
$ b_0\rangle$	$\hat{P}$	0	$ \langle b_0 a_0\rangle ^2$	$ a_0\rangle$	$\hat{Q}$	>0	$1- \langle b_0 a_0\rangle ^2$
$ a_0\rangle$	$\hat{Q}$	0	$ \langle b_0 a_0\rangle ^2$	$ b_0\rangle$	$\hat{P}$	>0	$1- \langle b_0 a_0\rangle ^2$
o – operador r – resultado p – probabilidade e – estado retransmitido							

Tabela C6 – Casos em que a presença de Eva causa um erro na medição de Bob.

A ação de Eva é realizar uma medição no fóton enviado por Alice, usando $\hat{P}$ ou $\hat{Q}$, e retransmitir um fóton, segundo o estado que foi medido, para Bob. Se Eva escolhe $\hat{P}$ e obtém um resultado nulo, então ela envia o estado $|a_0\rangle$ para Bob. Se Eva escolhe $\hat{Q}$ e obtém um resultado nulo, então ela envia o estado $|b_0\rangle$ para Bob. Da Tabela C6 é fácil verificar que a probabilidade de erro por bit, devido à presença de Eva, é $0,25|\langle b_0|a_0\rangle|^2(1-|\langle b_0|a_0\rangle|^2)$. A realização prática deste protocolo pode ser feita através do interferômetro da Fig. C6 [Ref. C2].

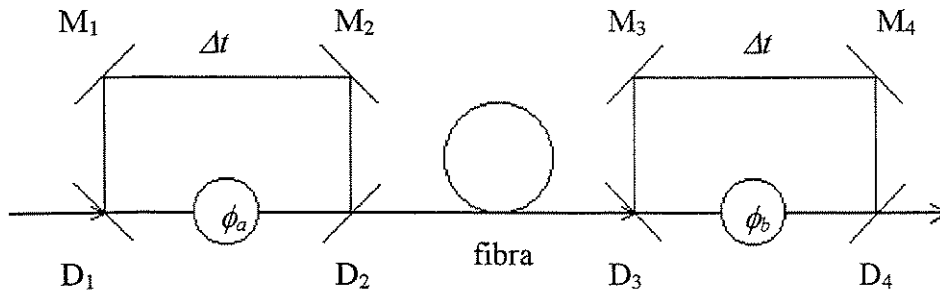


Fig. C6 Interferômetro para implementação do protocolo B92.

M_1 , M_2 , M_3 e M_4 são espelhos, D_1 , D_2 , D_3 e D_4 são divisores de feixes, aqui considerados iguais, com coeficientes de reflexão e transmissão dados por R e T respectivamente. ϕ_a e ϕ_b são moduladores de fase controlados por Alice e Bob respectivamente.

C3 Protocolos Baseados em EPR

C3.1 Introdução

Os protocolos baseados no paradoxo Einstein-Podolsky-Rosen, EPR, fazem uso da correlação quântica entre fótons preparados em estados quânticos entrelaçados [Refs. C12, C13]. Esta correlação é não local, implicando que, uma medida de um determinado observável no fóton, que chega a Alice, determina completamente o observável complementar do fóton que chega a Bob. O primeiro protocolo baseado em EPR foi proposto por Ekert em 1991 [Ref. C14]. A Fig. C7 mostra um diagrama esquemático de blocos para criptografia quântica. O gerador de par de fótons correlacionados, GPFC, é um

experimento de conversão paramétrica descendente [Ref. C12]. Um fóton é enviado para Bob e o outro para Alice, sendo que estes contêm medidores de polarização ou interferômetros, segundo a codificação usada, polarização ou fase, respectivamente.

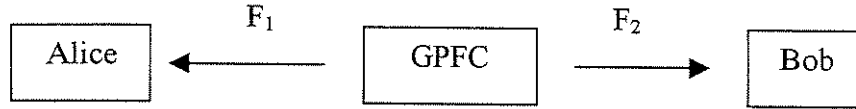


Fig. C7 – Diagrama de blocos para implementação dos protocolos tipo EPR

C3.2 Protocolo EPR Polarimétrico

De acordo com a Fig. C7, um par de fótons com polarizações lineares correlacionadas é gerado, sendo um enviado a Bob e o outro a Alice. O estado correlacionado é descrito por [Refs. C1, C13, C14]:

$$|\psi_{12}\rangle = \frac{1}{\sqrt{2}} \left(|0^\circ\rangle_1 \otimes |90^\circ\rangle_2 - |90^\circ\rangle_1 \otimes |0^\circ\rangle_2 \right). \quad (\text{C.24})$$

Ou seja, o sistema está numa superposição de dois estados possíveis: O fóton 1 (enviado à Alice) com polarização 0° e o fóton 2 (enviado ao Bob) com polarização 90° ou o fóton 1 com polarização 90° e o fóton 2 com polarização 0° . Esta situação ambígua só é resolvida quando uma medição de polarização é realizada em algum dos fótons. Se, após a medida em um dos fótons, o mesmo é encontrado com polarização 90° o outro estará com polarização 0° e vice-versa. Para realizar a medição da polarização Alice e Bob dispõem de três operadores, como mostrado na Tabela C7 [Ref. C1]:

OPERADOR	BASE DE AUTOESTADOS	90°	0°
P(0°)	$\{ 0^\circ\rangle, 90^\circ\rangle\}$	0/1	1/0
P(30°)	$\{ 30^\circ\rangle, 120^\circ\rangle\}$	0,5/0,5	0,5/0,5
P(60°)	$\{ 60^\circ\rangle, 150^\circ\rangle\}$	0,5/0,5	0,5/0,5

Tabela C7 - Operadores e autobases para codificação de polarização.

Por convenção, os primeiros estados, na segunda coluna da Tabela C7, representam o bit 0, enquanto que o demais representam o bit 1. As terceira e quarta colunas da referida tabela mostram as probabilidades de se obter, como resultado da medição em fótons de 90° ou 0° , com cada operador da primeira coluna, os bits 1 e 0. Como os fótons enviados para Alice e Bob são correlacionados, ocorre que, quando eles escolherem a mesma base, se um obtiver o bit 1(0) como resultado da medida o outro obterá o bit 0(1). Quando Alice e Bob escolhem bases diferentes nada pode-se afirmar pois se, por exemplo, Alice faz a medida primeiro usando P(30°) e obtém como resultado o bit 1 ($|120^\circ\rangle$), o fóton que foi para Bob estará no estado $|30^\circ\rangle$ e se Bob escolher outro operador para a medição, que não o mesmo de Alice, ele obterá como resultado o bit 1 ou 0 probabilisticamente, de acordo com os

coeficientes da expansão do estado $|30^\circ\rangle$ na base do referido operador usado por Bob. Com o acima exposto, descrevemos, a seguir, o protocolo de criptografia usando estados de polarização correlacionados [Refs. C1]:

PROTOCOLO EPR - Polarimétrico

1. A fonte gera pares de fótons correlacionados em fatias temporais sincronizadas (*slots*) e, para cada par, envia um fóton para Alice e o outro para Bob.
2. Alice e Bob escolhem aleatoriamente e independentemente, para cada *slot* de tempo, uma base de medida de polarização, entre as três da Tabela C7.
3. Após a transmissão, em uma discussão pública, Bob e Alice informam um ao outro quais bases usaram, sem no entanto revelarem o resultado das medidas.
4. Os bits pertencentes ao *slots* nos quais Alice e Bob escolheram a mesma base formarão a chave.

Alice e Bob obterão chaves complementares (bits invertidos); por isso, é necessário que um dos dois inverta todos os bits de sua chave. A presença de Eva é verificada comparando-se publicamente alguns bits da chave escolhidos aleatoriamente.

C3.3 Protocolo EPR com Codificação de Fase

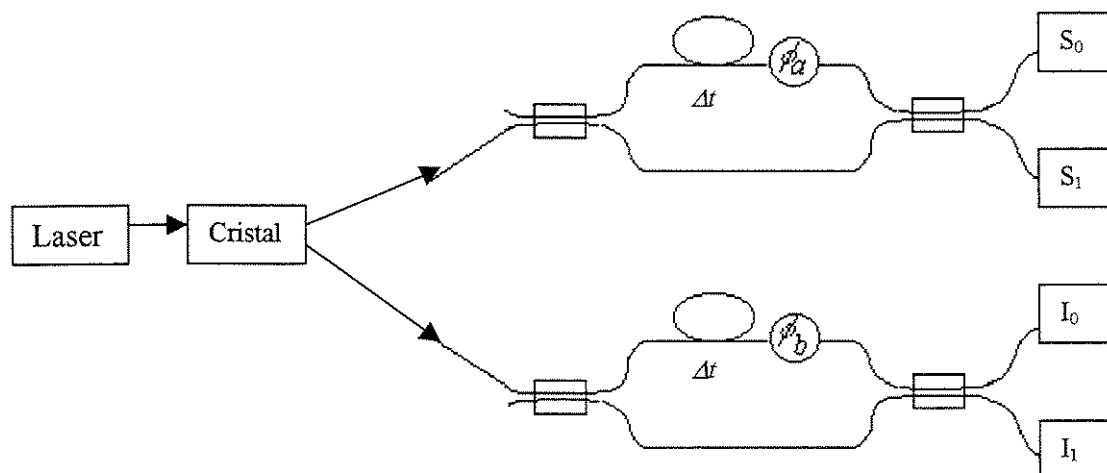


Fig. C8 - Criptografia quântica interferométrica com EPR.

A configuração para criptografia quântica interferométrica usando EPR é mostrada na Fig. C8. Nela, um laser ilumina um cristal que, através da conversão paramétrica descendente [Ref. C13], divide cada fóton incidente, de frequência $2\omega_0$, num par de fótons chamados de *signal*, ω_s , e *idler*, ω_i , conservando a energia e o momento total. Os fótons de cada par são enviados através da fibra óptica, um a Alice e o outro a Bob. Alice e Bob

possuem interferômetros idênticos, sendo um dos braços mais longo, o que proporciona um atraso Δt , seguido de um modulador de fase. Alice recebe seus fótons nos detectores S_0 e S_1 , enquanto que Bob recebe os seus nos detectores I_0 e I_1 [Refs. C14-C17]. O estado quântico entrelaçado, na saída do cristal, é [Refs. C14-C17]:

$$|\psi\rangle = \int \xi(\omega) |1; \omega\rangle \otimes |1; 2\omega_0 - \omega\rangle d\omega \quad , \quad (C25)$$

onde ω é a frequência do fóton *signal*, ω_s , enquanto $\omega_i = 2\omega_0 - \omega$ é a frequência do fóton *idler*. A função $\xi(\omega)$ dá a quantidade de correlação entre os modos e $|\xi(\omega)|^2$ deve ser positiva, num intervalo $\Delta\omega$ centrado em ω_0 [Ref. C17]. Se a condição $(\Delta\omega)^{-1} \ll \Delta t$ for satisfeita, então as probabilidades conjuntas de receber um fóton no detector i , em Alice, e um fóton no detector j , em Bob, $P(i,j)$, são dadas por [Refs. C14, C17]:

$$P(1,1) = P(0,0) = \frac{1}{4} [1 + \cos(\phi_a + \phi_b + \theta)] \quad (C26)$$

$$P(1,0) = P(0,1) = \frac{1}{4} [1 - \cos(\phi_a + \phi_b + \theta)] \quad (C27)$$

$$\theta = (\omega_s + \omega_i)\Delta t = 2\omega_0\Delta t \quad . \quad (C28)$$

Se os detectores são perfeitos, então, para $\theta = 2\pi k$, $k = 1, 2, 3, \dots$, o coeficiente de correlação é dado por [Ref. C14, C17]:

$$J(\phi_s, \phi_i) = P(1,1) + P(0,0) - P(0,1) - P(1,0) = \cos(\phi_a + \phi_b) \quad . \quad (C29)$$

Portanto, o coeficiente de correlação depende de dois parâmetros locais; logo, a correlação entre os fotocontadores é não-local. Com as Eqs. (C26) - (C29), temos que:

$$\phi_a + \phi_b = 0 \Rightarrow \begin{cases} P(0,0) = P(1,1) = 0,5 \\ P(0,1) = P(1,0) = 0 \end{cases} \quad (C30)$$

$$\phi_a + \phi_b = \pm \frac{\pi}{2} \Rightarrow P(0,0) = P(1,1) = P(0,1) = P(1,0) = 0,25 \quad . \quad (C31)$$

A Eq. (C.30) nos diz que, quando o coeficiente de correlação é unitário, a probabilidade de coincidência, isto é, dos fótons serem recebidos nas saídas S_0 e I_0 ou nas saídas S_1 e I_1 , é unitária. Este fato é o cerne do protocolo de criptografia. A seguir, descrevemos o protocolo de criptografia proposto nas Referências C14 e C17.

