UNIVERSIDADE ESTADUAL PAULISTA
”Júlio de Mesquita Filho”

Pós-Graduação em Ciência da Computação

Camila Brandão

Ensaios sobre computação e informação quânticas: fundamentação e simulações sobre o efeito da entropia

UNESP

2010

Brandão, Camila.

Ensaios sobre computação e informação quânticas: fundamentação e simulações sobre o efeito da entropia / Camila Brandão. - São José do Rio Preto: [s.n.], 2010.

106 f. : il. ; 30 cm.

Orientador: Manoel Ferreira Borges Neto

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas

1. Mecânica quântica. 2. Computação quântica. 3. Informação quântica. 4. Criptografia. 5. Entropia de Tsallis. 6. Entropia de Von Neumann. I. Borges Neto, Manoel Ferreira. II. Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU - 530.145

Ficha catalográfica elaborada pela Biblioteca do IBILCE
Campus de São José do Rio Preto - UNESP

Camila Brandão

Ensaios sobre computação e informação quânticas: fundamentação e simulações sobre o efeito da entropia

Orientador: Prof. Dr. Manoel Ferreira Borges Neto

Dissertação apresentada para obtenção do título de Mestre em Ciência da Computação, área de Computação Científica junto ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

UNESP

2010

CAMILA BRANDÃO

Ensaios sobre computação e informação quânticas: fundamentação e simulações sobre o efeito da entropia

Dissertação apresentada para obtenção do título de Mestre em Ciência da Computação, área de Computação Científica junto ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

BANCA EXAMINADORA

Prof. Dr. Manoel Ferreira Borges Neto
Professor Titular
UNESP - São José do Rio Preto
Orientador

Prof. Dr. Waldir Leite Roque
Professor Associado II
Universidade Federal do Rio Grande do Sul

Prof. Dr. José Márcio Machado
Professor Adjunto
UNESP - São José do Rio Preto

São José do Rio Preto, 30 de Abril de 2010.

"Para descobrir todos os
fenômenos que deseja,
basta ao sábio três coisas:
pensar, pensar, pensar."
Isaac Newton

A Deus e aos meus pais,
pelo apoio de sempre.
Dedico

AGRADECIMENTOS

A Deus, por guiar e iluminar meu caminho.

Ao Prof. Manoel Borges, pela sabedoria, atenção, presteza e paciência.

Aos meus estimados pais Nestor e Silvia, por tudo que fazem por mim, e pelo apoio nas horas mais difíceis.

Ao meu namorado, Ricardo Fantozzi, pelo carinho, paciência e compreensão.

E ao meu irmão Neto e minha cunhada Adriana, pelas risadas nos finais de semana e pela Nina claro!

Aos meus amigos, companheiros e todos aqueles que contribuiram direta ou indiretamente para a realização deste trabalho, em especial Adriana F. Roberto Ártico, Cleiton Nobuo Akaike, Rafael Henrique Moretti e Tiago A. Dócusse.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Nesta dissertação, além da apresentação de um ensaio teórico sobre a fundamentação da Mecânica Quântica, Computação, Informação Quântica, Criptografia e Entropias Quânticas, serão mostradas, de forma inédita, algumas implementações sobre o efeito da Entropia no Emaranhamento Quântico, importante para processos de transmissão da Informação Quântica, com o uso dos programas Mathematica e Matlab. Primeiramente é apresentado um breve histórico sobre a Computação Quântica e a Informação Quântica, junto com uma perspectiva do futuro. Logo em seguida uma breve introdução sobre a Mecânica Quântica, com o estudo de autovetores e autovalores e seus postulados, produtos tensoriais e o micro-universo. Na seqüência um texto sucinto com os conceitos fundamentais da Computação Quântica como os bits quânticos, e portas lógicas. Além dos principais algoritmos quânticos. Depois passa-se a estudar a Informação Quântica, as operações quânticas, canais de inversão e polarização, para então chegar-se a Entropia, quando é feito um estudo comparativo entre as entropias de Von Neumann e Tsallis. E por fim um pouco de Criptografia Quântica.

Palavras-chave: Mecânica Quântica, Computação Quântica, Informação Quântica, Criptografia, Entropia de Tsallis, Entropia de Von Neumann.

Abstract

In this dissertation, beyond the presentation of a theoretical essay on the basis of the Quantum Mechanics, Computation, Quantum information, Quantum Criptografy and Entropies, it will also be shown, for first time, some implementations on the effect of the Entropy tests on Quantum Entanglement for processes of transmission of Quantum Information, through the uses Mathematica and Matlab Programs. First I present a historical briefing on the Quantum Computation and Quantum Information, together with a perspective of the future. Afterwards it will shown on introduction on the Quantum Mechanics, and its postulates, and the micro-universe. In sequence, a brief text with the fundamental concepts of the Quantum Computation, as the quantum bits, logic gates, and the main quantum algorithms. Later we will start to study Quantum Information, the quantum operations, channels of inversion and polarization. Furthermore we will go to discuss Entropy, where it is made a comparative study of Entropies of Von Neumann and Tsallis. And finally a little of Quantum Criptografy will be worked out.

Keywords: *Quantum mechanics, Quantum Computation, Quantum Information, Criptografy, Entropy of Tsallis, Entropy of Von Neumann.*

Capítulo 1

Introdução

Nos dias atuais tem-se dado muita importância ao aperfeiçoamento dos computadores, que vem se tornando cada vez menores e mais velozes. De acordo com Gordon Moore esse avanço acontece a cada 18 meses, mas com o aumento de transistores em um circuito integrado. Porém, com o aumento da quantidade de transistores deve-se diminuir o tamanho dos mesmos, e a previsão é que cada bit de informação seja representado em um átomo. Como aumentar a capacidade dos computadores? Devido a isso é que vários estudos vem sendo realizados, principalmente nas áreas de tecnologia quântica.

Os computadores quânticos são muito mais rápidos que os computadores clássicos, por aproveitar de propriedades que caracterizam sistemas microscópicos como a superposição de estados, paralelismo quântico e o emaranhamento quântico, mas ainda se encontra em desenvolvimento.

Porém, com a evolução dos computadores novos sistemas criptográficos baseados na Teoria Quântica deverão ser usados para proteger informações, visto que se trata de uma teoria completa e complexa, que explica fenômenos que acontecem tanto em escala macroscópica quanto microscópica, um mundo que viola nossa intuição, onde um elétron pode estar em dois lugares ao mesmo tempo, um núcleo atômico pode girar em sentido horário e anti-horário ao mesmo tempo, e a matéria se dissolve num borrão fantasmagórico (31) chamado de emaranhamento quântico.

Esses emaranhamentos são importantíssimos no desenvolvimento da informação quântica, permitindo o aumento da capacidade de transporte de informações e melhor eficiência (5), pode ser a chave para a segurança na comunicação, através da criptografia quântica (6).

Estudaremos neste a quantificação do grau de emaranhamento para campos de entrada

que estão nos "estados de Fock", para isso é necessário o uso de uma "medida"de pureza, e tal medida será feita através da entropia. A entropia clássica de Boltzmann, tem sua equivalente quântica conhecida como entropia de Von Neumann (7) que associada com o estado quântico de um sistema descrito pelo operador densidade ρ é

$$S(\rho) \equiv -Tr[\rho\, ln\, \rho]$$

e em 1988 uma generalização foi proposta por Tsallis (8)

$$S_q(\rho) \equiv -\frac{1 - Tr[\rho^q]}{1 - q}$$

e vem sendo aplicada com sucesso em vários problemas como na analise da radiação do corpo negro (9).

Com as entropias de Von Neumann e Tsallis faremos uma comparação do grau de emaranhamento, verificando qual das duas oferece melhor desenvoltura, e para tal comparação faremos uso dos aplicativos Mathematica ® e Matlab ®.

1.1 Objetivos

Temos como objetivo explorar outros casos de informação quântica, estudados inicialmente em (12) e (18), ampliando as comparações entre as entropias de Tsallis e Von Neumann na transmissão da Informação, com um programa mais abrangente e comparar dois programas em linguagens diferentes.

1.2 Descrição dos capítulos

Objetivando clareza na exposição dos assuntos, dividimos este trabalho em 9 capítulos.

O primeiro capítulo é dedicado para a introdução. Nesta parte é apresentado um breve esboço da evolução histórica e os objetivos do trabalho.

No segundo capítulo, sucintamente, é exposto alguns conceitos principais da teoria da Mecânica Quântica, introduzindo os colchetes de Poisson, um pouco sobre fótons e elétrons, o espaço de Hilbert e a notação de Dirac, operadores, ket's, bra's, postulados, dentre outros tópicos.

O terceiro capítulo é dedicado a informação quântica, onde falaremos dos *qubits*, que são os bits quânticos.

O quarto capítulo fica reservado à Computação Quântica, as principais portas lógicas e suas representações.

Em seguida, no quinto capítulo, primeiramente, é feita uma introdução a entropia, e às entropias de Von Neumann e Tsallis, com suas respectivas definições e propriedades, e em seguida, uma introdução ao emaranhamento.

O sexto capítulo é feita a análise comparativa entre as entropias de Von Neumann e Tsallis, e conjuntamente são apresentados os resultados obtidos nos testes com o uso do Matlab® e Mathematica®.

No capítulo 7, faz-se uma introdução aos algoritmos quânticos em especial o algoritmo de Shor, usado na fatoração de grandes números inteiros, e na Criptografia RSA.

O oitavo capítulo é dedicado a Criptografia, com um pouco da sua história, exemplos de criptografia, seguidos pela criptografia clássica com a distribuição de chave secreta e a criptografia RSA com o uso da chave pública, finalizando com a Criptografia Quântica ou Distribuição Quântica de Chaves.

O capítulo 9 é deixado para as conclusões do trabalho juntamente com apresentação de sugestões para trabalhos futuros.

Nos apêndices A e B encontra-se uma das simulações, executadas no Matlab® e no Mathematica®, respectivamente e utilizados na realização deste trabalho, para a obtenção dos gráficos comparativos entre as Entropias de Von Neumann e Tsallis.

Capítulo 2

Fundamentos Matemáticos da Mecânica Quântica

A mecânica quântica é o ramo da física que estuda os fenômenos atômicos e sub-atômicos, além da repercussão destes fenômenos a nível macroscópico. Por se tratar de algo que não faz parte de nossas noções intuitivas, como os fenômenos clássicos, a Mecânica Quântica pode a princípio não ser tão facilmente interpretável. Neste capítulo estudam-se as propriedades básicas, princípios, peculiaridades e aplicações da Mecânica Quântica. (7) (15) (16) (17)

2.1 Introdução - Os colchetes de Poisson

Na passagem ou transição da Teoria Clássica para a Teoria Quântica, os colchetes de Poisson tiveram um papel fundamental. Os colchetes de Poisson são construções matemáticas definidas numa "variedade"(por exemplo o espaço de fase). Em geral se X e Y forem duas variáveis dinâmicas e q e p coordenadas generalizadas que os momentam, respectivamente. Os colchetes de Poisson são definidos como sendo:

$$[X,Y]_{q,p} = \sum_i \left(\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i} \right) \tag{2.1}$$

Os colchetes de Poisson possuem as seguintes propriedades

$$\begin{cases} i)\,[X,X]=0 \\ ii)\,[X,Y]=-\,[Y,X] \\ iii)\,[X,Y+Z]=[X,Y]+[X+Z] \\ iv)\,[X,YZ]=Y\,[X,Z]+[X,Y]\,Z \end{cases} \tag{2.2}$$

Demonstração: [X,X]= 0

$$[X,X]=\sum_i(\frac{\partial X}{\partial q_i}\frac{\partial X}{\partial p_i}-\frac{\partial X}{\partial p_i}\frac{\partial X}{\partial q_i})=\sum_i(\frac{\partial X}{\partial q_i}(1\frac{\partial X}{\partial p_i}-\frac{\partial X}{\partial p_i}1))=\sum_i(\frac{\partial X}{\partial q_i}(\frac{\partial X}{\partial p_i}-\frac{\partial X}{\partial p_i}))=$$

$$=\sum_i(\frac{\partial X}{\partial q_i}\underbrace{(\frac{\partial X}{\partial p_i}-\frac{\partial X}{\partial p_i})}_{0})=\sum_i(\frac{\partial X}{\partial q_i}.0)=0$$

Demonstração: [X,Y]=-[Y,X]

$$[X,Y]=\sum_i(\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i}-\frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i})=-\sum_i(\frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i}-\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i})=$$

$$=-\sum_i(\frac{\partial Y}{\partial q_i}\frac{\partial X}{\partial p_i}-\frac{\partial Y}{\partial p_i}\frac{\partial X}{\partial q_i})=-[Y,X]$$

Demonstração: [X,Y+Z]=[X,Y]+[X,Z]

$$[X,Y+Z]=\sum_i(\frac{\partial X}{\partial q_i}\frac{\partial(Y+Z)}{\partial p_i}-\frac{\partial X}{\partial p_i}\frac{\partial(Y+Z)}{\partial q_i})=$$

$$=\sum_i(\frac{\partial X}{\partial q_i}(\frac{\partial Y}{\partial p_i}+\frac{\partial Z}{\partial p_i})-\frac{\partial X}{\partial p_i}(\frac{\partial Y}{\partial q_i}+\frac{\partial Z}{\partial q_i}))=$$

$$=\sum_i(\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i}+\frac{\partial X}{\partial q_i}\frac{\partial Z}{\partial p_i}-\frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i}-\frac{\partial X}{\partial p_i}\frac{\partial Z}{\partial q_i})=$$

$$=\sum_i(\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i}-\frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i}+\frac{\partial X}{\partial q_i}\frac{\partial Z}{\partial p_i}-\frac{\partial X}{\partial p_i}\frac{\partial Z}{\partial q_i})=$$

$$= \sum_i (\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i}) + \sum_i (\frac{\partial X}{\partial q_i}\frac{\partial Z}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Z}{\partial q_i}) = [X,Y] + [X,Z]$$

Demonstração: [X,YZ]=Y[X,Z]+[X,Y]Z

$$[X,YZ] = \sum_i (\frac{\partial X}{\partial q_i}\frac{\partial (YZ)}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial (YZ)}{\partial q_i}) =$$

$$= \sum_i (\frac{\partial X}{\partial q_i}(\frac{\partial Y}{\partial p_i}Z + Y\frac{\partial Z}{\partial p_i}) - \frac{\partial X}{\partial p_i}(\frac{\partial Y}{\partial q_i}Z + Y\frac{\partial Z}{\partial q_i})) =$$

$$= \sum_i (Y(\frac{\partial X}{\partial q_i}\frac{\partial Z}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Z}{\partial q_i}) + (\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i})Z) =$$

$$= \sum_i Y(\frac{\partial X}{\partial q_i}\frac{\partial Z}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Z}{\partial q_i}) + \sum_i (\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i})Z =$$

$$= Y\sum_i (\frac{\partial X}{\partial q_i}\frac{\partial Z}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Z}{\partial q_i}) + \sum_i (\frac{\partial X}{\partial q_i}\frac{\partial Y}{\partial p_i} - \frac{\partial X}{\partial p_i}\frac{\partial Y}{\partial q_i})Z = Y[X,Z] + [X,Y]Z$$

É possível mostrar também que se:

$$\begin{cases} X = q_i \\ Y = q_j \end{cases} \Rightarrow [q_i, q_j]_{q,p} = 0 \tag{2.3}$$

$$\begin{cases} X = p_i \\ Y = p_j \end{cases} \Rightarrow [p_i, p_j] = 0 \tag{2.4}$$

$$\begin{cases} X = q_i \\ Y = p_j \end{cases} \Rightarrow [q_i, p_j]_{q,p} = \delta_{ij} \tag{2.5}$$

Com $\delta_{ij} = \begin{cases} 0, & \text{se} \quad i \neq j; \\ 1, & \text{se} \quad i = j. \end{cases}$ (Delta de Kronecker)

Demonstração: (2.3)

$$[q_i, q_j] = \sum_j (\frac{\partial q_i}{\partial q_j}\frac{\partial q_j}{\partial p_j} - \frac{\partial q_i}{\partial p_j}\frac{\partial q_j}{\partial q_j}) = 0$$

Pois os $q_i^{'}s$ e os $p_i^{'}s$ são independentes, logo resulta que:

$$\frac{\partial q_j}{\partial p_j} = 0 = \frac{\partial q_i}{\partial p_j}; \qquad \frac{\partial q_j}{\partial q_j} = 1;$$

e

$$\frac{\partial q_i}{\partial q_j} = \delta_{ij}, \qquad \text{onde:} \begin{cases} \delta_{ij} = 0; & \text{se} \quad i \neq j \\ \delta_{ij} = 1; & \text{se} \quad i = j \end{cases}$$

Demonstração: (2.4)

$$[p_i, p_j] = \sum_j (\frac{\partial p_i}{\partial q_j}\frac{\partial p_j}{\partial p_j} - \frac{\partial p_i}{\partial p_j}\frac{\partial p_j}{\partial q_j}) = 0$$

Já que $q_i^{'}s$ e os $p_i^{'}s$ são independentes, temos:

$$\frac{\partial p_i}{\partial q_j} = 0 = \frac{\partial p_j}{\partial q_j}; \qquad \frac{\partial p_j}{\partial p_j} = 1;$$

e

$$\frac{\partial p_i}{\partial p_j} = \delta_{ij}, \qquad \text{onde:} \begin{cases} \delta_{ij} = 0; & \text{se} \quad i \neq j \\ \delta_{ij} = 1; & \text{se} \quad i = j \end{cases}$$

Demonstração: (2.5)

$$[q_i, p_j] = \sum_j (\frac{\partial q_i}{\partial q_j}\frac{\partial p_j}{\partial p_j} - \frac{\partial q_i}{\partial p_j}\frac{\partial p_j}{\partial q_j}) = \delta_{ij}$$

pois:

$$\frac{\partial q_i}{\partial p_j} = 0 = \frac{\partial p_j}{\partial q_j}; \qquad \frac{\partial p_j}{\partial p_j} = 1;$$

e

$$\frac{\partial q_i}{\partial q_j} = \delta_{ij}, \qquad \text{onde:} \begin{cases} \delta_{ij} = 0; & \text{se} \quad i \neq j \\ \delta_{ij} = 1; & \text{se} \quad i = j \end{cases}$$

Além disso, podemos observar que $[q_i, p_j] = -[p_j, q_i]$

$$[q_i, p_j] = \sum_j (\frac{\partial q_i}{\partial q_j}\frac{\partial p_j}{\partial p_j} - \frac{\partial q_i}{\partial p_j}\frac{\partial p_j}{\partial q_j}) = -\sum_j (\frac{\partial q_i}{\partial p_j}\frac{\partial p_j}{\partial q_j} - \frac{\partial q_i}{\partial q_j}\frac{\partial p_j}{\partial p_j}) =$$

$$= -\sum_j (\frac{\partial p_j}{\partial q_j}\frac{\partial q_i}{\partial p_j} - \frac{\partial p_j}{\partial p_j}\frac{\partial q_i}{\partial q_j}) = -[p_j, q_i] \tag{2.6}$$

e

$$-[p_j, q_i] = \delta_{ij}, \qquad \text{onde:} \quad \begin{cases} \delta_{ij} = 0; & \text{se} \quad i \neq j \\ \delta_{ij} = 1; & \text{se} \quad i = j \end{cases}$$

Os colchetes de Poisson são invariantes em relação a transformações de coordenadas do tipo canônicas

$$\begin{cases} q_i' = q_i'(q_1, q_2, ..., q_n, p_1, p_2, ..., p_n, t) \\ p_i' = p_i'(q_1, q_2, ..., q_n, p_1, p_2, ..., p_n, t) \end{cases} \tag{2.7}$$

o que significa que:

$$[X, Y]_{q,p} = [X, Y]_{q',p'} \tag{2.8}$$

Colchetes de Poisson e os Comutadores nos levam ao Princípio da Incerteza, pois de acordo com as propriedades básicas, segue que:

$$\begin{cases} [X, YZ] = Y[X, Z] + [X, Y]Z \\ \quad \text{e} \\ [XY, Z] = [-Z, XY] = X[(-Z), Y] + [(-Z), X]Y = X[Y, Z] + [X, Z]Y \end{cases} \tag{2.9}$$

De (2.9) vem que para quatro variáveis quaisquer X, Y, Z, W:

$$[WX, YZ] = W[X, YZ] + [W, YZ]X = WY[X, Z] + W[X, Y]Z + Y[W, Z]X + [W, Y]ZX \tag{2.10}$$

Podemos também desenvolver (2.10) de outra forma:

$$[WX, YZ] = [WX, Y]Z + Y[WX, Z] = W[X, Y]Z + [W, Y]XZ + YW[X, Z] + Y[W, Z]X \tag{2.11}$$

Combinando (2.10) e (2.11), obtém-se que: (-)

$$(WY - YW)[X, Z] = [W, Y](XZ - ZX) \tag{2.12}$$

Uma solução trivial para (2.12), seria WY=YW e XZ=ZX. Mas, em geral, não é dito que [A, B] comute como no caso do espaço de fases da Mecânica Quântica. Se as variáveis W, X, Y, Z forem supostamente arbitrárias, segue-se que a identidade (2.12) é satisfeita somente se, para quaisquer A e B:

$$(AB - BA) \equiv \alpha[A, B] \tag{2.13}$$

Se o resultado (2.13) for introduzido em (2.12).

$$\alpha[W, Y].[X, Z] = \alpha[W, Y][X, Z] \tag{2.14}$$

Supondo em (2.13) que q_i e p_i representam as variáveis, então:

$$(q_i p_j - p_j q_i) = \alpha\delta_{ij}, \tag{2.15}$$

pois: lembre-se que $[p_j, q_i] = \delta_{ij}$, então temos que

$$(q_i p_i - p_i q_i) = \alpha \tag{2.16}$$

O colchete $[q_i, p_i]$ é invariante por transformações canônicas de coordenadas. Portanto, consideremos que $[p'_i, q'_i] = [p_i, q_i]$ e $[p'_i, q'_i] \equiv [p_i + \Delta p_i, q_i + \Delta q_i]$.

$$\begin{aligned} &\alpha = (p_i + \Delta p_i)(q_i + \Delta q_i) - (q_i + \Delta q_i)(p_i + \Delta p_i) = \\ &p_i q_i + p_i \Delta q_i + \Delta p_i q_i + \Delta p_i \Delta q_i - (q_i p_i + q_i \Delta P_i + \Delta q_i p_i + \Delta q_i \Delta p_i) \end{aligned} \tag{2.17}$$

Se considerarmos em (2.17) que $p_i = q_i = 0$, então:

$$\Delta p_i \Delta q_i - \Delta q_i \Delta p_i = \alpha \tag{2.18}$$

Se introduzirmos agora o postulado adicional da anti-comutatividade, ou seja:

$$\Delta p_i \Delta q_i = -\Delta q_i \Delta p_i \Rightarrow \Delta p_i \Delta q_i = \frac{\alpha}{2} \tag{2.19}$$

É conhecido como o "Princípio da Incerteza de Heisenberg"quando α é muito pequeno ($\sim 10^{-27}$).

Ou ainda, sejam A, B variáveis dinâmicas $\Rightarrow (AB - BA) \equiv \alpha[A, B]$
Se A, B estão associadas às variáveis dinâmicas q'_i e p'_i (lembre-se que: $[p'_i, q'_j] = \delta_{ij}$)$\Rightarrow$ $(q'_i p'_i - p'_i q'_i) = \alpha$ (constante). Portanto $[q'_i, p'_i] = \alpha$

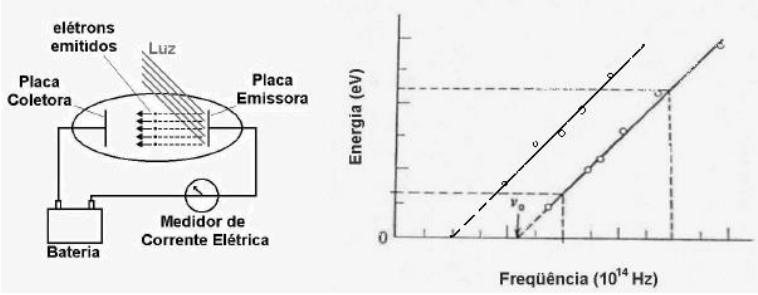


Figura 2.1: *Efeito Fotoelétrico: Energia do elétron liberado* $\times$ *freqüência do fóton incidente*

Estudemos brevemente, agora, o Efeito fotoelétrico (Einstein e Planck):

É um dos experimentos de difícil explicação na física clássica, assim como o da difração e interferência da luz (dualidade onda-particula). Na versão de Einstein e Planck, o efeito fotoelétrico (luz é partícula e não onda) é tal que, as inclinações das retas de cobre e silício, como mostrado na Figura 2.1 eram sempre as mesmas. Calculando-as chegou-se ao valor de $h \sim 10^{-34}$.

$$\begin{cases} \nu \Rightarrow & \text{freqüência da luz incidente;} \\ h\nu \Rightarrow & \text{energia da luz incidente;} \\ h\nu_o \Rightarrow & \text{energia gasta pelo elétron para se libertar do átomo.} \\ m \Rightarrow & \text{massa do elétron;} \end{cases}$$

$$h\nu = h\nu_o + \frac{1}{2}mv^2$$

Onde: $\frac{1}{2}mv^2$ corresponde a energia do elétron liberado.

