

Fabiano Alan Serafim Ferrari

***O Estudo da Entropia de Transferência em Sistemas
Dinâmicos Discretos***

PONTA GROSSA

2012

Fabiano Alan Serafim Ferrari

*O Estudo da Entropia de Transferência em Sistemas
Dinâmicos Discretos*

Dissertação para obtenção do título de mestre
na Universidade Estadual de Ponta Grossa,
Pró-Reitoria de Pesquisa e Pós-Graduação,
Mestrado em Ciências, Área de Concentração
Física.

Orientador:

Prof. Dr. Sandro Ely de Souza Pinto

PONTA GROSSA

2012

Ficha Catalográfica Elaborada pelo Setor Tratamento da Informação BICEN/UEPG

F375e Ferrari, Fabiano Alan Serafim
O Estudo da Entropia de Transferência em Sistemas Dinâmicos
Discretos / Fabiano Alan Serafim Ferrari . Ponta Grossa, 2012.
59 f.

Dissertação (Mestrado em Ciências - Área de Concentração :
Física), Universidade Estadual de Ponta Grossa.
Orientador: Prof. Dr. Sandro Ely de Souza Pinto

1.Entropia de Transferência. 2. Informação. 3. Probabilidade.
I. Pinto, Sandro Ely de Souza. II.T.

CDD: 621.402.1

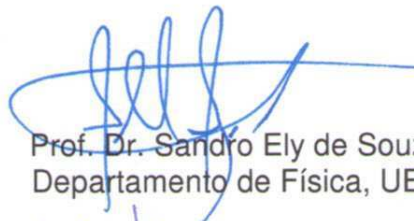
TERMO DE APROVAÇÃO

FABIANO ALAN SERAFIM FERRARI

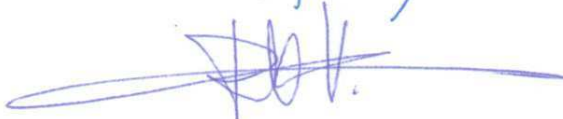
"O ESTUDO DA ENTROPIA DE TRANSFERÊNCIA EM SISTEMAS DINÂMICOS DISCRETOS"

Dissertação aprovada como requisito parcial para obtenção do grau de Mestre no Programa de Pós-Graduação em Ciências - Física da Universidade Estadual de Ponta Grossa, pela seguinte banca examinadora.

Orientador:



Prof. Dr. Sandro Ely de Souza Pinto
Departamento de Física, UEPG/PR



Prof. Dr. Ricardo Luiz Viana
Departamento de Física, UFPR/PR



Prof. Dr. Milton Domingos Michel
Departamento de Física, UEPG/PR

Ponta Grossa, 27 de fevereiro de 2012.

Dedico esta dissertação ao meu pai e minha mãe.

Agradecimentos

Agradeço à Crislaine da Cruz, minha musa inspiradora.

Agradeço à Romeu Miquéias Szmoski pelo trabalho conjunto que culminou no último capítulo desta dissertação.

Agradeço ao Prof. Antônio Marcos Batista pela amizade, conselhos e sugestões.

Agradeço a todos os membros do Grupo de Dinâmica Não-Linear e Sistemas Complexos da UEPG, pela amizade e por estarem sempre a disposição de discutir ideias. Em especial a Rodrigo Frehse Pereira e Kelly Cristiane Iarosz cujas sugestões refletiram diretamente em algum trecho do trabalho.

Agradeço a todos os membros e agregados da República Houston, assim como a todos os integrantes do Upalelê Sport Club, pela fraternidade.

Agradeço ao Judô Sagrada Família pelos momentos de descontração.

Agradeço a Comunidade Bahá'í de Ponta Grossa pelo auxílio no meu desenvolvimento pessoal e espiritual.

Agradeço ao Programa de Pós-Graduação em Ciências-Física e a Capes pelo suporte financeiro.

Agradeço ao meu orientador Sandro Ely de Souza Pinto pela sugestão de trabalho que culminou nesta dissertação.

Agradeço a toda minha família por acreditar e confiar que valeria a pena.

“Nem tudo o que um homem sabe pode ser revelado, nem tudo o que lhe é possível revelar deverá ser julgado oportuno, e nem todo dizer oportuno pode ser considerado apropriado à capacidade dos que o ouvem” (Bahá’u’lláh)

Resumo

Sistemas caóticos se caracterizam por um comportamento irregular, aparentemente aleatório, mas cuja sua evolução temporal é descrita por uma regra de evolução. Mesmo quando um sistema caótico é iniciado de duas condições iniciais muito próximas elas tendem a divergir exponencialmente uma da outra com o tempo. Esta sensibilidade às condições iniciais torna a previsibilidade de uma órbita caótica difícil de se obter. A imprevisibilidade de sistemas caóticos faz com que muitas vezes seja mais interessante estudar sua distribuição de probabilidade ao invés de sua série temporal diretamente. Através da teoria da informação é possível estudar sistemas dinâmicos a partir de sua probabilidade. Dentro da teoria da informação uma quantidade importante é a entropia de transferência que permite estudar coerências estatísticas em sistemas que evoluem no tempo. A partir desta coerência é possível transmitir informação de forma segura utilizando caos, apresentamos um modelo já existente na literatura e propomos um novo modelo para esta transmissão segura.

Palavras-chave: Entropia de transferência. Informação. Probabilidade.

Abstract

Chaotic systems are characterized by irregular behaviour, which some times are confused with random behaviour. The time evolution of these systems is described using an evolution rule. Even a chaotic system begins in two very close initial conditions, they will diverge exponentially to one another. Thus, this sensibility creates difficulties to predict and get the chaotic orbit. Chaotic systems unpredictness make it more interesting studying its probability distribution than its time series directly. Through information theory is possible study dynamical systems by mean of its probability. Inside information theory an important quantity is the transfer entropy, that allows us to study statistic coherence in systemns which have their evolution through time. With this coherence it is possible transmit information using chaos in a safe way. Therefore, we present a model present in the literature and we suggest a new model of this safe transmission.

Keywords: Transfer Entropy. Information. Probability.

Sumário

Introdução	9
1 Teoria da Informação	12
1.1 Conceito de Informação	12
1.2 Entropia de Shannon	14
1.3 Entropia Conjunta	17
1.4 Entropia Condicional	18
1.5 Informação Mútua	19
1.6 Entropia de Kullback	20
1.7 Regra da Cadeia da Entropia	20
1.8 Taxa de Entropia	21
1.9 Entropia de Transferência	21
2 Sistemas Dinâmicos	23
2.1 Expoente de Lyapunov	23
2.1.1 Expoente de Lyapunov a partir da média espacial	24
2.1.2 Generalização do Expoente de Lyapunov	25
2.1.3 Cálculo Numérico do Expoente de Lyapunov	26
2.2 Dinâmica de Mapas Não-Interagentes	27
2.2.1 Mapa da Tenda Assimétrico Generalizado	27
2.2.2 Mapa Logístico	28
2.3 Rede de Mapas Acoplados	29

2.3.1	Classes de Acoplamento Local	31
2.4	Sincronização de Caos	32
3	Mapa da Tenda Assimétrico Generalizado com Acoplamento Local	33
3.1	Dois Mapas Acoplados	34
3.2	Direcionalidade de Sinais Correlacionados	39
4	Sistemas de Comunicação usando Caos	44
4.1	Sistema de Comunicação Básico	44
4.2	Modelo de Hung e Hu	46
4.3	Transmissão de Informação entre Redes Sincronizadas através da Entropia de Transferência	50
4.3.1	Estágio Pré-Sincronização	50
4.3.2	Estágio pós-sincronização	52
	Conclusão	56
	Referências Bibliográficas	57

Introdução

O comportamento dinâmico é compreendido como algo que acontece e que se modifica ao longo do tempo. As ideias trazidas por Galileu Galilei e Isaac Newton introduziram o pensamento contemporâneo de que a natureza obedece leis imutáveis que podem ser descritas matematicamente [1].

Um sistema dinâmico pode ser definido como uma descrição matemática para a evolução do estado de um sistema através do tempo [2]. Um sistema dinâmico se caracteriza por um vetor de estado que descreve exatamente a posição de algum sistema real ou hipotético e uma função que determina a regra de evolução temporal [3].

Existem diferentes formas de se representar um sistema dinâmico, a partir de autômatos celulares [4], equações diferenciais [1] ou mapas [5]. Ao longo da dissertação nosso objeto de estudo serão sistemas dinâmicos descritos por mapas. Os mapas se caracterizam por possuírem sua imagem e domínio pertencentes ao mesmo espaço [5]. Na representação por mapas, o vetor de estado é descrito de forma contínua, enquanto, a evolução temporal é discreta. A evolução temporal em tempo discreto significa que os passos de tempo são medidos em termos de quantidades contáveis. A evolução de um estado descrito por um mapa é determinada a partir de uma relação de recorrência, $x_{n+1} = f(x_n)$.

Os resultados obtidos principalmente no estudo da mecânica celeste durante os séculos *XVIII* e *XIX*, deixaram a ideia de que a natureza poderia ser compreendida de maneira precisa a partir do conhecimento das leis que regem a natureza. A ideia intuitiva trazida pelo método científico é a de que se fosse possível conhecer o estado inicial com certa precisão seria possível descrever um sistema de maneira completa durante toda sua evolução temporal do início ao fim dos tempos.

Henri Jules Poincaré ainda no século *XIX* lançou as bases da teoria moderna de sistemas dinâmicos ao falar sobre os sistemas que exibem sensibilidade às condições iniciais. Poincaré demonstra que a predição de um sistema dinâmico não é válida para todos os casos. Só é possível prever a evolução de um sistema quando trajetórias que iniciam-se próximas tendem a continuar próximas. Existem sistemas dinâmicos cujas trajetórias próximas tendem a divergirem uma das outras rapidamente com a evolução temporal. Estes sistemas serão o nosso

objeto de estudo ao longo da dissertação e são chamados de sistemas caóticos ou descritos por uma dinâmica não-linear.

O efeito borboleta, termo cunhado por Edward Lorenz para descrever sistemas com sensibilidade a condições iniciais, diz que o bater das asas de uma borboleta no Brasil pode ser capaz de provocar um tornado nos Estados Unidos [6]. Apesar de o efeito borboleta ser apenas uma conjectura a interdependência do clima do planeta é um fato. Não apenas o clima, mas, todas as coisas do universo estão em constante interação.

Embora sistemas dinâmicos possuem sensibilidade local, para qualquer condição inicial aleatória pertencente ao domínio do mapeamento a densidade de probabilidade do sistema é invariante [7]. Esta propriedade permite que utilize-se a teoria de informação no estudo de sistemas dinâmicos. A quantidade de informação que um sistema possui é uma medida do grau de incerteza que existe ao se tentar prever sua evolução temporal, chamamos esta quantidade de entropia de Shannon [8].

No capítulo 1 exploramos diferentes propriedades da entropia de Shannon e mostramos como utilizá-la para tratar sistemas que interagem. Apresentamos quantidades como a informação mútua que permite determinar a existência de correlação entre sistemas [9]. Ainda neste capítulo apresentamos como é definida a quantidade principal do trabalho, a entropia de transferência que permite determinar se existe troca de informação em algum sentido preferencial [10].

Apresentamos no capítulo 2 alguns modelos clássicos de sistemas dinâmicos, como o mapa da tenda. O mapa da tenda é encontrado na literatura de diferentes maneiras [11], [12], [13], escolhemos como modelo de estudo o mapa da tenda generalizado assimétrico que permite estudar diferentes distribuições de probabilidade e ainda representa um modelo relativamente simples para extrair resultados analíticos. Para o estudo da interação entre mapas, utilizamos diferentes configurações de rede de mapas acoplados [14].

O capítulo 3 tem como objetivo demonstrar a aplicabilidade dos elementos da teoria da informação em sistemas dinâmicos. Demonstramos como é possível relacionar a taxa de divergência de trajetórias com a informação mútua [15] e como determinar a direção de acoplamento a partir da entropia de transferência.

Um sistema de comunicação é composto por cinco elementos, uma fonte de informação, um emissor que seleciona a mensagem que deve ser enviada, um codificador que transforma a mensagem de forma que ela possa ser transmitida na forma de um sinal, um canal que transmite o sinal ao receptor que têm a função de transformar o sinal novamente em uma mensagem que é então recebida pelo receptor [8]. No capítulo 4 apresentamos como Hung e Hu [16] construíram

um sistema de comunicação utilizando a direção de acoplamento para transmitir informação de forma segura. Como a entropia de transferência é medida em termos de probabilidades é necessário um tempo de observação das variáveis de estado para determinar corretamente a direção de acoplamento e conseqüentemente a mensagem que foi transmitida. Chamamos este tempo mínimo de tempo de relaxação. No modelo de Hung e Hu é possível transmitir apenas um *bit* de informação durante cada intervalo de tempo, o qual deve ser igual ou maior que o tempo de relaxação.

Propomos ainda no capítulo 4 um modelo de duas redes de mapas acoplados onde cada rede é composta por um vetor de estado que contém N variáveis de estado. As redes são acopladas de forma que seus vetores de estados se tornem idênticos. Uma rede é denominada emissora (E) e a outra a rede receptora (R), após se tornarem idênticas ambas são desconectadas. A mensagem é codificada em um sinal descrito por uma variável S . O modelo permite o envio de mensagens binárias de forma segura, o mecanismo funciona da seguinte maneira: O emissor contém a rede (E), quando um sítio de sua rede é acoplado a variável S ele codifica o sinal 1 e quando não é acoplado codifica o sinal 0. O receptor que possui a rede (R) mede a entropia de transferência dos sítios de sua rede com relação a variável S e recupera a mensagem. Este modelo é capaz de transmitir informação de maneira mais rápida que o mecanismo de Hung e Hu, pois, transmite N bits em um mesmo intervalo de tempo. Também é extramente robusto contra intruso, pois, apenas redes cujos vetores de estado são os mesmos da rede (E) são capazes de ler a mensagem escondida na sinal.

Com base nos resultados apresentados queremos mostrar como é possível utilizar a entropia de transferência na construção de um mecanismo de comunicação explorando a direção de acoplamento entre sítios em uma rede de mapas acoplados.

1 Teoria da Informação

A teoria da informação tem como propósito solucionar problemas técnicos envolvidos na transmissão de informação. Problemas semânticos, ou seja, problemas na forma como uma mensagem recebida é interpretada ou na forma como os envolvidos no processo de comunicação aceitam ou rejeitam uma mensagem não são considerados. O primeiro trabalho a apresentar um método matemático completo para estudar problemas de comunicação foi proposto por Claude Shannon, “The Mathematical Theory of Communication” [8].

A quantidade de informação que um sistema possui é definida em termos de distribuições de probabilidades o que permite a teoria da informação uma inter-relação com diversas áreas. Do ponto de vista da matemática, teoria da informação é basicamente um estudo de probabilidades. Dentro da visão da engenharia a teoria da informação pode ser interpretada como sendo uma teoria de incerteza. Enquanto na visão da física a teoria da informação é essencialmente uma teoria de entropia [17].

1.1 Conceito de Informação

“A informação é uma medida de liberdade de escolhas quando selecionamos uma mensagem¹.” (Weaver)

Enquanto o conceito usual da informação diz respeito ao que você diz, para a teoria da informação o termo informação está relacionado com o que você pode dizer [8]. Quando um indivíduo pretende enviar uma mensagem possui a sua disposição todo o alfabeto. As regras de linguagem permitem construir diferentes combinações de letras formando palavras dotadas de significado. Ao se transmitir uma mensagem o remetente faz uma escolha entre todas as combinações possíveis de mensagem que ele pode enviar.

Se o remetente pretende enviar uma mensagem usando o alfabeto latino contendo 26 letras, por exemplo, para cada letra que pretende enviar ao destinatário terá que escolher entre

¹Originalmente [8], “*Information is a measure of one’s freedom of choice when one selects a message*”.

26 possíveis símbolos. Caso o remetente pretenda utilizar dois símbolos do alfabeto terá $(26)^2$ possíveis combinações para formar sua mensagem. Uma mensagem contendo um tamanho arbitrário N , exigirá que seja feita uma escolha entre $(26)^N$ possíveis combinações. Se assumirmos que o remetente pode utilizar um conjunto arbitrário de símbolos s para transmitir a mensagem, então teremos s^N combinações possíveis. Hartley propôs uma maneira de expressar quantitativamente a quantidade de informação [18]

$$H = KN, \quad (1.1)$$

onde K é uma constante que depende do número de símbolos disponíveis s para transmitir a mensagem. Se pensarmos em dois sistemas idênticos com o mesmo número de símbolos disponíveis e constante para as N_1 e N_2 escolhas respectivamente então, temos

$$s_1^{N_1} = s_2^{N_2}, \quad (1.2)$$

a quantidade de informação de cada um deles deve ser idêntica, como indicado abaixo

$$H = K_1 N_1 = K_2 N_2, \quad (1.3)$$

se relacionarmos as equações (1.2) e (1.3), temos

$$N_1 \log s_1 = N_2 \log s_2 \quad (1.4)$$

$$\frac{K_1}{\log s_1} = \frac{K_2}{\log s_2}. \quad (1.5)$$

Para que sistemas idênticos tenham a mesma quantidade de informação a expressão para o valor de K deve ser tal que

$$K = K_0 \log s, \quad (1.6)$$

onde K_0 é uma constante, a medida da informação deve ser o logaritmo do número de possíveis sequências [18],

$$H = K_0 N \log s \quad (1.7)$$

$$H = K_0 \log s^N \quad (\text{medida de informação de Hartley}). \quad (1.8)$$

A medida de informação proposta por Hartley é anterior aos trabalhos de Claude Shannon sobre sistemas de comunicação, mas representa uma das primeiras formas para se quantificar a quantidade de informação. A equação (1.8) implica que quanto maior o número de distintas

mensagens mais informação um sistema possui.