PROTOCOLO EPR - Interferométrico

1. A fonte gera pares de fótons correlacionados em fatias temporais sincronizadas (*slots*) e envia um para Alice e o outro para Bob.
2. Alice e Bob escolhem para ϕ_a e ϕ_b , aleatoriamente e independentemente, para cada *slot* de tempo, dentre os valores 0 e $\pi/2$, para Alice, e dentre 0 e $-\pi/2$, para Bob.
3. Após a transmissão, em uma discussão pública, Bob e Alice informam, um ao outro, quais valores usaram, sem no entanto revelarem aonde os fótons foram detectados.
4. Os bits pertencentes ao *slots* nos quais Alice e Bob escolheram valores de fase tal que $\phi_a + \phi_b = 0$, formarão a chave. Os demais são descartados.

A presença de Eva é verificada comparando-se publicamente alguns bits da chave escolhidos aleatoriamente.

APÊNDICE D

PROBABILIDADE E TEORIA CLÁSSICA DA INFORMAÇÃO

D1. Probabilidades

A probabilidade do resultado de um dado experimento assumir um determinado valor ou conjunto de valores, pertencente ao espaço amostral, é a razão entre o número de casos favoráveis e o número de casos possíveis, onde o espaço amostral considerado é discreto e finito. Seja o resultado deste experimento representado pela variável aleatória discreta, x , e o espaço amostral $X = \{x_1, x_2, \dots, x_i, \dots, x_n\}$. Então, para cada x_i é associada uma probabilidade p_i de $x = x_i$ ocorrer. A função f tal que, $f(x_i) = p_i$, é chamada função densidade de probabilidade, FDP, discreta. A média ou valor esperado de x , a média da função $g(x)$ e a variância de x , são dadas, respectivamente, por [Ref. D1]:

$$\langle x \rangle = \sum_{i=1}^n x_i p_i \quad (D1)$$

$$\langle g(x) \rangle = \sum_{i=1}^n g(x_i) p_i \quad (D2)$$

$$\sigma^2 = \langle x^2 \rangle - \langle x \rangle^2 \quad (D3)$$

Obviamente, o primeiro termo do segundo membro da Eq. (D3) é obtido fazendo-se $g(x) = x^2$ na Eq. (D2). Se o resultado do experimento, representado pela variável aleatória x , pertence, agora, ao intervalo contínuo de valores (a, b) , então existe uma FDP, $P(x)$, tal que a probabilidade do resultado pertencer ao intervalo (c, d) , onde $c > a$ e $d < b$, é dada por [Ref. D1]:

$$P(c \leq x \leq d) = \int_c^d P(x) dx \quad (D4)$$

O valor esperado de x e a média da função $g(x)$, para x contínuo, são dados, respectivamente, por [Ref. D1]:

$$\langle x \rangle = \int_a^b x P(x) dx \quad (D5)$$

$$\langle g(x) \rangle = \int_a^b g(x) P(x) dx \quad (D6)$$

A variância continua sendo dada pela Eq. (D3).

Sejam dois experimentos com variáveis aleatórias de saída, A e B , com seus respectivos espaços amostrais. Então, além das probabilidades incondicionais $P(A)$ e $P(B)$, podemos definir as seguintes probabilidades [Ref. D1]:

1. Probabilidade Conjunta: $P(A \text{ } B)$ é a probabilidade de A e B acontecerem.
2. Probabilidade Condicional: $P(A|B)$ é a probabilidade de A ocorrer, dado que B ocorreu.

Estas probabilidades são relacionadas por [Ref. D1]:

$$P(AB) = P(B | A)P(A) \quad (D7)$$

$$P(B) = \sum_A P(B | A)P(A) . \quad (D8)$$

As probabilidades contrárias são obtidas trocando, em (D7) e (D8), B por A e vice-versa. Por fim, temos o teorema de Bayes, que fornece as probabilidades *a posteriori* a partir das probabilidades *a priori* [Ref. D1]:

$$P(A_i | B) = \frac{P(A_i)P(B | A_i)}{\sum_i P(A_i)P(B | A_i)} = \frac{P(A_i)P(B | A_i)}{P(B)} . \quad (D9)$$

D2. Teoria da Informação

A teoria da informação, criada por Shannon, se presta a estudar três problemas básicos [Ref. D2]:

1. Medida da informação disponível na fonte.
2. Capacidade do canal.
3. Utilização de codificação para se explorar toda a capacidade do canal, durante a transferência da informação.

Se a taxa de informação de uma fonte não excede à capacidade do canal de comunicação, então, existe uma técnica de codificação tal que, a informação pode ser transmitida pelo canal, com uma frequência de erros arbitrariamente pequena, apesar da presença do ruído. Podemos, ainda, afirmar que a função dos códigos é casar a fonte e o canal para que haja uma máxima transferência de informação. Quando esta máxima transferência ocorre, o código é dito ser ótimo. Quando isto não ocorre, mas chega próximo, o código é dito ser sub-ótimo [Ref. D2].

D2.1. Medida de Informação, Entropia e Taxa de Informação

Seja um transmissor fazendo uso do alfabeto X , o qual possui n símbolos, $\{x_i\}_n$. A informação quantifica a liberdade de escolha exercida pelo transmissor, ao selecionar um símbolo x_i . Se a probabilidade do símbolo x_i ser escolhido é p_i , então a informação própria de x_i , ou quantidade de informação associada com x_i , é definida como sendo [Ref. D2]:

$$I_i = -\log_b(p_i) . \quad (D10)$$

A base do logaritmo, b , determina a unidade de informação. Se $b = 2$, a unidade de informação é o bit. Desta forma, se $p(x_1) = p(x_2) = 0,5$, então, de (D10) temos que $I_1 = I_2 = 1$ bit. Em outras palavras, 1 bit é a quantidade de informação necessária para escolher entre duas alternativas equiprováveis. De (D10) também vemos que, $I_i \rightarrow 0$ quando $p_i \rightarrow 1$, isto é, quando não há incerteza na mensagem a ser escolhida não há informação transferida. Por outro lado, se $I_i > I_j$ então $p_i < p_j$, ou seja, quanto maior a incerteza, maior a informação. Por fim, se a fonte produz duas mensagens sucessivas e independentes, x_i e x_j , com probabilidade conjunta $p(x_i x_j) = p_i p_j$, então [Ref. D2]:

$$I_{ij} = -\log_b(p_i p_j) = -\log_b(p_i) - \log_b(p_j) = I_i + I_j . \quad (D11)$$

Seja, agora, uma fonte de informação com as probabilidades p_i , de escolha dos x_i , independentes do tempo, com símbolos sucessivos estatisticamente independentes e transmitidos em uma taxa média de t símbolos por segundo. A quantidade de informação produzida por esta fonte, durante um intervalo de símbolo, é uma variável aleatória discreta com os possíveis valores $I_1, I_2, \dots, I_n$, onde cada I_i está associada à probabilidade p_i . O valor esperado da informação por símbolo é chamada entropia e é dada por [Ref. D2]:

$$H(X) = \sum_{i=1}^n p_i I_i = \sum_{i=1}^n -p_i \log_b(p_i) . \quad (D12)$$

A unidade da entropia, para $b = 2$, é bits/símbolo. Se m símbolos são transmitidos, então a informação total média a ser transmitida é $mH(X)$ bits. Como a fonte produz t símbolos/s, então m símbolos durarão (m/t) segundos. Portanto, a taxa de informação por segundo é [Ref. D2]:

$$R = \frac{mH(X)}{m/t} = tH(X) , \quad (D13)$$

onde R é dado em bits/s ($b = 2$). Quando os símbolos são equiprováveis, $p_i = 1/N$, sendo N o tamanho do alfabeto utilizado, a entropia alcança seu valor máximo dado por $H(X) = \log_b(N)$ e, portanto, a taxa de informação por segundo também será máxima, dada por $R = t \log_b(N)$. Porém, quando os símbolos não são equiprováveis, $R < t \log_b(N)$, a transmissão necessita de um processo de codificação que leve em conta a quantidade de informação por símbolo. O codificador, que não gera informação adicional nem destrói informação já existente, converte os símbolos provenientes da fonte em palavras código, produzidas em uma taxa t_c . Desta forma, temos que [Ref. D2]:

$$R = tH(X) = t_c H_c(X_c) \leq t_c \log_b(N) . \quad (D14)$$

H_c é a entropia considerando o conjunto transmissor + codificador como uma nova fonte, e X_c é o alfabeto usado por esta fonte. Para códigos binários, $N = 2$, e $b = 2$ temos [Ref. D2]:

$$\langle L \rangle = \frac{t_c}{t} \geq H(X) , \quad (D15)$$

onde $\langle L \rangle$ é o comprimento médio do código e representa o número médio de dígitos binários por símbolo da fonte. $\langle L \rangle$ também é dado por [Ref. D2]:

$$\langle L \rangle = \sum_{i=1}^N p_i L_i , \quad (D16)$$

onde L_i é o comprimento da palavra código do i -ésimo símbolo, o qual ocorre com probabilidade p_i . A razão $H(X)/\langle L \rangle \leq 1$, mede a eficiência de códigos sub-ótimos. Quando a igualdade ocorrer, o código será ótimo. Por fim, o código é unicamente decifrável se a desigualdade de Kraft for satisfeita [Ref. D2]:

$$K = \sum_{i=1}^N 2^{-L_i} \leq 1 . \quad (D17)$$

Consideremos, agora, a transmissão de informação sobre um canal ruidoso. O transmissor faz uso do alfabeto X , enquanto que, no receptor, os símbolos recebidos pertencem ao alfabeto Y . Desta forma podemos definir as seguintes probabilidades [Ref. D2]:

$P(x_i)$ – Probabilidade da fonte escolher o símbolo x_i para a transmissão.