Einstein: Energia do fóton (total) $= Pc$ (c: velocidade da luz)

Mas $E = h\nu \Rightarrow \dfrac{h\nu}{c} = P \Rightarrow h = P\dfrac{c}{\nu} = P\lambda$

Faça $\lambda = q_i$ (λ: comprimento de onda).

$$\begin{gathered} [p_i', q_i'] = [p_i + \Delta p_i, q_i + \Delta q_i] \Rightarrow \\ \alpha = (p_i + \Delta p_i)(q_i + \Delta q_i) - (q_i + \Delta q_i)(p_i + \Delta p_i) = \\ p_i q_i + p_i \Delta q_i + \Delta p_i q_i + \Delta p_i \Delta q_i - (q_i p_i + q_i \Delta p_i + \Delta q_i p_i + \Delta q_i \Delta p_i) = \alpha \end{gathered} \tag{2.20}$$

Considerando: $p_i = q_i = 0 \Rightarrow \Delta p_i \Delta q_i - \Delta q_i \Delta p_i = \alpha$

Com o postulado adicional da anti-comutatividade:

$$\Delta p_i \Delta q_i = -\Delta q_i \Delta p_i \Rightarrow \Delta p_i \Delta q_i = \frac{\alpha}{2}$$

Fazendo: $\alpha = \frac{ih}{\pi}$ temos:

$$\Delta p \Delta q = \frac{ih}{2\pi} = \hbar$$

Conhecido como o Princípio da Incerteza de Heisenberg, que nos garante não ser possível determinar em simultâneo todos os estados físicos de uma partícula sem interferir na mesma, alterando-a de forma inegável.

Já a experiência de Huygens sobre "difração e interferência da luz", que comprova o caráter ondulatório da luz, ou suas características duais, de que a luz ou é uma partícula ou é uma onda nos mostra a Figura 2.2, ganhou grande simpatia na comunidade da física, pois a difração também foi observada ao final do século XIX para os elétrons.

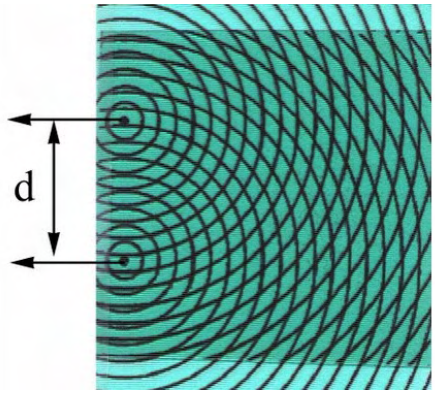


Figura 2.2: *Difração luminosa e interferências*

2.2 Elétrons

Os elétrons são importantíssimos na constituição atômica.

$$\begin{cases} Carga : e \approx -1,6 * 10^{-19} coulombs \\ Massa : m \approx 9,1 * 10^{-28} coulombs \end{cases}$$

A energia E do elétron é relacionada ao momentum P por

$$E = \frac{P^2}{2m} \tag{2.21}$$

(lembre-se que $E_c = \frac{1}{2}mv^2$ e que $P = mv$)

$E \ll mc^2$: equações não relativistas, que se obtém quando as velocidades envolvidas são muito menores que a velocidade da luz $= c$ (20).

Quando as velocidades não são tão pequenas em relação a c, como por exemplo as velocidades com as quais os elétrons "escapam"dos átomos, então 2.21 se transforma em

$$E = c[P^2 + (mc)^2]^{1/2} \tag{2.22}$$

Equação Relativista (Einstein).

De (2.21) e (2.22)

$$v = \frac{P}{m} \tag{2.23}$$

com $(v \ll c)$

$$\frac{v}{\left(1 - \frac{v^2}{c^2}\right)^{1/2}} = \frac{P}{m} \tag{2.24}$$

De (2.23) e (2.24) mostram como se comporta a velocidade dos elétrons em termos relativísticos e não relativísticos. Mas elétrons também podem ser refletidos sob a influência de campos elétricos e magnéticos, por turbulência ou em laboratórios.

A deflexão é computada usando a conhecida "Força de Lorentz"

$$F = c[E + \frac{v * H}{c}] \tag{2.25}$$

onde

$$\begin{cases} E: & \text{campo elétrico;} \\ H: & \text{campo magnético} \end{cases}$$

2.3 Fótons

Fótons podem ser interpretados como constituintes elementares da radiação. Eles se movem com velocidade da luz, e quando interagem com a matéria (elétrons, átomos, etc) eles transferem quantidades de momento e energia. A relação entre o momento e a energia do fóton é dada por:

$$E = cP \tag{2.26}$$

Observe que (2.26) é obtida através de (2.22) fazendo $m = 0$. Portanto o fóton tem massa de repouso igual a zero. Como vimos anteriormente, a energia do fóton pode estar

associada a frequência da luz (dualidade onda-partícula), então $E = h\nu$, onde h é a constante de Planck. Usando (2.26), e $\lambda\nu = c$, com λ o comprimento de onda temos

$$P = \frac{E}{c} = \frac{h\nu}{c} = \frac{h}{\lambda} \tag{2.27}$$

Observe que os valores de E e P são discretos, visto que λ e ν não ocorrem em todos os valores pois cada fóton está associado a uma frequência ν.

2.4 As relações de De Broglie

Elétrons, fótons e todas partículas elementares produzem efeitos como interferência e difração.

Difração de onda $\rightsquigarrow$ associada ao $\rightsquigarrow$ momentum do feixe de fótons incidentes

Temos

$$\lambda = \frac{h}{P} \tag{2.28}$$

e

$$v = \frac{E}{h} \tag{2.29}$$

As equações (2.28) e (2.29) conectam as "Propriedades de Partículas"(P, E) com as "Propriedades de Onda"(λ, v). As relações (2.28) e (2.29) são conhecidas como "Relações de De Broglie". De Broglie sugeriu suas relações e consequentemente as propriedades de onda também para o elétron em 1924 e estas foram confirmadas experimentalmente em 1927. Observe que em (2.28) a medida que a massa e/ou a velocidade aumenta - no caso não relativístico $P = mv$ -, diminui consideravelmente o comprimento de onda. Os corpos macroscópicos têm associados uma onda, porém a massa é tão grande que se pode afirmar que apresentam um comprimento de onda desprezível, porém não nulo (46), (47) e (48).

2.5 Difração de Elétrons

O mais contundente fenômeno do micro universo é o da dualidade onda-partícula. O experimento da difração/interferência de elétrons é um dos casos mais marcantes, que mostram as limitações da física clássica.

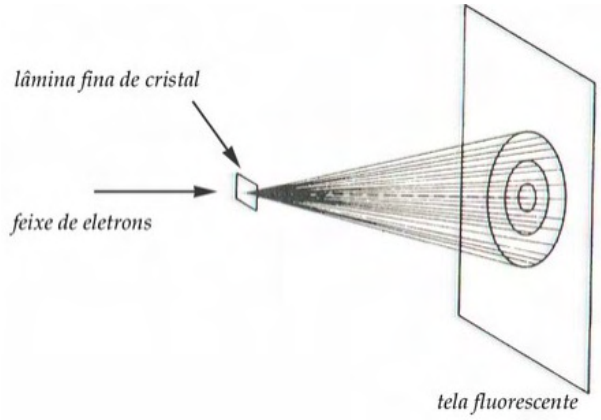


Figura 2.3: *Difração de Elétrons - Experiência de Gemer e Thonson*

Entre o feixe de elétrons e a lâmina de cristal podem existir placas de aceleração de elétrons, e o resultado da tela fluorescente é exemplificado na Figura (2.4).

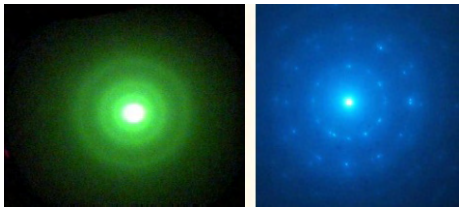


Figura 2.4: *Placas Fotográficas resultantes da Experiência de Gemer e Thomson*

Gemer (47) e Thomson (48) observaram que o padrão da fotografia independe da intensidade do feixe, caso o número de elétrons emitidos por segundo é cortado por uma fração f, e o tempo de exposição da placa é aumentado em f^{-1}. O padrão de interferência produzido na placa é idêntico, além disso o padrão é mantido se ao invés de elétrons houver emissão de Raio X.

O padrão de interferência da figura produzida só se altera dependendo da estrutura do cristal empregado no experimento, observe na figura que há máximos e mínimos indicando que há "uma probabilidade maior dos elétrons se agruparem nos pontos claros".

2.6 O Princípio de Heisenberg

Assuma que a relação:

$$\triangle P \triangle X \gtrsim h \tag{2.30}$$

é uma Lei da Natureza, ou seja, as leis da física nos dizem que é impossível saber o momento e posição de um elétron com incerteza menor. Examinando a difração dos

elétrons é útil observar as posições de cada elétron, individualmente, aparece na tela da placa durante o processo de difração, com não previsibilidade. Contudo, e esse é o ponto crucial da nossa consideração, o padrão da distribuição da posição dos elétrons no detector, ou seja, o "Padrão de Difração", pode ser previsto.

A qualquer tempo e em diferentes lugares, um feixe de elétrons com momento bem definido, ao incidir num cristal, produz a mesma distribuição na placa do detector, ou seja, o mesmo padrão de figura de interferência. É claro que não é possível predizer a localização de um único elétron, mas é possível a distibuição da posição na placa de um grande número de elétrons.

Como conseqüência da experiência de Gemer (47) e Thomson (48) temos que a teoria dos processos microfísicos parece ter um caráter estatístico/probabilístico. Em geral, propriedades estatísticas, ao invés de propriedades de entidades isoladas são as propriedades determinadas no micro universo. Na verdade não é um simples elétron que possui a propriedade de onda, ou seja, não é um elétron único com momento definido que é similar a uma onda, mas um grande número de elétrons, todos com um momento bem definido (47), (48).

Para exemplificar este fato temos o seguinte exemplo: Um neutron livre se transforma espontaneamente em um próton com a emissão de um elétron e um neutrino. Diz-se que a meia-vida de um neutron é de 12 minutos. Esta proposição não é válida para neutrons individuais, mas sim para um agrupamento de neutrons. Se por exemplo, tivéssemos um conjunto de neutrons em repouso, alguns se transformariam após um minuto, enquanto outros demorariam pelo menos uma hora. Nós não podemos predizer precisamente quando um neutron isolado se trasformará num próton, mas metade do conjunto se transformará em 12 minutos. O termo vida média é uma propriedade de agrupamento.

Neste momento, algumas observações são relevantes, tais como: Mesmo na chamada física clássica (Newton, Lagrange, Hamilton) muitas vezes por razões práticas, não é possível obter ao mesmo tempo a posição e o momentum de todos os componentes de um dado sistema. Por exemplo, um gás composto por 10^9 moléculas. No mundo clássico, embora, por razões práticas, seja impossível de obter algumas relações, no entanto relações de propriedades estatísticas como a pressão e a temperatura são obtidas. É importante assinalar que pressão e temperatura, por exemplo, não são propriedades individuais, mas propriedades de todo o conjunto de elementos considerado.

Um certo cuidado é necessário ao tratar elétrons como partículas ao incidir no cristal devido ao fato de que eles deveriam ser tratados como ondas. O único elétron parece percorrer ao mesmo tempo os orifícios do cristal, a que se explica apenas pelo caráter dual, e não apenas de partícula. A interferência, além da difração é uma característica do elétron onda.

2.7 Espaço de Hilbert e Notação de Dirac

Definição: Espaço L^P

Seja (Ω, Σ, μ) um espaço topológico Ω, com medida μ e uma álgebra Σ. Seja ainda P um real fixo, $P \geqslant 1$. Definimos $L^P = L^P(\Omega, d\mu)$ pelo conjunto de todas as funções mensuráveis $f : \Omega \to C$ tal que $|f|^P \in L^1$, e para $f \in L^P$, define-se a norma de f como sendo:

$$\|f\|_P = (\int |f|^P du)^{\frac{1}{P}} \tag{2.31}$$

Que satisfaz as propriedades:

i) $\|\lambda f\|_P = \|\lambda\|\|f\|_P$;

ii) $\|f + g\|_P \leqslant \|f\|_P + \|g\|_P$;

iii) $\|f\|_P = 0$ se $f(x) = 0$, $\forall x$.

Demonstração:

Primeiramente, a função $0 \leq \|f\|_P = (\int |f|^P d\mu)^{\frac{1}{P}} \leq \infty$ pois $|f|^P$ é integrável com respeito a μ.

i) $\|\lambda f\|_P = (\int |\lambda f|^P du)^{\frac{1}{P}} = \lambda(\int |f|^P du)^{\frac{1}{P}} = |\lambda|\|f\|_P$;

ii) $\|f + g\|_P \leqslant \|f\|_P + \|g\|_P$, pela desigualdade de Minkowiski;

iii) $\|f\|_P = 0 \Rightarrow |f(x)| = 0 \Rightarrow f(x) = 0$, $\forall x$.

Definição: Espaço Pré-Hilbertiano

Seja H um espaço vetorial sobre o corpo $\mathbb{C}$. Um produto interno em H é uma função $(,)$ definida em $H \times H$, e tomando valores em $\mathbb{C}$, satisfazendo as seguintes condições.
Para todos $x, y, z \in H$ e $\lambda \in \mathbb{C}$:

1. $(x, x) \geqslant 0$ e $(x, x) = 0 \Leftrightarrow x = 0$;

2. $(x + y, z) = (x, z) + (y, z)$;

3. $(\lambda x, y) = \lambda(x, y)$;

4. $(x, y) = \overline{(y, x)}$, lembrando que $\overline{a}$ representa o conjugado de a.

Um espaço vetorial provido de um produto interno chama-se Espaço Pré-Hilbertiano. Consequentemente, um espaço Pré-Hilbertiano satisfaz a seguinte propriedade:

$(x, y + z) = (x, y) + (x, z)$ e $(x, \lambda y) = \overline{\lambda}(x, y)$, para todo $x, y, z \in H$ e $\lambda \in \mathbb{C}$.

Proposição: Desigualdade Cauchy-Schwarz
Seja H um espaço Pré-Hilbertiano. Se $x, y \in H$, então:

$$|(x, y)|^2 \leqslant (x, x)(y, y)$$

Proposição: Espaço de Hilbert
A função $\|x\|$ dada por

$$\|x\| := (x, x)^{\frac{1}{2}}$$

definida para todo $x \in H$ é uma norma em H.

De fato: A única propriedade que requer alguma argumentação é que $\|x + y\| \leqslant \|x\| + \|y\|$ para todo $x, y \in H$, que segue diretamente da Desigualdade Cauchy-Schwarz.

$$\|x + y\|^2 = (x + y, x + y) = \|x\|^2 + 2Re(x, y) + \|y\|^2 \leqslant (\|x\| + \|y\|)^2 \tag{2.32}$$

Dizemos que H é um espaço de Hilbert, se o Espaço Pré-Hilbertiano H com a métrica definida por essa norma é completo.

Definição: Ortogonalidade
Um vetor x num espaço Pré-Hilbertiano H diz-se ortogonal a $y \in H$, e escrevemos $x \perp y$, se $(x, y) = 0$. Um subconjunto $S \subset H$ diz-se ortonormal se $(x, x) = 1$ e $(x, y) = 0$ para todos $x, y \in S$ com $x \neq y$.

Teorema: Pitágoras

Se $\{x_i\}_{i=1}^n$ é um conjunto ortogonal num espaço Pré-Hilbertiano H, então para todo $x \in H$, vale a seguinte relação

$$\|x\|^2 = \sum_{i=1}^{n} |(x, x_i)|^2 + \|x - \sum_{i=1}^{n} (x, x_i)x_i\|^2 \tag{2.33}$$

Demonstração:

Considere

$$x = \sum_{i=1}^{n} (x, x_i)x_i + x - \sum_{i=1}^{n} (x, x_i)x_i. \tag{2.34}$$

Afirmamos que $\sum_{i=1}^{n} (x, x_i)x_i$ e $x - \sum_{i=1}^{n} (x, x_i)x_i$ são ortogonais. De fato:

$$\left(\sum_{i=1}^{n} (x, x_i)x_i, x - \sum_{j=1}^{n} (x, x_j)x_j \right) = \sum_{i=1}^{n} |(x, x_i)|^2 - \sum_{i=1}^{n} \sum_{j=1}^{n} \overline{(x, x_i)}(x, x_j)(x_i, x_j) =$$

$$\sum_{i=1}^{n} |(x, x_i)|^2 - \sum_{i=1}^{n} \sum_{j=1}^{n} \overline{(x, x_i)}(x, x_j)\delta_{i,j} = \sum_{i=1}^{n} |(x, x_i)|^2 - \sum_{i=1}^{n} |(x, x_i)|^2 = 0 \tag{2.35}$$

Logo,

$$\|x\|^2 = \| \sum_{i=1}^{n} (x, x_i)x_i\|^2 + \|x - \sum_{i=1}^{n} (x, x_i)x_i\|^2 = \sum_{i=1}^{n} |(x, x_i)|^2 + \|x - \sum_{i=1}^{n} (x, x_i)x_i\|^2 \tag{2.36}$$

Corolário: Se $\{x_i\}_{i=1}^n$ é um conjunto ortonormal num espaço Pré-Hilbertiano H, então para todo $x \in H$.

$$\|x\|^2 \geqslant \sum_{i=1}^{n} |(x, x_i)|^2 \tag{2.37}$$

De fato, da proposição anterior temos

$$\|x\|^2 = \| \sum_{i=1}^{n} (x, x_i)x_i\|^2 + \|x - \sum_{i=1}^{n} (x, x_i)x_i\|^2 = \sum_{i=1}^{n} |(x, x_i)|^2 + \|x - \sum_{i=1}^{n} (x, x_i)x_i\|^2,$$

como a norma é um número real então de $a = b + c,\ a, b, c \in \mathbb{R} \Rightarrow a \geq b$ segue, diretamente, o resultado.

Dado um subconjunto S de um espaço Pré-Hilbertiano H, define-se como ortogonal de S:

$$S^{\perp} = \{x \in H : (x, y) = 0 \quad \forall y \in S\} \tag{2.38}$$

Definição: Bases Ortonormais

Dado um espaço de Hilbert H diz-se que um subconjunto S de H é uma base ortonormal de H se S não esta estritamente contido em nenhum outro conjunto ortonormal de H.

Uma observação a ser feita é que todo espaço de Hilbert tem uma base ortonormal, pois, pelo Lema de Zorn, todo espaço vetorial possui base. Logo, basta aplicar o procedimento de Gram-Schmidt e obter uma base ortonormal.

Teorema: Seja H um espaço de Hilbert e $\{e_\alpha\}_{\alpha\in I}$ uma base ortonormal. Então para cada $x \in H$ temos:

$$x = \sum_{\alpha\in I}(x, e_\alpha)_{e_\alpha} \quad \text{e} \quad \|x\|^2 = \sum_{\alpha\in I} |(x, e_\alpha)|^2 \tag{2.39}$$

Demonstração:

Seja $\{e_\alpha\}_{\alpha\in I}$, onde I é uma família de indíces, uma base ortonormal, então

$$x = \sum_{\alpha\in I}(x, e_\alpha)e_\alpha$$

Logo

$$(x, x) = \|x\|^2 = \sum_{\alpha\in I}\sum_{\beta\in I} \overline{(x, e_\alpha)}(x, e_\beta)(e_\alpha, e_\beta) = \sum_{\alpha\in I} |(x, e_\alpha)|^2 \tag{2.40}$$

pois $(e_\alpha, e_\beta) = \delta_{\alpha\beta}$.

2.8 Introdução à estrutura Matemática da Mecânica Quântica

Devido a dualidade onda-partícula é necessário rever alguns conceitos:

1. O conceito clássico de trajetória, deve ser substituído pelo conceito de estado variável com o tempo. O estado quântico de uma partícula, como um elétron, é caracterizado por uma função de onda $\psi(r, t)$, a qual contém toda informação possível de se obter da partícula.

2. $\psi(r, t)$ é interpretada como a amplitude de probabilidade da partícula. Desde que sejam contínuas as possíveis posições da partícula, a probabilidade $dP(r, t)$ de uma

partícula estar, no instante t, no elemento de volume $d^3r = dx\,dy\,dz$, situado em um ponto r deve ser proporcional a d^3r e portanto, infinitesimal.

$|\psi(r,t)|^2$ é interpretado com a correspondente densidade de probabilidade,

$$dP(r,t) = c|\psi(r,t)|^2 d^3r \tag{2.41}$$

onde c é chamada de constante de normalização.

Alguns comentários importantes:

Para um sistema composto de uma única partícula, a probabilidade total de se achar a partícula em algum lugar do espaço, num dado instante t, é igual a 1.

$$\int dP(r,t) = 1 \tag{2.42}$$

Como $dP(r,t)$ é dado por (2.41), conclui-se que a função de onda $\psi(r,t)$ deve ser quadrado integrável, ou seja, a integral dada por

$$\int |\psi(r,t)|^2 d^3r \tag{2.43}$$

é finita.

Portanto as funções $\psi(r,t)$ pertencem ao espaço de Hilbert. É evidente que o conjunto de funções contidas no espaço de Hilbert é extremamente extenso. No entanto, do ponto de vista físico, estamos interessados em uma família de funções que possuem certas propriedades. Vamos concentrar nossa atenção apenas em funções de onda $\psi(r,t)$ que são definidas em todos os pontos, contínuas e infinitamente diferenciáveis pois estabelecer que uma função é descontínua em um dado ponto não tem significado físico, desde que nenhum experimento nos permite acessar um fenômeno real em uma escala muito pequena devido ao Princípio da Incerteza.

Podemos também nos restringir a funções de onda que têm um domínio limitado (o que torna certo que a partícula pode ser encontrada em uma região finita do espaço, por exemplo dentro do laboratório).

Chamaremos de Γ o conjunto composto de funções de onda pertencentes de L^2, mas que sejam regulares, ou seja, (Γ é um subespaço de L^2).

2.9 Estrutura do Espaço Vetorial Γ das Funções de Onda

2.9.1 Produto escalar

Definição: Sejam $\varphi(r), \psi(r) \in \Gamma$, então o produto escalar de $\varphi(r)$ e $\psi(r)$, que denotaremos pelo número complexo (φ, ψ) é definido por:

$$(\varphi, \psi) = \int \varphi^*(r)\psi(r)d^3r, \tag{2.44}$$

Esta integral converge pois ψ e φ pertencem a Γ.

Tal definição implica nas seguintes propriedades:

1.

$$(\varphi, \psi) = (\psi, \varphi)^* \tag{2.45}$$

pois

$$(\varphi, \psi) = \int \varphi^*(r)\psi(r)d^3r = \int (\psi(r)^*\varphi(r))^* d^3r = (\psi, \varphi)^* \tag{2.46}$$

2.

$$(\varphi, \lambda_1\psi_1 + \lambda_2\psi_2) = \lambda_1(\varphi, \psi_1) + \lambda_2(\varphi, \psi_2) \tag{2.47}$$

Segue diretamente do fato que integral da soma é a soma das integrais.

3.

$$(\varphi, \lambda_1\psi_1 + \lambda_2\psi_2) = \lambda_1^*(\varphi_1, \psi) + \lambda_2^*(\varphi_2, \psi) \tag{2.48}$$

Segue diretamente das propriedades 1. e 2..

Tais propriedades implicam que o produto escalar é linear com respeito a segunda coordenada e anti-linear com respeito a primeira. Se $(\varphi, \psi) = 0$, então φ e ψ são chamados de ortogonais. A norma de $\psi \in \Gamma$ é definida por

$$(\|\psi\|^2 = (\psi, \psi)) = \int |\psi(r)|^2 d^3r. \tag{2.49}$$

2.9.2 Operador Linear

Definição: Um operador linear A, é por definição um ente matemático que associa a cada função $\phi(r) \in \Gamma$, outra função $\psi(r)$, tal que:

$$\psi(r) = A\varphi(r) \tag{2.50}$$

$$A[\lambda_1\varphi_1(r) + \lambda_2\varphi_2(r)] = \lambda_1 A\psi_1(r) + \lambda_2 A\psi_2(r) \tag{2.51}$$

Produto de Operadores: Sejam A e B dois operadores lineares.
O produto AB é definido como:

$$(AB)\psi(r) = A[B\psi(r)]; \tag{2.52}$$

Em geral, AB≠BA. Podemos definir o comutador de A e B como sendo operador $[A, B]$, definido por:

$$[A, B] = AB - BA \tag{2.53}$$

2.9.3 Base discreta ortonormal em Γ : $\{u_i(r)\}_i$

Definição: Consideremos que o conjunto de funções de Γ, com índice discreto $i = 1, 2, 3, ...$, $u_i(r) \in \Gamma$ seja uma base ortonormal de Γ. Logo, as observações seguintes são imediatas:

1. Se o conjunto $\{u_i(r)\}$ é ortonormal, então

$$(u_i, u_j) = \int u_i^*(r)u_j(r)d^3r = \delta_{ij} \tag{2.54}$$

2. Como $\{u_i(r)\}$ constitui uma base, por isso toda função $\psi(r) \in \Gamma$ pode ser expandida em uma única combinação dos elementos da base, ou seja, se

$$\psi(r) = \sum_i c_i u_i(r) \tag{2.55}$$

então,

$$c_i = (u_i, \psi(r)) = \int u_i^*(r)\psi(r)d^3r$$

2.10 Espaço de Estado - Notação de Dirac

Consideremos que a posição de um ponto no espaço pode ser descrito por um conjunto de 3 números (R^3), os quais são as coordenadas com respeito a um dado sistema de eixos bem definidos, cuja alteração do sistema de eixos, faz com que um outro conjunto de coordenadas passe a corresponder ao mesmo ponto. Contudo, o conceito geométrico de vetor, nos isenta da preocupação de mencionar um sistema de eixos específicos, e assim na Mecânica Quântica: cada estado quântico de uma partícula será caracterizado por um vetor de estado, pertencente a um estado abstrato, ξ_r, chamado de espaço de estados de uma partícula. Definem-se agora a notação e as regras da álgebra e cálculo vetorial em ξ_r.

2.10.1 O KET

Notação: Qualquer elemento, ou vetor, do espaço ξ_r, é chamado de KET. É representado pelo símbolo $|>$. Por exemplo $|\psi>$.

