UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Ciências e Tecnologia
Câmpus de Presidente Prudente

# Uma Análise Sobre o Mapa de Hénon e Sua Aplicação em Criptografia

Muriel Henrique Bueno

Orientadora: Profa. Dra. Tatiana Miguel Rodrigues

Programa de Pós-Graduação em Matemática Aplicada e Computacional

Bauru, setembro de 2024

**UNIVERSIDADE ESTADUAL PAULISTA**

Faculdade de Ciências e Tecnologia de Presidente Prudente

Programa de Pós-Graduação em Matemática Aplicada e Computacional

# Uma Análise Sobre o Mapa de Hénon e Sua Aplicação em Criptografia

Muriel Henrique Bueno

Orientadora: Profa. Dra. Tatiana Miguel Rodrigues

Dissertação apresentada ao Programa de Pós-Graduação em Matemática Aplicada e Computacional da Faculdade de Ciências e Tecnologia da UNESP para obtenção do título de Mestre em Matemática Aplicada e Computacional.

Bauru, setembro de 2024

B928a

Bueno, Muriel Henrique
Uma Análise Sobre o Mapa de Hénon e Sua Aplicação em Criptografia / Muriel Henrique Bueno. -- Presidente Prudente, 2024
93 p.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Faculdade de Ciências e Tecnologia, Presidente Prudente
Orientadora: Tatiana Miguel Rodrigues

1. Sistemas Dinâmicos. 2. Caos. 3. Mapa de Hénon. 4. Criptografia. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

**UNIVERSIDADE ESTADUAL PAULISTA**

**Câmpus de Presidente Prudente**

## CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: **Uma Análise Sobre o Mapa de Hénon e Sua Aplicação em Criptografia**

**AUTOR: MURIEL HENRIQUE BUENO**
**ORIENTADORA: TATIANA MIGUEL RODRIGUES**

Aprovado como parte das exigências para obtenção do Título de Mestre em Matemática Aplicada e Computacional, pela Comissão Examinadora:

gov.br Documento assinado digitalmente
TATIANA MIGUEL RODRIGUES
Data: 10/09/2024 07:29:57-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. TATIANA MIGUEL RODRIGUES (Participaçao Presencial)
Departamento de Matematica / UNESP/Campus de Bauru

gov.br Documento assinado digitalmente
FERNANDO PEREIRA MICENA
Data: 10/09/2024 10:09:05-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. FERNANDO PEREIRA MICENA (Participaçao Virtual)
Departamento de Matemática e Computação / Universidade Federal de Itajubá

gov.br Documento assinado digitalmente
LUIS ANTONIO DA SILVA VASCONCELLOS
Data: 10/09/2024 09:36:22-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. LUIS ANTONIO DA SILVA VASCONCELLOS (Participaçao Presencial)
Departamento de Matemática / Faculdade de Ciencias de Bauru - FC/Unesp

Presidente Prudente, 04 de setembro de 2024

*Dedico este trabalho a todos que estiveram comigo ao longo desta jornada.*

# Agradecimentos

Agradeço à minha esposa, Maryana Machado Albano Bueno, por estar ao meu lado, me apoiar e me ajudar a superar todas as adversidades que tive que enfrentar durante esse processo. Obrigado por tudo, eu amo você.

Agradeço aos meus pais, Marcos Antônio Farias Bueno e Silvana Cardoso dos Santos Bueno, por proporcionarem, com todo carinho e amor, o ambiente necessário para que eu pudesse chegar até aqui. Obrigado por todo incentivo, apoio e esforço.

Agradeço aos meus irmãos, Marcos Antônio Farias Bueno Filho e Marana Lorran Bueno, por me apoiarem e me incentivarem a permanecer no caminho acadêmico.

Sou imensamente grato à minha orientadora, Tatiana Miguel Rodrigues, que, com toda a sua resiliência, entendeu as dificuldades que tive que enfrentar até aqui, me ajudou a superá-las e me proporcionou a oportunidade de produzir este trabalho. Obrigado.

Agradeço aos integrantes da banca examinadora pelas sugestões e correções.

Agradeço à UNESP e a todo o corpo docente do Departamento de Matemática e de Física do campus de Bauru por me proporcionarem uma formação acadêmica sólida.

*O tempo somente é porque algo acontece, e onde algo acontece o tempo está.*
***Milton Santos***

# Resumo

Neste estudo, investigamos minuciosamente as propriedades do mapa de Hénon, começando com uma exploração dos conceitos fundamentais de sistemas dinâmicos, com foco particular em sistemas dinâmicos discretos. Durante essa análise preliminar, identificamos as principais características que esses sistemas podem exibir. Em seguida, descrevemos a construção do modelo do mapa de Hénon conforme apresentado no artigo original de Hénon. Posteriormente, examinamos alguns resultados comuns encontrados na literatura, juntamente com suas demonstrações analíticas correspondentes, para compreender a dinâmica do mapa. Esses resultados forneceram o embasamento necessário para o estudo do atrator estranho de Hénon. Por fim, reproduzimos um algoritmo de encriptação com algumas adaptações realizadas pelo autor que foi analisada do ponto de vista do tempo computacional de execução.

Palavras-Chave: *Mapa de Hénon, Sistema Dinâmico, Caos, Criptografia.*

# Abstract

In this study, we thoroughly investigate the properties of the Hénon map, beginning with an exploration of the fundamental concepts of dynamical systems, with a particular focus on discrete dynamical systems. During this preliminary analysis, we identify the main characteristics that these systems can exhibit. We then describe the construction of the Hénon map model as presented in Hénon's original paper. Subsequently, we examine some common results found in the literature, along with their corresponding analytical demonstrations, to understand the dynamics of the map. These results provided the necessary foundation for studying the Hénon strange attractor. Finally, we reproduce an encryption algorithm with some adaptations made by the author, which was analyzed from the perspective of computational execution time.

Keywords: *Hénon map, Dynamical System, Strange Attractor, Chaos.*

# Lista de Figuras

# Sumário

Capítulo

# 1

# Introdução

Existem várias definições para o caos. Neste trabalho, iremos considerar um sistema caótico como aquele que demonstra sensibilidade às condições iniciais [2], além disso, o sistema analisado que seja de fato caótico deve satisfazer as propriedades da definição de caos segundo Devaney, 2018 [16]. Os sistemas caóticos têm sido amplamente estudados [2], e é significativo ressaltar a importância deste comportamento em sistemas físicos. No estudo da dinâmica desses sistemas, é comum explorar o pêndulo simples, no qual a amplitude de oscilação é suficientemente pequena; logo, $\sin\theta \approx \theta$. Neste caso, teremos uma equação diferencial linear simples de ser resolvida. No entanto, se o sistema não obedece à condição de $\theta$ suficientemente pequeno, a equação que o descreve deixa de ser linear. Além disso, nesse mesmo sistema, podemos presenciar um comportamento caótico ao considerarmos um pêndulo duplo. O comportamento caótico pode emergir em outros sistemas físicos. Portanto, é necessária uma abordagem eficaz para descrever esse tipo de sistema. Nesse sentido, o uso de mapas de fluxo podem fornecer informações importantes sobre a evolução do sistema e, ao mesmo tempo, detectar possíveis comportamentos caóticos.

Em sistemas dinâmicos, um atrator (definição mais a frente) é um subconjunto fechado $A$ no espaço de fase no qual, para muitas condições iniciais, a evolução do sistema converge para o subconjunto $A$ [2]. O mapa de iteração de Hénon bidimenssional é invertível, e ainda, apresenta soluções caóticas importantes chamadas de atratores estranhos. Em síntese os atratores estranhos são regiões do espaço de fase onde as soluções não descrevem trajetórias previsíveis ou periódicas, mas em contrapartida as trajetórias se encontram em regiões limitadas. Se utilizarmos $n$ para representar a sequência de tempo de um sistema e $x$ para denotar um observável físico do sistema, podemos descrever seu progresso não linear como a $(n+1)$-ésima iteração (ou estado) dependente da enésima iteração, isto é, obtemos a relação $x_{n+1} = f(x)$, frequentemente utilizada para descrever o comportamento de sistemas [51].

O mapa de Hénon foi proposto pelo astrônomo e matemático Michel Hénon como simplificação do modelo de Poincaré que surge de um solução das equações de Lorenz. O modelo de Hénon consiste no seguinte mapa quadrático:

$$\begin{aligned} x_{n+1} &= 1 - ax_n^2 + y_n \\ y_{n+1} &= bx_n, \end{aligned}$$

onde $a$ e $b$ são parâmetros de bifurcação positivo. Substituindo a segunda equação na primeira obtemos

$$x_{n+1} = 1 - ax_n^2 + bx_{n-1}. \tag{1.1}$$

O mapa de Hénon representa uma solução elegante das seções de Poincaré para o sistema de Lorenz [2]. Portanto, o modelo a ser apresentado preserva as propriedades importantes do sistema de Lorenz. Assim como no sistema de Lorenz, o mapa de Hénon também exibirá dependência sensível das condições iniciais e um atrator estranho.

O atrator estranho desempenha um papel central na compreensão do mapa de Hénon como um sistema caótico. Este tipo de atrator é obtido para valores específicos dos parâmetros $a$ e $b$. Em termos simples, o atrator estranho é uma região no espaço de fase na qual as soluções não seguem um padrão definido, mas permanecem confinadas nessa região. Além disso, nessa região, o sistema exibirá um comportamento caótico, caracterizado principalmente pela sensibilidade às condições iniciais.

Vale ressaltar, que o atrator estranho exibido para $a = 1,4$ e $b = 0,4$, conhecido como atrator de Hénon, possui uma estrutura fractal. Portanto, é interessante estudar a dimensão fractal desse atrator. Podemos concluir que o atrator de Hénon possui uma estrutura fractal ao ampliarmos partes dele. O processo de ampliação demonstra uma característica central dos fractais: a auto-semelhança. Isso significa, que ao ampliarmos um objeto com estrutura fractal, encontraremos a mesma geometria que a anterior. Ao ampliar o objeto sucessivamente, veremos a repetição infinita da geometria do objeto. No atrator de Hénon, observamos uma estrutura fractal marcante, muito semelhante ao conjunto de Cantor, sugerindo a possibilidade da existência de uma dimensão de auto-semelhança ou dimensão fractal. O estudo nesse ponto pode avançar muito, haja visto, que os fractais são objetos que ainda não possuem uma definição concreta e podem ser observados em atratores estranhos, por exemplo [29]. Essa não é a única relação do caos com os fractais, também podemos observar uma estrutura de auto-semelhança na dinâmica de bifurcações que pode ser atestada pelos diagramas de bifurcação explorados por Feigenbaum [20, 21].

Não houve, nesse trabalho, uma demonstração analítica da caoticidade do mapa de Hénon, entretanto, os experimentos computacionais nos levam a afirmar isso, observando a dinâmica de bifurcações e a dependência sensível das condições iniciais. Haja vista a utilização do mapa de Hénon em aplicações digitais, como telecomunicações, [8] e também observando a dependência sensível das condições iniciais, é viável a hipótese da possibilidade da aplicação do mapa de Hénon em sistemas criptográficos. Nesse contexto, a literatura é abundante quando se trata da aplicação do mapa de Hénon em criptografia de imagens. Os algoritmos de criptografia de imagens envolvendo o mapa de Hénon podem ser criados com uma vasta combinação de algoritmos e técnicas de processamento de imagem como usar algoritmos de separação em cores binárias e permutar usando o mapa de Hénon como proposto por Gao, 2021 [23]. Um algoritmo promissor é a combinação de planos de bits com filtros de borda de uma imagem permutada pelo mapa da Hénon, proposto por Rathore, 2021 [43]. Esse algoritmo será reproduzido nesse trabalho com pequenas alterações. A técnica proposta por Rathore pode ser feita combinando uma variedade de filtros de borda, nesse sentido é possível determinar qual filtro de borda pode ser o mais eficiente do ponto de vista de tempo de execução. A permutação da imagem usando o mapa de Hénon emerge um problema que é a sobreposição de bits que pode comprometer o processo de decriptação. Assim será um desafio a ser superado nesse trabalho.

Vale ressaltar que todas as figuras expostas nesse trabalho, com exceção das figuras referenciadas, foram feitas pelo próprio autor.

Capítulo

# 2

# Sistemas Dinâmicos

Henri Poincaré é frequentemente reconhecido como um dos principais estudiosos na área de sistemas dinâmicos, em grande parte devido ao seu estudo do problema dos três corpos que exibe uma dinâmica caótica. Sem dúvidas, seu trabalho foi fundamental ao introduzir uma nova abordagem para descrever a mecânica celeste [28]. Mas é importante dizer que o termo já poderia ter sido usado na mecânica formulada por Newton.

Um sistema pode ser compreendido como um conjunto de elementos que estão ligados entre si. Dessa forma quando dizemos que um sistema é dinâmico estamos tratando de um sistema que exibe configurações diferentes ao longo do tempo. Ou seja, trata-se de uma lei matemática que nos permite compreender como um elemento do sistema muda ao longo do tempo. Este elemento pode ser representado por uma variável que evolui ao longo do tempo [24]. Em geral o sistema dinâmico é uma lei matemática que mostra como a sua propriedade muda à medida que analisamos uma condição inicial. Os sistemas dinâmicos podem ser contínuos ou discretos representados por equações diferenciais ou mapas iterativos respectivamente.

## 2.1 Sistemas dinâmicos contínuos

Um sistema dinâmico contínuo é caracterizado por uma evolução ininterrupta ao longo do tempo, geralmente representado por meio de equações diferenciais. Nessas equações, descrevem-se as taxas de mudança das grandezas em relação ao tempo. As variáveis que se pretendem descrever são representadas por funções contínuas, enquanto as equações diferenciais capturam as variações de estado do sistema conforme suas condições iniciais.

Seja $f(x,t)$ contínua, definida no aberto $U \subset \mathbb{R}^n \times \mathbb{R}$ e com valores em $\mathbb{R}^n$ seja o sistema de equações diferenciais

$$\frac{dx}{dt} = f(x,t), \tag{2.1}$$

com $x \in \mathbb{R}^n$ e $t \in \mathbb{R}$. As variáveis dependentes são as componentes do vetor $x \in \mathbb{R}$ e $t$ é a variável independente. Uma solução da equação diferencial (2.1) é uma aplicação $\phi(t) : I \subset \mathbb{R} \to \mathbb{R}^n$. que verifica

$$\frac{d\phi}{dt} = f(\phi(t),t),$$

se a função $f$ obedece a $f(x+y,t) = f(x,t) + f(y,t)$, para todo $x, y \in \mathbb{R}^n$ e $t \in \mathbb{R}$ e se $\phi_1(t)$ e $\phi_2(t)$ são ambas soluções de (2.1), com $\phi_1(t) \neq \phi_2(t)$ então $\psi = \phi_1(t) + \phi_2(t)$, também é solução de (2.1). Neste caso o sistema é linear, além disso, se as equações

diferenciais dependem explicitamente do tempo elas são chamadas de autônomas. Uma curva de fase da equação diferencial (2.1) é imagem da solução $\phi(t; t_0, x_0)$, no espaço de fase. O conjunto de soluções possíveis da equação diferencial é chamada de órbita.

Para o ponto $x_0 \in \mathbb{R}^n$ a órbita de $x_0$ é o conjunto $O(x_0) = \{x \in \mathbb{R} : x = \phi(t; t_0, x_0), t \in I\}$. Geralmente os sistemas que buscamos modelar não apresentam linearidade, tornando a análise desse tipo de sistema mais complicada. Nesse contexto, o teorema que segue poderá ser uma ferramenta importante para analisar a estabilidade de sistemas que apresentam a não linearidade:

**Teorema 2.1.** *Seja $E$ um subconjunto aberto de $\mathbb{R}^n$ contendo a origem, seja $f$ de classe $C^1$ e $\varphi_t$ o fluxo de $x'(t) = f(x(t))$. Suponha que $f(0) = 0$ e que a matriz $A = Df(0)$ não possua nenhum autovalor com a parte real nula. Então, existe um homeomorfismo $h$ de um conjunto aberto $U$ contendo $x_0$ em um conjunto aberto $V$, contendo a origem, tal que para cada $x_0 \in U$, exista uma intervalo aberto $I_0 \in \mathbb{R}$ contendo $0$ tal que todo $t \in I_0$ temos*

$$h \circ \varphi_t(x_0) = e^{A.t} h(x_0),$$

*isto é, as trajetórias próximas de $x'(t) = f(x(t))$ próximas de $x_0$ são levadas em $x' = A.X$ próximas à origem e o tempo é preservado [7].*

### 2.1.1 O oscilador harmônico clássico

Na Física temos uma gama de exemplos de sistemas dinâmicos contínuos, sendo um deles um clássico no estudo de equações diferenciais: o oscilador harmônico. Os movimentos oscilatórios são comuns na natureza e na grande maioria dos casos exibem não linearidades e até mesmo comportamento caótico como é o caso do pêndulo duplo [38]. Quando estudamos movimentos oscilatórios lineares, as equações que surgem possuem coeficientes constantes, o que resulta em soluções diretas. Sendo assim, observamos que qualquer sistema com um ponto de equilíbrio estável executa, ao redor dessa posição, um movimento harmônico simples.

Considere uma mola em que a sua massa possa ser desprezível. A mola é deformada a ponto que sua elasticidade não seja comprometida. Sendo assim a mola tende a voltar ao seu ponto de relaxamento, onde a lei que rege o sistema é a lei de Hooke $F = -kx$, onde $x$ é a deformação da mola do seu ponto relaxado e $k$ é a sua constante de elasticidade. A força aplicada para que a mola seja deformada é $F = ma$ logo obtemos:

$$-kx = ma$$

$$\frac{d^2x}{dt^2} - \frac{k}{m}x = 0, \tag{2.2}$$

por análise dimensional note que $\omega^2 = \frac{k}{m}$ então podemos reescrever a equação (2.2) como

$$\frac{d^2x}{dt^2} - \omega^2 x = 0, \tag{2.3}$$

onde $\omega$ é a frequência angular do sistema.

Podemos impor outra situação. Considere um sistema dissipativo, isto é, a energia total do sistema tende a 0 à medida que o tempo varia. Sendo assim, existe uma força $-b\frac{dx}{dt}$ de caráter resistivo atuando no sistema. Repare que se $b < 0$ a velocidade aumenta contrapondo a situação proposta, logo, $b$ é positivo, pois assim, a velocidade diminui caracterizando um amortecimento do sistema [51, 17]. Então

$$m\frac{d^2x}{dt^2} = -b\frac{dx}{dt} - kx$$

$$m\frac{d^2x}{dt^2} + b\frac{dx}{dt} + kx = 0,$$

podemos escrever ainda

$$\frac{d^2x}{dt^2} + 2\beta\frac{dx}{dt} + \omega_0^2 x = 0, \tag{2.4}$$

nessa equação $\beta = b/2m$ é o parâmetro de amortecimento e $\omega_0 = \sqrt{\frac{k}{m}}$ é a frequência angular característica na ausência de amortecimento. Muitas vezes para facilitar a notação podemos representar a derivada temporal como $\dot{x}$. Assim, segue que $x_1 = x$ e $x_2 = \dot{x}$ logo $\dot{x}_1 = \dot{x}$ e $\dot{x}_2 = \ddot{x}$. Então podemos reescrever a equação diferencial (2.4) como um sistema de equações diferenciais

$$\begin{cases} \dot{x}_1 = \dot{x} \\ \dot{x}_2 = -2\beta\dot{x} - \omega_0^2 x \end{cases},$$

sendo assim, estudaremos a seguinte matriz:

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ -\omega_0^2 & -2\beta \end{pmatrix}.$$

Logo os autovalores associados a matriz $\mathbf{A}$ são:

$$\lambda_1 = -\beta + \sqrt{\beta^2 - \omega_0^2}$$

e

$$\lambda_2 = -\beta - \sqrt{\beta^2 - \omega_0^2}.$$

Assim, segue que a solução da equação (2.4) é

$$x(t) = e^{-bt}(A_1 e^{(\sqrt{\beta^2-\omega_0^2}t)} + A_1 e^{(-\sqrt{\beta^2-\omega_0^2}t)}).$$

Com base nos parâmetros $\beta$ e $\omega_0$ podemos analisar as diferentes dinâmicas que o oscilador harmônico pode ter.

Contrariamente ao oscilador em um sistema conservativo, o oscilador em um sistema dissipativo não conserva sua energia total. Portanto, a amplitude do movimento diminui à medida que o tempo passa. Isso ocorre porque a energia é gradualmente dissipada. Vale ressaltar, que este não é um movimento tipicamente periódico, pois seu caráter amortecido impede que o objeto em movimento oscilatório passe duas vezes no mesmo ponto. Note que as soluções convergem para um único ponto, que representa o estado de relaxamento do oscilador.

Observe que a condição $\omega_0^2 > \beta^2$ evidencia que os autovalores serão sempre complexos. Ou seja, o campo linear com essa propriedade é um atrator, e a origem é um ponto de equilíbrio estável ou um poço, como mostrado na Figura 2.1 (ver [17]). Observe que essa ideia tem sentido físico, uma vez que o ponto de equilíbrio estável representa o estado de relaxamento do oscilador. Em outras palavras, todas as soluções devem convergir para a origem. Nesse caso, dizemos que o oscilador possui um movimento subamortecido.

Quando o parâmetro de amortecimento $\beta$ é numericamente igual à frequência angular, temos que $\beta^2 = \omega_0^2$, logo $\sqrt{\beta^2 - \omega_0^2} = 0$, o que implica em $x_1 = x_2 = -\beta$. Este é um caso em que as soluções convergem para a origem assintoticamente, tangenciando um eixo que passa pela origem, caracterizando novamente um campo linear atrator [17]. Nesse caso, dizemos que o movimento é de amortecimento crítico.

Um terceiro caso é o superamortecimento, quando o movimento se aproxima de zero sem exibir oscilações. Se $\beta \gg \omega_0$, então a amplitude tende a zero em um intervalo de

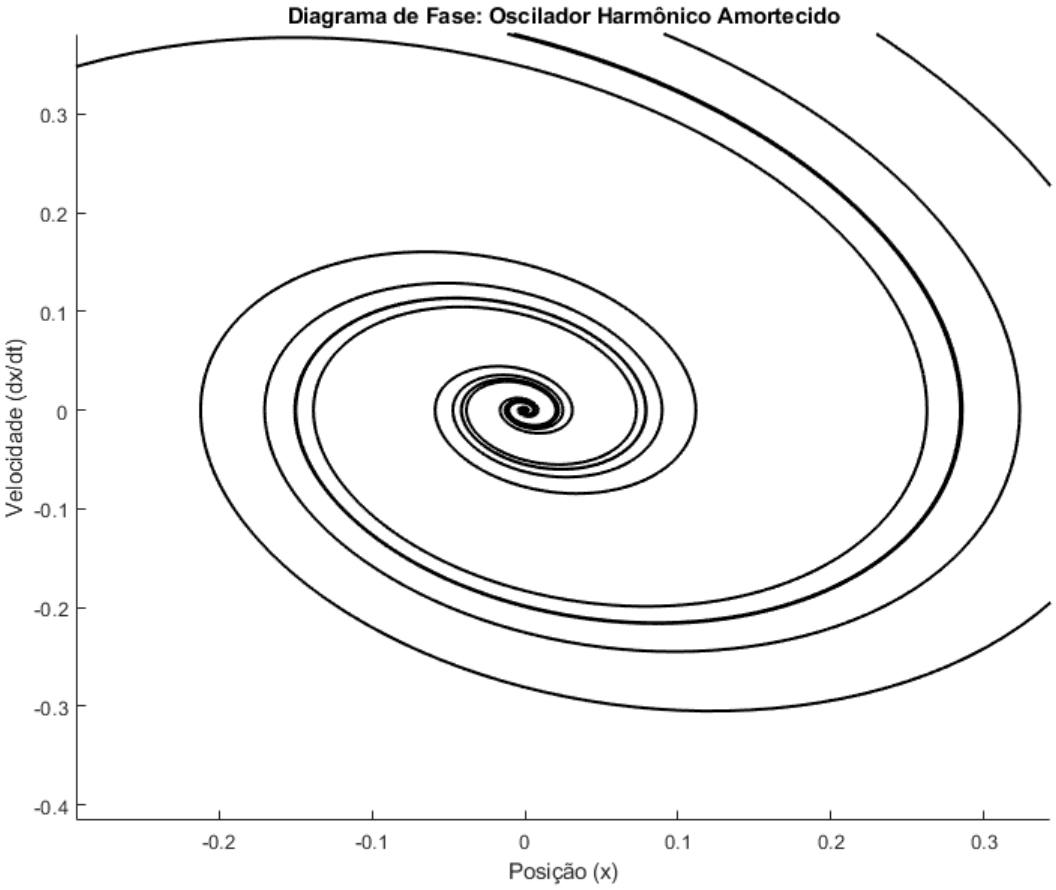



Figura 2.1: Diagrama de fase do oscilador harmônico amortecido: caso subamortecido. (Fonte: Autor)

tempo muito curto. À medida que $\beta \to \infty$, o intervalo de tempo no qual a amplitude diminui se torna ainda menor, resultando na interpretação física de que o objeto não está em movimento. Portanto, é importante destacar que o parâmetro de amortecimento não é infinitamente maior que a frequência angular, ou seja, $2\beta > 2\sqrt{\beta - \omega_0^2}$ [51]. Nesse caso, as oscilações são amortecidas ainda mais rapidamente, levando também ao equilíbrio.

### 2.1.2 Sistema de Lorenz

Edward Lorenz foi um grande estudioso na área da meteorologia, que ficou conhecido principalmente pelo seu estudo da dinâmica da atmosfera, nesse contexto Lorenz se dedicou ao estudo dos fenômenos de convecção na atmosfera. Quando um fluido é aquecido, duas moléculas ganham energia cinética, aumentando a possibilidade de colisão entre as partículas e diminuindo a interação de atração entre essas partículas. Quando isso ocorre leva na diminuição da densidade do fluido. A ocorrência desigual desse processo resulta em variações de densidade no fluido.

A região do fluido que tem mais energia cinética tem menor densidade, sendo assim, essa região tende a se deslocar para a parte superior do sistema enquanto a parte mais densa tem menor energia cinética e tende a se deslocar para a região inferior do sistema. À medida que a região mais densa é aquecida há um ganho de energia cinética diminuindo a densidade dessa região e por consequência disso, essa região tende a se deslocar para parte superior, como descrito anteriormente. Isso implica em um movimento de ciclo do fluido,

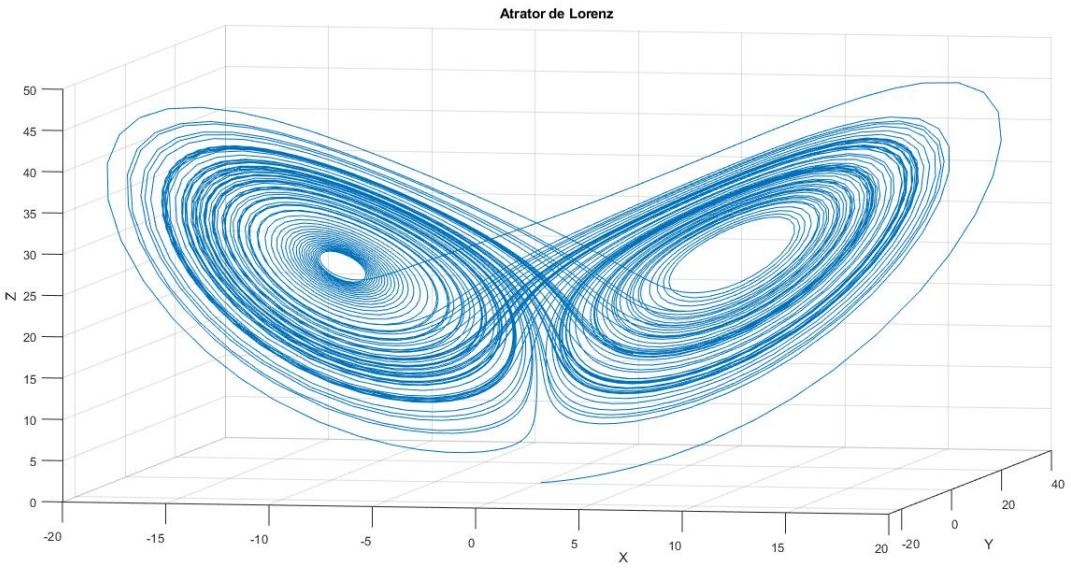



Figura 2.2: Atrator de Lorenz (Fonte: Autor)

chamado de convecção. Lorenz, visando criar modelos matemáticos para a previsão do tempo estudou profundamente esse processo na atmosfera. Ele escreveu as coordenadas velocidade para uma partícula sujeita a esse processo.

Denotando as coordenadas velocidade como $\dot{x}$, $\dot{y}$ e $\dot{z}$ obtemos o seguinte sistema

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = rx - y - xz \\ \dot{z} = xy - bz, \end{cases}$$

onde $\sigma$, $b$, e $r$ são parâmetros físicos da convecção com valores positivos, determinados empiricamente.[35]. Vamos considerar $\sigma = 10$, $r = 28$ e $b = 8/3$ assim podemos plotar as trajetórias.

Apenas observando a Figura 2.2, podemos identificar propriedades importantes nas trajetórias representadas. É evidente que não há periodicidade nessas trajetórias; no entanto, ao acompanhá-las, percebemos um movimento de um lado para o outro sem caracterizar um padrão típico e repetitivo. A forma geral da figura permanece inalterada, independentemente das condições iniciais selecionadas (contanto que desconsideremos as seções transitórias iniciais de uma trajetória) ou do método de integração adotado. Tanto um método de Euler de primeira ordem, com passos pequenos o suficiente, quanto uma técnica sofisticada de integração multi-ordem, produzirão imagens semelhantes [48]. No entanto, é crucial notar que os detalhes específicos das trajetórias são extremamente sensíveis às condições iniciais, como a quantidade de loops que as trajetórias executam. Portanto, torna-se incrivelmente complexo prever o comportamento de longo prazo das trajetórias. Pequenas variações nas condições iniciais podem resultar em diferenças significativas no desenrolar das trajetórias ao longo do tempo, o que torna a previsão precisa um desafio substancial [48].

Existem propriedades interessantes no atrator de Lorenz. Podemos notar que o sistema exibe uma simetria sob a transformação $(x, y, z) \longrightarrow (-x, -y, z)$ [36, 45]. Essa característica de invariância sob essa transformação específica mostra que o sistema mantém uma forma simétrica para todos valores de parâmetro, mesmo após a aplicação dessas mudanças nas variáveis.

**Teorema 2.2.** *Seja $E$ uma região sólida simples e seja $S$ a superfície fronteira de $E$, orientada positivamente (para fora). Seja $\boldsymbol{F}$ um campo vetorial cujas componentes tenha derivadas parciais contínuas em uma região aberta que contenha $E$. Então*

$$\iint_S \boldsymbol{F}.\boldsymbol{n}ds = \iiint_E \nabla.\boldsymbol{F}dv.$$

Agora definimos $\mathbf{F} = (\dot{x}, \dot{y}, \dot{z})$ e consideramos uma superfície fechada $S = S(t)$ em um instante que delimita um sólido $V = V(t)$. Vamos explorar o que ocorre com esse volume submetido a $\mathbf{F}$ à medida que o tempo passa. Os pontos iniciais estão em $S(t)$ e, após um certo intervalo $\Delta t$, a nova $S(t + \Delta t)$ terá um volume $V = V(t + \Delta t)$. É importante notar que, ao realizar esse procedimento, podemos estudar como o volume de $S$ se altera ao longo do tempo. Dessa forma, $\mathbf{F}$ representa o campo de velocidade que atravessa $S$, permitindo-nos escrever

$$\frac{V(t + \Delta t) - V(t)}{\Delta t} = \iint_S \mathbf{F}.\mathbf{n}ds. \tag{2.5}$$

Fazendo $\Delta t \longrightarrow 0$, teremos uma derivada do lado esquerdo da equação (2.5). Note que, $\nabla \cdot \mathbf{F} = -\sigma - \mathbf{1} - \mathbf{b}$. Logo, pelo Teorema 2.2(teorema do divergente), obtemos

$$\frac{dV}{dt} = \iiint (-\sigma - 1 - b)dV.$$

Assim obtemos a seguinte equação diferencial:

$$\frac{dV}{dt} = -(\sigma + 1 + b)V. \tag{2.6}$$

A equação diferencial (2.6) é simples de ser resolvida. então

$$V(t) = e^{-(\sigma+1+b)t}V(t_0), \tag{2.7}$$

pela equação (2.6) podemos observar que o vloume está se comrpimindo com o passar do tempo.

A contração de volumes é uma propriedade importante do sistema de Lorenz, pois a sua interpretação fornece informações importantes sobre a dinâmica do sistema. Quando consideramos um conjunto inicial abrangente de condições iniciais no sistema de Lorenz, ao longo do tempo, esse conjunto converge para um conjunto limite de volume extremamente reduzido, aproximando-se de um estado de volume zero. Essa trajetória de convergência é comparável à imagem de um balão cujo ar é gradualmente retirado, diminuindo seu volume [1].

É importante notar que todas as trajetórias que têm origem nesse conjunto inicial convergem para algum ponto dentro desse conjunto limite de volume quase nulo. Essa característica é um reflexo da contração de volumes presente nas soluções das Equações de Lorenz. Essa propriedade, ao restringir drasticamente as possíveis soluções, leva a um comportamento convergente em direção a esse conjunto limite.

A contração de volumes, portanto, não apenas indica uma redução no volume físico do sistema, mas também impõe limitações severas às trajetórias possíveis, restringindo as soluções válidas do sistema de Lorenz.

## 2.2 Sistemas dinâmicos dicretos

Um sistema dinâmico discreto tem como principal característica o seu comportamento ao longo de intervalos discretos de tempo. Isto é, a evolução do tempo é por meio de

funções iterativas que determina os estados do sistema em instantes específicos. Cada iteração representa uma etapa no tempo, marcando a transformação do sistema com base no seu estado anterior. O estado do sistema em um determinado intervalo de tempo é determinado pela aplicação de uma função iterativa ao estado no intervalo de tempo anterior. Isso significa que o estado atualizado é uma função do estado anterior, estabelecendo uma sequência de transformações ao longo do tempo discreto.

