Faculdade de Ciências da
Universidade de Lisboa

Sistemas Dinâmicos

Projecto Final

Dinâmica do Mapa Discreto do Gato de Arnold

Autor:
Cláudio Santos
Nº 42208

19 de Junho de 2017

Resumo

Um sistema dinâmico discreto conhecido como o mapa discreto do gato de Arnold é dado por:

$$\begin{bmatrix} x_{t+1} \\ y_{t+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_t \\ y_t \end{bmatrix} \pmod{N},$$

que actua numa rede quadrada dois dimensional de tamanho $N \times N$. A característica fundamental deste mapa é a propriedade de quando uma rede $N \times N$ é uma imagem cujos os pixéis têm coordenadas (x, y), o mapa baralha a imagem a cada iteração. Depois de um número finito de iterações, a imagem é recuperada à sua forma e ordem originais.

O objectivo deste projecto é explorar as propriedades dinâmicas do mapa discreto do gato de Arnold, um mapa simples que exibe um elevado nível de caos. São apresentados resultados numéricos sobre os periodos mínimos, o comprimento de periodo e as órbitas disjuntas do mapa discreto do gato de Arnold. Aborda-se também generalizações do mapa do gato de Arnold e no final são apresentados algumas aplicações do mapa discreto do gato de Arnold.

Conteúdo

1 Introdução

Considere um recipiente com uma determinada quantidade de café. De seguida, adicione a mesma quantidade de leite e misture ambos sempre com o mesmo movimento. Certamente ninguém pensaria que o café e o leite vão separar-se e aparecer nos seus estados originais após um certo número de misturas. E também não ia passar pela cabeça que nalgum ponto intermédio no tempo ter-se-ia subitamente uma mistura de café e leite como de um tabuleiro de xadrez se tratasse. Contudo é esta a consequência do *Teorema de Recurrência de Poincaré*: que alguns destes objectos matemáticos denominados de *sistemas dinâmicos*, após um tempo suficientemente longo mas finito, regressam a um estado muito próximo do seu estado inicial.

O mapa do gato de Arnold é provalvemente a transformação mais simples que exibe esta propriedade bem como um elevado nível de caos. O mapa deve o seu nome a Vladimir I. Arnold que utilizou a imagem de um gato antes e depois da aplicação do mapa. Este mapa serviu como guia no desenvolvimento da teoria de sistemas dinâmicos para ilustrar novos conceitos como entropia (Sinai 1959) e partições de Markov (Adler & Weiss 1967).

Uma imagem é composta por unidades discretas chamadas pixéis. Um pixel é um pequeno quadrado que representa um código de cor e quando se toma em conjunto todos os pixeís, forma-se um mosaico que é a imagem. A imagem é uma matriz $M \times N$, onde M representa o número de linhas dos pixéis e N o número de colunas dos pixéis. Cada entrada da matriz é um valor numérico que representa uma dada cor. Como exemplo considere a imagem 212×212 abaixo:

Figura 1.1: Fotografia de M&M's.

Seja a imagem a matriz X e pode examinar-se as entradas numéricas de X que representam um certo código de cor.

$$X = \begin{bmatrix} 139 & 70 & 77 & \cdots & 255 & 245 & 239 \\ 100 & 74 & 74 & \cdots & 254 & 253 & 251 \\ 98 & 159 & 156 & \cdots & 253 & 255 & 255 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 193 & 175 & 161 & \cdots & 220 & 220 & 220 \\ 219 & 181 & 156 & \cdots & 220 & 219 & 220 \\ 219 & 176 & 156 & \cdots & 218 & 219 & 219 \end{bmatrix}$$

Uma iteração do mapa do gato de Arnold é o efeito da multiplicação de todas as coordenadas do pixéis pela matriz $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right]$. Depois todos os valores são tomados com módulo igual ao lado da imagem. A imagem é por assim dizer esticada e depois dobrada de forma a caber nas fronteiras do quadrado original. Contudo, se iterado vezes suficiente, como se por magia, a imagem original reaparece.

