UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Bruno Belorte

A função de Sloane: um estudo à luz dos sistemas dinâmicos

São José do Rio Preto
2021

Bruno Belorte

A função de Sloane: um estudo à luz dos sistemas dinâmicos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Ali Messaoudi

Financiadora: CAPES

São José do Rio Preto

2021

B452f

Belorte, Bruno
A função de Sloane: um estudo à luz dos sistemas dinâmicos / Bruno Belorte. -- São José do Rio Preto, 2021
59 f.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientador: Ali Messaoudi

1. Matemática. 2. Teoria Ergódica. 3. Teoria dos números. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Bruno Belorte

A função de Sloane: um estudo à luz dos sistemas dinâmicos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Prof. Dr. Ali Messaoudi
UNESP - São José do Rio Preto
Orientador

Prof. Dr. Márcio Ricardo Alves Gouveia
UNESP - São José do Rio Preto

Prof. Dr. Marcelo Sobottka
UFSC - Florianópolis

São José do Rio Preto
27 de maio de 2021

À minha família, amigos e orientadores.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, à qual agradeço.

RESUMO

O objetivo deste trabalho é estudar dois resultados de Faria e Tresser (2013) para o problema da persistência multiplicativa de Sloane para bases inteiras $q > 1$, explorando conexões com a função do círculo e das $\mathbb{Z}^d$-ações ergódicas. Veremos que os resultados principais nos dão uma resposta positiva no sentido probabilístico, relativo a densidade dos números inteiros que contém zeros em suas expansões.

Palavras-chave: Persistência. Função do círculo. Ações $\mathbb{Z}^d$-ergódicas.

ABSTRACT

The aim of this work is to study two results of Faria e Tresser (2013) for the Sloane multiplicative persistence problem for integer bases $q > 1$, exploiting connections of the circle map and ergodic $\mathbb{Z}^d$-actions. We will see that the main results give us a positive answer in the probabilistic sense, regarding the density of integers that contain zeros in their expansions.

Keywords: Persistence. Circle maps. Ergodic $\mathbb{Z}^d$-actions.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

No artigo de Sloane (1973), publicado em uma revista de matemática recreacional, Sloane deu o seguinte problema:

Problema: Encontre o próximo termo da sequência:

$$679 \rightarrow 378 \rightarrow 168 \rightarrow 48 \rightarrow 32 \rightarrow ?$$

Resposta: 6. A razão para isto é que cada termo é o produto dos dígitos do termo anterior. Não importa o tamanho do inteiro positivo que inicia o processo, sempre terminaremos com um só dígito de 0 a 9, como neste exemplo anterior. O número de passos para que isso ocorra é chamado de persistência. Então a persistência de 679 é 5.

O interessante é que, nenhum número com persistência maior do que 11 foi encontrado.

O objetivo desta dissertação é estudar o problema de Sloane como um sistema dinâmico ergódico. O problema não se resume somente a base decimal, mas sim a todas as bases inteiras maiores do que dois.

Com base no que foi escrito até aqui, podemos definir a função de Sloane da seguinte maneira: Sejam q e n dois inteiros naturais positivos. É clássico que podemos escrever n na base q de uma maneira única como

$$n = [d_1 d_2 d_3 \cdots d_k]_q = \sum_{j=1}^{k} d_j q^{k-j},$$

onde os dígitos são da forma $d_j \in \{0, 1, \ldots, q-1\}$ e $d_1 > 0$.
Assim, definimos $S_q : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ por $S_q(n) = d_1 \cdot d_2 \cdots d_k$ que é a função de Sloane, que pega os dígitos de n e os multiplica gerando um novo número $S_q(n)$. Da mesma forma se $n_1 = S_q(n)$ então podemos fazer $S_q(n_1) = n_2$ e assim por diante, iterando a função até que só reste um dígito.
Por exemplo, $S_{10}(679) = 378$, $S_{10}(S_{10}(679)) = S_{10}(378) = 168$, ..., até que teremos $S_{10}^5(679) = S_{10}(32) = 6$ e assim paramos as iterações.

Nesta dissertação, estudaremos em detalhes dois teoremas Faria e Tresser (2013). O primeiro nos diz que a densidade de números na base 3 que tem zeros na sua expansão é 1. O valor 1 da densidade é o valor máximo, já que ela varia de 0 a 1. Então temos que há muitos números com zeros em sua expansão.