**Definição 2.3.** *Seja $x_{n+1} = f(x_n)$, com $n \geq 0$. A função $f$ é chamado de mapa e a sequência de pontos $\{x_{n+1}\}$ é chamado de órbita.*

**Definição 2.4.** *Dada uma função $f : X \to Y$, o gráfico da função de $f$ é o subconjunto, $G$ do produto cartesiano $X \times Y$, definido por*

$$G = \{(x, y) \in X \times Y : y = f(x)\}.$$

**Definição 2.5.** *Um ponto $p \in X$ chama-se ponto fixo da função $f : X \to Y$ se $f(p) = p$.*

**Definição 2.6.** *Seja $f$ um mapa sobre $\mathbb{R}$. Chamamos $p$ de ponto periódico de período $n$ (ponto $n$-periódico) se $n$ é o menor número inteiro, tal que $f^n(p) = p$. A órbita (com $n$ pontos) cujo o ponto inicial é $p$ é chamada de órbita periódica de período $n$ (órbita $n$-periódica).*

**Exemplo 2.7.** *Seja $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2 - 2$. Assim, para $f(x) = x$, temos $x^2 - 2 = x$, consequentemente, temos que resolver, $x^2 - x - 2 = 0$, então $x = -1$ e $x = 2$ são únicos pontos fixos de $f$. Note que, para $f^2(x) = x$, temos $(x^2 - 2)^2 - 2 = x$, desenvolvendo, obtemos $x^4 - 4x^2 - x + 2 = 0$. Logo, $x = -1, x = 2, x = \frac{-\sqrt{5}-1}{2}$ e $x = \frac{\sqrt{5}-1}{2}$ são pontos fixos de $f^2$ com $x = -1, x = 2$ já sendo pontos fixos de $f$. Note que os pontos $x = \frac{-\sqrt{5}-1}{2}$ e $x = \frac{\sqrt{5}-1}{2}$ aparecem resolvendo $f^2(x) = x$, logo eles são pontos periódicos de $f$ de período 2.*

**Exemplo 2.8.** *Não são todas as funções que possuem pontos fixos. Considere $f(x) = x^2 + 3$, logo temos que resolver $x^2 - x + 3 = 0$. Essa equação não possui raízes reais logo não tem pontos fixos.*

Os pontos fixos são cruciais para encontrar pontos periódicos, uma vez, que por definição os pontos periódicos são pontos fixos da função $f^n$. Assim é evidente que os pontos fixos são pontos periódicos de período 1. Em síntese, um ponto fixo pode ser considerado um caso particular de ponto periódico.

**Definição 2.9.** *Seja $f$ um mapa sobre $\mathbb{R}$ e seja $p \in \mathbb{R}$ tal que $f(p) = p$. Se todos os pontos nas proximidades de $p$ são atraídos para $p$, então $p$ é um ponto fixo atrator. Mais precisamente, se existe um $\epsilon > 0$, tal que para todo o $x < \epsilon$, $\lim_{n\to\infty} f^n(x) = p$, então $p$ é um ponto fixo atrator. Se todos os pontos na vizinhança $p$ tendem a se afastar de $p$, então $p$ é um ponto fixo repulsor.*

Quando as derivadas de todas as ordens existirem e a função for contínua, esse tipo de função será chamado de função **suave**.

**Teorema 2.10.** *Seja $f$ (suave) um mapa sobre $\mathbb{R}$ e $p$ um ponto fixo de $f$, então*

- *se $| f'(p)| < 1$, então $p$ é atrator.*
- *se $| f'(p)| > 1$, então $p$ é repulsor.*

*Demonstração.* Seja $p$ um ponto fixo de uma função suave $f$, onde $f$ é um mapa sobre $\mathbb{R}$. Considere um sistema dinâmico discreto $x_{n+1} = f(x_n)$ e um ponto $x_0$ nas proximidades de $p$, logo $x_0 = p + \epsilon$, com $\epsilon > 0$. Usando os termos lineares da expansão em série de Taylor, obtemos

$$x_1 = f(p + \epsilon) = p + f'(p)\epsilon$$

realizando o processo iterativo, temos que

$$\begin{gathered} x_2 = f(x_1) = f(p + f'(p)\epsilon) = p + (f'(p))^2\epsilon \\ x_3 = f(x_2) = p + (f'(p))^3\epsilon \\ \vdots \\ x_{n+1} = f(x_n) = p + (f'(p))^{n+1}\epsilon. \end{gathered}$$

Dessa forma, é possível notar que quando $\mid f'(p) \mid < 1$, o termo $f'(p)\epsilon$ diminui progressivamente à medida que as iterações acontecem. Nesse cenário, $p$ representa um ponto fixo atrator. Por outro lado, se $\mid f'(p) \mid > 1$, o termo $f'(p)\epsilon$ cresce indefinidamente conforme as iterações prosseguem, afastando-se de $p$. Logo, nesse caso, $p$ é um ponto fixo repulsor. □

**Exemplo 2.11.** *Considere a função $g(x) = x^2$, os pontos fixos dessa função são os pontos de intersecção entre $g(x)$ e $y = x$. Então basta resolver $x^2 - x = 0$. As raízes dessa equação são $0$ e $1$, isto é, os pontos fixos dessa função são $(0, 0)$ e $(1, 1)$. Sendo assim, temos que $f'(x) = 2x$, logo $f'(0) = 0$ e $f'(1) = 2$. Então pelo Teorema 2 temos que $p_1 = 0$ é atrator e $p_2 = 1$ é repulsor. De fato, ver pelo processo iterativo que para $x_0 = 0.5$ sequência de pontos $\{x_n\}$ converge para $0$. Se a escolha inicial $x_0 > 1$ ($x_0 = 1.5$) por exemplo, vamos notar que a sequencia de pontos se afasta de $1$ e tende a infinito.*

A partir das definições acima, podemos observar que todo ponto da forma $(x_0, y_0)$ que pertença ao gráfico da função $f$ é um ponto fixo. É fácil notar que os pontos fixos podem ser obtidos sem a necessidade de analisar o gráfico de $f$. Basta verificar os pontos de interseção entre o gráfico de $f$ com a reta $y = x$.

### 2.2.1 Análise Gráfica

Como visto anteriormente, os pontos fixos de um mapa podem ser encontrados determinando os pontos de interseção do gráfico de $f$ com a reta $y = x$ (função identidade). Nesse sentido, existe uma técnica que permite a observação do comportamento das órbitas em relação ao ponto fixo, trata-se da análise gráfica. Essa ferramenta que será explorada nessa seção é crucial para uma visualização qualitativa do comportamento das órbitas em relação aos pontos fixos do sistema.

Para realizar essa análise, é necessário traçar o gráfico da função $f$ junto com a reta identidade. Em seguida, é possível acompanhar a iteração da função através do desenho dos caminhos no gráfico. Para isso, partimos de um ponto arbitrário $x_0$, traçamos um caminho até sua reflexão no gráfico de $f$, chamaremos esse ponto de $A$. Em seguida, faremos um caminho horizontal até a reta identidade e, partindo dela, retornamos ao gráfico de $f$, alcançando um ponto $B$. É importante notar que a coordenada horizontal desses pontos forma a órbita do sistema. Esse procedimento é repetido sucessivamente, traçando novos caminhos para compreender a evolução da órbita do sistema em sua iteração com o ponto fixo. Essa técnica gráfica permite uma visualização intuitiva e compreensão do comportamento do sistema ao longo das iterações.

Pela Figura 2.3 observamos um padrão definido pelo trajeto percorrido pela órbita. Devido à semelhança desse padrão com uma escada, denominamos esse tipo específico de iteração como iteração tipo escada [3].

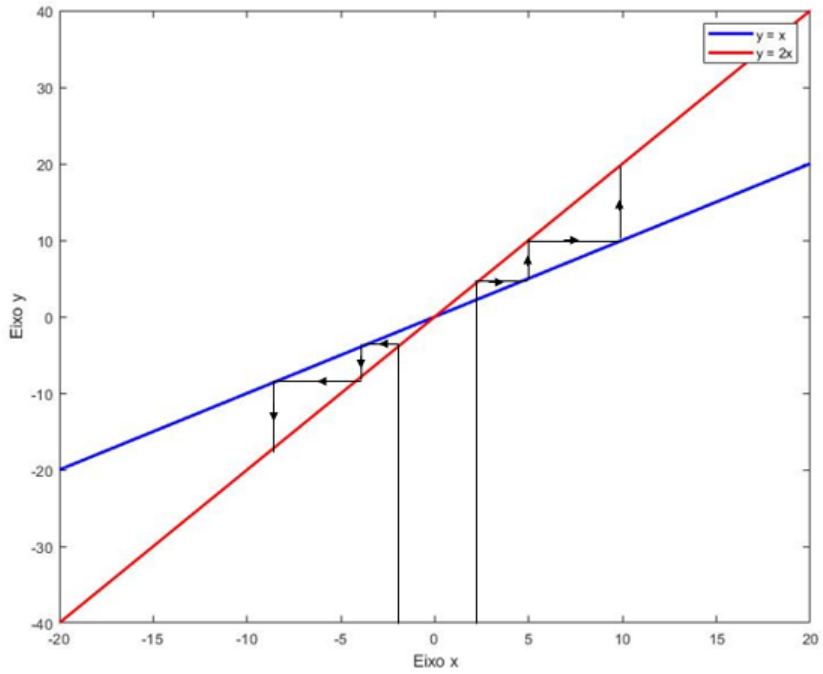



Figura 2.3: Exemplo de análise gráfica para $x_{n+1} = 2x_n$(Fonte: Autor)

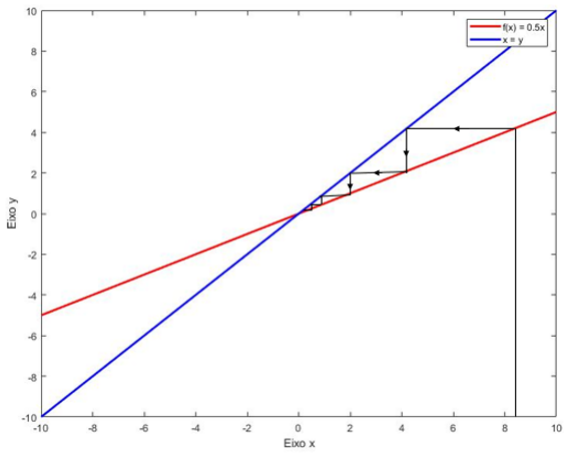
A Figura 2.3 ilustra um dos tipos de iteração possíveis entre os quatro padrões que os mapas lineares podem apresentar. Em geral, um mapa do tipo $x_{n+1} = sx_n$ exibirá diferentes comportamentos nos pontos fixos, dependendo dos valores que $s$ assumir. Observando a Figura 2.4 podemos ver os diferentes tipos de iterações que o mapa linear pode ter. A Figura 2.4(a) apresenta um exemplo de iteração em forma de escada. No entanto, diferentemente do caso ilustrado na Figura 2.3, notamos que as iterações convergem para o ponto fixo. A Figura 2.4(b) e Figura 2.4(c) exibem comportamento em espiral. No entanto, enquanto a Figura 2.4(b) mostra uma convergência para o ponto fixo, a Figura 2.4(c) apresenta iterações que se afastam do ponto fixo.

Então temos o seguintes casos para um mapa linear:

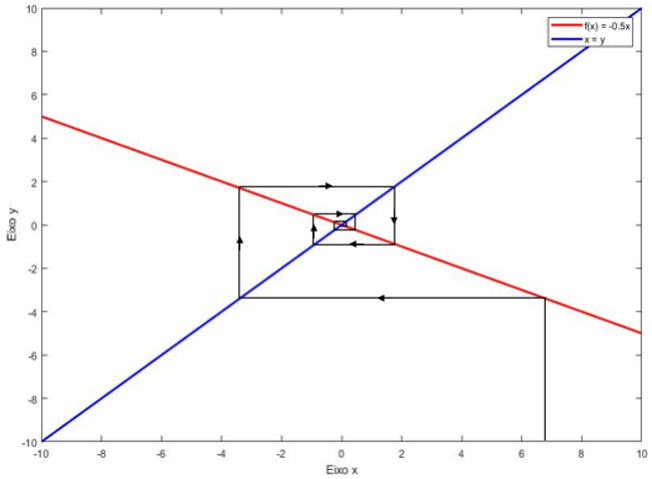
- iteração em escada para o ponto fixo $0 < s < 1$,
- iteração em espiral para o ponto fixo $-1 < s < 0$,
- iteração em escada para fora do ponto fixo $s > 1$,
- $U2$: iteração em espiral para fora do ponto fixo $s < -1$.

A análise gráfica é uma ferramenta valiosa na compreensão de sistemas dinâmicos não lineares. Para exemplificar essa aplicação, consideremos a família dos mapas logísticos definidos como $f_a = ax(1 - x)$. Esse mapa também conhecido como mapa de fluxo representam a evolução de populações ou fenômenos que dependem da interação entre crescimento e limitação do ambiente, sendo $a$ um parâmetro que controla essa dinâmica. A variação de $a$ influencia drasticamente o comportamento do sistema. Veremos mais à frente que o parâmetro $a$ pode nos levar a diferentes cenários de estabilidade, caos ou bifurcações. Entretanto, já nessa seção veremos o comportamento dos pontos fixos desse sistema.

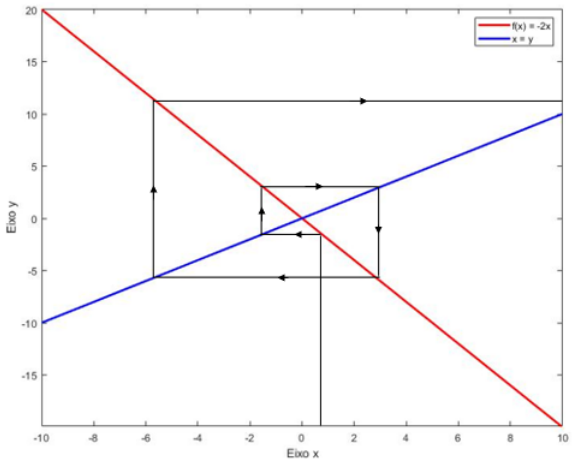
Resolvendo a equação $ax(1 - x) = x$, obtemos os pontos fixos do sistema logístico. Encontramos dois pontos fixos: $p_0 = 0$ e $p_a = \frac{a-1}{a}$. Esses pontos representam as situações de equilíbrio do sistema onde não há mudanças ao longo do tempo.




(a) 0<s<1

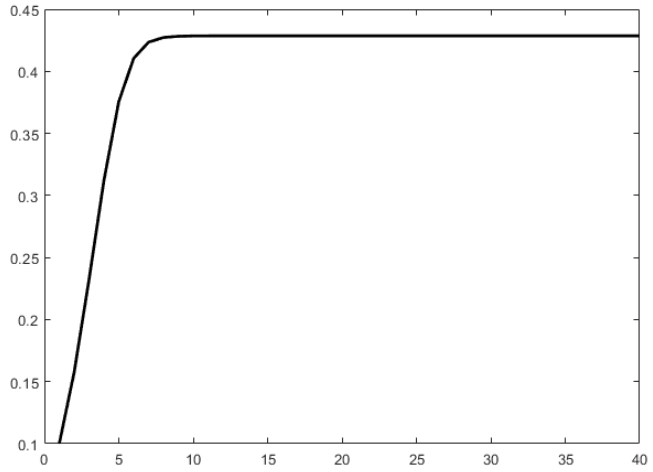



(b) $-1 > s > 0$.

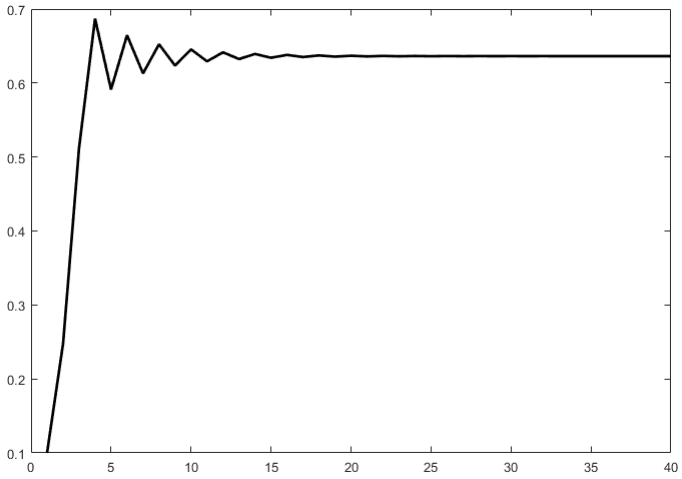



(c) $-1 > s$.

Figura 2.4: Iteração em torno do ponto fixo de mapas lineares. (Fonte: Autor)




(a) Convergência para o ponto fixo $p_a$ com parâmetro $a = 1.75$.




(b) Convergência para o ponto fixo $p_a$ com parâmetro $a = 2.75$.

Figura 2.5: Convergência para o ponto fixo da Equação 2.9 (Fonte: Autor)

Estudando as Figuras 2.5(a) e 2.5(b), podemos observar que ao ajustar o parâmetro $a$ resulta em duas formas distintas de convergência em relação ao ponto fixo. Especificamente, na Figura 2.5(b), o gráfico mostra um padrão de convergência oscilatória em direção ao ponto fixo.

A convergência oscilatória na Figura 2.5(b) sugere uma dinâmica complexa que se manifesta para valores de $a$ superiores a 3, constituindo um fenômeno que merece uma exploração mais detalhada ao longo deste estudo. Para essa investigação, adotaremos a abordagem gráfica mencionada anteriormente como uma ferramenta fundamental, buscando desvendar padrões e fenômenos associados.

Ao expandirmos essa análise gráfica, almejamos identificar regiões específicas no espaço de parâmetros onde comportamentos singulares, como oscilações e convergências distintas, se manifestam de maneira proeminente. Essa abordagem não apenas contribuirá para a compreensão do sistema em estudo, mas também lançará luz sobre as nuances dos padrões dinâmicos associados à variação do parâmetro $a$.

Dessa forma, a análise gráfica não se limita apenas à descrição de padrões observados, mas se estende à pesquisa mais profunda desses fenômenos, delineando um caminho para uma compreensão mais abrangente e refinada do comportamento do sistema.

A derivada da função logística, é dada por $f'_a(x) = -2ax + a$, pelo Teorema 2.10 a derivada nos ajuda a compreender a dinâmica dos pontos fixos do sistema. Vamos analisar especificamente o comportamento dessa derivada nos pontos $p_0$ e $p_a$ pois fornece informações cruciais da dinâmica e estabilidade do sistema. Veja que $f'(p_0) = a$ e $f'(p_a) = 2 - a$ como a derivada dos dois pontos dependem de $a$ será interessante analisarmos os dois pontos fixos ao mesmo tempo.

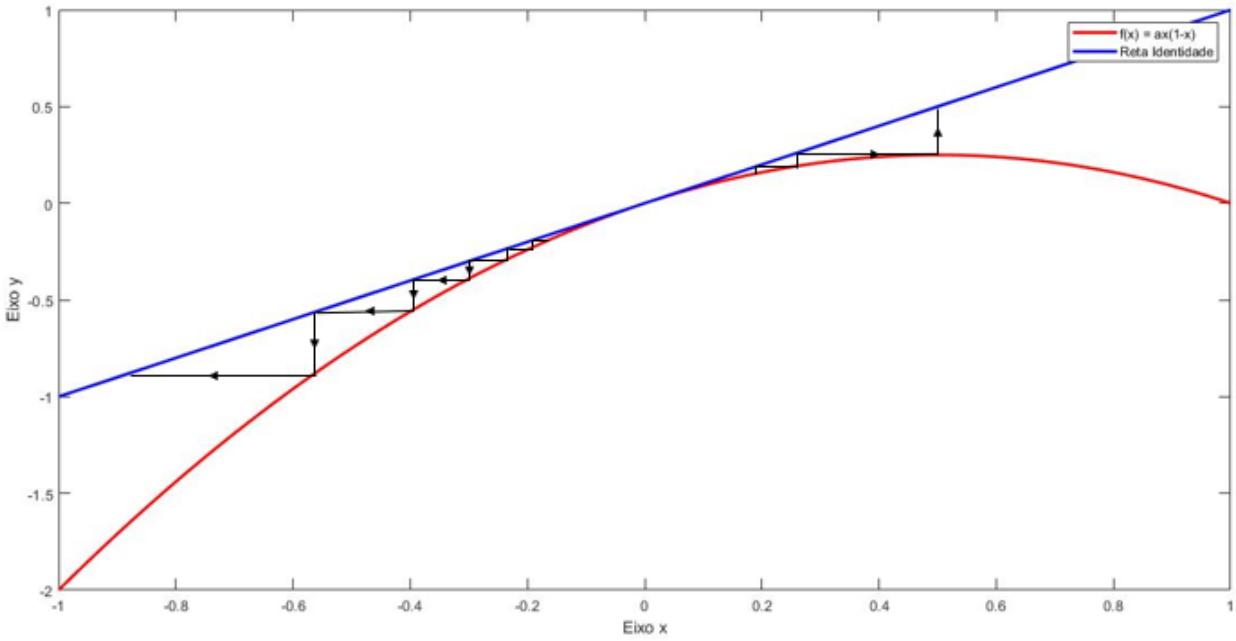



Figura 2.6: Mapa de fluxo iteração em torno do ponto fixo $p_0$ para $a = 1$ (Fonte: Autor)

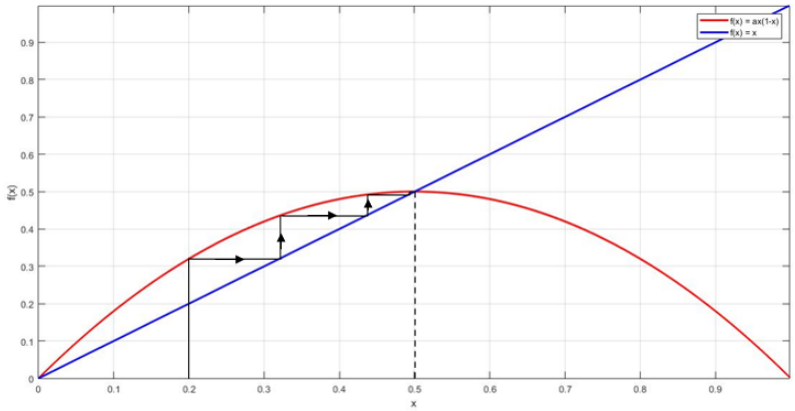
.

No caso em que $a = 1$, o ponto fixo $p_a = p_0 = 0$. Nesse cenário, a derivada nesse ponto é igual a 1. Utilizando análise gráfica, como demonstrado na Figura 2.6, observamos que as órbitas se afastam do ponto fixo. Isso significa que, para $a = 1$, temos um ponto fixo repulsor.

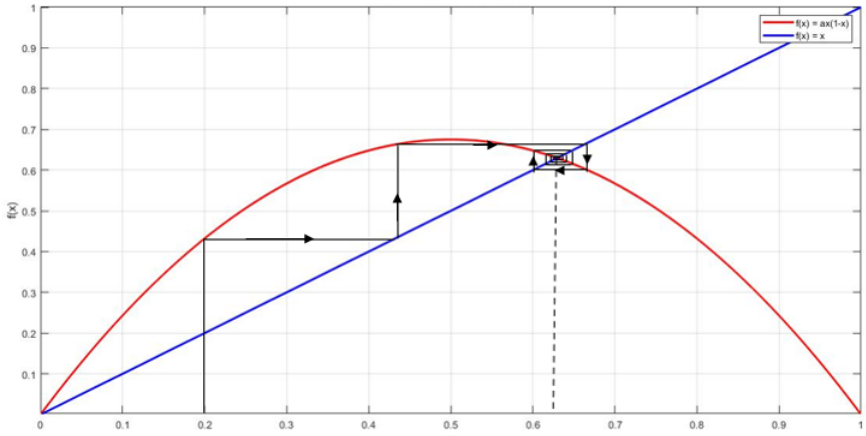
Vamos analisar o comportamento dos pontos fixos para $a > 1$. Primeiramente, observamos que $p_0 < p_a$. À medida que o parâmetro $a$ varia, diferentes dinâmicas de iteração emergem. Na Figura 2.7(a), é visível a iteração com o ponto fixo $p_a$ apresentando uma forma em escada, onde $p_a$ atua como um ponto atrator. Enquanto isso, $p_0$ também exibe uma iteração em forma de escada, permanecendo como um ponto repulsor.

Ao analisar as Figuras 2.7(a) e 2.7(b), percebemos que $p_0$ continua sendo um ponto repulsor em uma forma de escada. No entanto, a dinâmica da órbita ao redor de $p_a$ se modifica conforme $a$ varia. Note que para $a = 2.7$ a iteração tende para o ponto fixo de forma espiralada. De fato, os resultados obtido a partir da análise gráfica estão em consonância com o Teorema 2.10. Então, pelas derivadas de $f_a$, podemos obter algumas informações importantes. Quando $0 < a < 1$, $p_0 < 0$. Dessa forma, temos um ponto repulsor na forma de escada, pois $|f'_a(x)| > 1$.

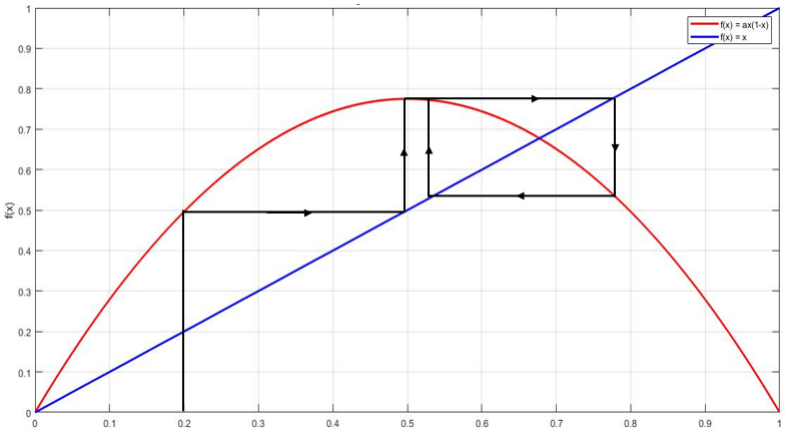
Agora, observe pela Figura 2.7(c) que quando $a = 3$ a dinâmica do sistema começa a se tornar mais complexa. Podemos observar, que órbitas periódicas começam a surgir quando $a > 3$, tais órbitas não são atraídas nem repelidas pelo ponto fixo $p_a$. Quando estudamos a derivada da função no ponto $p_a$ vemos que tal ponto se comporta como repulsor. A




(a) mapa de fluxo para $a = 2$.




(b) mapa de fluxo para $a = 2,7$.




(c) mapa de fluxo para $a = 3$.

Figura 2.7: Iterações do mapa de fluxo com as variações do parâmetro $a$ (Fonte: Autor)

dinâmica do sistema se torna cada vez mais complexa à medida que $a$ cresce, no entanto, o parâmetro $a$ não cresce indefinidamente. Ao longo deste trabalho, exploraremos a possibilidade de estudar a dinâmica do sistema mesmo quando $a > 3$.

## 2.3 Caos

Nas ciências exatas, a busca pela compreensão e previsão dos fenômenos muitas vezes envolve a descrição precisa de sistemas ao longo de um intervalo de tempo. A precisão na

previsão, oferecida por modelos matemáticos, é um objetivo central para se obter informações consistentes e precisas sobre fenômenos que se busca estudar. No entanto, nem todos os sistemas são previsíveis, tampouco, são bem comportados. Mesmo os sistemas aparentemente simples podem revelar comportamentos complexos com alta sensibilidade a perturbações mínimas.

É nesse cenário de extrema sensibilidade que entra o conceito de caos. Estudar sistemas acaba tendo extrema importância visto que muitos fenômenos reais apresentam uma dinâmica altamente sensível. O caos desafia nossa compreensão tradicional de previsibilidade e estabilidade, oferecendo um vislumbre de como pequenas variações podem levar a resultados imprevisíveis e complexos. Explorar o caos não é apenas uma jornada por sistemas complicados, mas uma incursão pela fronteira entre a ordem e a complexidade.

Mesmo em sistemas determinísticos, nos quais não há entradas aleatórias ou interferências externas, comportamentos irregulares podem surgir devido à presença de não linearidade, dimensionalidade ou falta de diferenciação do sistema. Apesar de obedecer a leis determinísticas precisas ao longo do tempo, o sistema pode exibir um comportamento aparentemente imprevisível. Antes de adentrarmos na definição do caos dentro da estrutura matemática, é crucial discutir alguns conceitos preliminares e definições dos espaços topológicos e métricos. Esses conceitos formam a base essencial para a compreensão e análise da teoria do caos [1, 3].

**Definição 2.12.** *Seja $X$ um conjunto não vazio e $\tau \subset P(X)$, onde $P(X)$ é um conjunto das partes de $X$. Então dizemos que $\tau$ é uma topologia sobre $X$ se*

*(a) O conjunto nulo $\phi$ e todo o conjunto $X$ pertencem a $\tau$.*

*(b) A união de qualquer coleção de subconjuntos $\tau$ pertence a $\tau$.*

*(c) A intersecção finita da coleção de subconjuntos de $\tau$ pertence a $\tau$.*

Dado um conjunto $X$, o conjunto potência de $X$ é denotado por $P(X)$ e definido por

$$P(X) = \{U \subseteq A : U \subseteq X\},$$

ou seja, $P(X)$ é o conjunto de todos os subconjuntos de $X$.

Se $\tau$ é uma topologia em $X$, então o par $(X, \tau)$ constitui um espaço topológico, no qual os subconjuntos de $\tau$ são denominados conjuntos abertos. Em um espaço topológico $(X, \tau)$, um subconjunto $A$ de $X$ é considerado uma vizinhança de um ponto $x \in X$ se existe um conjunto aberto $G$, tal que $x \in G \subset A$. Assim, um subconjunto $A \in (\tau, X)$ é uma vizinhança do ponto $x \in X$ se $A$ é um conjunto aberto. O complemento de um conjunto aberto é um conjunto fechado. Para qualquer subconjunto $A$ em um espaço topológico, sempre existe um menor conjunto fechado contendo $A$, que é a interseção de todos os conjuntos fechados contendo $A$. Esse menor conjunto fechado é conhecido como o fecho de $A$ e é denotado por $\bar{A}$.

**Definição 2.13.** *Um espaço métrico $(X, d)$ contém um conjunto não vazio $X$ e uma função distância $d : X \times X \longrightarrow \mathbb{R}^+ \cup \{0\}$, tal que para todo $x, y, z \in X$ temos as seguintes propriedades:*

*(a) $d(x, x) = 0$, (identidade).*

*(b) $d(x, y) = d(y, x)$, (simetria).*

*(c) $d(x, y) \leq d(x, z) + d(y, z)$ (desigualdade triangular).*

A função $d$ é chamada de uma métrica sobre $X$. Quando temos um conjunto $M$ e uma função $d$ que satisfaz as propriedades de uma métrica em $M$, cada valor $d(x, y)$ é denominado a distância entre os pontos $x$ e $y$. Esse par $(M, d)$, onde $d$ é uma métrica definida em $M$, é o que conhecemos como um espaço métrico. Nos referimos a qualquer elemento pertencente a um espaço métrico como um ponto desse espaço. Esse elemento pode ser um ponto em si, um número, uma função ou um vetor, dependendo do contexto ou dos exemplos que estamos considerando [18].

Se $x_1, ..., x_n$ e $y_1, ..., y_n$ são números reais arbitrários, então

$$\sum_{i=1}^{n} \mid x_i y_i \mid \leq \left[\sum_{i=1}^{n} x_i^2\right]^{1/2} \left[\sum_{i=1}^{n} y_i^2\right]^{1/2}. \tag{2.8}$$

Vamos mostrar que essa desigualdade é verdadeira. Primeiro veja que a desigualdade $2rs \leq r^2+s^2$ é verdadeira para quaisquer $r, s \in \mathbb{R}$, uma vez que $(r-s)^2 = r^2-2rs+r^2 \geq 0$, Assim se fizermos $p = \sqrt{x_1^2 + ... + x_n^2}$ e $q = \sqrt{y_1^2 + ... + y_n^2}$. logo

$$2\frac{\mid x_i \mid . \mid y_i \mid}{p.q} \leq \frac{x_i^2}{p^2} + \frac{y_i^2}{q^2}$$

para qualquer $i(1 \leq i \leq n)$. Somando em relação ao indice $i$, temos que

$$\frac{2}{p.q} \sum \mid x_i y_i \mid \leq 2$$

e portanto

$$\sum \mid x_i y_i \mid \leq p.q = (\sqrt{x_1^2 + ... + x_n^2})(\sqrt{y_1^2 + ... + y_n^2})$$

que é a desigualdade de Cauchy-Schwarz, ou seja está desmonstrado desigualdade (2.8).

**Exemplo 2.14.** *Para $X = \mathbb{R}^n$ e dados $x = (x_1, ..., x_n)$ e $y = (y_1, ..., y_n)$, mostraremos que:*

*(a)* $d(x, y) = \sqrt{(x_1 - y_1)^2 + ... + (x_n - y_n)^2}$

*(b)* $d_1(x, y) =\mid x_1 - y_1 \mid +...+ \mid x_n - y_n \mid$

*(c)* $d_2(x, y) = max\{\mid x_1 - y_1 \mid, ..., \mid x_n - y_n \mid\}$

*são métricas do $\mathbb{R}^n$. A métrica d é chamada de métrica euclidiana e naturalmente se inspira na fórmula da distância entre dois pontos no espaço usual [18]. As métricas $d_1$ e $d_2$ apesar de não parecerem tão naturais do ponto de vista prático são vantajosas [18]. Usando a desigualdade de Cauchy-Shwarz podemos mostrar a desigualdade triangular para primeira métrica. Então:*

$$[d(x, y)]^2 = \sum_{i=1}^{n} (x_i - y_i)^2 = \sum (x_i - z_i + z_i - y_i)^2$$

$$= \sum (x_i - z_i)^2 + 2\sum (x_i - z_i)(z_i - y_i)^2 + \sum (z_i - y_i)^2$$

$$\leq \sum (x_i - y_i)^2 + 2\left[\sum (x_i - z_i)\right]^{1/2} \left[\sum (z_i - y_i)^2\right]^{1/2} + \sum (z_i - y_i)^2$$

$$= \left[\sum (x_i - z_i)^2\right]^{1/2} + \left[\sum (z_i - y_i)^2\right]^{1/2} = [d(x, z) + d(z, y)]^2$$

*extraindo a raíz, obtemos*

$$d(x,y) \leq d(x,z) + d(z,y).$$

*Assim está provada a desigualdade triangular.*

*Para que* $d(x,y) = 0$, *então* $\sum_{i=1}^{n}(x_i - y_i) = 0$, *logo* $x_i - y_1 = 0$, *para todo* $i = 1, 2, ..., n$, *portanto* $x = y$. *Está demonstrado a identidade. Note que* $[\sum_{i=1}^{n}(x_i - y_i)]^{1/2} = [\sum_{i=1}^{n}(y_i - x_i)]^{1/2}$ *isso implica que* $d(x,y) = d(y,x)$. *Assim, está demonstrado a simetria.*

*Para a segunda métrica temos que* $d_1(x,y) = \sum_{1=1}^{n} |x_i - y_i|$. *então segue que:*

$$d_1(x,y) = \sum_{i=1}^{n} |x_i - y_i| = \sum \mid x_i - z_i + z_i - y_i \mid \leq \sum \mid x_i - z_i \mid + \sum \mid z_i - y_i \mid$$

$$= d_1(x,z) + d(z,y).$$

*Logo, obtemos* $d_1(x,y) \leq d_1(x,z) + d(z,y)$. *Note que as propriedade de simetria e identidade é análogo a métrica anterior, sendo assim, omitiremos alguns passos. Como* $\mid x_i - y_i \mid = \mid y_i - x_i \mid$, *então a propriedade de simetria é satisfeita, além disso, podemos ver que* $\mid x_i - y_i \mid = 0$ *se* $x_i = y_i$, *logo* $d(x,x) = 0$. *Portanto,* $d_1(x,y)$ *é uma métrica em* $\mathbb{R}^n$.