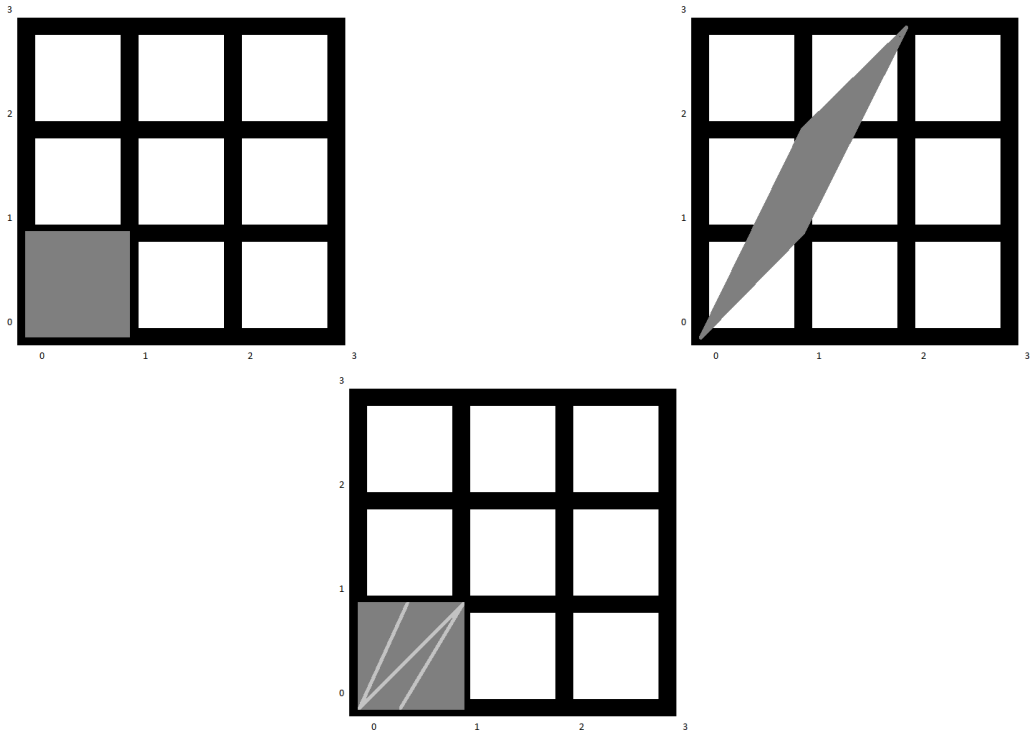


Figura 1.2: lustração geométrica de uma iteração do mapa do gato de Arnold.

2 Definição do Mapa do Gato de Arnold

O mapa do gato de Arnold é o mapeamento num toro dois dimensional. O toro $\mathbb{T}^2$, que topologicamente tem a forma de um *donut*, pode ser definido como os pontos no plano $\mathbb{R}^2$ módulo translações inteiras em $\mathbb{Z}^2$. Isto resulta na representação de $\mathbb{T}^2$ como a família de espaços $\mathbb{R}^2/\mathbb{Z}^2 := \{x+\mathbb{Z}^2 : x \in \mathbb{R}^2\}$. O mapa do gato é agora um mapeamento $\Gamma_{cat} : \mathbb{T}^2 \to \mathbb{T}^2$ definido por $x \mapsto Ax \pmod{\mathbb{Z}^2}$, onde:

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \qquad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

desde que $a, b, c, d \in \mathbb{Z}$ sejam escolhidos tal que:

1. $|\det(A)| = 1$;
2. A tenha valores próprios $|\lambda_{\pm}| \neq 1$

A propriedade (1.) implica que o mapa preserva a área e a orientação (como observado na Figura 1.2) e a propriedade (2.) implica que os valores próprios são reais e distintos. Mapas com estas propriedades são conhecidos na literatura como *automorfismo torais*.

A matriz A estudada neste projecto é

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

e por isso o sistema dinâmico discreto induzido pelo mapa do gato de Arnold é

$$\Gamma_{cat}\left(\begin{bmatrix} x_{t+1} \\ y_{t+1} \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_t \\ y_t \end{bmatrix} \pmod 1$$

Para uma imagem com coordenadas racionais $0 \leq \frac{x}{N}, \frac{y}{N} < 1$ o escalamento da imagem torna possível trabalhar com coordenadas inteiras $0 \leq x, y < N-1$. Isto obriga a usar módulo N em vez de módulo 1 e define-se o mapa discreto do gato de Arnold $\Gamma_A : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$ que é

$$\Gamma_A\left(\begin{bmatrix} x_{t+1} \\ y_{t+1} \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_t \\ y_t \end{bmatrix} \pmod N$$

Seja Φ a transição das coordenadas racionais no intervalo $[0,1[$ para as coordenadas inteiras $(0,1,2,\ldots,N-1)$, tem-se o seguinte diagrama comutativo

$$\begin{array}{ccc} \mathbb{T}^2 & \xrightarrow{\Gamma_{cat}} & \mathbb{T}^2 \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\Phi} \\ \mathbb{Z}_N \times \mathbb{Z}_N & \xrightarrow{\Gamma_A} & \mathbb{Z}_N \times \mathbb{Z}_N \end{array}$$