Como o conceito de função de onda é familiar, pode-se definir o espaço ξ_r dos estados de partícula pela associação com toda função $\psi(r)$ quadrado integrável, um vetor KET $|\psi>$ de ξ_r:

$$\psi(r) \in \Gamma \Leftrightarrow |\psi> \in \xi_r \tag{2.56}$$

2.10.2 O BRA

Por definição, um funcional linear χ, é uma operação linear que associa um número complexo a todo KET $|\psi>$, ou seja,

$$|\psi> \in \xi \Rightarrow \chi(|\psi>) \in \mathbb{C} \tag{2.57}$$

Pode ser mostrado que um conjunto de funcionais lineares definidas nos KETs $|\psi> \in \xi$, constitui um espaço vetorial, chamado de Espaço dual de ξ, e que será doravante simbolizado por ξ^*. Qualquer elemento do espaço ξ^* é chamado de vetor BRA, ou simplesmente BRA. É simbolizado por $<|$. Por exemplo o BRA $<\chi|$ designa o funcional linear χ. Logo, pode-se usar a notação: $<\chi|\psi>$, para denotar o número obtido da atuação do funcional linear $<\chi|$ no KET $|\psi>$, ou seja,

$$\chi(|\psi>) = <\chi|\psi>$$

2.10.3 O BRA KET

A existência de um produto escalar em ξ nos possibilita mostrar que pode-se associar, a todo KET $|\varphi>\in\xi$, um elemento de ξ^*, ou seja, um BRA que será representado por $<\varphi|$. O KET $|\varphi>$ nos possibilita definir um funcional linear, o qual associa (linearmente), com cada KET $|\psi>\in\xi$, um número complexo que é igual ao produto escalar $(|\varphi>,|\psi>)$ de $|\psi>$ por $|\varphi>$.

Seja $<\varphi|$ um funcional linear; portanto pode-se definir a relação:

$$<\varphi|\psi>=(|\varphi>,|\psi>) \tag{2.58}$$

No espaço ξ, o produto escalar é anti-linear com respeito ao primeiro vetor e na notação (2.58), pode-se dizer que:

$$\begin{aligned}&(\lambda_1|\varphi_1>+\lambda_2|\varphi_2>,|\psi>)=\lambda_1^*(|\varphi_1>,|\psi>)+\lambda_2^*(|\varphi_2>,|\psi>)=\\&\lambda_1^*<\varphi_1|\psi>+\lambda_2^*<\varphi_2|\psi>=(\lambda_1^*<\varphi_1|+\lambda_2^*<\varphi_2|)|\psi>\end{aligned} \tag{2.59}$$

Portanto:

$$\lambda_1|\varphi_1>+\lambda_2|\varphi_2>\Rightarrow\lambda_1^*<\varphi_1|+\lambda_2^*<\varphi_2| \tag{2.60}$$

Produto escalar na notação de Dirac

$$<\varphi|\psi>=<\psi|\varphi>^* \tag{2.61}$$

$$<\varphi|\lambda_1\psi_1+\lambda_2\psi_2>=\lambda_1<\varphi|\psi_1>+\lambda_2<\varphi|\psi_2> \tag{2.62}$$

$$<\lambda_1\varphi_1+\lambda_2\varphi_2|\psi>=\lambda_1^*<\varphi_1|\psi>+\lambda_2^*<\varphi_2|\psi> \tag{2.63}$$

$$<\psi|\psi> \quad \text{real, positiva, será zero se, e somente se,} \quad |\psi>=0 \tag{2.64}$$

2.10.4 Operador Linear

Definição: Um operador linear A, é por definição uma entidade matemática que associa a cada KET $|\psi>\in\xi$, outro KET $|\psi'>$, tal que:

$$|\psi'>=A|\psi> \tag{2.65}$$

$$A[\lambda_1|\psi_1>+\lambda_2|\psi_2>]=\lambda_1A|\psi_1>+\lambda_2A|\psi_2> \tag{2.66}$$

O produto de dois operadores A e B, representado por AB, é dado por:

$$(AB)|\psi >= A(B|\psi >) \tag{2.67}$$

Primeiramente B atua em $|\psi >$, levando ao KET $(B|\psi >)$; então A atua no KET $(B|\psi >)$. Em geral AB≠BA. O comutador [A,B] de A e B, é por definição:

$$[A, B] = AB - BA \tag{2.68}$$

Sejam $|\varphi >$ e $|\psi >$ dois KETs. Chama-se de elemento da matriz de A entre $|\varphi >$, o produto escalar:

$$< \varphi|(A|\psi >) \tag{2.69}$$

Consequentemente, é um número, o qual depende linearmente de $|\psi >$ e anti-linearmente de $|\varphi >$.

2.10.5 Operador Adjunto $A^\dagger$ do operador linear A

A correspondência entre os KETs e os BRAs, aqui estudada, permite associar a todo operador linear A, outro operador linear $A^\dagger$, chamado de operador adjunto (ou Hermitiano conjugado) de A.

Seja $|\psi >$ um KET arbitrário de ξ. O operador A associa a ele outro KET

$$|\psi' >= A|\psi >$$

Para cada KET $|\psi >$ corresponde um BRA $< \psi|$; da mesma maneira, $|\psi' >$ corresponde a um $< \psi'|$. Esta correspondência entre BRAs e KETs, nos permite definir a ação de um operador $A^\dagger$ associado ao BRA $< \psi|$ correspondente ao KET $|\psi >$, o BRA $< \psi'|$ correspondente ao KET $|\psi' >= A|\psi >$:

$$|\psi >\Rightarrow |\psi' >= A|\psi >$$

$$< \psi| \Rightarrow < \psi'| = A^\dagger < \psi'|$$

$A^\dagger$ é um operador linear, definido por:

$$|\psi' >= A|\psi > \Leftrightarrow < \psi'| = A^\dagger < \psi'| \tag{2.70}$$

De (2.70) deduzimos outra importante relação do operador $A^\dagger$. Usando as propriedades do produto escalar, escrevemos:

$$< \psi' | \varphi >=< \varphi | \psi' >^* \tag{2.71}$$

onde $|\varphi>$ é um KET arbitrário de ξ. Usando (2.70) para $|\psi'>$ e $<\psi'|$, obtém-se que:

$$< \psi | A^\dagger \varphi' >=< \varphi | A | \psi >^* \tag{2.72}$$

Um operador Hermitiano, ou de Hermite é definido se ele for igual ao seu adjunto, ou seja:

$$A = A^\dagger \tag{2.73}$$

2.10.6 Representação no espaço de estados

Escolher uma representação significa escolher uma base ortonormal no espaço de estados ξ. Vetores e operadores são então representados nesta base por números: componentes para os vetores e elementos de matriz para os operadores.

A escolha de uma base é a principio, arbitrária, contudo é óbvio que um problema particular a ser estudado, pode ser resolvido com cálculos mais simples dependendo da representação escolhida.

Relação de ortonormalização: Um conjunto de KETs ($\{|u_i>\}$) é dito ser ortonormal, se os KETs deste conjunto satisfazem a relação de ortonormalização:

$$< u_i | u_j >= \delta_{ij} \tag{2.74}$$

Relação de fechamento: A relação

$$P = \sum_i |u_i >< u_i| = 1 \tag{2.75}$$

onde 1 é o operador identidade em ξ, é chamada de operação de fechamento. Ela expressa o fato de que o conjunto de KETs ($\{|u_i>\}$) constitui uma base. Para todo KET $|\psi>$ pertencente a ξ pode-se escrever:

$$|\psi >= 1|\psi >= P|\psi >= \sum_i |u_i >< u_i|\psi > \tag{2.76}$$

$$|\psi >= \textstyle\sum_i c_i |u_i >, \quad \text{com} \quad c_i =< u_i|\psi > \tag{2.77}$$

Portanto, todo KET tem uma única expansão na base $\{|u_i>\}$.

2.10.7 Equações de autovalor - observáveis

Autovalor e Autovetor de um operador:

Definição: $|\psi>$ é dito ser um autovetor (ou auto KET) de um operador linear A, se:

$$A|\psi>=\lambda|\psi> \tag{2.78}$$

onde λ é um número complexo. Pode-se também apresentar algumas propriedades da equação (2.78), que é a equação do autovalor do operador linear. Em geral, esta equação possui soluções apenas quando λ assume certos valores, chamados de autovalores de A. O conjunto de autovalores é chamado de espectro de A. Pode-se notar que, se $|\psi>$ é um autovetor de A com autovalor λ, $\alpha|\psi>$ (onde α é também um complexo arbitrário) é também um autovetor de A com o mesmo autovalor:

$$A(\alpha|\psi>)=\alpha A\lambda|\psi>=\alpha\lambda|\psi>=\lambda(\alpha|\psi>) \tag{2.79}$$

Observável:

Propriedades dos autovalores e autovetores de um operador Hermitiano:

Apresentam-se dois importantes resultados que são válidos quando o operador é Hermitiano, ou seja: $A^\dagger = A$.

1. Os autovalores de um operador Hermitiano são reais.

De fato:

$$\left.\begin{aligned} &<\psi|A|\varphi>=<\psi|\lambda|\varphi>=\lambda<\psi|\varphi> \\ &<\psi|A|\varphi>=<\varphi|A^\dagger|\psi>^*=<\psi|A|\varphi>^*=\overline{\lambda}<\psi|\varphi> \end{aligned}\right\} \Rightarrow \lambda<\psi|\varphi>=\overline{\lambda}<\psi|\varphi> \tag{2.80}$$

Logo, $\lambda=\overline{\lambda}\Rightarrow\lambda\in\mathbb{R}$.

2. Dois autovetores de um operador Hermitiano correspondentes a autovalores diferentes, são ortogonais entre si.

De fato:

Sejam λ_1 e λ_2 dois autovalores de $A=A^\dagger$ e ψ e φ autovetores correspondentes, então temos

$$\left.\begin{aligned} &<\varphi|A\psi>=\lambda<\varphi|\psi> \\ &<\varphi|A\psi>=<\psi|A^\dagger\varphi>^*=<\psi|A\varphi>^*=\lambda_2<\varphi|\psi> \end{aligned}\right\} \Rightarrow (\lambda_1-\lambda_2)<\varphi|\psi>=0 \tag{2.81}$$

Como $\lambda_1 \neq \lambda_2$, então $< \varphi|\psi >= 0$.

Definição de Observável: Considerando um operador Hermitiano.

Por simplicidade, considere que o conjunto de autovalores forma um espectro discreto $\{a_n : n = 1, 2, 3, ...\}$. Chame de $|\psi_n >$ os auto KET's associados aos autovalores a_n.

$$A|\psi_n >= a_n|\psi_n > \tag{2.82}$$

Das propriedades 1 e 2, tem-se que:

$$< \psi_i|\psi_j >= \delta_{ij} \tag{2.83}$$

Por definição, o operador Hermitiano A é um observável, se o seu sistema ortonormal de autovetores forma uma base no espaço de estados. Isto pode ser expresso pela relação de fechamento:

$$\sum_i |\psi_n >< \psi_n| = 1 \tag{2.84}$$

2.10.8 Conjunto de observáveis que comutam

Teorema 1: Se dois operadores A e B comutam, e se $|\psi >$ é um auto-vetor de A, então $(B|\psi >)$ é também auto-vetor de A, com o mesmo auto-valor.
De fato:

Considere que $AB = BA$ e que λ é autovalor de A com autovetor $|\varphi >$, temos:

$$A|\varphi >= \lambda|\varphi > \Rightarrow A(B|\varphi >) = B(A|\varphi >) = \lambda B|\varphi > . \tag{2.85}$$

Logo, λ é autovalor de A com autovetor $B|\varphi >$.

Teorema 2: Se dois observáveis A e B comutam, e se $|\psi_1 >$ e $|\psi_2 >$ são dois auto-vetores de A com diferentes auto-valores, então o elemento de matriz é tal que $< \psi_1|B|\psi_2 >= 0$.
De fato:

Sejam $A|\psi_1 >= \lambda_1|\psi_1 >$ e $A|\psi_2 >= \lambda_2|\psi_2 >$ com $\lambda_1 \neq \lambda_2$, temos:

$$\left.\begin{array}{l} < \psi_1|BA|\psi_2 >= \lambda_2 < \psi_1|B|\psi_2 > \\ < \psi_1|AB|\psi_2 >=< \psi_1|A(B|\psi_2 >) =< \psi_1|\lambda_1 B|\psi_2 > \end{array}\right\} \Rightarrow < \psi_1|B|\psi_2 >= 0 \tag{2.86}$$

Teorema 3: "O teorema fundamental da Mecânica Quântica"− Se dois observáveis A e B comutam, é sempre possível construir uma base ortonormal no espaço de estados com

auto-vetores comuns a A e B.

Por definição, um conjunto completo de observáveis A, B e C é assim chamado se:

1. Todos os observáveis $A, B, C, ...$ comutam aos pares;

2. Especificando os auto-valores de todos os operadores $A, B, C, ...$ determinamos um único auto-vetor comum; ou de maneira equivalente: "Um conjunto de observáveis $A, B, C, ...$ é um CSCO (*Complete Sets of Commuting Observables*), se existe uma única base ortonormal composta de auto-vetores comuns a todos eles."Assim para um dado sistema físico, existem vários CSCO.

2.10.9 As representações: $\{|r>\}$, $\{|P>\}$ e $\{|\varphi_n>\}$

Definição: Sejam $\{\xi_{r_0}(r)\}$ e $\{\upsilon_{P_0}(r)\}$ duas bases em Γ.

$$\{\xi_{r_0}(r)\} = \delta(r - r_0) \tag{2.87}$$

$$\{\upsilon_{P_0}(r)\} = (2\pi\hbar)^{-3/2} e^{i/\hbar P_0 r} \tag{2.88}$$

Contudo, toda função quadrado integrável pode ser expandida em uma ou outra base.

Como foi feito anteriormente, associe a cada uma dessas bases um ket do espaço de estados.

$$\xi_{r_0}(r) \Leftrightarrow |r_0> \tag{2.89}$$

$$\upsilon_{P_0}(r) \Leftrightarrow |P_0> \tag{2.90}$$

Usando as bases $\{\xi_{r_0}(r)\}$ e $\{\upsilon_{P_0}(r)\}$ de Γ, pode-se definir em ξ_r duas representações: $\{|r_0>\}$ e $\{|P_0>\}$.

A base de vetores de primeira representação é caracterizada por três índices contínuos x_0, y_0, z_0, os quais são coordenadas de um ponto no espaço tridimensional. Para a segunda representação, os três índices são também componentes de um vetor ordinário.

Se assumirmos que $\{|\varphi_0>\}$ é normalizado, então $a\,|\varphi_n>=0$ se reduz a um fator de fase $e^{i\theta}$, onde θ é real, e temos que $|\varphi_1>= c_1 a^\dagger|\varphi_0>$ e consequentemente $|\varphi_2>= c_2 a^\dagger|\varphi_1>$ e desenvolvendo $<\varphi_2|\varphi_2>$ chegamos em $c_2 = \dfrac{1}{\sqrt{2}}$ e para sucessivas escolhas de fase obtemos:

$$|\varphi_n>= c_n\, a^\dagger|\varphi_{n-1}> \tag{2.91}$$

com $c_n = \dfrac{1}{\sqrt{n}}$

$$|\varphi_n >= \frac{1}{\sqrt{n}}\, a^{\dagger}|\varphi_{n-1} > \tag{2.92}$$

Relação de ortonormalização e fechamento

Calcula-se $< r_0|r_0' >$. Usando a definição de produto escalar de ξ_r:

$$< r_0|r_0' >= \int d^3r \xi^*_{r_0}(r)\xi_{r_0'}(r) = \delta(r_0 - r_0') \tag{2.93}$$

(onde $\delta(r_0 - r_0')$= função Delta de Dirac). Da mesma maneira, temos

$$< P_0|P_0' >= \int d^3r \upsilon^*_{P_0}(r)\upsilon_{P_0'}(r) = \delta(P_0 - P_0') \tag{2.94}$$

Observação: O fato de que os conjuntos de $|r_0 >$ ou que $|P_0 >$ constitui uma base em ξ_r.

$$< r_0|r_0' >= \delta(r_0 - r_0') \tag{2.95}$$

$$\int d^3r_0 |r_0 >< r_0| = 1 \tag{2.96}$$

$$< P_0|P_0' > \delta(P_0 - P_0') \tag{2.97}$$

$$\int d^3P_0 |P_0 >< P_0| = 1 \tag{2.98}$$

Componentes de um KET

Considere um KET arbitrário $|\psi >$, correspondendo a uma função de onda $\psi(r)$. As relações de fechamento (2.96) e (2.98), nos possibilitam expressar o KET das seguintes maneiras:

$$|\psi >= \int d^3r_0 |r_0 >< r_0|\psi > \tag{2.99}$$

$$|\psi >= \int d^3P_0 |P_0 >< P_0|\psi > \tag{2.100}$$

os coeficientes $< r_0|\psi >$ e $< P_0|\psi >$, podem ser calculados usando as fórmulas:

$$< r_0|\psi >= \int d^3r \xi^*_{r_0}(r)\psi(r) \tag{2.101}$$

$$< P_0|\psi >= \int d^3r \upsilon^*_{P_0}(r)\psi(r) \tag{2.102}$$

Encontra-se então:

$$< r_0|\psi >= \psi(r_0) \tag{2.103}$$

$$< P_0|\psi >= \overline{\psi}(P_0) \tag{2.104}$$

onde o $\overline{\psi}(P)$ é a transformada de Fourier de $\psi(r)$.

Concluímos que o valor $\psi(r_0)$ da função de onda no ponto r_0, é, a componente do KET $|\psi >$ no vetor base $|r_0 >$ na representação $\{|r_0 >\}$. Assim como a função de onda no espaço dos momentos $\overline{\psi}(P)$, é representado por $\{|P >\}$.

Uma vez que os autovetores $|\varphi_n >$ já são normalizados, eles satisfazem a relação de ortonormalização $< \varphi_n|\varphi_n >= \delta_{m,n}$ e pode ser representado pela relação de fechamento $\sum_n |\varphi_n >< \varphi_n| = 1$.

2.11 Os Postulados da Mecânica Quântica

A base da Mecânica Quântica, (1):

Postulado 1: *A qualquer sistema físico isolado existe a ele associado um espaço vetorial complexo chamado de espaço de Hilbert. Os elementos do espaço de Hilbert são vetores complexos $|\psi >$, chamados de kets, e representam o estado físico do sistema. O complexo conjugado de um ket é chamado de bra, representado por $< \psi|$.*

Postulado 2: *A evolução de um sistema quântico fechado, ou seja, que não interage com sua vizinhaça, se dá através de transformações unitárias*:

$$|\psi(t) >= U(t)|\psi(0) > \tag{2.105}$$

onde $U^\dagger U = I$, ou ainda por:

$$\rho' = U\rho U^\dagger \tag{2.106}$$

onde, ρ é o estado do sistema em um instante t_1, ρ' é o estado do sistema em um instante t_2 e U o operador unitário que depende de t_1 e t_2.

Postulado 3: *As medidas quânticas são representadas por um conjunto de operadores de medidas $\{M_m\}$, onde índice m refere-se aos possíveis resultados da medida. A probabilidade de que o resultado m seja encontrado em uma medida feita em um sistema quântico preparado no estado $|\psi >$ é dada por*

$$p(m) =< \psi|M_m^\dagger M_m|\psi > \tag{2.107}$$

e o estado do sistema após a medida com resultado m será:

$$|\psi_m >= \frac{M_m}{\sqrt{p(m)}}|\psi > . \tag{2.108}$$

A normalização das probabilidades, $\sum_m p(m) = 1$*, a hipótese de que* $< \psi|\psi >= 1$ *e a Eq.(2.107) implicam na relação de completitude*:

$$\sum_m M_m^\dagger M_m = I \tag{2.109}$$

Postulado 4: *Os elementos do espaço de Hilbert de um sistema quântico composto* $A - B$ *é formado pelo produto tensorial dos kets dos espaços de Hilbert dos sistemas individuais*:

$$|\psi_{A-B} >= |\psi_A > \otimes |\psi_B >, \tag{2.110}$$

e estendendo para N *sub-sistemas, temos*:

$$|\psi_{A-B-...-N} >= |\psi_A > \otimes |\psi_B > \otimes ... \otimes |\psi_N > . \tag{2.111}$$

Capítulo 3

Informação Quântica

3.1 Introdução à Informação Quântica

Informação Quântica é a identificação e o estudo dos recursos quânticos utilizáveis na área da informação ou para o tratamento da Informação. Surgiu da união de duas áreas científicas do século XX: a Teoria Quântica e a Teoria da Informação. O processamento da "informação quântica", utiliza as propriedades que caracterizam os sistemas microscópicos, as quais os sistemas clássicos não possuem, como o emaranhamento quântico e a superposição de amplitudes de probabilidades.

Os sistemas clássicos baseados na arquitetura de Von Neumann fazem uma distinção entre processamento (seqüencial com desvios condicionais ou incondicionais) e armazenamento de informação (organização em dados, instruções programas executáveis), que apesar de algumas restrições os computadores clássicos são eficientes e ainda não existe forma melhor de realizar cálculos matemáticos, editar textos, acessar a Internet, etc. Porém deixam a desejar em áreas que exigem maior potência computacional ou velocidade de processamento como na Inteligência Artificial, velocidade essa que segundo a Lei de Moore dobra a cada 18 meses e que não altera o poder computacional, e além disso o armazenamento da informação se aproxima de um limite próximo de escalas atômicas, com isso será necessário substituir a tecnologia atual por uma totalmente nova, dentre as alternativas temos a Computação Quântica.

A computação quântica surgiu como uma disciplina inserida neste modelo da informação quântica ligada aos problemas da definição de portas lógicas, algoritmos e outros protocolos "quânticos". De acordo com Nielsen e Chuang (1), algumas questões impor-

tantes na teoria da informação quântica se referem ao significado de quando dois ítens de informação são semelhantes, ou quando a informação é preservada em algum processo quântico, e podem ser respondidas em termos das chamadas normas de distância.

Já no processamento da informação quântica, precisa-se controlar as interações entre os q-bits, e os físicos e químicos experimentais estão aproveitando os vários sistemas físicos que podem fornecer o isolamento e o controle necessários para implementar um computador quântico, sendo que um *emsamble - conjunto infinito de realizações de um certo estado* de spins nucleares em Ressonância Magnética Nuclear (RMN) é a que, até o momento, apresenta mais vantagens com relação às implementações práticas de algoritmos quânticos, em sistemas contendo poucos q-bits e requer que o sistema esteja colocado em um estado adequado, relativo ao qual a informação pode ser armazenada (3).

3.2 Teoria Quântica

Todo sistema quântico possui um *espaço de estados* que é um espaço vetorial *complexo* com produto escalar hermitiniano, ξ, que na notação de Dirac chamaremos de $|\psi>$, e ainda o vetor dual ξ^*, será denotado por $<\phi|$ e o produto escalar entre $<\phi|$ e $|\psi>$ é $<\phi|\psi>$.

3.3 Unidades de Informação Quântica (Q-Bit, *qubit*, bit quântico)

A unidade de informação clássica é o bit, com valores lógicos "0"ou "1", que correspondem a cada uma dentre duas posibilidades de um dispositivo bi-estável, como positivo ou negativo, a carga ou descarga elétrica. A informação quântica é processada através da manipulação de bits quânticos, que é a unidade de informação quântica, geralmente tomado como um estado puro $|0>$ de uma disposição de N sistemas quânticos de dois estados (*qubits*), cujos estados da base correspondem a uma codificação binária dos inteiros, de 0 a $2^N - 1$.

Na natureza, os *qubits* podem ser representados por diferentes objetos, sendo os mais comuns os fótons (partículas de luz), o *spin* (ou rotação) dos núcleos atômicos e os átomos em geral. De certa forma, essas entidades, na função de *qubits*, desempenham papel

semelhante ao dos componentes eletrônicos em um computador convencional (ou clássico), que armazenam informação na forma de zeros e uns, ou em qualquer superposição deles, porém para um *qubit* já não falamos de seus valores, e sim de seus estados, podendo estar num estado (representado por) $|0>$ ou no estado (representado por) $|1>$. Um *qubit* é um estado quântico $|\Psi>$ descrito por

$$|\Psi>= \alpha|0> +\beta|1> \tag{3.1}$$

onde α e β são números complexos, e a normalização exige $|\alpha|^2 + |\beta|^2 = 1$. Essa notação é conhecida como Notação de Dirac onde $|\Psi>$ denota o ket psi e o seu dual $|\phi>$ é denotado por $<\phi|$ bra fi, para clariar a notação, o produto escalar entre $|\phi>$ e $|\Psi>$ é dado por $<\phi|\Psi>$ braket. A informação quântica utiliza as notações de Dirac chamadas bra ($<|$) e ket ($|>$) para a representação dos estados quânticos. Utilizando o modelo matricial da mecânica quântica, pode-se definir os *qubits* $|0>$ e $|1>$ como:

$$|0>= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{e} \quad |1>= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3.2}$$

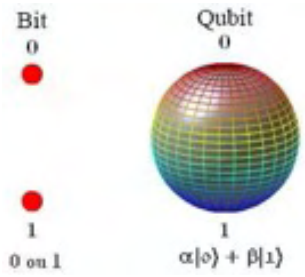


Figura 3.1: *Estados do bit clássico e quântico*

Segundo Nielsen e Chuang (1), o *qubit* pode ser representado por uma partícula de $\frac{1}{2}$ rotação/spin. Esta é uma das realizações físicas concebíveis a um *qubit* num computador quântico. Então uma medição da componente de partículas do spin ao longo da direção z pode produzir os resultados $+\frac{1}{2}$ e $-\frac{1}{2}$ apenas, o que correspondem as funções de onda ortogonais comumente denotado por $|+z>$ e $|-z>$, respectivamente. Do mesmo modo, se uma medição da componente de spin ao longo da direção y é realizada sobre uma partícula do spin que tinha encontrado $+\frac{1}{2}$ ao longo da direção de z, os únicos resultados possíveis são novamente $+\frac{1}{2}$ e $-\frac{1}{2}$, que correspondem as funções de onda ortogonais $|+y>$

e $|-y>$, respectivamente. Mas nenhuma das funções de onda $|+y>$ e $|-y>$, é idêntica à função de onda $|+z>$ e $|-z>$.