1.2 Entropia de Shannon

Embora a definição proposta por Hartley para a medida de informação apresente resultados interessantes, não permite determinar diretamente qual é a incerteza contida em um sistema conhecendo os possíveis estados que podem ser acessados e suas respectivas probabilidades. Para um sistema discreto cujos estados acessíveis são $i = 1, 2, \dots, n$, com respectivas probabilidades p_i . Então, Shannon propôs que a medida da quantidade de informação do sistema, $H(p_1, p_2, \dots, p_n)$, deve satisfazer três propriedades [8]:

1. H deve ser contínua em p .
2. Se todos os p_i são iguais, $p_i = \frac{1}{n}$, então H deve crescer monotonicamente com a quantidade de estados acessíveis (n).
3. Se uma escolha é dividida em duas sucessivas escolhas, então, H deve ser a soma das entropias individuais.

A primeira propriedade leva em conta que o número de estados possíveis para um sistema pode crescer exponencialmente com o tamanho da mensagem que se pretende enviar, todavia a quantidade de informação não deve ser uma quantidade divergente. Baseado nas ideias de Hartley, Shannon propôs que a quantidade de informação deve ser medida em termos do logaritmo das probabilidades.

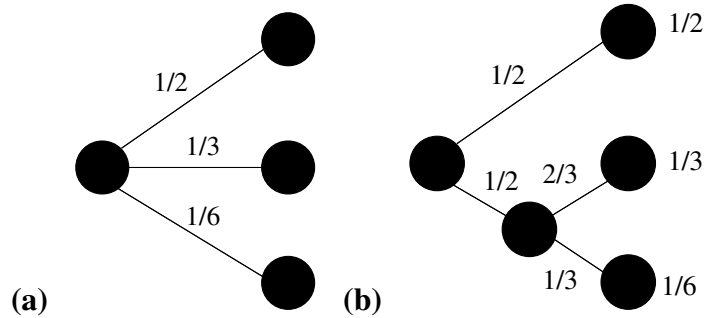
Se assumirmos que o nosso sistema é descrito dentro de uma região finita, a medida que a dividimos estados cada vez menores, de acordo com a segunda propriedade a medida da informação deve aumentar. Na figura 1.3 apresentaremos uma exemplificação para compreender como ocorre este aumento.

A terceira propriedade pode ser compreendida de maneira mais simples a partir do exemplo mostrado nas figuras 1.1 (a) e (b). Na figura 1.1 (a) existem três possíveis estados que podem ser escolhidos enquanto na figura 1.1 (b) existem duas escolhas possíveis em um primeiro momento, dependendo da primeira escolha outras duas escolhas podem existir, caso a escolha seja a esfera inferior. A função H para este caso deve satisfazer a seguinte relação

$$H\left(\frac{1}{2}, \frac{1}{3}, \frac{1}{6}\right) = H\left(\frac{1}{2}, \frac{1}{2}\right) + \frac{1}{2}H\left(\frac{2}{3}, \frac{1}{3}\right), \quad (1.9)$$

onde a equação do lado esquerdo é a entropia de uma única escolha entre três eventos possíveis. A equação da direita é a entropia para duas escolhas sucessivas. O termo $H(\frac{1}{2}, \frac{1}{2})$ é a entropia da primeira escolha e o termo $\frac{1}{2}H(\frac{2}{3}, \frac{1}{3})$ é a entropia da segunda escolha, o fator multiplicativo $1/2$ aparece, pois, conforme mostra a figura 1.1 (b) ocorre apenas metade das vezes.

Figura 1.1: Decomposição da escolha entre três eventos: (a) Apenas uma escolha a ser feita, (b) Duas escolhas sucessivas.



A função H que satisfaz as três propriedades tem a forma

$$H = -K \sum_{i=1}^n p(i) \log p(i), \quad (1.10)$$

onde K é uma constante. A forma usual da entropia de Shannon para uma variável X é [9]:

$$H(X) = - \sum_{i=1}^n p(i) \log_a p(i), \quad (1.11)$$

onde a é um parâmetro e indica a unidade de medida da entropia. Quando $a = 2$ indica que a medida da entropia é *bits* (dígito binário), quando a é igual ao número natural, então a unidade de medida é o *nats* (dígito natural). O *bit* representa a quantidade de informação contida em um sistema, quando é necessário fazer uma escolha entre dois possíveis eventos equiprováveis. Podemos pensar em um lance de moeda, onde existem apenas dois resultados possíveis e equiprováveis, cara ou coroa. Pode-se atribuir ao resultado cara o índice 1 e para o resultado coroa o índice 2, dessa forma, $p_1 = \frac{1}{2}$ e $p_2 = \frac{1}{2}$. A quantidade de informação em um arremesso de moeda será portanto,

$$\begin{aligned} H(\text{lançamento da moeda}) &= -\left[\frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{2} \log_2 \frac{1}{2}\right] \\ H(\text{lançamento da moeda}) &= 1 \text{ bit}. \end{aligned} \quad (1.12)$$

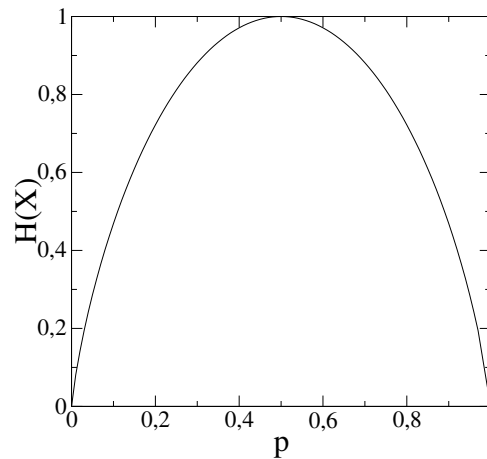
Se ao invés de utilizarmos uma moeda honesta utilizarmos uma moeda viciada, ou seja, com um dos eventos sendo mais provável que outro, desta forma teremos $p_1 = 1 - p$ e $p_2 = p$, onde $p \in [0, 1]$. Este exemplo pode ser comparado com uma caminhada aleatória em uma

dimensão [19]. A quantidade de informação contida no lançamento da moeda será então,

$$H(\text{lançamento da moeda}) = -[(1 - p) \log_2(1 - p) + p \log_2(p)], \quad (1.13)$$

a entropia de Shannon deste sistema é então uma função de p . Se considerarmos o lance de moedas como sendo uma variável, que denominamos por X , então, $H(X) = H(p)$. Na figura 1.2 apresentamos a entropia para todos os valores possíveis do parâmetro p . Conforme pode ser observado na figura 1.2 existem dois casos importantes para o lançamento de uma moeda, o caso onde apenas um resultado é possível e o caso equiprovável. Quando apenas um resultado é possível, cara ou coroa, então a entropia de Shannon possui valor zero, pois, não existe incerteza em se determinar o estado do sistema. No caso equiprovável, $p = 0,5$, a quantidade de informação é máxima, pois representa a situação onde existe a maior incerteza possível para este sistema.

Figura 1.2: Entropia de Shannon para ocorrência de dois eventos.



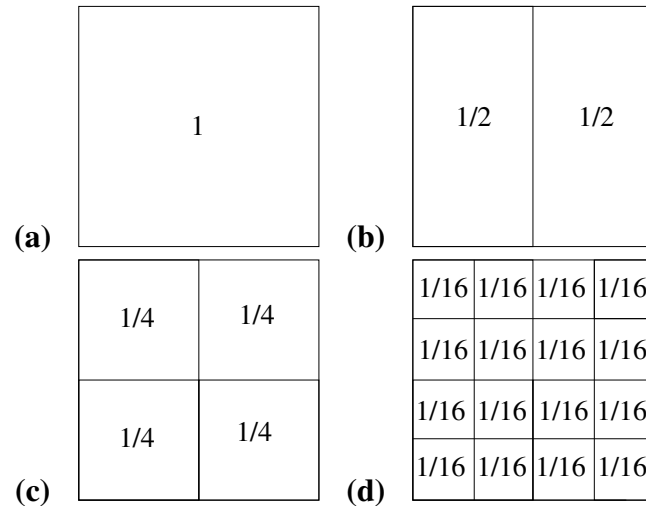
É necessário enfatizar que só faz sentido falar em informação antes do lançamento da moeda. Quando efetua-se uma medida no sistema, por exemplo, e obtêm-se o resultado cara, então toda a informação foi extraída do sistema e a entropia de Shannon é zero. A curva observada na figura 1.2 apresenta simetria, pois, a quantidade de informação independe da natureza do resultado, cara ou coroa.

O fato da entropia de Shannon não permitir determinar se a moeda viciada fornece mais caras ou mais coras é porque para a teoria da informação não importa a natureza do evento mas sua probabilidade de ocorrência.

A entropia de Shannon é uma função que depende exclusivamente da probabilidade. Existem diversas formas possíveis de se estimar a probabilidade associada a uma variável, uma ferramenta simples e conveniente é o uso de histogramas. Quanto maior o número de caixas que dividimos o espaço de fase, maior será a entropia de Shannon. Nas figuras 1.3 (a),(b),(c) e

(d) apresentamos um exemplo para a contagem de caixas e sua relação com a entropia quando os eventos estão distribuídos uniformemente pelo espaço de fase.

Figura 1.3: Crescimento da entropia com o número de estados. (a) Uma partição: $H = \log_2 1 = 0 \text{ bits}$, (b) Duas partições: $H = \log_2 2 = 1 \text{ bit}$, (c) Quatro partições: $H = \log_2 4 = 2 \text{ bits}$, (d) Dezesseis partições: $H = \log_2 16 = 4 \text{ bits}$.



Na figura 1.3 (a) temos que todo o espaço de fase é descrito por um único estado representando uma única partição cuja entropia de Shannon é nula, pois não existe incerteza. Na figura 1.3 (b) dividimos o espaço de fase em duas partições, como ambos os estados são equiprováveis então a entropia de Shannon é de 1 *bit*. As figuras 1.3 (c) e (d) nos evidencia o aumento da entropia quando o número de estados acessíveis aumenta.

1.3 Entropia Conjunta

Quando estudamos sistemas que são descritos por duas ou mais variáveis uma quantidade importante a ser definida é a entropia conjunta. A entropia conjunta representa a quantidade de informação total disponível no sistema. Para um par de variáveis X e Y a entropia conjunta é

$$H(X, Y) = - \sum_{x=1}^n \sum_{y=1}^n p(x, y) \log p(x, y), \quad (1.14)$$

onde x e y representam n estados acessíveis discretos associados às variáveis X e Y respectivamente. Estas quantidades devem obedecer as propriedades básicas de probabilidades, ou

seja,

$$\bullet \sum_{x=1}^n p(x) = 1 \quad (1.15)$$

$$\bullet \sum_{y=1}^n p(y) = 1 \quad (1.16)$$

$$\bullet \sum_{y=1}^n \sum_{x=1}^n p(x,y) = 1. \quad (1.17)$$

Assumindo X e Y duas moedas, ambas com a mesma probabilidade de fornecerem como resultado cara ou coroa, atribuindo para cara o rótulo 1 e para coroa o rótulo 2, então os eventos possíveis e equiprováveis serão 11,12,21 e 22. A entropia conjunta deste sistema será:

$$\begin{aligned} H(X,Y) &= -\left[\frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{4} \log_2 \frac{1}{4}\right] \\ H(X,Y) &= 2bits. \end{aligned} \quad (1.18)$$

1.4 Entropia Condicional

Quando as variáveis X e Y estão correlacionadas, isto é, $p(x,y) \neq p(x)p(y)$, então, a entropia de cada uma das variáveis é condicionada a outra. Ou seja, os eventos que influenciam uma variável influenciam diretamente a quantidade de informação na outra variável devido à correlação existente entre elas.

Para que se possa definir a entropia condicional é necessário relacionar a probabilidade conjunta com a probabilidade condicional, a conexão entre elas é determinada a partir do teorema de Bayes, onde [20]

$$p(x,y) = p(x)p(y|x) \quad . \quad (1.19)$$

A entropia condicional será

$$H(Y|X) = -\sum p(x)p(y|x) \log p(y|x) \quad (1.20)$$

$$H(Y|X) = -\sum p(x,y) \log p(y|x), \quad (1.21)$$

a equação (1.21) é a forma usual para a entropia condicional, todavia, outra relação importante pode ser obtida,

$$H(Y|X) = -\bullet p(x,y)[\log p(x,y) - \log p(x)] \quad (1.22)$$

$$H(Y|X) = -\bullet p(x,y) \log p(x,y) + \bullet p(y|x)p(x) \log p(x) \quad (1.23)$$

$$H(Y|X) = H(X,Y) - H(X), \quad (1.24)$$

ou seja, a entropia condicional representa a quantidade de informação contida na variável Y conhecendo a informação da variável X com ela relacionada. É possível obter também a quantidade de informação contida em X conhecendo a variável Y

$$H(X|Y) = H(X,Y) - H(Y), \quad (1.25)$$

esta relação não é simétrica entre as variáveis.

1.5 Informação Mútua

Quando duas variáveis X e Y estão correlacionadas, o conhecimento de uma variável reduz a incerteza associada à outra variável. A redução da incerteza, que está diretamente relacionada com a redução da quantidade de informação devido à correlação, chamamos de informação mútua:

$$I(X,Y) = H(X) - H(X|Y) \quad (1.26)$$

$$I(X,Y) = H(Y) - H(Y|X), \quad (1.27)$$

a forma usual pode ser obtida utilizando o teorema de Bayes,

$$I(X,Y) = \bullet p(x,y) \log p(x|y) - \bullet p(x) \log p(x) \quad (1.28)$$

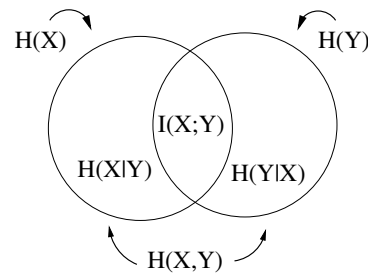
$$I(X,Y) = \bullet p(x,y) \log \frac{p(x,y)}{p(y)} - \bullet p(x,y) \log p(x) \quad (1.29)$$

$$I(X,Y) = \bullet p(x,y) \log \frac{p(x,y)}{p(y)p(x)}. \quad (1.30)$$

A equação (1.30) nos mostra que esta quantidade é simétrica para as variáveis X e Y . As quantidades fundamentais da teoria da informação para duas variáveis podem ser observadas a partir do diagrama de Venn, conforme a figura 1.4. Cada círculo no diagrama representa a quantidade de informação contida em uma variável. A região de intersecção representa a informação mútua enquanto a área total menos a intersecção representa a entropia condicional

de cada variável.

Figura 1.4: Diagrama de Venn para a teoria da informação



1.6 Entropia de Kullback

A entropia de Kullback é também conhecida como a distância de Kullback-Leibler, que determina a quantidade de informação inserida em um sistema descrito por uma probabilidade $p(x)$ quando atribui-se uma outra medida $q(x)$ a este sistema [21]. Representa a distância² entre duas distribuições de probabilidade. A entropia de Kullback é definida como sendo

$$K(X) = \bullet p(x) \log \frac{p(x)}{q(x)}. \quad (1.31)$$

Algumas entropia de Kullback importantes:

$$K(X, Y) = \bullet p(x, y) \log \frac{p(x, y)}{q(x, y)} \quad \text{entropia de Kullback conjunta} \quad (1.32)$$

$$K(X|Y) = \bullet p(x, y) \log \frac{p(x|y)}{q(x|y)} \quad \text{entropia de Kullback condicional} \quad (1.33)$$

A informação mútua é um caso particular da entropia de Kullback conjunta, onde $p = p(x, y)$ e $q = p(x)p(y)$. Ou seja, a informação mútua é a medida da informação inserida no sistema em função da correlação entre as variáveis X e Y . Ou ainda, é a quantidade de informação que as variáveis X e Y compartilham entre si.

1.7 Regra da Cadeia da Entropia

As expressões apresentadas até então, dizem respeito a sistemas envolvendo apenas duas variáveis. Todas as medidas fundamentais de entropia, entropia conjunta, entropia condicional e informação mútua, obedecem à regra da cadeia para sistemas com mais de duas variáveis [9].

²A distância aqui é não-euclidiana e determinada em termos da quantidade de informação.

Seja um sistema N dimensional, descrito pelas variáveis X_1, X_2, \dots, X_N , então a entropia conjunta será expressa por:

$$H(X_1, X_2, \dots, X_N) = \bullet \prod_{i=1}^N H(X_i | X_{i-1}, \dots, X_1) \quad (1.34)$$

todas as outras propriedades podem ser extraídas a partir desta regra da cadeia. Podemos verificar a propriedade obtida pela expressão (1.24). Caso o sistema seja descrito por apenas duas variáveis X_1 e X_2 , aplicando a regra da cadeia, então,

$$\begin{aligned} H(X_1, X_2) &= H(X_1) + H(X_2 | X_1) \\ H(X_2 | X_1) &= H(X_1, X_2) - H(X_1). \end{aligned} \quad (1.35)$$

1.8 Taxa de Entropia

A taxa de entropia representa o número médio de *bits* necessários para codificar um estado adicional ao sistema,

$$h(X) = \bullet \sum p(x_{n+1}, x^{(k)}) \log p(x_{n+1} | x^{(k)}), \quad (1.36)$$

onde x_{n+1} representa o estado adicional e $x^{(k)} = (x_n, x_{n-1}, \dots, x_{n-k})$ representa a história associada à variável X . Embora a história relativa à variável possa ser extensa, apenas parte da história influencia o futuro da variável X . Quando uma variável depende exclusivamente de seu estado anterior, então dizemos que é um processo de Markov de ordem 1. Desta forma k representa a ordem do processo de Markov [22] e não a história completa da variável, pois, $p(x_{n+1}, x^{(k)}) = p(x_{n+1}, x^{(k)}, x_{n-k-1})$.