O *polinómio característico* da matriz A é

$$\lambda^2 - \mathrm{Tr}(A)\lambda + \det(A) = \lambda^2 - 3\lambda + 1$$

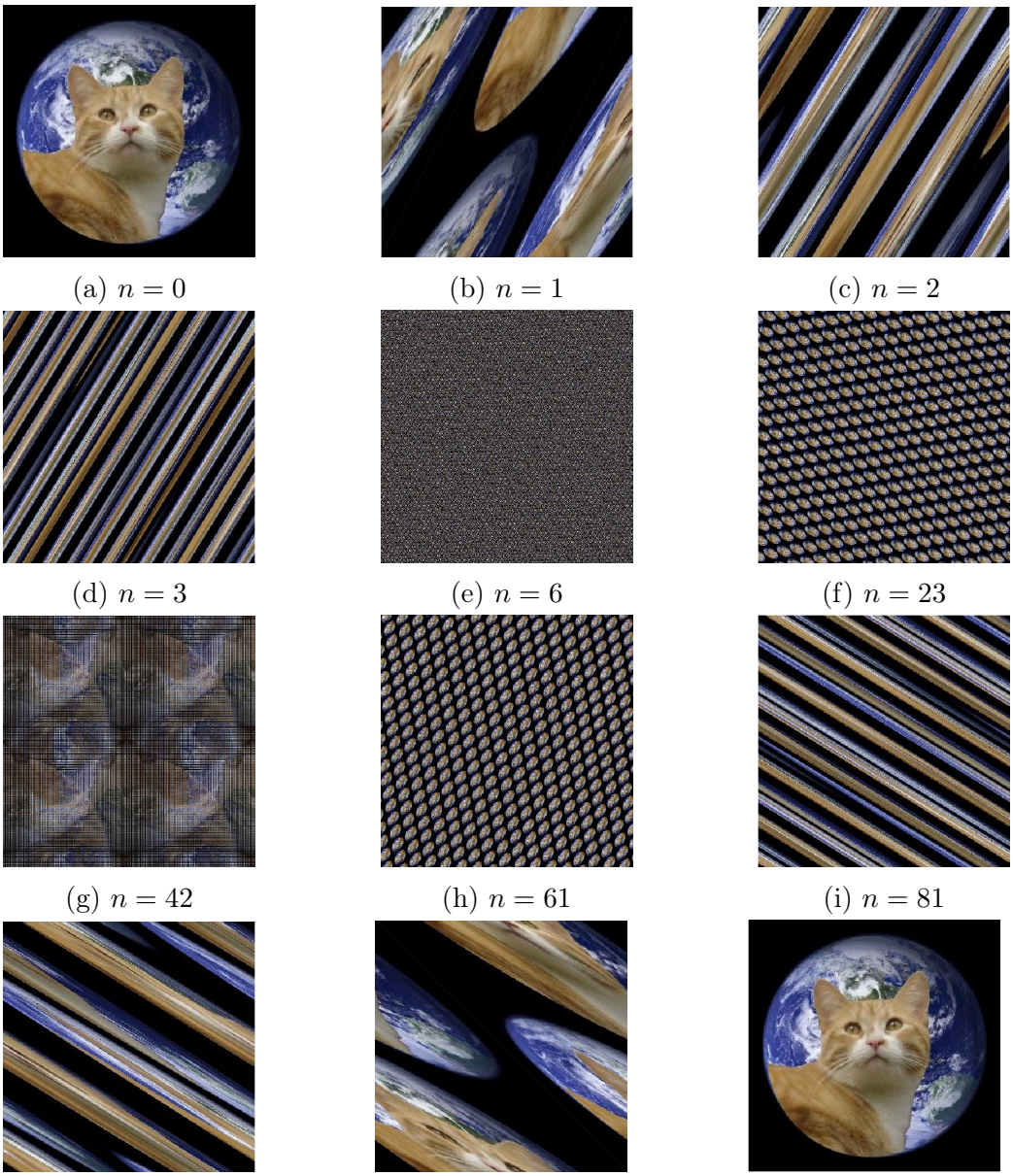
e os dois valores próprios da matriz A (as raízes do polinómio característico) são $\lambda_1 = \frac{3+\sqrt{5}}{2} \approx 2,61803$ e $\lambda_2 = \frac{3-\sqrt{5}}{2} \approx 0,38167$. Como os dois valores próprios de A são diferentes da unidade, o mapa $\Gamma_{cat} : \mathbb{T}^2 \to \mathbb{T}^2$ é um *automorfismo toral hiperbólico*. Por outro lado os dois vectores próprios de A são ortogonais pois a matriz é simétrica.