$P(y_j)$ – Probabilidade do símbolo y_j ser recebido.

$P(x_i y_j)$ – Probabilidade (conjunta) de x_i ser transmitido e y_j ser recebido.

$P(x_i | y_j)$ – Probabilidade (condicional) de x_i ter sido transmitido, dado que y_j foi recebido.

$P(y_j | x_i)$ – Probabilidade (condicional) de y_j ser recebido, dado que x_i foi transmitido.

Assumimos que o canal é sem memória e invariante no tempo, tal que, as probabilidades condicionais são independentes do tempo e dos símbolos transmitidos previamente. A quantidade de informação transferida quando x_i é transmitido e y_j recebido é chamada informação mútua, sendo dada por [Ref. D2]:

$$I(x_i; y_j) = \log_2 \left[\frac{P(x_i | y_j)}{P(x_i)} \right] . \quad (D18)$$

Se há muito ruído no canal, x_i se torna independente de y_j , isto é, $P(x_i | y_j) = P(x_i)$, portanto, de (D18), $I(x_i; y_j) = 0$. Se não há ruído no canal então $P(x_i | y_j) = 1$ e a informação mútua é igual a auto-informação. Tal como a auto-informação média, podemos definir a informação mútua média, dada por:

$$I(X; Y) = \sum_{x,y} P(x_i y_j) I(x_i; y_j) = \sum_x \sum_y P(x_i y_j) \log_2 \left[\frac{P(x_i | y_j)}{P(x_i)} \right] . \quad (D19)$$

A informação mútua é dada em bits/símbolo. Como visto na Eq. (D19), a média é tomada sobre ambos os alfabetos. A quantidade $I(X;Y)$ representa a quantidade média de informação ganha por símbolo recebido. Usando (D7) e (D8) em (D19), obtemos:

$$I(X;Y) = \sum_x \left(\sum_y P(x_i, y_j) \right) \log_2 \left[\frac{1}{P(x_i)} \right] - \sum_x \sum_y P(x_i, y_j) \log_2 \left[\frac{1}{P(x_i | y_j)} \right] \quad (D20)$$

$$I(X;Y) = \sum_x P(x_i) \log_2 \left[\frac{1}{P(x_i)} \right] - \sum_x \sum_y P(x_i, y_j) \log_2 \left[\frac{1}{P(x_i | y_j)} \right] = H(X) - H(X | Y) . \quad (D21)$$

$H(X|Y)$ representa a informação perdida no canal ruidoso. Entretanto:

$$\frac{P(x_i | y_j)}{P(x_i)} = \frac{P(y_j | x_i)}{P(y_j)} \Rightarrow I(X;Y) = I(Y;X) . \quad (D22)$$

Portanto, a informação mútua também pode ser representada por [Ref. D2]:

$$I(X;Y) = H(Y) - H(Y | X) , \quad (D23)$$

onde

$$H(Y) = \sum_y -P(y_j) \log_2 [P(y_j)] \quad (D24)$$

$$H(Y | X) = \sum_y \sum_x -P(x_i, y_j) \log_2 [P(y_j | x_i)] . \quad (D25)$$

A máxima quantidade de informação, transferida por símbolo através do canal, é chamada de capacidade do canal. Matematicamente, é dada por [Ref. D2]:

$$C_c = \max\{I(X;Y)\} \text{ [bits/símbolo]} \quad (D26)$$

Se a máxima taxa de símbolos permitida pelo canal é r , então a máxima taxa de transferência de informação é dada por [Ref. 2]:

$$C = rC_c \text{ [bits/s]} . \quad (D27)$$

Finalmente, o teorema fundamental de Shannon, para um canal com ruído [Ref D2], é: Se um canal tem capacidade C_c e uma fonte tem taxa de informação $R \leq C$, então existe um sistema de codificação tal que a saída da fonte pode ser transmitida pelo canal com uma frequência de erros arbitrariamente pequena. Por outro lado, se $R > C$, então não é possível transmitir a informação sem erros.

APÊNDICE E

POLARIZAÇÃO DA LUZ

E1. Introdução

A matriz transferência, matriz coerência e os parâmetros de Stokes são as ferramentas utilizadas para trabalhar com a polarização da luz. As duas primeiras trabalham diretamente com o campo elétrico, enquanto o terceiro lida com a potência óptica, sendo este último, portanto, o mais utilizado na prática.

E2. Matriz de Transferência

Quando um feixe de luz polarizada incide sobre um dispositivo óptico, a luz resultante, na saída do dispositivo, pode ter sua polarização diferente da luz incidente. A matriz transferência, T , relaciona as componentes do campo emergente do dispositivo com as componentes do campo incidente no mesmo. Um dispositivo de duas portas é representado por uma matriz transferência 2×2 [Refs. E1-E3]:

$$\begin{pmatrix} E_x^s \\ E_y^s \end{pmatrix} = \begin{pmatrix} T_{xx} & T_{xy} \\ T_{yx} & T_{yy} \end{pmatrix} \begin{pmatrix} E_x^e \\ E_y^e \end{pmatrix} . \quad (E1)$$

Na Eq. (E1) os índices s e e significam saída e entrada, respectivamente. A seguir, nos restringiremos à descrição da matriz de transferência de polarizadores, rotacionadores, compensadores e fibras ópticas. O polarizador é um dispositivo linear que transmite apenas a componente do campo elétrico na direção que faz um ângulo θ com o eixo x , sendo θ o ângulo que caracteriza o polarizador. A componente do campo na direção dada por θ é:

$$E(\theta) = E_x \cos(\theta) + E_y \sin(\theta) . \quad (E2)$$

A matriz transferência do polarizador é dada por [Refs. E1-E3]:

$$P(\theta) = \begin{pmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta) \\ \sin(\theta)\cos(\theta) & \sin^2(\theta) \end{pmatrix} . \quad (E3)$$

O rotacionador é o dispositivo óptico que dá um incremento no ângulo de polarização de um determinado valor. A matriz transferência de um rotacionador de ângulo θ é [Refs. E1-E3]:

$$R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}. \quad (\text{E4})$$

O compensador dá um atraso de fase de δ entre as componentes do campo; sua matriz transferência é [Refs. E1-E3]:

$$C(\delta) = \begin{bmatrix} e^{i\frac{\delta}{2}} & 0 \\ 0 & e^{-i\frac{\delta}{2}} \end{bmatrix}. \quad (\text{E5})$$

A determinação exata da matriz transferência de uma fibra óptica é extremamente complicada, pois é dependente de diversos fatores. Desprezando os efeitos não-lineares (baixa potência óptica), um dos modelos propostos para a transmissão através de uma fibra de comprimento L é [Refs. E4-E5]:

$$T_f = \exp(-\alpha L + i\beta L) \begin{pmatrix} \varepsilon e^{i\xi_1} & \sqrt{1-\varepsilon^2} e^{i\xi_2} \\ -\sqrt{1-\varepsilon^2} e^{-i\xi_2} & \varepsilon e^{-i\xi_1} \end{pmatrix}, \quad (\text{E6})$$

onde α é a constante de atenuação e β é a constante de propagação do modo. Os parâmetros ε , ξ_1 e ξ_2 , que definem o acoplamento entre as componentes do campo, variam com o tempo e precisam ser estimados. Para estimar a matriz transferência de um dispositivo óptico aplicamos a este três entradas de polarizações conhecidas e trabalhamos com os campos de saída [Ref. E1]. Sejam os três estados de polarização incidentes conhecidos:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \frac{\sqrt{2}}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad (\text{E7})$$

gerando, respectivamente, na saída do dispositivo óptico a ser caracterizado, as saídas:

$$\begin{bmatrix} Ex_1^s \\ Ey_1^s \end{bmatrix}, \begin{bmatrix} Ex_2^s \\ Ey_2^s \end{bmatrix}, \begin{bmatrix} Ex_3^s \\ Ey_3^s \end{bmatrix}. \quad (\text{E8})$$

Então, a matriz transferência estimada do dispositivo é dada por [Ref. E1]:

$$T_{est} = K \begin{pmatrix} k_1 k_4 & k_2 \\ k_4 & 1 \end{pmatrix} \quad (\text{E9})$$

$$k_1 = \frac{Ex_1^s}{Ey_1^s}, \quad k_2 = \frac{Ex_2^s}{Ey_2^s}, \quad k_3 = \frac{Ex_3^s}{Ey_3^s} \quad (\text{E10})$$

$$k_4 = \frac{k_3 - k_2}{k_1 - k_3}, \quad (\text{E11})$$

onde K é uma constante complexa a ser determinada. Se não há perdas, o determinante da matriz transferência é unitário, o que nos leva a:

$$\det(T_{est}) = 1 \Rightarrow K = \frac{1}{\sqrt{k_1 k_4 - k_2 k_3}} \quad (E12)$$

E3. Parâmetros de Stokes

O vetor de Stokes é um vetor coluna no qual cada elemento representa a diferença de potência óptica entre estados de polarização de referência. Os parâmetros de Stokes são apresentados na Tabela E1 [Refs. E1-E3]:

PARÂMETRO	SIGNIFICADO
S_0	Potência total (luz polarizada + luz despolarizada)
S_1	Potência LH – Potência LV
S_2	Potência +45° – Potência -45° (linearmente polarizados nos ângulos indicados)
S_3	Potência CD – Potência CE (circular a direita - circular a esquerda)

Tabela E1- Definição dos parâmetros de Stokes.

O vetor de Stokes é da forma $[S_0 \ S_1 \ S_2 \ S_3]^T$. Quando a luz é parcialmente polarizada, a potência óptica da parte polarizada é dada por [Refs. E1-E3] :

$$P_p = \sqrt{S_1^2 + S_2^2 + S_3^2} \quad (E13)$$

Define-se o grau de polarização da luz parcialmente polarizada, como sendo [Refs. E1-E3]:

$$g_p = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0} \quad (E14)$$

Quando a luz é totalmente polarizada temos:

$$S_1^2 + S_2^2 + S_3^2 = S_0^2 \quad (E15)$$

A Eq. (E15) pode ser representada numa esfera (esfera de Poincaré), de raio S_0 , no espaço vetorial definido pelos vetores $(S_1, 0, 0)$, $(0, S_2, 0)$ e $(0, 0, S_3)$. Desta forma, para luz completamente polarizada, qualquer polarização pode ser representada por um ponto sobre a superfície da referida esfera. Quando $S_0 = 1$ então temos as potências normalizadas.