1.9 Entropia de Transferência

Quando estudamos uma variável isoladamente a taxa de entropia fornece resultados definitivos quanto a quantidade de informação necessária para codificar um estado adicional. Quando temos variáveis X e Y correlacionadas, então, devemos levar em consideração não apenas a história da variável mas de todas as partes do sistema que interagem entre si. Desta forma, a entropia de transferência é a entropia de Kullback condicional entre $p(x_{n+1}, x^{(k)})$ e $p(x_{n+1}, x^{(k)}, y^{(k)})$, ou seja,

$$T_{Y \rightarrow X} = \bullet \sum p(x_{n+1}, x^{(k)}, y^{(k)}) \log \frac{p(x_{n+1} | x^{(k)}, y^{(k)})}{p(x_{n+1} | x^{(k)})}. \quad (1.37)$$

A entropia de transferência é uma quantidade que permite determinar o efeito causal de uma variável sobre a outra [10]. Conforme veremos com detalhes nos capítulos posteriores esta ferramenta nos permite identificar a direção do acoplamento entre as variáveis e estudar a dinâmica de interação. Ao longo da dissertação utilizamos a entropia de transferência com $k = 1$.

Se assumirmos que duas variáveis podem possuir três tipos de acoplamento possíveis: unidirecional onde X influencia Y e Y não influencia X , o caso unidirecional inverso onde a variável Y influencia X e X não influencia Y ou o caso bidirecional onde X e Y são influenciadas uma pela outra, a entropia de transferência nos permite discernir cada uma das situações, enquanto a informação mútua não é capaz de fazê-la.

2 *Sistemas Dinâmicos*

Um sistema dinâmico consiste de um par (χ, f) , onde χ é o espaço de fase e representa todos os valores possíveis que o sistema pode assumir e f representa a regra de evolução temporal. O estado de um sistema físico pode ser representado como um ponto no espaço de fase. A dinâmica de um estado é fornecida a partir da regra de evolução [23].

2.1 Expoente de Lyapunov

Os sistemas dinâmicos que iremos estudar se caracterizam por possuírem sensibilidade às condições iniciais. Uma forma de se quantificar a sensibilidade com relação às condições iniciais é medindo a taxa média de divergência de duas trajetórias iniciadas próximas [12]. Se considerarmos duas trajetórias descritas pelas variáveis de estado $x(n)$ e $y(n)$ e os valores $x(0)$ e $y(0)$ suas respectivas condições iniciais, que devem ser suficientemente próximas. Caso as duas variáveis de estado permaneçam durante n tempos na mesma região linear, então,

$$|x(n+1) - y(n+1)| = |f'(x(n))||x(n) - y(n)| \quad \text{para } n = 0, \dots, (n-1), \quad (2.1)$$

onde $f'(x(n))$ denota a derivada da função no ponto x . As trajetórias tendem a se aproximar ou divergir exponencialmente uma da outra, então,

$$|x(n+1) - y(n+1)| = e^{\lambda n} |x(n) - y(n)|, \quad (2.2)$$

podemos reescrever esta equação em função de λ , de forma que:

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \bullet \ln |f'(x(n))|. \quad (2.3)$$

O valor de λ no limite de $n \rightarrow \infty$ é conhecido como o expoente de Lyapunov. Quando este valor é positivo significa que as trajetórias que se iniciaram próximas divergem exponencialmente com o tempo, desta forma a dinâmica do sistema é dita caótica. Caso λ seja negativo então a dinâmica do sistema é regular. O expoente de Lyapunov é uma medida capaz de deter-

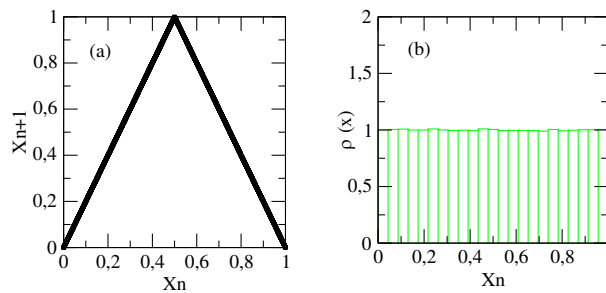
minar se um sistema possui ou não uma dinâmica caótica.

Um exemplo simples de sistema caótico é o chamado mapa da tenda, o qual iremos explorar em detalhes no próximo capítulo, definido como:

$$x_{n+1} = \begin{cases} 2x_n & \text{se } 0 \leq x_n \leq 0,5 \\ 2 - 2x_n & \text{se } 0,5 < x_n \leq 1,0 \end{cases} . \quad (2.4)$$

Na figura 2.1 (a) o diagrama de retorno do mapa da tenda é mostrado, onde evoluímos a série temporal e depois montamos um diagrama para cada instante de tempo contra seu estado anterior, sua aparência de tenda foi o motivo do nome atribuído ao mapa. A figura 2.1 (b) nos mostra a partir do histograma de 23 caixas que a distribuição de probabilidade do mapa é uniforme. Para as figuras 2.1 (a) e (b) foi utilizado uma série de 10^7 pontos.

Figura 2.1: (a) Mapa da tenda; (b) histograma do mapa.



Se aplicarmos a equação (2.3) ao mapa da tenda, então

$$\begin{aligned} \lambda &= \frac{1}{N} \prod_{n=0}^{N-1} \ln(2) \\ \lambda &= \ln(2), \end{aligned} \quad (2.5)$$

ou seja, o mapa da tenda é caótico e duas trajetórias descritas pelo mapa da tenda que iniciem próximas irão divergir com a evolução temporal.

2.1.1 Expoente de Lyapunov a partir da média espacial

Conforme verificamos pela equação (2.3), o expoente de Lyapunov é definido em termos da evolução temporal de uma trajetória caótica, todavia, se a função que descreve a dinâmica caótica for continuamente diferenciável exceto para um número finito de pontos e possuir distribuição de probabilidade invariante é possível determinar o expoente de Lyapunov a partir da média espacial [12]. Pois nesse caso o sistema é ergódico e a média temporal é igual a média

espacial. O expoente de Lyapunov será então:

$$\lambda = \int_a^b \ln |f'(x)| \rho(x) dx, \quad (2.6)$$

onde a e b representam o domínio da função $f(x)$, e $\rho(x)$ representa a densidade de probabilidade. Podemos novamente usar o mapa da tenda, que possui densidade de probabilidade uniforme, para exemplificar esta propriedade. Desta forma podemos aplicar a equação (2.6) ao mapa da tenda descrito pela equação (2.4)

$$\lambda = \int_0^{0,5} \ln |2| dx + \int_{0,5}^1 \ln |-2| dx \quad (2.7)$$

$$\lambda = \ln(2). \quad (2.8)$$

2.1.2 Generalização do Expoente de Lyapunov

Para o estudo de sistemas com mais de uma dimensão o expoente de Lyapunov será caracterizado pela expansão ou contração das direções ortogonais que compõem o sistema N -dimensional centrado em torno de uma posição inicial \vec{x}_0 com a evolução temporal. É possível determinar a expansão ou contração destas direções a partir da matriz jacobiana DF do sistema.

Para um sistema de duas dimensões descrito pelo conjunto de equações $x_{n+1}^{(1)} = F_1(x_n^{(1)}, x_n^{(2)})$ e $x_{n+1}^{(2)} = F_2(x_n^{(1)}, x_n^{(2)})$, a matriz jacobiana associada será

$$DF(x_n^{(1)}, x_n^{(2)}) = \begin{bmatrix} \frac{\partial F_1(x_n^{(1)}, x_n^{(2)})}{\partial x^{(1)}} & \frac{\partial F_1(x_n^{(1)}, x_n^{(2)})}{\partial x^{(2)}} \\ \frac{\partial F_2(x_n^{(1)}, x_n^{(2)})}{\partial x^{(1)}} & \frac{\partial F_2(x_n^{(1)}, x_n^{(2)})}{\partial x^{(2)}} \end{bmatrix}, \quad (2.9)$$

de maneira geral a matriz jacobiana será:

$$DF(x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(N)}) = \begin{bmatrix} \frac{\partial F_1(x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(N)})}{\partial x^{(1)}} & \dots & \frac{\partial F_1(x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(N)})}{\partial x^{(N)}} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n(x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(N)})}{\partial x^{(1)}} & \dots & \frac{\partial F_n(x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(N)})}{\partial x^{(N)}} \end{bmatrix}. \quad (2.10)$$

Os autovetores da matriz jacobiana determinam as direções onde ocorrem contrações ou expansões. Os autovalores da matriz irão determinar as respectivas intensidades. De maneira similar ao caso unidimensional, se um autovalor é menor que 1 a direção está contraindo, se um autovalor é maior que 1 a direção está se expandindo. O expoente de Lyapunov será definido em termos dos autovalores da matriz jacobiana DF ,

$$\Lambda = \lim_{n \rightarrow \infty} \frac{1}{2n} \ln |DF_n^T DF_n|, \quad (2.11)$$

DF_n representa a n -ésima jacobiana, o produto $DF_n^T DF_n$ é utilizado, pois, existem casos em que a matriz jacobiana possui autovalores complexos. Um sistema com N dimensões terá então N expoentes de Lyapunov associados. Um exemplo simples é o sistema descrito pelo conjunto de equações abaixo:

$$\vec{X} = \begin{cases} x_{n+1} = (1 - \varepsilon)f(x_n) + \varepsilon f(y_n) \\ y_{n+1} = (1 - \varepsilon)f(y_n) + \varepsilon f(x_n) \end{cases}, \quad (2.12)$$

onde $f(x)$ representa o mapa da tenda descrito pela equação (2.4). A matriz jacobiana do mapa será

$$DF(x_n, y_n) = 2 \begin{pmatrix} (1 - \varepsilon) & \varepsilon \\ \varepsilon & (1 - \varepsilon) \end{pmatrix}, \quad (2.13)$$

os autovalores da matriz jacobiana são $\lambda_1 = 2$ e $\lambda_2 = 2(1 - 2\varepsilon)$. Desta forma o sistema terá dois expoentes de Lyapunov

$$\Lambda_1 = \ln(2) \quad (2.14)$$

$$\Lambda_2 = \Lambda_1 + \ln(1 - 2\varepsilon). \quad (2.15)$$

2.1.3 Cálculo Numérico do Expoente de Lyapunov

É comum encontrar casos onde não existe uma maneira direta de se determinar os autovalores da matriz jacobiana, pois o cálculo do expoente de Lyapunov envolve a n -ésima aplicação do mapa no limite $n \rightarrow \infty$ fazendo com que os coeficientes da matriz se tornem muito grandes ou muito pequenos. Uma das maneiras de se determinar o expoente de Lyapunov é utilizando o procedimento de ortogonalização de Gram-Schmidt [5].

O procedimento de ortogonalização de Gram-Schmidt nos permite, a partir de um conjunto inicial de vetores linearmente independentes, construir uma base de vetores ortogonais em termos das direções de expansão e contração do mapa. O mecanismo para a determinação do conjunto de vetores é através da subtração da projeção de um vetor sobre o outro [24].

Primeiramente define-se uma base inicial linearmente independente N -dimensional: $\vec{w}_1, \dots, \vec{w}_N$. A partir dos vetores iniciais, define-se um novo conjunto de vetores que fornecerão a contração ou expansão de uma região inicial¹, serão determinados a partir da matriz jacobiana

$$\vec{z}_1^0 = DF(\vec{x}_0)\vec{w}_1^0, \dots, \vec{z}_m^0 = DF(\vec{x}_0)\vec{w}_m^0, \quad (2.16)$$

¹Geralmente esta região inicial é uma hiper-esfera de N dimensões que a partir da aplicação do mapa deforma-se numa hiper-elipse de também N dimensões.

todavia, este conjunto não é necessariamente ortogonal, para podermos determinar a contração ou expansão será necessário determinar um novo conjunto ortogonal de vetores

$$\begin{aligned}\bar{y}_1^n &= \bar{z}_1^n \\ \bar{y}_2^n &= \bar{z}_2^n - \frac{\bar{z}_2^n \cdot \bar{y}_1^n}{\|\bar{y}_1^n\|^2} \bar{y}_1^n \\ &\vdots\end{aligned}\tag{2.17}$$

$$\bar{y}_N^n = \bar{z}_N^n - \frac{\bar{z}_N^n \cdot \bar{y}_1^n}{\|\bar{y}_1^n\|^2} \bar{y}_1^n - \dots - \frac{\bar{z}_N^n \cdot \bar{y}_{m-1}^n}{\|\bar{y}_{m-1}^n\|^2} \bar{y}_{m-1}^n,\tag{2.18}$$

onde \cdot é o produto escalar e $\|\cdot\|$ é a norma euclidiana.

Como este procedimento preserva o volume da esfera inicial com a evolução temporal algumas direções podem se tornar extremamente grandes enquanto outras extremamente pequenas. Este problema pode ser resolvido, fazendo uma renormalização da base ortogonal a cada instante de tempo

$$\vec{w}_i^{n+1} = \frac{\bar{y}_i^{n+1}}{\|\bar{y}_i^{n+1}\|},\tag{2.19}$$

onde i representa cada uma das N direções ortogonais. O expoente $n + 1$ indica que o procedimento deve ser repetido para $n \rightarrow \circ$ e dessa forma w_i^{n+1} representa a nova base de vetores linearmente independentes e o procedimento deve ser repetido. Os N expoentes de Lyapunov serão então

$$\Lambda_i = \frac{\ln \|\bar{y}_i^n\| + \dots + \ln \|\bar{y}_i^1\|}{n}.\tag{2.20}$$

2.2 Dinâmica de Mapas Não-Interagentes

Os mapas não interagentes são aqueles que não sofrem influência de agentes externos, sua dinâmica é essencialmente local. Existe uma vasta quantidade de mapas que apresentam comportamento caótico, apenas o mapa da tenda e o mapa logístico serão apresentados aqui, mas outros mapas podem ser encontrados em [5].

2.2.1 Mapa da Tenda Assimétrico Generalizado

Muito presente na literatura, um modelo que apresenta comportamento caótico é o mapa da tenda [2] [5]. Apresentamos aqui uma forma mais geral deste mapa que nos permite estudar mudanças na geometria e distribuição de probabilidade [12] [13]. O mapa é descrito pela

equação:

$$\begin{aligned}
 x_{n+1} &= f(x_n) \\
 x_{n+1} &= \begin{cases} b + ((1-b)/a)x_n & \text{se } 0 \leq x \leq a \\ (1-x_n)/(1-a) & \text{se } a < x \leq 1 \end{cases}, \quad (2.21)
 \end{aligned}$$

onde $0 < a < 1$ e $0 < b < 1$. A versão mais encontrada na literatura de mapa da tenda assimétrico², consiste na equação (2.21), com $b = 0$. A figura 2.2 (a) mostra a forma da mapa da tenda para diferentes valores do parâmetro b , quando este for diferente de zero ele modifica a distribuição de probabilidade do mapa. A figura 2.2 (b) apresenta diferentes valores do parâmetro a quando este for modificado não causa mudança na distribuição de probabilidade, apenas desloca o ponto onde ocorre a mudança de inclinação da função.