*Para* $d_2(x,y) = max\{\mid x_1 - y_1 \mid, ..., \mid x_n - y_n \mid\}$, *novamente a demonstração da primeira e segunda propriedade é análoga as métricas anteriores. Para provar a desigualdade triangular, temos que*

$$d_2(x,y) = \max\{\mid x_i - y_i \mid \ i = 1, ..., n\} \leq \max\{\mid x_i - z_i \mid + \mid z_i - y_i \mid, i = 1, ..., n\}.$$

*Como* $\mid x_i - z_i \mid \leq 0$ *e* $\mid z_i - y_i \mid \leq 0$, *temos:*

$$\max\{\mid x_i - z_i \mid + \mid z_i - y_i \mid, i = 1, ..., n\} = \max\{\mid x_i - z_i, i = 1, ..., n\} + \{\mid z_i - y_i \mid, i = 1, ..., n\}.$$

*Assim, obtemos a desigualdade triangular* $d_2(x,y) \leq d_2(x,z) + d_2(z,x)$.

**Definição 2.15.** *Uma transformação* $f : X \longrightarrow X$ *é expansiva se dados* $x, y \in X$, $x \neq y$ *existe* $k \in \mathbb{Z}$ *tal que* $d(f^k(x), f^k(y)) \geq \varepsilon$.

**Exemplo 2.16.** *Seja* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *dada por* $f(x) = 2x$ *é expansiva. De fato, dados* $x, y \in \mathbb{R}$, $\curvearrowleft \neq \curvearrowright$, *temos*

$$d(f^n(x), f^n(y)) = 2^n |x - y|.$$

*Logo, dado qualquer* $\varepsilon > 0$ *e tomando* $n \in \mathbb{N}$ *suficientemente grande de modo que* $2^n > \dfrac{\varepsilon}{|x-y|}$ *logo temos* $d(f^n(x), f^n(y)) > \varepsilon$.

**Definição 2.17.** *Em um espaço métrico* $(X,d)$, *uma bola aberta com centro* $a \in X$ *e raio* $r > 0$ *é um conjunto* $B(a,r) = \{x \in X : d(x,a) < r\}$ *e uma bola fechada com centro* $a \in X$ *e raio* $r > 0$ *é o conjunto* $B[a,r] = \{x \in X : d(x,a) \leq r\}$.

Seja $(X,d)$ um espaço métrico. Um subconjunto aberto de $X$ define uma topologia sobre $X$ [1], denominada de topologia métrica sobre $X$. Uma sequência de pontos $x_n$ em um espaço métrico $(X,d)$ converge para um ponto $p \in X$ se, para qualquer $\epsilon > 0$, existe um inteiro positivo $N$ tal que $d(x_n, p) < \epsilon$ para todo $n > N$. Em um espaço métrico $(X,d)$, uma sequência de pontos $x_n$ é chamada de sequência de Cauchy se, para qualquer $\epsilon > 0$, existe um inteiro positivo $N$ tal que $d(x_m, x_n) < \epsilon$ sempre que $m$ e $n$ satisfazem $m > n \geq N$. Um espaço métrico $(X,d)$ no qual toda a sequência de Cauchy converge para uma ponto de $X$ é chamado de espaço métrico completo.

**Exemplo 2.18.** *Um espaço métrico $(\mathbb{R}, d)$, quando $d$ é a métrica usual, é completo. De fato, Seja $(x_n)$ uma sequência de Cauchy em $(\mathbb{R}, d)$. Queremos mostrar que a sequência converge para algum ponto $x \in \mathbb{R}$. Para cada $n \in \mathbb{N}$, seja $B_n(x_n)$ o círculo aberto com centro $x_n$ e raio $1/n$. Como $(x_n)$ é uma sequência de Cauchy, temos que*

$$d(x_m, x_n) < \frac{1}{m},$$

*para todos $m, n \geq N$, para algum $N \in \mathbb{N}$. Isso implica que $x_n \in B_m(x_m)$ para todos $m, n \geq N$. Como $B_m(x_m)$ é aberto, temos que $x_n \in \bigcap_{m \geq N} B_m(x_m)$. A interseção de uma coleção infinita de conjuntos abertos é um conjunto aberto, portanto, $\bigcap_{m \geq N} B_m(x_m)$ é um conjunto aberto. Além disso, $\bigcap_{m \geq N} B_m(x_m)$ é não vazio, pois contém todos os $x_n$ para $n \geq N$. Portanto, existe um ponto $x \in \bigcap_{m \geq N} B_m(x_m)$. Queremos mostrar que $x$ é o limite da sequência $(x_n)$. Para cada $r > 0$, existe um $m \in \mathbb{N}$, tal que $1/m < r$. Então, para todos $n \geq m$, temos que $d(x, x_n) \leq d(x, x_m) + d(x_m, x_n) < \frac{1}{m} + \frac{1}{m} = \frac{2}{m} < r$. Isso implica que $x_n \to x$ conforme $n \to \infty$. Portanto, a sequência $(x_n)$ converge para $x \in \mathbb{R}$, o que prova que o espaço métrico $(\mathbb{R}, d)$ é completo.*

Um sistema dinâmico pode ser visto como o par ordenado $(X, f)$ onde $f : X \longrightarrow X$ é uma função no espaço topológico (ou espaço métrico). O sistema é dito reversível se $f$ é um homeomorfismo (a definição será vista mais a frente) de $X$ em $X$ [1].

**Definição 2.19** (Dependência sensível das condições inciais)**.** *Um mapa $f : X \longrightarrow X$ tem dependência sensível das condições iniciais, se existe $\delta > 0$ tal que para todo $x \in X$ e toda vizinhança $N_\epsilon = B(x, \epsilon)$ de $x$ existe $y \in N_\epsilon$ e um número inteiro $k > 0$ tal que a propriedade $\mid f^k(x) - f^k(y) \mid > \delta$ é satisfeita.*

Essa relação sugere que, para qualquer $x \in X$, existem pontos em $X$ que estão tão próximos de $x$ quanto se desejar, mas que se diferenciam dele por pelo menos $\delta$ após várias iterações do mapa $f$.

**Exemplo 2.20.** *Seja $g : S \longrightarrow S$ um mapa sobre um circulo unitário $S$ definido por $g(\theta) = 2\theta$. Seja $\theta_1 \in S$ e $N_\epsilon(\theta_1 - \epsilon, \theta_1 + \epsilon)$ uma vizinhança de $\theta_1$. Seja $\delta > 0$, então existe $\theta_2 \in N_\epsilon(\theta_1)$ e $k > 0$, tal que*

$$\mid g^k(\theta_1) - g^k(\theta_2) \mid = \mid 2^k\theta_1 - 2^k\theta_2 \mid = 2^k \mid \theta_1 - \theta_2 \mid > \delta, \forall\ \theta_1, \theta_2 \in N_\epsilon(\theta_1).$$

*Isso implica que o mapa $g$ é sensível às condições iniciais. Podemos verificar isso ao considerar dois pontos em uma vizinhança próxima, digamos $x = 0.25$ e $y = 0.2501$, e calcular a diferença $\mid g^k(x) - g^k(y) \mid$ após $k$ iterações. Na primeira iteração, obtemos $g(x) = 0.5$ e $g(y) = 0.5002$, resultando em $\mid g(x) - g(y) \mid = 0.0002$. Ao continuar as iterações indefinidamente, observamos um crescimento linear na diferença $\mid g^k(x) - g^k(y) \mid$ à medida que o número de iterações aumenta. Isso evidencia a propriedade de sensibilidade às condições iniciais (consulte o exemplo com mais detalhes em [1]).*

**Definição 2.21** (Conjunto denso)**.** *Em um espaço topológico $(X, \tau)$, um subconjunto $A$ de $X$ é dito ser um subconjunto denso se $\bar{A} = X$. Em outras palavras, $A$ é dito ser um subconjunto denso de $X$ se para qualquer $x \in X$, uma vizinhança de $x$ contém pelo menos um ponto de $A$.*

**Definição 2.22** (Transitividade topológica)**.** *Um mapa $f : X \longrightarrow X$ é dito ser topologicamente transitivo sobre $X$ se para quaisquer dois conjuntos abertos $U, V \subset X$ existe $k \in \mathbb{N}$, tal que $f^k(U) \cap V \neq \phi$. A função $f$ é chamada de transitividade total quando a composição $f^n$ é uma transitividade topológica para todo inteiro $n \geq 1$.*

Um mapa topologicamente transitivo implica que os pontos fixos, eventualmente, se movem de uma vizinhança arbitrariamente pequena para outra através de iterações. Isso significa que a órbita não pode ser dividida em dois conjuntos abertos disjuntos que permanecem invariantes sob o mapa. Um sistema de dinâmica discreta é considerado decomponível se houver uma cobertura aberta finita (com pelo menos dois elementos) de $X$, em que cada conjunto aberto na cobertura seja positivamente invariante sob o mapa $f$ [1]. Por outro lado, o sistema é classificado como indecomponível se não puder ser expresso como a união de dois subconjuntos não vazios, fechados e positivamente invariantes de $X$ [1]. Assim, a transitividade topológica implica a indecomponibilidade.

**Definição 2.23** (Mapa caótico)**.** *Um mapa $f : X \longrightarrow X$ é dito ser um mapa caótico sobre um subconjunto invariante $A \subseteq X$ se as seguintes condições são satisifeitas:*

*(a) a função $f$ tem dependência sensível das condições iniciais sobre $A$;*

*(b) $f$ é topológicamente transitivo sobre $A$;*

*(c) os pontos periódicos de $f$ são densos em $A$.*

Muitas vezes a tarefa de provar analiticamente que um mapa é caótico não é uma tarefa fácil. Nesse sentido, para mapas, cuja prova do seu comportamento caótico é mais complicada é possível recorrer a simulações computacionais ou comparações com mapas em que o caos já foi provado. O mapa shift, por sua vez, apresenta uma dinâmica caótica no qual é possível demonstrar segundo a definição.

Vamos dedicar o restante desta seção a exemplificar um mapa caótico. Nesse contexto, vamos considerar um conjunto finito de símbolos, chamado de alfabeto. Assim é possível construir infinitas sequências sobre esse espaço finito de símbolos [33]. Dessa forma, podemos definir $\Sigma_N$ como uma sequência de símbolos em um espaço de N-símbolos, como

$$\Sigma_N = \{s = (s_0 s_1 \dots) \mid s_i \in \{0, 1, 2, \dots, N-1\}\}.$$

Se $s$ e $t$ são dois elementos de $\Sigma_N$ então a distância entre $s$ e $t$ é definida por

$$d_\Sigma = \sum_{i=0}^{\infty} \frac{\mid s_i - t_i \mid}{N^i}$$

desde que, $\mid s_i - t_i \mid \leq N-1$ e $d_\Sigma(s,t) \leq \sum_{i=0}^{\infty} \frac{N-1}{N^i} = N$, logo $\Sigma_N$ é limitado.

**Teorema 2.24.** *Seja $s = (s_0 s_1 s_2 \dots)$, e $t = (t_0 t_1 t_2 ...)$ dois elementos em $\Sigma_2$.*

*(a) Se $s_i = t_i$ para $i = 0, 1, 2 \dots, k$, então $d_\Sigma \leq 1/2^k$.*

*(b) Se $d_\Sigma(s,t) < 1/2^k$ para algum $k$, então $s_i = t_i$ para $i = 0, 1, 2, \dots, k$.*

*Demonstração.* (a) Supondo que $s_i = t_i$ para cada $i = 0, 1, 2 \dots, k$, Assim segue que

$$d_\Sigma(s,t) = \sum_{i=0}^{\infty} \frac{\mid s_i - t_i \mid}{2^i} = \sum_{i=0}^{k} \frac{\mid s_i - t_i \mid}{2^i} + \sum_{i=k+1}^{\infty} \frac{\mid s_i - t_i \mid}{2^i} \leq \sum_{i=k+1}^{\infty} \frac{1}{2^i} = \frac{1}{2^k}.$$

(b) Suponha que $d_\Sigma < \frac{1}{2^k}$ para algum $k \geq 0$. Temos que mostrar que $s_i = t_i$ para $i = 0, 1, 2, ..., k$. Vamos supor por absurdo que existe um inteiro $j$, com $j \leq k$, isto é $j \in \{0, 1, 2, ..., k\}$ tal que $s_j \neq t_j$. Então

$$d_\Sigma(s,t) = \frac{1}{2^j} + \sum_{i=k+1}^{\infty} \frac{\mid s_i - t_i \mid}{2^i} \geq \frac{1}{2^j} \geq \frac{1}{2^k}.$$

Isso é uma contradição. Então $j$ não existe. Portanto $s_i = ti$, para $i = 0, 1, 2, 3, \dots, k$.

□

Vamos agora definir um mapa $S$ sobre o espaço de símbolos que faça um deslocamento de símbolo, isto é,

$$S(s_0 s_1 s_2 s_3 \dots) = s_1 s_2 s_3 \dots$$

esse mapa pode ser definido de muitas formas, mas aqui vamos considerar $S : [0,1) \longrightarrow [0,1)$. Desse modo podemos determinar os pontos fixos do mapa. Seja $x \in [0,1)$ então fazendo $S(x)$ e repetindo as iterações obtemos

$$S(0, a_1 a_2 a_3 \dots a_n) = 0, a_2 a_3 \dots a_n$$

$$S^2(0, a_2 a_3 a_4 \dots a_n) = 0, a_3 a_4 \dots a_n$$

$$\vdots$$

note que para $x = 0$, $S^n = 0$ logo 0 é um ponto fixo de $S$, além disso, se $x = 0, \bar{b}$ onde $0, \bar{b}$ é um decimal periódico, se o período é 1 então, $x$ para esse caso também é um ponto fixo, pois $S^n(0, \bar{b}) = 0, \bar{b}$. Veja ainda, que

$$S^n(0, a_1 a_2 a_3 \dots a_n \overline{b_1 b_2 \dots b_k}) = 0, \overline{b_1 b_2 \dots b_k}$$

então

$$S^{n+k}(0, a_1 a_2 a_3 \dots a_n \overline{b_1 b_2 \dots b_k}) = 0, \overline{b_1 b_2 \dots b_k},$$

logo,

$$S^{n+k}(x) = S^n(x).$$

Se $x \in \mathbb{Q}$, existem duas possibilidades: $x$ é um número decimal finito ou $x$ é uma dizima periódica. Se $x$ é um decimal finito quando se acabam as casas decimais após $n$ iterações $S^n(x) = 0$. Nesse contexto, se $x$ é um decimal periódico infinito é possível concluir que $x$ é um ponto periódico de período $k$.

Agora se $x \in [0,1)$ cuja sua representação binária é dada por

$$x = 0, a_1 a_2 a_3 \dots a_n = a_1 2^{-1} + a_2 2^{-2} + \dots + a_n 2^{-n}$$

para todo $i \in \mathbb{N}$ podemos definir $S : [0,1) \longrightarrow [0,1)$, como

$$S(x) = 2x \mod 1 = \begin{cases} 2x, & 0 \leq x < \frac{1}{2} \\ 2x - 1, & \frac{1}{2} \leq x < 1 \end{cases}.$$

Esse mapa é caótico, e para porvar isso, vamos verificar que o sistema satisfaz as três propriedades da Definição 2.23.

(a) Sejam $x, y \in I = [0,1)$ tal que $x = 0, a_1 a_2 \dots a_n a_{n+1} \dots$ e $y = 0, a_1 a_2 \dots a_n b_{n+1} b_{n+2} \dots$, de modo que, se $a_{n+i} = 0$ então $b_{n+i} = 1$ e se $a_{n+i} = 1$ então $b_{n+i} = 0$ para todo $i \in \mathbb{N}$. Assim temos que $\mid x - y \mid = 2^{-(n+1)} < 2^{-n}$. Isso implica que $\mid s(x) - s(y) \mid = 2^{-1}$. Se $2^{-1} = \delta$, então para qualquer $\varepsilon > 0$ podemos escolher $n$ suficientemente grande, tal que $\mid x - y \mid < \varepsilon$ implica que $\mid S^n(x) - S^n(y) \mid > \delta$. Portanto, o mapa $S(x)$ tem dependência sensível das condições iniciais.

(b) Seja $A$ e $B$ dois subintervalos de $I$, tal que o comprimento de $\mid A \mid = \mid B \mid = 2^{-(2n+1)}$. Desde que os pontos periódicos sejam densos em $I$ então existe um ponto periódico $b = 0, \overline{b_1 b_2 \dots b_k} \in B$. Seja $c = 0, a_1 a_2 a_3 \dots$ um ponto médio de $A$ e $z = 0, a_1 a_2 a_3 \dots \overline{b_1 b_2 \dots b_k}$ onde $\overline{b_i}$ é a parte periódica de $z$. Então $\mid c - z \mid = 2^{-n+2}$. Isso implica que $z \in A$ e $S^{n+2}(z) = 0, \overline{b_1}$ sobre $I$. Desde que $A$ e $B$ sejam disjuntos e o mapa $S(x)$ tenha topologia mista.

(c) Seja $x = 0, a_1a_2a_3\ldots$ qualquer número em $I$ e $\varepsilon > 0$ muito pequeno os núemros $t_n = 0, a_1a_2a_3\ldots$ são pontos periódicos do mapa $S(x)$ e sua diferença é dada por

$$\mid x - t_n \mid = \mid 0, a_1a_2\cdots - 0, a_1a_2\ldots a_n \mid = \sum_{i=0}^{\infty} \frac{a_{n+i}}{2^{n+i}}$$

para $a_i = 0$ ou $a_i = 1$

$$\leq \sum_{i=0}^{\infty} 2^{-(n+i)} = \frac{1}{2^n} < \varepsilon$$

quando $n$ é suficientemente grande. Isso mostra que os pontos periódicos de $S(x)$ são densos $I$.

Como as três propriedades foram satisfeitas então $S(x)$ é caótico.00

### 2.3.1 Expoentes de Lyapunov

Vimos em seções anteriores que um ponto fixo de um sistema dinâmico discreto é fortemente influenciado pela derivada do mapa. Através da análise da derivada, podemos determinar se um ponto fixo atua como atrator ou repulsor. Para um ponto periódico de período $k$, é necessário examinar a derivada da $k$-ésima iteração do mapa, que, pela regra da cadeia, é o produto das derivadas nos $k$ pontos da órbita. Suponhamos que o produto das derivadas seja $a > 1$. Isso implica que a órbita de cada vizinhança $x$ do ponto periódico $x_1$ se separa aproximadamente $a$ vezes a cada $k$ iterações. Esse é um acúmulo de separação ao longo do tempo, significando que são necessárias $k$ iterações para separar por uma distância $a$ [3]. O conceito de número de Lyapunov é introduzido para quantificar a média multiplicativa da separação entre o ponto $x$ e o ponto $x_1$. Um número de Lyapunov igual a 2 significa que, em média, a distância entre a órbita de $x_1$ e a órbita de qualquer vizinhança do ponto $x$ dobra a cada iteração.

Queremos compreender esse conceito mesmo quando $x_1$ não é um ponto fixo ou periódico. Um número de Lyapunov igual a 1/2 indicaria que a distância entre as órbitas de $x$ e $x_1$ está sendo reduzida pela metade a cada iteração, fazendo com que estas órbitas se aproximem cada vez mais. A importância do número de Lyapunov é sua aplicabilidade às órbitas não periódicas. A característica fundamental das órbitas caóticas é sua sensibilidade às condições iniciais, o que implica na separação eventual das trajetórias dessas condições iniciais à medida que o tempo avança. De fato, outra definição para órbitas caóticas ou mapas caóticos é a não periodicidade, ou seja, quando o número de Lyapunov é maior que 1.

**Definição 2.25.** *Seja $f$ um mapa real linear. O número de Lyapunov $L(x_1)$ da órbita $\{x_1, ...x_n\}$ é definido como*

$$L(x_1) = \lim_{n\to\infty} (|f'(x_1)|...|f'(x_n)|)^{1/n},$$

*se o limite existe. O expoente de Lyapunov $h(x_1)$ é definido como*

$$h(x_1) = \lim_{n\to\infty} \frac{1}{n}[\ln\ |f'(x_1)| + ... + \ln\ |f'(x_n)|],$$

*se o limite existe.*

**Observação 2.26.** *$h$ existe, se e somente se, $L$ diferente de zero existir. Então* $\ln\ L = h$

**Observação 2.27.** *O número e expoente de Lypunov são indefinidos para algumas órbitas. Em particular, uma órbita contendo um ponto $x_i$ com $f'(x_i) = 0$, então o expoente de Lyapunov é indefinido.*

Segue da definição do número de Lyapunov que o ponto fixo $x_1$ para um mapa $f$ é $\mid f'(x) \mid$, ou equivalentemente, o expoente de lyapunov é $h = ln|f'(x_1)|$. Se $x_1$ é um ponto periódico de periodo $k$, então:

$$h(x_1) = \frac{\ln \ |f'(x_1)| + ... + \ln \ |f'(x_k)|}{k}$$

para uma órbita periódica, o número de Lyapunov $e^{h(x_1)}$ descreve o alongamento local médio, por iteração, próximo a um ponto da órbita.

**Definição 2.28.** *Seja $f$ um mapa suave. Uma órbita $\{x_1, x_2, ..., x_n, ...\}$ é chamado assintóticamente periódico, se a órbita periódica converge a medida que $n \longrightarrow \infty$; isso significa que existe uma órbita periódica $\{y_1, y_2, ..., y_k, y_1, y_2\}$ tal que:*

$$\lim_{n\to\infty} |x_n - y_n| = 0$$

**Teorema 2.29.** *Seja $f$ um mapa real linear. Se a órbita $\{x_1, x_2...\}$ de $f$ satisfaz $f'(x) \neq 0$ para todo $i$ e é assintóticamente periódico, à órbita periódica $\{y_1, y_2...\}$, então as duas órbitas tem expoentes de Lyapunov idênticos.*

*Demonstração.* Usando o fato de que uma sequência média converge para uma sequência limite; isto é, se $s_n$ é uma sequência infinita com $\lim_{n\to\infty} s_n = s$ então

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} s_i = s$$

Assuma $k = 1$ para começar com $y_1$ sendo um ponto fixo. Desde que $\lim_{\to\infty} = y_1$ o fato de que a derivada $f'$ é contínua implica que

$$\lim_{n\to\infty} ln|f'(x_n)| = ln|f'(y_1)|.$$

Esta equação nos fornece o limite de uma sequência infinita. Usando o fato de que a média da sequência converge para a sequência limite, vemos que

$$h(x_1) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} = \ln \ |f'(y_1)| = h(y_1).$$

Quando assumimos $k > 1$ e $y_1$ não é necessariamente o ponto fixo, podemos arfirmar que $y_1$ é de fato, um ponto fixo de $f^k$. Isso decorre da relação entre a órbita periódica e $x_1$ e $f^k$ a cada $k$ iterações, a órbita $x_1$ retorna a um ponto que é um ponto fixo do mapa $f^k$, ou seja, $y_1$ é esse ponto fixo. Dessa forma, estabelecemos que $y_1$ é um ponto fixo de $f^k$, e a órbita periódica $x_1$ é assintoticamanete periódica sob $f^k$. Isso significa que, à medida que avaçamos as iterações de $f^k$ a órbita $x_1$ tende a se aproximar cada vez mais da órbita periódica $y_1$ sob o mapa $f^k$.

□

## 2.4 Bacia de Atração

Em sistemas dinâmicos, certos pontos ou conjuntos de pontos podem ser atratores, ou seja, regiões do espaço de estados para onde o sistema evolui ao longo do tempo. A bacia de atração é a região ao redor desse atrator que captura todas as condições iniciais que eventualmente convergem para esse estado estável.

**Definição 2.30.** *Seja $F$ um mapa sobre $\mathbb{R}^n$ e $p$ um ponto fixo atratator ou periódico de $F$. A bacia de atração de $p$ ou somente bacia de $p$ é o conjunto de pontos $x$ tal que $|f^k(x) - f^k(p)| \to 0$, a medida que $k \to \infty$.*

**Exemplo 2.31.** *Para o mapa $f(x) = ax$ sobre $\mathbb{R}$ com $|a| < 1$, zero é um ponto fixo atrator, em que a bacia de atração é toda a linha real. Mais genericamente se $F$ é um mapa sobre $\mathbb{R}$ cuja matriz representação tem autovalores distintos menores que um em módulo, então a origem é um ponto fixo atrator e o $\mathbb{R}^n$ é uma bacia de atração.*

**Teorema 2.32.** *Seja $f$ um mapa contínuo sobre $\mathbb{R}$*

*(a) Se $f(b) = b$ e $x < f(x) < b$, para todo $x$ em $[a, b)$, então $f^k(a) \to b$.*

*(b) Se $f(b) = b$ e $b < f(x) < x$ para todo $x$ em $(b, c]$, então $f^k(c) \to b$.*

*Demonstração.* Primeiro vamos provar o item 1. Se $f(b) = b$ e $x < f(x), b$ para todo $x$ em $[a, b)$, então $f^k(a) \to b$. Seja $x_0 = a$ e $x_{i+1} = f(x_i)$, para $i \geq 0$. Suponha $x \in [a, b)$, então $f(x) \in [a, b)$ devido $x < f(x) < b$. Portanto, todos os $x_i$ estão em $[a, b)$. Além disso, os $x_i$ são estritamente crescentes e limitados superiormente por $b$. Como $x_i \to_\star$ para $x_\star \in [a, b]$, temos:

$$x_\star = \lim_{i\to\infty} x_{i+1} = \lim_{i\to\infty} = f(x_\star),$$

pela continuidade de $f$. Como $b$ é o único ponto fixo em $[a, b]$ e sabemos que $x_* \in [a, b]$ e $x_* = f(x_*) = b$, concluimos que $f^k(a) \to b$.

Agora vamos provar o item 2. Seja $x_0 = c$ e $x_{i+1} = f(x_i)$ para $i \geq 0$. Suponha $x \in (b, c]$, então $f(x) \in (b, c]$ devido a $b < f(x) < x$. Portanto, todos os $x_i$ estão em $(b, c]$. Além disso, os $x_i$ são estritamente decrescente e limitados por $b$. Como $x_i \to x_*$ para $x_* \in [b, c]$, temos:

$$x_\star = \lim_{i\to\infty} x_{i+1} = \lim_{i\to\infty} = f(x_\star),$$

pela continuidade $f$. Como $b$ é o único ponto fixo em $[b, c]$ e sabemos que $x_* \in [b, c]$ e $x_\star = f(x_*) = b$, concluimos que $f^k(c) \to b$. □

**Exemplo 2.33.** *Considere o mapa logístico $f(x) = ax(1 - x)$. Se $0 < a < 1$, existe um ponto fixo atrator $p = 0$. Do Teorema 2.32, $((a - 1)/a, 1]$ está na bacia de atração $x = 0$. A representação gráfica das órbitas, além disso, o intervalo $[1, 1/a)$ contém uma base de atração de 0. Os intervalos $(-\infty, (a - 1)/a)$ e $(1/a, \infty)$ consitem de condições iniciais que divergem para o inifinito.*

**Definição 2.34.** *Seja $f$ um mapa suave sobre $\mathbb{R}$. A derivada Schwarziana de $f$ é definida por*

$$S(f)(x) = \frac{f'''(x)}{f'(x)} - \frac{3}{2}\left(\frac{f''(x)}{f'(x)}\right)^2.$$

*Nós iremos dizer que um mapa tem Schwarziana negativa se $S(f)(x)$ é negativa sempre que $f'(x) \neq 0$*

**Teorema 2.35.** *Sejam $f$ e $g$ mapas sobre $\mathbb{R}$ com derivadas Schwarzianas negativas, então a composição $f \circ g$ possui derivada Schwarziana negativa.*

*Demonstração.* Primeiro vamos calcular

$$(f \circ g)'' = (g'(f \circ g))' = (g')^2.(f'' \circ g) + g''.(f' \circ g)$$

e

$$S(f \circ g)''' = (g')^3.(f''' \circ g) + 3g'g''.(f'' \circ g) + g'''.(f \circ g).$$

Assim, segue que

$$S(f \circ g) = (g')^2 \frac{f''' \circ g}{f' \circ g} + 3g'' \frac{f'' \circ g}{f' \circ g} + \frac{g'''}{g'} - \frac{3}{2}\left(g' \frac{f'' \circ g}{f' \circ g} + \frac{g''}{g'}\right)^2,$$

desenvolvendo o último termo da equação obtemos

$$S(f \circ g) = (g')^2 \frac{f''' \circ g}{f' \circ g} + 3g'' \frac{f'' \circ g}{f' \circ g} + \frac{g'''}{g'} - \left[\frac{3}{2}\left(g' \frac{f'' \circ g}{f' \circ g}\right)^2 + 3g'' \frac{f'' \circ g}{f' \circ g} + \frac{3}{2}\left(\frac{g''}{g'}\right)\right]$$

arrumando os termos obtemos

$$S(f \circ g) = (g')^2 \left[\frac{f''' \circ g}{f' \circ g} - \frac{3}{2}\left(\frac{f'' \circ g}{f' \circ g}\right)^2\right] + \left[\frac{g'''}{g'} - \frac{3}{2}\left(\frac{g''}{g'}\right)^2\right]$$

Note que,

$$S(f) \circ g = \left[\frac{f''' \circ g}{f' \circ g} - \frac{3}{2}\left(\frac{f'' \circ g}{f' \circ g}\right)^2\right]$$

e

$$S(g) = \frac{g'''}{g'} - \frac{3}{2}\left(\frac{g''}{g'}\right)^2.$$

Logo, obtemos:

$$= (g')^2.(Sf \circ g) + S(g)$$

Como $S(f) < 0$ e $S(g) < 0$ por hipótese, então $(g')^2.(Sf \circ g) + S(g) < 0$. □

**Observação 2.36.** *Se $S(f) < 0$, então $S(f)^n < 0$ para todo $n > 0$. Esta é a razão pela qual podemos usar o Schwarziano em dinâmica [11].*

**Teorema 2.37.** *Se o mapa $f$ sobre $\mathbb{R}$ tem derivada schwarziana negativa, e se $p$ é um ponto fixo ou um ponto periódico de $f$ então*

*(a) $p$ tem uma bacia infinita; ou*

*(b) existe um ponto crítico de $f$ na bacia de $p$; ou*

*(c) $p$ é um repulsor.*

*Demonstração.* Vamos assumir que $p$ não é um ponto repulsor nem um atrator com bacia infinita, e vamos provar que existe um ponto crítico $c$ na bacia de $p$. Primeiro considere o simples caso em que $f(p) = p, f'(p) \geq 0$. Se $p$ é umponto crítico de $f$, entaão terminamos. Por outro lado, $0 < f'(p) \leq 1$, então $p$ não é repulsor. Note que $f'(x)$ não pode ser repulsor na vizinhança de $p$ ja que nesse intervalo $f'' = f''' = 0$ implicaria $S(f) = 0$. É claro pelo que pelo Teorema 2.32 desde que p não tenha uma bacia infinita, nós podemos concluir que $f$ tem ponto crítico na bacia de $p$, nessa caso terminamos, ou existe um

intervalo $(a, b)$ na bacia de contração de $p$ tal que $f'(a) \geq 1$ e $f'(b) \leq 1$. Como $f'(b) \leq 1$, existe um minimo local $m$ para $f'$ na abacia de $p$. Note que , $f''(m) = 0$ e $f'''(m) > 0$ de modo que a derivada schwarziana implica que $f'(m) < 0$. Pelo teorema do valor médio existe um número $c$ entre $p$ e $m$ tal que $f'(c) = 0$. Como o intervalo (a, b) está contido na bacia de $p$ e $a < c < b$, encontramos um ponto crítico na bacia de $p$.

Podemos agora, descrever o caso geral, no qual $p$ é um ponto periódico de período $k$. Como $p$ não é um repulsor nem um atrator com bacia infinita para o mapa $f$, o mesmo é verdade para o ponto fixo do mapa $f^2k$. Como $(f^{2k})'(p) = f(k)(p)^2$, sabemos que $0 \leq (f^{2k})'(p) \leq 1$, e podemos aplicar o argumento acima desde que pela Observação 2.36 também tem schwarziano negativo. Assim nós concluímos que $f^{2k}$ tem um ponto crítico na bacia de $p$, e então $f$ também tem. □

O mapa logístico $f(x) = ax(1 - x)$, quando $0 \leq a \leq 4$ tem no máximo um atrator periódico. E de fato se $f$ tem Schwarzina negativa então podemos aplicar o Teorema 2.32. Toda órbita que começa fora do intervalo $[0, 1]$ tende para $-\infty$ então não há pontos em $[0, 1]$ tem uma bacia infinita. Como o único ponto crítico de $f$ é $x = 1/2$, pode haver no máximo uma órbita periódica. Para $a = 4$ todas as órbitas periódicas são repulsoras. Aqui está outra maneira de ver esse fato, desde quando $a = 4$, a órbita com valor inicial $x = 1/2$ mapeia em duas iterações para a ponto fixo repulsor 0.

## 2.5 Bifurcações

Exploramos em seções anteriores que os pontos fixos são indicativos de situações de equilíbrio em sistemas dinâmicos. Além disso, identificamos que esses pontos de equilíbrio podem assumir diversas formas e que há diferentes abordagens para investigá-los. É interessante notar que a dinâmica dos pontos fixos, e até mesmo dos pontos periódicos, pode sofrer alterações conforme os parâmetros do sistema são modificados. Portanto, torna-se essencial estudar o comportamento do sistema variando esses parâmetros. Essa análise permite uma compreensão mais profunda do sistema, enriquecendo nossa compreensão e fornecendo informações mais precisas sobre suas características e possíveis estados. Ao investigar as variações dos parâmetros, somos capazes de capturar nuances e mudanças fundamentais no comportamento do sistema, ampliando nossa visão sobre sua dinâmica e possíveis transições entre diferentes estados de equilíbrio e comportamentos.

### 2.5.1 Duplicação de Período e Bifurcações

Denominamos um valor do parâmetro no qual ocorre uma mudança no número ou na estabilidade dos pontos fixos ou periódicos como um valor de bifurcação do parâmetro, e a trajetória em si como uma trajetória de bifurcação.