E4. Matriz Coerência

A matriz coerência representa as autocorrelações e correlações cruzadas das

componentes do campo elétrico. Ela é definida por [Refs. E1-E3]:

$$J = \begin{bmatrix} J_{xx} & J_{xy} \\ J_{yx} & J_{yy} \end{bmatrix} = \begin{bmatrix} \langle E_x E_x^* \rangle & \langle E_x^* E_y \rangle \\ \langle E_y^* E_x \rangle & \langle E_y^* E_y \rangle \end{bmatrix} = \langle E X E^+ \rangle . \quad (\text{E16})$$

A intensidade total do campo é, então, dada por [Refs. E1-E3]:

$$I = \langle E_x E_x^* \rangle + \langle E_y E_y^* \rangle = \text{Tr}(J) . \quad (\text{E17})$$

Usando as Eqs. (E1) e (E16) verificamos que, ao passar através de um dispositivo óptico com matriz de transferência T , a matriz coerência do campo na saída é dada por [Refs. E2, E3]:

$$J_s = T J_e T^+ , \quad (\text{E18})$$

onde T^+ é a adjunta Hermiteana da matriz transferência. A polarização de um sinal luminoso está diretamente relacionada com a coerência deste sinal. Quando não há correlação entre as componentes do campo, isto é, $J_{xy} = J_{yx} = 0$, a luz é totalmente despolarizada e, além disso, $J_{xx} = J_{yy}$. Por outro lado, quando a correlação entre as componentes é máxima, $|J_{xy}| = (J_{xx})^{1/2} (J_{yy})^{1/2}$, a luz é completamente polarizada. Quando a luz é parcialmente polarizada pode-se dividir a matriz coerência na soma de duas matrizes, sendo uma referente à luz totalmente polarizada e outra referente à luz totalmente despolarizada [Refs. E2, E3]:

$$J = J_{np} + J_p = A \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} B & D \\ D^* & C \end{bmatrix} , \quad (\text{E19})$$

com as condições para unicidade da relação [Refs. E2, E3]:

$$BC - |D|^2 = 0 \quad (\text{E20})$$

$$A \geq 0, B \geq 0 \text{ e } C \geq 0 . \quad (\text{E21})$$

Os elementos da decomposição de J são obtidos a partir de [Refs. E2, E3]:

$$A = \frac{1}{2} \left\{ \text{Tr}(J) - \sqrt{[\text{Tr}(J)]^2 - 4 \det(J)} \right\} \quad (\text{E22})$$

$$B = \frac{1}{2} (J_{xx} - J_{yy}) + \frac{1}{2} \sqrt{[\text{Tr}(J)]^2 - 4 \det(J)} \quad (\text{E23})$$

$$C = \frac{1}{2} (J_{yy} - J_{xx}) + \frac{1}{2} \sqrt{[\text{Tr}(J)]^2 - 4 \det(J)} \quad (\text{E24})$$

$$D = J_{xy} . \quad (\text{E25})$$

O grau de polarização pode ser obtido através de J usando [Refs. E2, E3]:

$$g_p = \frac{Tr(J_p)}{Tr(J)} = \sqrt{1 - \frac{4det(J)}{[Tr(J)]^2}} . \quad (E26)$$

Por fim, os elementos da matriz coerência e os parâmetros de Stokes podem ser relacionados através de [Refs. E2, E3]:

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & -i & i & 0 \end{bmatrix} \begin{bmatrix} J_{xx} \\ J_{xy} \\ J_{yx} \\ J_{yy} \end{bmatrix} \quad (E27)$$

ou, ainda, através das matrizes sigma [Refs. E2, E3]:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad \sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_3 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} , \quad (E28)$$

com as quais obtém-se [Refs. E2, E3]:

$$J = \frac{1}{2} \sum_{i=0}^3 S_i \sigma_i \quad (E29)$$

$$S_i = Tr(J \sigma_i) . \quad (E30)$$

APÊNDICE F

TEORIA QUÂNTICA DA INFORMAÇÃO

F1. Introdução

Com a utilização de estados quânticos para fins de comunicações faz-se necessário definir novos protocolos de comunicações entre as partes, redefinir conceitos clássicos comuns em sistemas de comunicações como a capacidade de canal e a implementação sistemas de codificação e criptografia baseados na teoria quântica. Mais ainda, surgem conceitos novos como a unidade básica de informação quântica, o *qubit*, e as formas de processá-lo como a clonagem e a teleportação. Este apêndice se destina a expor, de forma simples, os principais conceitos da teoria quântica da informação.

F2. Detecção de Eva, em Criptografia Quântica, Através da Teoria da Informação

O Apêndice C descreveu os principais protocolos de criptografia quântica mas sem levar em conta a teoria da informação. Nesta seção, seguindo as Referências F1 e F2, mostramos como a presença de Eva perturba a informação mútua entre Alice e Bob. Consideremos inicialmente que Alice faz uso dos estados $\{|a_i\rangle\}$ para se comunicar com Bob. Este, por sua vez, usa uma medida representada pelo operador $\hat{B}$, com autoestados $\{|b_i\rangle\}$, para identificar o estado enviado por Alice. Por fim, quando Eva estiver presente ela fará uma medida no fóton enviado por Alice com o operador $\hat{E}$, com autoestados $\{|e_i\rangle\}$, e retransmitirá o estado obtido da medição para Bob. Suponhamos agora que haverá sucesso na comunicação quando Alice enviar o estado $|a_i\rangle$ e, após a medida, Bob obtiver o estado $|b_k\rangle$. A probabilidade de sucesso é então dada por $P_s = |\langle b_k | a_i \rangle|^2$, que é a probabilidade do estado $|a_i\rangle$ colapsar para o estado $|b_k\rangle$ após uma medida com o operador $\hat{B}$. Consideremos agora as duas situações possíveis, ausência e presença de Eva. No primeiro caso, ausência, temos a situação mostrada na Fig F1.

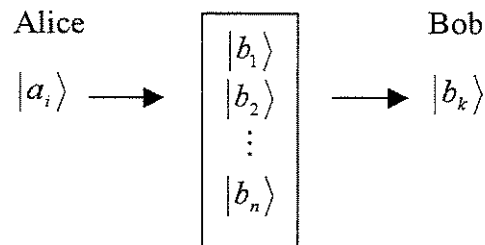


Fig. F1 – Recepção de $|b_k\rangle$ devido à transmissão de $|a_i\rangle$.

A probabilidade de sucesso é dada simplesmente por:

$$P_{ik}^1 = |\langle b_k | a_i \rangle|^2 \quad (\text{F1})$$

Expandindo $|a_i\rangle$ na base de autoestados de Eva, $\{|e_n\rangle\}$, obtemos:

$$|a_i\rangle = \sum_j |e_j\rangle \langle e_j | a_i \rangle \quad (\text{F2})$$

Substituindo a Eq. (F2) em (F1), a probabilidade de sucesso fica da forma:

$$P_{ik}^1 = |\langle b_k | a_i \rangle|^2 = \langle b_k | a_i \rangle \langle a_i | b_k \rangle = \langle b_k | \sum_j \langle e_j | a_i \rangle |e_j\rangle \langle e_i | \sum_l \langle a_i | e_l \rangle |b_k\rangle \Rightarrow \quad (\text{F3})$$

$$P_{ik}^1 = \sum_j \sum_l \langle e_j | a_i \rangle \langle b_k | e_j \rangle \langle a_i | e_l \rangle \langle e_l | b_k \rangle \quad (\text{F4})$$

Vejamos agora o segundo caso, presença de Eva, mostrada na Fig. F2.

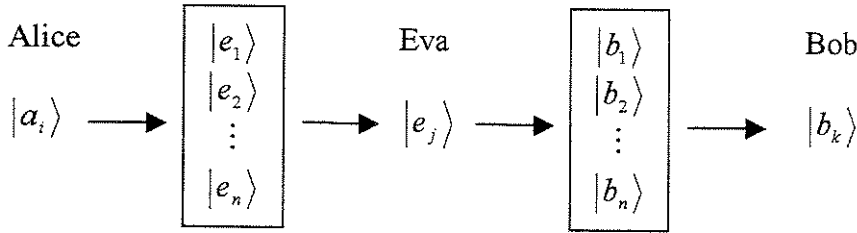


Fig. F2 – Recepção de $|b_k\rangle$ devido a transmissão de $|a_i\rangle$, passando por Eva.

A probabilidade de Bob obter $|b_k\rangle$, é igual ao produto das probabilidades, de Eva obter $|e_j\rangle$ dado que Alice enviou $|a_i\rangle$, e Bob obter $|b_k\rangle$ dado que Eva enviou $|e_j\rangle$, Eq. (F5).

$$P_{ik}^j = |\langle e_j | a_i \rangle|^2 |\langle b_k | e_j \rangle|^2 \quad (\text{F5})$$

Portanto, a probabilidade total de sucesso de Bob, na presença de Eva, é dada por:

$$P_{ik}^2 = \sum_j P_{ik}^j = \sum_j |\langle e_j | a_i \rangle|^2 |\langle b_k | e_j \rangle|^2 \Rightarrow \quad (\text{F6})$$

$$P_{ik}^2 = \sum_j \langle e_j | a_i \rangle \langle a_i | e_j \rangle \langle b_k | e_j \rangle \langle e_j | b_k \rangle \quad (\text{F7})$$

Comparando as Eqs. (F4) e (F7) chegamos a Eq. (F8).

$$P_{ik}^1 = P_{ik}^2 + \sum_j \sum_l \langle e_j | a_i \rangle \langle b_k | e_j \rangle \langle a_i | e_l \rangle \langle e_l | b_k \rangle (1 - \delta_{jl}) \quad (\text{F8})$$

Portanto, observando a Eq. (F8), vemos que a probabilidade de Bob receber o estado correto, $|b_k\rangle$, dado que Alice enviou $|a_i\rangle$, é menor quando Eva está presente. Desta forma, a presença de Eva pode ser detectada por uma maior taxa de erro na recepção.

Cada um dos operadores $\hat{A}$, $\hat{B}$ e $\hat{E}$, de Alice, Bob e Eva, respectivamente, constituem os alfabetos do sistema de comunicação. Os autoestado destes operadores são os símbolos dos respectivos alfabetos. Assumimos que todos os alfabetos possuem o mesmo número de símbolos, N , ou seja, todos pertencem a espaços de Hilbert de dimensão N . Mais ainda, assumimos também que os símbolos a_i são escolhidos por Alice com a mesma probabilidade, $p(a_i) = N^{-1}$. A informação mútua, que define a taxa de fluxo de informação entre Alice e Bob, nas condições especificadas, é dada por [Apêndice D e Ref. F2]

$$I(\hat{A}, \hat{B}) = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N P(b_k | a_i) \log_2[P(b_k | a_i)] \quad (\text{F9})$$

onde $P(b_k | a_i)$ é a probabilidade de Bob obter o estado $|b_k\rangle$ dado que Alice enviou $|a_i\rangle$, dada pela Eq. (F4) na ausência de Eva, e pela Eq. (F7) na presença de Eva. O termo $\log_2(N)$ é a entropia máxima da fonte (Alice) uma vez que os estados (símbolos) são equiprováveis. Assim, a informação mútua na ausência de Eva é obtida substituindo (F4) em (F9):

$$I_1(\hat{A}, \hat{B}) = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N P_{ik}^1 \log_2(P_{ik}^1) \Rightarrow \quad (\text{F10})$$

$$I_1(\hat{A}, \hat{B}) = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N |\langle b_k | a_i \rangle|^2 \log_2(|\langle b_k | a_i \rangle|^2) \quad (\text{F11})$$