Para mostrar que o sistema dinâmico discreto referente ao mapa do gato de Arnold segue o Teorema de Recurrência de Poincaré e, por isso, ser periódico leva à seguintes definição.

Definição 2.1. O *periodo mínimo* do mapa discreto do gato de Arnold é o inteiro positivo n mais pequeno tal que $A^n = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \pmod N$ (matriz identidade). Define-se por $\Pi_A(N)$ o periodo mínimo do mapa discreto do gato de Arnold módulo N.

Exemplo 2.2. Da Figura 2.3 conclui-se que $\Pi_A(332) = 84$, ou seja não existe um inteiro positivo menor do que $n = 84$ tal que a imagem original reaparece.

Notar que com apenas $n = 6$ (2.3e iterações a imagem é uma *chuva* de pixéis sem quaisquer características que a relacionem à imagem original. Daí uma das aplicações do mapa do gato de Arnold ser a encriptação (ver secção 5). Os casos 2.3f, 2.3g e 2.3h, conhecidos como miniaturas e fantasmas, são analisados na secção 4.5.



(a) $n = 0$ (b) $n = 1$ (c) $n = 2$

(d) $n = 3$ (e) $n = 6$ (f) $n = 23$

(g) $n = 42$ (h) $n = 61$ (i) $n = 81$

(j) $n = 82$ (k) $n = 83$ (l) $n = 84$

Figura 2.3: O efeito do mapa do gato de Arnold numa imagem de 332×332 pixéis após n iterações.

3 Conexão entre o Mapa do Gato de Arnold e a sequência de Fibonnaci

Definição 3.1. Seja n o número da *sequência de Fibonacci* definido pela relação de recorrência $F_n = F_{n-1} + F_{n-2}$, com $F_1 = 1$ e $F_0 = 0$.

Os primeiros números de Fibonacci são $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

A sequência de Fibonacci pode ser encontrada em vários contextos desde o triângulo de Pascal a situações reais, como a forma de uma concha ou a reprodução de coelhos.

Potências da matriz $F = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} F_0 & F_1 \\ F_1 & F_2 \end{smallmatrix}\right]$ geram números da sequência de Fibonacci

$$F^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}$$

Muitas vezes a matriz F é chamada do *mapa dourado* devido a relação dos números de Fibonacci com o número de ouro. O número de ouro é o limite da razão de dois números sucessivos da sequência de Fibonacci e também é igual ao maior valor próprio de F.

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \phi = \frac{1+\sqrt{5}}{2} \approx 1,61803\ldots$$

Como F e A têm a relação

$$F^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = A$$

os números de Fibonacci também aparecem quando se toma potências da matrix A

$$A^n = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^n = \begin{bmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{bmatrix}$$

com as primeiras potências de A

$$A^2 = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 5 & 8 \\ 8 & 13 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 13 & 21 \\ 21 & 34 \end{bmatrix}, \quad A^5 = \begin{bmatrix} 34 & 55 \\ 55 & 89 \end{bmatrix}, \quad \ldots$$

Da definição 2.1 de periodo mínimo do mapa do gato de Arnold, está-se à procura do menor inteiro n tal que $A^n = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \pmod N$. Isto significa que

n satisfaz as condições $F_{2n} \equiv 0 \pmod{N}$ e $F_{2n-1} \equiv 1 \pmod{N}$. Por isso o periodo do mapa do gato de Arnold tem uma conexão directa com o *periodo de Pisano* dos números de Fibonacci.

O periodo de Pisano n, escrito $\Pi(n)$, é o periodo no qual a sequência de números de Fibonacci tomada módulo n se repete.

Exemplo 3.2. A sequência de Fibonacci F tomada módulo 3 é

$$0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, \ldots$$

A sequência tem periodo 8, por isso $\Pi(3) = 8$.

Da relação definida entre as matrizes A e F segue que o periodo do mapa do gato de Arnold é exacmente metade do periodo de Pisano para qualquer $N \gneq 3$.

4 Propriedades do Mapa do Gato de Arnold

Como ilustrado na Fig. 4.1, não existe uma conexão óbvia entre os periodos mínimos do mapa do gato de Arnold, e por isso o periodo de Pisano e o número N.