**Definição 2.38.** *Uma família uniparamétrica de mapas sobre o $\mathbb{R}^n$ é um conjunto de mapas $F_a$, uma para cada valor de parâmetro pertencente a um intervalo $I$ de números reais. Referimo-nos a $\mathbb{R}^n$ como o espaço de estados e a $I$ como o espaço de parâmetros, e digamos que $F$ depende de um parâmetro escalar $a \in I$.*

Dado o foco deste trabalho no estudo do mapa de Hénon, o qual é bidimensional, buscamos analisar mapeamentos em espaços de estado $\mathbb{R}$ e $\mathbb{R}^2$. Dois tipos de bifurcações são fundamentais. Na primeira, chamada de bifurcação de sela-nó, os pontos fixos surgem. A segunda é chamada de bifurcação de duplicação de período, onde um ponto fixo perde sua estabilidade e simultaneamente uma nova órbita de período duplicado é criada. Ambas essas bifurcações básicas ocorrem na família quadrática unidimensional.

**Observação 2.39.** *Seja $f_a = a - x^2$, onde $a$ é um parâmetro escalar. Quando $a < -1/4$, não há pontos fixos. No ponto $a = -1/4$, a reta identidade tangencia o gráfico da função $f_a$, resultando em exatamente um ponto fixo em $x = -1/2$. Para cada $a$ estritamente maior que $-1/4$, o gráfico de $f_a$ intersecta a reta $y = x$ em dois pontos, gerando assim dois pontos fixos para $f_a$. O ponto $(a, x) = (-1/4, -1/2)$ é um ponto de bifurcação para o mapa $f$, visto que o número de pontos fixos varia em $a = -1/4$. Quando $a = 1/2$, o mapa $f$ apresenta um ponto fixo repulsor em $x = (-1-\sqrt{3})/2$ e um ponto fixo atrator em $x = (-1+\sqrt{3})/2$. O fenômeno no qual um par de pontos fixos surge em uma região onde não existia nenhum, à medida que um parâmetro é variado, é denominado bifurcação nó de sela .*

*Na bifurcação nó de sela, dois pontos fixos de $f_a$ nascem à medida que o parâmetro $a$ aumenta, um sendo estável e o outro instável. O termo "nó de sela"deriva desse tipo de bifurcação em uma estrutura bidimensional no espaço de estados, onde a órbita instável representa uma sela, e a órbita estável atua como um atrator ou "nó". Para mapas nos quais o espaço de estados é unidimensional, essa bifurcação também é ocasionalmente chamada de bifurcação tangente. Esse nome decorre do fato de que a derivada $f_a$ em uma órbita de bifurcação nó de sela de ponto fixo deve ser igual a 1, resultando na reta $y = x$ sendo tangente ao gráfico de $f$.*

*Em seções anteriores, estabelecemos que se $|f'_a| < 1$, então o ponto fixo é um atrator, enquanto se $|f'_a| > 1$, o ponto fixo é um repulsor. É fácil observar que à medida que o parâmetro $a$ varia, o comportamento dos pontos fixos se modifica. Conforme $a$ aumenta de $-1/4$ para $3/4$, a derivada de $f_a$ no ponto fixo atrator diminui de 1 para $-1$. Para valores de $a < 3/4$, a derivada de $f_a$ no ponto fixo ultrapassa a fronteira de $-1$, tornando o ponto fixo repulsor. Entretanto, para parâmetros na faixa de $(3/4, \infty)$, o mapa não possui pontos fixos atratores.*

*No entanto, $f_a$ tem um atrator de período dois para $a$ em $(3/4, 5/4)$. Em $a = 3/4$, os dois pontos nesta órbita se separam do ponto fixo $x = 1/2$. Para $a$ ligeiramente maior que $1/2$, um ponto na órbita é maior que $1/2$ e outro é menor que $1/2$. Essa bifurcação é chamada de bifurcação de período duplo. Dado que a derivada no ponto fixo (positivo) é negativa para valores de parâmetro próximos a $3/4$, as órbitas de pontos próximos ao ponto fixo oscilam de um lado para o outro em torno do ponto fixo. O ponto fixo, que se torna instável após a bifurcação, é chamado de repulsor de inversão, pois sua derivada é menor que -1. Um ponto fixo com derivada maior que 1 é chamado de repulsor regular.*

O Exemplo 2.39 é uma tentativa de compreensão dos pontos de bifurcação, investigando o que ocorre com as órbitas à medida que variamos o parâmetro $a$. Apesar de apresentar um exemplo que, à primeira vista, facilita o entendimento desses pontos, percebemos que o conceito é um tanto abstrato. Uma ferramenta que simplifica a investigação dos pontos de bifurcação é a análise gráfica, discutida na Seção 2.2.1. Ao realizar a análise gráfica dos mapas, podemos compreender o comportamento do ponto fixo em relação ao mapa, estudando suas iterações. No entanto, a verdadeira necessidade aqui é obter um panorama geral do sistema dinâmico. Para isso, é crucial observar o comportamento das órbitas à medida que variamos o parâmetro. Na próxima seção, introduziremos o diagrama de bifurcação para facilitar essa compreensão.

No contexto de mapas bidimensionais, torna-se necessário analisar a bifurcação por meio da matriz jacobiana, cuja definição será apresentada posteriormente. Para identificar os pontos de bifurcação, é fundamental que o módulo de pelo menos um autovalor seja igual a 1. Se um autovalor $\lambda$ assume o valor 1, caracterizamos um ponto de nó de sela; por outro lado, se pelo menos um autovalor $\lambda$ é igual a -1, temos um ponto de período duplo (ver [3]).

### 2.5.2 Diagrama de bifurcação

A teoria do Caos tem início com resultados importantes do trabalho do matemático francês Henri Poincaré [41]. Além disso, mesmo havendo uma linha tênue entre o caos e a ordem, por muito tempo acreditou-se que o caos representava outra face da ciência, ou seja, a ordem e o caos eram vistos como antagônicos. Em outras palavras, os sistemas caóticos pareciam ter uma descrição mais complexa, e as leis da natureza pareciam não funcionar para esse tipo de sistema. Mas o que chamou muita atenção é o fato de que a natureza não mostra dificuldade na transição da ordem para o caos. Esses tipos de sistemas podem ser estudados com o uso de mapas logísticos, sendo as iterações quadráticas uma ferramenta importante de estudo. Nesse contexto, obter uma visão abrangente do sistema torna-se crucial. Na seção anterior, exploramos a presença de pontos de bifurcação em sistemas dinâmicos, os quais desempenham um papel fundamental no estudo da dinâmica do sistema. Esses pontos emergem à medida que o parâmetro real aumenta, e nossa abordagem envolve a análise desses pontos ao variarmos os parâmetros e estudarmos as iterações da função. Contudo, observamos que essa abordagem pode ser bastante localizada. Em diversos momentos da seção anterior, referimo-nos a pontos na forma $(a, x)$. Utilizaremos esses pontos para obter uma visão abrangente do sistema dinâmico, construindo o diagrama de bifurcação. O objetivo é analisar as órbitas do sistema conforme realizamos variações nos parâmetros.

$$x_{n+1} = ax_n(1 - x_n) \tag{2.9}$$

Então, mesmo parecendo antagônicos, existe a transição ordem-caos ou caos-ordem, e esse fenômeno pode ser governado por uma lei simples. O percurso da transição é universal, isto é, as bifurcações podem ser encontradas em muitos sistemas naturais, tanto qualitativa quanto quantitativamente.

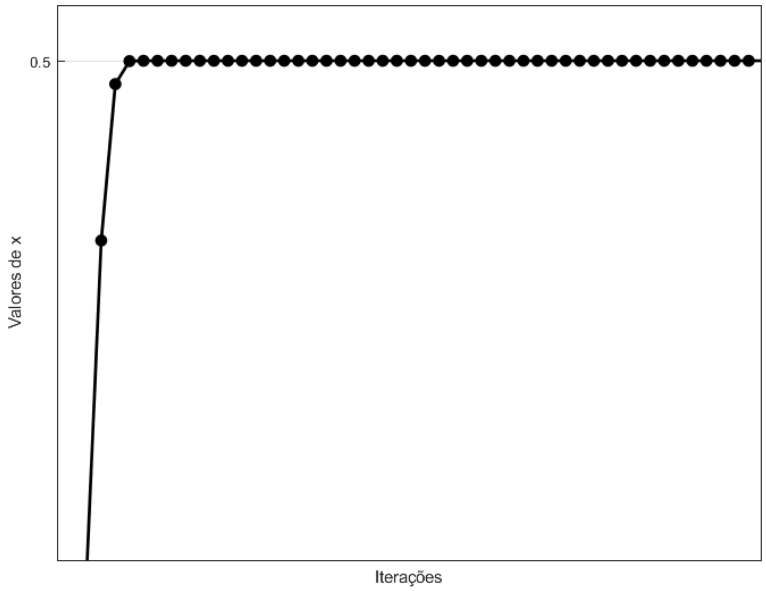



Figura 2.8: Iteração quadrática com parâmetro $a = 2$ e $x_0 = 0,1$ (Fonte: Autor)

Vamos analisar o que acontece com o iterador quadrático para o parâmetro $a$ entre 1 e 4. Em outras palavras, queremos entender o comportamento do iterador quadrático quando a escolha inicial $x_0$ tende a zero. Podemos começar nosso estudo fixando o valor

do parâmetro $a = 2$ e observar o que acontece com $x_n$ nesse caso. Podemos notar que se a escolha de $x_0$ está entre 0 e 1, a sequência converge para $0,5$ como mostra a Figura 2.8.

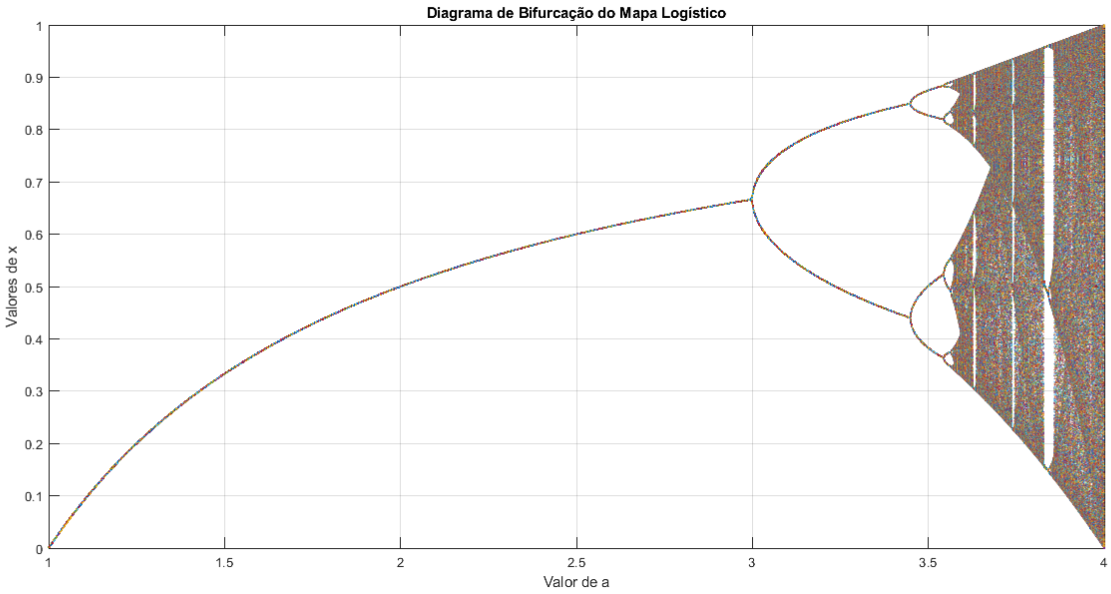



Figura 2.9: Diagrama de Bifurcação com $a \in [1, 4]$ (Fonte: Autor)

A Figura 2.9 mostra o mapa logístico para o parâmetro $a$ entre 1 e 4. Note que, para $a = 3$, a derivada $f'_a(p_a) = -1$, sendo assim, temos o primeiro ponto de bifurcação, além disso, quando $a > 3,55$ não temos mais um único ponto e sim uma coleção de pontos. Agora perceba que quando $a = 4$ temos uma estrutura caótica que será discutida com mais detalhes posteriormente.

O diagrama da Figura 2.9 frequentemente assemelha-se a uma árvore. Observe a curva de pontos que se estende de 1 a 3; essa curva lembra o tronco de uma árvore, visto que dela emergem duas ramificações, os primeiros galhos do diagrama. Cada um dos galhos origina dois novos galhos, que por sua vez geram mais dois galhos. Para $a > 3,55$, não observamos mais bifurcações, apenas uma coleção de pontos. No entanto, se examinarmos a faixa entre $3,55$ e 4 podemos notar pequenas manifestações de ramificações, de modo similar às copas das árvores, onde predominantemente vemos a folhagem, mas também há o aparecimento de alguns galhos. A árvore ramificada é o que representa as mudanças qualitativas no sistema no comportamento do iterador. Como mencionado anteriormente, a partir do tronco inicial, ocorre a primeira duplicação, resultando em duas ramificações adicionais. E, a partir de cada uma delas, emergem mais duas. Esse tipo de comportamento é denominado duplo período, ou simplesmente bifurcação. Observe que, onde vemos apenas um único ramo, o comportamento de longo prazo leva a um único ponto. Logo após, podemos observar a primeira bifurcação. Isso significa que o sistema agora oscila entre dois estados diferentes e alternados, um tipo de comportamento conhecido como periódico. Como nesse momento vemos duas ramificações dizemos que o período é dois, mas em um estágio posterior a ramificação passa de dois para quatro. Essa é uma característica fundamental da bifurcação, o período duplica para cada estado do sistema. Mais a direita da Figura 2.9 vemos uma cascata de pontos, isto é, temos um comportamento caótico.

### 2.5.3 Constantes de Feigenbaum

Como visto anteriormente, de modo geral, o diagrama de bifurcação é construído por meio da variação do parâmetro de controle $a$ versus a variável $x$. Nesse contexto, é possível analisar o comportamento das órbitas em função do parâmetro de controle. De acordo com o que já foi estabelecido, conforme variamos os valores do parâmetro $a$ novas ramificações emergem. Podemos notar que próximo de $a = 3,5$ acontece a segunda bifurcação e se prosseguirmos com a variação do parâmetro $a$ acontecerão novas bifurcações. Em síntese, para $a = 3$ teremos o primeiro ponto de bifurcação, chamaremos essa ramificação de ciclo-2 em seguida para a próxima ramificação teremos o ciclo-4 e assim sucessivamente surgindo novos ciclos 8, 16, 32, 64... com intervalos cada vez menores. Observe pela Figura 2.9, que existe um $a$ para o qual as ramificações convergem, dizemos que para esse valor de $a$ acontece um cascata de duplicação de duplo período.

Os estudos de Mitchell Feigenbaum foram cruciais para o entendimento de propriedades importantes do diagrama de bifurcação. Em seu artigo *Universal behavior in nonlinear system* [21] e *Quantitative Universality for a Class of Nonlinear Transformations* [20] Feigenbaum estudou a dinâmica das ramificações do diagrama de bifurcação. O estudo consistiu em variar o parâmetro de controle e investigar a razão da diferença dos valores nos quais acontecem as bifurcações. Os ciclos ocorrem com período $2^m$ desse modo podemos definir

$$\delta_m = \frac{a_{m-1} - a_{m-2}}{a_m - a_{m-1}},$$

onde $a_{m-1}, a_{m-2}, a_m$ e $a_{m-1}$ são os valores de parâmetro em que ocorre bifurcações. Se

| Período | $a_m$ | $a_m - a_{m-1}$ | $\delta$ |
|---|---|---|---|
| 2 | 3,0000 | - | - |
| 4 | 3,4494 | 0,4494 | - |
| 8 | 3,5441 | 0,0946 | 4,7514 |
| 16 | 3,5644 | 0,0203 | 4,6562 |
| 32 | 3,5687 | 0,0043 | 4,6683 |
| 64 | 3,5696 | 0,0009 | 4,6686 |
| 128 | 3,5698 | 0,0002 | 4,6692 |

Tabela 2.1: Pontos de bifurcação de duplo período e aproximação para $\delta_m$.

tomarmos o limite, para $m \to \infty$, obtemos

$$\lim_{m\to\infty} \delta_m = \frac{a_{m-1} - a_{m-2}}{a_m - a_{m-1}} = \delta = 4,6692...$$

podemos ver ainda pela Tabela 2.1, que

$$\lim_{m\to\infty} a_m = a_\infty = 3,56994$$

onde $a_\infty$ é o ponto em que a cascata de bifurcação de duplo período se acumula.

Veja, pela Figura 2.9 que quando o regime de bifurcação ocorre, se observarmos que o diagrama de bifurcação lembra um árvore podemos ver que em cada ponto onde as ramificações ocorrem, podemos compará-lo a forquilha de uma árvore. Tendo isso em vista, outra observação importante é que as sucessivas duplicações de período criam forquilhas com aberturas variáveis. Para prosseguir nessa investigação vamos determinar o ponto crítico do mapa logístico. Sabemos que $f'(x) = a - 2ax$, assim, segue que $a - 2ax_c = 0$

então $x_c = \frac{1}{2}$. Vamos definir o fator de estabilidade como $\Lambda = f'(x)$. Então, para os casos de órbitas de período $m$ podemos estudar sua estabilidade pela derivada da m-ésima iterada avaliada em qualquer um dos pontos do m-ciclo, por exemplo $x_0^*$. logo,

$$\lambda_m = \frac{d}{dx}(f^m(x_0^*))$$

pela regra da cadeia

$$\lambda_m = \frac{d}{dx}(f^m(x_0^*)) = \frac{d}{dx}(f(f^{m-1}(x_0^*))\frac{d}{dx}(f^{m-1}(x_0^*))$$

$$= \frac{d}{dx}(f(f^{m-1}(x_0^*))\frac{d}{dx}(f^{m-1}(f^{m-2}(x_0^*))\ldots\frac{d}{dx}(f^2(f(x_0^*))\frac{d}{dx}(f((x_0^*)).$$

Assim, obtemos que

$$\Lambda_m = \prod_{i=0}^{m-1} \Lambda(x_i^*), \tag{2.10}$$

para o caso em que $\Lambda_m = 0$ vamos dizer que a órbita é super-estável, sendo assim, note que $x_c$ é super-estável, pois $\lambda_m(x_c) = 0$.

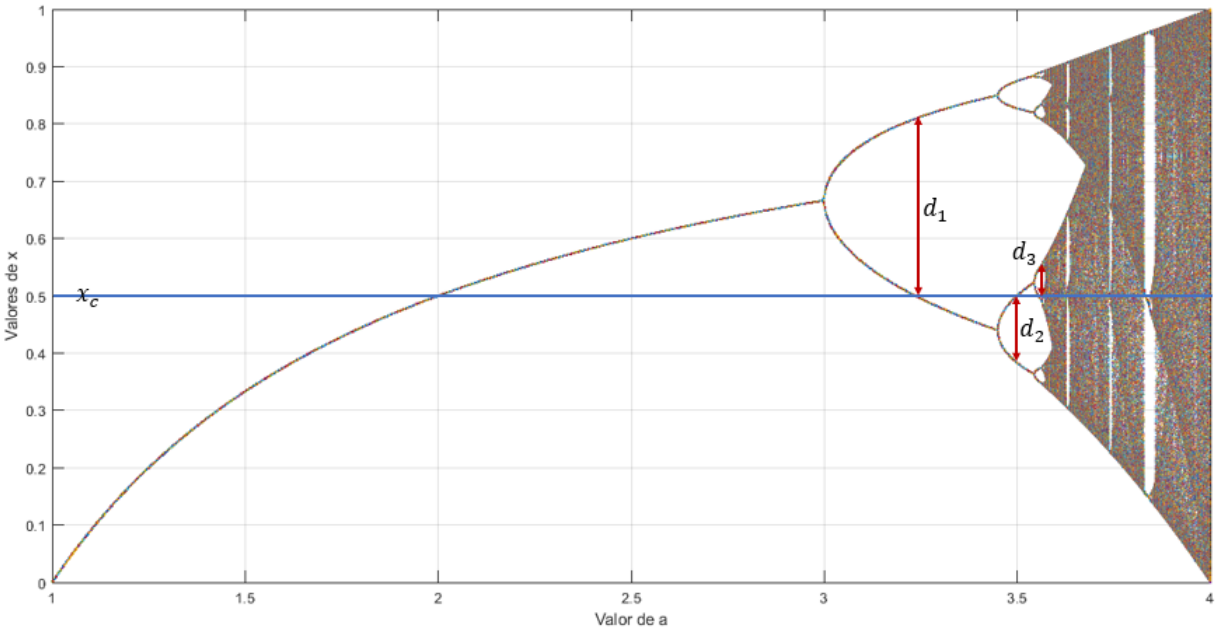



Figura 2.10: Digrama de bifurcação do mapa logistico com demonstração da abertura das forquilhas nos pontos de bifurcação(Fonte: Autor).

Vamos denotar por $r_m$ os valores de $a$ para os quais, existe uma órbita super-estável, de período $2^m$. Diante disso, a distância $d_m$ do ponto crítico ao ponto mais próximo dele configura a abertura da forquilha. Vale ressaltar, que para dois ciclos sucessivos $d_m$ muda de sinal. O processo de obtenção de $d_m$ pode ser visualizado pela Figura 2.10. Assim, podemos finalmente obter a chamada segunda constante de Feigenbaum definida pela razão entre $d_m$ e $d_{m-1}$, onde $d_{m-1}$ é a abertura da forquilha anterior. Denotamos essa constante por $\alpha_m$. logo,

$$\alpha_m = \frac{d_m}{d_{m-1}}.$$

Note que,

$$\lim_{m\to\infty} \alpha_m = -2,502907875\ldots.$$

As constantes de Feigenbaum indicam um limite para os quais as ramificações vão ocorrer. As ramificações não deixam de ocorrer conforme o parâmetro $a$ tende a $a_\infty$. Em vez disso, as ramificações ocorrem de modo que os pontos de bifurcação fiquem cada vez mais frequente. Chamamos essa etapa do diagrama de cascata de bifurcação de duplo período. Além disso, se escolhermos uma ramificação do diagrama e ampliarmos, observaremos uma geometria auto-semelhante, isso significa, que a nova estrutura obtida será muito parecida ou semelhante a estrutura anterior. Podemos ampliar a imagem quantas vezes se queira que a nova estrutura encontrada será semelhante a anterior. Essa é uma propriedade importante do diagrama de bifurcação, haja visto que, essa geometria é consequência direta das constantes de Fegenbaum.

## 2.6 Geometria Fractal

Diariamente, estamos naturalmente inclinados a utilizar conceitos geométricos que se alinham com a intuição e a realidade tangível que nos cerca. Nesse contexto, a geometria euclidiana se estabelece como uma ferramenta fundamental para descrever objetos que encontramos em nosso dia a dia, abordando situações mais comuns. Sua aplicação é extensiva, mesmo em objetos mais complexos, oferecendo uma descrição suficiente. Contudo, ao nos depararmos com uma classe específica de objetos geométricos, os fractais, a geometria euclidiana se mostra insuficiente. Os fractais, caracterizados por sua notável auto-semelhança em diferentes níveis de ampliação, desafiam as convenções da geometria tradicional. Cada parte mínima de um fractal reflete a forma do objeto como um todo, um fenômeno único que os diferencia de objetos não fractais. Enquanto ampliamos um fractal, sua forma original é revelada em cada etapa, contrastando com a descaracterização que ocorre em objetos convencionais. Um exemplo ilustrativo dessa propriedade pode ser percebido ao contemplarmos nosso planeta Terra. Devido à nossa escala em relação ao tamanho do planeta, podemos ter a ilusão de que estamos em um plano bidimensional. Em uma abordagem mais detalhada, um *zoom* suficientemente alto em uma curva pode criar a ilusão de linearizar localmente essa seção curva. No entanto, tal abordagem teria um efeito distorcido se aplicada a um círculo ou uma elipse, desconfigurando sua geometria. Por outro lado, os fractais mantêm sua integridade e forma original ao longo de ampliações sucessivas. Embora a geometria fractal possa parecer distante do entendimento cotidiano e frequentemente seja associada a abstrações matemáticas, ela está presente em fenômenos naturais e objetos do nosso dia a dia, tais como descargas elétricas, padrões de fumaça e formações de nuvens [1]. Além disso, a aplicabilidade dos fractais não se restringe a contextos específicos; ela também emerge em órbitas caóticas de sistemas dinâmicos, demonstrando a versatilidade e a presença impactante dessa geometria única em diferentes domínios.

Para compreender a auto-semelhança, consideremos um quadrado que dividiremos em quatro partes iguais. Ao escolher qualquer um dos quatro quadrados resultantes e ampliá-lo, veremos que ele se assemelha ao quadrado original, conforme ilustrado na Figura 2.11. Essa característica intrigante revela que, ao examinar uma parte menor de um objeto fractal, encontramos uma repetição da estrutura geral do objeto por completo. A propriedade de auto-semelhança é uma propriedade fundamental para a compreensão de fractal, no entanto, não podemos reduzir a definição de fractal a presença de auto-semelhança. Trata-se de uma característica dos fractais que pode ser estendido para objetos complexos da natureza.

Objetos naturais podem ser geralmente aproximados por fractais, em vista disso, é importante ressaltar, que não é possível encontrar qualquer objeto ou fenômeno natural que seja exatamente auto-semelhante. Em contraste, os fractais matemáticos são fractais

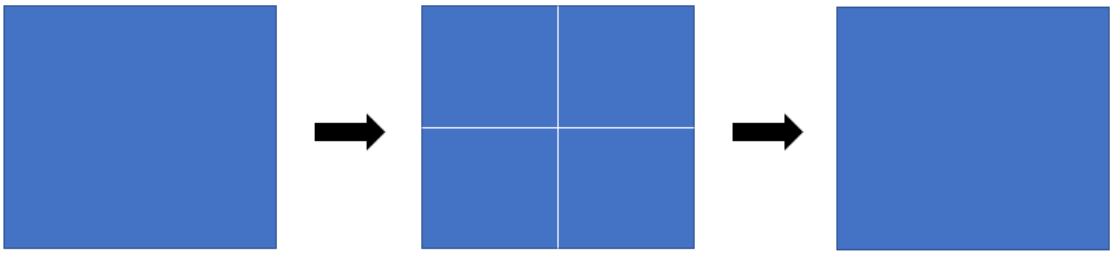


Figura 2.11: Exemplo de auto-similaridade (Fonte: Autor).

perfeitos, onde cada cópia menor é uma cópia exata do original. Se o padrão de um objeto ou processo dinâmico em grandes estruturas for obtido sob repetição de estrutura menor, então a semelhança exibida pelo objeto é chamada de auto-semelhança no espaço.

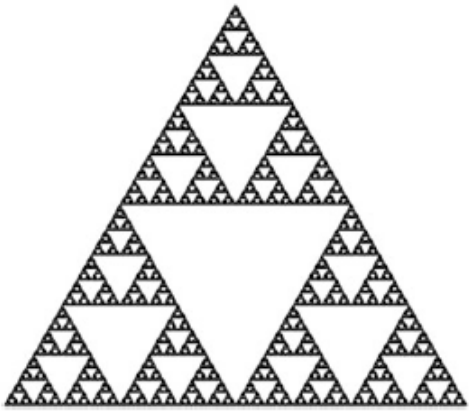


Figura 2.12: Triângulo de Sierpinski (Fonte: [1])

É claro que na natureza não encontraremos objetos que apresentem auto-semelhança perfeita; no entanto, podemos analisá-los como se fossem, tratando essa idealização como uma ferramenta conveniente para estudo, uma vez, que os objetos naturais podem ser aproximadamente considerados fractais. Nesta seção, abordaremos os fractais matemáticos, oferecendo uma visão mais aprofundada de sua construção.

Para ilustrar o processo, considere o triângulo apresentado na Figura 2.12. Iniciamos com um triângulo equilátero preenchido de lado unitário, chamado de $S_0$. Em seguida, dividimos o triângulo em quatro partes iguais, utilizando os pontos médios dos três vértices originais. Removemos o interior do triângulo central, gerando assim o estágio $S_1$. Repetimos esse processo em cada um dos três triângulos sólidos restantes, produzindo o estágio $S_2$.

Esse procedimento é continuamente repetido, gerando uma sequência de estágios $S_i$ que convergem para um objeto geométrico que exibe auto-semelhança em diferentes escalas. A Figura 2.13 ilustra a progressão desse processo de construção.

Na Figura 2.13, observamos que $S_1$ é composto por $N = 3$ , cada um com lado $\epsilon = 1/2$. Da mesma forma, $S_2$ é composto por $N = 3^2$ triângulos, cada um com lado $\epsilon = 1/2^2$. Prosseguindo com esses passos sucessivamente, chegamos a $S_n$ coberto por $N = 3^n$ triângulos equiláteros, cada um com lado $\epsilon = 1/2^n$. A área no enésimo estágio é dada por $3^n \frac{\sqrt{3}}{4} \left(\frac{1}{2}\right)^{2n} = \frac{\sqrt{3}}{4} \left(\frac{1}{2}\right)^n \to 0$ conforme $n \to \infty$. Esse resultado ilustra uma propriedade intrigante dos fractais, em que, apesar de sua complexidade visual aparente,

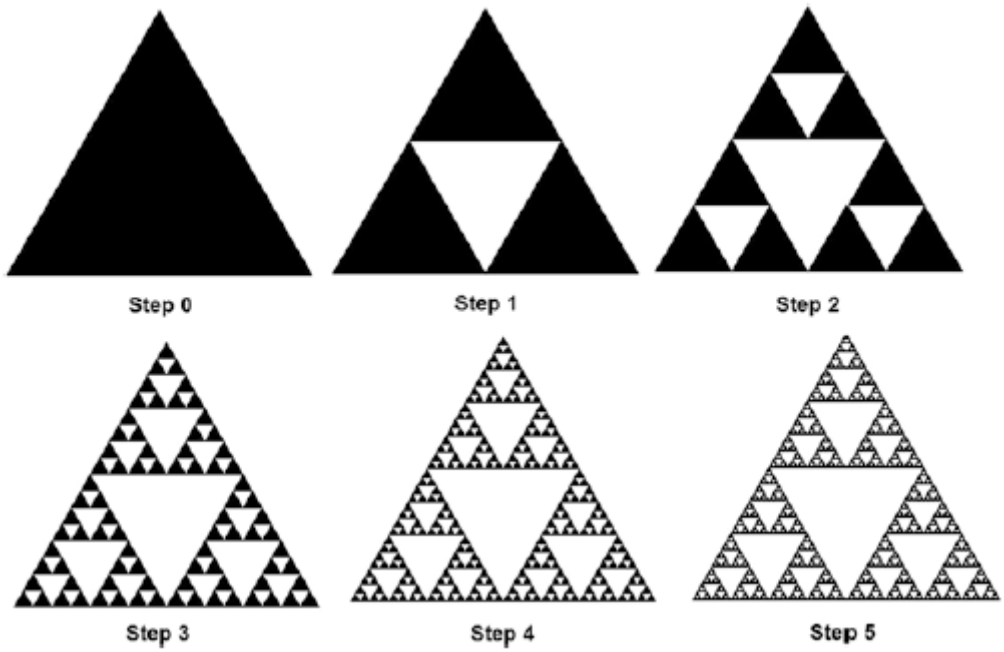



Figura 2.13: Processo de construção do triangulo de Sierpinski (Fonte: [1]).

a área total ocupada por esses objetos torna-se cada vez menor à medida que avançamos nos estágios de construção.

Esse tipo de auto-semelhança é conhecido como auto-semelhança exata, representando a forma mais robusta desse fenômeno em imagens fractais. O fractal do triângulo de Sierpinski, o conjunto de Cantor, a curva de von Koch, a ponta de samambaia, a esponja de Menger, entre outros, são exemplos que exibem a propriedade de auto-semelhança exata. Vale ressaltar que, embora a maioria dos objetos fractais seja auto-semelhante, a recíproca não é verdadeira; um objeto auto-semelhante não é necessariamente um fractal. Por exemplo, um quadrado sólido pode ser subdividido em quatro pequenos quadrados sólidos que se assemelham ao quadrado original, e cada um desses quadrados menores pode ser dividido em quatro quadrados sólidos ainda menores, mantendo a semelhança com o quadrado original, e assim por diante. Portanto, um quadrado é auto-similar, mas não é considerado um fractal. Trata-se de uma forma geométrica regular cujas propriedades são adequadamente descritas pela geometria euclidiana. Ademais, sua dimensão fractal coincide com sua dimensão topológica, e ele não apresenta outras características próprias de fractais.

É crucial identificar um fractal por meio da dimensão do objeto estudado. Um exemplo ilustrativo desse conceito é observado ao mensurarmos a extensão de uma linha costeira. Inicialmente, ao utilizar uma fotografia de satélite e ajustar para uma escala específica, obtemos um valor definido. No entanto, ao percorrermos a linha costeira a pé, utilizando cada passo como uma nova escala, o comprimento se amplia. Caso nossa intenção seja examinar detalhes minuciosos, como os contornos das rochas, podemos continuar esse processo indefinidamente, ajustando escalas cada vez menores e obtendo comprimentos progressivamente maiores. Vale notar que essa abordagem transcende as medidas espaciais, sendo passível de generalização para outras grandezas físicas.

Podemos estender essa ideia para diversas situações, como a determinação do peso de uma fruta. Inicialmente, utilizando uma balança comum de cozinha, obtemos um peso aproximado. No entanto, ao empregar uma balança analítica de laboratório, mais sensível, conseguimos uma medição mais precisa, inclusive considerando pequenas variações. Se

buscarmos uma precisão ainda maior, podemos usar uma balança de precisão subatômica, detectando variações de peso em uma escala ainda menor, contemplando partículas individuais. Essa abordagem, claramente, pode ser estendida para mensurar diversas grandezas com crescente precisão.