De acordo com Scarani (43), pode ser que cada função de onda $|+z>$ e $|-z>$, seja uma combinação linear da conhecida função de onda $|+y>$ e $|-y>$, e vice-versa. Temos então que o *qubit* é representado pelos vetores $|0>$ e $|1>$ sobre C (conjunto dos números complexos), assim qualquer tipo de questionamento tem um conjunto de alternativas distintas de $|\Psi>$ ou seja $|0>$ e $|1>$ cada alternativa é relacionada a um vetor, cujo conjunto desses vetores é ortogonal. Então como $|\Psi>=\alpha|0>+\beta|1>$ vetor normalizado de $|\Psi>$ e $<\Psi|\Psi>=|\alpha|^2+|\beta|^2=1$, a probabilidade de obtermos a alternativa 0 é $|\alpha|^2$ e obtermos 1 é $|\beta|^2$ após a filtragem dos testes temos $|0>$ se obtido 0 e $|1>$ se obtido 1. Portanto $|0>=1.|0>+0.|1>$ e $|1>=0.|0>+1.|1>$. Existe também uma representação matricial que facilita o entendimento da superposição de estados e portas lógicas, como visto anteriormente na equação (3.2), onde $|0>=\begin{bmatrix}1\\0\end{bmatrix}$ e $|1>=\begin{bmatrix}0\\1\end{bmatrix}$. E para dois *qubits* temos:

$$|00>=\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\quad |01>=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\quad |10>=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\quad \text{e}\quad |11>=\begin{bmatrix}0\\0\\0\\1\end{bmatrix} \tag{3.3}$$

e a função de onda fica

$$|\Psi>=\alpha_{00}|00>+\alpha_{01}|01>+\alpha_{10}|10>+\alpha_{11}|11> \tag{3.4}$$

onde $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2$, ou para simplificar

$$\Psi=\alpha_0|0>+\alpha_1|1>+\alpha_2|2>+\alpha_3|3>, \tag{3.5}$$

para $|i>$ e α_i, com i= 0,...,3 e n = número de *qubits*, generalizando temos

$$\Psi=\textstyle\sum_{i=0}^{2^n-1}\alpha_i|i> \quad \text{com} \quad \sum_{i=0}^{2^n-1}|\alpha_i|^2=1$$

Não é obrigatório o uso da base ortonormal $\{|0>,|1>\}$, podemos usar uma outra base ortonormal qualquer, por exemplo $\{|+>,|->\}$ do espaço de estados ξ que definimos os vetores como:

$$|+>=\frac{1}{\sqrt{2}}(|0>+|1>)\quad \text{e}\quad |->=\frac{1}{\sqrt{2}}(|0>-|1>) \tag{3.6}$$

3.4 A Esfera de Bloch

Trata-se da esfera dos estados de um *qubit*, após ser parametrizado pelos ângulos $\theta \in [0, \pi]$ e $\phi \in [0, 2\pi]$, para estados puros de um *qubit*.

$$|\Psi >= \cos(\frac{\theta}{2})|0 > + e^{i\phi} \sin(\frac{\theta}{2})|1 > \tag{3.7}$$

que se trata da substituição a equação (3.1) de α por $\cos(\frac{\theta}{2})$ e de β por $e^{i\phi}\sin(\frac{\theta}{2})$. Assim $|0>$ será o pólo norte da esfera e $|1>$ será seu pólo sul, e todos os estados de um q-bit podem ser representados, por três parâmetros: dois explícitos, θ e ϕ, e um implícito, o comprimento do vetor, que é sempre igual a 1. Esses parâmetros podem ser utilizados para obtermos uma representação polar no $\mathbb{R}^3$, por:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \cos\phi \sin\theta \\ \sin\phi \sin\theta \\ \cos\theta \end{bmatrix} \tag{3.8}$$

e a representação da base computacional será $|0>= \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ e $|1>= \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$ e para outra base ortonormal como por exemplo na equação (3.6) $\frac{1}{\sqrt{2}}(|0> + |1>)$ será representado por $(1, 0, 0)$ e $\frac{1}{\sqrt{2}}(|0> - |1>)$ por $(-1, 0, 0)$.

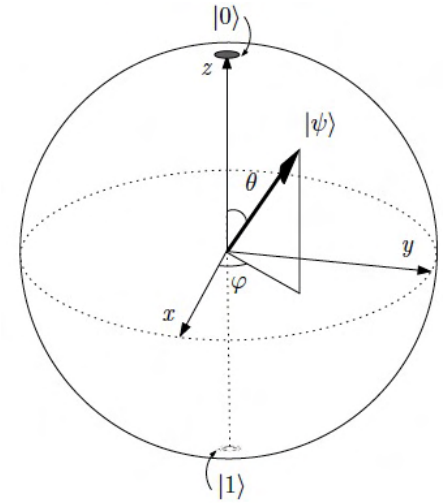


Figura 3.2: *Esfera de Bloch*

Capítulo 4

Computação Quântica

A computação quântica teve início com Feynman em 1982, que apontou que os sistemas clássicos não modelariam eficientemente os sistemas quânticos e que esses só poderiam ser modelados por outro sistema quântico e sugeriu que os computadores fossem baseados nas leis da mecânica quântica para processar informações.

A principal vantagem do computador quântico é o chamado paralelismo quântico baseado na superposição coerente de estados distintos, devido a unidade básica de informação ser o *qubit* que pode assumir os valores de 0 ou 1 ou ambos ao mesmo tempo, fazendo com que o sistema cresça exponencialmente.

Com isso problemas praticamente sem solução em computadores clássicos podem ser resolvidos em tempos razoáveis ou normais. Porém, somente quando Shor publicou em 1994 o algoritmo quântico que resolve o problema de fatoração de números grandes inteiros é que despertou o interesse de várias comunidades cientificas e gerando esforços para a produção de um hardware quântico. (2)

O hardware quântico ainda não foi lançado, mas deverá usar técnicas como ressonância magnética nuclear, armadilha de íons ou eletrodinâmica quântica de cavidade.

4.1 Portas Lógicas

Sabemos que a computação clássica funciona através de portas lógicas (*NOT, AND, OR, XOR*), na computação quântica não é diferente, porém é necessária apenas uma única porta $QXor_q$ de dois *qubits* para se construir outras portas (1), (31), mas a mais simples ainda é a porta $NOT = QNot$ onde apenas se troca o estado do qubit $QNot|0 >= |1 >$

e $QNot|1>=|0>$.

A matriz transformação da porta NOT é $U_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, temos então que:

$$U_{not}(|0>) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.1 + 1.0 \\ 1.1 + 0.0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{4.1}$$

$$U_{not}(|1>) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.0 + 1.1 \\ 1.0 + 0.1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{4.2}$$

Já a porta quântica $QXor$ também chamada de porta não controlada ou $CNOT$, ela modifica o estado do *qubit* alvo. Neste caso temos o *qubit* alvo e o *qubit* de controle então se o *qubit* de controle é 0 mantém o alvo senão modifica o alvo.

$$QXor|00>=|00>, \quad QXor|01>=|01>, \quad QXor|10>=|11> \quad \text{e} \quad QXor|11>=|10> \tag{4.3}$$

Generalizando temos a porta quântica $QXor$ definida através do produto tensorial:

$$\begin{aligned} QXor|0>\otimes|\psi>&=|0>\otimes|\psi> \\ QXor|1>\otimes|\psi>&=|1>\otimes Xor|\psi> \end{aligned} \tag{4.4}$$

Temos ainda uma porta conhecida como Hadamard (H) ou raiz quadrada de NOT é uma porta comumente usada como primeiro passo de vários algoritmos quânticos,

$$H|0>=\tfrac{1}{\sqrt{2}}(|0>+|1>)=|+> \quad \text{e} \quad H|1>=\tfrac{1}{\sqrt{2}}(|0>-|1>)=|-> \tag{4.5}$$

E também definida na forma:

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4.6}$$

Uma operação utilizada para construir portas lógicas na computação quântica é o chamado produto tensorial. Este produto de dois estados

$$|\Psi>=\begin{bmatrix} \Psi_1 \\ \Psi_2 \\ \vdots \\ \Psi_m \end{bmatrix} \quad \text{e} \quad |\varphi>=\begin{bmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_p \end{bmatrix},$$

denotado por $|\Psi> \otimes |\varphi>$, tem como resultado o estado $|\chi>$ com mp-linhas, dado por

$$|\chi>= \begin{bmatrix} \Psi_1\varphi_1 \\ \Psi_1\varphi_2 \\ \vdots \\ \Psi_1\varphi_p \\ \Psi_2\varphi_1 \\ \Psi_2\varphi_2 \\ \vdots \\ \Psi_m\varphi_1 \\ \Psi_m\varphi_2 \\ \vdots \\ \Psi_m\varphi_p \end{bmatrix},$$

onde $\Psi_i\varphi_j$ é o produto usual dos complexos. Pode-se estender o produto tensorial para matrizes quaisquer. Dadas as matrizes $A \in C^{m\times n}$ e $B \in C^{p\times q}$, a matriz $A \otimes B \in C^{mp\times nq}$ é definida por

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix},$$

onde A_{ij} é o elemento da linha i e da coluna j de A. De maneira mais precisa $A \otimes B$ é definido por $(A \otimes B)_{rs} = A_{ij}B_{kl}$, onde $r = (i-1)p + k$ e $s = (j-1)q + l$, com os índices variando da seguinte forma: $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, $1 \leqslant k \leqslant p$ e $1 \leqslant l \leqslant q$.

É através do produto tensorial de dois estados que chegamos à equação (3.3):

$$|01>= |0> \otimes |1>= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{4.7}$$

e

$$|10>= |1> \otimes |0>= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \tag{4.8}$$

E na representação matricial com $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ então

$$A \otimes B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

4.2 Estados de Bell

Os vetores descritos na forma: (1), (31)

$$|\phi_{\pm}>= \frac{1}{\sqrt{2}}(|00> \pm |11>) \quad \text{e} \quad |\psi_{\pm}>= \frac{1}{\sqrt{2}}(|01> \pm |10>) \tag{4.9}$$

e/ou

$$\begin{aligned} |\phi_{00}>= \frac{(|00> + |11>)}{\sqrt{2}} \quad , \quad |\phi_{01}>= \frac{(|01> + |10>)}{\sqrt{2}}, \\ |\phi_{10}>= \frac{(|00> - |11>)}{\sqrt{2}} \quad \text{e} \quad |\phi_{11}>= \frac{(|01> - |10>)}{\sqrt{2}}, \end{aligned} \tag{4.10}$$

são conhecidos como estados de Bell e são vetores do tipo não-decomponíveis, ou emaranhados. Os estados de *Bell ou pares EPR (Einstein, Podolsky e Rosen)* são encontrados tendo-se uma porta Hadamard, seguida por uma porta *QXor*, assim, por exemplo, uma entrada $|00>$ quando passa pela porta Hadamard se transforma em $\frac{(|0> + |1>)|0>}{\sqrt{2}}$ e a porta *QXor* o transforma em $\frac{(|00> + |11>)}{\sqrt{2}}$.

As portas lógicas devem ser implementadas com alta precisão, lembrando sempre que a alta incidência de erros em um computador quântico se dá ao próprio ambiente, pois a influência do meio sobre o computador quântico pode causar alteração dos *qubits* invalidando toda a computação, devido ao fato de que na Física Quântica o ato de medir

ou observar o sistema quântico destrói a superposição de estados. Para evitar esse tipo de problema estão estudando com afinco ressonância magnética nuclear, armadilha de íons, eletrodinâmica quântica de cavidade, e várias outras técnicas.

4.3 O Computador Quântico

Não se viu ainda um modelo físico que sacie a nossa curiosidade, mas no ano de 2007, a empresa canadense D-Wave apresentou um protótipo funcional do que seria o primeiro computador quântico comercial do mundo, com um chip quântico de 16 qubits. Era

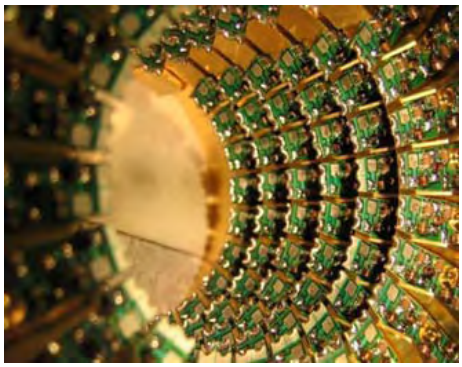


Figura 4.1: *Protótipo funcional do computador quântico (49)*

esperado que até o final de 2008, alcançasse os 1.024 qubits. Não há, no entanto, nenhuma indicação de que esse resultado tenha sido alcançado. O protótipo do chip quântico foi desenhado pela D-Wave e a fabricação é feita sob encomenda pela NASA, com materiais supercondutores, como alumínio e nióbio e depois resfriado em hélio líquido.

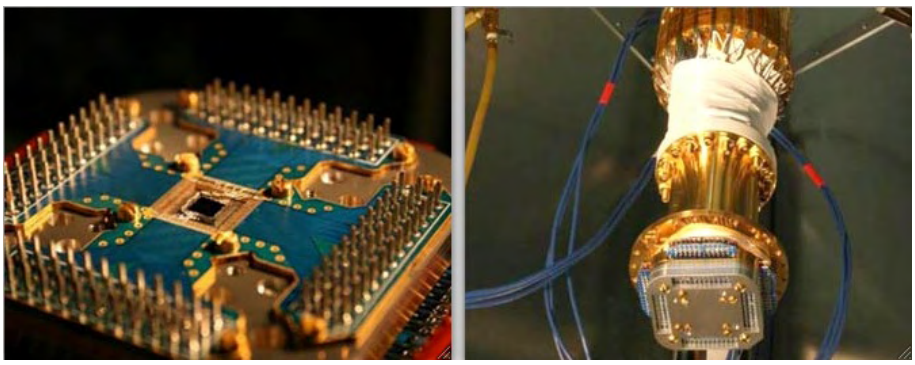


Figura 4.2: *Protótipo do chip do computador quântico e os condutores (49)*

Capítulo 5

Algoritmos Quânticos

Os algoritmos quânticos utilizam a superposição quântica para otimizar a solução de problemas, os algoritmos mais famosos são (2):

1. Algoritmo de Deutsch (1989): o algoritmo pode responder em apenas um passo se a função é balanceada ou constante.

2. Algoritmo de Grover (1996): nos proporciona um método quântico de acelerar o processo de busca não estruturada em bancos de dados de n itens.

3. Algoritmo de Shor (1994): fatoração de grandes números inteiros em tempo polinomial.

5.1 O algoritmo de Shor e a Criptografia RSA

Em 1994, Peter Shor mostrou que para N suficientemente grande, um Computador Quântico poderia executar a fatoração com muito menos esforço computacional, em tempo polinomial, explorando algumas propriedades matemáticas de números compostos e respectivos fatores que estão particularmente bem adaptada para produzir o tipo de interferência construtiva e destrutiva de que um computador quântico pode prosperar.

O algoritmo de Shor é a base da criptografia do sistema da chave pública da RSA[1]. A fatoração de $N = p.q$ usando a propriedade dos inteiros co-primos de N demonstra um grande potencial do Algoritmo de Shor na computação quântica, a fatoração de Shor é rápida porque utiliza a Transformada de Fourier Quântica (TFQ), que necessita da ordem

[1]RSA é a abreviação das letras dos sobrenomes de Ron Rivest, Adi Shamir e Leonard Adleman os mentores da criptografia de chave pública.

de $O(n^2)$ operações para realizar a transformada de Fourier de 2^n números, enquanto que a sua análoga clássica, a Transformada de Fourier Rápida (FFT - Fast Fourier Transform) requer algo em torno de $O(n2^n)$ operações.

A Transformada Quântica de Fourier (1) em notação vetorial com ação sobre superposições pode ser implementada como um circuito quântico na forma:

$$\sum_{j=0}^{2^n-1} x_j|j> \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j \right] |k> = \sum_{k=0}^{2^n-1} y_k|k> \tag{5.1}$$

5.1.1 Etapas do Algoritmo Quântico de Shor

1. Escolha um inteiro y tal que y seja menor que N $(y < N)$
2. Calcule o $mdc\,(y, N)$
3. Aplica-se a transformada de Hadamard (4.5) no registrador 1.
4. Depois aplica-se a transformada unitária no registrador 2 e mede o seu valor.
5. Usa-se a Transformada Quântica de Fourier (5.1) no registrador 1, utilizando no registrador 2 o valor obtido no passo 4, para calcular o período (r) de $f(a) = |y^a \; mod \; N>$
6. Verificar r, se r for ímpar ou $y^{r/2} = -1(mod\; N)$
7. Se r for ímpar ou $y^{r/2} = -1(mod\; N)$, então ERRO volte para o passo 1
8. Senão o mdc é calculado por: $mdc\,(y^{r/2} + 1, N)$.

Os primeiros passos do algoritmo quântico são semelhantes ao algoritmo clássico, a diferença entre eles encontra-se nos passos 3, 4 e 5 onde o algoritmo clássico calcula $y^a \; mod \; N$ para cada período da função, enquanto que o algoritmo quântico cria um registrador quântico com duas partes $|\phi>= |0>|0>$ em que na 1^a parte ele armazena os $a's$ de $f(a)$ em sobreposição e armazena o resultado de $f(a) = x^a \; (mod\; n)$ para cada valor armazenado na 1^a parte na 2^a parte do registrador quântico, isso é realizado em um único passo devido ao paralelismo quântico, pois o computador quântico calcula na verdade $y^{|a>} \; mod \; N$. Assim com a escolha de um q num intervalo de $(n^2, 2n^2)$ teremos uma boa aproximação da Transformada Quântica de Fourier, e podemos encontrar um número inteiro positivo n co-primo de $N = p.q$ tal que p e q sejam números primos grandes e distintos.

Assim $n^j \equiv f_j \; (mod\; pq)$ com $0 < f_j < N$ e $n^\phi = n^{(p-1)(q-1)} \equiv 1 \; (mod\; pq)$ com $f_\phi = 1$

para qualquer n, lembrando que $1 \leqslant j \leqslant \phi = (p-1)(q-1)$ para $\forall f_j = 1$.

Para $j = r$ temos $n^r - 1 \equiv 0\ (mod\ p.q)$, onde r determina a ordem de n módulo $p.q$ e r é tal que $n^{r/2}$ é um inteiro. Supondo que r seja a ordem de um inteiro $n < N$ e co-primo de N conhecido $\left(n^{r/2}-1\right)\left(n^{r/2}+1\right) \equiv 0\ (mod\ p.q)$ tal que $\left(n^{r/2}-1\right) \neq 0\ (mod\ p.q)$ e $\left(n^{r/2}+1\right) \neq 0\ (mod\ p.q)$, mas pode ser que $\left(n^{r/2}-1\right)$ seja divisível por p ou q e $\left(n^{r/2}+1\right)$ seja divisível por p ou q.

Assim N é dividido por $\left(n^{r/2}+1\right)$ ou por $\left(n^{r/2}-1\right)$.

Portanto $\dfrac{N}{n^{r/2}+1} = q$ e então determinamos p através da divisão $\dfrac{N}{q} = p$, tudo isso classicamente.

Já na computação quântica, a determinação de r e a fatoração de N é feita usando a propriedade de periodicidade da seqüência f_j, $j = 1, 2, 3, ...$, definida por $n_j \equiv f_j\ (mod\ p.q)$ onde para $\forall n$ inteiro, f_1, f_2,...,f_{r-1}, $f_r = 1$ são diferentes, mas a seqüência f_j é periódica com período r, para extração da ordem r é empregada a Transformada Quântica de Fourier de acordo com a função de onda do computador quântico construído especialmente para exibir este r periodicamente com a seleção randômica de r.

5.1.2 Um exemplo do uso do Algoritmo de Shor

Exemplo realizado analiticamente, com um valor de N pequeno com a finalidade apenas de facilitar os cálculos e o entendimento. Não foram usados os passos: 3, 4 e 5.

Tomando $N = 65$, escolha por exemplo de $n = 12$ e o algoritmo de Shor trará $r = 4$. Então a seqüência f_j para $n = 12$ precisamos inserir $f_1 = 12$,

$f_{r/2} = f_2 = 12^2\ (mod\ 65) = 14$,

$f_3 = 12^3\ (mod\ 65) = 38$,

$f_4 = 12^4\ (mod\ 65) = 1$,

$f_5 = 12^5\ (mod\ 65) = 12$, a partir deste momento a seqüência f_j começa a se repetir, portanto $r = 4$.

Como $\left(n^{r/2}-1\right) \neq 0\ (mod\ p.q)$ e $\left(n^{r/2}+1\right) \neq 0\ (mod\ p.q)$ são ambas satisfeitas por este f_2, imediatamente sabemos que $f_2 + 1 = 15$ deve ser divisível por fatores de 65 ($mdc\ (15, 65) = 5$), e que $f_2 - 1 = 13$ ser divisível por fatores de 65 ($mdc\ (13, 65) = 13$). Temos assim que $p = 5$ e $q = 13$.

5.1.3 Um exemplo do uso do Algoritmo Quântico de Shor

Como exemplo apenas para visualizar a diferença de cálculos, realizada analiticamente entre os Algoritmos de Shor Clássico e Quântico foi escolhido o mesmo valor para N.

O número $N = 65$ não é par e não é primo, então escolhemos um número inteiro positivo $n = 12$, como mdc $(65, 12) = 1$, então $f(n) = 12^n \, mod \, 65$.

Escolhemos agora um $q = 2^{13} = 8192$ tal que $N^2 \leqslant q \leqslant 2N^2$. A partir deste momento inicializa-se os registradores $|\psi >= |0 > |0 >$ e aplica-se a transformada de Hadamard no registrador 1, e obtém-se:

$$\frac{1}{\sqrt{8192}} \sum_{n=0}^{8191} |n > |0 >$$

Aplicando a transformada unitária $f(n) = 12^n \, mod \, 65$ no registrador 2, temos:

$$\frac{1}{\sqrt{8192}} \sum_{n=0}^{8191} |n > |12^n \, mod \, 65 >$$

O estado dos registradores fica:

$$\begin{aligned} \frac{1}{\sqrt{8192}} \sum_{n=0}^{8191} |n > |12^n \, mod \, 65 >= \\ = \frac{1}{\sqrt{8192}} (|0 > |1 > + |1 > |12 > + |2 > |14 > + |3 > |38 > + \\ + |4 > |1 > + 5 > |12 > + |6 > |14 > + ... \\ + ... + |8189 > |12 > + |8190 > |14 > + |8191 > |38 >) \end{aligned}$$

Temos agora um estado quântico emaranhado, e se medirmos o registrador 2, teremos o valor de $k = 1$, e:

$$\frac{1}{\sqrt{|A|}} \sum_{a' \in A} |a' > |1 >, \quad \text{onde} \quad |A| = 2048$$

Assim, o estado dos registradores fica:

$$\begin{aligned} \frac{1}{\sqrt{2048}} (|0 > |1 > + |4 > |1 > + |8 > |1 > + |12 > |1 > + \\ + |16 > |1 > + |20 > |1 > + |24 > |1 > + ... \\ + ... + |8184 > |1 > + |8188 > |1 >) \end{aligned}$$

Aplicando a Transformada Quântica de Fourier no registrador 1, o estado dos registradores fica:

$$\frac{1}{\sqrt{5}}(|0>|1>+|2040>|1>+|4080>|1>+|6120>|1>+|8160>|1>)$$

Como o período é $r = 4$ utilizamos o algoritmo de Euclides (27) e assim obtemos :

$$mdc\,(12^{4/2} - 1, 65) = mdc\,(143, 65) = 13$$

e

$$mdc\,(12^{4/2} + 1, 65) = mdc\,(145, 65) = 5$$

Onde 13 e 5 são fatores de $N = 65$.

É esperado que o computador quântico resolva a fatoração de grandes números com o Algoritmo Quântico de Shor em velocidade surpreendente.

Capítulo 6

Criptografia

Criptografia é o estudo de técnicas para a segurança e a proteção de dados, para que duas ou mais pessoas possam se comunicar de forma segura por um canal de comunicação.

6.1 Um pouco de História

As tentativas de manter as comunicações em segredo, vem desde os tempos de rainhas e reis, onde as mensagens em mãos erradas poderiam causar novas guerras ou a perda de uma delas, essa ameaça do inimigo interceptar as mensagens gerou a criação de códigos e cifras, e junto com a criação os criadores e os decifradores de códigos. Simon Singh em "O Livro dos Códigos"(24) mostra vários exemplos de sistemas de códigos e relata várias histórias com heróis e vilões.

6.1.1 Cerca de Ferrovia

É a alternação das letras de uma mensagem entre duas linhas:

UM ENSAIO SOBRE CRIPTOGRAFIA

U E S I S B E R P O R F A
M N A O O R C I T G A I

U E S I S B E R P O R F A M N A O O R C I T G A I A

6.1.2 Citale

Consiste em um bastão de madeira onde era enrolada uma tira de couro ou pergaminho, onde o remetente escreve a mensagem e depois desenrola a tira de couro, assim só se consegue reler a mensagem se tiver um bastão de mesmo diâmetro. Ver Figura (6.1).

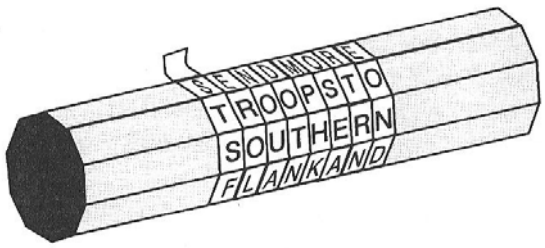


Figura 6.1: *Citale (24)*

Neste caso, quando esta desenrolado aparece:

S T S F E R O L N O U A D O T N M P H K O S E A R T R N E O N D.