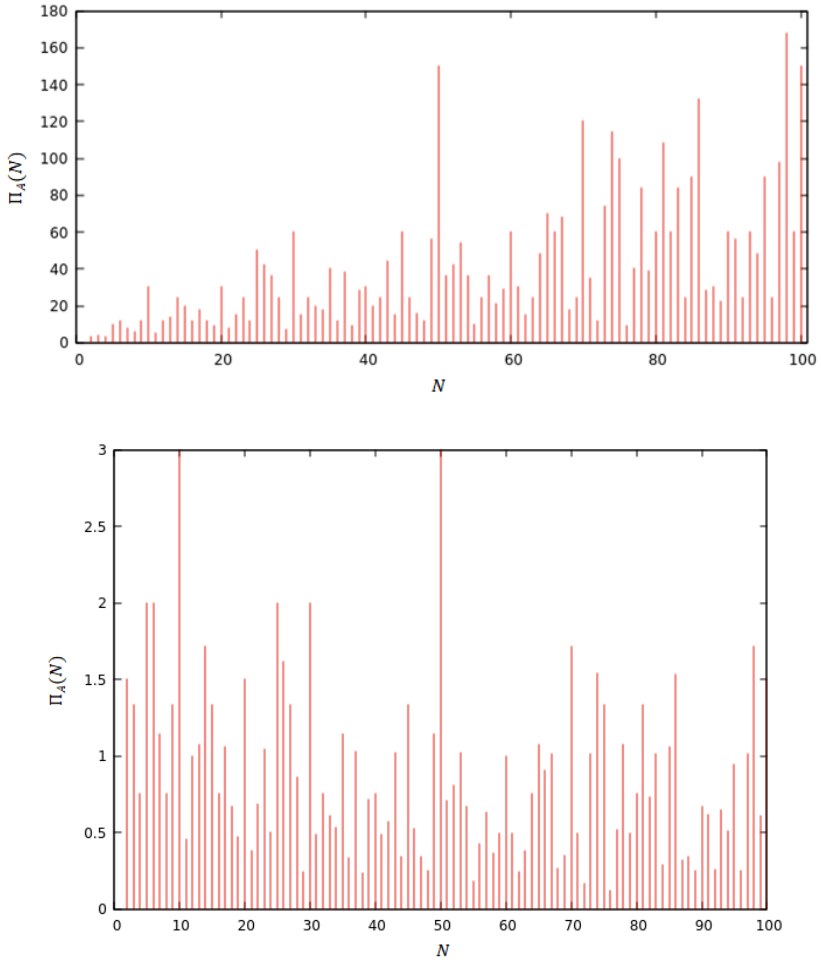


Figura 4.1: Os periodos mínimos $\Pi_A(N)$ do mapa do gato de Arnold e a razão $\frac{\Pi_A(N)}{N}$ para o intervalo $2 \lneq N \lneq 100$.

É importante referir que não é conhecido uma expressão em forma fechada de $\Pi(N)$ válida para todos o N. Por isso, recorreu-se a cálculos numéricos para calcular o periodo minímo.

4.1 Comprimento do periodo

Analisando apenas os periodos mínimos de números primos p entre $5 \lneq p \lneq 100$, observa-se o padrão ilustrado na Fig. 4.1.1

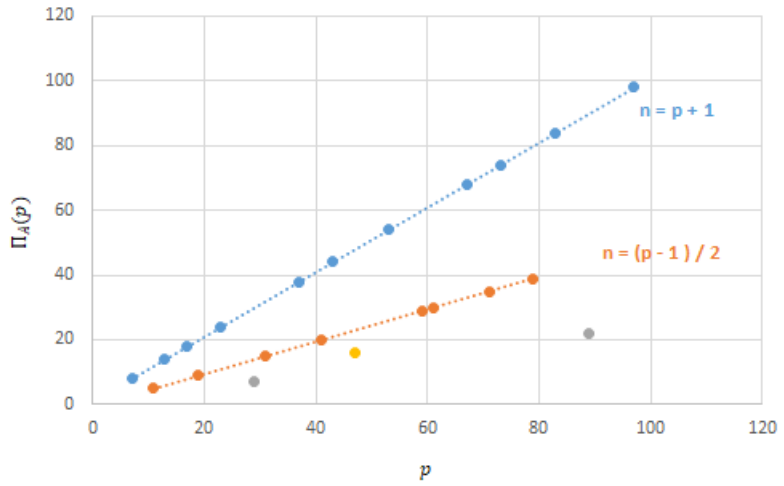


Figura 4.1.1: Os periodos mínimos do mapa do gato de Arnold para números primos no intervalo $5 < p < 100$.

A maior fatia dos números primos $(87,5\%)$ inserem-se ou na linha $\Pi_A(p) = p+1$ ou em $\Pi_A(p) = \frac{p-1}{2}$. Os restantes são conhecidos como números primos *curtos* por o periodo mínimo ser inferior que as fórmulas referidas. O caso $p = 5$ é uma exceção pois $\Pi_A(5) = 10$. O periodo $\Pi_A(N)$ pode ser calculado devido à factorização de primos de qualquer número composto N usando o seguinte teorema, demonstrado em **[4]**.