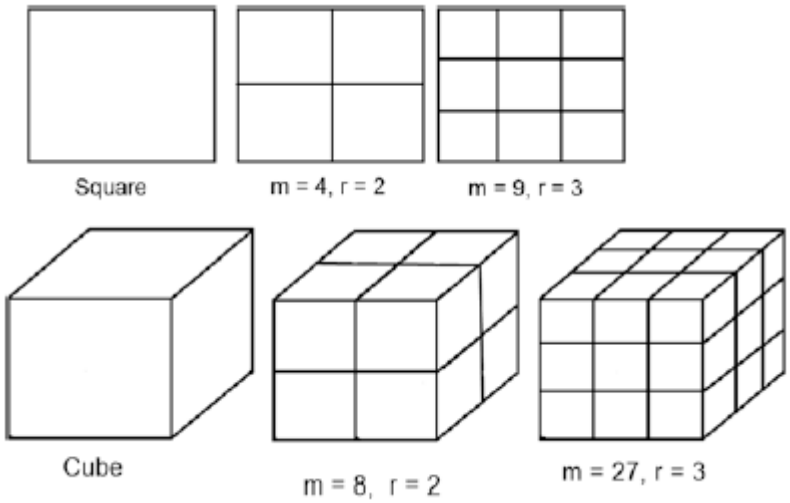



Figura 2.14: Número de cópias similares para o quadrado e cubo (Fonte: [29]).

$$N = \frac{1}{r^D}$$

Onde $D$ é a dimensão do objeto, então

$$N = \left(\frac{1}{r}\right)^D$$

Aplicando o logarítimo a ambos os lados, temos que:

$$D = \frac{\log N}{\log 1/r} \tag{2.11}$$

Então a dimensão $D$ de objetos auto-semelhantes, é dado pela equação 2.11. Anteriormente, vimos a construção do triângulo de Sierpinski. Então, vimos que $r = 1/2$ e $N = 3$, logo

$$D = \frac{\log 3}{\log 2} \approx 1,59.$$

Podemos estender esse conceito para outros objetos. Considere, por exemplo, o intervalo $[0, 1]$. Inicialmente, chamemos esse intervalo de $S_0$. Em cada iteração, dividimos o intervalo atual em três partes iguais e removemos o terço do meio. No primeiro passo, obtemos $S_1$ ao retirar o intervalo $\left(\frac{1}{3}, \frac{2}{3}\right)$. Portanto,

$$S_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right].$$

Esse processo é repetido infinitamente, gerando conjuntos $S_0, S_1, S_2, \ldots$, chamamos esse conjunto de conjunto de Cantor . A medida do conjunto de Cantor no $n$-ésimo estágio é proporcional a $\left(\frac{2}{3}\right)^n$, que se aproxima de zero à medida que $n$ tende ao infinito.

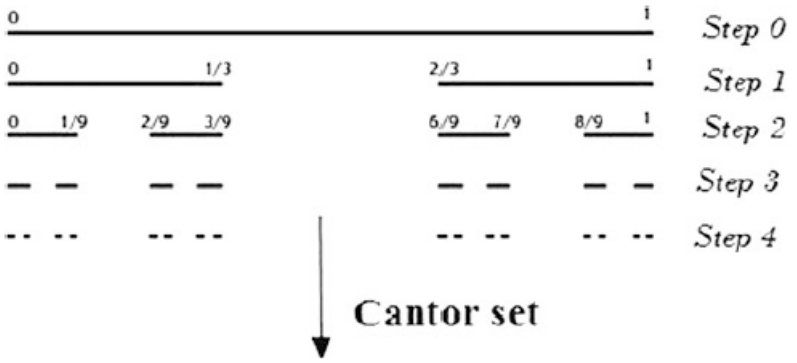



Figura 2.15: Representação do conjunto de Cantor (Fonte: [1])

Na construção do conjunto $C$ (conjunto de Cantor) sabemos que ele é composto de duas cópias de si mesmo e cada uma reduzida por um fator de 3, assim como dito anteriormente, o número de cópias a cada passo é 2 logo as sua dimensão é

$$D = \frac{\log 2}{\log 3} \approx 0,63.$$

O conjunto de Cantor exibe propriedades notáveis que o distinguem: a auto-semelhança e a dimensão fracionária. A auto-semelhança é evidenciada pelo processo iterativo de sua construção, onde a remoção sucessiva de intervalos resulta em subconjuntos que são semelhantes ao conjunto original. Quanto à dimensão, o conjunto de Cantor possui uma dimensão fracionária devido à sua estrutura fracional e ao padrão de remoção de intervalos.

Um outro exemplo importante que podemos citar aqui é a curva de Koch também conhecido como "floco de neve". Sabemos que a tangente num vértice de uma curva é indefinido. A curva de Koch é feita de cantos em todos os lugares, portanto não é possível traçar tangente em nenhum de seus pontos, portanto, em nenhum lugar é diferenciável. Esta curva pode ser construída geometricamente por iterações sucessivas como segue.

Vamos começar com um segmento de reta $S_0$ de comprimento $L_0$. Para gerar $S_1$ dividimos o segmento de reta em três partes iguais. Em seguida substituímos o seguimento do meio por um triângulo equilátero, assim completando o primeiro passo e gerando $S_1$, dessa forma obtemos uma curva de quatro segmentos de comprimento $l = L_0/3$. Dessa forma podemos gerar a curva com um processo sucessivo de divisões $l = L_0/3^n$. Assim, no e-nésimo estágio o número de cópias de segmentos de reta $N = 4^n$.

A curva de von Koch é um fractal auto-semelhança, composta por quatro peças idênticas, cada uma delas semelhante à curva original, reduzida por um fator de 3 a cada etapa de sua construção. Isso resulta em um número total de cópias igual a $N = 4$. A partir dessas características, podemos determinar sua dimensão fractal, $D$.

$$D = \frac{\log 4}{\log 3} \approx 1,26.$$

## 2.7 Atrator estranho

**Definição 2.40** (Conjunto invariante)**.** *Seja $f : X \to X$ um mapa. Um conjunto $A \subseteq X$ é dito ser invariante sob o mapa $f$ se para qualquer $x \in A$, $f^n(x) \in A$ para todo $n$. Especificamente, o conjunto $A$ é invariante se $f(A) = A$. Seja $(X, f)$ um sistema dinâmico discreto. um subconjunto $A$ de $X$ é dito positivamente invariante se $f(A) \subset A$. Se*

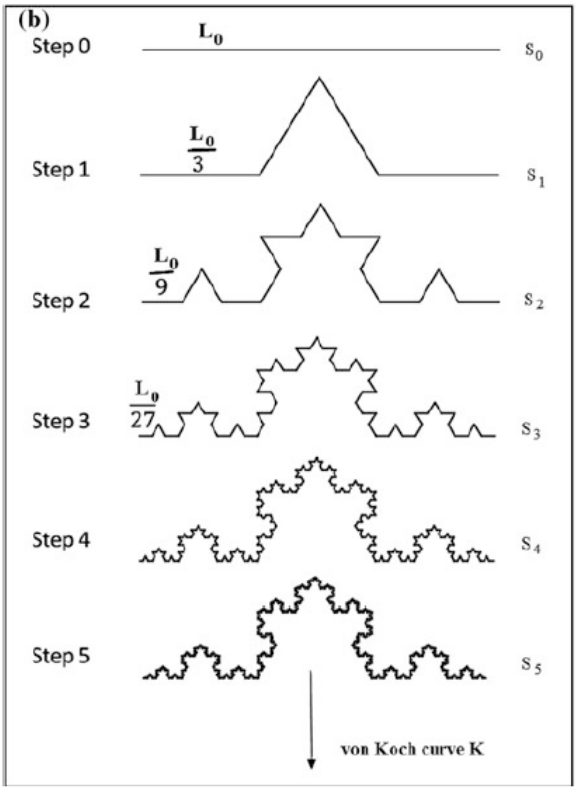



Figura 2.16: Representação da curva de Koch (Fonte: [41])

*$f(A) = A$, então $A$ é estritamente invariante. O conjunto de pontos periódicos do mapa é sempre invariante.*

Considere um conjunto fechado invariante $A \subset X$ sob a ação de $f : X \to X$. O conjunto $A$ é denominado conjunto caótico ou atrator em relação a $f$ se, e somente se, demonstrar ser sensivelmente dependente das condições iniciais, topologicamente transitivo, e se o conjunto de todos os pontos periódicos for denso em $A$. Vale ressaltar que $A$ é repulsor se, e somente se, não for um atrator [1].

Em outras palavras, um sistema dinâmico tem um atrator se houver um subconjunto adequado $\mathcal{M}$ no espaço de fase euclidiano $\mathbb{R}^E$, tal que, para quase todos os estados iniciais e ao longo do tempo infinito $t$, a órbita permanece próxima a algum ponto de $\mathcal{M}$.

Um atrator estranho é descrito como o produto local de uma variedade bidimensional por um conjunto de Cantor. No interior desse conjunto, as trajetórias de um sistema dinâmico movem-se de maneira errática e são altamente sensíveis às condições iniciais. Os atratores de sistemas simples, como o representado pelo mapa logístico $x_{n+1} = rx_n(1-x_n)$ para $r$ real e $x \in [0, 1]$, são considerados estranhos, destacando-se como características de sistemas complexos e realistas.

Esses padrões, conhecidos como atratores estranhos, delineiam o estado final de sistemas dissipativos extremamente complexos e caóticos. A geometria do conjunto de atratores estranhos é notavelmente peculiar, assemelhando-se a uma superfície complexa infinita que não pode ser representada na geometria euclidiana com dimensões inteiras. Importante notar que o caos e os fractais emergem simultaneamente nos pontos dos atratores estranhos. Geometricamente, os atratores estranhos são fractais e, dinamicamente, são caóticos. São gerados pela iteração de um mapa ou pela solução de um sistema de equações diferenciais de valores iniciais que exibem comportamento caótico.

Atualmente, os cientistas acreditam que atratores estranhos podem colaborar em problemas complexos e não resolvidos, como o clima da Terra, a atividade cerebral humana

e fenômenos de turbulência. Atratores estranhos, caracterizados por dimensões fractais predominantemente maiores que suas dimensões topológicas, consolidam-se como ferramentas fundamentais na compreensão de sistemas dinâmicos complexos.

Capítulo

# 3

# A Construção do Modelo

## 3.1 Sistemas dinâmicos bidimensionais

Como mencionado anteriormente, a teoria de sistemas dinâmicos abrange diversas áreas, sendo os sistemas físicos uma parcela específica na qual essa teoria pode ser aplicada para análise. Podemos compreender a dinâmica de uma particula ao longo do tempo ao estudar como sua posição varia. As equações de Newton nos elucidam que o movimento de uma particula é ocasionado pela força de interação que este objeto experimenta. Assim, ao considerarmos a mecânica celeste, a lei que governa um determinado sistema é a Lei Universal da Gravitação proposta por Newton:

$$F = G\frac{Mm}{r^2}, \tag{3.1}$$

onde $r$ representa o módulo do vetor posição $\mathbf{r} = (x, y, z)$. A partir da equação 3.1, surgem outras seis equações. Para cada coordenada de posição, há uma equação correspondente que descreve a variação dessa coordenada com o tempo. Similarmente, existirá uma equação para cada coordenada da velocidade, descrevendo sua variação ao longo do tempo. As equações mencionadas anteriormente são derivadas das soluções de equações diferenciais que decorrem das leis fundamentais de Newton para um sistema físico específico. Por exemplo, ao considerarmos a órbita de um satélite ao redor da Terra ou a interação gravitacional entre a Terra e a Lua, aplicamos as leis de Newton para compreender o movimento desses corpos celestes.

Ao resolver as equações de Newton para esses sistemas, obtemos um conjunto de equações em função do tempo que descreve a evolução do sistema. Com isso somos capazes de obter informações do sistema como a posição dos elementos que o compõem assim como a aceleração e a velocidade. Essas equações diferenciais, quando resolvidas, oferecem informações importantes sobre a dinâmica dos corpos do sistema, permitindo a previsão do seu comportamento futuro.

A adição de um terceiro corpo com massa considerável torna o sistema substancialmente mais complexo. Agora, além de considerar as interações entre esses corpos, precisamos lidar com um conjunto expandido de equações. Para cada corpo, são necessárias seis equações resultando em dezoito equações no total interdependentes umas das outras. Esse é o conhecido problema dos três corpos [38]. As soluções para algumas configurações específicas são conhecidas, como no caso em que as três massas estão alinhadas com o centro de massa do sistema, como descrito por Euler [38]. No entanto, na maioria das situações, o problema dos três corpos desafia a obtenção de soluções analíticas diretas.

Há uma abordagem bastante elegante proposta por Poincaré para lidar com esse problema. Em vez de estudar as trajetórias geradas pelas soluções das equações diferenciais, Poincaré examina os pontos nos quais as trajetórias atravessam um plano $S$. Dessa forma, para obter informações mais abrangentes sobre o sistema, permitimos que as trajetórias cruzem o plano *n-vezes* resultando em $n$ pontos nos quais esse processo ocorre. Se $\mathbf{A}$ é o ponto no qual a trajetória atravessa o plano pela *n-ésima* vez então $\mathbf{B}$ é o ponto no qual a trajetória atravessa o plano pela *(n+1)-ésima* vez. Sendo assim, podemos observar que os pontos são obtidos em intervalos discretos de tempo. Desta forma se $\mathbf{X}_n \in S$ então podemos obter o próximo ponto da seguinte forma:

$$X_{n+1} = P(X_n). \tag{3.2}$$

Assim, se $p$ é um ponto fixo de $P$ então a trajetória perfura o plano $S$ no mesmo ponto. Além disso, observando o comportamento de $P$ perto deste ponto fixo, podemos determinar a estabilidade da órbita fechada. Assim, o mapa de Poincaré converte problemas sobre órbitas fechadas (que são difíceis) em problemas sobre pontos fixos de um mapeamento (que são mais fáceis em princípio, embora nem sempre na prática) [49].

**Exemplo 3.1.** *Considere um vetor dado em coordenadas polares por* $\frac{dr}{dt} = r(1-r^2)$, $\frac{d\theta}{dt} = 1$. *Seja* $S$ *o eixo* $x$ *positivo que calcula o mapa de Poincaré. Vamos mostrar que o sistema tem uma única órbita periódica e classificaremos sua estabilidade. Primeiro vamos encontrar uma expressão para* $P$. *Então considere* $r_0$ *uma condição inicial em* $S$. *Assim segue que o primeiro retorno em* $S$ *acontece em* $t = 2\pi$. *Logo,* $r_1 = P(r_0)$ *quando,* $r_1$ *satisfaz*

$$\int_{r_0}^{r_1} \frac{dr}{r(1-r^2)} = \int_0^{2\pi} dt = 2\pi.$$

*Sendo assim, obtemos que* $r_1 = \left[1 + e^{-4\pi}(r_0^{-2} - 1)\right]^{-1/2}$. *Então* $P(r) = \left[1 + e^{-4\pi}(r^{-2} - 1)\right]^{-1/2}$

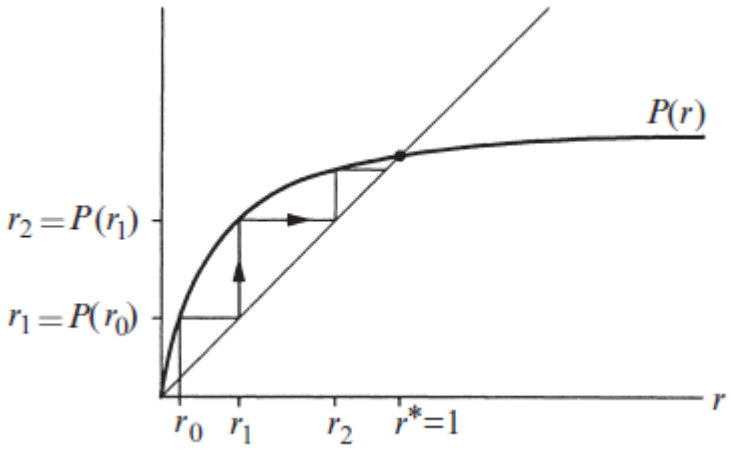



Figura 3.1: Gráfico de $P$ (Fonte: [49])

*Vamos fazer a análise gráfica para investigar as itrações do mapa* $P$. *Analisando o gráfico da Figura 3.1, note que, as iterações convergem para o único ponto fixo estável* $r^* = 1$.

Muitas vezes, a técnica das seções de Poincaré é utilizada para simplificar problemas, reduzindo sua dimensionalidade. Como mencionado anteriormente, as seções de Poincaré foram propostas para realizar uma análise que pudesse fornecer informações gerais sobre o problema dos três corpos. Como a mecânica celeste clássica ocorre no espaço tridimensional, o mapa de Poincaré resultará em duas dimensões.

Nos anos 60, Stephen Smale se interessou em estudar as ideias de Poincaré, tendo contribuído para teoria dos sistemas dinâmicos. Em seus primeiros estudos nessa área Smale chegou a cogitar a inexistência de caos [22]. Entretanto, a continuidade dos seus estudos o levou a desconsiderar a sua ideia inicial, diante disso, Smale propôs o mapa em ferradura também conhecido como ferradura de Smale. Trata-se de uma transformação topológica que fornece base para o entendimento de sistemas caótico.

O mapa em questão, consiste em um quadrado que é esticado até que forme um retângulo longo e fino, em seguida é dobrado em forma de ferradura e sobreposto no quadrado inicial. Cada iteração adiciona uma curva e dobra as existentes. Se escolhermos dois pontos no início do processo, dado o número suficiente de iterações os pontos estarão arbitrariamente afastados, em virtude, do esticamento e dobramento. O mapa em ferradura proposto por Smale apresentou a propriedade de dependência sensível das condições iniciais que Lorenz observou mais tarde em se eu estudo do clima. Para mais informações ver o Teorema 4.2 em [46].

O mapa de Poincaré e a Ferradura de Smale são apenas alguns exemplos dentre uma diversidade de mapas bidimensionais que podem ser utilizados. Em geral, existem os mapas lineares e os mapas não lineares. Um mapa linear em $\mathbb{R}^2$ pode ser representado da seguinte forma:

$$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{11}x + a_{12}y \\ a_{21}x + a_{22}y \end{pmatrix}$$

**Definição 3.2.** *Um mapa* $A(v)\ \mathbb{R}^m \longrightarrow \mathbb{R}^m$ *é linear, se para todo* $a, b \in \mathbb{R}$ *e* $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^m$, $A(a\boldsymbol{v} + b\boldsymbol{w}) = aA(\boldsymbol{v}) + bA(\boldsymbol{w})$.

Note que um mapa linear pode ser denotado por $f(x) = ax$. Deste modo, todos os mapas lineares tem um ponto fixo na origem [3]. Considere a matriz $A$ como sendo a matriz dos coeficientes do mapa, então

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Dizemos que $\lambda$ é o autovalor de $A$ se $A(\mathbf{v}) = \lambda\mathbf{v}$, então $\mathbf{v}$ é um autovetor de $A$. Sendo assim, se $\mathbf{v}_0$ é um autovetor de $A$ podemos escrever

$$\mathbf{v}_{n+1} = A\mathbf{v}_n. \tag{3.3}$$

Assim, segue que

$$\begin{aligned} \mathbf{v}_1 &= A(\mathbf{v}_0) = \lambda\mathbf{v}_0 \\ \mathbf{v}_2 &= A(\mathbf{v}_1) = \lambda\mathbf{v}_1 = \lambda A(\mathbf{v}_0) = \lambda^2\mathbf{v}_0 \\ &\vdots \\ \mathbf{v}_n &= \lambda^n\mathbf{v}_0. \end{aligned}$$

A compreensão dos mapas bidimensionais, é essencial para se estudar a dinâmica de diversos fenômenos. No contexto dos mapas lineares em $\mathbb{R}^2$, a representação matricial e a noção de autovalores e autovetores fornecem uma visão fundamental.

Ao analisarmos um mapa linear representado pela matriz $A$, observamos que os autovetores desempenham um papel crucial, representando direções especiais que permanecem inalteradas pela aplicação do mapa. A relação entre os autovetores e os autovalores, expressa por $\mathbf{v}^n = \lambda^n \mathbf{v}_0$, demonstra a influência desses valores próprios na evolução das transformações lineares ao longo do tempo.

Podemos estudar um mapa bidimensional linear pela matriz $A$, note que, os autovetores desempenham um papel importante no estudo da dinâmica do mapa, uma vez que, eles representam direções inalteradas pela aplicação do mapa. Os autovalores por sua vez, representa a contração ou a dilatação dos autovetores. Assim, a relação entre os autovetores e autovalores expressa por $\mathbf{v}^n = \lambda^n \mathbf{v}_0$ é um ferramental de extrema importância para o estudo de propriedades fundamentais de mapas lineares, sendo central, para compreender a dinâmica de longo prazo e analisar a estabilidade do sistema dinâmico.

## 3.2 Matriz Jacobiana

Nas seções anteriores, nosso estudo estava centrado na análise dos pontos de estabilidade dos mapas, tendo como objetivo a compreensão da dinâmica ao longo do maior intervalo de tempo possível. Pelo Teorema 2.10, podemos investigar a dinâmica de um mapa unidimensional por meio da análise de sua derivada no ponto fixo. Dessa forma, podemos classificar os pontos fixos com base na dinâmica do seu comportamento. Nesta seção, buscaremos estender a generalização do Teorema 2.10 para o estudo de mapas bidimensionais. Estendendo esse resultado para mapas bidimensionais seremos capazes de fazer a mesma análise para esses mapas nos fornecendo um ferramental para a compreensão mais abrangente do mapa.

**Definição 3.3.** *Seja $F = (f_1, ..., f_m)$ um mapa sobre $\mathbb{R}^m$ e seja $p \in \mathbb{R}^m$. A matriz Jacobiana de $f$ no ponto $p$ denotado por $JF(p)$ é dado por*

$$JF(p) = \begin{pmatrix} \dfrac{\partial f_1}{\partial x_1}(p) & \cdots & \dfrac{\partial f_1}{\partial x_m}(p) \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_m}{\partial x_1}(p) & \cdots & \dfrac{\partial f_m}{\partial x_m}(p) \end{pmatrix}.$$

**Exemplo 3.4.** *A função $F : \mathbb{R}^2 \to \mathbb{R}^2$ definida por $F = ((x+y)^2, xy^2 + x^2y)$ tem uma derivada representada pela matriz jacobiana*

$$JF(x, y) = \begin{pmatrix} 2x + 2y & 2x + 2y \\ y^2 + 2xy & x^2 + 2xy \end{pmatrix},$$

*pois, por definição, os elementos da matriz jacobiana são dados pelas derivadas parciais de $F(x, y)$.*

O jacobiano de uma função multivariada é uma generalização do conceito de derivada para várias variáveis. Em particular, o jacobiano representa a matriz das derivadas parciais de uma função vetorial. Cada elemento da matriz jacobiana é uma derivada parcial que indica como a respectiva componente da função de saída varia em relação a cada uma das variáveis de entrada. Os autovetores da matriz $J$ representam as direções especiais ao redor do ponto $p$. Nesse sentido, podemos fazer uma generalização do Teorema 2.10 para o $\mathbb{R}^m$, e assim, podemos afirmar que se $\mid \lambda \mid < 1$ então $p$ é um poço e se $\mid \lambda \mid > 1$ então $p$ é uma fonte. O leitor interessado poderá aprofundar a análise desse resultado junto com a sua demonstração em [3, 16, 19].

Os mapas também podem apresentar pontos nos quais em algumas direções esse ponto é atrator e repulsor em outras direções.

**Definição 3.5.** *Seja $F$ um mapa sobre $\mathbb{R}^m$, para $m \geq 1$ então o ponto fixo $p$ é chamado de hiperbólico se todos autovalores tem magnitude diferente de 1. Se $p$ é hiperbólico e se pelo menos um autovalor de $JF(p)$ tem módulo menor que 1 e pelo menos um autovalor maior que 1 então $p$ é chamado de ponto de sela.*

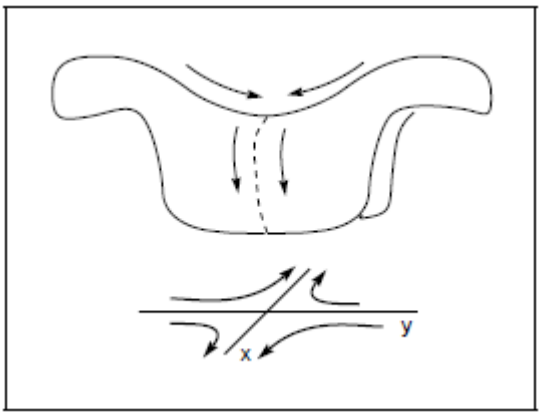



Figura 3.2: Exemplo geral do ponto de sela (Fonte: [3]).

Podemos observar, pela Figura 3.2, que o termo "ponto de sela" é bastante ilustrativo. Isso se deve à representação tridimensional da superfície, que se assemelha à forma de uma sela de cavalo. Em um contexto bidimensional, ao projetar essa superfície em um plano, notamos a presença de hipérboles cujas assíntotas coincidem com os eixos $x$ e $y$. É importante ressaltar que isso não é uma regra universal; as assíntotas podem se manifestar como outras formas de retas no plano. Ao seguir as trajetórias das curvas, é possível perceber que os vetores posicionados ao longo das assíntotas são atraídos em direção a um ponto fixo, enquanto na direção oposta são repelidos. Em contextos de sistemas dinâmicos bidimensionais, essa característica evidencia claramente a presença de um ponto de sela.

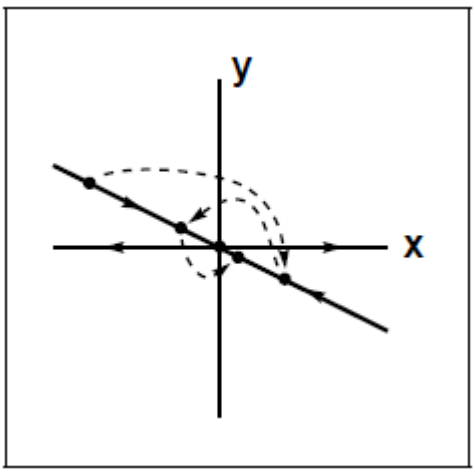



Figura 3.3: Ilustração do ponto de sela tipo *flip* sela (Fonte: [3]).

Os pontos de sela, em geral, são instáveis, visto que a maioria dos pontos iniciais ao redor desses pontos se afasta. No entanto, existe um conjunto específico de pontos que são

atraídos em direção ao ponto de sela. Chamamos esse conjunto de pontos de variedade estável, como discutido em [3]. Em termos simples uma variedade é conjunto localmente euclidiano (ver [30]).

**Exemplo 3.6.** *Seja* $f = (2x + 5y, -\frac{1}{2}y)$. *Os autovalores de* $f$ *são* $2$ *e* $-\frac{1}{2}$ *correspondentes aos autovetores* $(1, 0)$ *e* $(2, -1)$. *Os pontos em uma linha na direção do vetor* $(2, -1)$ *sofrem uma transformação* $\boldsymbol{v} \to -0.5\boldsymbol{v}$ *a cada iteração da função* $f$. *Como resultado, imagens sucessivas mudam de um lado da origem para o outro ao longo da linha. Esse comportamento de inversão das órbitas em torno do ponto fixo é mostrado na Figura 3.3. Isso é característica de todos os pontos fixos para os quais o Jacobiano tem autovalores negativos, mesmo quando o mapa é não linear. Uma sela com pelo menos um autovalor negativo às vezes é chamado de sela flip. Caso contrário, é uma sela regular.*

## 3.3 Contração de Área

Descrever bifurcações sela-nó e de duplicação de período para famílias arbitrárias de mapas bidimensionais é uma tarefa complexa, pois pontos fixos e periódicos podem envolver tanto direções de contração quanto de expansão. A propriedade de ter um autovalor com valor absoluto menor que 1 em todos os pontos (ou, de forma análoga, um autovalor com valor absoluto maior que 1 em todos os pontos) é característica de uma classe ampla e significativa de mapas. Para tais mapas, os tipos de bifurcações possíveis são limitados aos observados em mapas unidimensionais. A contração de área é uma propriedade fundamental em sistemas dinâmicos, desempenhando um papel crucial na compreensão do comportamento local e global desses sistemas. Ela está intrinsecamente ligada à estabilidade dos pontos fixos e órbitas periódicas em um espaço de estados. A principal ideia por trás da contração de área é que, em regiões próximas a um ponto fixo ou periódico, as trajetórias do sistema tendem a ser "espremidas"ou "contraídas". Uma maneira de formalizar essa propriedade é através do conceito de matriz Jacobiana, que fornece informações sobre a taxa de variação local do sistema[3]. Em particular, o determinante da matriz Jacobiana é um elemento central ao indicar a mudança na área em torno de um ponto. Se o determinante for menor que 1 em todas as regiões do espaço de estados, então o sistema exibe contração de área local.

**Definição 3.7.** *Seja* $F$ *um mapa suave de* $\mathbb{R}^2$ *e seja* $JF(x)$ *a matriz jacobiana de* $F$ *com respeito a um ponto* $x \in \mathbb{R}^2$. *Dizemos´que* $F$ *é uma contração de área se* $|det(JF(x))| < 1$ *para todo* $x \in \mathbb{R}^2$. *O mapa* $F$ *preserva área se* $|det(Jf(x))| = 1$ *para todo* $x \in \mathbb{R}^2$.

Por [3] $|det(Jf(x))|$ determina a mudança na área efetuada pelo mapa $F$ perto do ponto $x$. De fato, se $S$ é uma região em $\mathbb{R}^2$, então

$$A(F(S)) = \iint_S |det(JF(x))|dx.$$

A compreensão da contração de área é essencial ao explorar a estabilidade, bifurcações e comportamentos de longo prazo em sistemas dinâmicos. Ela oferece conhecimentos valiosos sobre como as perturbações locais se propagam no sistema e como as regiões atratoras são formadas. Nesse contexto, o estudo da contração de área é uma ferramenta essencial para analisar a dinâmica complexa que pode surgir em uma variedade de sistemas.

## 3.4 Conjunto de medida nula

Seja $X$ não vazio, queremos definir uma família de subconjuntos, onde a família é fechada segundo o complemento e uniões enumeráveis.

**Definição 3.8.** *Uma família $A_X$ de subconjuntos de $X$ é uma $\sigma$-álgebra se*

1. *$A \in A_X$, então $A^c \in A_X$;*
2. *$\{A_n\}_{n\in\mathbb{N}}$, é uma sequência em $A_X$, então $\cup_{n\in\mathbb{N}} A_n \in A_x$.*

*O par $(X, A_X)$ é chamado de espaço mensurável os elementos da família de $A_X$, é chamado de conjunto mensurável.*

**Definição 3.9.** *Seja $(X, A_x)$ um espaço mensurável. Uma medida em $(X, A_X)$ é uma função $\mu \to [0, +\infty]$, tal que:*

1. *$\mu(\emptyset) = 0$;*
2. *Se $A_{nn\in\mathbb{N}}$ é um sequência em $A_x$, cujos elementos são dois a dois disjuntos então*

$$\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty}(A_n).$$

*Se $\mu$ é uma medida em $(A, A_X)$, então $(X, A_X, \mu_X)$ é um subconjunto mensurável $Z \subset A_X$, dizemos que $X$ é um conjunto de medida.*

**Definição 3.10.** *Dado um espaço de medida $(X, A_X, \mu)$ e um sub conjunto mensurável $Z \subset A_X$, dizemos que $Z$ é um conjunto de medida nula quando*

$$\mu(Z) = 0.$$

## 3.5 Construindo o mapa de Hénon

Considere uma região limitada $R$, na qual toda trajetória que seja solução de um sistema de equações diferenciais fica presa nessa região. Essa região será atratora se todas as trajetórias tendem a um conjunto de **medida nula** [26].

Vamos considerar $(M, B, \mu)$ um espaço de medida, e seja $f : M \to M$ uma transformação mensurável. Dizemos que a medida $\mu$ é invariante por $f$ se

$$\mu(E) = \mu(f^{-1}(E)), \tag{3.4}$$

para todo conjunto mensurável $E \subset M$. Nesse caso dizemos que $f$ preserva $\mu$. Note que, a expressão 3.4 faz sentido, haja visto, que a pré-imagem de um conjunto mensurável por uma transformação mensurável ainda é um conjunto mensurável. Isso significa que a probabilidade de um ponto estar num dado conjunto é igual à probabilidade de que sua imagem esteja nesse conjunto.

**Teorema 3.11** (Recorrência de Poincaré)**.** *Seja $f : M \to M$ uma transformação mensurável e seja $\mu$ uma medida finita invariante por $f$. Seja, $E \subset M$ qualquer conjunto mensurável com $M(E) > 0$. Então, para $\mu$-quase todo ponto $x \in E$ existem infinitos valores de $n$ para os quais $f^n(x)$ também está em $E$.*

*Demonstração.* Representamos por $E_0$ o conjunto dos pontos $x \in E$ que nunca regressam a E. Inicialmente, vamos provar que $E_0$ tem medida nula. Para isso começamos por observar que suas pré-imagens $f^{-n}(E_0)$ são disjuntas duas-a-duas. De fato, suponhamos que existem $m > n \geq 1$ tais que $f^{-}m(E_0)$ intersecta $f^{-n}(E_0)$. Seja $x$ um ponto de intersecção e seja $y = f^n(x)$. Então $y \in E_0$ e $f^{m-n}(y) = f^m(x) \in E_0$ que está contido em $E$ isto quer dizer que $y$ volta pelo menos uma vez a $E$ o que são disjuntas duas-a-duas, como afirmamos.

Observando que $\mu(f^{-n}(E_0)) = \mu(E_0)$ para todo $n \geq 1$ porque $\mu$ é invariante, concluimos que

$$\mu\left(\bigcup_{n=1}^{\infty} f^{-n}(E_0)\right) = \sum_{n=1}^{\infty} \mu(f^{-n}(E_0)) = \sum_{n=1}^{\infty}(E_0).$$

como supomos que a medida é infinita, a expressão do lado esquerdo é finito. Por outro lado, à direita temos uma soma de inifinitos termos, todos iguais. O único jeito dessa soma ser finita é que as parcelas sejam nulas. Portanto devemos ter $\mu(E_0)$ como foi afirmado.

Agora denotamos $F$ o conjunto de pontos $x \in E$ que regressam um número finito de vezes. Assim temos que para todo ponto $X \in F$ algum iterado $f^k(x)$ em $E_0$. Ou seja,

$$F \subset \bigcup_{k=0}^{\infty} f^{k=-1}(E_0)$$

Como $\mu(E_0)$=0 e $\mu$ é invariante, temos:

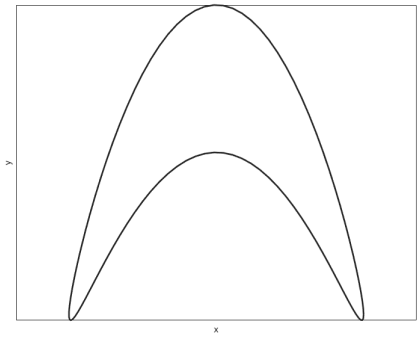
$$\mu(F) \leq \mu\left(\bigcup_{k=0}^{\infty} f^{-k}(E_0)\right) \leq \sum_{k=0}^{\infty} \mu(f^{-k}(E_0)) = \sum_{k=0}^{\infty} \mu(E_0) = 0.$$

Portanto, $\mu(F) = 0$ como queriamos provar. □

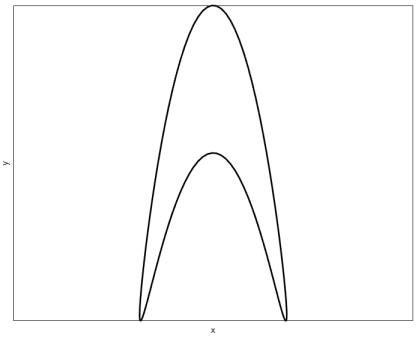
Em termos simples, o teorema de recorrência implica que a dinâmica de um sistema fechado retorna com certa proximidade ao estado inicial do mesmo. Esse resultado também pode ser estendido para sistemas de tempo continuo [39]. Oliveira e Viana (2014), mostram outras versões desse teorema, uma vez que esse resultado expressos de outras formas traz outras implicações interessantes que não abordaremos nesse trabalho (ver [39]).