Quando Alice e Bob usam o mesmo alfabeto, isto é, $|a_i\rangle = |b_i\rangle$ para todo valor de i , I_1 alcança seu valor máximo. Neste caso, com uso de $\langle a_k | a_i \rangle = \delta_{ik}$ (ortonormalidade) em (F11) obtemos $I_1(\hat{A}, \hat{A}) = \log_2(N)$. Quando Alice e Bob usam alfabetos conjugados tal que, $|\langle b_k | a_i \rangle|^2 = 1/N$, I_1 alcança seu valor mínimo, $I_1(\hat{A}, \hat{B}) = 0$. Assim, temos $0 \leq I_1 \leq \log_2(N)$. Na presença de Eva a informação mútua é dada por:

$$I_2(\hat{A}, \hat{B}) = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N P_{ik}^2 \log_2(P_{ik}^2) \quad (\text{F12})$$

Substituindo a Eq. (F7) na Eq. (F12) obtemos:

$$I_2(\hat{A}, \hat{B}) = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N \left[\sum_j |\langle e_j | a_i \rangle|^2 |\langle b_k | e_j \rangle|^2 \right] \log_2 \left(\sum_j |\langle e_j | a_i \rangle|^2 |\langle b_k | e_j \rangle|^2 \right) \quad (\text{F13})$$

Se Eva usa o mesmo alfabeto que Alice ($|e_i\rangle = |a_i\rangle$, $\forall i$), temos:

$$I_2 = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N \left(\sum_{j=1}^N |\langle a_j | a_i \rangle|^2 |\langle b_k | a_j \rangle|^2 \right) \log_2 \left(\sum_{m=1}^N |\langle a_j | a_i \rangle|^2 |\langle b_k | a_j \rangle|^2 \right) \quad (\text{F14})$$

que com a ortonormalidade dos estados $|a_i\rangle$ se torna:

$$I_2 = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N |\langle b_k | a_i \rangle|^2 \log_2 \left(|\langle b_k | a_i \rangle|^2 \right) = I_1 \quad (\text{F15})$$

Se, entretanto, Eva usa o mesmo alfabeto que Bob ($|e_i\rangle = |b_i\rangle$), temos:

$$I_2(\hat{A}, \hat{B}) = \log_2(N) + \frac{1}{N} \sum_{i=1}^N \sum_{k=1}^N \left[\sum_j |\langle b_j | a_i \rangle|^2 |\langle b_k | b_j \rangle|^2 \right] \log_2 \left(\sum_j |\langle b_j | a_i \rangle|^2 |\langle b_k | b_j \rangle|^2 \right) \quad (\text{F16})$$

Usando a ortonormalidade dos estados $|b_i\rangle$, a Eq. (F16) se torna igual a Eq. (F15). Por fim, se Alice e Bob usam o mesmo alfabeto e Eva escolhe um alfabeto conjugado ao escolhido por Alice e Bob, então encontramos que $I_2 \neq I_1$. Com o acima exposto, pode-se definir o parâmetro ε , dado por [Refs. F1, F2]:

$$\varepsilon = \frac{I_2(\hat{A}, \hat{B}) - I_1(\hat{A}, \hat{B})}{I_1^{\max}} = \frac{I_2(\hat{A}, \hat{B}) - I_1(\hat{A}, \hat{B})}{\log_2(N)} \quad (\text{F17})$$

que mede o grau de distúrbio introduzido por Eva no canal. Um valor negativo de ε implica que Eva causou uma redução no fluxo de informação entre Alice e Bob. Um valor positivo de ε implica que Eva causou um aumento no fluxo de informação entre Alice e Bob. Nestas duas situações Eva está sujeita a ser descoberta, ou seja, quando $I_1 \neq I_2 \Rightarrow \varepsilon \neq 0$ Eva pode ser detectada. Quando a Eq. (F15) for satisfeita, isto é, quando Eva usar o mesmo alfabeto que Alice e/ou Bob temos $\varepsilon = 0$. Como afirmado na Seção E.2.1, nesta situação Eva não pode ser detectada.

F3. Distinção de Estados Quânticos

Em comunicações quânticas a distinção dos estados quânticos é importante pois as mensagens, que precisam ser perfeitamente distinguíveis umas das outras para que a conversação entre as partes seja inteligível às mesmas, são codificadas em estados quânticos. Qualquer estado quântico é completamente caracterizado pela sua matriz densidade, entretanto, diferentes sistemas quânticos podem ter a mesma matriz densidade e, neste caso, os sistemas são indistinguíveis. Mais ainda, a distinção de dois estados quânticos depende da medida escolhida para identificá-los. Nesta seção mostramos dois métodos de distinção de matrizes densidades descritas nas Referências F3 e F4.

F3.1 Probabilidade de Erro

Sejam ρ_0 e ρ_1 matrizes densidades pertencentes ao mesmo espaço de Hilbert.

Desejamos, através das distribuições de probabilidade resultantes destas matrizes densidades, distinguir os estados. Suponhamos ainda que ρ_0 e ρ_1 sejam escolhidos com probabilidades π_0 e π_1 , respectivamente. Para distinguir os estados realizamos uma medida com o POVM dado pelos operadores $\{E_1, E_2, \dots, E_m\}$ representando os resultados $\{\xi_1, \xi_2, \dots, \xi_m\}$. Desta forma, as distribuições de probabilidades quando aplicamos o POVM aos estados descritos por ρ_0 e ρ_1 são:

Distr. Prob.	P_e^*	ξ_1	ξ_2	...	ξ_m
P_0	π_0	$p_0(1) = \text{Tr}(\rho_0 E_1)$	$p_0(2) = \text{Tr}(\rho_0 E_2)$	...	$p_0(m) = \text{Tr}(\rho_0 E_m)$
P_1	π_1	$p_1(1) = \text{Tr}(\rho_1 E_1)$	$p_1(2) = \text{Tr}(\rho_1 E_2)$	...	$p_1(m) = \text{Tr}(\rho_1 E_m)$

Tabela F1 - Distribuições de probabilidades das matrizes densidades ρ_0 e ρ_1 para o POVM especificado. * - probabilidades a priori de ρ_0 e ρ_1 .

Consideramos uma variável aleatória x , que assume os valores 0 ou 1, como identificadora do estado escolhido, ρ_0 ou ρ_1 , respectivamente. Desta forma, π_0 e π_1 são as probabilidades a priori da variável x , bem como, por exemplo, $p_0(1)$ é a probabilidade condicional de $\xi = \xi_1$ dado que $x = 0$, $p_c(\xi = \xi_1 | x=0)$. Podemos determinar as probabilidades a posteriori da variável x fazendo uso do teorema de Bayes [Apêndice D]:

$$p(x=i | \xi = \xi_j) = \frac{p(x=i)p_c(\xi = \xi_j | x=i)}{p(\xi = \xi_j)} = \frac{\pi_i p_i(j)}{\pi_0 p_0(j) + \pi_1 p_1(j)} \equiv q_i(j) \quad (\text{F18})$$

Suponhamos, agora, sem perda de generalidade, que os estados ρ_0 e ρ_1 são equiprováveis, $\pi_0 = \pi_1 = 0,5$. Desta forma, se Alice envia um daqueles estados para Bob, a estratégia ótima de Bob para adivinhar, através de uma medida, o estado enviado é observar as probabilidades a posteriori dada pela Eq. (F18). Obviamente, a probabilidade de sucesso de Bob depende da medida que ele realizar, portanto, Bob deve escolher a medida que minimize a probabilidade de erro. Mostra-se que o POVM que minimiza o erro é um PVM [Ref. F3, F4]. Portanto, se Bob através de uma medida obtiver o valor ξ_i , ele optará, como estimativa para o valor da variável x , o valor de x que corresponda a $\max\{q_0(i), q_1(i)\}$. A probabilidade média de sucesso é então dada por [Refs. F3, F4]:

$$PS(\rho_0, \rho_1) = \sum_i p(\xi_i) \max\{q_0(i), q_1(i)\} \quad (\text{F19})$$

Da mesma forma podemos definir a probabilidade de erro como sendo [Refs. F3, F4]:

$$PE(\rho_0, \rho_1) \equiv \sum_i p(\xi_i) \min\{q_0(i), q_1(i)\} \quad (\text{F20})$$

Usando a equiprobabilidade de ρ_0 e ρ_1 e a Eq. (F18) na Eq. (F20), esta última fica da forma:

$$PE(\rho_0, \rho_1) \equiv \frac{1}{2} \sum_i \min\{p_0(i), p_1(i)\} \quad (\text{F21})$$

Da Tabela F1 vemos que a Eq. (F21) depende da medida escolhida. Escolhendo o POVM ótimo como aquele que minimiza a Eq. (F21) podemos expressar a probabilidade de erro em função dos autovalores μ_j da matriz diferença $\rho_0 - \rho_1$ [Refs. F3, F4]:

$$PE(\rho_0, \rho_1) \equiv \frac{1}{2} + \frac{1}{2} \sum_{\mu_j \leq 0} \mu_j = \frac{1}{2} - \frac{1}{4} \sum_{j=1}^N |\mu_j| = \frac{1}{2} - \frac{1}{4} \text{Tr}(|\rho_0 - \rho_1|) \quad (\text{F22})$$

A probabilidade de erro é uma medida de distinção mas não é uma medida de distância. Uma medida de distância deve ser nula quando os estados são indistinguíveis e unitária quando os estados são maximamente distinguíveis. É possível relacionar a probabilidade de erro à conhecida distância de Kolmogorov, K , onde $0 \leq K \leq 1$, por [Refs. F3, F4]:

$$PE(\rho_0, \rho_1) = \frac{1}{2} - \frac{1}{2} K(\rho_0, \rho_1) \quad (\text{F23})$$

logo

$$K(\rho_0, \rho_1) = \frac{1}{2} \text{Tr}(|\rho_0 - \rho_1|) \quad (\text{F24})$$

F3.2 Fidelidade e Purificação

Sejam $|\alpha\rangle$ e $|\beta\rangle$ estados puros. Estes estados, como já visto, podem ser representados geometricamente por vetores no espaço a que pertencem. Uma medida natural de distinção entre estes estados quânticos é o cosseno do ângulo entre os vetores que os representam. Para estados normalizados temos que [Refs. F3-F5]:

$$|\langle \alpha | \beta \rangle| = |\alpha| |\beta| \cos(\theta) \quad (\text{F25})$$

Defini-se então, como uma medida de distinção, a sobreposição ou *overlap*, sendo dada por [Refs. F3-F5]:

$$\text{overlap}(|\alpha\rangle, |\beta\rangle) = |\langle \alpha | \beta \rangle| \quad (\text{F26})$$

Se os estados não são puros a situação é mais complicada e precisamos do conceito de purificação. Se ρ_0 é a matriz densidade de um estado misto no espaço H_1 , então pode-se estender este espaço de Hilbert tal que o estado misto, representado por ρ_0 , se torne um estado puro no espaço combinado $H_1 \otimes H_2$. Ou ainda, sempre podemos encontrar uma extensão H_2 de H_1 e um estado $|\varepsilon\rangle \in H_1 \otimes H_2$ tal que [Refs. F3-F5]:

$$\text{Tr}_2(|\varepsilon\rangle\langle\varepsilon|) = \rho_0 \quad (\text{F27})$$