2.2.2 Mapa Logístico

Um dos sistemas clássicos que apresentam comportamento caótico é o mapa logístico. Destaca-se por sua grande variedade de comportamentos dinâmicos possíveis de serem observados, é definido como [5]:

$$x_{n+1} = ax_n(1 - x_n), \quad (2.22)$$

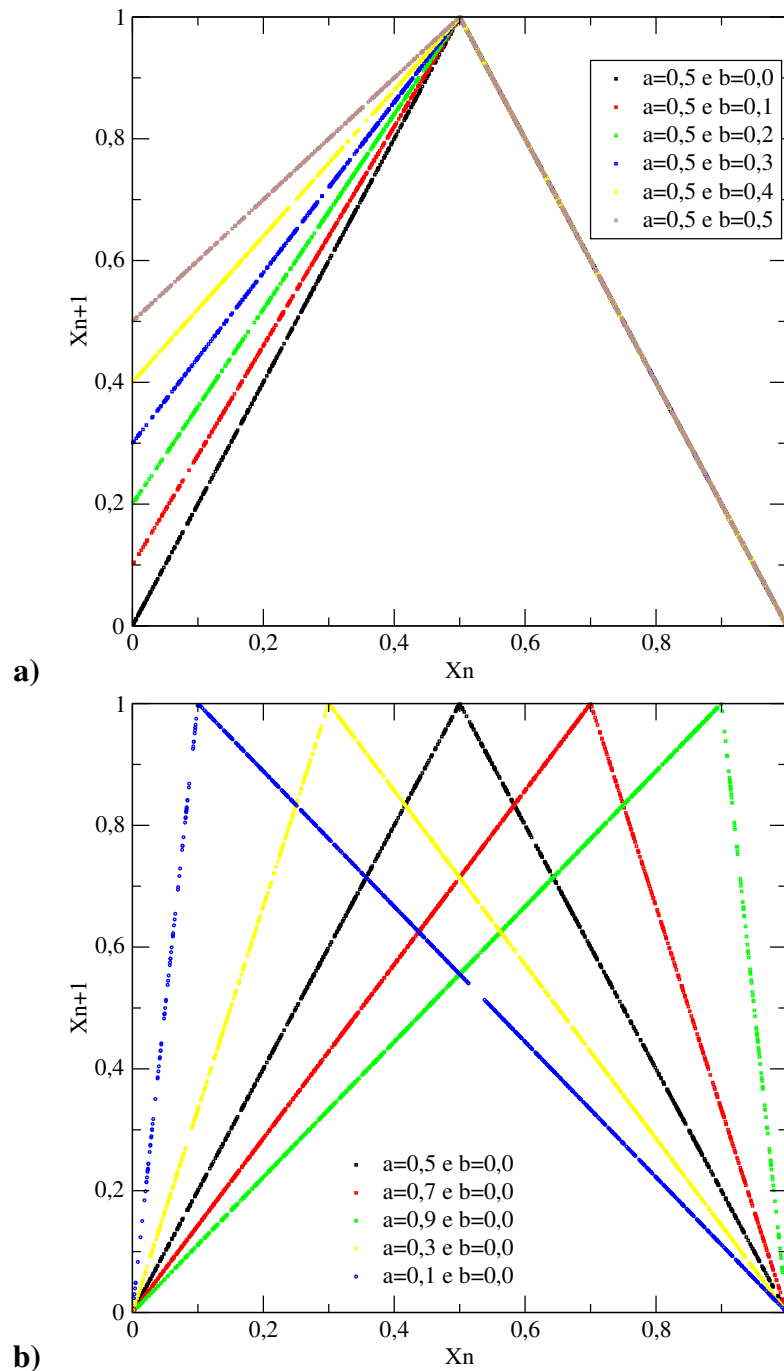
onde $a \in [0; 4]$, o parâmetro a é chamado de parâmetro de bifurcação, pois, a modificação deste implica em mudança na dinâmica do sistema. É possível observar as mudanças do mapa em termos do parâmetro a a partir da figura 2.3, onde temos os pontos para os quais a trajetória caótica evolui após 10000 iteradas.

A partir do diagrama de bifurcação é possível observar que o mapa depois de um tempo transiente converge para um ponto fixo se $a \in [1; 3]$, quando o valor de a está na região entre 3 e aproximadamente 3,57, então, a dinâmica do sistema converge para um comportamento periódico. Um fato interessante é que a medida que a vai aumentando o período de oscilação aumenta até que a dinâmica se torne caótica com $a \in [3,57; 4]$. Este fator interessante é conhecido como sendo um dos mecanismos capazes de produzir caos, chamado de rota para o caos a partir da duplicação de período ou rota de Feigenbaum [5]. Entre a região $[3,57; 4]$, existem, algumas regiões pequenas que voltam a apresentar periodicidade de forma similar ao digrama de bifurcação, conforme podemos observar na figura 2.4.

Regiões como as descritas pela figura 2.4 são conhecidas como janelas de periodicidade. É possível identificá-las a partir do expoente de Lyapunov do mapa logístico.

²Na versão original conhecido como *skew tent map* [12].

Figura 2.2: Mapa da Tenda Generalizado Assimétrico. Em (a) variação do parâmetro b ; em (b) variação do parâmetro a .



2.3 Rede de Mapas Acoplados

As redes de mapas acoplados são modelos dinâmicos que descrevem a evolução de sistemas espacialmente estendidos no tempo [25]. Uma rede de mapas acoplados (sistema) consiste de diversos mapas (subsistemas) interagindo conforme alguma regra de acoplamento. Desta forma uma rede de mapas acoplados é determinada por um vetor de estado contínuo em um espaço e

Figura 2.3: O gráfico representa os valores de x possíveis para cada valor do parâmetro a depois de 10000 iteradas do mapa descrito pela equação (2.22).

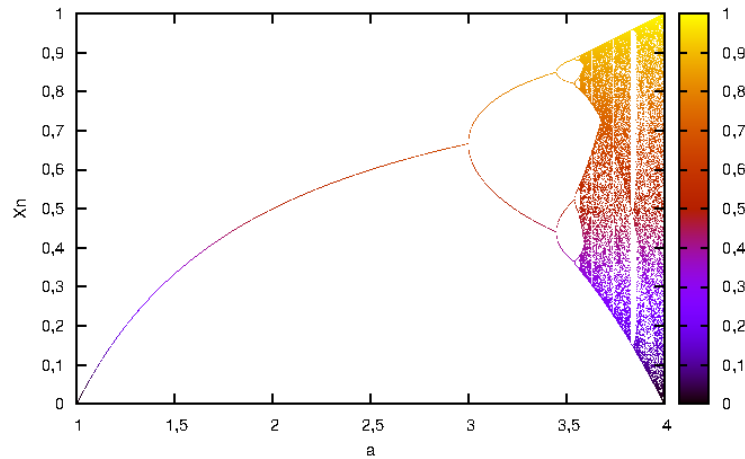
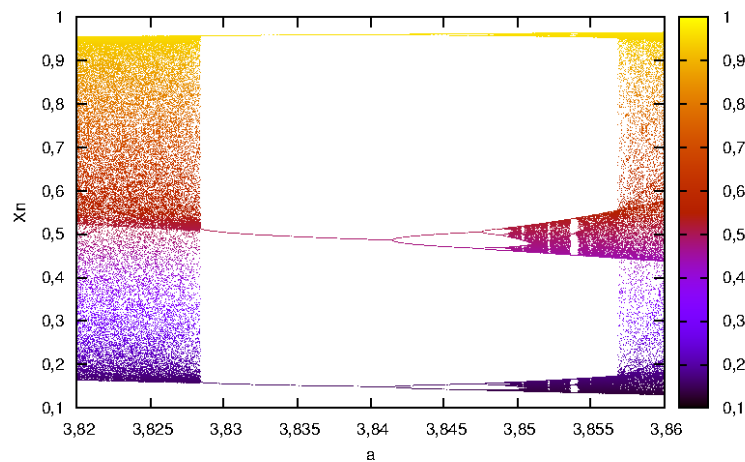


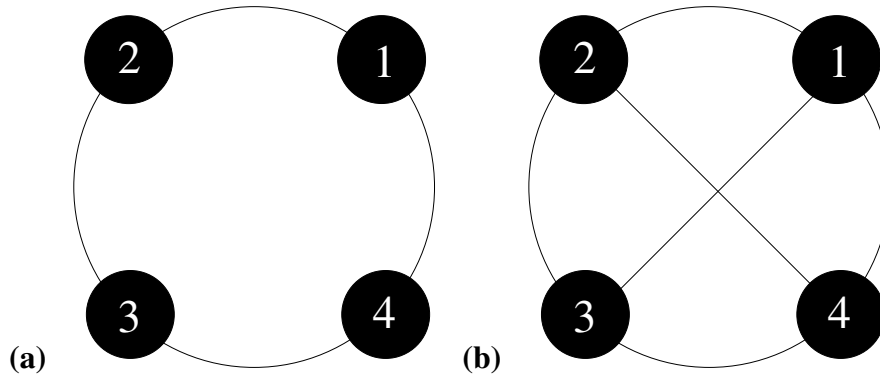
Figura 2.4: Janela de periodicidade no diagrama de bifurcação do mapa logístico.



tempo discretos [14].

Uma rede de mapas pode ser compreendida como um grafo onde os sítios são os vértices e as conexões determinadas pelas regras de acoplamento são as arestas [24]. Um mapa pode interagir apenas com seus vizinhos mais próximos, bem como com sítios mais distantes. Quando todos os sítios da rede estão apenas acoplados com seus primeiros vizinhos a rede é do tipo local, conforme a figura 2.5 (a). Se todos os sítios da rede estão acoplados entre si então o acoplamento é global, conforme a figura 2.5 (b).

Figura 2.5: Em (a) acoplamento local; em (b) acoplamento global.



Outras formas de redes mais sofisticadas podem ser encontradas na literatura, como as redes do tipo *scale-free* (sem-escala) [26] e as redes do tipo *small-world* (mundo pequeno) [27]. As redes do tipo *scale-free* são redes onde poucos sítios da rede possuem muitas conexões e muitos sítios possuem poucas conexões. A quantidade de conexões que cada sítio em uma rede sem escala obedece uma lei de potência [28]. Descrevem comportamentos como o de páginas de *internet*, rodovias, ligações aéreas. Está presente ainda em redes de neurônios do córtex cerebral, na formação de complexos proteicos como o caso da levedura de cerveja *Saccharomyces cerevisiae* e propagação de epidemias.

As redes do tipo mundo pequeno ou *small-world* são caracterizadas por conexões locais entre os sítios da rede acompanhadas de um pequeno número de conexões não-locais distribuídas aleatoriamente na rede [29]. O nome atribuído a este tipo de acoplamento é em função das cartas de Milgram, que comprovaram que o grau de separação de todas as pessoas do mundo é seis³. Redes sociais, aglomerados de neurônios, podem ser descritos a partir de redes do tipo mundo pequeno.

Embora possam existir muitas outras configurações de acoplamento, ao longo da dissertação nos limitaremos a estudar redes que se caracterizam por acoplamentos locais.

2.3.1 Classes de Acoplamento Local

A forma geral de uma rede que possui acoplamento local é:

$$x_{n+1}^{(i)} = f(x_n^{(i)}) + \varepsilon_0 g(x_n^{(i)}) + \varepsilon_{RG}(x_n^{(i+1)}) + \varepsilon_{LG}(x_n^{(i-1)}) \quad (2.23)$$

³Pesquisas atuais têm demonstrado que este número pode ser menor.

o vetor $\vec{\varepsilon} = (\varepsilon_0, \varepsilon_R, \varepsilon_L)$ é o núcleo de acoplamento [30]. A função $g(x)$ fornece a dinâmica do acoplamento. Os casos onde $g(x) = x$ é chamado de acoplamento linear; se $g(x) = f(x)$, onde $f(x)$ é a função que contém a dinâmica local, ou seja, a dinâmica do mapa desacoplado, então o acoplamento é do tipo futuro. A simetria de um núcleo de acoplamento é determinado a partir dos valores de acoplamento $\varepsilon_0, \varepsilon_R$ e ε_L . Alguns casos importantes:

Acoplamento laplaciano é um caso simétrico onde $-\frac{\varepsilon_0}{2} = \varepsilon_R = \varepsilon_L$, também conhecido como acoplamento do tipo primeiros vizinhos, conforme apresentado na figura 2.5 (a).

Acoplamento unidirecional é o mais simples caso anti-simétrico, pois o acoplamento é inserido apenas em uma direção, neste caso o núcleo de acoplamento é dado como $-\varepsilon_0 = \varepsilon_L$ e $\varepsilon_R = 0$ ou então, $\varepsilon_R = 0$ e $\varepsilon_L = -\varepsilon_0$.

O acoplamento ainda pode possuir condições de contorno. É comum redes de mapas acoplados apresentarem condições de contorno periódicas.

2.4 Sincronização de Caos

Um dos fenômenos mais curiosos que envolvem sistemas caóticos é o fato de duas trajetórias caóticas evoluídas a partir de condições iniciais distintas podem sincronizar depois de um tempo de evolução transiente. O fenômeno de sincronização de caos é observado em diversos sistemas físicos como, osciladores acoplados, marca passos implantado no coração de pessoas com problemas cardíacos, e muitos outros [31].

Quando temos duas trajetória caóticas correlacionadas podemos determinar o expoente de Lyapunov do sistema a partir da equação (2.11). Obtendo, desta maneira, dois valores de expoente, é comum classificar os expoentes de Lyapunov a partir de sua intensidade, da maior para a menor. Se o primeiro resultado for positivo e o segundo for negativo, indica que o sistema é caótico e a condição de sincronização, se ocorrer, é estável e eles tendem a evoluir assintoticamente para um estado sincronizado mesmo iniciando de condições distintas [32]. Pecora demonstrou que este resultado é válido para sistemas com mais de duas dimensões [32].

Se assumirmos duas variáveis X e Y cuja dinâmica local é descrita pelo mapa da tenda e estão sujeitos a uma mesma intensidade de acoplamento entre si, conforme descrito pela equação (2.13) então, temos que o primeiro expoente de Lyapunov é $\Lambda_1 = \ln(2)$ e o segundo expoente de Lyapunov é $\Lambda_2 = \Lambda_1 + \ln(1 - 2\varepsilon)$. A sincronização completa ocorrerá se $\Lambda_2 < 0$ ou então $\varepsilon > \frac{1}{2}$.

3 *Mapa da Tenda Assimétrico Generalizado com Acoplamento Local*

O propósito deste capítulo é explorar as quantidades definidas no primeiro capítulo, como a entropia de Shannon, a informação mútua e a entropia de transferência, para um modelo simples de sistema dinâmico que consiste de dois mapas da tenda assimétrico generalizado com diferentes configurações de acoplamento local. A escolha do mapa e do acoplamento é devida à facilidade para a extração de resultados analíticos.

Conforme já apresentado no capítulo anterior o mapa da tenda assimétrico generalizado é descrito pela equação:

$$x_{n+1} = \begin{cases} b + ((1-b)/a)x_n & \text{se } 0 \leq x \leq a \\ (1-x_n)/(1-a) & \text{se } a < x \leq 1 \end{cases}, \quad (3.1)$$

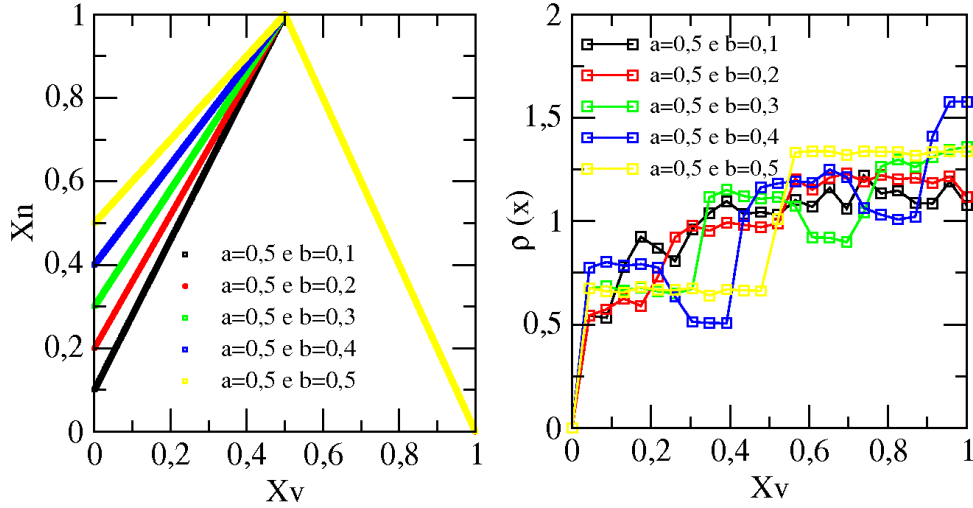
onde $0 < a < 1$ e $0 < b < 1$. Nas figuras 2.2 (a) e 2.2 (b) são mostradas as modificações ocorridas na forma da função quando variamos os parâmetros a e b . Enquanto as modificações do parâmetro a preservam a mesma densidade de probabilidade, as modificações no parâmetro b implicam em modificação na densidade de probabilidade do mapa que está restrito ao domínio $[0; 1]$. A figura 3.1 (b) nos mostra que a densidade de probabilidade perde sua uniformidade quando $b \neq 0$.

É importante determinar o expoente de Lyapunov do mapa para verificar as regiões onde ele apresenta comportamento caótico. Pode ser determinado a partir da equação (2.6), a derivada do mapa será

$$f'(x) = \begin{cases} \frac{(1-b)}{a} & \text{se } 0 \leq x \leq a \\ \frac{-1}{(1-a)} & \text{se } a < x \leq 1 \end{cases}, \quad (3.2)$$

sendo a e b parâmetros. A variação da função é definida em termos de valores constantes, desta

Figura 3.1: A figura (a) mostra o mapa da tenda assimétrico egeneralizado com $a = 0,5$ e diferentes parâmetros b enquanto a figura (b) mostra a respectiva mudança na distribuição, foram utilizados 23 partições para a construção dos histogramas.



forma o expoente de lyapunov do mapa será

$$\lambda = \ln\left(\frac{1-b}{a}\right) \int_0^a \rho(x) dx + \ln\left(\frac{1}{1-a}\right) \int_a^1 \rho(x) dx, \quad (3.3)$$

para o caso particular $b = 0$ a solução é analítica [12]

$$\lambda = -a \ln(a) - (1-a) \ln(1-a). \quad (3.4)$$

As regiões que apresentam valores positivos representam as regiões onde a dinâmica do mapa é caótica. Podemos observar para diferentes valores de a e b os respectivos valores do expoente de Lyapunov a partir da figura 3.2.

Ainda na figura 3.2 podemos observar uma região lilás que corresponde a supressão de caos.