Teorema 4.10. *Se* $1 < p < q$ *são tais que* $\log_q p$ *é irracional, então o conjunto* $A = \{n \in \mathbb{Z}_+ : S_q(p^n) = 0\}$ *tem densidade assintótica igual a 1.*

O segundo teorema é uma generalização do primeiro para bases $q > 3$ e que também mostra a densidade 1 para números com zeros na sua expansão.

Teorema 5.5. *Sejam* $1 \leq i_1 < i_2 < \cdots < i_k \leq m$ *escolhidos de forma que os números* $1, \alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ *são racionalmente independentes. Então para todo divisor* d *de* q*, o conjunto*

$$A = \left\{(n_1, n_2, \ldots, n_k) \in \mathbb{Z}_+^k : S_q(p_{i_1}^{n_1} p_{i_2}^{n_2} \cdots p_{i_k}^{n_k} \cdot d) = 0\right\}$$

tem densidade assintótica igual a 1.

A dissertação está dividida da seguinte maneira: O Capítulo 2 nos dá os pedaços necessários da teoria ergódica, bem como das ações de grupos, necessários para entender os resultados aqui demonstrados. Veremos primeiramente algumas noções de transformações que preservam medida, ergodicidade e unicidade ergódica, sendo esta última importante para a demonstração do Teorema de Birkhoff com ações ergódicas. A segunda seção deste capítulo aborda o caso das ações de grupos e como estas se relacionam com a teoria ergódica e, por fim, temos a demonstração do Teorema de Birkhoff. Omitimos das preliminares um texto introdutório sobre teoria dos números, já que estes são assuntos mais básicos, porém, mesmo que omitidos quando utilizados no texto virão com referência a bons livros que abordam o conteúdo.

No Capítulo 3 faremos uma formulação em forma de função do problema de Sloane de forma que as órbitas, ou iterações desta função, seja o problema em si. Também há uma seção interessante sobre os testes computacionais já feitos, tanto para a base decimal quanto para outras bases. Por fim, terminamos com uma

estimativa de persistência para a base ternária, um número limitante baseado no número utilizado.

Para o Capítulo 4 vemos os primeiros resultados de densidade, mas na base ternária e, consequentemente na base 4. A ideia é que na base ternária, dado um número inteiro, o segundo elemento (e próximos), da sequência de Sloane, é na verdade uma potência de 2. Isto pois os dígitos que são possíveis nesta base são 0,1 e 2, logo, multiplicando-os temos uma potência de 2. Entendido isto, empiricamente podemos desconfiar que a partir de uma certa potência de 2, a maioria (ou todas) as seguintes terão um 0 na sua expansão o que acarreta uma persistência igual a um. Assim, é feito o processo de, utilizar uma $\mathbb{Z}$-ação determinada por uma função linear, de grau um, definida por partes homeomorfas ao círculo e encontrar uma medida a qual esta será ergódica. Com isso calcularemos a densidade destas potências de 2 que tem zero na expansão.

Para bases maiores do que 4, o sistema dinâmico relevante para a função de Sloane não é mais uma $\mathbb{Z}$-ação, mas $\mathbb{Z}^k$-ação com $k > 1$. Mais precisamente, essas ações são dadas por certos grupos abelianos livres do pedaço da função afim de grau um do círculo, como veremos no Capítulo 5. Vamos explorar algumas propriedades simples destas ações de grupos abelianos livres em ordem de derivar nosso resultado principal na função de Sloane, nomeado Teorema 5.5. Aqui, apresentaremos dois resultados sobre expansões que contém zeros. Na verdade, o caso $q > 4$ é uma generalização do caso anterior sobre a densidade, logo acreditamos que as contas estão bem detalhadas para o caso $q = 3, 4$ e que do Capítulo 4 é possível entender o Capítulo 5. Outros pontos interessantes desse Capítulo é que utilizamos vários resultados importantes, como o Teorema de Birkhoff demonstrado para ações de grupo (que está nas nossas preliminares) e uma generalização da função densidade.

2 PRELIMINARES

Veremos aqui alguns tópicos necessários para os capítulos posteriores relacionados a teoria ergódica e ações de grupos.