6.1.3 Cifra de Substituição

Envolve o emparelhamento ao acaso das letras do alfabeto, onde cada letra é substituída por outra diferente ou por números. Substituindo as letras conforme abaixo:

$$
\begin{aligned}
U &-> E \\
M &-> J \\
N &-> P \\
S &-> X \\
A &-> H \\
I &-> R \\
O &-> W \\
B &-> L \\
C &-> D \\
T &-> G \\
F &-> K
\end{aligned}
$$

Podemos enviar: E J U P X H R W X W L I U D I N G W T I H K R H e ler como: UM ENSAIO SOBRE CRIPTOGRAFIA.

6.1.4 Código Morse

Usado para a comunicação através do telégrafo, não se trata de uma criptografia, apenas um alfabeto alternativo. Veja alguns símbolos do código Morse na Figura (6.2).

Letras			
A	.-	N	-.
B	-...	O	---
C	-.-.	P	.--.
D	-..	Q	--.-
E	.	R	.-.
F	..-.	S	...
G	--.	T	-
H	....	U	..-
I	..	V	...-
J	.---	W	.--
K	-.-	X	-..-
L	.-..	Y	-.--
M	--	Z	--..

Números	
1	·----
2	··---
3	···--
4	····-
5	·····
6	-····
7	--···
8	---··
9	----·

Sinais de pontuações	
Ponto [.]	·-·-·-
Vírgula [,]	--··--
Interrogação [?]	··--··
Apóstrofo [']	·----·
Exclamação [!]	-·-·--
Barra [/]	-··-·
Parênteses [(]	-·--·
Parênteses [)]	-·--·-
E comercial [&]	· ···
Dois pontos [:]	---···
Ponto e vírgula [;]	-·-·-·
Igual [=]	-···-
Hífen [-]	-····-
Linha baixa [_]	··--·-
Aspas ["]	·-··-·
Cifrão [$]	···-··-
Arroba [@]	·--·-·

Figura 6.2: *Símbolos do Código Morse internacional*

Se quisermos enviar CRIPTOGRAFIA QUANTICA, teríamos que teclar:

−.−..−..−−.−−−−−..−..−..−..−−.−..−.−−.−..−.−..−

6.1.5 Algumas "Máquinas" de Cifragem

Algumas imagens de máquinas de cifragem que antecederam os computadores como o disco de cifra (6.3), e a máquina Enigma (6.4), podem ser vistas ainda neste capítulo.

6.1.6 O computador

Com a criação dos computadores, a briga por quebrar cifras continuou, porém com maior velocidade e flexibilidade, levando em consideração que o computador pode ser programado para imitar a ação de centenas de misturadores, alguns que girem no sentido horário, outros em sentido anti-horário, um mais rápido outro mais lento, um a partir da terceira

Figura 6.3: *Um disco de cifra - utilizado na Guerra Civil americana*

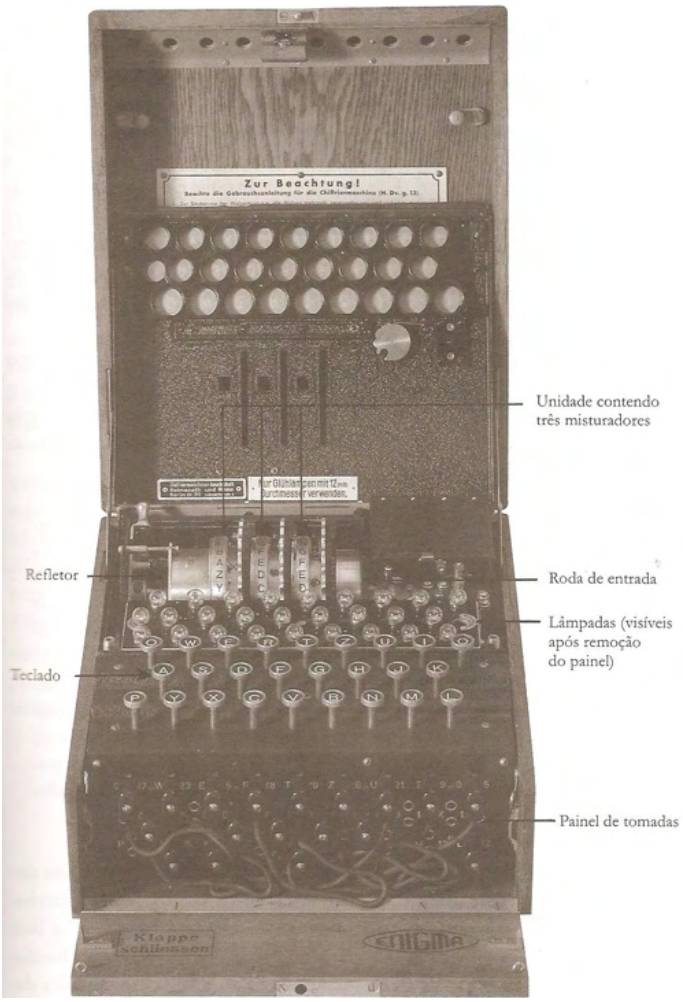


Figura 6.4: *Uma máquina Enigma aberta com 3 misturadores usada na Segunda Guerra Mundial (24)*

letra outra a partir da vigésima letra. A principal diferença é que o computador mistura números ao invés de letras, o computador trabalha com os *bits* números binários (exemplo da tabela ASCII Figura (6.5).

Binário	Glifo
0100 0001	A
0100 0010	B
0100 0011	C
0100 0100	D
0100 0101	E
0100 0110	F
0100 0111	G
0100 1000	H
0100 1001	I
0100 1010	J
0100 1011	K
0100 1100	L
0100 1101	M

Binário	Glifo
0100 1110	N
0100 1111	O
0101 0000	P
0101 0001	Q
0101 0010	R
0101 0011	S
0101 0100	T
0101 0101	U
0101 0110	V
0101 0111	W
0101 1000	X
0101 1001	Y
0101 1010	Z

Figura 6.5: *Números Binários em ASCII para letras maiúsculas*

Vamos tentar entender o procedimento usado pelo computador, nós escrevemos ou digitamos: C R I P T O G R A F I A. E o computador lê ou entende: 01000011 01010010 01001001 01010000 01010100 01001111 01000111 01010010 01000001 01000110 01001001 01000001. Uma forma simples de transposição é trocando os dígitos o primeiro e o segundo, o terceiro e quarto e assim em diante.

Vamos ao nosso exemplo com a palavra CRIPTOGRAFIA

Mensagem: C R I P T O G R A F I A

Mensagem em ASCII: 1000011 1010010 1001001 1010000 1010100 1001111 1000111 1010010 1000001 1000110 1001001 1000001.

Texto Cifrado: 0100101 1100001 0110001 1100000 0101011 0001111 0100111 1100001 0100001 1001001 0110001 1000010.

Temos agora uma única fileira de 84 dígitos que deverá ser enviada ao receptor, o qual deverá inverter o processo e obter o texto original.

Texto Cifrado: 0100101 1100001 0110001 1100000 0101011 0001111 0100111 1100001 0100001 1001001 0110001 1000010.

Texto Original: 1000011 1010010 1001001 1010000 1010100 1001111 1000111 1010010 1000001 1000110 1001001 1000001.

Agora veremos um outro processo de criptografia, onde a mesma mensagem é enviada mas com o uso de uma chave na substituição e não transposição, funciona assim, temos a mensagem e a chave traduzidas em bits, então compara-se o elemento da mensagem com o correspondente na chave, se forem iguais então substitui por zero 0, se forem diferentes então substitui por 1 no texto cifrado que será enviado ao receptor, que fazendo uso da mesma chave reverterá a mensagem usando o mesmo processo.

Mensagem: C R I P T O G R A F I A
Mensagem em ASCII: 01000011 01010010 01001001 01010000 01010100 01001111 01000111 01010010 01000001 01000110 01001001 01000001.
Chave: GRAFIA
Chave em ASCII: 01000111 01010010 01000001 01000110 01001001 01000001 01000111 01010010 01000001 01000110 01001001 01000001.
Texto Cifrado a ser enviado ao receptor: 00000100 00000000 00001000 00010110 00011101 00001110 00000000 00000000 00000000 00000000 00000000 00000000.

O receptor recebe o texto cifrado e com o uso da chave faz a comparação dos elementos, mas agora entre o texto cifrado e a chave:
Texto cifrado recebido pelo receptor: 00000100 00000000 00001000 00010110 00011101 00001110 00000000 00000000 00000000 00000000 00000000 00000000.
Chave em ASCII: 01000111 01010010 01000001 01000110 01001001 01000001 01000111 01010010 01000001 01000110 01001001 01000001.
Mensagem recuperada: 01000011 01010010 01001001 01010000 01010100 01001111 01000111 01010010 01000001 01000110 01001001 01000001.

6.2 Criptografia Clássica

A teoria que utilizaremos neste capítulo, versa sobre a teoria dos números e a matemática modular. Brevemente, (27):

Formulação Aritmética Modular: *Sejam a, m, b e r, o dividendo, divisor, quociente e resto da divisão, respectivamente, onde q também representa um quociente então* $\frac{a}{m} = b{+}r$ *e* $\frac{a-b}{m} = q + 0 => a \equiv r \ (mod\ m)$.

Teorema de Fermat: *Seja m um número primo. Se a é um número inteiro tal que mdc (m, a) = 1, então* a^{m-1}*=1 (mod m).*

Teorema de Euler: *Sejam a, m inteiros com* $m > 0$ *tal que mdc (a, m) = 1, então* $a^{\varphi(m)} \equiv 1$ *(mod m).*

A partir daqui lidaremos com 3 personagens muito utilizados na literatura de criptografia, que são: Alice, Bob e Eve (1), (2), (5), (24), (36) e (40).

Alice quer trocar mensagens com Bob e vice-versa, mas Eve quer lê-las, então Alice deverá cifrar as mensagens antes de enviá-las; mas antes disso terá de enviar uma chave secreta para Bob, senão ele não conseguirá entender as mensagens. Fazendo uso da aritmética modular, a troca de chave será feita com a função $Y^X \ (mod\ N)$, onde Y e N são escolhidos anteriormente por um meio não secreto, desde que $Y < N$.

Suponhamos que tenham sido escolhidos: $Y = 7$ e $N = 23$, então teremos a função $7^X \ (mod\ 23)$, agora Alice escolhe o seu número secreto e Bob também escolhe um número secreto. Sabendo que o número escolhido por Bob é 2 (B=2) e o número escolhido por Alice é 6 (A=6).

É hora de começar a substituição de X pelo número escolhido; então Bob deverá calcular $7^B \ (mod\ 23)$, ou seja, $7^2 \ (mod\ 23) = 49 \ (mod\ 23) = \dfrac{49}{23} = 2$ inteiros que multiplicado por 23 obtemos 46, onde $49 - 46 = 3$, assim $7^2 \ (mod\ 23) = 3$, que será o número enviado para Alice. Ao mesmo tempo Alice deverá fazer os seus cálculos $7^A \ (mod\ 23)$, onde $7^6 \ (mod\ 23) = 117649 \ (mod\ 23) = \dfrac{117649}{23} = 5115$ inteiros que multiplicado por 23 é 117645, assim $117649 - 117645 = 4$, portanto $7^6 \ (mod\ 23) = 4$ número que deverá ser enviado ao Bob, esses números enviados correm o risco de serem interceptado por Eve, porém ela não saberá quais foram os números secretos escolhidos por cada um.

De posse agora do número calculado por Alice, Bob terá de encontrar a chave secreta usando $A^B \ (mod\ 23)$ e Alice com o número de Bob terá de usar $B^A \ (mod\ 23)$, vamos aos cálculos, de Bob e Alice:

Bob:
$4^2 \ (mod\ 23) = 16 \ (mod\ 23) => \dfrac{16}{23} = 0$ inteiros $(0 * 23 = 0)$ então $16 - 0 = 16$.

Alice:
$3^6 \ (mod\ 23) = 729 \ (mod\ 23) => \dfrac{729}{23} = 31$ inteiros $(31 * 23 = 713)$ então $729 - 713 = 16$.

Observe que chegaram ao mesmo número, ou seja a chave secreta é 16.

O processo de envio de mensagem será praticamente o mesmo que o que veremos na seção seguinte.

6.3 Criptografia RSA

Vejamos como ela funciona, Alice e Bob continuam querendo trocar mensagens, e Eve continua querendo lê-las, então Alice deverá enviar as mensagens cifradas para Bob. Com o uso novamente da aritmética modular, a troca de mensagens é feita agora com o uso de uma chave pública.

Então Bob escolhe dois grandes números primos p e q e calcula $N = p.q$ e depois calcula $\varphi(N) = (p-1)(q-1)$ e escolhe um ϵ co-primo de $\varphi(N)$, ou seja, mdc (ϵ, $\varphi(N)$)=1 e calcula d tal que $L = d.\epsilon$.

Suponhamos que Bob tenha escolhido $p = 5$ e $q = 13$ então $N = 65$ e $\epsilon = 7$, Bob divulga N e ϵ (chave pública) e para cifrar a mensagem deve converter a mensagem para um número M, que depois será cifrado para C, de modo que: $C = M^{\epsilon}$ (mod N).

Agora suponha que Alice queira enviar uma mensagem para Bob, e a mensagem seja Ola.

Utilizando os números binários e a Tabela ASCII, temos:

Ola [79 108 61] ou [01001111 01101100 01100001], onde

O [em ASCII = 01001111, binário = 79 decimal]

l [em ASCII = 01101100, binário = 108 decimal]

a [em ASCII = 01100001, binário = 61 decimal]

Para cifrar a mensagem Alice precisa da chave pública de Bob, e ela já sabe $N = 65$ e $\epsilon = 7$, assim, $C_1 = 79^7$ (mod 65) e usando a aritmética modular temos que:

79^7 (mod 65) = [79^4 (mod 65) x 79^2 (mod 65) x 79^1 (mod 65)] (mod 65) onde

79^1= 79 => 14 (mod 65)

79^2= 6241 => $\frac{6241}{65}$=96 => 96 x 65 = 6240 = 1 (mod 65)

79^4= 38950081 => $\frac{38950081}{65}$ = 599232 => 599232 x 65 = 38950080 = 1 (mod 65)

Portanto, $79^7 = 14 \pmod{65}$ e assim $C_1 = 14$.

$C_2 = 108^7 \pmod{65} = [108^4 \pmod{65}$ x $108^2 \pmod{65}$ x $108^1 \pmod{65}] \pmod{65}$ onde $108^1 = 108 = 43 \pmod{65}$

$108^2 = 11664 => \frac{11664}{65} = 179 => 179$ x $65 = 11635 = 29 \pmod{65}$

$108^4 = 136048896 => \frac{136048896}{65} = 2093059 => 2093059$ x $65 = 136048835 =$
$108^4 = 61 \pmod{65}$

$108^7 = 76067 \pmod{65} => \frac{76067}{65} => 1170$ x $65 = 76050 = 17 \pmod{65}$, assim
$C_2 = 17$.

Utilizamos o mesmo processo para obter C_3:
$C_3 = 61^7 \pmod{65} = [61^4 \pmod{65}$ x $61^2 \pmod{65}$ x $61^1 \pmod{65}] \pmod{65}$, então
$61^7 = 256 \pmod{65} = 61 \pmod{65} =$ - $4 \pmod{65}$, ou seja, $C_3 =$ - 4.

Portanto Alice envia para Bob: $C_1 = 14$, $C_2 = 17$ e $C_3 =$ - 4, ou seja, 00001110 00010001 00011101.

Como a Bob conhece ϵ, p e q ele calcula d usando $\epsilon * d = 1 \pmod{((p-1)(q-1))}$, ou seja,
7*d = 1 (mod 4*12) = 1 (mod 48) assim d=$\frac{49}{7}$=7, portanto $d = 7$.

Assim para decifrar a mensagem de Alice, Bob usa $M = C^d \pmod{65}$, então:
$M_1 = C_1^d \pmod{65} = 14^7 \pmod{65} = 14 \pmod{65}$, assim $M_1 = 65 + 14 = 79 =>$ O
$M_2 = C_2^d \pmod{65} = 17^7 \pmod{65} = 43 \pmod{65}$, assim $M_2 = 65 + 43 = 108 =>$ l
$M_3 = C_3^d \pmod{65} = -4^7 \pmod{65} =$ - $4 \pmod{65}$, assim $M_3 = 65 +$ (- 4) $= 61 =>$ a

Portanto $M_1 = 79 =>$ O, $M_2 = 108 =>$ l e $M_3 = 61 =>$ a, ou seja: Ola.

Porém com o avanço dos computadores, o processo de fatoração de grandes números não levará mais tanto tempo e será necessário também avanços na criptografia.

6.4 O Princípio da Superposição de Estados - Um salto para a Criptografia Quântica

O princípio de superposição de estados nos diz que os estados de um sistema podem ser adicionados de forma a produzir um novo estado. Uma grandeza matemática que satisfaz essa condição é o vetor. Em outras palavras: Dados dois estados admissíveis de um sistema quântico, então a soma desses dois estados também é um estado admissível do sistema, assim temos o seguinte estado

$$|\psi >= \frac{1}{\sqrt{2}}|\psi_A > + \frac{i}{\sqrt{2}}|\psi_B >$$

É desejável ter um nome especial para descrever os vetores, o qual são conectados com os estados do sistema na mecânica quântica, que chamaremos de kets, e denotaremos geralmente por um símbolo especial $| >$ como já foi mencionado em capítulos anteriores, assim como foi visto no capítulo 2, na Figura (2.2) a difração luminosa e interferência também foi observada com fótons e elétrons, para explicar tal fenômeno de como apenas um fóton tenha passado por duas fendas físicos recorreram a física quântica e presumem que o fóton tenha passado pelas duas fendas ao mesmo tempo, onde cada possibilidade é chamada de *estado* e como o fóton preenche as duas possibilidades como se estivesse se dividido em dois *fótons fantasmas* diz-se que se encontra em uma *superposição de estados*, isso ocorre quando não sabemos o que acontece, como no caso do *Gato de Schrödinger* parábola inventada por Erwin Schrödinger, ganhador do Prêmio Nobel de física em 1933, resumidamente, o gato esta dentro de uma caixa e pode estar vivo ou morto, no inicio sabemos que esta vivo, ao colocarmos um vidro com veneno dentro da caixa e fecharmos a caixa, não podemos ver o gato e saber se esta vivo ou morto, mas de acordo com a teoria quântica o gato se encontra vivo e morto ao mesmo tempo, o que satisfaz ambas as possibilidades então uma superposição de estados que termina quando vemos o gato.

6.5 Criptografia Quântica e a Distribuição Quântica de Chaves

A criptografia quântica trata-se de um novo método para comunicações secretas que oferece garantia de segurança máxima por ser fundamentado na inviolabilidade de uma lei

da natureza "O Princípio de Incerteza de Heisenberg". Esta seção foi baseada no artigo publicado em 1992 pela Scientific American (5) e será discutida a criptografia quântica, e a execução do protocolo quântico BB84 criado por Charles Bennett e Gilles Brassard em 1984, para a geração de uma chave criptográfica segura.

A criptografia quântica permite que Alice e Bob escolham uma chave secreta segura sem jamais terem se encontrado, desde que o sinal seja um objeto quântico, além disso precisamos de um canal de comunicação seguro. Este canal de comunicação suporta o envio e recebimento de fótons orientados na horizontal, vertical ou inclinado, para a direita, esquerda, para baixo ou para cima. Assim Alice envia os fótons com as suas devidas orientações e Bob tem que decidir como detectar os fótons enviados pela Alice. Alice pode enviar bits a Bob usando o código representado na Tabela (6.1).

Tabela 6.1: *Conversão de bits para estados quânticos*

Estado de polarização do fóton	Bits	Orientação da Polarização	Base
Fóton vertical	1	↕	A
Fóton horizontal	0	↔	A
Fóton inclinado para esquerda	1	↘	B
Fóton inclinado para direita	0	↙	B

A Distribuição Quântica de Chaves também é baseada nas Leis da Mecânica Quântica, e no fenômeno da polarização. A Figura (6.6) representa uma fonte não polarizada passando por um filtro polarizador o qual absorve uma certa quantidade de luz e polariza o restante na direção vertical. O segundo filtro absorve uma certa quantidade de luz polarizada e polariza o restante na direção formada pelo ângulo α.

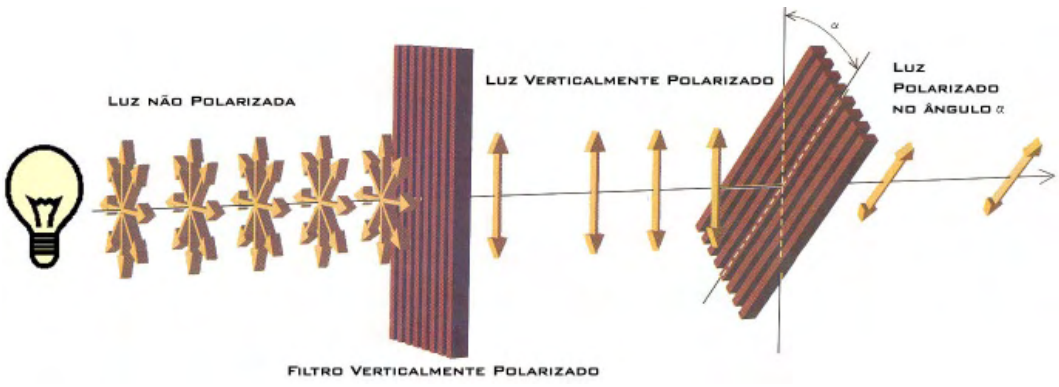


Figura 6.6: *Fonte não polarizada e filtros polarizadores (5)*

Enquanto viajam, fótons vibram em alguma direção: para cima e para baixo, para a direita e para a esquerda, ou mais provavelmente em algum ângulo, os filtros polarizadores permitem que apenas fótons polarizados numa mesma direção passem, os outros são bloqueados. Mas na mecânica quântica, cada partícula tem uma probabilidade de repentinamente trocar sua polarização e ficar com a mesma do filtro. Se os ângulos diferirem de 90 graus, a probabilidade é zero. Se diferirem de 45 graus, a probabilidade é de 50%.

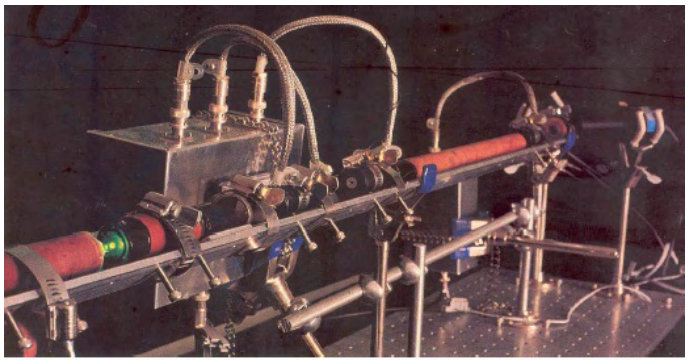


Figura 6.7: *Protótipo de um sistema de criptografia quântica (5)*

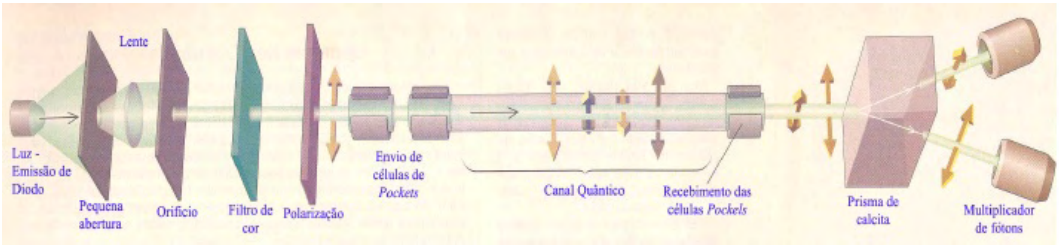


Figura 6.8: *Representação experimental de um sistema de criptografia quântica (5)*

Se um fóton está polarizado em uma base (vertical, horizontal, inclinada), e medirmos nesta base descobrimos qual a sua polarização, senão obtemos um resultado aleatório.

Utilizaremos esta propriedade para gerar uma chave secreta entre Alice e Bob:

1 > Alice escolhe os bits que quer enviar ao Bob, suponha que seja:

$$1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0.$$

2 > Alice escolhe a base na qual irá transmitir seus bits, retilinear ($\oplus$) ou diagonal ($\otimes$), ela escolhe:

$$+\ |\ +\ |\ \times\ |\ +\ |\ \times\ |\ \times\ |\ +\ |\ +\ |\ +\ |\ \times\ |\ \times\ |\ \times\ |\ \times\ |\ +\ |\ \times\ |\ \times$$

3 > Alice então envia para Bob uma seqüência de fótons, polarizados aleatoriamente.

A representação por *kets* dos bits enviado por Alice ao Bob seria:
$|1>_A |1>_A |0>_B |0>_A |1>_B |0>_B |1>_A |0>_A |1>_A |1>_B |0>_B |1>_B |1>_B$
$|1>_A |1>_B |0>_B$, note que:

$$|1>_A = (\frac{1}{\sqrt{2}})(|0>_B - |1>_B),$$

$$|0>_A = (\frac{1}{\sqrt{2}})(|0>_B + |1>_B),$$

$$|1>_B = (\frac{1}{\sqrt{2}})(|0>_A - |1>_A),$$

$$|0>_B = (\frac{1}{\sqrt{2}})(|0>_A + |1>_A).$$

4 > Bob tem um detector de polarização, então, ele escolhe a base que utilizará para detectar os fótons, de maneira retilinear ($\oplus$) ou diagonal ($\otimes$), assim como Alice:

5 > Bob não sabe se acertou ou errou, mas obteve:

6 > Bob e Alice, por um canal inseguro, abrem o jogo de como configuraram suas bases e comparando as bases consideram apenas os resultados que utilizaram a mesma base, ou seja, apenas as polarizações medidas corretamente.

7 > Utilizando o código pré-combinado da Tabela (6.1), eles têm agora uma seqüência aleatória de bits que poderá ser usada como chave:

8 > Assim, eles obtiveram: 1 1 1 1 0 1 1 1 0.