A afirmação de que uma região atrai quando as trajetórias tendem a um conjunto de medida nula é uma implicação do teorema da recorrência de Poincaré [39]. Este teorema estabelece que, em um sistema dinâmico com um espaço de fase limitado, a maioria dos pontos no espaço de fase retornará infinitamente próximo de suas posições iniciais inúmeras vezes, em outras palavras, cada solução após um número $n$ de interações poderá retornar tão próximo quanto se queira de uma determinada condição inicial. No entanto, o conjunto de pontos que não retornam tem medida nula. Nos casos do sistema de Lorenz e do mapeamento de Hénon, o espaço de fase é limitado, e as trajetórias permanecem confinadas a uma região específica. Quando as trajetórias tendem a um conjunto de medida nula, isso implica que praticamente todos os pontos no espaço de fase eventualmente retornarão à região. Assim, essa região torna-se um atrator, atraindo as trajetórias do sistema.

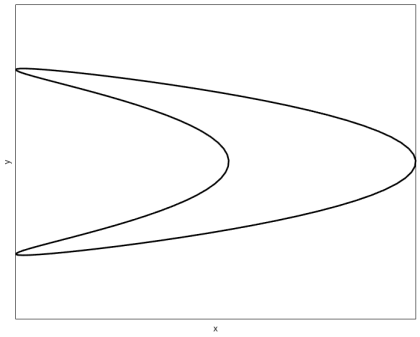
Essa propriedade é importante para compreender o comportamento das trajetórias em resposta as condições a iniciais, indicando a presença de um atrator para o qual as trajetórias convergem ao longo do tempo. Essa concepção é crucial para a análise de sistemas dinâmicos, visto que dessa forma podemos revelar o comportamento de longo



(a) $H_1$ aplicada na elipse centrada na origem.



(b) Transformação por $H_2$.



(c) Transformação por $H_3$.

Figura 3.4: Transformações sucessivas por $H_1$, $H_2$ e $H_3$ (Fonte: Autor)

prazo do sistema, podendo também determinar os pontos de estabilidade. Em alguns casos, o atrator será uma região no espaço de fase que tem sensibilidade as condições iniciais e mesmo que as trajetórias demonstrem um comportamento caótico, as soluções permanecem confinadas na mesma região. esse tipo de atrator é chamado de atrator estranho, descrito por Lorenz em 1963 ([35]).

Vamos definir um mapeamento $H$ de $S$. Então dado um ponto $P$ de $S$ seguimos sua trajetória até que ele cruze $S$ novamente, este novo ponto é $H(P)$. Uma trajetória é assim substituída por um conjunto infinito de pontos em S, obtidos pela aplicação repetida do mapeamento $H$.

As propriedades essenciais da trajetória são refletidas nas propriedades correspondentes do conjunto de pontos, ou seja, queremos conservar a sensibilidade as condições iniciais e a presença de um atrator estranho. Reduzimos assim formalmente o problema ao estudo de um mapeamento bidimensional. Agora o mapeamento $H$ será definido por equações explícitas que expressam diretamente $H(A)$ quando $A$ é conhecido. Após a conclusão desse processo, não existe mais correspondência com o sistema de Lorenz; por outro lado, as propriedades mencionadas anteriormente que merecem ser estudadas são preservadas, além disso, há uma simplificação significativa nos cálculos [26].

Para definir $H$, consideramos uma elipse alongada ao longo do eixo das abscissas e centrada em $(0, 0)$. É importante ressaltar que a aplicação não está restrita apenas a uma elipse. Optamos por demonstrar as transformações aplicadas a uma elipse devido à abordagem original de Hénon, conforme descrito em [26]. No entanto, é possível aplicar $H_1$ a outras regiões, e ainda observar os mesmos efeitos, como discutido em [41]. A aplicação de $H_1$ na elipse é descrita pela equação:

$$H_1 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ 1 - ax^2 + y \end{pmatrix}.$$

$H_1$ gera a Figura 3.4(a). Seja $H_2$ e $H_3$ dadas por:

$$H_2 = \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} bx \\ y \end{pmatrix}, H_3 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}, b < 1.$$

Onde $H_2$ faz uma contração em $x$ e $H_3$ projeta a figura ao longo da reta $x$. Gerando a Figura 3.4(b) e 3.4(c). Finalmente, podemos fazer o produto das transformações obtendo $H_{ab}$. Note que, uma parábola da forma $F_c(x) = 1 - cx^2$ poderia ser formada aplicando as três transformações acima, sendo assim, a função descrita forma uma parábola aberta para esquerda onde seu vértice está em $(1, 0)$ [2].

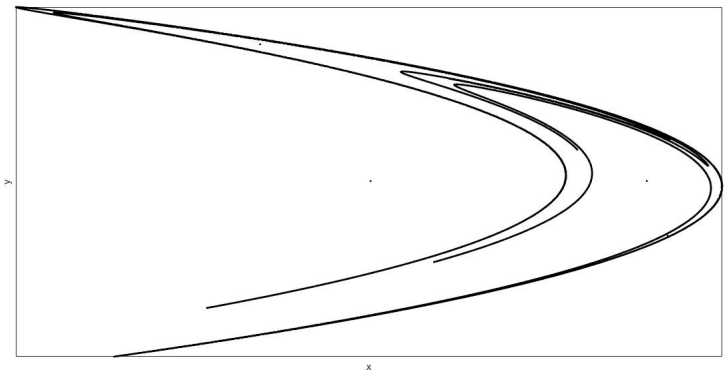


Figura 3.5: Atrator de Hénon com $a = 1,4$ e $b = 0,3$ (Fonte: Autor)

Vamos explorar o funcionamento de cada fase dessa transformação: $H_1$ corresponde à transformação não linear que converte uma reta $y = constante$ em uma parábola. Logo após, $H_2$ realiza uma contração em relação ao eixo $x$, determinada pelo parâmetro $b$. Por fim, a reflexão em relação à reta $x = y$ é efetuada pela transformação $H_3$. A forma resultante apresenta uma semelhança com uma parábola que se abre para a esquerda, conforme previamente estabelecido [47], dessa forma, fazendo o processo iterativo obtemos o gráfico da Figura 3.5.

## 3.6 Algumas propriedades matemáticas do mapa de Hénon

Nesta seção, serão abordadas as características matemáticas significativas do mapa de Hénon. Essencialmente, o mapa de Hénon constitui uma família de funções $H_{ab} : \mathbb{R}^2 \to \mathbb{R}^2$ denotada por

$$H_{ab} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 - ax^2 + y \\ bx \end{pmatrix}, \tag{3.5}$$

onde $a, b \in \mathbb{R}$. Em geral, considera-se que tanto $a$ quanto $b$ são diferentes de zero, assegurando, assim, a natureza bidimensional contínua do mapa de Hénon. No caso específico de $a = 0$, o mapa se simplifica para uma única equação logística, já que o termo quadrático é eliminado. Note que a suposição de $a$ ser não nulo é fundamental para que o mapa mantenha sua característica de equação de recorrência, definindo assim

uma sequência $\{x_n\}$ em que $x_n$ é um polinômio de segundo grau, expresso de maneira genérica como $x_n = ax_{n-1}^2 + bx_{n-1} + c$. Este contexto enfatiza a importância da escolha de $a$ diferente de zero para preservar as propriedades dinâmicas do mapa de Hénon.

**Teorema 3.12.** *O mapa de Hénon tem o seguinte Jacobiano:*

$$JH_{ab}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2ax & 1 \\ b & 0 \end{pmatrix}$$

*com $det(J(H_{ab})) = -b$ para $a$ e $b$ fixos e $x, y \in \mathbb{R}$. Se $a^2x^2 + b \geq 0$ então os autovalores de $det(J(H_{ab}))$ são números reais $\lambda = -ax \pm \sqrt{a^2x^2 + b}$.*

*Demonstração.* A matriz jacobiana é composta pelas derivadas parciais da função, logo

$$JF = \begin{pmatrix} \dfrac{\partial x_{n+1}}{\partial x_n} & \dfrac{\partial x_{n+1}}{\partial y_n} \\ \dfrac{\partial y_{n+1}}{\partial x_n} & \dfrac{\partial y_{n+1}}{\partial y_n} \end{pmatrix}.$$

Como o mapa de Hénon é uma equação iterativa as derivadas de $x_{n+1}$ será em relção a $x_n$ e a derivada de $y_n$ será em relção a $y_n$, segue que

$$\frac{\partial x_{n+1}}{\partial x_n} = -2ax_n$$

$$\frac{\partial y_{n+1}}{\partial x_n} = b$$

$$\frac{\partial x_{n+1}}{\partial y_n} = 1$$

$$\frac{\partial y_{n+1}}{\partial y_n} = 0$$

logo,

$$J(H_{ab}) = \begin{pmatrix} -2ax & 1 \\ b & 0 \end{pmatrix}$$

É facil notar que $det(J(H_{ab})) = -b$.

Para determinar os autovalores de $J(H_{ab})$ basta resolver

$$det(J(H_{ab} - I\lambda) = det\begin{pmatrix} -2ax - \lambda & 1 \\ b & 0 - \lambda \end{pmatrix}.$$

Sendo assim, temos de resolver $\lambda^2 + 2ax\lambda - b = 0$ então

$$\lambda = -ax \pm \sqrt{a^2x^2 + b},$$

portanto, os autovalores são reais se $a^2x^2 + b \geq 0$. □

**Observação 3.13.** *Pela Definição 3.7 podemos notar que se $|b| < 1$ temos uma contração de área.*

**Teorema 3.14.** *$H_{ab}$ é injetiva.*

*Demonstração.* Se $H_{ab}$ é injetiva, dados $x$, $y$, $z$ e $w$ distintos, precisamos provar que se a igualdade abaixo é verdadeira, então $(x, y) = (z, w)$:

$$H_{ab}\begin{pmatrix} x \\ y \end{pmatrix} = H_{ab}\begin{pmatrix} z \\ w \end{pmatrix}, \tag{3.6}$$

Ao desenvolver a Equação (3.5), obtemos:

$$\begin{pmatrix} 1 - ax^2 + y \\ bx \end{pmatrix} = \begin{pmatrix} 1 - az^2 + w \\ bz \end{pmatrix} \tag{3.7}$$

Suponhamos, por contradição, que $H_{ab}$ não seja injetiva. Isso implica que existem $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ e $\begin{pmatrix} z_0 \\ w_0 \end{pmatrix}$, tais que, $H_{ab}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ e $H_{ab}\begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} z_0 \\ w_0 \end{pmatrix}$, com $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} z_0 \\ w_0. \end{pmatrix}$. A partir da Equação (3.5) , chegamos a $1 - ax^2 + y = 1 - az^2 + w$ e $bx = bz$.

Rearranjando os termos, obtemos $y - w = a(x^2 - y^2)$ e, como $b \neq 0$, concluímos que $x = z$. Além disso, note que $y - w = 0$, logo $y = w$. Portanto, $H_{ab}$ é injetiva. □

**Teorema 3.15.** *Para $b \neq 0$ $H_{ab}$ é invertível e a sua inversa é injetora.*

*Demonstração.* $H_{ab}$ é invertível por hipótese, então para $y = x - 1 + ay^2/b^2$ e $x = y/b$, temos

$$H_{ab}^{-1} = \begin{pmatrix} \frac{b}{y} \\ -1 + \frac{ay^2}{b^2} + x \end{pmatrix}$$

Assim, segue que

$$H_{ab} \circ H_{ab}^{-1} = \begin{pmatrix} 1 - a(\frac{y}{b})^2 + x - 1 + a(\frac{y}{b})^2 \\ b(\frac{y}{b}) \end{pmatrix}$$

simplificando,

$$H_{ab} \circ H_{ab}^{-1} = \begin{pmatrix} x \\ y \end{pmatrix}$$

sendo assim, $H_{ab}$ é invertível.

Agora suponha que $H_{ab}^{-1}$ não seja injetora. Isso é um absurdo, pois pelo Teorema 2 $H_{ab}$ é injetora, logo a sua inversa é injetora. □

Como já vimos em seções anteriores, em sistemas dinâmicos, muitas vezes busca-se compreender a evolução de um sistema e, se possível, tentar descrever essa evolução ao longo de um intervalo de tempo considerável. Vimos também que as derivadas tem um papel crucial no entendimento de como esses sistemas evoluem. Nesse contexto, é necessário estudar os estados de equilíbrio do sistema, as trajetórias das soluções, as transições de fase e a previsão do comportamento desses sistemas. Portanto, como dito anteriormente o estudo dos pontos fixos desempenham um papel importante no entendimento dessas características dos sistemas dinâmicos.

Considere o mapa de Hénon, pela Definição 2.9 e considerando $a \neq 0$ temos que resolver

$$H_{ab}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 - ax^2 + y \\ bx \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}. \tag{3.8}$$

Note que na equação (3.8), $y = bx$, então podemos escrever $x = 1 - ax^2 + bx$, resolvendo obtemos a expressão $x = \frac{1}{2a}(b - 1 \pm \sqrt{(1-b)^2 + 4a})$. Fazendo $x = \frac{y}{b}$ obtemos os pontos fixos $p$ e $q$.

$$p = \left(\frac{1}{2a}\left(b - 1 + \sqrt{(1-b)^2 + 4a}\right), \frac{b}{2a}\left(b - 1 + \sqrt{(1-b)^2 + 4a}\right)\right)$$

$$q = \left( \frac{1}{2a}\left(b - 1 - \sqrt{(1-b)^2 + 4a}\right), \frac{b}{2a}\left(b - 1 - \sqrt{(1-b)^2 + 4a}\right)\right).$$

Note que, os seus pontos fixos dependem de $a$ e $b$. Além disso, os pontos fixos serão reais se $a \geq -\frac{1}{4}(1-b)^2$.

**Definição 3.16.** *Sejam $U, V \subset \mathbb{R}^m$, abertos. Um homeomorfismo $f : U \longrightarrow V$ é uma bijeção contínua cuja a inversa $f^{-1} : V \longrightarrow U$ também é continua.*

**Definição 3.17.** *Sejam $U, V \subset \mathbb{R}^m$, abertos. Um difeomorfismo $f : U \longrightarrow V$ é uma bijeção diferenciável cuja a inversa também é diferenciavel. se $f$ e $f^{-1}$ são de classe $C^k$, dizemos que $f$ é um difeomorfismo de classe $C^k$.*

**Exemplo 3.18.** *O gráfico de uma função continua é homeomorfa ao seu domínio.*

*Seja $f : U \longrightarrow V$ contínua onde $G(f) = \{(x, f(x)) : x \in U\}$. Se $f$ é homeomorfa ao seu domínio existe $\phi : G(f) \longrightarrow U$ sendo $\phi$ um homeomorfismo.*

*Podemos definir $\phi : G(f) \longrightarrow U$ como $\phi(x, f(x)) = x$. Note que $\phi$ é uma bijeção, pois $x$ é um elemento qualquer de $U$, logo evidentemente $\phi$ é sobrejetora e como para cada $x$ existe um único $f(x)$ então $\phi$ é injetora. Além disso $\phi$ é uma projeção do par ordenado em $U$ logo $\phi$ é continua. A inversa de de $\phi$ existe, sendo, $\phi^{-1} : U \longrightarrow G(f)$ definida por $\phi^{-1} = (x, f(x))$. Na primeira coordenada temos a função identidade e $f$ é continua por hipótese, logo $\phi^{-}1$ é continua. Como $x \in U$ e cada par ordenado está associado a um único $x$ então podemos concluir que $\phi$ é um homeomorfismo.*

**Exemplo 3.19.** *Seja $f : \mathbb{R} \longrightarrow (0, \infty)$ com $f(x) = e^x$. Então $f$ é um difeomorfismo, pois $f$ é uma bijeção diferenciável e existe $f^{-1} : (0, \infty) \longrightarrow \mathbb{R}$ definida por $f^{-1} = ln(y)$ que também é diferenciável.*

**Observação 3.20.** *Embora todo difeomorfismo seja um homeomorfismo, nem todo homeomorfismo é um difeomorfismo.*

**Exemplo 3.21.** *Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$ com $f(x) = x^3$ para todo $x \in \mathbb{R}$. $f$ é uma função claramente bijetora, possuindo uma inversa bem definida e existente, que pode ser expressa por $f^{-1} = y^{\frac{1}{3}}$. Como $f$ e $f^{-1}$ são continuas $f$ é um homeomorfismo. No entanto, $f^{-1}$, não é diferenciável na origem então não é um difeomorfismo.*

Dado um difeomorfismo $f : U \longrightarrow V$, onde $U$ e $V$ são abertos em $\mathbb{R}^m$ a inversa também é um difeomorfismo. Se $f$ é um difemorfismo por hipótese implica que $f$ é injetora, portanto $f^{-1}$ também é injetiva. De fato, a matriz jacobiana de $f$ é invertível para todo $x \in U$ pois a continuidade e diferenciabilidade de $f$ garante a inversa da matriz jacobiana. Sendo assim, como $f$ é de classe $C^k$ então $f^{-1}$ também é de classe $C^k$, logo $f^{-1}$ é um difeomorfismo. Considere dois difeormorfismos $f$ e $g$ tais que $f : U \longrightarrow V$ e $g : V \longrightarrow W$, onde $U$, $V$ e $W$ são conjuntos abertos em $\mathbb{R}^m$, então a composta possui as mesmas propriedade de continuidade e diferenciabilidade que ambas as funções, além disso a composta também é bijetora de classe $C^k$. Portanto, $f \circ g$ é um difeomorfismo.

Note que $H_{ab}$ com $b \neq 0$ é um difemorfismo. Essa afirmação é uma consequência direta dos Teoremas 3.14 e 3.15.

**Definição 3.22.** *Seja $f$ um difeomorfismo e $x$ um ponto fixo de $f$. Dizemos que $x$ é um ponto fixo hiperbólico se $\mid Df(x) \mid \neq 1$. Se $\mid Df(x) \mid < 1$ dizemos que este ponto fixo é um atartor, e se $\mid Df(x) \mid > 1$ dizemos que é um ponto fixo repulsor. Se $x$ é um ponto periódico de período $n$, dizemos que $x$ é um ponto periódico hiperbólico (atrator ou repulsor) se $x$ é ponto hiperbólico atrator ou repulsor de $f^n$. Um ponto fixo de derivada igual a $-1$ ou $1$ é dito não-hiperbólico.*

Observa-se que, se $a < -\frac{1}{4}(1-b)^2$, então $a$ não pertence ao conjunto dos números reais. Diante disso, iremos investigar o que ocorre quando $a_1 = a = -\frac{1}{4}(1-b)^2$. Substituiremos $a_1$ nas coordenadas $x$ e $y$ dos pontos fixos $p$ e $q$. Assim, temos:

$$x = \frac{1}{2\left(-\frac{1}{4}(1-b)^2\right)}\left(b-1 \pm \sqrt{(1-b)^2 - 4\frac{1}{4}(1-b)^2}\right).$$

Simplificando, obtemos

$$x = -\frac{2}{b-1}$$

para coordenada $y$ dos pontos fixos o processo é análogo, então

$$y = -\frac{2b}{(b-1)}.$$

Note que $p = q$, sendo assim, para este caso, temos apenas um ponto fixo. Se substituirmos $x$ e $a = -\frac{1}{4}(1-b)^2$ na expressão dos autovalores de $H_{ab}$ obtemos

$$\lambda_{1,2} = -\frac{1}{4}(1-b)^2\left(-\frac{2}{b-1}\right) \pm \left[\left(-\frac{1}{4}(1-b)^2\right)^2\left(-\frac{2}{b-1}\right)^2 + b\right]^{1/2},$$

simplificando, temos que

$$\lambda_{1,2} = -\frac{1}{2}(b-1) \pm \sqrt{\frac{1}{4}(b-1)^2 + b}. \tag{3.9}$$

A fim de preservar a propriedade de contração de área, assumimos $|b| < 1$. Para $\lambda_1$ e $\lambda_2$, é necessário que $\frac{1}{4}(b-1)^2 + b > 0$. Vamos considerar apenas a parte positiva da Equação (3.9). Assim, rearranjando os termos da Equação (3.9), segue que

$$\left[\lambda + \frac{1}{2}(b-1)\right]^2 = \frac{1}{4}(b-1)^2 + b.$$

. Desenvolvendo o lado esquerdo da equação

$$\lambda^2 + \lambda(b-1) + \frac{1}{4}(b-1)^2 = \frac{1}{4}(b-1)^2 + b$$

então temos que resolver

$$\lambda^2 + \lambda(b-1) - b = 0.$$

Note que $\lambda = 1$ é solução para a equação. Logo, $p_1$ é um ponto de sela.

Como visto anteriormente quando $\lambda_1$ ou $\lambda_2$ é igual a $-1$ teremos um ponto de bifurcação de período duplo quando isso ocorre a dinâmica dos pontos fixos mudam [3]. Vamos investigar para qual valor de $a$ ocorre uma bifurcação de duplo período. Para tanto podemos notar que $\lambda_1 + \lambda_2 = -2ax$ e $\lambda_1\lambda_2 = -b$. Se considerarmos $\lambda_1 = -1$, temos que $\lambda_2 = b$, então obtemos

$$b - 1 = -2ax, \tag{3.10}$$

sabemos que a coordenada x dos pontos fixos é dado por

$$x = \frac{1}{2a}\left((b-1) \pm \sqrt{(1-b)^2 + 4a}\right).$$

Substituindo a Equação (3.10) em $x$, resulta em

$$-(b-1) = (b-1) \pm \sqrt{(1-b)^2 + 4a}$$

assim, segue que

$$-2(b-1) = \pm\sqrt{(1-b)^2 + 4a}$$
$$4(1-b)^2 = (1-b)^2 + 4a$$
$$a = \frac{3}{4}(1-b)^2.$$

Logo temos um ponto de bifurcação de duplo período quando $a = \frac{3}{4}(1-b)^2$.

Para $a > -\frac{1}{4}(1-b)^2$ temos que $(1-b)^2 + 4a > 0$ logo obtemos dois pontos fixos: um ponto atrator e um ponto nó de sela.

## 3.7 O Atrator de Hénon

O atrator de Hénon, para os valores dos parâmetros $a = 1,4$ e $b = 0,3$, apresenta um comportamento caótico notável. Além disso, veremos que ele é um atrator estranho, pois é possível determinar sua dimensão fractal sob os valores de parâmetros mencionados anteriormente. Nesta seção, exploraremos essa ideia. Primeiramente, é evidente que o atrator de Hénon exibe sensibilidade às condições iniciais. Podemos observar isso mais claramente ao plotar um gráfico para duas condições iniciais próximas ao longo do número de iterações. Como mencionado anteriormente, existe uma relação entre o fator de redução

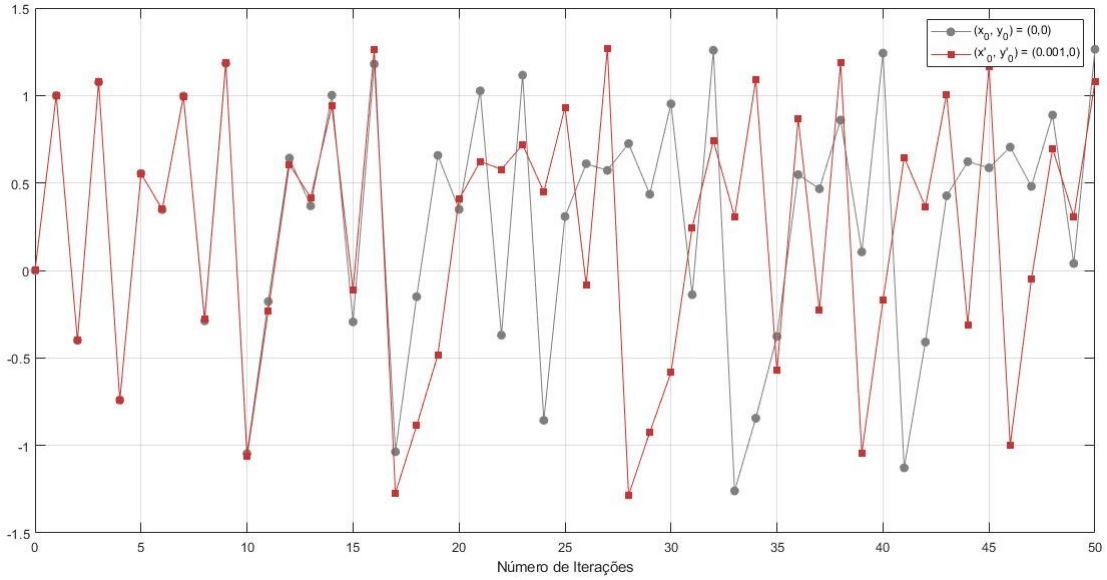



Figura 3.6: Valores para $x$ ao longo de 50 iterações para duas condições iniciais $x_0 = 0$ e $x_0' = 0,001$(Fonte: Autor)

$r$ e o número de etapas $N$. Para a curva de Koch, determinamos que $D \approx 1,26$, implicando uma parte fracionária de $0,26$. Podemos aplicar a ideia de fractais para estabelecer uma lei de medida. Consideremos um polígono não necessariamente regular ou convexo, onde nosso objetivo é aproximar o seu perímetro. Para isso, vamos cobrir esse objeto com "caixas"de um certo fator de escala $r$. Assim, essa medida pode ser expressa por $u = c(1/r)^d$, onde $c$ é uma constante que depende do tamanho dos intervalos dessas caixas. Por exemplo, se tomarmos um quadrado de lado com tamanho 2 em um plano e o

cobrirmos com caixas de lado com tamanho $r = 1/n$, então $u = 4(1/r^2)$ chamaremos esse método de lei de potência de medição. Podemos estender essa ideia para estudar outros fractais. A Figura 3.7 ilustra como essa abordagem pode ser aplicada no estudo da curva de Koch, como discutido na seção 2.6. Observamos que é natural escolher tamanhos de escala da forma $1/3^n$. Na seção 2.6 vimos que os segmentos de reta podem ser medidos como $l = L_0/3^n$ ocorrendo o número de passo na forma de $4^n$, assim, a medida total $u = (4/3)^n$.

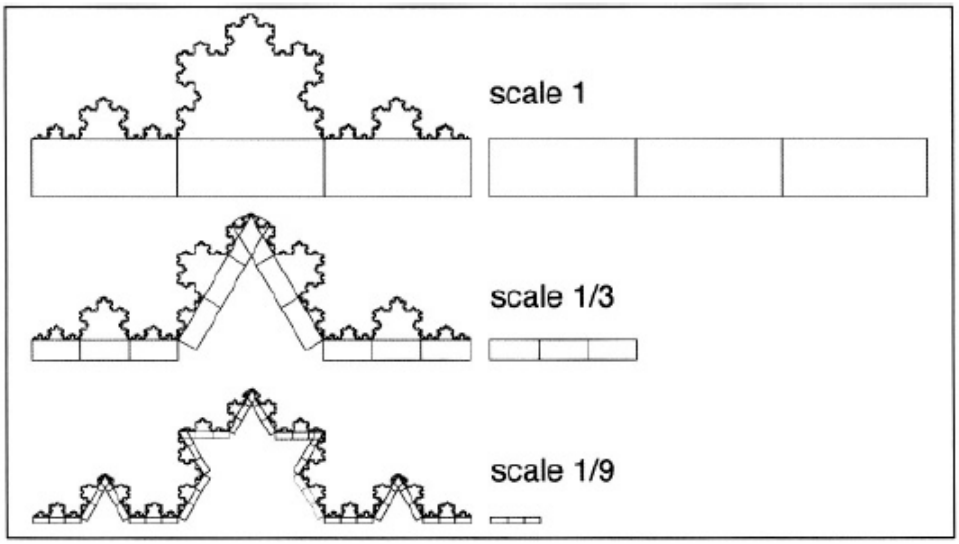



Figura 3.7: Medida da curva de Koch para diferentes escalas (Fonte: [41]).

Há uma relação entre a lei de potência de medição e a dimensão de auto-similaridade de um fractal (ver [41]). Podemos simplificar a escolha de $c$ da seguinte forma:

$$u = \frac{1}{r^d}, \tag{3.11}$$

assim, temos que

$$\log u = d \log \frac{1}{r}, \tag{3.12}$$

onde $u$ representa o comprimento do fator de escala correspondente. Por outro lado, temos $N = 1/r^D$, que representa o número de etapas de auto-semelhança. Como feito anteriormente, podemos aplicar o logaritmo em ambos os lados, logo

$$\log N = D \log \frac{1}{r}. \tag{3.13}$$

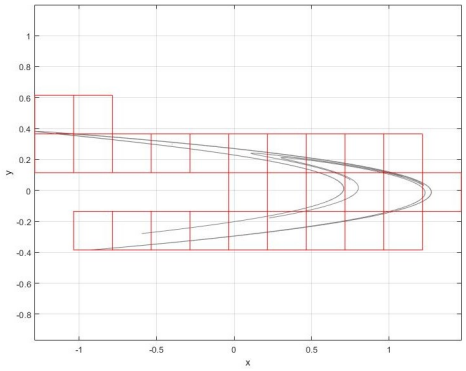
Observe que existe uma relação entre o comprimento $u$ e o número de passos $N$. Quando o fator de escala $r = 1$, medimos um comprimento $u = 1$. Portanto, ao medirmos uma escala $r$, onde cada objeto é composto por $N$ cópias do tamanho $r$, obtemos um comprimento total de $u = Nr$. Aplicando o logaritmo,

$$\log u = \log N + \log r. \tag{3.14}$$

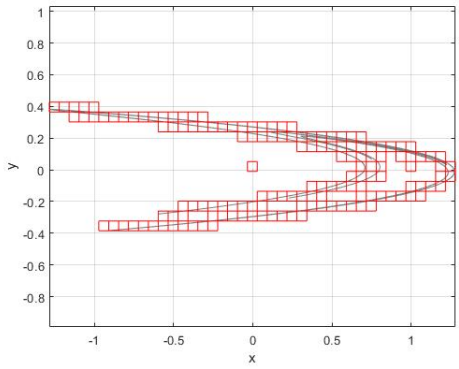
Substituindo as equações (3.12) e (3.13) em (3.14), obtemos

$$d \log \frac{1}{r} = D \log \frac{1}{r} + \log r,$$

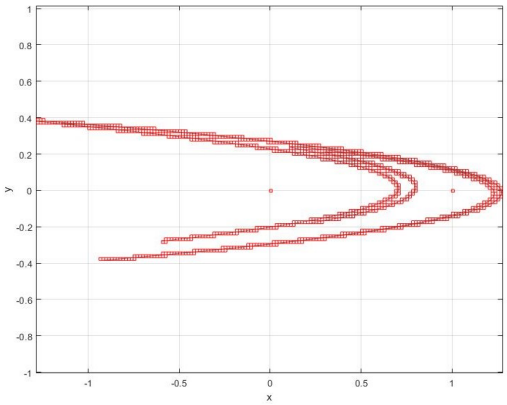
como $\log 1/r = -\log r$, então



(a) $r = 1/4$



(b) $r = 1/16$.



(c) $r = 1/64$

Figura 3.8: Atrator de Hénon coberto por caixas para diferentes fatores de escala (Fonte: Autor)

$$-d \log \frac{1}{r} = -D \log r + \log r,$$
$$D = 1 + d. \tag{3.15}$$

Agora podemos expandir a dimensão encontrada para abranger formas que não são curvas auto-similares, como linhas costeiras e outras semelhantes. Assim, introduzimos a dimensão da bússola (às vezes também denominada dimensão do divisor ou da régua).

Podemos estender essa ideia ao mapa de Hénon para determinar sua dimensão. Ao ampliarmos a imagem do atrator, encontraremos um padrão que se assemelha a um conjunto de Cantor (basta ampliar a Figura 3.5). Utilizando a equação (3.15), obtemos $D = 1 + (\log 2/\log 3) \approx 1,63$. No entanto, $\log 2/\log 3$ representa apenas a dimensão de um conjunto específico de Cantor, ou seja, o padrão obtido pela exclusão recursiva dos terços intermediários de intervalos. Podemos alterar a construção subdividindo cada intervalo em $p$ partes iguais, mantendo apenas o primeiro e o último intervalo enquanto excluímos todos os outros. Isso resulta em um conjunto de Cantor com dimensão $\log 2/\log p$. Escolhendo $p = 12$, obtemos

$$D = 1 + \frac{\log 2}{\log 12} \approx 1,27.$$

A abordagem de cobrir o atrator de Hénon com caixas pode ser a técnica que vamos utilizar para determinar sua dimensão. Observa-se na Figura 3.8(a), 3.8(b) e 3.8(c) que, à

medida que reduzimos o tamanho da escala da caixa, aumentamos a resolução da cobertura do atrator de Hénon. Sendo assim vamos diminuir ao máximo o tamanho das caixas obtendo

$$D_{box} = \lim_{r \to 0} \frac{\log N(r)}{\log 1/r}.$$

Denominamos essa dimensão de dimensão de *Box-Counting*. Existem definições alternativas, que não serão abordadas aqui.

A partir desse conceito, temos outra maneira de obter a dimensão do atrator de Hénon, conforme proposto por P. Grassberger em 1983 [25]. Com base nesse estudo, investigaremos a dependência de $N(r, n)$ com o número de iterações. Os dados tabulados por Grassberger em 1983 [25] sugerem o seguinte comportamento:

$$N(r, n) \approx -Cr^{-\alpha} n^{-\beta}. \tag{3.16}$$

Para testar essa conjectura considere as taxas de crescimento de $N(r, n)$ a medida que $n$ aumenta.

$$\frac{\Delta N(r, n)}{\Delta n} \approx -Cr^{-\alpha} n^{-\beta-1}. \tag{3.17}$$

Dada uma tabela de valores de $N(r, n)$ para diferentes tamanhos de caixa e contagens de iteração, podemos extrair as taxas de crescimento usando um incremento $\Delta n$ não muito pequeno. Esses dados podem ser plotados em diagramas log/log. Se esses gráficos revelarem linhas retas, então a conjectura é apoiada e os expoentes e podem ser obtido a partir das inclinações correspondentes. Grassberger, 1983 Obteve os seguintes resultados para os expoentes: $\alpha = 2,42 \pm 0,15$ e $\beta = 0,89 \pm 0,03$.