Teorema 4.1.2. Se N tiver factorização primo $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$, então $\Pi_A(N) = mmc\ (\Pi_A(p_1^{\alpha_1}), \Pi_A(p_2^{\alpha_2}), \ldots, \Pi_A(p_k^{\alpha_k}))$, onde *mmc* é o *mínimo múltiplo comum.*

Exemplo 4.1.3. $\Pi_A(21) = mmc\ (\Pi_A(3), \Pi_A(7)) = mmc\ (4, 8) = 8$

Notar que $p = 2$ é o único primo onde $\Pi_A(p) = \Pi_A(N^2)$. Para todos os outros primos acredita-se que $\Pi_A(p^n) = p^{n-1}\ \Pi_A(p)$.

Exemplo 4.1.4. Para números compostos N têm-se casos onde $\Pi_A(N^2) = \Pi_A(N)$, como por exemplo $\Pi_A(6) = \Pi_A(36) = 12$ e $\Pi_A(12) = \Pi_A(144) = 12$.

O limite superior para o periodo mínimo do mapa do gato de Arnold é $3N$. Como mostra **[5]**, em particular para $k = 1, 2, 3, \ldots$ tem-se:

$$\begin{cases} \Pi_A(N) = 3N, & \text{se } N = 2 \cdot 5^k \\ \Pi_A(N) = 2N, & \text{se } N = 5^k \text{ ou } N = 6 \cdot 5^k \\ \Pi_A(N) \lesneq \frac{12}{7}N & \text{para qualquer outro } N \end{cases}$$

4.2 Órbitas disjuntas

Além da periodicidade podem-se definir outras propriedades distintas e válidas para sistemas dinâmicos discretos.

Definição 4.2.1. Seja a *órbita* de um ponto definido como o conjunto de coordenadas que um ponto individual assume perante iterações do mapa do gato de Arnold, até retornar ao seu valor inicial. O número de coordenadas únicas na órbita recebe o nome de *comprimento de periodo*. Claro que todos os pontos que pertencem a uma e mesma órbita têm o mesmo comprimento de periodo.

Definição 4.2.2. Para um sistema dinâmico discreto todos os pontos com comprimento de órbita 1 recebem o nome de *pontos fixos*.Pontos com comprimento de órbita maiores que 1 são chamados de pontos *não-triviais*.

Exemplo 4.2.3. Para o mapa discreto do gato de Arnold $\Gamma_A : \mathbb{Z}_N \times \mathbb{Z}_N$, o ponto com coordenadas $(0, 0)$ é um ponto trivial. Todos os outros pontos são não-triviais pois são periódicos e têm um comprimento de órbita maior do que 1.

Exemplo 4.2.4. A órbita, com comprimento 12, do ponto $(1, 1)$ para o mapa do gato de Arnold com $N = 6$ consiste nas coordenadas $\{(1, 1), (2, 3), (5, 2), (1, 3), (4, 1), (5, 0), (5, 5), (4, 3), (1, 4), (5, 3), (2, 5), (1, 0)\}$.

Como se sabe que $(0, 0)$ é um ponto trivial e que o limite superior para o mapa do gato de Arnold é $3N$, para $N > 3$, nenhum ponto pode ter uma órbita que inclua todos os $N^2 - 1$ pontos não triviais. Daqui é possível concluir que vão existir órbitas disjuntas e o comprimento destas órbitas é ou igual ao periodo mínimo ou um divisor deste. Por outras palavras, uma imagem não é densa nela própria sobre o mapa discreto do gato de Arnold.

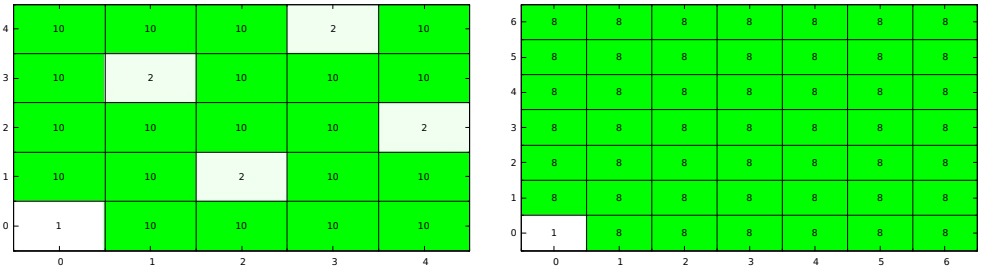


Figura 4.2.5: Comprimento de órbitas do mapa do gato de Arnold para $p = 5$ e $p = 7$.