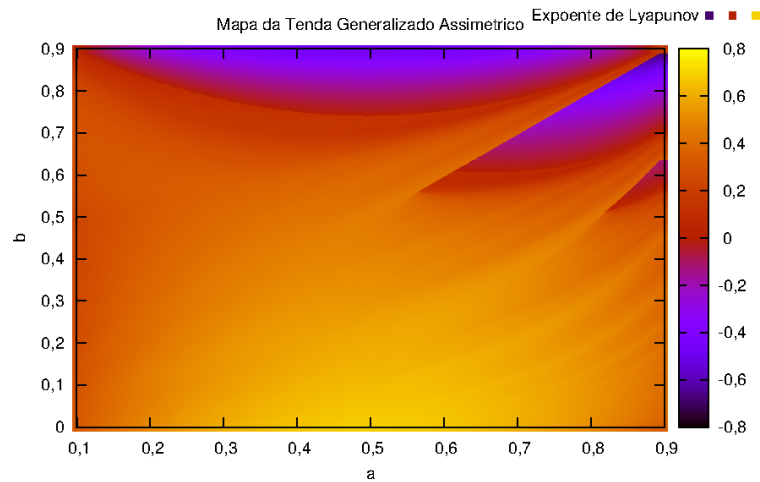
3.1 Dois Mapas Acoplados

Para estudar como ocorre a interação do mapa da tenda assimétrico generalizado, o primeiro passo é estudar as diferentes configurações de acoplamento do tipo futuro. A equação que descreve a evolução temporal de duas variáveis X e Y , respectivamente, é da forma:

$$x_{n+1} = (1-\varepsilon)f(x_n) + \varepsilon f(y_n) \quad (3.5)$$

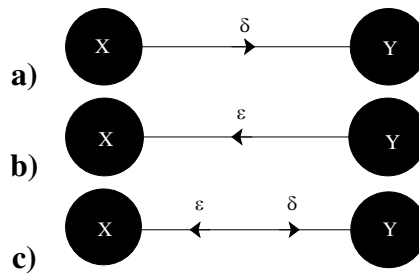
$$y_{n+1} = (1-\delta)f(y_n) + \delta f(x_n), \quad (3.6)$$

Figura 3.2: Os valores do expoente de Lyapunov são apresentados em escala de cores.



onde $f(x)$ é o mapa e $\varepsilon, \delta \in [0; 1]$. Desta forma existe uma interação entre as variáveis X e Y onde as intensidades de acoplamento não são necessariamente idênticas. Esta forma de acoplamento pode ser dividida em três casos, o acoplamento bidirecional descrito pela figura 3.3 (c) e o acoplamento unidirecional em ambos os sentidos conforme mostram as figuras 3.3 (a) e (b).

Figura 3.3: Configurações de acoplamento. (a) Acoplamento unidirecional $X \rightarrow Y$ (b) Acoplamento unidirecional $Y \rightarrow X$ (c) Acoplamento bidirecional.



É necessário determinar se a dinâmica do sistema é caótica. No caso para os quais $\varepsilon = \delta$ e $b = 0$ podem ser obtidos analiticamente, um caso mais particular, com $a = 0,5$ foi resolvido no capítulo anterior. A solução do expoente de Lyapunov para o subspaço de sincronização, ou seja, para os casos onde $x = y$, pode ser determinada a partir da equação (2.11). Neste caso teremos duas matrizes jacobianas possíveis uma quando $x, y \in [0; a]$ que vamos rotular como o evento 00 e o outro caso quando $x, y \in (a; 1]$ que vamos rotular como o evento 11. Para facilitar os cálculos introduziremos as constantes, $k_1 = \frac{(1-b)}{a}$ e $k_2 = \frac{1}{(1-a)}$. Dessa formas as matrizes

jacobianas possíveis serão:

$$DF(0,0) = k_1 \begin{pmatrix} (1-\varepsilon) & \varepsilon \\ \delta & (1-\delta) \end{pmatrix} \quad (3.7)$$

e

$$DF(1,1) = k_2 \begin{pmatrix} (1-\varepsilon) & \varepsilon \\ \delta & (1-\delta) \end{pmatrix}, \quad (3.8)$$

as soluções para as equações de autovalores das matrizes acima diferem apenas no termo constante que multiplica a matriz e os autovalores são os mesmos obtidos na solução da matriz da equação (2.13), desta forma teremos:

$$\begin{aligned} \Lambda_1(0,0) &= \ln k_1 \\ \Lambda_2(0,0) &= \Lambda_1(0,0) + \ln(|1-d|) \end{aligned} \quad (3.9)$$

e

$$\begin{aligned} \Lambda_1(1,1) &= \ln k_2 \\ \Lambda_2(1,1) &= \Lambda_1(1,1) + \ln(|1-d|), \end{aligned} \quad (3.10)$$

onde $d = \varepsilon + \delta$. Os expoentes de Lyapunov para o par de mapas acoplados serão

$$\Lambda_1 = p(0,0)\Lambda_1(0,0) + p(1,1)\Lambda_1(1,1) \quad (3.11)$$

$$\Lambda_2 = \Lambda_1 + \ln(|1-d|), \quad (3.12)$$

este resultado é importante, pois, basta estimar a distribuição de probabilidade para determinar o valor do expoente de Lyapunov. Para o caso particular $b = 0$ o resultado é completamente analítico [12] e temos então

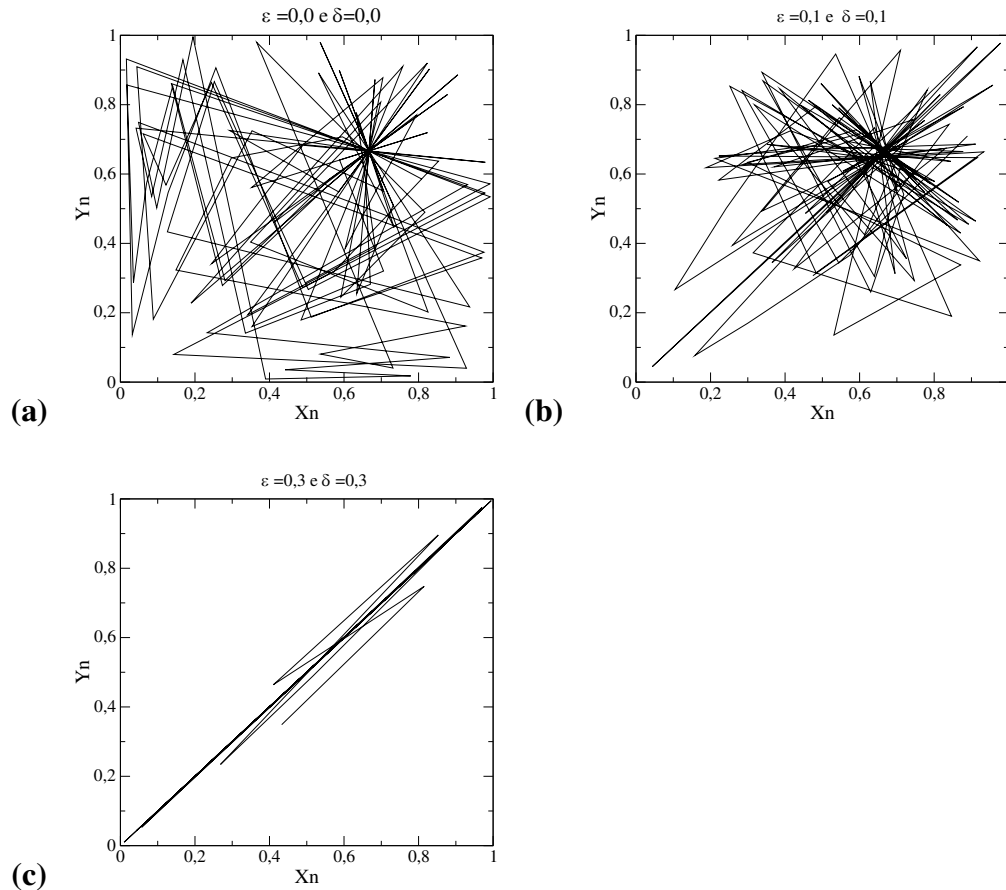
$$\Lambda_1 = -a \ln(a) - (1-a) \ln(1-a) \quad (3.13)$$

$$\Lambda_2 = \Lambda_1 + \log(|1-d|). \quad (3.14)$$

Pode-se observar que a equação (3.13) é a mesma obtida na equação (3.4). O primeiro expoente de Lyapunov, Λ_1 é o expoente de Lyapunov do mapa desacoplado. Quando o segundo expoente de Lyapunov, o qual está associado a correlação entre as variáveis, for menor do que 0, então, será a região onde, para quaisquer condições iniciais no intervalo $[0; 1]$ das variáveis X e Y , elas irão convergir assintoticamente para a sincronização de caos. As figuras 3.4 (a),(b) e (c) mostram como se modificam os estados acessíveis quando ocorre sincronização. Na figura 3.4 (a) todo o plano $\{xy|x \in [0, 1] \text{ e } y \in [0, 1]\}$ é preenchido com a evolução temporal. A medida que

a intensidade de acoplamento (ε e δ) entre as variáveis aumenta, as variáveis X e Y passam a se aproximar cada vez mais da reta $x = y$, diminuindo o espaço acessível, conforme pode-se observar pela figura 3.4 (b). Quando ocorre sincronização as trajetórias convergem assintoticamente para o subespaço de sincronização, $x = y$, como mostra a figura 3.4 (c).

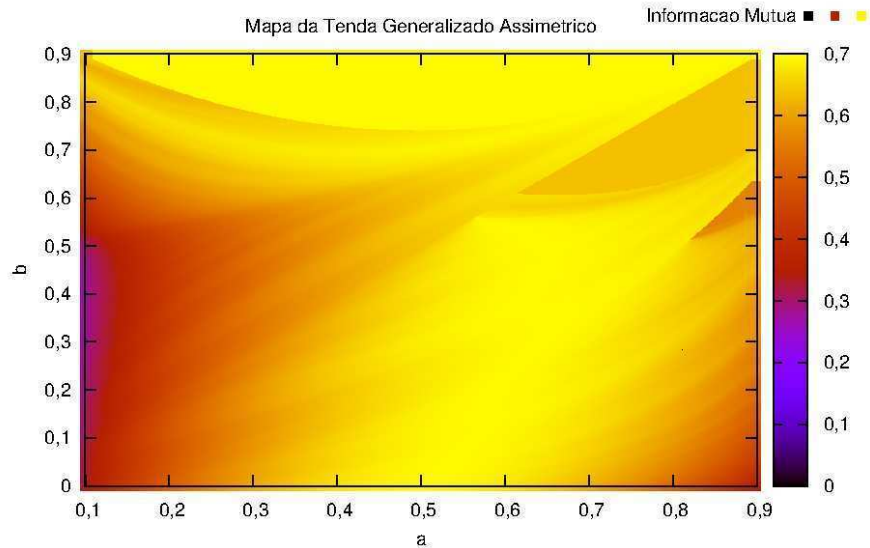
Figura 3.4: Algumas diferenças em consequência do acoplamento: (a) Caso desacoplado (b) Acoplamento fraco (c) Acoplamento forte (sincronização).



Outra quantidade que pode ser extraída deste modelo é a informação mútua. Podemos aplicar a definição descrita pela equação (1.30) que nos permitirá determinar a quantidade de informação que as variáveis X e Y estão compartilhando. O particionamento do espaço de fase é feito de acordo com a derivada do mapa da tenda generalizado assimétrico, desta forma, definimos a partição 0 como sendo a partição da esquerda onde $x, y \in [0, a]$ e 1 a partição da direita onde $x, y \in (a, 1]$. O resultado pode ser observado a partir da figura 3.5.

Novamente o caso particular $b = 0$ pode ser determinado analiticamente, a partir de um raciocínio simples. A distribuição de probabilidade de cada mapa individual, quando estão no regime de sincronização de caos é idêntico ao de um mapa desacoplado. Então seguindo as partições definidas, as respectivas probabilidades serão:

Figura 3.5: Valor da informação mútua para diferentes valores de a e b .



$$p(x) = p(y) = \begin{cases} p(0) = a \\ p(1) = 1 - a \end{cases} \quad (3.15)$$

$$p(x,y) = \begin{cases} p(00) = a \\ p(01) = 0 \\ p(10) = 0 \\ p(11) = (1 - a) \end{cases}, \quad (3.16)$$

desse modo a informação mútua será:

$$I(X;Y) = -a \ln(a) - (1 - a) \ln(1 - a). \quad (3.17)$$

Podemos ver então que a equação (3.17) e a equação (3.13) são idênticas. Ou seja, a medida da informação mútua é idêntica a medida do expoente de Lyapunov positivo. Esse fato é observado, pois, quando a região onde o fenômeno de sincronização de caos ocorre, ambos os valores convergem para o mesmo resultado [15].

3.2 Direcionalidade de Sinais Correlacionados

Iremos nos limitar aos casos onde o mapa da tenda generalizado assimétrico descrito pela equação (3.1) possui parâmetro $b = 0$. O propósito desta seção é demonstrar que é possível determinar a direção de acoplamento entre duas séries temporais a partir da informação que uma variável transfere para a outra. Para isso utilizaremos duas variáveis X e Y descritas pelo conjunto de equações (3.5) e (3.6), com a diferença que cada variável possui um valor distinto do parâmetro a [33], ou seja,

$$x_{n+1} = \varepsilon f_1(y_n) + (1 - \varepsilon)f_2(x_n) \quad (3.18)$$

$$y_{n+1} = \delta f_1(x_n) + (1 - \delta)f_2(y_n), \quad (3.19)$$

onde as funções f_1, f_2 indicam que cada variável está associada com um valor distinto de a .

É possível medir a quantidade de informação que uma variável envia para outra a partir da entropia de transferência [10]. A entropia de transferência neste caso será:

$$T_{X \rightarrow Y} = \bullet p(x_{n+1}, x_n^{(k)}, y_n^{(l)}) \log \frac{p(x_{n+1} | x_n^{(k)}, y_n^{(l)})}{p(x_{n+1} | x_n^{(k)})} \quad (3.20)$$

$$T_{Y \rightarrow X} = \bullet p(y_{n+1}, y_n^{(k)}, x_n^{(l)}) \log \frac{p(y_{n+1} | y_n^{(k)}, x_n^{(l)})}{p(y_{n+1} | y_n^{(k)})}, \quad (3.21)$$

onde $T_{X \rightarrow Y}$ é a quantidade de informação que a variável X transfere para Y e $T_{Y \rightarrow X}$ é quantidade de informação de Y para X . Também assumiremos que $k = l = 1$, que representa que o estado futuro de uma variável depende apenas do seu estado anterior. Os casos que iremos estudar são os casos apresentados na figura 3.3:

Caso I acoplamento unidirecional $X \rightarrow Y$;

Caso II acoplamento unidirecional $Y \rightarrow X$;

Caso III acoplamento bidirecional $X \leftrightarrow Y$;

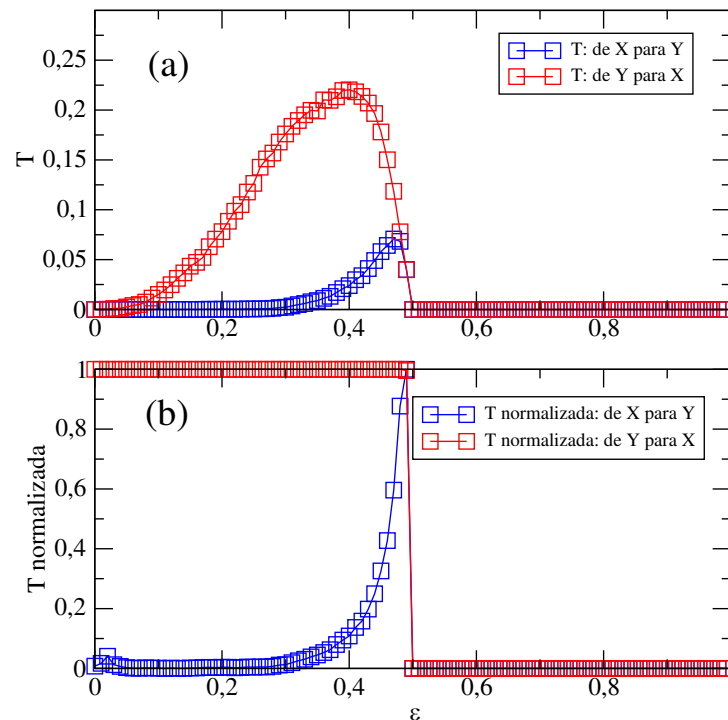
Para determinar a direção de acoplamento entre as variáveis X e Y vamos utilizar a entropia de transferência normalizada [34]:

$$t_{X \rightarrow Y} = \frac{T_{X \rightarrow Y}}{\max\{T_{X \rightarrow Y}, T_{Y \rightarrow X}\}} \quad (3.22)$$

$$t_{Y \rightarrow X} = \frac{T_{Y \rightarrow X}}{\max\{T_{X \rightarrow Y}, T_{Y \rightarrow X}\}}. \quad (3.23)$$

Quando o acoplamento é unidirecional a entropia de transferência deve ser positiva no sentido em que existe um acoplamento, como os casos I e II. Para demonstrar este comportamento nas figuras 3.6 (a) e (b) apresentamos um exemplo onde apenas Y influencia a variável X ($\delta = 0$). Neste caso, o acoplamento é do tipo mestre-escravo. A configuração mestre-escravo é caracterizada por uma variável sendo independente (variável mestre) e outra dependente (variável escrava). A figura 3.6 (a) representa a medida da transferência de entropia em ambos os sentidos. Podemos observar que existe uma medida de entropia de transferência no sentido contrário ao acoplamento, devido a flutuação estatística. A figura 3.6 (b) nos permite ver claramente qual é o sentido do acoplamento entre as variáveis onde Y é quem transfere informação para X , ou seja, caso II. O valor nulo da entropia de transferência quando $\varepsilon > 0,5$ é devido ao fenômeno de sincronização, onde não existe correlação entre as variáveis, ou seja, uma variável não influencia a outra, pois, ambas comportam-se como se fossem independentes do acoplamento.