O sub-índice 2 na Eq. (F27) indica que os graus quânticos de liberdade pertencentes ao espaço H_2 devem ser descartados. Quando isto acontece o estado $|\varepsilon\rangle$ é dito ser uma purificação de ρ_0 . Este conceito leva ao entendimento de que, quando um estado puro perde alguns graus quânticos de liberdade ele se torna um estado misto. Ou ainda, quando não temos acesso ao espaço completo mas a apenas a uma parte dele acabamos por obter um estado misto. Existem muitas purificações de uma mesma matriz densidade, cada uma correspondendo a um *ensemble* que o preparador do estado misto pode ter usado para construí-lo. Da mesma forma, se $|\xi\rangle$ é uma purificação de ρ_1 , então podemos usar a Eq. (F26) como uma medida de distância entre as duas matrizes densidades representando os estados mistos [Refs. F3, F4]:

$$\text{overlap}(\rho_0, \rho_1) = \max |\langle \varepsilon | \xi \rangle| \quad (\text{F28})$$

onde o máximo é tomado sobre todas as purificações $|\varepsilon\rangle$ e $|\xi\rangle$ de ρ_0 e ρ_1 , respectivamente. A equação explícita para a sobreposição a partir das matrizes densidade é [Refs. F3-F5]:

$$\text{overlap}(\rho_0, \rho_1) = \text{Tr}(\sqrt{\rho_0} \rho_1 \sqrt{\rho_0}) \quad (\text{F29})$$

Defini-se, a partir do *overlap*, a fidelidade de um estado em relação a outro como sendo [Refs. F3-F6]:

$$F(\rho_0, \rho_1) = [\text{overlap}(\rho_0, \rho_1)]^2 \quad (\text{F30})$$

No caso de dois estados puros a fidelidade, usando as Eqs. (F26) e (F30), é dada por:

$$F = |\langle \xi | \varepsilon \rangle|^2 \quad (\text{F31})$$

cuja interpretação física é óbvia, ela dá a probabilidade do estado $|\varepsilon\rangle$ colapsar para o estado $|\xi\rangle$, ou seja, é a projeção de um estado sobre o outro. Se ρ_1 é uma mistura e ρ_0 é um estado puro então

$$F(\rho_0, \rho_1) = \langle \varepsilon | \rho_1 | \varepsilon \rangle \quad (\text{F32})$$

é a probabilidade da partícula no estado misto ρ_1 colapsar para o estado $|\varepsilon\rangle$. Se ρ_0 e ρ_1 são ambos estados mistos então a fidelidade é dada pelas Eqs. (F29) e (F30), mas não há interpretação física para a fidelidade [Ref. F3].

F4. Teoria da Informação em Comunicações Quânticas

Em um sistema de comunicação quântica precisamos inicialmente definir quais estados quânticos representarão as mensagens ou bits. Por exemplo, os estados com operadores densidade ρ_0 e ρ_1 poderiam representar os bits 0 e 1, respectivamente. O receptor, por sua vez, deve ser capaz de distinguir perfeitamente os estados ρ_0 e ρ_1 para que

as mensagens enviadas possam ser recuperadas sem erros. Se a fonte transmite os estados $\rho_0, \rho_1, \dots, \rho_n$ os quais são puros e ortogonais, com probabilidades $p_0, p_1, \dots, p_n$, então existe uma medida que os distingue perfeitamente. Uma consequência direta disso é que a entropia quântica é igual a informação mútua uma vez que a única incerteza provém das probabilidades clássicas dos estados serem transmitidos. Se os estados transmitidos pela fonte são puros porém não ortogonais, então não existe nenhuma medida que possa distingui-los completamente, ou seja, o receptor não poderá extrair informação completa da fonte e determinar qual estado foi transmitido. O que se pode fazer é escolher uma medida que maximize a distância entre os estados o que também maximiza a informação mútua. O mesmo também é válido se os estados são mistos. Suponhamos, agora, que o transmissor escolhe entre os estados ρ_0 e ρ_1 com probabilidades a priori π_0 e π_1 , respectivamente, e o receptor usa uma medida representada pelo operador $\hat{A}$, com autoestados $|a_i\rangle$, para distingui-los. A entropia de Shannon é então dada por [Refs. Apêndice D, Refs. F3-F5]:

$$H(\rho) = -\sum_i p(a_i | \rho) \log_2 p(a_i | \rho) = -\sum_i \langle a_i | \rho | a_i \rangle \log_2 \langle a_i | \rho | a_i \rangle \quad (\text{F33})$$

$$\rho = \pi_0 \rho_0 + \pi_1 \rho_1 \quad (\text{F34})$$

e a informação mútua é [Apêndice D, Refs. F3-F5]:

$$I = H(\rho) - H(\rho | a) \quad (\text{F35})$$

onde o segundo termo do lado direito da Eq. (F35) é dado por:

$$H(\rho | a) = -\sum_i p(\rho_0) p(\rho_0 | a_i) \log_2 [p(\rho_0 | a_i)] + p(\rho_1) p(\rho_1 | a_i) \log_2 [p(\rho_1 | a_i)] = \quad (\text{F36})$$

$$-\pi_0 \sum_i p(\rho_0 | a_i) \log_2 [p(\rho_0 | a_i)] - \pi_1 \sum_i p(\rho_1 | a_i) \log_2 [p(\rho_1 | a_i)] = \quad (\text{F37})$$

$$-\pi_0 \sum_i \langle a_i | \rho_0 | a_i \rangle \log_2 \langle a_i | \rho_0 | a_i \rangle - \pi_1 \sum_i \langle a_i | \rho_1 | a_i \rangle \log_2 \langle a_i | \rho_1 | a_i \rangle \Rightarrow \quad (\text{F38})$$

$$H(\rho | a) = -\pi_0 H(\rho_0) - \pi_1 H(\rho_1) = -\sum_i \pi_i H(\rho_i) \quad (\text{F39})$$

Portanto, a quantidade de informação clássica que podemos extrair de uma fonte de estados quânticos, fazendo uso de uma medida, é dada pelas Eqs. (F33)-(F35) e (F39). Entretanto, a máxima quantidade de informação que podemos extrair de uma fonte de estado quânticos através de uma medida ótima é limitada pelo teorema de Kholevo [Refs. F3-F7]:

$$I \leq S\left(\sum_i p_i \rho_i\right) - \sum_i p_i S(\rho_i) \quad (\text{F40})$$

onde a igualdade ocorre quando todos os ρ_i 's comutam entre si. S é a entropia quântica de Von Neumann dada por [Refs. F3-F7]:

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i \quad (\text{F41})$$

onde λ_i são os autovalores de ρ . Se ρ_i é um estado puro então $S(\rho_i) = 0$. Portanto, se o transmissor envia apenas estados puros, através de um canal ideal, para o receptor e este, por sua vez, usa uma medição nos estados para determinar identidade dos mesmos, a quantidade de informação obtida pelo receptor não pode ser maior que a entropia da fonte:

$$I \leq S\left(\sum_i p_i \rho_i\right) \quad (\text{F42})$$

Se os estados pertencem a um espaço de Hilbert de dimensão N , de forma que tenhamos $i = 1 \dots N$, então, pela Eq. (F41) vemos que o máximo valor da entropia ocorre quando $\lambda_i = N^{-1}$ e é igual a $S_{\max} = \log_2 N$. Semelhantemente, também existe um limite inferior de informação acessível dado pelo teorema de Jozsa-Robb-Wooters. Segundo este limite temos que [Ref. F8]:

$$I \geq Q\left(\sum_i p_i \rho_i\right) - \sum_i p_i Q(\rho_i) \quad (\text{F43})$$

onde $Q(\rho)$ é a sub-entropia da matriz densidade dada, em função dos autovalores de ρ , por [Ref. F8]:

$$Q(\rho) = -\sum_{i=1}^n \left(\prod_{i \neq j} \frac{\lambda_i}{\lambda_i - \lambda_j} \right) \lambda_i \log_2 \lambda_i \quad (\text{F44})$$

Se dois ou mais autovalores são iguais então o limite quando eles se tornam iguais deve ser tomado na Eq. (F44). Portanto, de forma simples, temos que: Se usarmos uma medida para identificar os estados de uma fonte de estados quânticos, os teoremas de Kholevo e Jozsa-Robb-Wooters afirmam, respectivamente, que não há medida capaz de extrair uma quantidade de informação nem maior que a dada pela Eq. (F40) nem menor que a dada pela Eq. (F43).

Até este momento temos falado apenas da informação clássica de sistemas quânticos. Entretanto, os estados quânticos possuem também a sua própria informação quântica, sendo a quantidade básica desta informação chamada de *qubit*. Um *qubit* corresponde a um sistema quântico de dois estados (puros) ou seja, um sistema que pertença a um espaço de Hilbert de dimensão 2. Usando o teorema de Kholevo mostra-se que a máxima quantidade de informação clássica que pode ser extraída de um *qubit* é um bit pois, como o *qubit* é um sistema bidimensional temos, $I_{\max} \leq S_{\max}(\rho) = \log_2 2 = 1$ bit.

Uma questão interessante é que *qubits* não podem, em geral, ser clonados ou copiados. Isto é, se alguém dispõe de um estado, este alguém não pode criar outro igual e permanecer com o que já tinha. Este fato está diretamente ligado a distinção dos estados quânticos uma vez que, para copiar um estado precisa-se inicialmente identificá-lo através de uma medida para só depois produzir outro igual. A Fig. F1 ilustra a situação.

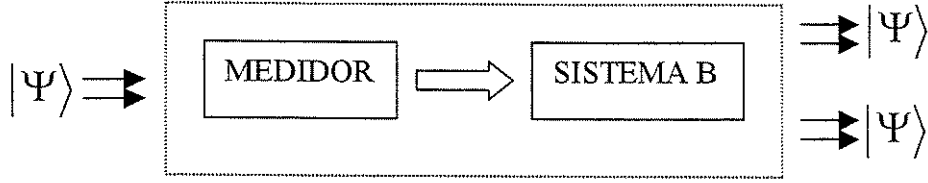


Fig. F1 - Esquema de clonagem de *qubit*.