Com esses procedimentos Bennett e Brassard (5) superaram os problemas da distribuição em segurança da série aleatória da cifra de uma única vez. E como Bob e Alice conseguiram montar um bloco de uma única vez, a cifra passou a ser absolutamente inquebrável, como prevê as leis da física quântica, e Eve não conseguirá interceptá-la sem que seja descoberta.

Dessa forma, Alice e Bob geraram 9 bits. Eles podem gerar quantos bits quiserem usando este esquema. Em média, Bob acerta a polarização 50% das vezes, então Alice tem que enviar $2.n$ fótons para gerar uma chave de n bits. Agora, vem a parte mais interessante, porque Eve não consegue espionar passivamente?

Assim como Bob, Eve tem que escolher uma polarização para detectar os fótons de Alice, e assim como Bob, metade das suas escolhas estarão erradas. Como erros trocam a polarização dos fótons, ela introduz erro na comunicação. Dessa forma Alice e Bob terminarão com seqüências de bits diferentes. Para verificar se ouve espionagem, Alice e Bob finalizam o protocolo da seguinte forma:

9 > Alice e Bob revelam parte dos resultados, por exemplo os três primeiros, publicamente, se coincidirem podem utilizar os fótons restantes como chave. Se houver discrepância, eles sabem que estão sendo monitorados, e terão de refazer o procedimeto.

Alice e Bob podem criar uma longa série de zeros e uns, repetindo o processo várias vezes.

A criptografia quântica acabaria com a batalha entre os criadores e os quebradores de código, pois não existe espionagem passiva no mundo quântico. Se Eve tentar receber todos os bits ela vai obrigatoriamente interferir nas comunicações, mas se algum dia for quebrada, significaria falhas na teoria quântica, voltando os estudos do universo ao nível fundamental. O desafio no momento tem sido construir um sistema criptográfico quântico que funcione em grandes distâncias. Já se conseguiu a transmissão por fibra ótica por 40 quilômetros, mas pelo ar ainda é um problema, pois as moléculas de ar interagem com os fótons e mudam sua polarização. O objetivo seria a transmissão via satélite.

De acordo com Singh (24) fica a pergunta: "Será que a criptografia quântica chegará a tempo de nos salvar da ameaça dos computadores quânticos?"

Capítulo 7

Entropia e Emaranhamento

Para o estudo do emaranhamento, usaremos uma medida que cresce com o aumento do emaranhamento, e que chamamos de *entropia*.

7.1 Entropia

Shannon (13) diz que "informação é uma redução de incerteza oferecida quando se obtém resposta a uma pergunta". No desenvolvimento de uma teoria da comunicação que pudesse ser utilizada por engenheiros eletricistas na projeção de melhores sistemas de telecomunicação, Shannon definiu uma medida chamada de entropia, definida como:

$$S(X) \equiv S(p_1, p_2, ..., p_n) \equiv -1 \sum_{i}^{W} p_i \, log_2 \, p_i \tag{7.1}$$

que determina o grau de caoticidade da distribuição de probabilidade p_i e a capacidade do canal de comunicação[1] necessária para transmitir a informação associada a uma distribuição clássica de probabilidade.

A entropia de um sistema binário (S_B), que apresenta apenas dois estados possíveis com probabilidades p e $q = 1 - p$, pode ser representada como uma função de p,

$$S_B(p) \equiv S_B(p, 1-p) \equiv -p \, log_2 \, (p) - (1-p) \, log_2 \, (1-p)$$

7.1.1 Entropia de Von Neumann

Tem conceito análogo a Entropia de Shannon, porém para a mecânica quântica. Definimos a Entropia de Von Neumann do estado associado a ρ (*operador densidade*) por:

[1] Canal de comunicação, designa o meio usado para transportar uma mensagem do emissor ao receptor.

$$S(\rho) \equiv -Tr(\rho \, log_2 \, \rho) \tag{7.2}$$

ou ainda, se λ_x são os autovalores de ρ pode ser descrita por:

$$S(\rho) = -\sum_x \lambda_x \, log_2 \, \lambda_x, \tag{7.3}$$

onde

$$\rho(t) = |\psi(t) >< \psi(t)|$$

e

$$\rho^\dagger = \rho(t), \quad \rho(t) = \rho^2(t), \quad \text{e} \quad Tr\rho^2(t) = 1 \tag{7.4}$$

são propriedades válidas.

Teorema: Propriedades básicas da entropia de Von Neumann, (1):

1. *A entropia de Von Neumann é não-negativa. A entropia é zero se, e somente se, o estado é puro.*

2. *Num espaço d-dimensional de Hilbert a entropia é no máximo log d. Este valor é atingido se, e somente se, o sistema é um estado de mistura máxima,* $\frac{I}{d}$. *(Sabendo que* $0 \leqslant S(\rho \| I/d) = -S(\rho) + log_2 d$*)*

3. *Se um sistema composto AB estiver em um estado puro, resulta que* $S(A) = S(B)$.

4. *Suponha que* p_i *são probabilidades e que os operadores densidade* ρ_i *têm suporte em subespaços ortogonais. Então*

$$S\left(\sum_i p_i \rho_i\right) = H(p_i) + \sum_i p_i \, S(\rho_i). \tag{7.5}$$

5. *Sejam* p_i *probabilidades,* $|i >$ *estados ortogonais de um sistema A, e* ρ_i *qualquer conjunto de operadores densidade de um sistema B. Resulta que*

$$S\left(\sum_i p_i \, |i >< i| \otimes \rho_i\right) = H(p_i) + \sum_i p_i \, S(\rho_i), \tag{7.6}$$

conhecida também como teorema da entropia conjunta.

7.1.2 Entropia de Tsallis

A entropia Tsallis é uma possível generalização da entropia de Boltzmann/Gibbs/Shannon, se adapta as características físicas de muitos sistemas físicos e ainda preserva as propriedades fundamentais da entropia na segunda lei da termodinâmica. Além de poder ser utilizada como uma medida de informação adequada para a utilização em sistemas de informação que apresentam características não extensivas.

$$S_q \equiv k \sum_i^W p_i^q . \frac{(1 - p_i^{1-q})}{q-1} \tag{7.7}$$

ou ainda

$$S_q = k \frac{1 - \sum_i^W p_i^q}{q-1} \tag{7.8}$$

onde k é uma constante positiva (a qual é atribuído o valor unitário), q é um número real, W é o número total de microestados e p_i é o conjunto de probabilidades associado aos estados.

Teorema: Propriedades básicas da entropia de Tsallis, (9):

1. *S_q é contínua em p_i, para $0 < p_i < 1$.*

2. *Para um conjunto W de eventos equiprováveis, ou seja, $p_i = \frac{1}{W}$, então S_q é uma função monotônica crescente.*

3. *Para dois subsistemas estatisticamente independentes A e B a entropia generalizada S_q do sistema composto $A + B$ satisfaz a relação de pseudo-aditividade*

$$S_q(A + B) = S_q(A) + S_q(B) + (1 - q)\, S_q(A)\, S_q(B) \tag{7.9}$$

7.2 O emaranhamento

O emaranhamento[2] é tido como o recurso essencial para o processamento da informação quântica, vários protocolos envolvendo o fenômeno do emaranhamento já foram reportados, incluindo um experimento de teleporte de estado quântico[3]. A idéia de emaranhamento surge, quando dois ou mais sistemas quânticos interagem e o estado final de um deles pode depender do estado final dos outros.

O conceito de emaranhamento é definido como uma qualidade de todo estado físico que não pode ser representado como um produto tensorial simples dos elementos dos espaços de Hilbert multiplicados (34).

Diz-se que um subsistema é emaranhado quando a matriz densidade do subsistema não for de um estado puro, ou seja:

$$\psi_{ab} \neq |\psi_a > \otimes |\psi_b > \tag{7.10}$$

Para verificarmos se existe o emaranhamento ou se o estado é puro, considere um sistema com duas componentes em um estado total puro:

$$\rho_{ab} \neq |\psi_{ab} >< \psi_{ab}| \tag{7.11}$$

Por exemplo: suponha que um estado de 1-*qubit* pode ou não ser o resultado do produto tensorial de estados de 1-qubit. Considere os estados de 1-*qubit*:

$$|\varphi >= a|0 > +b|1 > \quad \text{e} \quad |\psi >= c|0 > +d|1 >, \tag{7.12}$$

onde a, b, c e $d \in C$. Lembrando que $|ij >= |i > \otimes |j >$, então o estado definido pelo produto tensorial de $|\varphi >$ e $|\psi >$ é

$$|\varphi > \otimes |\psi >= (a|0 > +b|1 >) \otimes (c|0 > +d|1 >) = ac|00 > +ad|01 > +bc|10 > +bd|11 > \tag{7.13}$$

[2]Emaranhamento, entrelaçamento quântico ou princípio de correspondência quântica (terminologia usada por Bohm (15)), é um fenômeno da mecânica quântica que permite que dois ou mais objetos, mesmo que separados espacialmente, estejam de alguma forma tão ligados que um objeto não pode ser corretamente descrito sem mencionar sua contra-parte (33).

[3]Teleporte quântico também conhecido como teletransporte quântico é uma tecnologia que permite a transferência da informação quântica, como o *spin* ou polarização, sem passagem por um meio físico entre os pontos inicial e final (50).

Observando um estado de 2-*qubits* genéricos como na equação (3.4) é da forma da equação (7.13) se, e somente se,
$\alpha_{00} = ac$, $\alpha_{01} = ad$, $\alpha_{10} = bc$ e $\alpha_{11} = bd$.

Destas igualdades temos $\frac{\alpha_{00}}{\alpha_{01}} = \frac{c}{d}$ e $\frac{\alpha_{10}}{\alpha_{11}} = \frac{c}{d}$, assim $\alpha_{00}.\alpha_{11} = \alpha_{01}.\alpha_{10}$.

Logo, um estado de 2-*qubits*, em geral, não é o produto tensorial de estados de 1-*qubit*, então diz-se que o estado está emaranhado.

Pela definição de operador densidade, sabemos que $\rho(a) = Tr_b\rho$ e que $\rho(b) = Tr_a\rho$, $\rho(a)$ é necessariamente puro quando

$$Tr_b[|\psi_b><\psi_b|] = 1 \tag{7.14}$$

nos leva a

$$\rho(a) = |\psi_a><\psi_a| \tag{7.15}$$

assim quando

$$Tr\ \rho^2_{a(b)}(t) \tag{7.16}$$

são mínimos, o estado é de máximo emaranhamento.

Para quem se interessar por algo mais completo e complexo: *Emaranhamento: caracterização, manipulação e conseqüências (34).*

7.3 Emaranhamento no divisor de feixe

O divisor de feixes[4] efetua uma transformação linear do vetor com amplitudes de entrada em amplitudes de saída. Assim, quando um único fóton se aproxima de um divisor de feixe, a onda se divide em dois: uma parte é refletida e a outra é transmitida. O fóton fica então em superposição entre duas trajetórias diferentes.

Observando a Figura (7.1), considere que os operadores pertencem ao espaço de Hilbert, o campo de entrada descrito pelo operador a, cujo operador de saída é c, é superposto

[4]Um divisor de feixe é um espelho com um revestimento reflexivo muito fino. Dessa forma, nem toda luz é refletida, sendo alguma transmitida através do espelho; ele atua como um anteparo de cristal, onde a entrada do feixe de luz, nos leva a uma saída de estados emaranhados.

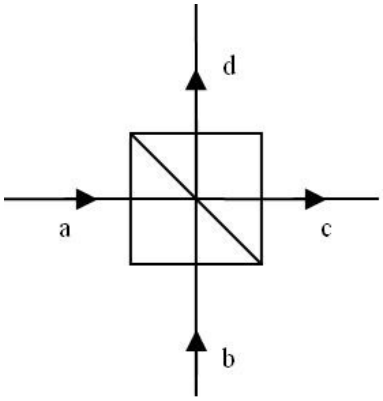


Figura 7.1: Configuração da operação de um divisor de feixe

com o campo de entrada b, cujo o operador de saída é d, onde os coeficientes de reflexão (R) e transmissão (T) com $R^2 + T^2 = 1$. Os operadores do campo de saída são:

$$c = BaB^\dagger \quad \text{e} \quad d = BbB^\dagger \tag{7.17}$$

onde

$$B = e^{i\phi_0} \begin{pmatrix} \cos\theta e^{i\phi_T} & \sin\theta e^{i\phi_R} \\ -\sin\theta e^{-i\phi_R} & \cos\theta e^{-i\phi_T} \end{pmatrix} \tag{7.18}$$

com $T = cos\frac{\theta}{2}$, $R = sen\frac{\theta}{2}$ e ϕ a diferença de fase entre os campos refletido e transmitido. Assim

$$c = BaB^\dagger = e^{\theta/2\,(a^\dagger b e^{i\phi} - a b^\dagger e^{i\phi})} a\, e^{-\theta/2\,(a^\dagger b e^{i\phi} - a b^\dagger e^{-i\phi})} \tag{7.19}$$

levando em conta que

$$e^A B e^{-A} = B + [A,B] + \frac{1}{2!}[A,[A,B]] + \frac{1}{3!}[A,[A,[A,B]]] + ...$$

temos

$$c = BaB^\dagger = a + \frac{\theta}{2}[(a^\dagger b e^{i\phi} - a b^\dagger e^{i\phi}), a] + \frac{1}{2!}\left(\frac{\theta}{2}\right)^2 [(a^\dagger b e^{i\phi} - a b^\dagger e^{i\phi}), [(a^\dagger b e^{i\phi} - a b^\dagger e^{i\phi}), a]] + ...$$

Portanto $c = a\ \cos(\theta/2) - b\ e^{i\theta}\ \sin(\theta/2) = T\,a - R\,e^{i\theta}\,b$ e de maneira análoga chegamos em $d = T\,b + R\,e^{-i\theta}\,a$.

Para dois estados de entrada *(estados de Fock)* independentes $|n_1 n_2> = |n_1>_a\,|n_2>_b$ a superposição destes será o estado de saída $|\psi>$, dado por

$$|\psi> = B|n_1 n_2> = \sum_{N_1 N_2} < N_1 N_2|B|n_1 n_2 > |N_1 N_2> = \sum_{N_1 N_2} B^{N_1 N_2}_{n_1 n_2} |N_1 N_2> \tag{7.20}$$

onde

$$B_{n_1n_2}^{N_1N_2} = e^{-i\theta(n_1-N_1)} \sum_{k=0}^{n_1}\sum_{l=0}^{n_2}(-1)^{n_1-k} R^{n_1+n_2-k+l} T^{k+l} \frac{\sqrt{n_1!n_2!N_1!N_2!}}{k!(n_1-k)!l!(n_2-l)!}\times$$
$$\times\delta_{N_1,n_2+k-l}\delta_{N_2,n_1-k+l} \tag{7.21}$$

utilizando a equação (2.91) ou (2.92) e fazendo algumas substituições e sabendo que δ é a função de kronecker, chegamos finalmente em

$$B|n_1>_a |n_2>_b =$$
$$= \sum_{k=0}^{n_1}\sum_{l=0}^{n_2} \frac{(-1)^{n_1-k} e^{-i\theta(n_1N_1)} R^{n_1+n_2-k+l} T^{k+l} \sqrt{n_1!n_2!(n_2+k-l)(n_1-k+l)}}{k!(n_1-k)!l!(n_2-l)!}\times$$
$$\times|n_2+k-l, n_1-k+l> \tag{7.22}$$

E assim para o operador densidade reduzido $\rho_c = Tr_d\, B|n_1n_2><n_1n_2|\, B^\dagger$ temos:

As entropias de Von Neumann ($S(\rho_c)$) e de Tsallis ($S_q(\rho_c)$):

$$S(\rho_c) = -\sum_{N_1N_2} |B_{n_1n_2}^{N_1N_2}|^2\, ln\, |B_{n_1n_2}^{N_1N_2}|^2 \tag{7.23}$$

$$S_q(\rho_c) = \frac{1}{q-1}\left(1 - \sum_{N_1N_2} |B_{n_1n_2}^{N_1N_2}|^{2q}\right) \tag{7.24}$$

Capítulo 8

Os resultados

Neste capítulo faremos uma analise do comportamento da Entropia de Von Neumann ($S(\rho_c)$) e de Tsallis ($S_q(\rho_c)$) em função do índice entrópico q tal que com $0 \leqslant q < 1$ conseguimos detectar variações na correlação das variáveis. Para nossos testes ou medições, usaremos $q = 1$ na entropia de Von Neumann e q variando em $0,3$, $0,5$ e $0,8$ para a entropia de Tsallis. A escolha é aleatória para esses índices entrópicos.

Observação: Todos os gráficos e/ou figuras apresentados neste capítulo referem-se a medida do emaranhamento de determinado número de fótons de entrada, em função da amplitude de reflexão.

Observação: Os resultados foram obtidos usando vários computadores diferentes, com sistemas operacionais diferentes (Mac OS X versão 10.4.11, Windows 2000, Windows XP), com processadores diferentes (Intel Core 2 Duo (2 GHz), Intel Pentium 4 (3.2 GHz), Intel Core 2 Quad (2.33 GHz)), com memória RAM diferentes e versões de softwares diferentes (Mathematica 7.0.0 for Mac OS X, Matlab 7.6.0.324 (R2008a) for Mac OS X, Mathematica 5.2 for Windows e Matlab 7.4.0 (R2007a) for Windows).

Tomando $r = \sqrt{R}$ e $t = \sqrt{1 - r^2}$ como visto no capítulo anterior, e os fótons de entrada como sendo $n_1 = a$ e $n_2 = b$ e os de saída $N_1 = n_2 + k - l = c$ e $N_2 = n_1 - k + l = d$.

Desenvolvendo a equação (7.23) de Von Neumann temos:

$$S = -\sum_{c=0}^{a+b}\sum_{d=0}^{a+b}(|\sum_{k=0}^{a}\sum_{l=0}^{b}((-1)^{a-k}\ r^{a+b-k-l}\ t^{k+l}\frac{\sqrt{a!b!c!d!}}{k!(a-k)!l!(b-l)!}\ \delta_{c,b+k-l}\ \ \delta_{d,a-k+l})|^2)*$$

$$*\ log_2\ [|\sum_{k=0}^{a}\sum_{l=0}^{b}((-1)^{a-k}\ \ r^{a+b-k-l}\ t^{k+l}\frac{\sqrt{a!b!c!d!}}{k!(a-k)!l!(b-l)!}\ \delta_{c,b+k-l}\ \delta_{d,a-k+l})|^2 + 1\times 10^{-29}] \tag{8.1}$$

E para a equação (7.24) de Tsallis:

$$S_q = \frac{1}{q-1}(1 - \sum_{c=0}^{a+b}\sum_{d=0}^{a+b}(|\sum_{k=0}^{a}\sum_{l=0}^{b}((-1)^{a-k}\ r^{a+b-k-l}\ t^{k+l}\frac{\sqrt{a!b!c!d!}}{k!(a-k)!l!(b-l)!}\ \delta_{c,b+k-l}\ \delta_{d,a-k+l})|^{2q})) \tag{8.2}$$

As equações (8.1) e (8.2) foram as implementadas nos testes de emaranhamento realizados usando programas no Mathematica® e no Matlab®.

8.1 Única Entrada

Injetamos fótons em apenas uma das entradas do divisor de feixe, e obtemos os seguintes gráficos para $n_1 = a = 10$ e $n_2 = b = 0$, usando o Mathematica® (Figura 8.1) e usando o Matlab® (Figura 8.2).

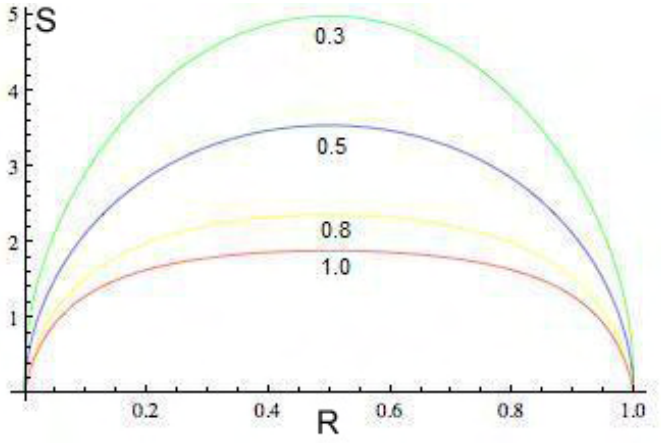


Figura 8.1: *Entropia para entradas de* $a = 10$ *e* $b = 0$ *fótons, com Mathematica®*

Comparando os gráficos (8.1) e (8.2) com os gráficos obtidos por (18), usando um outro programa, não encontramos nenhuma diferença. Porém, percebemos que os testes com o Matlab® demoram muito; para se ter uma idéia da diferença de tempo, o Mathematica® levou menos de 1 minutos, enquanto que o Matlab® demorou mais de 1 hora para a mesma

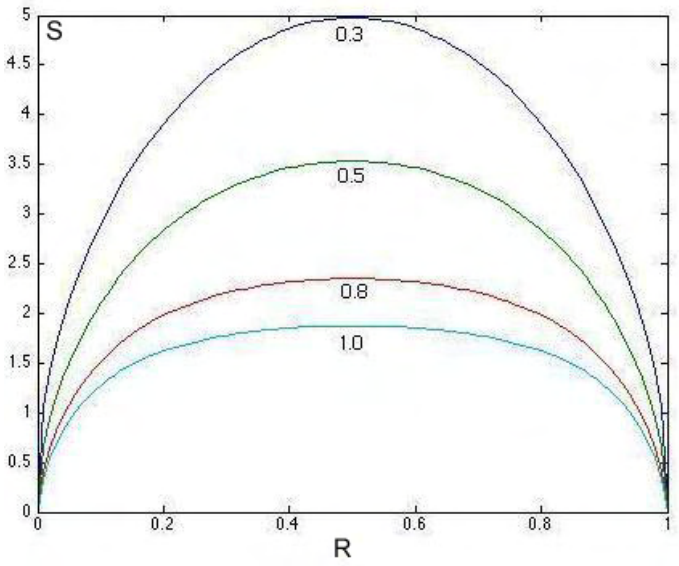


Figura 8.2: *Entropia para entradas de* $a = 10$ *e* $b = 0$ *fótons, com Matlab®*

quantidades de fótons de entrada, devido ao tempo gasto, os testes com o Matlab® foram suspensos.

Continuamos a injetar fótons em uma única entrada, porém com valores de entrada maior $a = 100$ e $b = 0$ na Figura (8.3), na Figura (8.4) com entrada de $a = 200$ e $b = 0$ e na Figura (8.5) com entrada de $a = 500$ e $b = 0$ todos usando o Mathematica®.

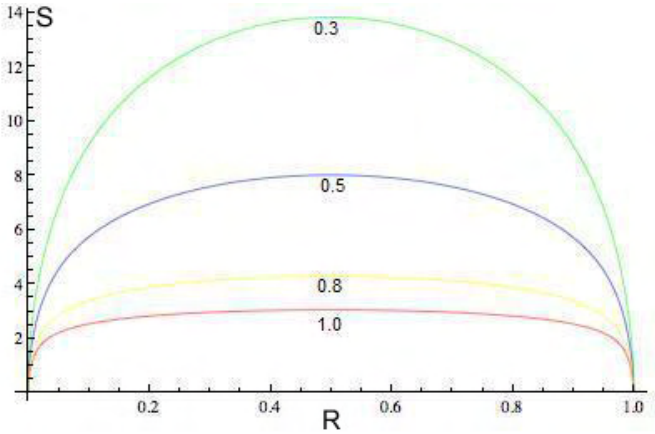


Figura 8.3: *Entropia para entradas de* $a = 100$ *e* $b = 0$ *fótons, com Mathematica®*

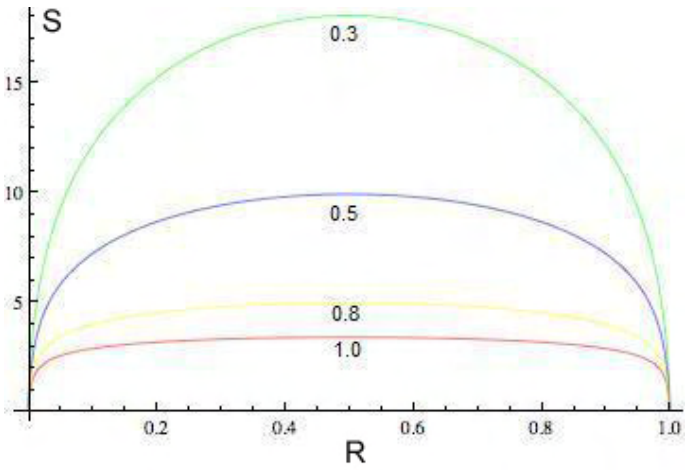


Figura 8.4: *Entropia para entradas de* $a = 200$ *e* $b = 0$ *fótons, com Mathematica®*

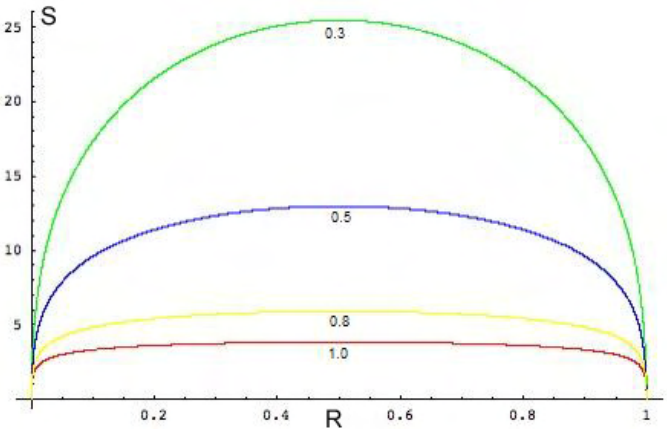


Figura 8.5: *Entropia para entradas de* $a = 500$ *e* $b = 0$ *fótons, com Mathematica®*

Percebe-se em todas as Figuras (8.1, 8.2, 8.3, 8.4 e 8.5), que em ambas as entropias, mesmo para um número de fótons de entrada muito maior, nos mostram que o grau de emaranhamento é uma função convexa com máximo em $r = 0,5$.