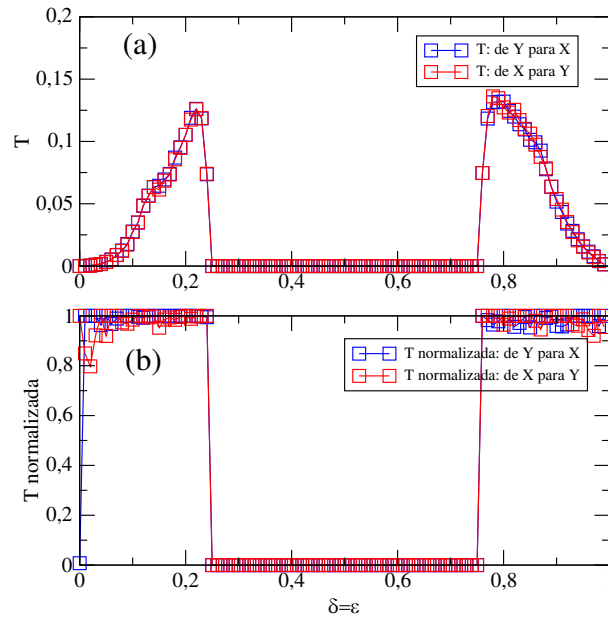
Figura 3.6: A figura (a) representa as medidas da entropia de transferência nas duas direções de acoplamento. Os parâmetros $a_1 = a_2 = 0,5$ para as variáveis X e Y . Na figura (b) temos a entropia de transferência normalizada indicando que apenas a variável X recebe informação da variável Y .



Nas figuras 3.7 (a) e (b) temos uma análise de uma configuração particular do caso III onde temos um acoplamento bidirecional com $\varepsilon = \delta$. O caso III nos mostra que existe transferência de informação tanto da variável X em Y como o contrário também ocorre.

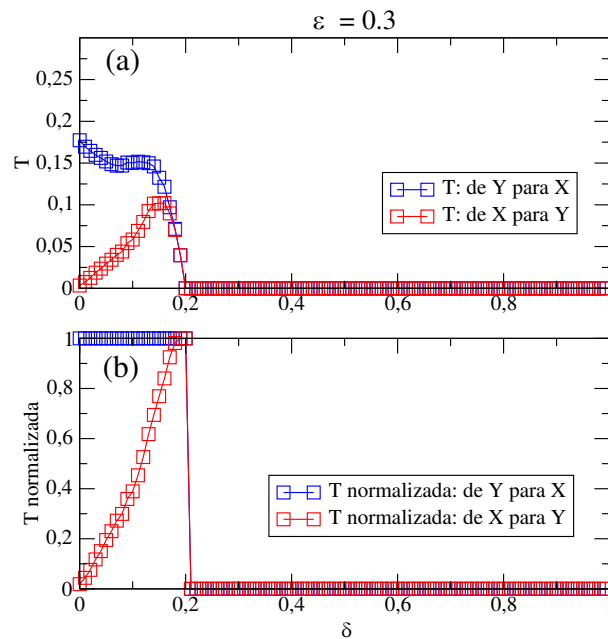
Para situações do caso III onde as intensidades de acoplamento do caso bidirecional são diferentes para as variáveis X e Y ainda é possível identificar que existe entropia de trans-

Figura 3.7: A figura (a) nos mostra que a transferência de informação de uma variável sobre a outra é idêntica, como esperado devido a $\varepsilon = \delta$. A figura (b) nos mostra a intensidade da entropia de transferência. Neste caso temos $a_1 = a_2 = 0,5$.



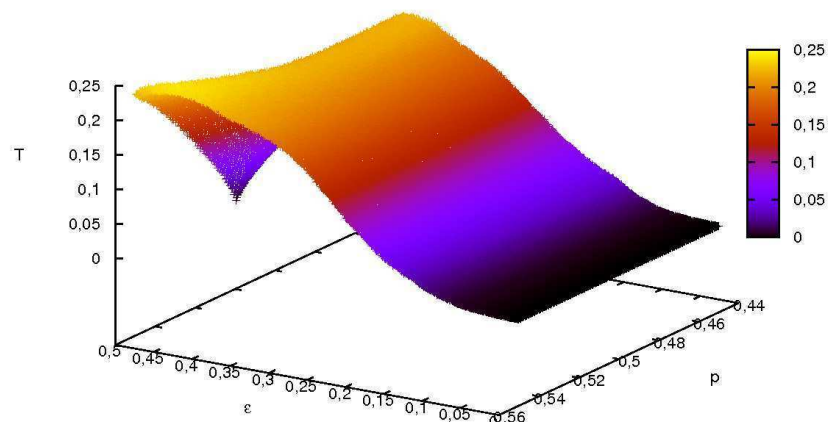
ferência em ambos os sentidos mesmo quando as intensidades são diferentes. Na figura 3.8 (a) e (b) temos a entropia de transferência e sua normalização respectivamente, podemos observar claramente que quando os acoplamentos são distintos a entropia de transferência também é distinta.

Figura 3.8: A figura (a) nos mostra que a transferência de informação de uma variável sobre a outra é distinta para intensidades de acoplamento distintas. A figura (b) nos mostra entropia de transferência normalizada. Neste caso temos $a_1 = a_2 = 0,5$.

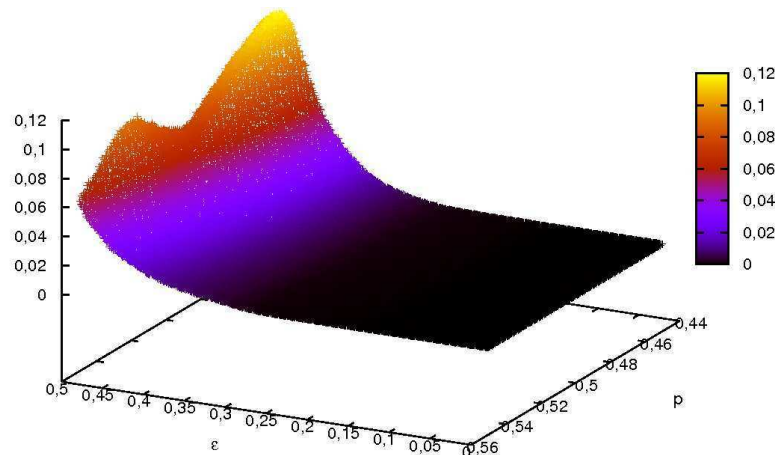


A entropia de transferência normalizada nos permite determinar claramente qual o sentido da transferência de informação e conseqüentemente o sentido de acoplamento. Para garantir-mos que a entropia de transferência é uma quantidade robusta para determinar a direção de acoplamento, fixamos o parâmetro da variável X como sendo $a_1 = 0,5$ e variamos o parâmetro da variável Y na vizinhança de a_1 . Podemos ver um panorama geral da medida da entropia de transferência para os casos I e II, a partir das figuras 3.9 (a) e (b).

Figura 3.9: (a) Entropia de Transferência $X \rightarrow Y$. (b) Entropia de Transferência $Y \rightarrow X$. O parâmetro p representa os diferentes valores de a_2 enquanto $a_1 = 0,5$ é mantido constante, temos ainda $\delta = 0$ e $\varepsilon \neq 0$.



(a)

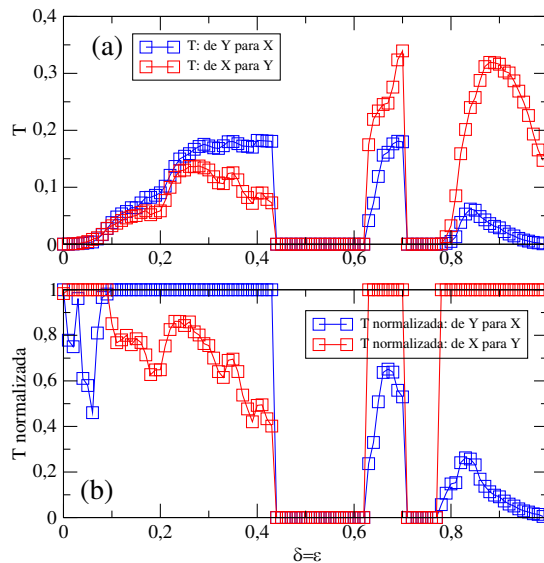


(b)

Para verificarmos que é possível distinguir a quantidade de informação transmitida de uma variável para outra no caso III, podemos analisar uma configuração na qual ambos sofrem a mesma intensidade de acoplamento $\varepsilon = \delta$ porém existe uma diferença entre a_1 e a_2 . Esta diferença muda a transmissão de informação, pois, ela desencadeia uma mudança nos estados acessíveis. Nas figuras 3.10 (a) e (b) escolhemos $a_1 = 0,5$ e $a_2 = 0,3$.

Os resultados apresentados nos permitem perceber a eficiência da entropia de transferência

Figura 3.10: As figuras (a) e (b) mostram que a transferência de informação de uma variável sobre a outra deixa de ser idêntica para diferentes valores de a .



para determinar o sentido do fluxo de informação. Esta característica direcional é importante em diversos estudos envolvendo principalmente séries temporais. Determinar a direção de fluxo de informação é extremamente importante no caso da bolsa de valores, por exemplo, pois, permite determinar se um determinado índice da bolsa é ou não influenciado por outros índices de mercado [35]. Ou seja, é possível analisar influências de um sistema qualquer sobre outro.

4 *Sistemas de Comunicação usando Caos*

Como resultado final desta dissertação este capítulo tem como finalidade mostrar a aplicabilidade da conexão entre teoria da informação e sistemas dinâmicos. O ponto chave é o uso de sistemas dinâmicos para a transmissão de informação de forma segura. Mecanismos que tratam de sistemas de comunicação envolvendo caos não são novidades na literatura [32], [36]. Todavia, ainda representam um tema atual de pesquisa [15], [37]. Em geral sistemas de comunicação usando caos consistem em transmissão de informação utilizando o fenômeno de sincronização de caos. Uma nova abordagem utilizando entropia de transferência para transmissão de dados surgiu com Hung e Hu [16]. Construímos a partir do modelo de Hung e Hu um mecanismo mais seguro e com maior velocidade de transmissão de dados unindo o fenômeno de sincronização com a entropia de transferência.

4.1 Sistema de Comunicação Básico

Os componentes elementares de um sistema de comunicação, conforme mostrado na figura 4.1, são [8]:

Fonte de Informação: Produz a mensagem ou a sequência de mensagens que deverá ser transmitida para o destinatário. Pode ser uma sequência de letras, uma função que oscila no tempo como no caso do rádio ou uma função que varia no tempo e no espaço como no caso da televisão.

Transmissor: Atua como um codificador da mensagem em um sinal que possa ser transmitido para o destinatário através do canal. Por exemplo, quando falamos ao telefone existe uma codificação de nossa voz em pulsos elétricos que são enviados para um destinatário.

Canal: Representa o meio pelo qual a mensagem é enviada do transmissor para o receptor. No caso de uma ligação telefônica o canal representa a linha telefônica que liga o reme-

tente ao destinatário. No caso de mecanismos digitais a própria internet é um canal de comunicação.

Receptor: Realiza a operação inversa daquela feita pelo transmissor, atua como um decodificador do sinal, transformando-o em uma mensagem novamente. Quando recebemos uma ligação telefônica ocorre a decodificação dos pulsos elétricos novamente em uma onda sonora.

Destinatário: É a pessoa ou objeto para quem a mensagem foi enviada.

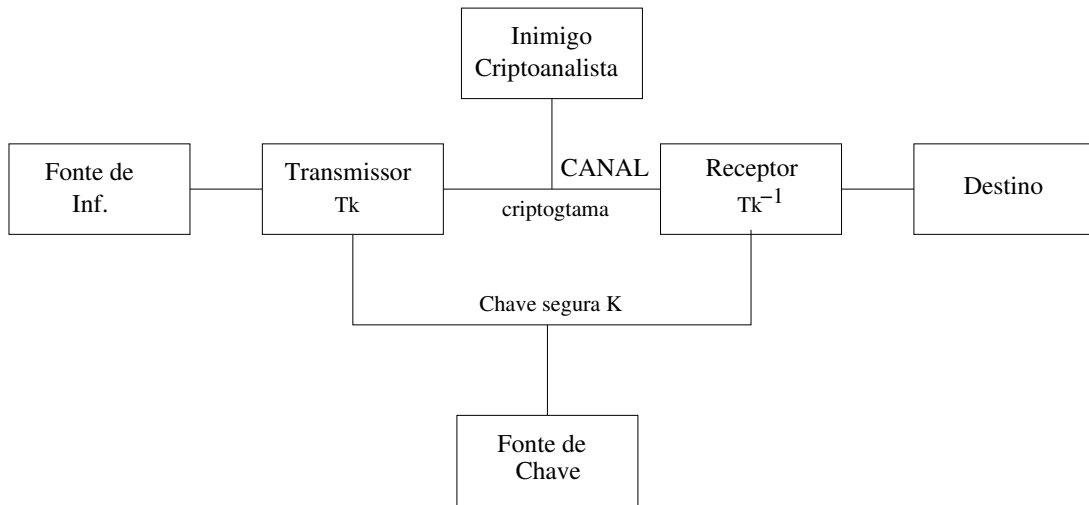
Figura 4.1: Diagrama esquemático de um sistema de comunicação.



Em sistemas de comunicação reais o canal de comunicação está sujeito a uma fonte de ruído atuando sobre ele, todavia, sistemas com presença de ruídos não serão analisados, pois, o objetivo é a construção de diferentes abordagens para sistemas de comunicação e não o desenvolvimento prático destes modelos.

Shannon definiu ainda em 1948 os mecanismos que um sistema de comunicação precisa ter para transmitir informação de forma segura [38]. Podemos ver um esquema deste mecanismo proposto a partir da figura 4.2. Enquanto para uma comunicação usual basta transformar a mensagem em um sinal capaz de ser transmitido entre um remetente e um destinatário no caso de um mensagem que precisa ser protegida é necessário que este sinal seja um criptograma. Este criptograma deve ser construído de forma que impeça um inimigo criptoanalista de descobrir a mensagem. A construção do criptograma ocorre com o transmissor transformando o sinal em um código através de uma função T realizando deste modo uma cifragem do sinal. O receptor para decifrar a mensagem deve atuar no sinal a função inversa T^{-1} da aplicada pelo transmissor. Para decifrar a mensagem é comum associar uma chave de segurança k ao sistema. Quando o emissor e o receptor são os únicos que conhecem a chave de segurança podem então se comunicar secretamente. Para aumentar a segurança é comum que exista uma fonte de chave de segurança, ou seja, existem diferentes chaves para decifrar o sinal, mas apenas a chave correta permite esta operação.

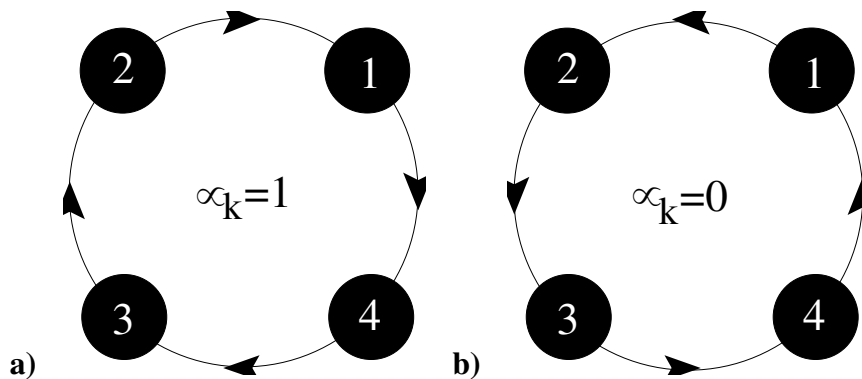
Figura 4.2: Diagrama esquemático de um sistema de comunicação segura. O inimigo criptoanalista atua sobre o canal para tentar descobrir a mensagem.



4.2 Modelo de Hung e Hu

Conforme apresentado anteriormente a entropia de transferência é uma quantidade capaz de determinar efeitos causais em uma rede de mapas acoplados. O modelo de Hung e Hu apresenta um novo paradigma para comunicações seguras ao transmitir mensagem binárias escondidas na direção de acoplamento de um anel de mapas acoplados contendo dinâmica caótica [16]. Conforme mostrado nas figuras 4.3 (a) e (b), quando o acoplamento é no sentido horário então $\alpha_k = 1$ e quando o acoplamento do anel é no sentido anti-horário então $\alpha_k = 0$. O coeficiente k determina o k -ésimo símbolo de uma mensagem de tamanho K .

Figura 4.3: (a) Acoplamento no sentido horário ($\alpha_k = 1$) (b) Acoplamento no sentido anti-horário ($\alpha_k = 0$).