Tendo os valores dos expoentes podemos estimar $N(r)$ com base na medida de $N(r_0, n_0)$ e $N(r_0, 2n_0)$ vamos denotar a constante da equação 3.16 por $\gamma_1$. Então

$$N(r_0, n_0) = N(r_0) - \gamma_1 r_0^{-\alpha} n_0^{-\beta}$$
$$N(r_0, 2n_0) = N(r_0) - \gamma_1 r_0^{-\alpha} 2n_0^{-\beta}.$$

Podemos estimar a constante $\gamma_1$ resolvendo as equações acima,

$$\gamma_1 = \frac{N(r_0, 2n_0) - N(r_0, n_0)}{(1 - 2^{-\beta}) r_0^{-\alpha} n_0^{-\beta}}$$

obtendo o resultado com $r$ e $n$

$$N(r) = N(r, n) + \gamma_1 r^{-\alpha} n^{-\beta}.$$

Grassberger calculou $N(r) = 238,513 \pm 200$ para $r = 0,00169/60$. Podemos prosseguir com o cálculo da dimensão *box-counting* seguindo a mesma abordagem. Com outra constante de proporcionalidade $\gamma_2$ obtemos

$$N(s) = \gamma_2 r^D$$

$$N(2s) = \gamma_2 2^{-D} r^{-D}.$$

Então,

$$\frac{N(r)}{N(2r)} = 2^D.$$

Assim, segue que

$$D = \frac{\log N(r) - \log N(2r)}{\log 2}.$$

Essas estimativas levaram Grassberger a obter o número para dimensão do Atrator de Hénon $D = 1,28 \pm 0,01$ [25].

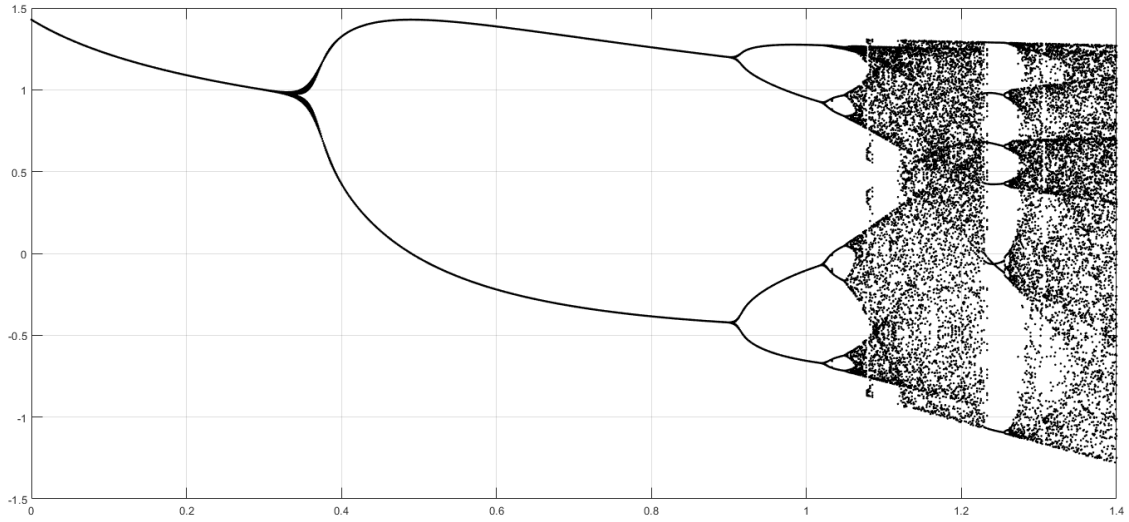



Figura 3.9: Diagrama de bifurcação do mapa de Hénon (Fonte: Autor)

O mapa de Hénon não possui atrator estranho para todos valores dos parâmetros $a$ e $b$, onde os parâmetros $a$ e $b$ controlam a não linearidade e a dissipação. Para $a = 1,4$ e $b = 0,3$ o mapa mostra um comportamento caótico pelas iterações. A Figura 3.5 mostra o resultado do cálculo para $a = 1,4$ e $b = 0,3$. Este mapa de Hénon possui um atrator estranho. Se ampliarmos partes desse atrator, poderemos ver uma estrutura fractal [2]. Basicamente o Hénon definiu um quadrilátero no qual todos os pontos dentro deste quadrilátero não escapavam para o infinito. Em vez disso permaneceram dentro do quadrilátero a medida que eram iterados. A cada iteração o quadrilátero é esticado e dobrado pelo mapa de Hénon até que é obtido o atrator geométrico [26]. As órbitas são muito sensíveis as condições iniciais, então trata-se de um sinal de caos. Para o estudo da dinâmica do sistema, podemos plotar o diagrama de bifurcação no espaço de fase e assim podemos observar as transições de estrutura. O mapa de Hénon tem bifurcação de duplo período quando $a = \frac{3}{4}(1-b)^2$.

O diagrama de bifurcação para o mapa de Hénon varia o parâmetro $a$ entre 0 e $1,4$ e retorna valores em $[-3/2, 3/2]$. É possível notar que quando $a$ está entre 0 e $0,32$, a sequência $\{x_n\}$ converge para o ponto fixo independente dos valores iniciais de $x_0$ e $y_0$. O gráfico da Figura 3.9 mostra que quando $a > 0,32$ a sequência $\{x_n\}$ converge para a órbita periódica de período 2. Se $b = 0,4$ temos pontos de período 1 (quando $a = 0,2$), pontos de período 2 (quando $a = 0,9$), e então teremos a duplicação de período sucessiva com 4,8,16,32... Chamamos esse processo de cascata, e além disso quando $a > 1,4$ podemos observar o comportamento caótico. Realizando um *close-up* na segunda ramificação inferior, podemos observar o mesmo fenômeno descrito na Seção 2.5.3. Assim, o diagrama de bifurcação também exibe uma auto-semelhança marcante. Essa observação nos leva a considerar não apenas o atrator de Hénon como uma estrutura fractal mas tabmém o diagrama de bifurcação para o mapa de Hénon apresentando uma geometria fractal.

Capítulo

4

# Criptografia e Caos

## 4.1 Contextualização histórica

Durante a história da humanidade, as relações sociais fizeram com que as informações produzidas ou transmitidas fossem escondidas. Essa necessidade é produto de uma diversidade de contextos históricos; em especial, podemos ver essa demanda surgindo em tempos de guerra. Uma forma de esconder informações é usar uma língua da qual poucos têm domínio. Um exemplo ascendente dessa ideia foi o uso de línguas nativas americanas na transmissão de mensagens durante a Segunda Guerra Mundial. A marinha estadunidense utilizava o navajo para se comunicar; essa é uma língua indígena do oeste dos Estados Unidos [5].

A técnica utilizada pela marinha dos Estados Unidos mostrou-se eficaz para o momento; entretanto, outras situações demandam formas mais elaboradas de se esconder informações. É possível utilizar uma língua mais conhecida e embaralhar as letras, substituir por outros símbolos e usar regras matemáticas para reger a forma como as mensagens serão ocultadas. Embora as técnicas pareçam ser complicadas, os primeiros registros históricos dessas técnicas para ocultar mensagens enviadas foram na Grécia. As mensagens eram embaralhadas de forma que poderiam ser desembaralhadas por quem conhecia a técnica em questão. O mecanismo utilizado pelos gregos consistia em um bastão no qual uma fita era enrolada em espiral, dessa forma, a mensagem era escrita horizontalmente na fita seguindo o sentido espiralado. A fita desenrolada gera uma série de letras sem sentido, e o mesmo acontece se a fita for enrolada em um bastão de tamanho diferente daquele que foi utilizado para escrever a mensagem. Ou seja, só é possível ler a mensagem se houver um bastão gêmeo. Os gregos chamavam esse processo de "escrita escondida"e então a palavra criptografia tem origem grega; haja vista a sua etimologia, *kryptós* significa escondido e *graphé* significa escrita.

Durante o decorrer da história, novos tipos de cifras surgiram, como a cifra de César. Essa técnica consiste em substituir as letras do alfabeto deslocando-as para uma nova posição. A Figura 4.1 é um modelo do equipamento utilizado para cifrar e decifrar as mensagens. Esse equipamento, chamado algumas vezes de disco de César, consiste em um anel superior fixo com um disco móvel no centro. Ambas as peças podem ser divididas em 26 casas, onde cada uma terá uma letra do alfabeto, como mostrado na Figura 4.1. A chave pode ser escolhida pela quantidade de casas que o giro do disco substitui as letras do alfabeto.

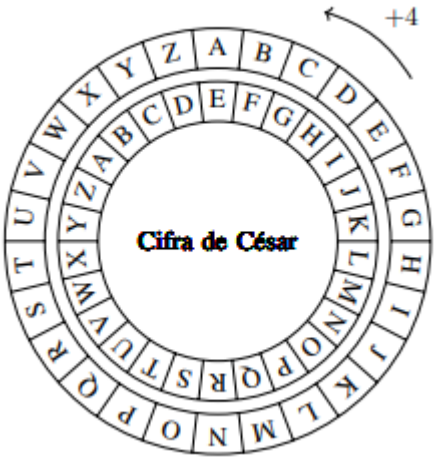



Figura 4.1: Equipamento utiliazado pelo exército de César para cifrar mensagens (Fonte: Autor)

**Exemplo 4.1.** *Considere a mensagem "estamos em guerra"para ser enviada pelo método de César. Usando a chave 4 o disco de Cesar estrá configurado como mostra a Figura 4.1. Assim, a mensagem cifrada, será da seguinte forma:*

*IWXEQW IQ KYIVVE*

Mesmo que haja formas de tornar a decodificação mais difícil, como trocar a chave a cada letra escrita, o avanço da criptoanálise e da computação tornaram o disco de César obsoleto. Um grande avanço na criptografia é a máquina Enigma, utilizada pelos alemães durante a Segunda Guerra Mundial. Quando as mensagens das tropas da Alemanha eram interceptadas pela inteligência britânica, eles se deparavam com uma mensagem cifrada de uma forma que nunca tinham visto antes. As mensagens eram embaralhadas com o uso da máquina Enigma. A máquina possuía três engrenagens com vinte e seis posições cada, havia cinco tipos de engrenagens que podiam ser trocadas entre si. Além disso, na parte frontal da máquina, era possível conectar as letras do alfabeto, que eram substituídas. Apenas ter uma máquina Enigma não era o suficiente para decifrar as mensagens enviadas, era necessário descobrir as configurações da máquina remetente para decodificar. Essa configuração ou chave mudava a cada vinte e quatro horas. A máquina foi vencida com a colaboração majoritária de Alan Turing, matemático britânico que, além de decifrar as mensagens da tropa alemã, projetou a máquina chamada Colossus, que quebrava os códigos da Enigma. A máquina eletromecânica de Turing é precursora dos computadores digitais como temos hoje.

De fato, a criptografia esteve presente na história da humanidade. Na atualidade, com a era digital, o avanço da criptografia justifica a sua necessidade. Com o crescimento da internet, o uso da criptografia tornou-se uma necessidade ainda maior para proteger os dados do usuário. É possível trocar mensagens e dados sem que seja possível um acesso decifrado.

## 4.2 Noções preliminares

Nesta seção iremos expor alguns conceitos básicos de sistemas criptográficos. Nesse contexto, é importante estarmos familiarizados com o vocabulário comum nessa área. Assim, segue alguns termos centrais para o estudo da criptografia:

- **Texto plano**: dados não encriptados;
- **Texto cifrado**: dados encriptados;
- **Chave (key)**: dados utilizados para encriptar um texto plano ou desincriptar um texto cifrado;
- **Encriptação**: converção de textos legíveis para um formato ilegível. Dessa forma, uma pessoa autorizada (que possua a chave de decriptação) pode decriptar a mensagem.

Quando estudamos um criptossistema o nosso intuito geralmente é atestar a técnica de cifra utilizada. Isto é, tentaremos "quebrar"a encriptação com o objetivo de validar ou descartar a técnica utilizada. Chamaremos esse processo de criptoanálise. Com base na chave de encriptação podemos definir dois tipos de sistemas criptográficos: criptossistema de chave privada (ou simétrica) e o criptossistema de chave pública (ou assimétrica).

A criptografia de chave privada utiliza apenas uma chave para encriptar e decritptar um texto, por isso, muitas vezes, esta técenica também é chamada de criptografia simétrica.

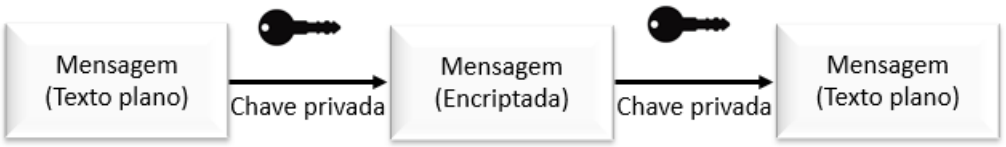



Figura 4.2: Esquema de demonstração de um criptossitemas de chave privada (ou simétrica)(Fonte: Autor)

**Definição 4.2** (Algoritmo)**.** *Chamamos de algoritmo uma sequência ordenada finita de operações para a realização de uma tarefa.*

A fim de compreender os algoritmos de chave privada os criptossistemas de chave privada notamos que a cifra depende de um par de algoritmo, sendo $E$ o algoritmo de encriptação e $D$ o algoritmo de desencriptação [4]. Denotamos ainda por $k$ a chave de criptografia, $m$ a mensagem original ou texto plano e por $c$ o texto final encriptado. Naturalmente,

$$c = E(k, m)$$

e

$$m = D(k, c).$$

A chamada equação de consistencia é dada por:

$$m = D(k, E(k, m)).$$

**Exemplo 4.3.** *Um clássico exemplo de criptossistema de chave privada ou de chave simétrica é a cifra de César brevemente explorada na seção anteriror. A cifra de Vigenére pode ser considerada uma sofisticação da cifra de César onde, além da substiuição de letras usamos uma palavra como chave. Dessa forma uma tabela com 26 letras do alfabeto em linha com 26 letras do alfabeto em coluna nos guiam para fazer a encriptação como*

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

Figura 4.3: A grade de Vigenère, conhecido também por tabula recta, usado para criptografia e descriptografia (Fonte: Autor)

| C | I | F | R | A | | D | E | | V | I | G | E | N | E | R | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | R | A | S | I | | L | B | | R | A | S | I | L | B | R | A |

Figura 4.4: Exemplo de criptografia utilizando a chave Brasil(Fonte: Autor)

*podemos ver na figura 4.3. Vamos criptografar a frase "CIFRA DE VIGENERE"usando a palvra "BRASIL". Primeiro repetimos a chave até obtermos o comprimento do texto como mostra a Figura 4.4 Agora basta encontrarmos a letra correspondente ao par ordenado da primeira letra da chave com a primeira letra do texto plano. Ou seja, a primeira letra do texto cifrado é D, haja visto, que* $(C, B)$ *corresponde a letra D. Faremos esse processo para todas as letras da chave combinadas com o texto plano. Note que, trata-se de uma cifra de César atribuindo uma chave diferente para cada letra do texto plano. Isto é para letra C usa-se a chave* $k = 1$ *que leva A em B; para a letra I usaremos a chave* $k = 17$ *que leva A em R até obtermos finalmente a mensagem cifrada "DZFJI OF MIYMYFIE".*

No criptossistema de chave pública a chave de encriptação é acessível para qualquer usuário. Em contra partida, a chave de desencriptação é privada, sendo assim, apenas uma pessoa autorizada pode ler a mensagem enviada. Nesse contexto, muitas vezes esse tipo de criptossitema é chamado de assimétrico.

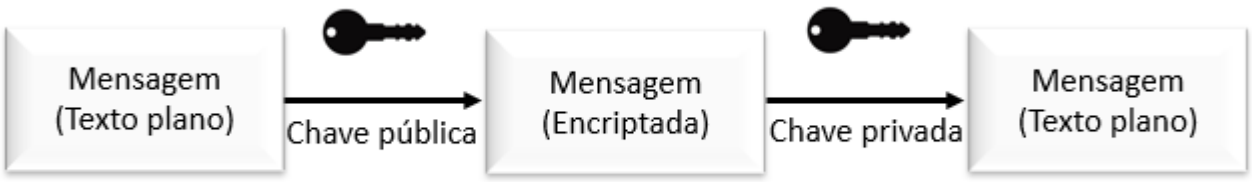



Figura 4.5: Esquema de demonstração de um criptossitemas de chave pública (ou assimétrica)(Fonte: Autor).

**Definição 4.4.** *Seja $G$ um conjunto munido de operação, logo*

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto a.b$$

*Dizemos que $G$ é um grupo quando a operação . satisfizer os seguintes axiomas:*

*(a) (Associatividade)$(a.b).c = a.(b.c)$, para todo $a, b, c \in G$;*

*(b) (Existência do elemento neutro) Existe $e \in G$ tal que $a.e = e.a = a$, para todo $a \in G$*

*(c) (Existência do elemento inverso) Para cada $a \in G$ existe $a^{-1} \in G$ tal que $a.a^{-1} = a^{-1}.a = e$;*

*Dizemos que $G$ é um grupo Abeliano ou comutativo quando $a.b = b.a$ para todo $a, b \in G$.*

**Definição 4.5** (Criptossistema de chave pública)**.** *Sejam $(G, .)$ um grupo abeliano e $X$ um conjunto. Uma ação $G$ em $X$ é uma função*

$$\divideontimes : G \times X \to X$$

*que cada par $(g, x)$ associa $g \divideontimes x \in X$ de modo que*

1. *$e \divideontimes x = x$ para todo $x \in x$;*
2. *Se $a, b \in G$ então $a \divideontimes (b \divideontimes b) \divideontimes x$.*

**Exemplo 4.6.** *Digamos que Alice e Bob desejam se comunicar secretamente. Para isso, Alice possui um cadeado $\boldsymbol{A}$ e uma chave para abri-lo, $\boldsymbol{a}$. Além disso, o mesmo ocorre com Bob. Façamos da seguinte maneira: Alice envia para Bob uma caixa de mensagem, fechada com cadeado $\boldsymbol{A}$ e cuja a chave só a Alice possui. Bob, ao receber a caixa coloca tmabém seu cadeado $\boldsymbol{B}$ e devolve para Alice a caixa com os dois cadeados $\boldsymbol{A}$ e $\boldsymbol{B}$. Desde que a ordem dos cadeados não importe, Alice usa agora a sua cheve para abrir seu cadeado $\boldsymbol{A}$ e devolve a caixa para Bob apenas com o cadeado $\boldsymbol{B}$. Bob, ao receber a caixa usa sua chave $\boldsymbol{b}$ para abrir o cadeado $\boldsymbol{B}$ e, finalmente, poder ler a mensagem que está dentro da caixa [4].*

**Exemplo 4.7.** *No exemplo 4.6, com o ponto de vista de ação de grupos, os cadeados e chaves são elementos inversos no grupo. Usando a notação anterior, $\boldsymbol{A} = g, a = g^{-1} \in G, \boldsymbol{B} = h, b = h^{-1} \in G$ e a mensagem pertence a um conjunto $X$ onde $G$ age. Assim temos a situção ilustrada na Figura 4.6*

| *Alice* | | *Bob* |
|---|---|---|
| $x$ | $\rightarrow$ | $g * x$ |
| $h * (g * x)$ | $\leftarrow$ | $a * x$ |
| $(h * g) * x = (g * h) * x =$ | | |
| $= (g * h) * x$ | $\rightarrow$ | $g^{-1} * [(g * h) * x] =$ |
| | | $g^{-1} * = [(g * h) * x] = h * x$ |
| | | $h^{-1} * (h * x) = x$ |

Figura 4.6: Comunicação entre Alice e Bob por meio da da ação de grupos (Fonte: [4]).

*Vamos agora introduzir uma forma mais realista de modelo de criptossitema assimétrico. A ideia central passa pelo conceito de par de chaves. Assim, cada usuário do*

*sistema terá duas chaves, sendo que uma delas é pública e a outra é privada. A chave pública pode transitar em meios inseguros de comunicação, enquanto a chave privada deve ser mantida em segredo por seu proprietário. A chave privada não pode ser derivada da chave pública. Em um criptossitema assimétrico qualquer pessoa pode criptografar uma mensagem utilizando a chave pública do destinatário e, somente este, sua chave privada, é capaz de decifrar a mensagem [4].*

**Exemplo 4.8.** *Novamente consideremos que Alice deseja enviar uma mensagem secreta m para Bob, sem terem se encontrado previamente. Utilizaremos a ideia do cadeado e da chave, apresntada no exemplo 4.6. Sob o ponto de vista de ações de grupo. Para isto, consideraremos o cadeado e sua chave como o par chaves pública e privada, respectivamente. desta forma, utilizaremos os pares* $(\boldsymbol{B}, \boldsymbol{a}$ *e* $\boldsymbol{B}, \boldsymbol{b})$ *para denotar as chaves públicas e privada de Alice e Bob, respectivamente. A chave pública serve para encriptar e a secreta para decriptar. Se Alice deseja enviar a mensagem para Bob, ela deve usar a chave pública de Bob para encriptar a mensagem. Nesse caso, Bob receberá* $\boldsymbol{B}$ *e, com a sua chave secreta, utilizando operações do grupo associado, Bob será capaz de ler a mensagem. A ideia de par de chaves é também muito útil para elaborar esquemas de assinatura digital.*

| Binário | Decimal | Hexa | Glifo |
|---|---|---|---|
| 0010 0000 | 32 | 20 | |
| 0010 0001 | 33 | 21 | ! |
| 0010 0010 | 34 | 22 | " |
| 0010 0011 | 35 | 23 | # |
| 0010 0100 | 36 | 24 | $ |
| 0010 0101 | 37 | 25 | % |
| 0010 0110 | 38 | 26 | & |
| 0010 0111 | 39 | 27 | ' |
| 0010 1000 | 40 | 28 | ( |
| 0010 1001 | 41 | 29 | ) |
| 0010 1010 | 42 | 2A | * |
| 0010 1011 | 43 | 2B | + |
| 0010 1100 | 44 | 2C | , |
| 0010 1101 | 45 | 2D | - |
| 0010 1110 | 46 | 2E | . |
| 0010 1111 | 47 | 2F | / |
| 0011 0000 | 48 | 30 | 0 |
| 0011 0001 | 49 | 31 | 1 |
| 0011 0010 | 50 | 32 | 2 |
| 0011 0011 | 51 | 33 | 3 |
| 0011 0100 | 52 | 34 | 4 |
| 0011 0101 | 53 | 35 | 5 |
| 0011 0110 | 54 | 36 | 6 |
| 0011 0111 | 55 | 37 | 7 |
| 0011 1000 | 56 | 38 | 8 |
| 0011 1001 | 57 | 39 | 9 |
| 0011 1010 | 58 | 3A | : |
| 0011 1011 | 59 | 3B | ; |
| 0011 1100 | 60 | 3C | < |
| 0011 1101 | 61 | 3D | = |
| 0011 1110 | 62 | 3E | > |
| 0011 1111 | 63 | 3F | ? |

| Binário | Decimal | Hexa | Glifo |
|---|---|---|---|
| 0100 0000 | 64 | 40 | @ |
| 0100 0001 | 65 | 41 | A |
| 0100 0010 | 66 | 42 | B |
| 0100 0011 | 67 | 43 | C |
| 0100 0100 | 68 | 44 | D |
| 0100 0101 | 69 | 45 | E |
| 0100 0110 | 70 | 46 | F |
| 0100 0111 | 71 | 47 | G |
| 0100 1000 | 72 | 48 | H |
| 0100 1001 | 73 | 49 | I |
| 0100 1010 | 74 | 4A | J |
| 0100 1011 | 75 | 4B | K |
| 0100 1100 | 76 | 4C | L |
| 0100 1101 | 77 | 4D | M |
| 0100 1110 | 78 | 4E | N |
| 0100 1111 | 79 | 4F | O |
| 0101 0000 | 80 | 50 | P |
| 0101 0001 | 81 | 51 | Q |
| 0101 0010 | 82 | 52 | R |
| 0101 0011 | 83 | 53 | S |
| 0101 0100 | 84 | 54 | T |
| 0101 0101 | 85 | 55 | U |
| 0101 0110 | 86 | 56 | V |
| 0101 0111 | 87 | 57 | W |
| 0101 1000 | 88 | 58 | X |
| 0101 1001 | 89 | 59 | Y |
| 0101 1010 | 90 | 5A | Z |
| 0101 1011 | 91 | 5B | [ |
| 0101 1100 | 92 | 5C | \ |
| 0101 1101 | 93 | 5D | ] |
| 0101 1110 | 94 | 5E | ^ |
| 0101 1111 | 95 | 5F | _ |

| Binário | Decimal | Hexa | Glifo |
|---|---|---|---|
| 0110 0000 | 96 | 60 | ` |
| 0110 0001 | 97 | 61 | a |
| 0110 0010 | 98 | 62 | b |
| 0110 0011 | 99 | 63 | c |
| 0110 0100 | 100 | 64 | d |
| 0110 0101 | 101 | 65 | e |
| 0110 0110 | 102 | 66 | f |
| 0110 0111 | 103 | 67 | g |
| 0110 1000 | 104 | 68 | h |
| 0110 1001 | 105 | 69 | i |
| 0110 1010 | 106 | 6A | j |
| 0110 1011 | 107 | 6B | k |
| 0110 1100 | 108 | 6C | l |
| 0110 1101 | 109 | 6D | m |
| 0110 1110 | 110 | 6E | n |
| 0110 1111 | 111 | 6F | o |
| 0111 0000 | 112 | 70 | p |
| 0111 0001 | 113 | 71 | q |
| 0111 0010 | 114 | 72 | r |
| 0111 0011 | 115 | 73 | s |
| 0111 0100 | 116 | 74 | t |
| 0111 0101 | 117 | 75 | u |
| 0111 0110 | 118 | 76 | v |
| 0111 0111 | 119 | 77 | w |
| 0111 1000 | 120 | 78 | x |
| 0111 1001 | 121 | 79 | y |
| 0111 1010 | 122 | 7A | z |
| 0111 1011 | 123 | 7B | { |
| 0111 1100 | 124 | 7C | \| |
| 0111 1101 | 125 | 7D | } |
| 0111 1110 | 126 | 7E | ~ |

Figura 4.7: Tabela de pré-codificação ASCII (Fonte: [4])

**Exemplo 4.9** (Assinatura digital)**.** *Considere que Alice envie uma mensagem $m$, encriptada ou não para Bob e que ela queira Bob tenha certeza que ela foi a emissora da mensagem. Para isso ela pode encriptar a mensagem com chave privada. Assim Bob receberá $\boldsymbol{a} \circledast m$ e agora, utilizando a chave pública de Alice ele tem a segurança de que a mensagem realmente enviada foi por ela.*

O processo de encriptação, muitas vezes, pode se mostrar complicado. O uso de computadores para transmissão de mensagens é utilizado a fim facilitar processamento de dados e transmitir mensagens. Nesse contexto, é necessário estabelecer uma pré-codificação, basta ver, a forma com que os computadores processam os dados numéricos, além disso, os algoritmos de criptografia são baseados em operações matemáticas[4]. Atualmente é mais comum usar como modelo de précodificação os sistema ASCII (*American Standard*

*code for Information Interchange*). Esse sistema é uma tabela em código binário de 7 bits que codifica um conjunto de 128 caracteres incluindo letras, maiúsculas e minúsculas, números e sinais de pontuação, sinais matemáticos e sinais de controle. Como um byte possui 8 bits, o bit excedente dos caracteres da tabela ASCII é utilizado de maneira diferente não unificada. Isso significa que sistemas operacionais diferentes podem definir extensões ASCII que usam o oitavo bit para reperesentar caracteres adicionais.

Tendo em vista que um computador entende apenas a linguagem binária, se um indivíduo pretende mandar uma mensagem ele deverá fazer a pré-codificação. A tabela ASCII associa os caracteres a um número de base decimal e podemos escrever o mesmo número na base binária.

## 4.3 Base binária e operadores lógicos

Um computador se comunica por meio de sinais digitais em circuitos elétricos que compõem a parte física da máquina. Esses sinais são transmitidos pela passagem ou não de corrente elétrica. Em razão disso, tornou-se necessária a criação de uma nova álgebra que envolve essa noção de "ligado" e "desligado". Nesse sentido, surge a álgebra Booleana que trabalha justamente com essa noção binária. Diante disso, é necessário estabelecer uma base numérica que compreenda essa lógica de "ligado" e "desligado" ou ainda a ideia de "verdadeiro" ou "falso". Dito isso, é estabelecido uma base numérica na qual os números são representados apenas por combinações de 0 e 1.

Usualmente é utilizado o sistema decimal para representações e operações, entretanto, como dito anteriormente, um computador opera utilizando o sistema binário de numeração. No sistema decimal um número pode ser representado pela composição de dez algarismos (0 1, 2, 3, 4, 5, 6, 7, 8, 9). O valor representativo em termos de quantidade do algarismo depende da sua composição e posição.

**Exemplo 4.10.** *O número* 2024 *significa* $2 \times 1000 + 0 \times 100 + 2 \times 10 + 4 \times 1$. *Note que, o 2 é o algarismo mais significativo e ocupa a posição mais a esquerda enquanto o 4 representa o algarismo menos significativo e ocupa uma posição mais à direita.*

No sistema binário, por sua vez, existem apenas dois algarismos, onde cada algarismo é chamado de bit e um número binário de 8 bits é chamado de byte. Visto como é construído um número na base decimal e um número na base binaria é possível converter e mudar as bases desses números. Nesse contexto, podemos estabelecer a relação

$$P = \sum_{i=1}^{n-1} V_i 2^i = V_0 2^0 + V_1 2^1 + V_2 2^2 + ... + V_{n-1} 2^{n-1}. \tag{4.1}$$

Onde $P$ é um número na base binária e cada $V_i$ é um bit onde $i$ corresponde a sua posição.

Uma vez formulada a base binária de numeração, podemos estabelecer as operações básicas nesse sistema. Assim, vamos começar pela adição, que obedece às seguintes regras: $0 + 0 = 0$; $0 + 1 = 1$; $1 + 0 = 1$. Em particular, $1 + 1 = (10)_2$, logo, em uma soma de mais bits o bit excedente 1 será acrescido no próximo bit, similar à soma comum na base decimal. As regras para a subtração são análogas, exceto para $0 - 1$ em que o resultado é 1. O produto segue a mesma regra da base decimal uma vez que, todo número multiplicado por 0 é 0 e 1 multiplicado por ele mesmo é 1. Além disso, para o produto de números com mais de um bit pode ser utilizado o método do deslocamento de adição exatamente como feito na base decimal. O quociente ocorre exatamente da mesma maneira que no sistema decimal, porém, de uma forma simplificada visto que, trata-se de operações realizadas com 0 e 1 [31].

Uma vez estabelecida a operação com números no sistema binário, é possível também levantar as interpretações computacionais desse sistema. Nesse contexto, iremos assimilar o bit 0 como falso e 1 verdadeiro. Essas ideias são suficientes para estabelecer os conceitos que estão por vir e que irá suprir os objetivos desse trabalho. Dito isso, e com todos os conceitos postos anteriormente é possível finalmente estabelecer a ideia de operador lógico. Um operador lógico pode ser entendido como uma função que opera em valores de verdadeiro ou falso, além disso, os operadores lógicos seguem fundamentalmente as regras da álgebra Booleana [12].

| AND | OR | NOT |
|---|---|---|
| E | OU | NÃO |
| $A \wedge B$ | $A \vee B$ | $\neg A$ |
| $A.B$ | $A + B$ | $A'$ |

Tabela 4.1: Tabela de operadores lógicos.

A Tabela 4.1 mostra alguns operadores lógicos juntos de suas notações algébricas. O operador lógico AND devolve uma afirmação verdadeira se duas afirmações $A$ e $B$ forem verdadeiras, se qualquer uma das duas afirmações for falsa isso significa que o resultado da operação é falso. Por outro lado, o operador OR apresenta um resultado verdadeiro se a afirmação $A$ e a afirmação $B$ forem verdadeiras e ainda, se pelo menos um dos resultados são verdadeiros então o resultado da operação também é verdadeiro. Uma operação OR só é falsa se tanto a afirmação $A$ quanto a afirmação $B$ forem falsas. O operador NOT, por sua vez, nega uma afirmação, isto é, se $A$ é uma afirmação verdadeira então o operador NOT faz com que ela se torne falsa. O análogo acontece se a afirmação $A$ é falsa.

Existem outros operadores lógicos, que podem ser vistos como uma composição dos operadores vistos anteriormente, como por exemplo, o operador NAND que faz a negação do operador AND. Diante disso, é possível obter um operador lógico que advém do operador OR. Esse operador inclui como verdadeiro duas afirmações verdadeiras. Toda via, o chamado operador "ou exclusivo" (XOR) denotado algebricamente por $A \oplus B$, que simplesmente torna falso a operação entres duas afirmações verdadeiras. O operador XOR

| $A$ | $B$ | $S$ |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

Tabela 4.2: Tabela verdade do operador lógico XOR.

é interessante para aplicações em criptossistemas devido a sua propriedade de reversibilidade. Isso significa que, se $A \oplus B = S$ então $A \oplus S = B$ e $B \oplus S = A$. Em razão disso, é possivel usar esse operador para encriptar e desincriptar um texto.

**Exemplo 4.11.** *Seja* $A = 1001$ *e* $B = 0101$ *então* $A \oplus B = 1100$. *Sendo* $S = 1100$ *vamos mostrar que* $A \oplus S = B$. *Então* $1001 \oplus 1100 = 0101$. *Analogamente vemos também que* $B \oplus S = A$.

## 4.4 Algumas noções sobre porcessamento de imagens digitais

O processamento de imagens digitais é uma área da ciência da computação que consiste na melhoria da análise humana de imagens digitais por meio de técnicas computacionais. Essa área é de suma importância, uma vez que, corrobora com a melhoria da representação virtual e visual dos objetos. O processamento de imagens digitais envolve uma série de etapas para que de fato essa análise possa apresentar alguma eficácia. Primeiro a imagem é capturada e convertida em sinais elétricos, e então esses sinais elétricos são convertidos em sinais digitais. Esse processo é realizado por um aparelho de captura, como por exemplo, uma câmera digital. O processo de conversão em sinal digital envolve uma amostragem de valores de intensidade de luz representada discretamente por pixels (o menor elemento de uma imagem digital) [15].

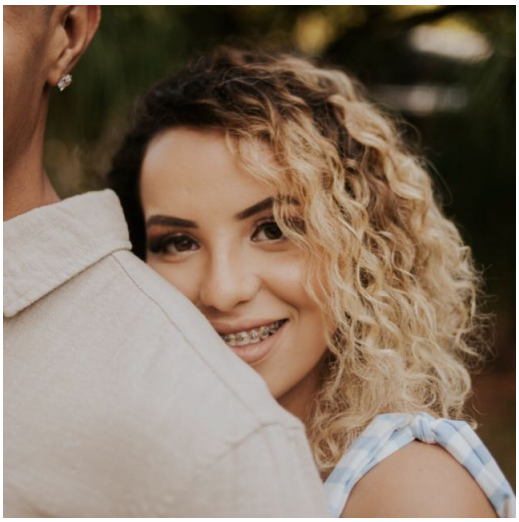


Figura 4.8: Imagem de teste: Maryana (Fonte: Autor)

Em segundo lugar, é feito o processamento da imagem, essa etapa consiste em transformar a imagem bruta em algo mais proveitoso para a análise. Essa fase do processamento de imagem inclui uma vasta diversidade de técnicas, dentre elas a segmentação. Na segmentação o objetivo é separar a imagem em regiões ou objetos significativos. Nesse sentido, os filtros ou detectores de borda são ótimas ferramentas para empregar essa técnica.