2.1 Teoria ergódica

Nossa ideia nesta seção é escrever um pouco sobre ergódica, começando por ergodicidade, passando para medidas invariantes onde veremos alguns resultados de unicidade ergódica e, por fim chegando as ações ergódicas. A base para esta discussão (e notação) será o livro do Einsiedler e Ward (2010), utilizando outros quando uma escrita for mais compreensível ou complementar ao que veremos nos próximos capítulos desse trabalho.

2.1.1 Transformações que preservam medida

Definição 2.1. Sejam $(X, \mathscr{B}, \mu)$ e $(Y, \mathscr{C}, \nu)$ espaços de probabilidade. Uma aplicação ϕ de X até Y é mensurável se $\phi^{-1}(A) \in \mathscr{B}$ para qualquer $A \in \mathscr{C}$, e preserva medida se é mensurável e $\mu(\phi^{-1}(B)) = \nu(B)$ para todo $B \in \mathscr{C}$, neste caso também dizemos que μ é invariante por ϕ. Se, além disso, ϕ^{-1} existe quase sempre e é mensurável, então ϕ é chamada de aplicação invertível que preserva medida. Se $T : (X, \mathscr{B}, \mu) \to (X, \mathscr{B}, \mu)$ preserva medida, então μ é dita T-invariante, $(X, \mathscr{B}, \mu)$ é chamado de sistema que preserva medida e T é uma transformação que preserva medida

Vemos que da definição anterior, a imagem inversa de um conjunto mensurável por uma aplicação mensurável ainda é um conjunto mensurável. Isto significa que a probabilidade de um ponto estar num dado conjunto é igual à probabilidade de que sua imagem também esteja.

Seja a relação de equivalência

$$x \sim y \quad \Leftrightarrow \quad x - y \in \mathbb{Z}.$$

Representamos por $[x] \in \mathbb{R}/\mathbb{Z}$ a classe de equivalência de qualquer $x \in \mathbb{R}$ e denotamos por $\mathbb{R}/\mathbb{Z}$ o espaço de todas as classes de equivalência. Este espaço será chamado de círculo e também é denotado por $\mathbb{S}^1 = \mathbb{R}/\mathbb{Z}$. Esta terminologia é desta forma pois existe um homeomorfismo do círculo com $\mathbb{R}/\mathbb{Z}$ dado por

$$h : \mathbb{R}/\mathbb{Z} \to \mathbb{S}^1, \quad [x] \mapsto e^{2\pi i x}.$$

Notemos que h não depende da escolha do representante da classe uma vez que a função $x \mapsto e^{2\pi i x}$ é periódica de período 1 .

Vamos então definir um sistema dinâmico em $\mathbb{S}^1$ chamado de rotação no círculo. Para qualquer $\alpha \in \mathbb{R}$, definimos a rotação no círculo por α como a função

$$R_\alpha : \mathbb{S}^1 \to \mathbb{S}^1, \quad R_\alpha(t) = t + \alpha \pmod 1.$$

O número real α é chamado de ângulo da rotação. Lembremos também que $t + \alpha \pmod 1$ é o mesmo que tomar somente a parte fracionária de $t + \alpha$. Temos que R_α preserva a medida de Lebesgue m no círculo (VIANA; OLIVEIRA, 2014, Página 16), (KUEHN, 2007).

Vamos denotar por L^1_μ o espaço das funções mensuráveis $f : X \to \mathbb{R}$ com $\int |f| \mathrm{d}\mu < \infty$ e, $\mathscr{L}^\infty$ como o espaço das funções mensuráveis limitadas e $\mathscr{L}^1_\mu$ para o espaço das funções mensuráveis integráveis.

Lema 2.2. *Uma medida μ em X é T-invariante se e somente se*

$$\int f \mathrm{d}\mu = \int f \circ T \mathrm{d}\mu$$

para toda $f \in \mathscr{L}^\infty$. Mais ainda, se μ é T-invariante, então a equação anterior vale para $f \in L^1_\mu$.

Prova. A demonstração pode ser vista em (EINSIEDLER; WARD, 2010, página 15) e (VIANA; OLIVEIRA, 2014, página 2).

2.1.2 Ergodicidade

Vamos olhar a ideia de ergodicidade, que é uma noção natural de indecomponibilidade em teoria ergódica. A definição de ergodicidade para $(X, \mathscr{B}, \mu, T)$

significa que é impossível dividir X em dois subconjuntos de medida positiva cada qual invariante sob T.