8.2 Entradas Iguais

Nesta seção estão os testes com a injeção do mesmo número de fótons nas entradas do divisor de feixe.

Injetamos o mesmo número de fótons em ambas entradas do divisor de feixe, e obtemos os seguintes gráficos para $n_1 = a = 5$ e $n_2 = b = 5$, usando o Mathemathica® (Figura 8.6) e usando o Matlab® (Figura 8.7).

O tempo de desempenho, também nesse caso, foi muito maior com o uso do Matlab®,

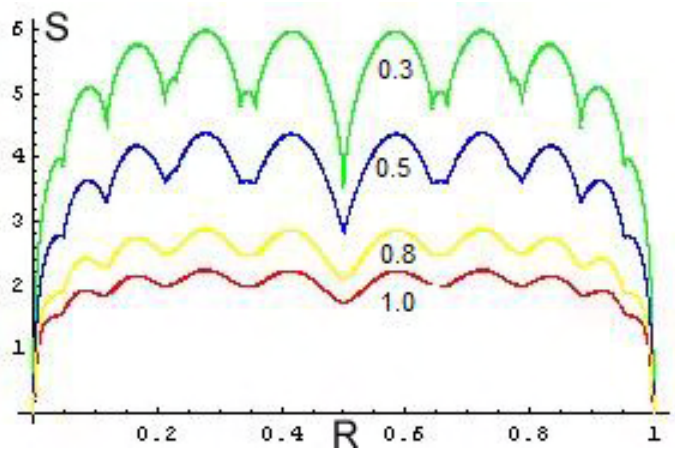


Figura 8.6: *Entropia para entradas de* $a = 5$ *e* $b = 5$ *fótons, com Mathematica®*

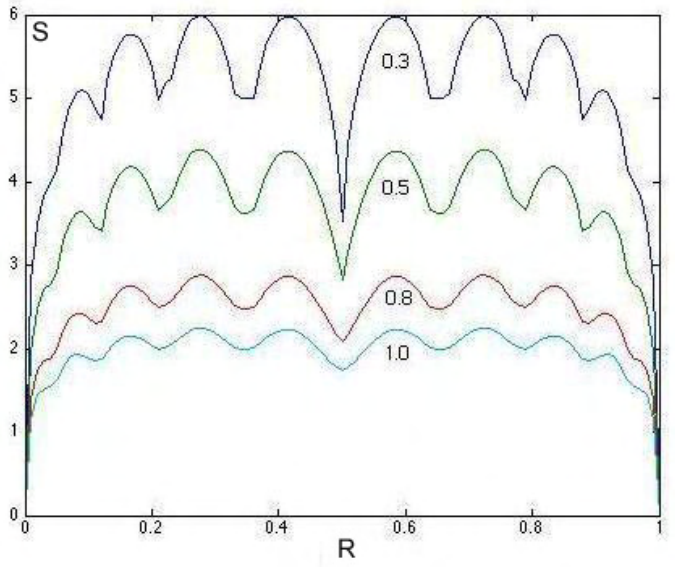


Figura 8.7: *Entropia para entradas de* $a = 5$ *e* $b = 5$ *fótons, com Matlab®*

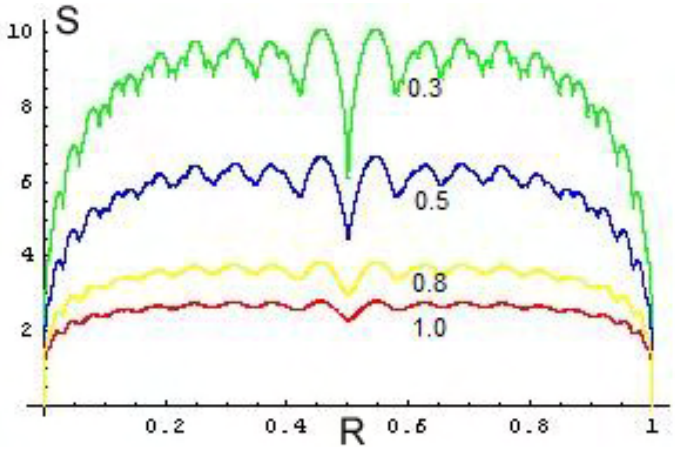


Figura 8.8: *Entropia para entradas de* $a = 10$ *e* $b = 10$ *fótons, com Mathematica®*

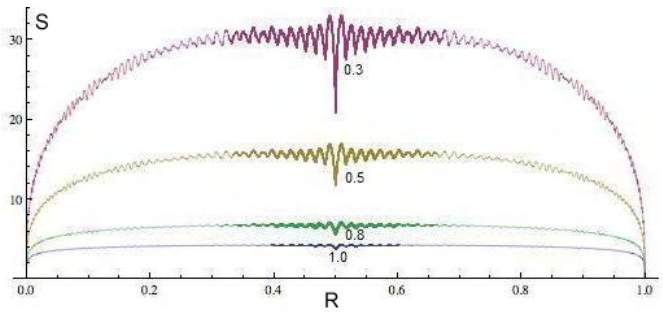


Figura 8.9: *Entropia para entradas de* $a = 50$ *e* $b = 50$ *fótons, com Mathematica®*

sendo o Mathematica® bem mais rápido, embora para muitos fótons na entrada do divisor de feixes tenha demorado alguns dias.

Nos gráficos ((8.6), (8.7), (8.8), (8.9)) em que o número de fótons de entrada são iguais, nota-se uma queda do emaranhamento em função da amplitude de reflexão, assim temos que o grau de emaranhamento é mínimo em $r = 0,5$, para ambas as Entropias.

Observando agora, o gráfico (8.10) cujo as entradas foram maiores, observamos que para a Entropia de Tsallis o máximo emaranhamento ainda ocorre em $r \sim 0,5$, entretanto para a Entropia de Von Neumann em $r = 0,5$, temos agora o mínimo emaranhamento.

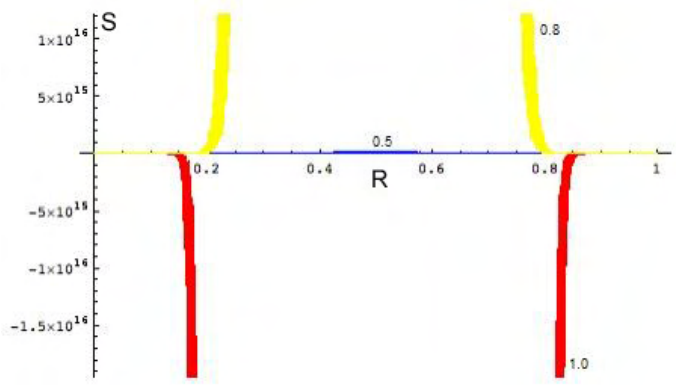


Figura 8.10: *Entropia para entradas de* $a = 100$ *e* $b = 100$ *fótons, com Mathematica®*

8.3 Entradas com diferentes números de fótons

Injetamos diferentes números de fótons em cada uma das entradas do divisor de feixe, e obtemos os seguintes gráficos para $n_1 = a = 3$ e $n_2 = b = 7$, usando o Mathematica® (Figura 8.11) e usando o Matlab® (Figura 8.12).

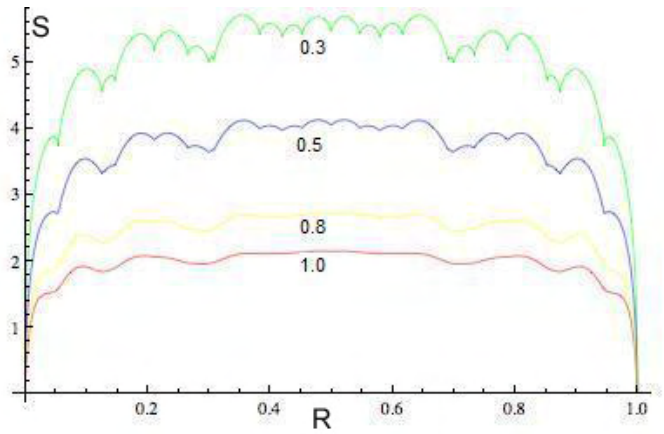


Figura 8.11: *Entropia para entradas de* $a = 3$ *e* $b = 7$ *fótons, com Mathematica®*

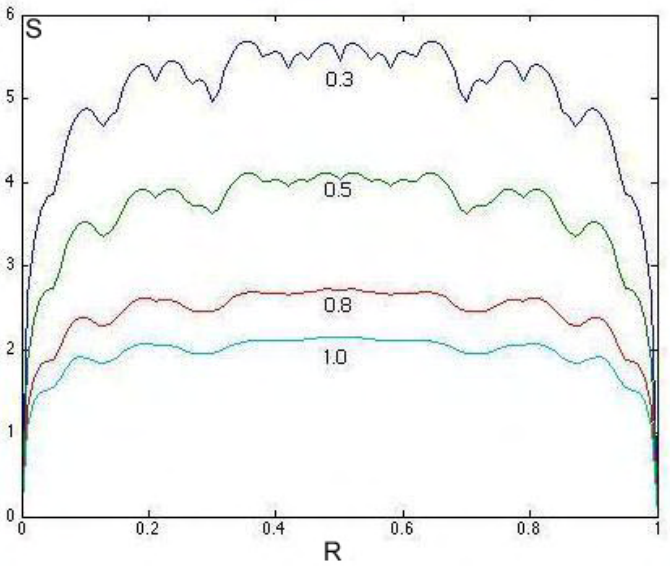


Figura 8.12: *Entropia para entradas de* $a = 3$ *e* $b = 7$ *fótons, com Matlab®*

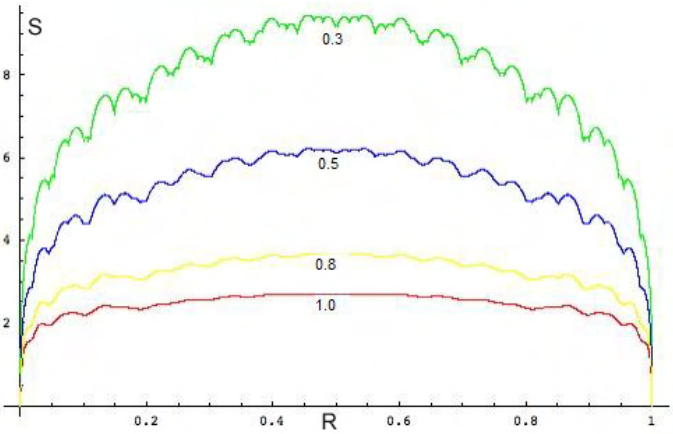


Figura 8.13: *Entropia para entradas de* $a = 4$ *e* $b = 16$ *fótons, com Mathematica®*

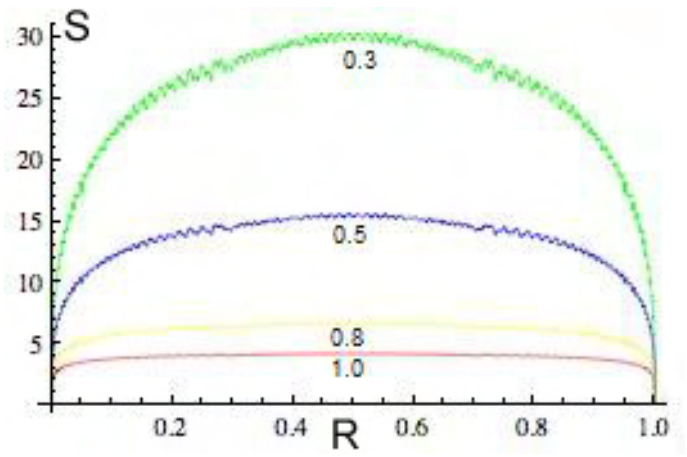


Figura 8.14: *Entropia para entradas de* $a = 30$ *e* $b = 70$ *fótons, com Mathematica®*

Analisando os gráficos (8.11, 8.12, 8.13, 8.14) cujo as entradas de fótons no divisor de feixe foram diferentes, temos que para a Entropia de von Neumann o máximo emaranhamento volta a ocorrer em $r = 0,5$, porém para a Entropia de Tsallis o máximo emaranhamento não ocorrem em $r = 0,5$, mas em $r \sim 0,5$, pois em $r = 0,5$ ocorre uma leve queda da amplitude.

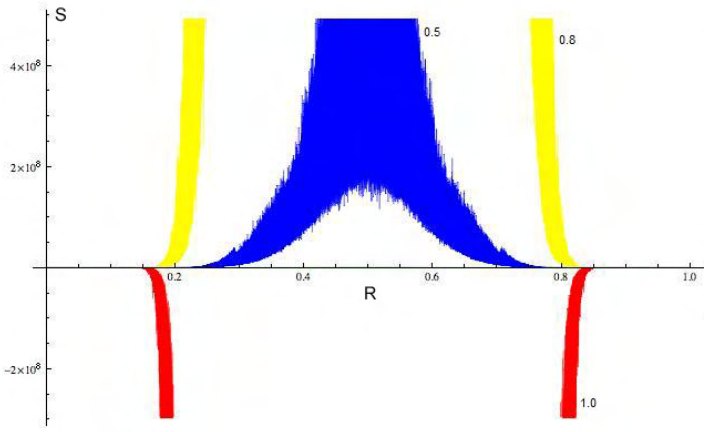


Figura 8.15: *Entropia para entradas de* $a = 50$ *e* $b = 150$ *fótons, com Mathematica®*

Agora observando os gráficos (8.15, 8.16 e 8.17) cujo as entradas além de diferentes foram maiores, observamos que ocorre uma nuvem de emaranhamento para a Entropia de Tsallis quando $q = 0,5$, porém o máximo emaranhamento ainda ocorre em $r \sim 0,5$, entretanto para a Entropia de Von Neumann em $r = 0,5$, temos novamente o mínimo emaranhamento. Na Figura (8.16) observa-se uma pequena diferença na imagem, aparecendo a linha que representa o índice entrópico $q = 0,3$, apenas tivemos um menor grau de emaranhamento para este caso.

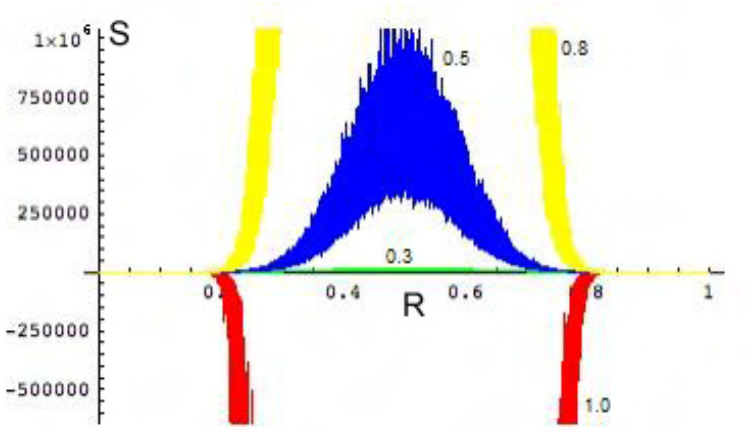


Figura 8.16: *Entropia para entradas de* $a = 40$ *e* $b = 160$ *fótons, com Mathematica®*

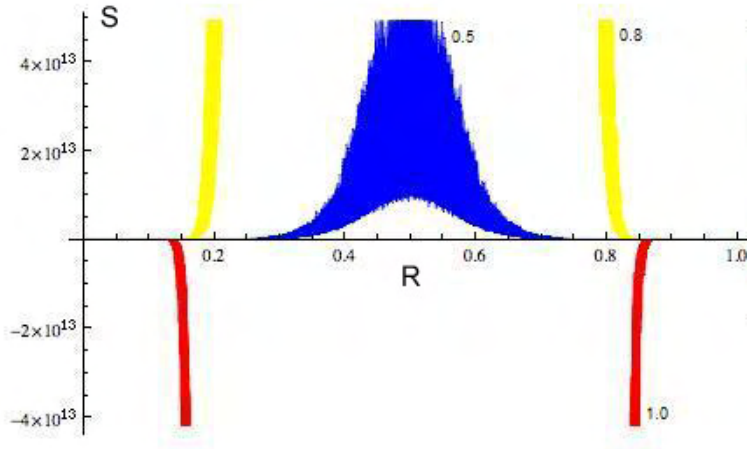


Figura 8.17: *Entropia para entradas de* $a = 80$ *e* $b = 120$ *fótons, com Mathematica®*

Contudo, concluímos que quando uma das entradas do divisor de feixes recebe o estado de vácuo $|0>$, a Entropia de Tsallis é semelhante a Entropia de Von Neumann; pelo menos pelos gráficos nada se pode ver de novo. Esse resultado coincide com o trabalho apresentado por Borges et al. (12).

Já quando um mesmo número de fótons é injetado nas entradas do divisor de feixe, a Entropia de Tsallis ainda apresenta alguma semelhança com a Entropia de Von Neumann, porém com maior variação na amplitude de reflexão.

E por fim, quando um número diferente de fótons é injetado nas entradas do divisor de feixe ocorre uma pequena diferença em relação ao emaranhamento em função da amplitude, como visto nos últimos gráficos o emaranhamento é máximo em $r \sim 0,5$ para a Entropia de Tsallis, porém para a Entropia de Von Neumann, quando um número muito maior é inserido no divisor de feixes esse emaranhamento passa a ser mínimo em $r = 0,5$.

Capítulo 9

Considerações Finais e Sugestões para Trabalhos Futuros

9.1 Considerações Finais

O objetivo maior deste trabalho foi ampliar os casos de estudos comparativos entre as entropias de Von Neumann e Tsallis na transmissão de informação quântica, estudadas brevemente por Borges et. al (12).

A Mecânica Estatística não extensiva, foi uma teoria originalmente proposta em 1988, pelo Prof. Constantino Tsallis do Centro Brasileiro de Pesquisas Físicas (Rio/RJ). Pela Teoria de Tsallis (11) não faz sentido afirmar "a priori" que a entropia de um sistema é extensiva (ou não extensiva) sem indicar a lei de composição de seus elementos. A princípio, esta simples observação permite uma análise mais crítica da entropia de Boltzmann e Gibbs, incluindo também as suas possíveis generalizações. A entropia não extensiva "a la" Tsallis, ou simplesmente Entropia de Tsallis, como mencionada ao longo da Dissertação é uma das peculiaridades da Mecânica Estatística não extensiva.

Em Mecânica Quântica o uso da Entropia não Extensiva (S_q) tem sido considerado como uma medida do emaranhamento quântico, em processos quânticos de transmissão da Informação. Nesta Dissertação vários casos foram considerados:

1. N fótons em uma entrada do divisor de feixes, e nenhum fóton no outro divisor;

2. O mesmo número de fótons em ambas as entradas do divisor;

3. Diferentes números de fótons em ambos os divisores;

Os resultados apresentam a Entropia não Extensiva (S_q) como uma função do coeficiente (amplitude) de reflexão para diferentes valores de $q \in [0, 1]$. Para $q = 1$ a Entropia não extensiva é conhecida também como Entropia de Von Neumann.

Como conclusão, fica evidente que o comportamento de (S_q) para pequenos valores de q é qualitativamente diferente, se comparadas as entropias "a la" Von Neumann e "a la" Tsallis. Nesta comparação entre a Entropia da Mecânica Quântica de Von Neumann e a Entropia não extensiva de Tsallis, é perceptível, que esta última é capaz (graças ao parâmetro entrópico q) de "levantar" correlações quânticas não percebidas pela primeira. Isto pode representar uma conexão do sistema físico (extensividade) e a medida do grau de emaranhamento.

9.2 Trabalhos Futuros

Seria de interesse, como ulteriores trabalhos, ir além dos estudos comparativos e qualitativos aqui apresentados através de simulações no Mathematica® e Matlab®.

Nesta Dissertação foram considerados estados-Fock, estados fatorizados, que interagem, e analisou-se o comportamento do emaranhamento através da entropia de Tsallis. Em ótica quântica é de interesse também a análise através de "estados Gaussianos"(10). As mesmas implementações realizadas na presente Dissertação, poderiam ser procedidas também em usando-se "estados Gaussianos emaranhados", o que acarretarão novos elementos para análise do Processo de Informação. Um aperfeiçoamento dos programas de implementação e análise utilizados, também é desejável, uma vez que o Mathematica® e o Matlab®, em alguns dos casos aqui estudados, mostraram-se demasiadamente lentos.

É intenção futura que se produzam programas em C ++, Fortran, etc, que possam levar a performances melhores de processamento, desempenho e complexidade.

Referências Bibliográficas

[1] Nielsen, M.A., Chuang, I.L.; *Quantum computation and Quantum information*, Cambridge University Press. Cambridge, 2002.

[2] Gerjuoy, E.; *Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers*, Am. J. Phys. vol. 73, 521-540, 2005.

[3] Bennett, C.H., DiVincenzo,D.P.; *Quantum information and computation*, Nature, 404, 247-255, 2000.

[4] Bennett, C.H., et.al; *Quantum Cryptography without Bell's Theorem*, Phys. Rev. Lett. 68, 557-559, 1992.

[5] Bennett, C.H., et.al; *Quantum Cryptography*, Scientific American, 26-33, out, 1992.

[6] Ekert, A.K.; *Quantum Cryptography based on Bell*, Phys. Rev. Lett., vol. 67, 661-663, 1991.

[7] Neumann, J.; *The Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1955.

[8] Tsallis, C., et.al; *Generalization of the Planck radiation law and application to the cosmic microwave background radiation* , Phys. Rev. E. 52, 1447, 1995.

[9] Tsallis, C.; *Nonextensive Statical Mechanics and Thermodynamics*, Braz. J. of Phys., 29, 1999.

[10] Tsallis, C.; Boon, J. P.; Gell-Monn, M.; Sato, Y.; *Extensivity and Entropy Production*, Europhysics News, 2005.

[11] Tsallis, C.; *Possible Generalizations of Boltzmann - Gibbs Statistics*, J. Stat. Phys., 52, 479-487, 1988.

[12] Borges, M. F.; Godoy, R.; Pratavieira, G. A.; *Towards a Quantum Information Process using Tsallis Entropy*, International Journal of Applied Mathematics, vol. 21, n. 4, 645-655, 2008.

[13] Shannon, C. E.; *A Mathematical Theory of Communication*, Bell Sys. Tech. J., vol. 27, 379-423 e 623-656, 1948.

[14] Balthazar, J.M., et.al; *Recents results on vibrating problems with limited power supply.* In. 6th Conference on Dynamical Systems Theory and Applications, $\pounds' odz$, Polonia, 2001.

[15] Bohm, A.; *Quantum Mechanics*, Ph.D. thesis, University of Winnebago, Winnebago, 1990.

[16] Eisenbud, L.; *The Conceptual Foundations of Quantum Mechanics* D. Van Nostrand, Princeton, 1968.

[17] Bühler, O.; *A Brief introduction to classical, statistical and Quantum Mechanics*, Acta Math. Acad. Sci. Hungar. (1957), 455-460.

[18] Godoy, R.; *Espaço de Hilbert e Quantificação de Emaranhamento via Entropia não Extensiva*, São José do Rio Preto, 2005.

[19] Dornellas, M. R., et.al; *Trabalho de 2007, curso de Mecânica Analítica.*, 2007.

[20] Dornellas, M. R., et.al; *Trabalho de 2008, curso de Teoria da Relatividade.*, 2008.

[21] Tipler, P.; *Física, para cientistas e engenheiros*, ed. Rio de Janeiro, 2000.

[22] Arnold, V.L.; *Métodos Matemáticos da Mecânica Clássica*, Ed. Mir. Moscovo. 1979.

[23] Hanselman, D.; Littlefield, B.; *Matlab 6 Curso Completo*, São Paulo, Pearson Prentice Hall, 2003.

[24] Singh, S.; *O Livro dos Códigos*, Rio de Janeiro, Record, 2005.

[25] Pessoa Jr, O.; *Conceitos de Física Quântica*, São Paulo, Ed. Livraria da Física, 2003.

[26] Lemos, N. A.; *Mecânica Analítica*, São Paulo, Ed. Livraria da Física, 2007.

[27] Shokranian, S., et.al; *Teoria dos Números*, Brasília, Ed. UNB, 1999.

[28] Dirac, P. A. M.; *General Theory of Relativity*, New Jersey, Princeton University Press, 1996.

[29] Shokranian, S.; *Criptografia para Iniciantes*, Brasília, Ed. UNB, 2005.

[30] Masuda, A.M., Panario, D.; *Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos*, Rio de Janeiro, IMPA, 2007.

[31] Cunha, M. O. T.; *Noções de Informação Quântica*, Rio de Janeiro, IMPA, 2007.

[32] Cunha, M. O. T., et.al; *Entropia: introdução à Teoria Matemática da (des)Informação*, Belo Horizonte, UFMG, 2004.

[33] Cunha, M. O. T.; *Emaranhamento: dos Gatos de Schrödinger à Álgebra Multilinear*, Belo Horizonte, UFMG, 2004.

[34] Cunha, M. O. T.; *Emaranhamento: caracterização, manipulação e consequências*, Belo Horizonte, UFMG, 2005.

[35] Vidiella, A.; *Entanglement and nonextensive statisics*, Physics Letters A 260, 335-339, 1999.

[36] Monroe, C.; *Quantum information processingg with atoms and photons*, Michigan, Nature, vol. 416, 238-246, 2002.

[37] Nielsen, M.A.; *Rules for a Complex Quantum World*, Scientific American, vol. 287, 66-75, 2002.

[38] Aaronson, S.; *The limits of Quantum*, Scientific American, 50-57, march, 2008.

[39] Monroe, C.R., et.al; *Quantum Computing with Ions*, Scientific American, 44-51, 2008.

[40] Peres, A., Terno, D. R.; *Quantum Information and relativity theory*, Rev. Mod. Phys., vol 76, 93-123, 2004.