Quando N é um número primo p, excepto para $p = 5$, todos os pontos não triviais têm o mesmo comprimento de órbita. Quando $p = 5$ o comprimento de órbita dos pontos não triviais é ou $\Pi(5) = 10$ ou $\frac{\Pi(5)}{5} = 2$.

Números compostos vão ter mais que um comprimento de periodo para pontos não-triviais. O maior número de órbitas até $N = 500$ ocorre para $N = 390$ e as 17 diferentes comprimentos de órbita são $2, 3, 4, 6, 10, 12, 14, 20, 28, 30, 42, 60, 70, 84, 140, 210$ e 420.

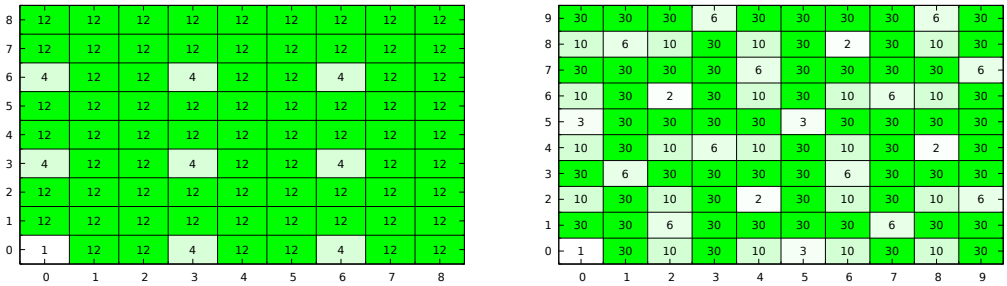


Figura 4.2.6: Comprimento de órbitas do mapa do gato de Arnold para $N = 9$ e $N = 10$.

4.3 Maiores dimensões do mapa

É possível extender o mapa do gato a maiories dimensões, fixando cada coordenada x,y e z e depois multiplicando os resultados para obter uma matriz três dimensional do mapa do gato A_{3D}.

$$\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 1 & 2\end{bmatrix}\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 2\end{bmatrix}\begin{bmatrix}1 & 1 & 0\\ 1 & 2 & 0\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 2 & 3 & 2\\ 3 & 4 & 4\end{bmatrix} = A_{3D}$$

Devido à as propriedades não comutativas da multiplicação de matrizes, a matriz A_{3D} não é única mas todos os mapas A_{3D} têm os mesmos valores próprios $\lambda_1 = 7,18$, $\lambda_2 = 0,57$ e $\lambda_3 = 0,24$. Por outro lado, os periodos mínimos do mapa do gato três dimensional apresentam um padrão completamente diferente que $\Pi_A(N)$.

O mapa do gato quatro dimensional seria agora calculado usando A_{3D} e repetindo o mesmo procedimento com uma coordenada adicional. E assim sucessivamente até uma dimensão arbitária. A razão da escolha de um mapa do gato de dimensão maior é o comportamento que maior valor próprio toma. O mapa do gato de maior dimensão é considerado *mais caótico* pela medição da entropia topológica $\ln|\lambda_{max}|$. Esta propriedade é preferida num contexto criptográfico e, por exemplo, o maior valor próprio de A_{8D} é 1090.

4.4 Mapas do gato generalizados com determinante positivo unitário

Os mapas de gato generalizados, com determinante 1, de tipo 1 e 2 podem ser definidos como

$$\Gamma_{G_1}\left(\begin{bmatrix}x_{t+1}\\ y_{t+1}\end{bmatrix}\right) = \begin{bmatrix}1 & a\\ a & a^2+1\end{bmatrix}\begin{bmatrix}x_t\\ y_t\end{bmatrix} \pmod N$$

e

$$\Gamma_{A_2}\left(\begin{bmatrix}x_{t+1}\\ y_{t+1}\end{bmatrix}\right) = \begin{bmatrix}1 & a\\ b & ab+1\end{bmatrix}\begin{bmatrix}x_t\\ y_t\end{bmatrix} \pmod N$$

Estas famílias do mapa do gato ainda não foram muito estudadas mas acredita-se que apresentam também uma distribuição periódica.