Na Fig. F1, o estado incidente é medido e a informação sobre o resultado da medição é usada no sistema B para produzir o segundo *qubit*. Para mostrar que a clonagem não é possível usaremos os argumentos da Referência F9. Suponhamos dois sistemas *A* e *B* onde queremos fazer uma cópia de um estado de *A* em *B*. A Eq. (F45) é a representação matemática do processo.

$$|x_a, 0_b\rangle \rightarrow |x_a, x_b\rangle \quad (\text{F45})$$

onde $|x_a\rangle$ é o estado a ser copiado, $|0_b\rangle$ é a representação de um estado nulo de *B* e $|x_b\rangle$ é a representação de $|x_a\rangle$ em *B*. Então, se o processo de clonagem é possível de ser realizado, para dois estados distintos temos [Ref. F9]:

$$|x_a, 0_b\rangle \rightarrow |x_a, x_b\rangle \quad (\text{F46})$$

$$|y_a, 0_b\rangle \rightarrow |y_a, y_b\rangle \quad (\text{F47})$$

Seja, agora, o estado superposição dos dois anteriores $|z_a\rangle = |x_a\rangle + |y_a\rangle$. A clonagem deste estado daria [Ref. F9]:

$$|z_a, 0_b\rangle = |x_a, 0_b\rangle + |y_a, 0_b\rangle \rightarrow |x_a, x_b\rangle + |y_a, y_b\rangle = |z_a, z_b\rangle \quad (\text{F48})$$

Entretanto, como sabemos que evoluções de estados quânticos devem ser regidas por operadores unitários devemos ter [Ref. F9]:

$$|z_a, z_b\rangle = |x_a, x_b\rangle + |x_a, y_b\rangle + |y_a, x_b\rangle + |y_a, y_b\rangle \quad (\text{F49})$$

Portanto, como as Eqs. (F48) e (F49) são diferentes temos que, se dois estados distintos podem ser copiados fielmente, uma superposição destes dois estados não pode, há menos que os estados sejam todos ortogonais entre si. Diferentemente da cópia existe um processo, chamado de transposição, que não leva uma cópia do estado para o novo espaço:

$$|x_a, 0_b\rangle \rightarrow |0_a, x_b\rangle \quad (\text{F50})$$

Na Eq. (F50) vemos que após a transposição o estado original é destruído. A transposição é possível de ser realizada em sistemas entrelaçado, sendo verificada no processo de teleportação, que será resumidamente explicado mais a frente.

Por fim, até o presente momento temos considerado que os estados quânticos produzidos e enviados pelo transmissor chegam intactos ao receptor. Em sistemas reais isto não ocorre, ao ser transmitido por um canal ruidoso (canal que permite a interação do estado quântico com o ambiente) o estado quântico enviado sofre perturbações e evoluções para diferentes estados. Controlar e/ou corrigir estas perturbações é uma tarefa bastante complicada e que em parte foi considerada no Capítulo 2. A qualidade da transmissão dos estados quânticos pode ser medida pela fidelidade média do estado recebido em relação ao estado transmitido. Quanto mais próxima de 1 for a fidelidade, melhor será o canal para a transmissão. Se, por exemplo, o transmissor usa os estados puros $|\varepsilon\rangle$ e $|\xi\rangle$, os quais ocorrem com probabilidades π_0 e π_1 , e estes estados, após interagirem com o canal, evoluem para os estados mistos ρ_a e ρ_b , respectivamente, então a fidelidade média, com uso da Eq. (F32), é dada por:

$$F = \pi_0 \langle \varepsilon | \rho_a | \varepsilon \rangle + \pi_1 \langle \xi | \rho_b | \xi \rangle \quad (\text{F51})$$

F5. Estados Quânticos Entrelaçados

Como já discutido no Apêndice A, pode-se produzir estados quânticos entrelaçados ou correlacionados. Estes estados são bastante enigmáticos e apresentam uma rica fonte de pesquisa em teoria da informação quântica. Dizemos que os sistemas a e b , por exemplo dois fótons, são correlacionados se a medida de pelo ao menos um observável do sistema $a(b)$ projeta o sistema $b(a)$ em um novo estado. Se o estado conjunto dos sistemas individuais é representado por uma matriz densidade ρ , e os estados são realmente entrelaçados, então necessariamente temos que [Refs. F5, F6, F10-F12]:

$$\rho \neq \rho_{ab} = \rho_a \otimes \rho_b \quad (\text{F52})$$

Nos estados entrelaçados uma medida em uma das partes não pode prover informação completa sobre o conjunto, ou seja, existe informação na correlação entre os sistemas. A medida realizada em uma das partes é completamente caracterizada pela matriz densidade parcial do sistema em questão. Assim, se medirmos o observável $\hat{O}$ nos sistemas individuais, temos [Refs. F4-F6, F10-F12]:

$$\langle \hat{O} \rangle_a = \text{Tr}(\rho_a \hat{O}) = \text{Tr}[(\hat{O} \otimes \hat{I}_b) \rho] \quad (\text{F53})$$

$$\langle \hat{O} \rangle_b = \text{Tr}(\rho_b \hat{O}) = \text{Tr}[(\hat{I}_a \otimes \hat{O}) \rho] \quad (\text{F54})$$

onde $\hat{I}_a$ e $\hat{I}_b$ são os operadores identidade dos espaços aos quais ρ_a e ρ_b pertencem, respectivamente. As matrizes densidades parciais são dadas por [Refs. F4-F6, F10-F12]:

$$\rho_a = \text{Tr}_b(\rho) \quad (\text{F55})$$

$$\rho_b = \text{Tr}_a(\rho) \quad (\text{F56})$$

onde o sub-índice no operador traço indica que os graus quânticos de liberdade do sistema indicado devem ser descartados. A Eq. (F52) motiva a observação das relações entre as entropias individuais e a entropia do sistema entrelaçado. A primeira relação é a desigualdade de Araki e Lieb [Refs. F11, F12]:

$$|S_a - S_b| \leq S \leq S_a + S_b \quad (\text{F57})$$

onde

$$S_a = -\text{Tr}(\rho_a \log_2 \rho_a) \quad (\text{F58})$$

$$S_b = -\text{Tr}(\rho_b \log_2 \rho_b) \quad (\text{F59})$$

são as entropias dos sistemas individuais a e b , respectivamente. Assim, se o estado conjunto é um estado puro, $S = 0$, então, pela Eq. (F57), $S_a = S_b$. Como existe informação na correlação defini-se um índice de correlação como sendo [Refs. F11, F12]:

$$I_c = S_a + S_b - S \geq 0 \quad (\text{F60})$$

O valor máximo de I_c acontece quando $S = 0$, ou seja, para que a correlação seja máxima o estado conjunto deve ser um estado puro. Assim, pelo acima exposto, o valor máximo do índice correlação é $I_c^{\max} = 2S_a = 2S_b$. Por outro lado, quando os estados individuais são descorrelacionados temos $I_c^{\min} = 0$. Agora, se A e B são observáveis dos sistemas individuais a e b , respectivamente, então a informação mútua $H(A:B)$ obtida a partir de uma medida conjunta de A em a e B em b deve satisfazer a [Refs. F11, F12]:

$$H(A:B) \leq S(\rho_i) \quad i = a, b \quad (\text{F61})$$

Ou seja, a informação mútua é uma medida do grau de correlação entre os observáveis A e B . Portanto, a correlação entre os observáveis em diferentes sistemas é limitado pela entropia de cada sistema. A entropia de uma partícula depende do seu entrelaçamento com a outra partícula. Portanto uma medida do entrelaçamento de um estado puro é dada por [Refs. F5, F11, F12]:

$$E = S(\rho_1) = S(\rho_2) \quad (\text{F62})$$

F5.1. Medida POVM

Na Seção A6 do Apêndice A foram descritos dois tipos de medidas quânticas, POM e POVM ou PVM. A medida POM é baseada num conjunto completo de operadores projeção, $\hat{\Pi}_i$, $i = 1, 2, 3, \dots, n$ sobre n sub-espacos ortogonais do espaço de Hilbert do sistema quântico. Cada operador representa um dos possíveis resultados da medida. A probabilidade de cada possível resultado é dada por:

$$p_i = \text{Tr}(\rho \hat{\Pi}_i) \quad (\text{F63})$$

A medida POVM é mais geral, ela coloca o sistema a ser medido em contato com um sistema auxiliar, preparado em algum estado padrão. Os dois sistemas são então permitidos evoluir unitariamente tal que se tornem correlacionados ou entrelaçados. Por fim, faz-se uma medida reproduzível no sistema auxiliar. O esquema é mostrado na Fig. F2 [Refs. F3-F5]:

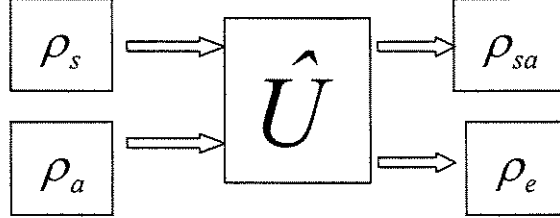


Fig. F2 - Esquema da medição POVM.

Na Fig. F2, ρ_s e ρ_a são os estados do sistema a ser medido e do sistema auxiliar, respectivamente, enquanto que, ρ_{sa} e ρ_e são as saídas entrelaçadas. Uma medida reproduzível do sistema auxiliar é descrita via um conjunto de operadores projeção ortogonais $\{\hat{I} \otimes \hat{\Pi}_i\}$ atuando no espaço de Hilbert do sistema auxiliar. A probabilidade do i -ésimo resultado ser obtido numa medição é dada por [Refs. F3-F5]:

$$p_i = \text{Tr}[\hat{U}(\rho_s \otimes \rho_a)\hat{U}^+ (\hat{I} \otimes \hat{\Pi}_i)] \quad (\text{F64})$$

pois

$$\text{Tr}(\hat{\Pi}_i \rho_a) = \text{Tr}[(\hat{I} \otimes \hat{\Pi}_i) \rho] \quad (\text{F65})$$

$$\text{Tr}(\hat{\Pi}_i \rho_s) = \text{Tr}[(\hat{\Pi}_i \otimes \hat{I}) \rho] \quad (\text{F66})$$

com $\rho = \hat{U}(\rho_s \otimes \rho_a)\hat{U}^+$. O número de resultados possíveis é limitado pela dimensão do espaço de Hilbert do sistema auxiliar. Sejam agora $\{|S_k\rangle\}_{k=1}^n$ e $\{|A_j\rangle\}_{j=1}^m$ bases para os espaços do sistema a ser medido e do sistema auxiliar, com dimensões n e m , respectivamente. Então, usando a propriedade cíclica do traço temos [Ref. F3]:

$$p_i = \sum_{k=1}^n \sum_{j=1}^m \langle S_k | \langle A_j | [(\rho_s \otimes \rho_a)\hat{U}^+ (\hat{I} \otimes \hat{\Pi}_i) \hat{U}] | S_k \rangle | A_j \rangle \quad (\text{F67})$$

ou ainda

$$p_i = \sum_{k=1}^n \langle S_k | \rho_s \left[\sum_{j=1}^m \langle A_j | (\hat{I} \otimes \rho_a) \hat{U}^+ (\hat{I} \otimes \hat{\Pi}_i) \hat{U} | A_j \rangle \right] | S_k \rangle \Rightarrow \quad (\text{F68})$$

$$p_i = \text{Tr}_s(\hat{E}_i \rho_s) \quad (\text{F69})$$

onde os operadores $\hat{E}_i$ são os mesmos usados na Seção 6 do Apêndice A e, pela Eq. (F68), são dados por [Ref. F3]:

$$\hat{E}_i = \text{Tr}_a \left[(\hat{I} \otimes \rho_a) \hat{U} (\hat{I} \otimes \hat{\Pi}_i) \hat{U}^\dagger \right] \quad (\text{F70})$$

Seja, por exemplo, o estado $|\theta\rangle = \alpha|0^\circ\rangle + \beta|90^\circ\rangle$ medido na base $\{|0^\circ\rangle, |90^\circ\rangle\}$ e $|\varphi\rangle$ o estado inicial do aparelho de medida. Então, no processo de medida temos:

$$|\theta\rangle|\varphi\rangle \rightarrow \hat{U} \rightarrow \alpha|0^\circ\rangle|\varphi_0\rangle + \beta|90^\circ\rangle|\varphi_1\rangle \quad (\text{F71})$$