A dinâmica da rede de mapas é variável ao longo do tempo para que possa ser possível

transmitir símbolos distintos (0 ou 1), o acoplamento é similar ao acoplamento unidirecional

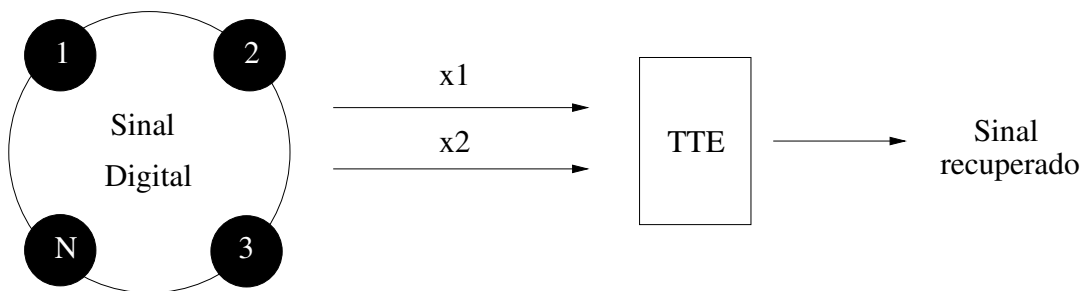
$$x_{n+1}^{(i)} = f((1 - \varepsilon)x_n^{(i)} + \varepsilon X_n) \quad (4.1)$$

$$X_n = \begin{cases} x_n^{(i-1)} & \text{se } \alpha^k = 1 \\ x_n^{(i+1)} & \text{se } \alpha^k = 0 \end{cases}, \quad (4.2)$$

onde i é um sítio da rede, n representa o instante de tempo e $\varepsilon \in [0, 1]$. A função $f(x)$ deve ser uma função que apresenta comportamento caótico, o mapa da tenda generalizado assimétrico no regime em que apresenta caos, assim como o mapa logístico são mapas que funcionam muito bem para este modelo. Uma das grandes vantagens no modelo de Hung e Hu é a independência na escolha da função não linear que deverá ser utilizada pelo mecanismo de comunicação. Em geral qualquer mapa caótico cuja função seja contínua funciona bem para mecanismos de transmissão usando entropia de transferência. A arbitrariedade na escolha de $f(x)$ ocorre porque o importante neste modelo é a interação de um sítio com a sua vizinhança e não as regras de evolução que determinam sua dinâmica individual.

O processo de transmissão da informação pode ser compreendido admitindo uma rede de tamanho N , o emissor envia as N séries temporais $x_n^{(1)}, \dots, x_n^{(N)}$, o receptor recebe todas as séries temporais e efetua uma medida da entropia de transferência em ambos os sentidos. Quando $T_{x^{(i)} \rightarrow x^{(i-1)}}$ é uma quantidade positiva então indica que o anel está acoplado no sentido anti-horário. Quando $T_{x^{(i)} \rightarrow x^{(i+1)}}$ é uma quantidade positiva então indica que o anel está acoplado no sentido horário. O esquema de transmissão pode ser observado a partir da figura 4.4.

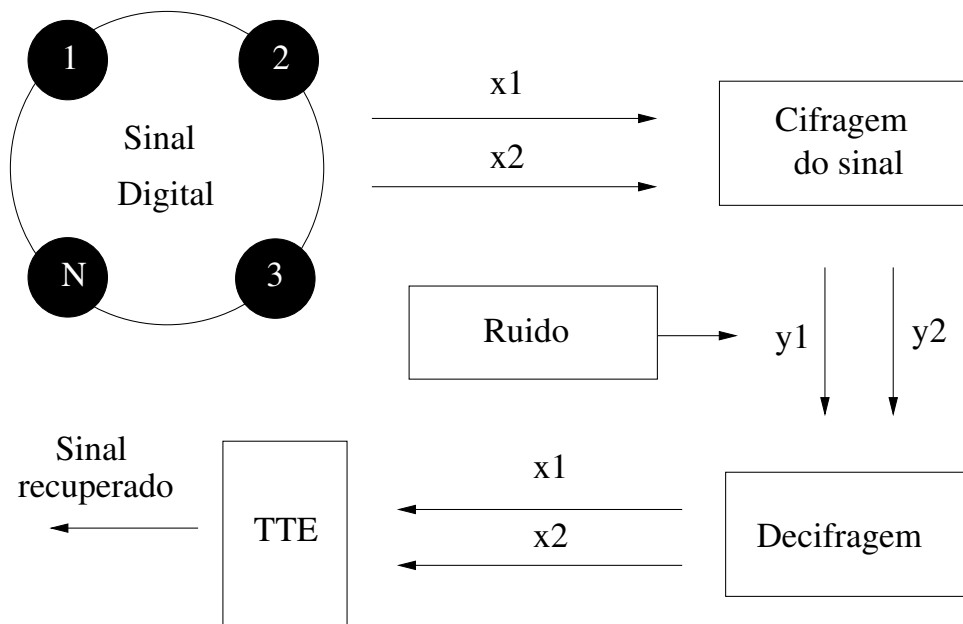
Figura 4.4: Processo de transmissão da informação.



Este procedimento permite ao destinatário receber a informação enviada. O mecanismo como está proposto na figura 4.4 não representa uma forma de transmissão segura. Caso um intruso tenha acesso as séries temporais ele poderá ler a mensagem binária que está sendo transmitida. Utilizando a ideia de criptografia proposta por Shannon [38], Hung e Hu propõem proteger o sinal utilizando uma função y para cada uma das séries temporais. Desta forma, o emissor protege o sinal emitindo um sinal cifrado da forma $y^{(i)} = h(x^{(i)}, k_i)$, onde k_i é a chave de segurança do i -ésimo sítio. O receptor para decifrar o sinal faz o processo inverso

ao do emissor $x^{(i)} = H(y^{(i)}, k_i)$, onde $H(x) = h^{-1}(x)$. Um esquema do mecanismo completo pode ser observado na figura 4.5. Quando a função $h(x)$ é escolhida corretamente ocorre a quebra de correlação entres as séries temporais de cada um dos sítios e a medida da entropia de transferência para os sinais criptografados não contem mais a mensagem original. Ou seja, $T_{x^{(i)} \rightarrow x^{(i-1)}} \neq T_{y^{(i)} \rightarrow y^{(i-1)}}$ e $T_{x^{(i)} \rightarrow x^{(i+1)}} \neq T_{y^{(i)} \rightarrow y^{(i+1)}}$, este é o procedimento que torna o sistema de comunicação segura contra intrusos.

Figura 4.5: Esquema geral do mecanismo de comunicação de Hung e Hu.



A entropia de transferência é uma quantidade que depende da probabilidade. Todavia, para cada sentido de acoplamento existe uma distribuição de probabilidade natural diferente. Para solucionar este problema podemos inserir uma quantidade que permite estimar a distribuição de probabilidade a cada instante de tempo. A distribuição de probabilidade atualizada será portanto

$$p(l)_{n+1} = \begin{cases} \frac{p(l)_n + \mathcal{O}p}{1 + \mathcal{O}p} & \text{se repetir a partição} \\ \frac{p(l)_n}{1 + \mathcal{O}p} & \text{caso não repita a partição} \end{cases}, \quad (4.3)$$

onde $p(l)_n$ é a probabilidade no tempo n e $\mathcal{O}p$ é uma parâmetro que deve ser ajustado. Quando o valor de $\mathcal{O}p$ é grande, $\mathcal{O}p \geq 0,5 \times 10^{-2}$, o tempo para a distribuição de probabilidade convergir para a distribuição natural do sistema, que chamamos de tempo de relaxação, é pequeno, todavia a possibilidade de erro na medida se torna maior. Quando o valor de $\mathcal{O}p$ é pequeno, $\mathcal{O}p \leq \times 10^{-3}$, então o tempo de relaxação aumenta, mas em contrapartida a possibilidade de erro na transmissão da mensagem se torna menor [16].

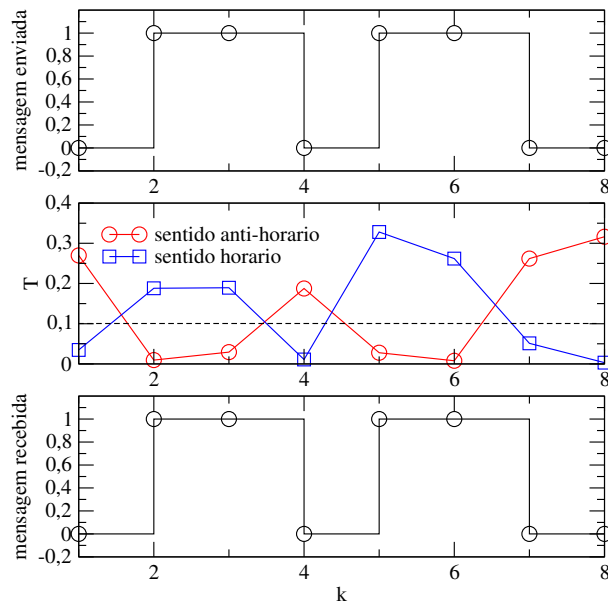
A partir da equação (4.3) podemos redefinir a entropia de transferência de forma a medi-la

em cada instante de tempo, a chamada entropia de transferência temporal

$$T_{n,X \rightarrow Y} = \bullet p(x_{n+1}, x_n, y_n)_n \log \frac{p(x_{n+1}|x_n, y_n)_n}{p(x_{n+1}|x_n)_n}, \quad (4.4)$$

deste modo é possível iniciar uma transmissão de dados entre um remetente e um destinatário. Para testar a eficiência do modelo iremos transmitir uma mensagem de oito *bits* ($K = 8$) utilizando como dinâmica local da rede a equação (2.22), o mapa logístico com parâmetro $a = 4$. A entropia de transferência será medida em cada instante de tempo, todavia, um *bit* de informação será medido a cada 200 iteradas do mapa, para evitar que a mensagem seja lida incorretamente. Esta quantidade de iteradas é suficiente para garantir que não ocorra erros se o valor de $\mathcal{O}p = 0.02$. Para verificar que é possível transmitir informação vamos considerar que o sistema não é criptografado ou seja $y^{(i)} = x^{(i)}$. O resultado é apresentado na figura 4.6.

Figura 4.6: Exemplo de transmissão de dados a partir do modelo de Hung e Hu. A curva em vermelho representa a entropia de transferência medida no sentido anti-horário. A curva em azul representa a entropia de transferência medida no sentido horário. Os valores acima da linha tracejada representam 1, abaixo representam 0.



Conforme podemos observar na figura 4.6, a mensagem recebida é a mesma mensagem enviada. A flutuação nos valores da entropia de transferência faz necessário o uso de um limiar de corte para a recuperação da mensagem.

4.3 Transmissão de Informação entre Redes Sincronizadas através da Entropia de Transferência

O nosso modelo para a transmissão de informação consiste de dois estágios, pré e pós-sincronização:

Estágio pré-sincronização: Tanto a fonte emissora quanto o receptor consistem de uma rede de mapas acoplados. Denominamos a rede emissora E e a rede receptora R , ambas possuem o mesmo número de sítios. Os sítios de cada uma das redes estão acoplados localmente entre si. A rede E é acoplada a rede R através de um acoplamento do tipo mestre-escravo, ou seja, a rede E influencia a rede R enquanto a rede R não influencia E . Após realizado este acoplamento é esperado um tempo, chamado de tempo de sincronização que é o tempo necessário para que as duas redes tornem-se idênticas quando iniciam de condições iniciais distintas. As duas redes serão consideradas idênticas quando a diferença entre elas for menor que 10^{-14} .

Estágio pós-sincronização: Após as redes se tornarem idênticas é desligado o acoplamento entre elas. A rede E é então acoplada com uma nova variável S que conterá o sinal criptografado. Quando um sítio da rede E está acoplado com a variável S significa que este sítio transmite a mensagem binária 1, quando desacoplado o respectivo sítio transmite a mensagem binária 0. O receptor que recebe apenas o sinal vindo da variável S decifra a mensagem, pois, a rede R é idêntica a rede E , dessa forma o emissor mede a entropia de transferência de cada sítio com a variável S , obtendo quais sítios estão ligados à S e quais não estão.

4.3.1 Estágio Pré-Sincronização

A dinâmica local de cada sítio para ambas as redes é idêntica e descrita por um mapa caótico, o mapa deve ser contínuo. Apresentaremos os resultados para o mapa da tenda clássico, que consiste da equação (2.21) com parâmetros $b = 0$ e $a = 0,5$. Tanto os sítios da rede emissora (E) como a rede receptora (R) estão acoplados com seus primeiros vizinhos e com condições de contorno periódicas. O acoplamento de cada uma das redes será caracterizado por

$$F(z^{(i)}) = (1 - \varepsilon)f(z_n^{(i)}) + \frac{\varepsilon}{2} \left[f(z_n^{(i-1)}) + f(z_n^{(i+1)}) \right], \quad (4.5)$$

onde $\varepsilon \in [0; 1]$ e $f(x)$ é a dinâmica local de cada sítio. Todavia a rede R está acoplada com a rede E através de um acoplamento do tipo mestre-escravo, a dinâmica do sistema como um todo

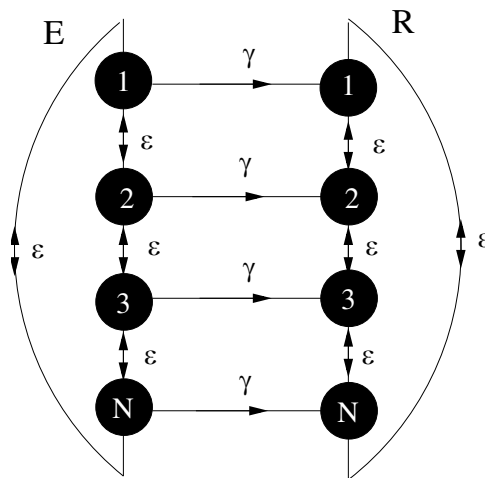
será

$$e_{n+1}^{(i)} = F(e_n^{(i)}) \quad (4.6)$$

$$r_{n+1}^{(i)} = (1 - \gamma)F(r_n^{(i)}) + \gamma F(e_n^{(i)}), \quad (4.7)$$

onde $\gamma \in [0; 1]$ é a intensidade de acoplamento entre as redes e $e^{(i)}, r^{(i)}$ representam a regra de evolução dos sítios da rede E e da rede R respectivamente. Quando o parâmetro γ é grande o suficiente, ele fará com que os valores dos sítios da rede R ($r^{(i)}$) evoluam assintoticamente para o mesmo valor do seu sítio respectivo na rede E, ou seja, $e^{(1)} = r^{(1)}, \dots, e^{(N)} = r^{(N)}$. Enquanto o valor do parâmetro de acoplamento ε deve ser pequeno para evitar que todo o sistema sincronize como um todo. Desta forma é necessário que γ seja suficientemente grande para que $r^{(i)}$ se torne igual ao seu respectivo sítio $e^{(i)}$ e ε deve ser pequeno para evitar que os sítios da rede E ou da rede R sincronizem entre si. Um esboço da rede descrita pelas equações (4.6) e (4.7) pode ser observado através da figura 4.7.

Figura 4.7: Acoplamento entre sítios de cada uma das redes determinado por ε e o acoplamento entre as redes determinado pelo parâmetro γ . O acoplamento entre sítios é do tipo primeiros vizinhos e entre as redes é do tipo mestre-escravo.



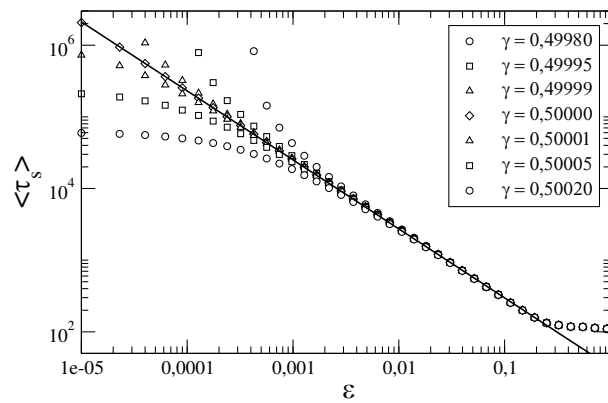
Para que as redes se tornem idênticas é necessário esperar que elas sincronizem. Determinamos então o tempo de sincronização nas vizinhanças do parâmetro $\gamma = 1/2$. Utilizamos o mapa da tenda e acoplamentos fracos de ε . Consideramos como tempo de sincronização, o tempo, neste caso o número de iterações, para que a diferença entre as variáveis de estado $e^{(i)}$ e $r^{(i)}$ se torne menor que 10^{-14} . Quando as redes sincronizam nesta precisão os termos de precisão superior são desprezados. O truncamento da série nos garante que a rede E e a rede R se tornem realmente idênticas.

A figura 4.8 nos mostra que quanto maior a intensidade de ε menor é o tempo de sincronização. Este fato acontece porque a medida que o acoplamento ε aumenta existe uma redução no

tamanho do espaço de fase [39], o que facilita para uma sincronização mais rápida. Este fenômeno é similar ao que ocorre no caso de dois mapas da tenda acoplados com a mesma intensidade de acoplamento.

Quando o parâmetro de acoplamento γ é igual a $1/2$ o tempo de sincronização decai como um lei de potência da forma $\langle \tau_s \rangle \propto \varepsilon^{-\alpha}$, onde $\alpha \approx 1$, esta quantidade independe do tamanho da rede e conseqüentemente independe da quantidade de *bits* que serão enviados. Este resultado é importante, pois, mantendo o acoplamento entre as redes fixos em $\gamma = 1/2$ o tempo necessário para as variáveis sincronizarem pode ser estimado analiticamente.

Figura 4.8: Tempo médio de sincronização ($\langle \tau_s \rangle$) em termos do acoplamento ε . A escala para ε é logarítmica. O gráfico foi determinado para uma rede de tamanho $N = 21$.