Definição 2.3. Uma transformação que preserva medida $T : X \to X$ de um espaço de probabilidade $(X, \mathscr{B}, \mu)$ é ergódica se para todo $B \in \mathscr{B}$ temos

$$T^{-1}B = B \quad \Rightarrow \quad \mu(B) = 0 \text{ ou } \mu(B) = 1.$$

Proposição 2.4. *As propriedades seguintes são equivalentes para uma transformação que preserva medida T de $(X, \mathscr{B}, \mu)$.*

1. *T é ergódica.*
2. *Para qualquer $B \in \mathscr{B}$, $\mu(T^{-1}B \triangle B) = 0$ implica que $\mu(B) = 0$ ou $\mu(B) = 1$.*
3. *Para $A \in \mathscr{B}$, $\mu(A) > 0$ implica que $\mu(\cup_{n=1}^{\infty} T^{-n}A) = 1$.*
4. *Para $A, B \in \mathscr{B}$, $\mu(A)\mu(B) > 0$ implica que existe $n \geq 1$ com*
$$\mu(T^{-n}(A \cap B) > 0).$$
5. *Para $f : X \to \mathbb{C}$ mensurável, $f \circ T = f$ para quase-sempre implica que f é igual a uma constante quase-sempre.*

Prova. A demonstração está no livro de Einsiedler e Ward (2010), página 23 e, página 27 do livro de Walters (2000).

2.1.3 Unicidade ergódica

Seja X um espaço compacto metrizável e d uma métrica em X. A σ-álgebra boreliana de subconjuntos de X será denotada por $\mathscr{B}(X)$ e a menor σ-álgebra contendo todos os fechados de X. Vamos denotar também por $M(X)$ a coleção de todas as medidas de probabilidade definidas no espaço mensurável $(X, \mathscr{B}(X))$. O conjunto de membros de $M(X)$ que são medidas invariantes de T é denotado por $M(X, T)$. Este conjunto consiste de todas $\mu \in M(X)$ que fazem de T uma transformação que preserva medida em $(X, \mathscr{B}(X), \mu)$.

Nesta seção falaremos de uma classe de sistemas dinâmicos que possuem uma única medida ergódica, isto é, o conjunto $M(X, T)$ é o menor possível.

Definição 2.5. Sejam X um espaço métrico compacto e $T : X \to X$ uma aplicação contínua. Então T é dita unicamente ergódica se $M(X, T)$ contém uma única medida de probabilidade invariante, i.é, $M(X, T)$ consiste de um ponto.

Teorema 2.6. *Seja $T : X \to X$ uma aplicação contínua em um espaço métrico compacto X. As afirmações seguintes são equivalentes:*

(i) para toda $f \in C(X)$ tal que $\left(\frac{1}{n}\right) \sum_{i=0}^{n-1} f(T^i x)$ converge uniformemente para uma constante;

(ii) para todo $f \in C(X)$ tal que $\left(\frac{1}{n}\right) \sum_{i=0}^{n-1} f(T^i x)$ converge pontualmente para uma constante;

(iii) existe $\mu \in M(X, T)$ tal que para toda $f \in C(X)$ e para todo $x \in X$,

$$\frac{1}{n} \sum_{i=0}^{n-1} f(T^i x) \to \int f \mathrm{d}\mu.$$

(iv) T é unicamente ergódica;

onde $C(X)$ é o espaço de todas as funções complexas contínuas em X.

Prova. Ver a demonstração em Walters (2000), páginas 160 e 161.

2.2 Ações ergódicas abelianas livres

Definição 2.7. Sejam G um grupo e X um conjunto. Então G é dito agindo em X se existe uma função $T : G \times X \to X$ com $T(g, x) := T^g x = g \cdot x$ tal que para todo $a, b \in G$ e $x \in X$ temos

(i) $a \cdot (b \cdot x) = (ab) \cdot x$,

(ii) $e \cdot x = x$.

A aplicação T é chamada de G-ação em X ou somente G-ação.

Como exemplo: Dado um sistema dinâmico discreto (X, f) onde f é invertível. Uma $\mathbb{Z}$-ação natural é dada por $T(n, x) = f^n(x)$.

Vamos a algumas definições sobre ações abelianas livres.