[41] Feyman, R. P.; *Simulating Physics with Computers*, Int. J. Theoretical Physics, vol. 21, 467-488, 1982.

[42] Feyman, R. P.; *Quantum Mechanical Computers*, Foundations of Physics, vol. 16, 507-531, 1986.

[43] Scarani, V., et.al; *The speed of quantum information and the preferred frame: analysis of experimental data*, Phys. Lett. A 276, 2000.

[44] Scarani, V., et.al; *Optical tests of quantum nonlocality: from EPR-Bell tests towards experiments with moving observers*, Annalen der Physik 9: 831-841, 2000.

[45] Heisenberg, W.; *The phisical principles of the quantum theory*, Dover Publications, Inc, New York, 1949.

[46] Broglie, L.; *A tentative theory of Light quanta*, Philosophical Magazine, 47, 446-458, 1924.

[47] Gemer, L. H.; *Diffraction of Electrons by a Crystal of Nickel*, Physical Review, 30, 705, 1927.

[48] Thomson, G. P.; *Experiments on the Diffraction of Cathode Rays*, Proc. Royal Society, A 117, 600, 1928.

[49] Grego, M.; *Computador quântico já funciona*. Revista InfoOnline, 15 de fevereiro de 2007. Disponível em: <http://info.abril.com.br/aberto/infonews/022007/15022007-3.shl>. Acesso em: 10 jul 2008.

[50] <http://www.agencia.fapesp.br/material/10006/divulgacao-cientifica/teletransporte-quantico.htm>. Acesso em: 15 out 2009.

Apêndice A

Programas em Matlab ®

Neste apêndice descrevemos um programa utilizando o Matlab® (23). Todos os outros programas diferem apenas pelo parâmetro de controle e as respectivas alterações que a mudança no parâmetro de controle acarreta.

A.1 A chamada do arquivo

Mostrando ainda o tempo de execução dos cálculos, incremento a ser utilizado (grau de precisão do gráfico), e o gráfico final.

```
t = cputime;
incremento = 0.001;
vetor1 = Grafico(5, 5, 0.3, incremento);
vetor2 = Grafico(5, 5, 0.5, incremento);
vetor3 = Grafico(5, 5, 0.8, incremento);
vetor4 = GraficoVon(5, 5, 1, incremento);
eX = 0:incremento:1;
z = (cputime - t)/60
z1=z/24
plot(eX, vetor1, eX, vetor2, eX, vetor3, eX, vetor4)
```

A.2 O cálculo do vetor A

```
function A = A(a, b, c, d, r, t)
```

```
A = 0.00;
parte1 = 0.00;
parteR = 0.00;
parteT = 0.00;
parteRaizNumerador = 0.00;
parteRaizDenominador = 0.00;
parteKroner = 0.00;
for k=0:a
   for l=0:b
      parte1 = (-1)^(a-k);
      parteR = r^(a+b-l-k);
      parteT = t^(k+l);
      parteNumerador = sqrt(factorial(a) * factorial(b) * factorial(c) *
                     *factorial(d));
      parteDenominador = factorial(k) * factorial(a-k) * factorial(l) *
                     *factorial(b-l);
      parteKroner = Kroner(c, b+k-l) * Kroner(d, a-k+l);
      A = A + parte1 * parteR * parteT * (parteNumerador / parteDenominador) *
                      *parteKroner;
   end
end
```

A.3 O cálculo da Entropia de Tsallis

```
function ent = Entropia(a,b,q,r,t)
parteSomatorio = 0;
for c=0:a+b
    for d=0:a+b
        X = abs(A(a,b,c,d,r,t));
        parteSomatorio = parteSomatorio + X^(2*q);
    end
end
```

```
ent = (1/(q-1)) * (1 - parteSomatorio);
```

A.4 O cálculo da Entropia de von Neumann

```
function von = EntropiaVon(a,b,q,r,t)
pteSomatorio = 0;
for c=0:a+b
    for d=0:a+b
        X = abs(A(a,b,c,d,r,t));
        pteSomatorio = pteSomatorio + ((X^2) * (log((X^2) +
                    + .00000000000000000000000000001)));
    end
end
von = (-1) * pteSomatorio;
```

A.5 Construção do Gráfico da Entropia de Tsallis

```
function vetor = Grafico(a, b, q, incremento)
cont = 1;
for R = 0:incremento:1
    r = sqrt(R);
    t = sqrt(1-R);
    vetor(cont) = Entropia(a,b,q, r, t);
    cont = cont+1;
end
```

A.6 Gráfico da Entropia de von Neumann

```
function vetor = Grafico(a, b, q, incremento)
cont = 1;
for R = 0:incremento:1
    r = sqrt(R);
    t = sqrt(1-R);
```

```
    vetor(cont) = EntropiaVon(a,b,q, r, t);
    cont = cont+1;
end
```

A.7 O Delta de Kronecker

```
function kroner = Kroner(i,j)
if(i==j)
    kroner = 1;
else
    kroner = 0;
end
```

A.8 O Gráfico

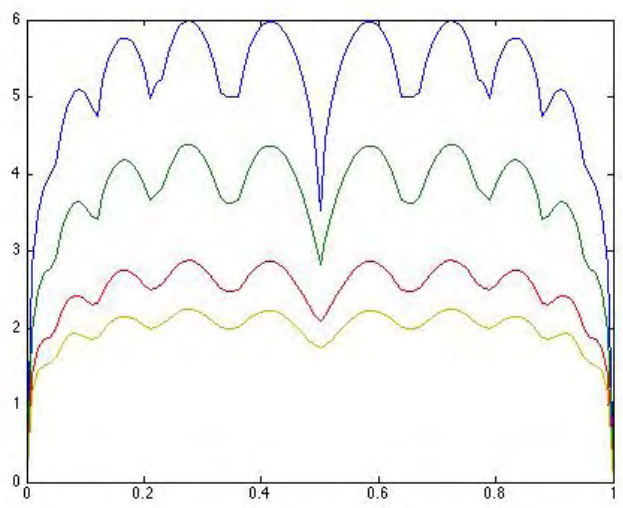


Figura A.1: *Entropia para entrada de* $a = 5$ *e* $b = 5$ *fótons, com Matlab®*

Onde o tempo de execução foi de z = 92.7125 minutos, ou seja, z1 = 3.8630 horas.

Apêndice B

Programas do Mathemathica ®

Neste apêndice descrevemos um programa utilizando o Mathemathica®. Todos os outros programas diferem apenas pelo parâmetro de controle e as respectivas alterações que a mudança no parâmetro de controle acarreta.

B.1 A programação

A programação - tempo do inicio do processamento, parâmetros e variáveis, Entropias de Tsallis e von Neumann, gráfico e tempo total de execução.

```
x = TimeUsed[]
Clear[N1, N2, n1, n2, q, j1, j2, r, a, b, c, d, q1, q2, t, k, l]
Needs["PlotLegends`"]
{a = 5, b = 5, r = Sqrt[R], t = Sqrt[1 - r^2], q = .3}
{a = 5, b = 5, r = Sqrt[R], t = Sqrt[1 - r^2], q1 = .5}
{a = 5, b = 5, r = Sqrt[R], t = Sqrt[1 - r^2], q2 = .8}
```

$$A[c\_, d\_] = \sum_{k=0}^{a}\sum_{l=0}^{b}\left((-1)^{a-k} * r^{a+b-l-k} * t^{k+l} * \frac{\sqrt{a! * b! * c! * d!}}{k! * (a-k)! * l! * (b-l)!} * \text{KroneckerDelta}[c, b+k-l] * \text{KroneckerDelta}[d, a-k+l]\right)$$

$$\text{entropia} = \frac{1}{q-1} * \left(1 - \sum_{c=0}^{a+b}\sum_{d=0}^{a+b}((\text{Abs}[A[c, d]])^{(2*q)})\right)$$

$$\text{entropia1} = \frac{1}{q1-1} * \left(1 - \sum_{c=0}^{a+b}\sum_{d=0}^{a+b}((\text{Abs}[A[c, d]])^{(2*q1)})\right)$$

$$\text{entropia2} = \frac{1}{q2-1} * \left(1 - \sum_{c=0}^{a+b}\sum_{d=0}^{a+b}((\text{Abs}[A[c, d]])^{(2*q2)})\right)$$

```
von =
  -Sum_{c=0}^{a+b} Sum_{d=0}^{a+b} ((Abs[A[c, d]])^(2) *
        Log[(Abs[A[c, d]])^(2) + .00000000000000000000000000001])

Plot[{von, entropia, entropia1, entropia2}, {R, 0, 1},
 PlotLegend → {"von N", 0.3, 0.5, 0.8}, PlotRange → {0, 10},
 PlotPoints → 10 001, LegendPosition → {1, -0.3}]

y = TimeUsed[]
z = (y - x)
tempo = z / 60
```

B.2 Os cálculos

Os resultados - início do processamento, parâmetros e variáveis utilizados e A[,].

Os resultados deste teste é para a injeção de 5 fótons nas duas entradas do divisor de feixe.

$$t_0 = 1746.52, \quad \{5, 5, R, 1-R, 0.3\}, \quad \{5, 5, R, 1-R, 0.5\} \quad \text{e} \quad \{5, 5, R, 1-R, 0.8\} \ .$$

$$\frac{1}{120}(1-R)^5\sqrt{c!\,d!}\ \text{KroneckerDelta}[5,c]\,\text{KroneckerDelta}[5,d] -$$
$$\frac{5}{24}(1-R)^4 R\sqrt{c!\,d!}\ \text{KroneckerDelta}[5,c]\,\text{KroneckerDelta}[5,d] + \frac{5}{6}(1-R)^3 R^2\sqrt{c!\,d!}\ \text{KroneckerDelta}[5,c]\,\text{KroneckerDelta}[5,d] -$$
$$\frac{5}{6}(1-R)^2 R^3\sqrt{c!\,d!}\ \text{KroneckerDelta}[5,c]\,\text{KroneckerDelta}[5,d] + \frac{5}{24}(1-R) R^4\sqrt{c!\,d!}\ \text{KroneckerDelta}[5,c]\,\text{KroneckerDelta}[5,d] -$$
$$\frac{1}{120}R^5\sqrt{c!\,d!}\ \text{KroneckerDelta}[5,c]\,\text{KroneckerDelta}[5,d] + \frac{1}{24}(1-R)^{9/2}\sqrt{R}\ \sqrt{c!\,d!}\ \text{KroneckerDelta}[4,d]\,\text{KroneckerDelta}[6,c] -$$
$$\frac{5}{12}(1-R)^{7/2}R^{3/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,d]\,\text{KroneckerDelta}[6,c] + \frac{5}{6}(1-R)^{5/2}R^{5/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,d]\,\text{KroneckerDelta}[6,c] -$$
$$\frac{5}{12}(1-R)^{3/2}R^{7/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,d]\,\text{KroneckerDelta}[6,c] + \frac{1}{24}\sqrt{1-R}\ R^{9/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,d]\,\text{KroneckerDelta}[6,c] -$$
$$\frac{1}{24}(1-R)^{9/2}\sqrt{R}\ \sqrt{c!\,d!}\ \text{KroneckerDelta}[4,c]\,\text{KroneckerDelta}[6,d] + \frac{5}{12}(1-R)^{7/2}R^{3/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,c]\,\text{KroneckerDelta}[6,d] -$$
$$\frac{5}{6}(1-R)^{5/2}R^{5/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,c]\,\text{KroneckerDelta}[6,d] + \frac{5}{12}(1-R)^{3/2}R^{7/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,c]\,\text{KroneckerDelta}[6,d] -$$
$$\frac{1}{24}\sqrt{1-R}\ R^{9/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[4,c]\,\text{KroneckerDelta}[6,d] + \frac{1}{12}(1-R)^4 R\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,d]\,\text{KroneckerDelta}[7,c] -$$
$$\frac{5}{12}(1-R)^3 R^2\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,d]\,\text{KroneckerDelta}[7,c] + \frac{5}{12}(1-R)^2 R^3\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,d]\,\text{KroneckerDelta}[7,c] -$$
$$\frac{1}{12}(1-R) R^4\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,d]\,\text{KroneckerDelta}[7,c] + \frac{1}{12}(1-R)^4 R\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,c]\,\text{KroneckerDelta}[7,d] -$$
$$\frac{5}{12}(1-R)^3 R^2\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,c]\,\text{KroneckerDelta}[7,d] + \frac{5}{12}(1-R)^2 R^3\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,c]\,\text{KroneckerDelta}[7,d] -$$
$$\frac{1}{12}(1-R) R^4\sqrt{c!\,d!}\ \text{KroneckerDelta}[3,c]\,\text{KroneckerDelta}[7,d] + \frac{1}{12}(1-R)^{7/2}R^{3/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[2,d]\,\text{KroneckerDelta}[8,c] -$$
$$\frac{5}{24}(1-R)^{5/2}R^{5/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[2,d]\,\text{KroneckerDelta}[8,c] + \frac{1}{12}(1-R)^{3/2}R^{7/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[2,d]\,\text{KroneckerDelta}[8,c] -$$
$$\frac{1}{12}(1-R)^{7/2}R^{3/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[2,c]\,\text{KroneckerDelta}[8,d] + \frac{5}{24}(1-R)^{5/2}R^{5/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[2,c]\,\text{KroneckerDelta}[8,d] -$$
$$\frac{1}{12}(1-R)^{3/2}R^{7/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[2,c]\,\text{KroneckerDelta}[8,d] + \frac{1}{24}(1-R)^3 R^2\sqrt{c!\,d!}\ \text{KroneckerDelta}[1,d]\,\text{KroneckerDelta}[9,c] -$$
$$\frac{1}{24}(1-R)^2 R^3\sqrt{c!\,d!}\ \text{KroneckerDelta}[1,d]\,\text{KroneckerDelta}[9,c] + \frac{1}{24}(1-R)^3 R^2\sqrt{c!\,d!}\ \text{KroneckerDelta}[1,c]\,\text{KroneckerDelta}[9,d] -$$
$$\frac{1}{24}(1-R)^2 R^3\sqrt{c!\,d!}\ \text{KroneckerDelta}[1,c]\,\text{KroneckerDelta}[9,d] + \frac{1}{120}(1-R)^{5/2}R^{5/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[0,d]\,\text{KroneckerDelta}[10,c] -$$
$$\frac{1}{120}(1-R)^{5/2}R^{5/2}\sqrt{c!\,d!}\ \text{KroneckerDelta}[0,c]\,\text{KroneckerDelta}[10,d]$$

Os resultados - das Entropias de Tsallis (q = 0.3, 0.5 e 0.8)

$$
\begin{aligned}
&-1.42857 \Big(1 - 10.5063\, \text{Abs}\Big[(1-R)^{5/2} R^{5/2}\Big]^{0.6} - 2\, \text{Abs}\Big[3\sqrt{70}\ (1-R)^3 R^2 - 3\sqrt{70}\ (1-R)^2 R^3\Big]^{0.6} - \\
&\quad \text{Abs}\Big[-4\sqrt{35}\ (1-R)^{7/2} R^{3/2} + 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} - 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^{0.6} - \\
&\quad \text{Abs}\Big[4\sqrt{35}\ (1-R)^{7/2} R^{3/2} - 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} + 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^{0.6} - \\
&\quad 2\, \text{Abs}\Big[\sqrt{210}\ (1-R)^4 R - 5\sqrt{210}\ (1-R)^3 R^2 + 5\sqrt{210}\ (1-R)^2 R^3 - \sqrt{210}\ (1-R) R^4\Big]^{0.6} - \\
&\quad \text{Abs}\Big[-\sqrt{30}\ (1-R)^{9/2}\sqrt{R} + 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} - 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} + 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} - \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^{0.6} - \\
&\quad \text{Abs}\Big[\sqrt{30}\ (1-R)^{9/2}\sqrt{R} - 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} + 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} - 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} + \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^{0.6} - \\
&\quad \text{Abs}\Big[(1-R)^5 - 25\,(1-R)^4 R + 100\,(1-R)^3 R^2 - 100\,(1-R)^2 R^3 + 25\,(1-R) R^4 - R^5\Big]^{0.6}\Big)
\end{aligned}
$$

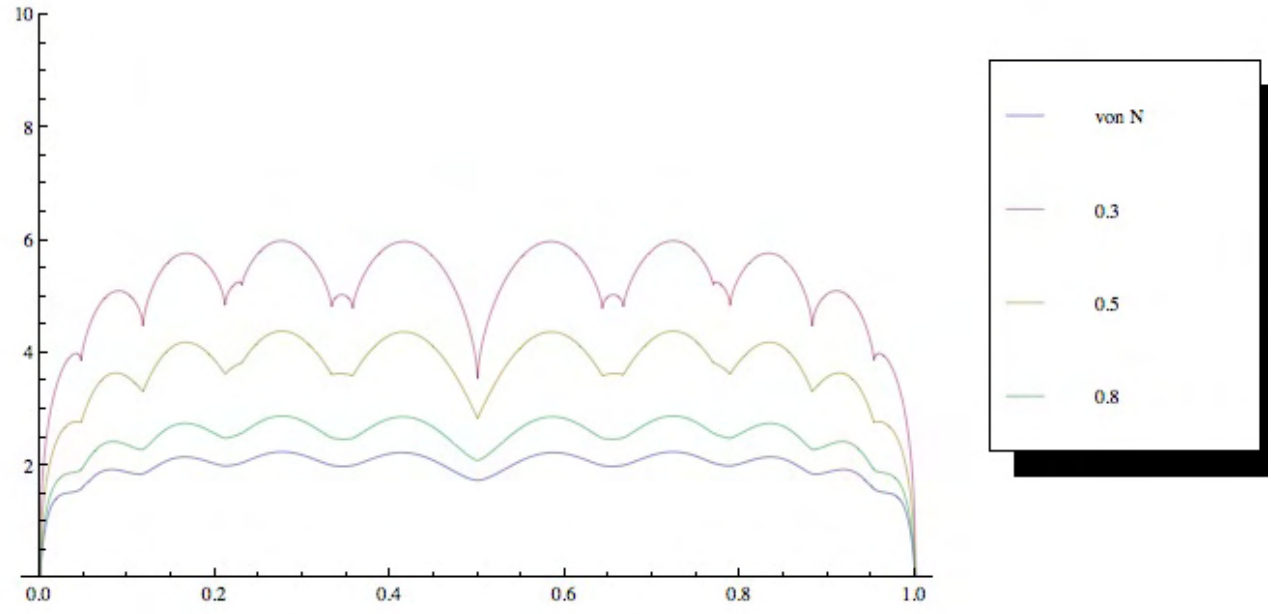
$$
\begin{aligned}
&-2. \Big(1 - 31.749\, \text{Abs}\Big[(1-R)^{5/2} R^{5/2}\Big]^{1.} - 2\, \text{Abs}\Big[3\sqrt{70}\ (1-R)^3 R^2 - 3\sqrt{70}\ (1-R)^2 R^3\Big]^{1.} - \\
&\quad \text{Abs}\Big[-4\sqrt{35}\ (1-R)^{7/2} R^{3/2} + 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} - 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^{1.} - \\
&\quad \text{Abs}\Big[4\sqrt{35}\ (1-R)^{7/2} R^{3/2} - 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} + 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^{1.} - \\
&\quad 2\, \text{Abs}\Big[\sqrt{210}\ (1-R)^4 R - 5\sqrt{210}\ (1-R)^3 R^2 + 5\sqrt{210}\ (1-R)^2 R^3 - \sqrt{210}\ (1-R) R^4\Big]^{1.} - \\
&\quad \text{Abs}\Big[-\sqrt{30}\ (1-R)^{9/2}\sqrt{R} + 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} - 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} + 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} - \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^{1.} - \\
&\quad \text{Abs}\Big[\sqrt{30}\ (1-R)^{9/2}\sqrt{R} - 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} + 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} - 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} + \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^{1.} - \\
&\quad \text{Abs}\Big[(1-R)^5 - 25\,(1-R)^4 R + 100\,(1-R)^3 R^2 - 100\,(1-R)^2 R^3 + 25\,(1-R) R^4 - R^5\Big]^{1.}\Big)
\end{aligned}
$$

$$
\begin{aligned}
&-5. \Big(1 - 166.782\, \text{Abs}\Big[(1-R)^{5/2} R^{5/2}\Big]^{1.6} - 2\, \text{Abs}\Big[3\sqrt{70}\ (1-R)^3 R^2 - 3\sqrt{70}\ (1-R)^2 R^3\Big]^{1.6} - \\
&\quad \text{Abs}\Big[-4\sqrt{35}\ (1-R)^{7/2} R^{3/2} + 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} - 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^{1.6} - \\
&\quad \text{Abs}\Big[4\sqrt{35}\ (1-R)^{7/2} R^{3/2} - 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} + 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^{1.6} - \\
&\quad 2\, \text{Abs}\Big[\sqrt{210}\ (1-R)^4 R - 5\sqrt{210}\ (1-R)^3 R^2 + 5\sqrt{210}\ (1-R)^2 R^3 - \sqrt{210}\ (1-R) R^4\Big]^{1.6} - \\
&\quad \text{Abs}\Big[-\sqrt{30}\ (1-R)^{9/2}\sqrt{R} + 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} - 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} + 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} - \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^{1.6} - \\
&\quad \text{Abs}\Big[\sqrt{30}\ (1-R)^{9/2}\sqrt{R} - 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} + 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} - 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} + \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^{1.6} - \\
&\quad \text{Abs}\Big[(1-R)^5 - 25\,(1-R)^4 R + 100\,(1-R)^3 R^2 - 100\,(1-R)^2 R^3 + 25\,(1-R) R^4 - R^5\Big]^{1.6}\Big)
\end{aligned}
$$

von Neumann (q = 1)

$$
\begin{aligned}
&-504\, \text{Abs}\Big[(1-R)^{5/2} R^{5/2}\Big]^2 \text{Log}\Big[1.\times 10^{-29} + 252\, \text{Abs}\Big[(1-R)^{5/2} R^{5/2}\Big]^2\Big] - \\
&2\, \text{Abs}\Big[3\sqrt{70}\ (1-R)^3 R^2 - 3\sqrt{70}\ (1-R)^2 R^3\Big]^2 \text{Log}\Big[1.\times 10^{-29} + \text{Abs}\Big[3\sqrt{70}\ (1-R)^3 R^2 - 3\sqrt{70}\ (1-R)^2 R^3\Big]^2\Big] - \\
&\text{Abs}\Big[-4\sqrt{35}\ (1-R)^{7/2} R^{3/2} + 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} - 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^2 \\
&\quad \text{Log}\Big[1.\times 10^{-29} + \text{Abs}\Big[-4\sqrt{35}\ (1-R)^{7/2} R^{3/2} + 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} - 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^2\Big] - \\
&\text{Abs}\Big[4\sqrt{35}\ (1-R)^{7/2} R^{3/2} - 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} + 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^2 \\
&\quad \text{Log}\Big[1.\times 10^{-29} + \text{Abs}\Big[4\sqrt{35}\ (1-R)^{7/2} R^{3/2} - 10\sqrt{35}\ (1-R)^{5/2} R^{5/2} + 4\sqrt{35}\ (1-R)^{3/2} R^{7/2}\Big]^2\Big] - \\
&2\, \text{Abs}\Big[\sqrt{210}\ (1-R)^4 R - 5\sqrt{210}\ (1-R)^3 R^2 + 5\sqrt{210}\ (1-R)^2 R^3 - \sqrt{210}\ (1-R) R^4\Big]^2 \\
&\quad \text{Log}\Big[1.\times 10^{-29} + \text{Abs}\Big[\sqrt{210}\ (1-R)^4 R - 5\sqrt{210}\ (1-R)^3 R^2 + 5\sqrt{210}\ (1-R)^2 R^3 - \sqrt{210}\ (1-R) R^4\Big]^2\Big] - \\
&\text{Abs}\Big[-\sqrt{30}\ (1-R)^{9/2}\sqrt{R} + 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} - 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} + 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} - \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^2 \text{Log}\Big[\\
&\quad 1.\times 10^{-29} + \text{Abs}\Big[-\sqrt{30}\ (1-R)^{9/2}\sqrt{R} + 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} - 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} + 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} - \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^2\Big] - \\
&\text{Abs}\Big[\sqrt{30}\ (1-R)^{9/2}\sqrt{R} - 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} + 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} - 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} + \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^2 \text{Log}\Big[\\
&\quad 1.\times 10^{-29} + \text{Abs}\Big[\sqrt{30}\ (1-R)^{9/2}\sqrt{R} - 10\sqrt{30}\ (1-R)^{7/2} R^{3/2} + 20\sqrt{30}\ (1-R)^{5/2} R^{5/2} - 10\sqrt{30}\ (1-R)^{3/2} R^{7/2} + \sqrt{30}\ \sqrt{1-R}\ R^{9/2}\Big]^2\Big] - \\
&\text{Abs}\Big[(1-R)^5 - 25\,(1-R)^4 R + 100\,(1-R)^3 R^2 - 100\,(1-R)^2 R^3 + 25\,(1-R) R^4 - R^5\Big]^2 \\
&\quad \text{Log}\Big[1.\times 10^{-29} + \text{Abs}\Big[(1-R)^5 - 25\,(1-R)^4 R + 100\,(1-R)^3 R^2 - 100\,(1-R)^2 R^3 + 25\,(1-R) R^4 - R^5\Big]^2\Big]
\end{aligned}
$$

O gráfico com as Entropias de Tsallis (q=0.3, 0.5 e 0.8) e von Neumann (q=1), e os tempos de processamento final, diferença entre inicial e final e o tempo real de processamento em segundos.




```
1767.57
21.0532
0.350886
```

Figura B.1: *Entropia para entradas de* $a = 5$ *e* $b = 5$ *fótons, com Mathematica® e tempos de execução*

Os valores acima 1767.57 referem-se ao tempo final da execução do programa, 21.0532 é a diferença entre o tempo inicial e o tempo final, ou seja o tempo real de execução em segundos e 0.350886 é o tempo em minutos.