4.5 Miniaturas e Fantasmas

Por vezes antes de se obter o periódo mínimo observa-se que a imagem parece menos caótica do que se esperava. Estes fenómenos recebem o nome de *miniaturas* e *fantasmas* e têm as seguintes propriedades

- Miniaturas podem acontecer quando os valores absolutos de todos os elementos de $A^t \pmod N$ são pequenos quando comparados a N.

$$min|a_{i,j}, N - a_{i,j}|, \quad \text{para } i, j = 1, 2$$

- A orientação das miniaturas vai depender dos vectores coluna de $A^t \pmod N$.
- Fantasmas têm mais tendência a aparecer quando N é um número composto do que quando é um número primo.
- O número de fantasmas e respectivos declives depende dos vectores, com menor valor absoluto, que são mapeados neles próprios por $A^t \pmod N$.

As figuras 2.3f e 2.3h são exemplos numéricos de miniaturas para uma imagem 322×322 que ocorrem após 23 e 61 iterações, respectivamente. Por outro lado a figura 2.3g é o exemplo de um fantasma. Contudo não são exemplos matematicamente perfeitos de miniaturas e fantasmas pois verificando as propriedades como indicado em [**1**], não se obtem resultados análogos.

5 Aplicações do Mapa do Gato de Arnold

Apesar de o conceito do mapa do gato ser abstracto, pode-se pensar nalgumas aplicações

5.1 Encriptação de imagens e texto

Umas das maneiras mais simples de usar o mapa do gato num contexto criptográfico é trocar a informação da cor de um pixel com uma letra do alfabeto. Após um certo número de iterações é produzido um texto cifrado onde as letras aparentamente desordenadas tem uma ordem subjacente e, por isso, o proprietário da chave pode recuperar o texto original. Ao usar um mapa do gato generalizado onde os elementos da matriz são parte da chave complica a cripto-análise ainda mais. A figura 5.1.1 ilustra como a frase *"SISTEMAS DINAMICOS É FIXE"* transforma-se em *"XMT OAFNIEÉDEIASSSI SSCM"* com apenas 2 iterações do mapa do gato de Arnold.

S	I	S	T	E
M	A	S		D
I	N	A	M	I
C	O	S		É
	F	I	X	E

	X	M	T	
O	A	F	N	I
E	É	D	E	I
A	S	S	S	I
	S	S	C	M

Figura 5.1.1: O texto original e o texto cifrado após 2 iterações do mapa do gato de Arnold.

5.2 Esteganografia, marca d'água e detecção de tratamento de imagem

Esteganografia é a arte de esconder uma mensagem dentro de outra mensagem. Isto pode ser também aplicado a imagens e é usado para inserir uma marca d'água ou detectar se uma imagem foi alterada de uma maneira não autorizada (detecção de tratamento de imagem).

O método consiste em utilizar que um conjunto de pixéis vizinhos é espalhado ao longo de uma imagem $N \times N$ após k iterações do mapa do gato de Arnold. Os pixéis da marca d'água são inseridos na imagem que queremos marcar e é tambem espalhada pela imagem toda. O algoritmo de detecção de tratamento de imagem consite em iterar a imagem $\Pi(N) - k$ vezes. A imagem aparece caótica mas a marca d'água aparece intacta se a imagem não foi alterada.

6 Conclusão

Este projecto consistiu em investigar algumas propriedades, e especialmente o periodo módulo N, de automorfismos torais hiperbólicos dois dimensional, fortemente ligados à sequência de Fibonacci, que recebem o nome de mapa do gato de Arnold. Isto inclui a generalização de mapas a determinante unitário positivo bem como a dimensões maiores. Explicou-se como se formam as miniaturas e fantasmas quando se aplica o mapa. Foram obtidos resultados numéricos sobre o periodo mínimo e o comprimento de periodo das orbitas. No final são apresentados algumas aplicações práticas do mapa do gato de Arnold como encriptação ou esteganografia.

Referências

[1] Fredrik Svanström, *Properties of a generalized Arnold's discrete cat map*, 2014,
http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A725545&dswid=-2366

[2] Jens Marklof, *Cat Map*,
https://people.maths.bris.ac.uk/~majm/bib/catmap.ps

[3] Geon Ho Choe, *Computational ergodic theory*, 2005,
http://www.ams.org/journals/bull/2007-44-01/S0273-0979-06-01120-7/S0273-0979-06-01120-7.pdf

[4] Freeman J. Dyson and Harold Falk, *Period of a Discrete Cat Mapping*, 1992,
http://www.jstor.org/stable/2324989

[5] Gabriel Peterson, *Arnold's Cat Map*, 1997,
https://pdfs.semanticscholar.org/edf4/23832801f51bdf3170cf64033913bac7ae2a.pdf

[6] Joe Nance, *Periods of the discretized Arnold's Cat Mapping andits extension to n-dimensions*, 2011,
https://arxiv.org/abs/1111.2984v1