Se, por exemplo, o estado do aparelho após a medida é $|\varphi_0\rangle$ então o estado medido é $|0^\circ\rangle$. Isto ocorre com probabilidade $|\alpha|^2$, enquanto que a outra situação, aparelho em $|\varphi_1\rangle$ e estado medido em $|90^\circ\rangle$ ocorre com probabilidade $|\beta|^2$. Uma consequência direta do acima exposto é que, dado dois estado não ortogonais, se existe uma medida que realizada nos referidos estados não os perturba, então esta medida não pode obter qualquer informação sobre em qual dos dois estados o sistema está. A prova é simples [Ref. F4], sejam os estados não ortogonais $|\alpha\rangle$ e $|\beta\rangle$, logo $\langle\alpha|\beta\rangle \neq 0$. Seja também $|\varphi\rangle$ o estado inicial do aparelho. Uma medida que não perturba os estados faria:

$$|\alpha\rangle|\varphi\rangle \rightarrow \hat{U} \rightarrow |\alpha\rangle|\varphi_\alpha\rangle \quad (\text{F72})$$

$$|\beta\rangle|\varphi\rangle \rightarrow \hat{U} \rightarrow |\beta\rangle|\varphi_\beta\rangle \quad (\text{F73})$$

onde $\hat{U}$ é o operador que caracteriza a medida. Como este operador é unitário o produto interno do estados antes e após a medida se conservam:

$$\langle\alpha|\beta\rangle\langle\varphi|\varphi\rangle = \langle\varphi, \alpha|\beta, \varphi\rangle = \langle\varphi_\alpha, \alpha|\beta, \varphi_\beta\rangle = \langle\alpha|\beta\rangle\langle\varphi_\alpha|\varphi_\beta\rangle \quad (\text{F74})$$

Como, $\langle\alpha|\beta\rangle \neq 0$ e $\langle\varphi|\varphi\rangle=1$ temos de (F74) que $\langle\varphi_\alpha|\varphi_\beta\rangle=1$. Entretanto, como os estados do aparelho são normalizados temos necessariamente que $|\varphi_\alpha\rangle = |\varphi_\beta\rangle$, ou seja, o estado final após a medida é o mesmo independente do estado que foi medido, portanto nenhuma informação é obtida.

O esquema da Fig. F2 é usado como modelo de medida mas um modelo igual também é usado num sistema de criptografia quântica com a presença de Eva [Ref. F4], uma vez que ela realiza uma medida nos fótons enviados por Alice.

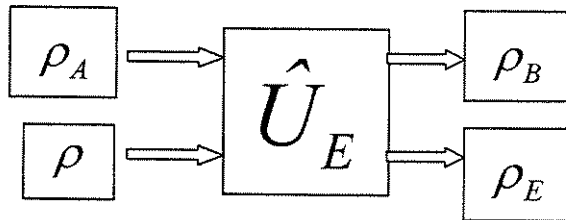


Fig. F3 - Esquema de criptografia quântica com Eva.

ρ_A e ρ_B são as matrizes densidade de Alice e Bob, respectivamente. ρ e ρ_E são os estado inicial e final de Eva, bem como $\hat{U}_E$ é o operador unitário da medida de Eva. Do já exposto nesta seção temos [Ref. F4]:

$$\rho_B = \text{Tr}_E [\hat{U}_E (\rho_A \otimes \rho) \hat{U}_E^\dagger] \quad (\text{F75})$$

$$\rho_E = \text{Tr}_B [\hat{U}_E (\rho_A \otimes \rho) \hat{U}_E^\dagger] \quad (\text{F76})$$

A distância entre ρ e ρ_E é uma medida da informação ganha por Eva, bem como a distância entre ρ_A e ρ_B é uma medida da quantidade de distúrbio que Eva, através de $\hat{U}_E$, causou. Portanto, se Eva tenta ganhar informação ela necessariamente causa distúrbios na comunicação entre Alice e Bob.

F5.2. Medida Não-Local

Seja um sistema de dois fótons entrelaçados, um é enviado para Alice e o outro para Bob. Quando, por exemplo, Alice faz uma medida individual em seu fóton, esta é uma medida local. Se, por outro lado, uma medida é realizada nos dois fótons pelo mesmo indivíduo, então a medida é dita não local. Outra forma de medida não local é a baseada na Fig. F4. Alice e Bob fazem, independentemente, uma medida em seus fótons. Depois, através de um canal clássico, Alice e Bob informam um ao outro o resultado de suas medições [Ref. F5].

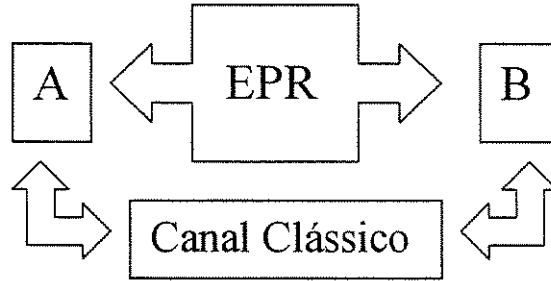


Fig. F4 - Medida não local = medida local + comunicação

Estando Alice e Bob de posse do resultado das duas medições, eles podem determinar o estado do sistema conjunto. Por exemplo, a fonte EPR é suposta produzir, com igual probabilidade, os estados:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|0^\circ\rangle|90^\circ\rangle - |90^\circ\rangle|0^\circ\rangle) \quad (\text{F77})$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}} (|0^\circ\rangle|0^\circ\rangle - |90^\circ\rangle|90^\circ\rangle) \quad (\text{F78})$$

Se Alice e Bob fazem uma medida, na base $\{|0^\circ\rangle, |90^\circ\rangle\}$, em seus fótons, eles obterão como resultado os estados $|0^\circ\rangle$ e $|90^\circ\rangle$ com 50% de probabilidade de ocorrência. Se eles não se

comunicam a medida realizada em nada ajuda a determinar em qual estado entrelaçado os fótons foram enviados. Por outro lado, se eles se comunicam informando um ao outro o resultado de suas medidas então, se os resultados das medidas forem opostos o estado conjunto é o da Eq. (F77) enquanto que, se os resultados das medidas são iguais, então o estado conjunto é da Eq. (F78). Portanto, uma medida local seguida de uma comunicação clássica determinam o estado não local.

F5.3. Teleportação

Um dos resultados mais impressionantes da teoria quântica da informação é a teleportação [Refs. F5, F13]. Ela consiste da transmissão de um qubit de Alice para Bob sem que o mesmo seja realmente transmitido. Inicialmente Alice e Bob dividem um par EPR e Alice tem um qubit que deseja enviar para Bob. Alice faz então uma medição combinada [Ref. F13], no espaço de Hilbert quadrimensional, de seu fóton e seu *qubit*. Esta medição vai determinar em qual dos seguintes estados o conjunto fóton-qubit está [Refs. F5, F13]:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) \quad (F79)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \quad (F80)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \quad (F81)$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \quad (F82)$$

Estes 4 estados são então codificados em 2 bits clássicos (00, 01, 10, 11) e enviados a Bob. De acordo com a informação que recebeu de Alice, Bob aplica em seu fóton um dos seguintes operadores [Refs. F5, F13]:

$$\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (F83)$$

sendo o primeiro correspondente à Eq. (F79) e assim por diante. O *qubit* que Bob agora detém é o *qubit* original que Alice queria enviá-lo, com perfeita fidelidade. É importante notar que a teleportação não viola nenhum princípio físico. A teleportação só ocorre depois que a informação clássica enviada por Alice chega a Bob, por isso ela se dá a uma velocidade menor que a luz. Além disso, não é cópia ou clonagem pois o *qubit* de Alice é destruído quando ela o mede. A Fig. 5 mostra o esquema em blocos da teleportação de um fóton.

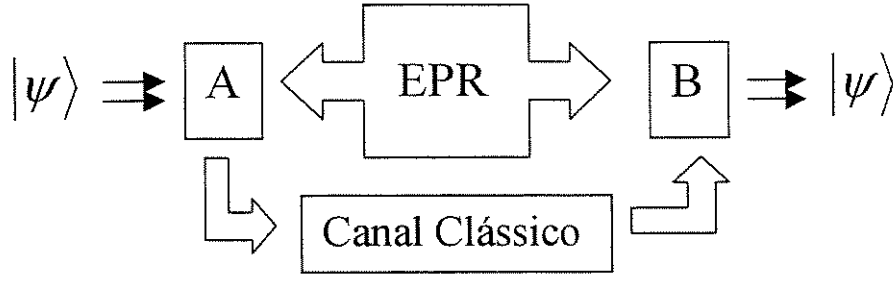


Fig. 5 - Esquema de Teleportação

Suponhamos, por exemplo, que Alice e Bob dividam inicialmente o par EPR:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} \left(|0^\circ\rangle_A |90^\circ\rangle_B - |90^\circ\rangle_A |0^\circ\rangle_B \right) \quad (\text{F84})$$

e que Alice quer teletransportar para Bob o *qubit*:

$$Q = (|0^\circ\rangle \pm |90^\circ\rangle) / \sqrt{2} \quad (\text{F85})$$

Alice faz então uma medida conjunta em seu fóton e no *qubit* e poderá obter como resultado de sua medida, com 25% de chance, cada um dos seguintes resultados:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} \left(|0^\circ\rangle_A |90^\circ\rangle_Q - |90^\circ\rangle_A |0^\circ\rangle_Q \right) \quad (\text{F86})$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} \left(|0^\circ\rangle_A |90^\circ\rangle_Q + |90^\circ\rangle_A |0^\circ\rangle_Q \right) \quad (\text{F87})$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}} \left(|0^\circ\rangle_A |0^\circ\rangle_Q - |90^\circ\rangle_A |90^\circ\rangle_Q \right) \quad (\text{F88})$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \left(|0^\circ\rangle_A |0^\circ\rangle_Q + |90^\circ\rangle_A |90^\circ\rangle_Q \right) \quad (\text{F89})$$

Suponhamos então que Alice obteve como resultado de sua medida conjunta a Eq. (F86). Com já visto, Alice avisará a Bob que ele deve usar em seu fóton o operador σ_1 . Assim temos duas situações possíveis:

- 1) O fóton de Alice está no estado $|0^\circ\rangle$, $[1 \ 0]^T$, e portanto Bob estará no estado $|90^\circ\rangle$, $[0 \ 1]^T$.
Logo, após Bob aplicar o operador σ_1 em seu fóton este irá para o estado:

$$|\theta\rangle_B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |90^\circ\rangle \quad (\text{F90})$$

2) O fóton de Alice está no estado $|90^\circ\rangle$, $[0 \ 1]^T$, e portanto Bob estará no estado $|0^\circ\rangle$, $[1 \ 0]^T$. Logo, após Bob aplicar o operador σ_1 em seu fóton este irá para o estado:

$$|\theta\rangle_B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0^\circ\rangle \quad (\text{F91})$$

As eqs. (F86), (F90) e (F91) nos mostram que o fóton de Bob vai para o mesmo estado que o *qubit* que estava em Alice.