4.3.2 Estágio pós-sincronização

Após as redes estarem sincronizadas é desligado o acoplamento entre elas, ou seja, $\gamma = 0$. É iniciado o processo de transmissão da mensagem, a mensagem binária é determinada em relação ao acoplamento dos sítios da rede emissora com uma nova variável S . Quando um sítio está acoplado com a variável S ele cifra a mensagem 1 e quando o sítio está desacoplado ele cifra a mensagem 0. Desta forma uma rede de tamanho N conterá uma mensagem de N *bits*. A dinâmica da variável S será

$$s_{n+1} = \frac{N-1}{N}s_n + \frac{1}{N\eta} \sum_{i=1}^N F(e_n^{(i)})m_i, \quad (4.8)$$

onde $m_i = \begin{cases} 1 & \text{modo on} \\ 0 & \text{modo off} \end{cases}$, o modo *on* indica que o sítio i está acoplado e o modo *off* indica que o sítio i está desacoplado. O termo η é a quantidade de sítios conectados com S . O sinal é transmitido para o receptor que, então utiliza a entropia de transferência para determinar se cada sítio de sua rede está ou não acoplado com S , ao efetuar esta medida o destinatário recebe

a mensagem enviada pelo remetente. A medida feita pelo destinatário é

$$T_{r^{(i)} \rightarrow S} = \bullet p(s_{n+1}, s_n, r_n^{(i)}) \log \frac{p(s_{n+1} | s_n, r_n^{(i)})}{p(s_{n+1} | s_n)}, \quad (4.9)$$

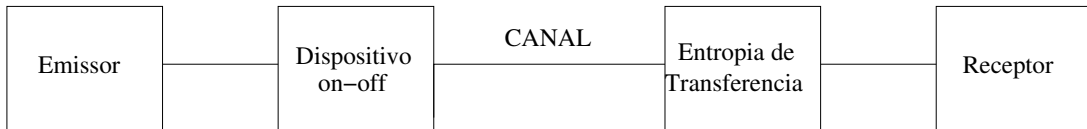
Cada *bit* da mensagem pode ser decodificado a partir da medida

$$\tilde{m} = \Theta(T_{r^{(i)} \rightarrow S} - \sigma(T)), \quad (4.10)$$

onde $\Theta(x)$ é a função de Heavside e $\sigma(T)$ é o filtro da mensagem. Neste caso utilizamos como filtro o desvio padrão com relação a todas as medidas de entropia de transferência realizada pelo destinatário.

Um esquema geral do mecanismo de comunicação pode ser observado a partir da figura 4.9. A codificação da mensagem é determinada pelo sítio da rede (E) estar com o acoplamento ligado ou desligado com a variável S , cujo sinal é transmitido pelo canal ao destinatário que através da entropia de transferência recupera a mensagem binária.

Figura 4.9: Mecanismo de transmissão de informação através de redes idênticas.

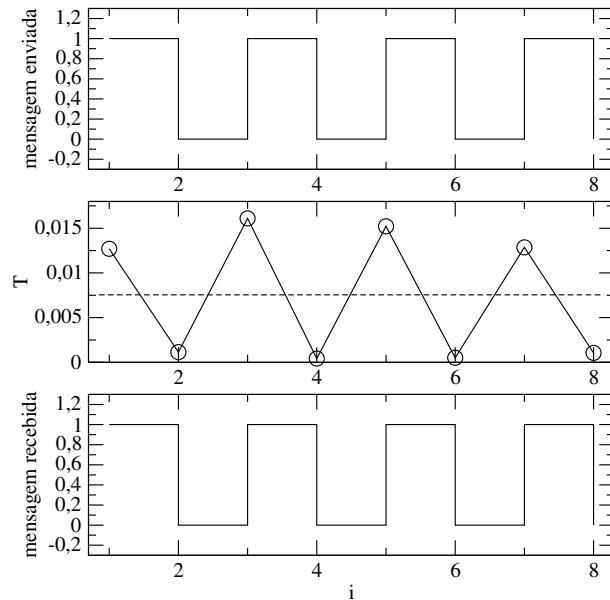


Para verificar a eficiência do sistema simulamos o envio de uma mensagem contendo 8 *bits*, o que implica em uma rede de tamanho 8. Utilizamos como parâmetros $\gamma = 0,5$ e $\varepsilon = 0,1$. O resultado pode ser observado a partir da figura 4.10.

Na figura 4.10 o filtro utilizado foi o desvio padrão. Se a entropia de transferência com relação a medida de todos os sítios for maior que o desvio padrão, indica que a medida representa o símbolo 1, caso contrário o valor da medida implica em um símbolo 0. A necessidade do filtro é consequência do tempo efetuado para a medida que é reduzido o máximo possível. A redução na diferença de entropia dos casos que representam 0 e dos casos que representam 1 também são consequência da correlação que existe entre os sítios da rede. É importante observar que neste exemplo oito *bits* foram enviados em um mesmo tempo de relaxação, contrariamente ao modelo de Hung e Hu, onde foi necessário oito observações para transmitir uma mensagem de mesmo tamanho. Quando o tempo de relaxação do nosso modelo utilizando redes idênticas for igual ao tempo de relaxação do modelo de Hung e Hu, então o nosso modelo será N vezes mais eficiente.

O mecanismo proposto permite que um bloco de símbolos binários seja transmitido em um

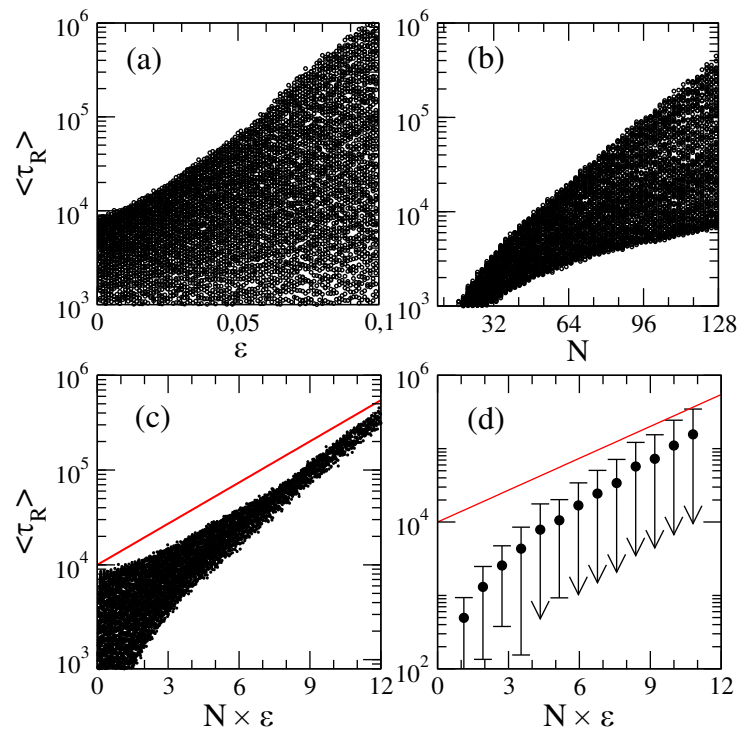
Figura 4.10: Exemplo de transmissão de 8 bits. Para estimar a probabilidade foi utilizado duas partições, esquerda (0;0,5) e direita(0,5;1), e uma série de tamanho 20000. A linha pontilhada representa o filtro.



mesmo instante de tempo, é possível continuar transmitindo a mensagem utilizando a entropia de transferência temporal da mesma forma que foi utilizada para o modelo de Hung e Hu. O tempo mínimo que se deve esperar para estimar a probabilidade e que define um instante de tempo, é denominado de tempo de relaxação, ou seja, é o tempo para a distribuição de probabilidade convergir para a medida natural do sistema. Determinamos o tempo de relaxação para diferentes valores de ε e para diferentes tamanhos de rede, conforme mostram as figuras 4.11 (a),(b),(c).

O conhecimento do tempo de relaxação é fundamental para a transmissão da mensagem, pois, a mensagem será transmitida apenas quando a medida for realizada sobre uma medida cujo o intervalo de tempo para a estimação da probabilidade for maior ou igual ao tempo de relaxação. Na figura 4.11 (d) apresentamos a dispersão para demonstrar que o limiar encontrado, $10^3 e^{N\varepsilon/3}$, garante que a medida seja feita sem erros.

Figura 4.11: Tempo de relaxação: (a) em termos do parâmetro de acoplamento ε ; (b) em termos do tamanho da rede N ; (c) Em termos do produto $(N\varepsilon)$. Na figura (d) temos a dispersão do tempo de relaxação com relação ao tempo médio de relaxação para 100 séries de mensagens aleatórias. A linha vermelha indica o limiar, qualquer tempo escolhido acima desta linha determinada por $10^3 e^{N\varepsilon/3}$, resulta em uma medida eficiente da mensagem.



Conclusão

É possível estudar a interação entre sistemas dinâmicos a partir de quantidades como a densidade de probabilidade. A conexão entre teoria da informação e sistemas dinâmicos pode ser observada a partir da relação entre informação mútua e o expoente de Lyapunov. No caso de duas variáveis a quantidade de informação que duas variáveis compartilham entre si na região de sincronização é idêntica a taxa de divergência das trajetórias.

O estudo da entropia de transferência é uma ferramenta que permite explorar efeitos devido a interação entre sistemas dinâmicos. A direção de acoplamento em uma rede de mapas acoplados é um efeito que pode ser determinado a partir da entropia de transferência. A partir da direção de acoplamento é possível construir sistemas de comunicação altamente seguros.

A ideia apresentada por Hung e Hu para transmitir informação utilizando a direção de acoplamento que permite enviar apenas um *bit* de informação a cada intervalo de tempo, pode ser expandida para um mecanismo de transmissão de dados em blocos através de duas redes de mapas acoplados idênticas.

O modelo que propomos para comunicação segura tem como principal vantagem sua segurança, pois, mesmo que um intruso tenha acesso ao sinal que esta sendo transmitido não possuindo uma rede sincronizada ao emissor jamais recuperará a mensagem. Embora a entropia de transferência não seja uma medida precisa, a inserção de um filtro, no nosso caso o desvio padrão, a torna uma medida eficiente.

As análises feitas ao longo da dissertação foram voltadas para aplicação da entropia de transferência em sistemas de comunicação, todavia, é uma ferramenta com aplicação em diversas áreas da física. É possível utilizar a entropia de transferência para identificar vínculos em redes de osciladores, determinar interferência em redes elétricas, ...

O mecanismo de comunicação proposto representa uma nova abordagem para estudo de sistemas de comunicação. Mas, ainda é necessário um estudo mais profundo sobre a eficiência do mecanismo a ruídos e sua capacidade de transmissão de dados para que ele possa ser utilizado em mecanismos reais de comunicação. Desta forma a ideia apresentada aqui é um caminho possível para a construção de dispositivos digitais seguros de transmissão de dados.

Referências Bibliográficas

- 1 HASSELBLATT, B.; KATOK, A. *A First Course in Dynamics*. Cambridge: Cambridge University Press, 2003. 435 p.
- 2 OTT, E. *Chaos in Dynamical Systems*. Cambridge: Cambridge University Press, 1993. 395 p.
- 3 SCHEINERMAN, E. R. *Invitation to Dynamical Systems*. New York: Prentice-Hall, Inc., 1995. 289 p.
- 4 WOLFRAM, S. Statistical mechanics of cellular automata. *Reviews of Modern Physics*, New York, v. 55, n. 3, p. 601–644, Julho 1983.
- 5 ALIGOOD, K. T.; SAUER, T. D.; YORKE, J. A. *Chaos: An Introduction to Dynamical Systems*. New York: Springer, 1996. 612 p.
- 6 STEWART, I. *Será que Deus Joga Dados?* São Paulo: Jorge Zahar Editor, 1991. 336 p.
- 7 BECK, C.; SCHLÖGL, F. *Thermodynamics of chaotic systems: An Introduction*. New York: Cambridge University Press, 1993. 306 p.
- 8 SHANNON, C. E.; WEAVER, W. *The Mathematical Theory of Communication*. 10. ed. Illinois: The University of Illinois Press, 1964. 132 p.
- 9 COVER, T. M.; THOMAS, J. A. *Elements of Information Theory*. 2. ed. New Jersey: Jhon Wiley & Sons, Inc., 2006. 774 p.
- 10 SCHREIBER, T. Measuring information transfer. *Physical Review Letters*, New York, v. 85, n. 2, p. 461–464, julho 2000.
- 11 GULICK, D. *Encounters with Chaos*. New York: McGraw-Hill, Inc., 1992. 308 p.
- 12 HASLER, M.; MAISTRENKO, Y. L. An introduction to the synchronization of chaotic systems: Coupled skew tent maps. *IEEE Transactions on Circuits and Systems - I : Fundamental Theory and Applications*, Piscataway, v. 44, n. 10, p. 856–866, Outubro 1997.
- 13 BILLINGS, L.; BOLLT, E. M. Probability density functions of some skew tent maps. *Chaos, Solitons and Fractals*, Atlanta, v. 12, p. 365–376, Dezembro 2001.
- 14 KANEKO, K. Overview of coupled map lattices. *Chaos*, Melville, v. 2, n. 3, p. 4, Julho 1992.
- 15 BAPTISTA, M. S.; KURTHS, J. Transmission of information in active networks. *Physical Review E*, New York, v. 77, p. 026205(13), Fevereiro 2008.

- 16 HUNG, Y.-C.; HU, C.-K. Chaotic communication via temporal transfer entropy. *Physical Review Letters*, New York, v. 101, p. 244102(4), Dezembro 2008.
- 17 YU, F. T. S. *Entropy and Information Optics*. New York: Marcel Dekker, Inc, 2000. 348 p.
- 18 HARTLEY, R. V. L. Transmission of information. *Bell System Technical Journal*, San Francisco, v. 7, n. 3, p. 535–363, Julho 1928.
- 19 REIF, F. *Fundamentals of statistical and thermal physics*. New York: McGraw-Hill, Inc., 1965. 666 p.
- 20 JAYNES, E. T. *Probability Theory: The Logic of Science*. Cambridge: Cambridge University Press, 2003. 757 p.
- 21 KULLBACK, S. *Information Theory and Statistics*. 2. ed. Washington: Dover Publications, Inc., 1968. 409 p.
- 22 NARSINGH, D. *Graph Theory with Applications to Engineering and Computer Science*. New Delhi: Prentice-Hall, Inc., 1974. 478 p.
- 23 MANIERI, R.; CVITANOVIĆ, P.; SPIEGEL, E. A. *Chaos: Classical and Quantum*. 13. ed. Copenhagen: Niels Bohr Institute, 2009. 950 p. Chapter: Go with the flow.
- 24 SZMOSKI, R. M. *Análise da Dinâmica de Partículas Brownianas Interagentes a partir de Redes de Mapas Acoplados*. Dissertação (Mestrado) — Universidade Estadual de Ponta Grossa, Ponta Grossa, março 2009.
- 25 SCOTT, A. (Ed.). *Encyclopedia of Nonlinear Science*. New York: Routledge Taylor & Francis Group, 2005. 1108 p.
- 26 BARABÁSI, A.-L.; ALBERT, R.; JEONG, H. Mean-field theory for scale-free random networks. *Physica A*, New York, v. 272, p. 173–187, Julho 1999.
- 27 WATTS, D. J.; STROGATZ, S. H. Collective dynamics of 'small-world' networks. *Nature*, San Francisco, v. 393, p. 440–442, junho 1998.
- 28 BATISTA, C. A. S.; BATISTA, A. M.; PINTO, S. E. de S.; VIANA, R. L.; LOPES, S. R.; CALDAS, I. Direction coherence in scale-free lattices of chaotic maps. *Physica A*, New York, v. 383, p. 725–732, Abril 2007.
- 29 BATISTA, A. M.; PINTO, S. E. de S.; VIANA, R. L.; LOPES, S. R. Mode locking in small-world networks of coupled circle maps. *Physica A*, New York, v. 322, p. 118–128, Setembro 2003.
- 30 CRUTCHFIELD, J. P.; KANEKO, K. *Phenomenology of Spatio-Temporal Chaos*. Singapore: World Scientific, 1987. 368 p.
- 31 PIKOVSKY, A.; ROSEMBLUM, M.; KURTHS, J. *Synchronization: A Universal Concept in Nonlinear Sciences*. Cambridge: Cambridge University Press, 2001. 433 p.
- 32 PECORA, L. M.; CAROLL, T. L. Synchronization in chaotic systems. *Physical Review Letters*, New York, v. 64, n. 8, p. 821–825, Fevereiro 1990.

- 33 BOLLT, E. M. Synchronization as a process of sharing and transferring information. Submetido a International Journal of Bifurcations and Chaos, Potsdam, 8p. 2012.
- 34 BAUER, M.; THORNHILL, N. F.; MEABURN, A. Specifying the directionality of fault propagation paths using transfer entropy. Cambridge, p. 1–6, Julho 2004. Preprint de artigo apresentado em DYCOPS 7.
- 35 MARSCHINSKI, R.; KANTZ, H. Analysing the information flow between financial time series. *The European Physical Journal*, Frascati, v. 30, p. 275–281, Novembro 2002.
- 36 CUOMO, K. M.; OPPENHEIM, A. V. Circuit implementation of synchronized chaos with applications to communications. *Physical Review Letters*, New York, v. 71, n. 1, p. 65–68, Julho 1993.
- 37 KINZEL, W.; ENGLERT, A.; KANTER, I. On chaos synchronization and secure communication. *Philosophical Transactions of The Royal Society A*, London, v. 368, p. 379–389, Outubro 2010.
- 38 SHANNON, C. E. Communication theory of secrecy systems. *Bell System Technical Journal*, Paris, v. 28, p. 656–715, Outubro 1949.
- 39 SZMOSKI, R. M.; PEREIRA, R. F.; FERRARI, F. A. S.; PINTO, S. E. de S. Locking-time and information capacity in cml with statistical periodicity. *Journal Physics: Conference Series*, Bristol, v. 285, p. 012043(9), Janeiro 2011.