Como exemplo, podemos observar a Figura 4.9 que se trata de uma representação da detecção de borda da imagem utilizada como teste desse trabalho. Note que a Figura 4.8 apresenta uma grande quantidade de detalhes visuais, além disso, como qualquer outra imagem, essa apresenta também uma diversidade de cores. Muitas vezes para simplificar a análise reduzimos a imagem em escala de cinza, isso significa que, a imagem colorida será convertida em uma imagem monocromática em que cada pixel irá apresentar uma intensidade de luz, dessa forma, quando o pixel está mais próximo do preto significa baixa intensidade e quanto mais próximo do branco teremos pixels de alta intensidade. Um contorno ou borda são aquelas regiões em que quando fizermos uma varredura pela imagem encontraremos mudanças abruptas de intensidade dos pixels.

Os filtros de borda são algoritmos utilizados em processamento de imagens digitais que buscam detectar as mudanças abruptas de intensidade dos pixels, isto é, a técnica em questão consiste em uma varredura da imagem a fim de identificar as descontinuidades presentes na imagem digital, assim, dessa maneira, podemos realizar uma separação entre fundo e objeto. Essas descontinuidades onde é possível observar as evidentes mudanças de

intensidade dos pixels são chamadas de borda e sua detecção implica no reconhecimento de dados importantes, sobretudo de movimento quando se tratar de uma sequência de dados ou separação entre objeto e fundo [44].

Figura 4.9: Representação visual do filtro de borda sobel aplicado a imagem de teste Maryana (Fonte: Autor)

Em processamento de imagens digitais cada pixel é representado por bits que fornecem tonalidades e intensidades das cores. A técnica de decomposição em *bit-plane* ou planos de bit consiste em apresentar camadas específicas de informação da imagem digital. Nesse sentido, dizemos que os bits mais significativos carregam informações mais importantes enquanto os bits menos significativos carregam as informações de menor relevância. A manipulação de bit-plano permite processar as imagens em diferentes níveis de precisão [42]. Em outras palavras, uma imagem digital pode ser decomposta em planos enumerados, como se fosse possível fatiar a imagem onde em cada fatia teremos bits que carregam consigo informações especificas da imagem. Os planos podem ser enumerados de 0 a 7 onde o plano-0 tem o bit de menor relevância (LSB) e o bit de maior relevância (MSB) é representado pelo plano-7 [40].

Como dito anteriormente, os bits representarão os valores de intensidade das cores dos pixels que são fornecidos, por sua vez, em números decimais, sendo assim, é preciso convertê-los para base binária, tendo em vista a forma que um computador processa os dados. Sendo assim, é possível interpretar a equação (4.1) de modo que $V_i$ é um bit específico em um plano de bits e $P$ é o número decimal que será decomposto. Cada plano representa um bit diferente do LSB ao MSB de todos os pixels da imagem [44].

A técnica de decomposição em planos de bits pode ser representada de forma visual. A Figura 4.8 é a imagem original de teste utilizada nesse trabalho. Geralmente, usamos a imagem em escala de cinza para demonstrar visualmente a decomposição em planos de bits. Fazemos isso, devido a facilidade que possui apenas um canal de cor, as tonalidades se tornam mais simples e eficientes de serem processadas. Por esse motivo a decomposição em planos de bits de imagens em escalas de cinza permite examinar como diferentes níveis de detalhes contribuem para a formação final da imagem.

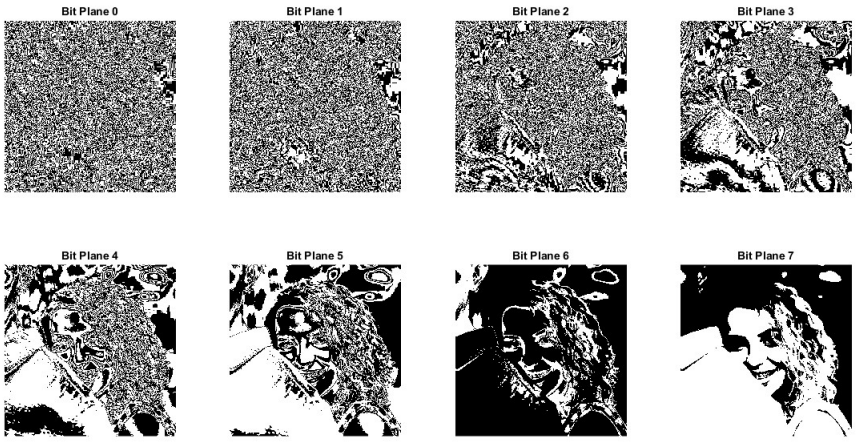



Figura 4.10: Demonstração visual da decomposição em planos de bit da imagem de teste (Fonte: Autor)

Observe pela Figura 4.10 que a imagem muda de nitidez para cada plano representado visualmente. Nesse contexto, vemos claramente a diferença de nitidez da imagem do Bit-plano-0 para o Bit-plano-7. Quanto mais próximo da primeira camada teremos aqueles Bits menos relevantes para a formação da imagem. A diferença de nitidez se dá pelas características dos bits menos significativos, eles apresentam características mais simples e suaves da imagem, por consequência disso, há uma redução dos detalhes finos da imagem. Em contra partida, os detalhes finos, são evidenciados pelos bits mais significativos. Podemos notar isso ao caminhar em direção ao plano-7, uma vez que os bits mais significativos carregam consigo os detalhes mais finos da imagem.

## 4.5 A aplicação do mapa de Hénon na criptografia

Sistemas caóticos apresentam uma propriedade central: a dependência sensível das condições iniciais. Embora essa propriedade seja muitas vezes ligada a complexidade de um problema de difícil solução, é importante analisar os sistemas caóticos por outra perspectiva. Dito isso, exploraremos nessa seção como a propriedade caótica do mapa de Hénon pode ser útil na criptografia.

A aplicação do caos em sistemas caóticos, se mostra, de certa forma, intuitiva, visto que, se um invasor deseja acessar um servidor, regido de alguma forma por um sistema caótico, sem conhecer o sistema e os seus valores de parâmetro, torna-se uma tarefa ainda mais árdua do que tentar apenas "quebrar"uma encriptação. Sob essa perspectiva Baptista [6] explora muito bem a característica caótica do mapa logístico, para aplicação em criptografia. O método proposto consiste em escolher uma condição inicial $x_0$ entre 0 e 1. Em seguida é necessário escolher os valores de parâmetro entre $3,57$ e 4, pois esses são os valores de parâmetro para os quais o mapa logístico apresenta uma dinâmica caótica [6]. É necessário também fixarmos a quantidade de caracteres que serão usados denotado por $S$, então se usarmos um conjunto de 256 caracteres $S = 256$ o mapa logístico deverá associar os caracteres a um intervalo $I$ definido como

$$I = [X_{min} + (i-1)E, X_{min} + iE],$$

onde o intervalo $[X_{max}, X_{min}]$ é uma parte do atrator caótico, deste modo podemos calcular $E$ como $E = (X_{max} - X_{min})/S$ [6].

**Exemplo 4.12.** *Se considerarmos um conjunto de* 256 *caracteres e que* $X_{min} = 0$ *e* $X_{max} = 1$*, temos que* $E = 1/256$*, pois* $S = 256$*. Se considerarmos "a"a primeira letra do conjunto de caracteres, então "h"é a oitava letra. Logo o intervalo que a letra "h"está associada é*

$$I_h = \left[0 + (8-1)\frac{1}{256}, 0 + 8\frac{1}{256}\right) = \left[\frac{7}{256}, \frac{8}{256}\right).$$

O processo de encriptação consiste em escolher um valor inicial $x_0$ que após $(n+1)$ iterações a trajetória atinge o intervalo $I$ de modo que o número inteiro de iterações para que isso ocorra seja o texto cifrado. Note que se escolhermos outra condição inicial de modo que $x_{n+1}$ seja a próxima condição inicial para cifrar outra letra, vamos observar uma trajetória completamente diferente da observada anteriormente devido a propriedade caótica do mapa logístico. Por consequência disso, há uma vantagem crucial no uso desse método: a dependência sensível das condições iniciais possibilita uma vasta diversidade de cifras. Nesse contexto, é viável pensar que o mapa de Hénon seja um sistema caótico promissor na aplicação em criptografia. De fato, a literatura sustenta essa suspeita, sobretudo, quando se trata de criptografia de imagens. Em [34] foi desenvolvido uma técnica que combina o algoritmo de marca d'agua com o mapa de Hénon para proteger imagens médicas. Sukirman No trabalho [50] é utilizado o mapa de Hénon para gerar números pseudo-aleatórios e com base nesses números é desenvolvido o algoritmo de encriptação. Os pesquisadores de [37], utilizam chaves de 128 bits combinados com o mapa de Hénon para embaralhar os pixels de imagens digitais. Esses trabalhos são apenas alguns exemplos dentre uma vastidão de estudos do mapa de Hénon aplicado a criptografia. Vale ressaltar, que apesar da abundância de estudos que podemos levantar da literatura ainda há limitações em alguns algoritmos propostos [50] isso nos motiva estudar e reproduzí-los para fornecer novas contribuições.

De acordo com os trabalhos citados anteriormente podemos observar que mapas caóticos podem ser promissores para a aplicação em criptografia, em especial o mapa de Hénon para a criptografia de imagens. Além da dependência sensível das condições iniciais, é interessante o uso do mapa de Hénon em criptografia devido a sua simplicidade para gerar sequências caóticas que culmina em um baixo custo computacional [43]. No trablho [43] é proposto um método de criptografia de imagens que será reproduzido nesta seção.

Como visto anteriormente, nota-se que o mapa de Hénon apresenta uma dinâmica caótica com atrator estranho para os valores de parâmetro $a = 1,4$ e $b = 0,3$, vale ressaltar, que para esses valores o mapa de Hénon apresenta uma dinâmica caótica que já foi explorada nas seções 3.7, 3.6 e 3.5. Para reproduzir o experimento será utilizado um computador pessoal com processador Intel Core(TM) i5 1.60GHz e memória RAM de 8GB com sistema operacional Windows11 64 bits. Todo o experimento será realizado no ambiente MATLAB2024a. Vamos utilizar a Figura 4.8 como teste de criptografia.

De início, iremos criar a sequência caótica utilizando como condição incial $(x_0, y_0) = (0, 0)$. A sequência gerada deve ser convertida para uma matriz binária $I_{binmat}$ de tamanho $V \times V$, de modo que a imagem que será definida pela matriz intensidade, seja:

$$M = \{(P_{ij}) : 0 < i \leq V, 0 < j \leq V, \forall\ i, j \in \mathbb{N}\}.$$

Note que, a imagem deve ter o mesmo tamanho da matriz $I_{binmat}$, desse modo, como a imagem utilizada tem 640 pixels, então a sequência caótica deverá ter 409600 elementos. A imagem utilizada como teste é colocada em escala de cinza, e assim a matriz $I_{binmat}$ é utilizada para permutar os elementos $P_{ij}$ da matriz de pixels, gerando uma imagem embaralhada. Para permutar a imagem fazemos a normalização da sequência $x_n$ de 0 a 1, e os novos dados são multiplicados por 409599 e somamos 1, isto é, a nova sequência

gerada é dado por $Seq_i = x_{nor} \times 409599 + 1$ e assim os números inteiros gerados, irão ditar as novas posições dos pixels.

**Exemplo 4.13.** *Para exemplificar, vamos permutar uma matriz* $3 \times 3$. *Tendo em vista, a ordem da matriz, podemos observar que essa matriz tem 9 elementos, assim a sequência caótica gerada pelo mapa de Hénon deve conter nove elementos. Se considerarmos as condições iniciais* $(x_0, y_0) = (0, 0)$ *iremos gerar uma sequência* $R_{eq} = \{x_n\}$, *onde*

$$R_{eq} = (0.0000, 1.0000, -0.4000, 1.0760, -0.7409, 0.5543, 0.3476, 0.9972, -0.2879).$$

*Vamos agora normalizar a sequência de* 0 *a* 1, *onde o elemento normalizado é dado por* $x_{nor}$, *em que*

$$x_{nor} = \frac{x - min(x)}{max(x) - min(x)}$$

*para* $x_1 = 0$, *obtemos* $x_{nor} = \frac{0+0.7409}{1.076+0.7409} = 0.4078$. *Faremos a normalização para todos os pontos, e para cada* $x$ *normalizado iremos fazer* $x_{nor} \times 8 + 1$ *obtendo a nova sequência*

$$Seq = (4.2622, 8.6654, 2.5010, 9.0000, 1.0000, 6.7030, 5.7925, 8.6530, 2.9947)$$

*Suponha que a matriz* $A_{3\times3}$ *de entrada seja definida por*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix},$$

*então vamos considerar as posições dos elementos da matriz de 1 a 9 da esquerda para direita. Iremos permutar a matriz primeiro olhando as partes inteiras da sequência caótica. Caso haja repetições de elementos iremos utilizar as casas decimais. Sendo assim, o primeiro elemento da matriz A irá para quarta posição, o segundo para oitava posição e assim sucessivamente. Note que, o oitavo elemento iria permanecer na oitava posição que já está sendo ocupado, então partiremos para as casas decimais. Pela primeira casa o elemento iria para sexta posição que também está ocupada, então iremos para próxima até encontrar uma posição desocupada. Assim a matriz A permutada ficará da seguinte forma:*

$$\begin{pmatrix} 5 & 3 & 8 \\ 1 & 7 & 6 \\ 9 & 2 & 4 \end{pmatrix}$$

.

O Exemplo 4.13 descreve uma simplificação do que foi feito para permutar a matriz de pixels. Vale ressaltar, que a solução para pixels sobrepostos apresentada no Exemplo 4.13 não foi utilizada no processo de encriptação. A utilização desse método consiste em identificar a possibilidade de sobreposição, e assim, considerar os próximos algarismos. Mesmo que o processo apresente a sobreposição de pixel realizamos as simulações para constatar que não há outros problemas no processo.

Figura 4.11: Imagem reconstruída com sobreposição de pixels (Fonte: Autor)

O problema de superposição de pixels foi notado logo nas primeiras simulações. A Figura 4.11 demonstra a imagem com sobreposição de pixels reconstruída. Podemos notar que a imagem não é reconstruída por inteiro e ainda claramente há perda de informações referente a pixels sobrepostos.

Após embaralhar a imagem podemos dividir o processo de encriptação em duas partes que acontecem de forma simutânea: na primeira parte iremos decompor a imagem embaralhada em planos de bits e na segunda vamos aplicar um filtro de contorno e em seguida também iremos decompor o resultado em planos de bit.

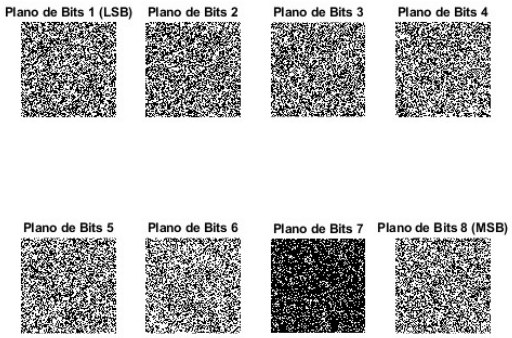



Figura 4.12: Decomposição em planos de bit da imagem permutada pela sequência caótica (Fonte: Autor)

Para gerar os planos de borda iremos aplicar o filtro de borda na matriz permutada alterando assim o limiar de detecção de mudanças abruptas na intensidade dos pixels, isto é, esse processo irá influenciar na detecção de bordas feita pelo operador utilizado. Após gerar a imagem resultante com aplicação do filtro borda vamos decompor essa imagem também será decomposta em planos de bits.

Uma vez obtida a imagem permutada em planos de bits e os planos de borda podemos aplicar uma operação XOR para finalmente obtermos a imagem encriptada. Os planos de bits são combinados com os planos de borda pela operação XOR, isso significa que se $P_i$ é o i-ésimo pixel da imagem permutada e $K_i$ o i-ésimo plano de borda, então $C_i$ é o

i-ésimo plano cifrado de modo que

$$C_i = P_i \oplus K_i.$$

Essa operação combina os dados da imagem permutada com os dados do plano de borda gerando a imagem final encriptada. Os planos de borda encriptam a imagem separadamente, nesse sentido os planos de borda também poderão ser chamados de chave. Para decriptar a imagem e obter o texto plano é necessário utilizar os mesmos parâmetros e condições iniciais para o mapa de Hénon e também deve utilizar o mesmo operador de bordas, visto que esse processo está intimamente ligado a geração de chave do criptossistema. Dessa forma, a sequência caótica deve ser utilizada para reverter a permutação e em seguida decompondo a imagem resultante em planos de bit iremos recombinar com os planos de borda por meio da função XOR, resultando na imagem original.

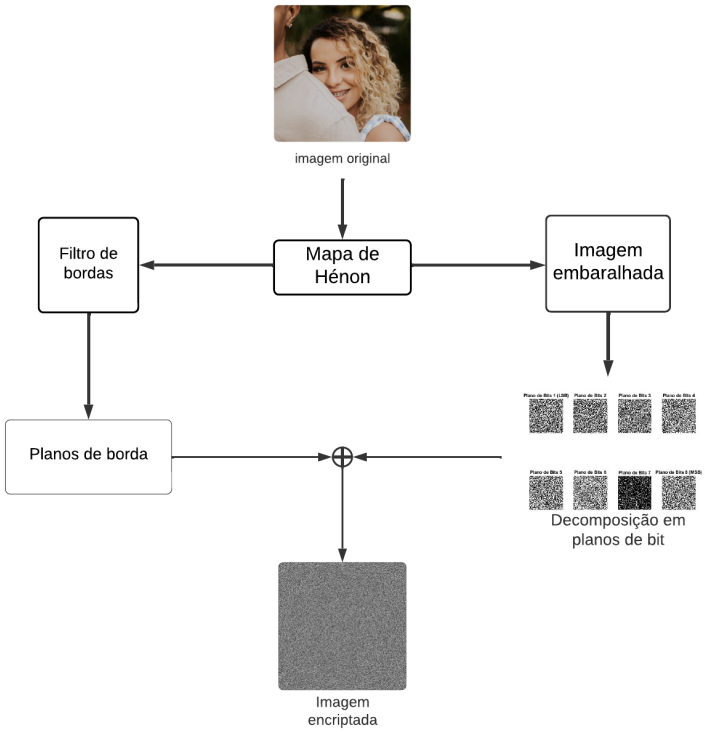



Figura 4.13: Diagrama do processo de encriptação (Fonte: Autor)

Do ponto de vista geral, podemos observar que o algoritmo possui abertura para o uso de diferentes filtros de borda. Vale ressaltar também que o algoritmo tem uma vantagem importante que é o uso do caos para gerar uma sequência pseudo-aleatória que tem um papel importante na encriptação. Nesse contexto, podemos notar que o processo independe do mapa de Hénon, mas uma pergunta surge naturalmente: o custo computacional depende de alguma forma do filtro de borda? A fim de responder a essa pergunta simulamos o tempo de processamento de encriptação pra quatro operadores de filtro de bordas diferentes. O primeiro filtro de borda utilizado foi o operador Sobel, essa técnica consiste em utilizar operadores diferenciais de primeira e segunda ordem para ressaltar contornos das bordas e também as variações indesejadas na intensidade dos pixels da imagem que é chamado de ruído [9]. O segundo operador testado foi o operador Prewitt, o operador calcula o gradiente da imagem em cada ponto resultando

no maior aumento possível do claro para o escuro resultando como os pixels se alteram de forma abrupta indicando assim as bordas da imagem [10]. O terceiro operador testado é o Robertcross, esse operador aproxima o gradiente da imagem por meio de uma função discreta obtida pelos pixels diagonais da imagem [14]. Por fim, fizemos uma simulação com o operador Canny. Esse filtro de borda consiste em suavizar a imagem por meio de uma função Gaussiana em seguida determina os gradientes de intensidade da imagem, diante disso, o algoritmo é capaz de detectar as bordas [9]. Nesse contexto é importante salientar que esses filtros de imagem envolvem maior complexidade do que o descrito anteriormente. Como nosso objetivo não é um aprofundamento nessas técnicas de detecção de borda não iremos incluir mais detalhes desses operadores.

| Operadores | Tempo de execução ($ms$) |
|---|---|
| Canny | 288 |
| Prewitt | 74 |
| Robertcross | 99 |
| Sobel | 71 |

Tabela 4.3: Tabela de tempos de execução do algoritmo de encriptação

Por meio das medições de tempo de execução obtida expostas na Tabela 4.3, podemos observar que o tempo de maior discrepância é apresentada pelo operador Canny. O operador Prewitt e Sobel tem os tempos de execução mais próximos $74ms$ e $71ms$ respectivamente. Essa diferença de tempo, mesmo que pequena, pode estar relacionado com a complexidade e eficácia de cada algoritmo. Como o número de iterações do mapa de Hénon depende do tamanho da imagem de entrada o tempo de execução das iterações independem do mapa de Hénon. Isso nos leva a questionar se o algoritmo possui de fato, eficácia computacional para todos operadores independe do tamanho da imagem de entrada. Além disso, se o custo computacional depende dos operadores de borda é necessário entender, qual dos operadores seria a combinação ideal com o mapa de Hénon para obter o menor custo computacional com a maior segurança possível contra invasões.

Capítulo

# 5

# Considerações finais

O estudo dos sistemas dinâmicos se faz importante devido a variedade de aplicações concretas que essa área da matemática pode ter. Além disso, o estudo de problemas de outras áreas como a Física, Economia e Biologia faz com que se torne ainda mais conivente o seu estudo, haja visto, que muitas vezes os problemas dessa área são modelados por sistemas dinâmicos. Nesse sentido, quando analisamos avanços no estudo desses sistemas podemos nos deparar com propriedades que valem ser estudadas como a não linearidade e o caos.

O mapa de Hénon é um sistema dinâmico bidimensional que é amplamente estudado na literatura, tal mapa apresenta as duas propriedades citadas no parágrafo anterior: o caos e a não linearidade. Vale ressaltar, que o mapa de Hénon é uma simplificação das seções de Poincaré para o sistema de Lorenz, que também consiste em um sistema caótico. Embora, o caos seja a propriedade do mapa de Hénon que chame mais atenção, existem outras propriedades importantes desse sistema dinâmico.

O determinante do jacobiano é um número real negativo, que culmina na contração de área, isso significa que as soluções são comprimidas em uma região do espaço. Além disso, trata-se de um mapa injetivo e invertível, no qual pode culminar em aplicações interessantes em uma diversidade de sistemas. A injetividade e a inveritibilidade permite com que possamos prosseguir e voltar no tempo, em vista de que podemos estabelecer uma relação entre iterações anteriores e posteriores no sistem. Nesse sentido, é possivel obter informações centrais de um modelo ou sistema.

Embora não tenhamos demonstrado analiticamente que o mapa de Hénon é um sistema caótico, os experimentos computacionais realizados demonstram que, de fato, trata-se de um sistema caótico. Podemos observar a presença de um atrator estranho que tem dependência sensível das condições iniciais, e ainda, pelo diagrama de bifurcação podemos observar, para quais valores de parâmetro de bifurcação o mapa de Hénon demonstra ser um sistema caótico. Nesse sentido, observamos o crescimento de aparições de pontos periódicos que emergem conforme o parâmetro $a$ aumenta. À vista disso, o trabalho desenvolvido por Feigenbaum quanto ao estudo das bifurcações nos ajuda a compreender ainda mais sobre dinâmica das bifurcações.

O atrator estranho que surge ao iterarmos o mapa caótico de Hénon demonstra uma geometria fractal. Essa propriedade foi observada ao estudar a ampliação do atrator que também é apresentado por Peitgen, 2003 [41]. A análise demonstrou que a auto-semelhança surge da ampliação do atrator de Hénon pertence à família de um conjunto de Cantor. O que torna possível determinar as dimensões fracionadas do mapa de Hénon. Essa propriedade era de certa forma esperada, uma vez que geralmente sistemas dinâmicos que apresentam atrator estranho e também apresentam auto-semelhança.

O fato de que o mapa de Hénon apresenta a propriedade de dependência sensível das condições inicias nos levou a considerar utilizar esse sistema dinâmico em aplicações para a criptografia. Esse sistema pode gerar caminhos completamente diferentes com uma pequena mudança nas condições iniciais, fazendo com que o mapa de Hénon seja promissor em gerar sequências pseudo-aleatórias tornando ascendente o êxito em sua aplicação na criptografia. O fato do mapa de Hénon ser amplamente estudado para processamento de imagens digitais nos fez levantar a hipótese de que o mesmo seria auspicioso para cifrar imagens. E de fato, o algoritmo proposto por Rathore, 2021 [43] e reproduzido nesse trabalho, se mostrou um instrumento valioso para a encriptação de imagens.

O algoritmo consiste em um processo de combinação da permutação da matriz de pixels com técnicas de processamento de imagem, como a decomposição em planos de bits e filtros de contorno. Vale ressaltar, que a permutação de pixels por uma sequência caótica gerada pelo mapa de Hénon é o suficiente para embaralhar os pixels e obter uma imagem cifrada, assim a sequência caótica gerada funcionaria como chave, de tal forma que a mesma sequência também indicará o processo inverso que irá reconstruir a imagem. Obtemos dessa forma, um criptossistema de chave privada. O algoritmo proposto por Rathore tem como um dos passos de encriptação a permutação por sequência caótica, entretanto não há especificação de um método para corrigir a sobreposição de pixels no momento da permutação da imagem. É importante atentar-se a esse problema, porque, a sobreposição de pixels pode comprometer a fase de decriptação, uma vez, que a sobreposição, nesse caso, pode acarretar em perdas de informação. Existem algumas maneiras de corrigir esse problema uma forma é combinar o mapa de Hénon com algoritmos de embaralhamento: os pixels de sobreposição são separados e rearranjados por um algoritmo de embaralhamento para posições que não estão ocupadas; completando assim, a permutação dos pixels. Nós mantemos a permutação apenas pela sequência caótica fazendo com que os pixels fossem sobrepostos. Embora a solução da sobreposição de elementos apresentada no Exemplo 4.13 tenha resolvido o problema para a matriz $3 \times 3$, não temos ainda é inconclusivo se é possível generalizar esse método para todas situações possíveis.

De fato, o algoritmo estudado funciona, e é aparentemente um algoritmo simples, no entanto, é importante notar que podemos utilizar uma variedade extensa de filtros de borda nesse tipo de algoritmo. Isto posto, fizemos um teste simples de tempo de execução, que seja, possível obtermos uma ideia do custo computacional do algoritmo para diferentes filtros de borda. Embora, os resultados apontam para operador Sobel como menor tempo de execução, acaba sendo inconclusivo se o algoritmo com essa combinação, é de fato, eficaz. É necessário, nesse sentido, analisar as deficiências dos algoritmos causado por diferentes planos borda. Diante disso, poderemos finalmente analisar qual comportamento dos tempos de execução em função do tamanho da imagem de entrada, podendo por fim, atestar a sua eficácia.

Em síntese, o mapa de Hénon é muito rico em termos de estudos teóricos e ainda pode ser usado para modelar uma diversidade de situações, inclusive na criptografia, como apresentamos nesse trabalho. Os estudos sobre esse tema não são escassos, mas ainda existem questões a serem respondidas. As combinações de algoritmos de encriptação por sequências caóticas combinadas com algoritmos de embaralhamento de pixels, pode também ser promissor para resolver o problema de sobreposição de pixels. Além disso, há abertura para se estudar outros filtros de bordas ou combinar esse algoritmo com outras técnicas de processamento de imagens digitais. envolva mapas caóticos.

# Referências


[1] Luis A Aguirre, Christophe Letellier, et al. Modeling nonlinear dynamics and chaos: A review. *Mathematical Problems in Engineering*, 2009, 2009.

[2] Wadia Faid Hassan Al-Shameri. Dynamical properties of the hénon mapping. *Int. Journal of Math. Analysis*, 6(49):2419–2430, 2012.

[3] Kathleen T Alligood, Tim D Sauer, James A Yorke, and David Chillingworth. Chaos: an introduction to dynamical systems. *SIAM Review*, 40(3):732–732, 1998.

[4] Sally Andria and Rodrigo Gondim. Introdução à criptografia com curvas elípticas.

[5] Claudia V Angelelli. Los hablantes del código navajo: estrategias de traducción, interpretación y encriptación. 2011.

[6] MS Baptista. Cryptography with chaos. *Physics letters A*, 240(1-2):50–54, 1998.

[7] Luis Barreira and Claudia Valls. Equações diferenciais ordinárias: teoria qualitativa. *São Paulo: Livraria da Física*, 2012.

[8] Vinicius S Borges and Marcio Eisencraft. Um estudo numérico do exponente de lyapunov do mapa hénon com filtro fir.

[9] John Canny. A computational approach to edge detection. *IEEE Transactions on pattern analysis and machine intelligence*, (6):679–698, 1986.

[10] Girish N Chaple, RD Daruwala, and Manoj S Gofane. Comparisions of robert, prewitt, sobel operator based edge detection methods for real time uses on fpga. In *2015 international conference on technologies for sustainable development (ICTSD)*, pages 1–4. IEEE, 2015.

[11] B Cooper. The schwarzian derivative in one-dimensional dynamics. *The University of Chicago Mathematics REU*, 2020.

[12] Jacob Daghlian. *Lógica e álgebra de Boole* . Editora Atlas SA, 2000.

[13] AM Davie and TK Dutta. Period-doubling in two-parameter families. *Physica D: Nonlinear Phenomena*, 64(4):345–354, 1993.

[14] Larry S Davis. A survey of edge detection techniques. *Computer graphics and image processing*, 4(3):248–270, 1975.

[15] José Eustáquio Rangel de Queiroz and Herman Martins Gomes. Introdução ao processamento digital de imagens. *Rita*, 13(2):11–42, 2006.

[16] Robert L Devaney. *A first course in chaotic dynamical systems: theory and experiment*. CRC Press, 2018.

[17] Claus Ivo Doering and Artur O Lopes. *Equações diferenciais ordinárias*. Number 517.2 DOE. 2008.

[18] Hygino Hugueros Domingues. *Espaços métricos e introdução à topologia*. Atual, 1982.

[19] Saber N Elaydi. *Discrete chaos: with applications in science and engineering*. Chapman and Hall/CRC, 2007.

[20] Mitchell J Feigenbaum. Quantitative universality for a class of nonlinear transformations. *Journal of statistical physics*, 19(1):25–52, 1978.

[21] Mitchell J Feigenbaum. Universal behavior in nonlinear systems. *Universality in chaos*, pages 49–84, 1980.

[22] Fernanda A Ferreira. Dinâmica simbólica e ferradura de smale. *Tékhne: Revista de Estudos Politécnicos*, pages 183–199, 2007.

[23] Xiaohong Gao. A color image encryption algorithm based on an improved hénon map. *Physica scripta*, 96(6):065203, 2021.

[24] Marco Giunti and Claudio Mazzola. Dynamical systems on monoids: Toward a general theory of deterministic systems and motion. In *Methods, models, simulations and approaches towards a general theory of change*, pages 173–185. World Scientific, 2012.

[25] P Grassberger. On the fractal dimension of the henon attractor. *Physics Letters A*, 97(6):224–226, 1983.

[26] Michel Hénon. A two-dimensional mapping with a strange attractor. *The theory of chaotic attractors*, pages 94–102, 2004.

[27] Nina ST Hirata. Notas de aula de mac0329–álgebra booleana e aplicações. *São Paulo: USP*, 2004.

[28] Philip Holmes. Poincaré, celestial mechanics, dynamical-systems theory and "chaos". *Physics Reports*, 193(3):137–163, 1990.

[29] GC Layek et al. *An introduction to dynamical systems and chaos*, volume 449. Springer, 2015.

[30] John M Lee. Introduction to smooth manifolds, 2003.

[31] Rafael Pinheiro Leite. Aritmética de números binários e suas relações com circuitos lógicos. 2020.

[32] Alexandre Luis Magalhães Levada. Fundamentos de lógica matemática. 2017.

[33] Douglas A Lind, Douglas Lind, and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge university press, 2021.

[34] Jing Liu, Jingbing Li, Jixin Ma, Naveed Sadiq, Uzair Aslam Bhatti, and Yang Ai. A robust multi-watermarking algorithm for medical images based on dtcwt-dct and henon map. *Applied Sciences*, 9(4):700, 2019.

[35] Edward N Lorenz. Deterministic nonperiodic flow. *Journal of atmospheric sciences*, 20(2):130–141, 1963.

[36] Rick Miranda and Emily Stone. The proto-lorenz system. *Physics Letters A*, 178(1-2):105–113, 1993.

[37] Kapil Mishra and Ravi Saharan. A fast image encryption technique using henon chaotic map. In *Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2017, Volume 1*, pages 329–339. Springer, 2019.

[38] EJ Moulton. H. goldstein, classical mechanics. 1952.

[39] Krerley Oliveira and Marcelo Viana. Fundamentos da teoria ergódica. *IMPA, Brazil*, 2014.

[40] Bilgi Özdemir and Nurettin Doğan. Data hiding to the image with bit plane slicing and double xor. *MANAS Journal of Engineering*, 10(1):66–72, 2022.

[41] Heinz-Otto Peitgen, Hartmut Jürgens, Dietmar Saupe, and Mitchell J Feigenbaum. *Chaos and fractals: new frontiers of science*, volume 106. Springer, 2004.

[42] Ram Ratan and Arvind Yadav. Security analysis of bit-plane level image encryption schemes. *Defence Science Journal*, 71(2), 2021.

[43] Vandana Rathore and Arup Kumar Pal. An image encryption scheme in bit plane content using henon map based generated edge map. *Multimedia Tools and Applications*, 80(14):22275–22300, 2021.

[44] Vandana Rathore and Arup Kumar Pal. An image encryption scheme in bit plane content using henon map based generated edge map. *Multimedia Tools and Applications*, 80(14):22275–22300, 2021.

[45] Nicholas Record. Introduction to lorenz's system of equations, 2003.

[46] Clark Robinson. *Dynamical systems: stability, symbolic dynamics, and chaos*. CRC press, 1998.

[47] Hemanta Kr Sarmah and Ranu Paul. Period doubling route to chaos in a two parameter invertible map with constant jacobian. *Int J Res Rev Appl Sci*, 3(1):72–82, 2010.

[48] Colin Sparrow. *The Lorenz equations: bifurcations, chaos, and strange attractors*, volume 41. Springer Science & Business Media, 2012.

[49] Steven H Strogatz. *Nonlinear dynamics and chaos*. 1996.

[50] Edi Sukirman, MT Suryadi, and M Agus Mubarak. The implementation of henon map algorithm for digital image encryption. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 12(3):651–656, 2014.

[51] Stephen T Thornton and Jerry B Marion. *Classical dynamics of particles and systems*. Cengage Learning, 2021.