Definição 2.8. Seja G um grupo abeliano livre com cardinalidade k, com um conjunto de geradores fixos $\{e_1, e_2, \ldots, e_k\}$, onde cada elemento $g \in G$ tem uma representação única

$$g = \sum_{i=1}^{k} n_i e_i$$

com $n_i \in \mathbb{Z}$ para todo $i = 1, 2, \ldots, k$. Definamos a norma de g como

$$\|g\| = \text{máx}_{1 \leq i \leq k} |n_i|.$$

Denotaremos por $G^+ \subset G$ o semigrupo consistindo de todos os elementos g para os quais $n_i \geq 0$ para todo i.
Para cada $N \in \mathbb{Z}_+$, definamos o conjunto

$$\Lambda_N(G) = \{g \in G : \|g\| \leq N\},$$

e também

$$\Lambda_N(G_+) = \Lambda_N(G) \cap G_+.$$

Agora suponhamos que o grupo G (ou o semigrupo G_+) age no espaço de medidas de probabilidade (X, μ) como um grupo (ou semigrupo) de transformações que preservam a medida (t.p.m.) e se $T^g : X \to X$ denota uma t.p.m. associada com $g \in G$ então $T^g_* \mu = \mu$ para todo g e $\mu \in M(X)$. Onde $T^g_* \mu(A) = \mu(g^{-1}.A)$ para qualquer boreliano $A \subset X$. Definamos:

Definição 2.9. Dizemos que a G-ação (ou G_+-ação) em (X, μ) é *ergódica* se os únicos conjuntos mensuráveis $E \subset X$ que são invariantes por G (ou G_+) (i.é, tal que $(T^g)^{-1}(E) \subseteq E$ para todo g) são ou conjuntos vazios ou conjuntos de medida total.

Podemos definir a unicidade ergódica por analogia ao caso de cardinalidade 1, ou seja, no caso que temos somente uma transformação, isto é

Definição 2.10. Uma G-ação (ou G^+-ação) em um espaço métrico compacto X através de funções contínuas é unicamente ergódica se existe uma única medida de probabilidade de Borel em X que é G-invariante (ou G^+-invariante).

2.2.1 O Teorema de Birkhoff

Os objetos básicos da teoria ergódica são sistemas dinâmicos que preservam medida. A ideia desta seção é generalizar o Teorema de Birkhoff para uma $\mathbb{Z}_+^d$-ação e aplicar a tais sistemas.

Definição 2.11. Um sistema dinâmico que preserva medida (s.d.p.m.) é uma quadrupla $(X, \mathscr{B}, \mu, \mathcal{T})$ consistindo de

(a) de um espaço de probabilidade $(X, \mathscr{B}, \mu)$ e

(b) de uma ação $\mathscr{B}$-mensurável $\mathcal{T} = (T^g : g \in G)$ do semigrupo $G = \mathbb{Z}_+^d$ ou de um grupo $G = \mathbb{Z}^d$ em X que deixa a medida μ invariante (simbolicamente: $\mathcal{T}\mu = \mu$). Isto significa que:

(i) $T^g : X \to X$ é $\mathscr{B}$-mensurável e $T^g\mu = \mu$ para todo $g \in G$,

(ii) $T^0 = Id_X$ e $T^{g+g'} = T^g \circ T^{g'}$ para todo $g, g' \in G$.

Observação 2.12. a) Observe que $\mathcal{T}\mu = \mu$ implica

$$\int_{T^{-g}A} f \circ T^g \mathrm{d}\mu = \int_A f \mathrm{d}\mu, \text{ em particular } \|f \circ T^g\|_1 = \|f\|_1$$

para todo $A \in \mathscr{B}$, $f \in L_\mu^1$ e $g \in G$.

b) Se $G = \mathbb{Z}^d$, então todas $T^g \in \mathcal{T}$ são invertíveis, isto pois $-g \in G$ para todo $g \in G$ e também $T^g \circ T^{-g} = T^0 = Id_X$.

Definição 2.13. Uma função mensurável $f : X \to \mathbb{R}$ é $\mathcal{T}$-invariante mod μ se $f \circ T^g = f$ μ-q.s. para cada $g \in G$. Adequadamente um conjunto $A \in \mathscr{B}$ é $\mathcal{T}$-invariante mod μ se $\mu(T^g A \Delta A) = 0$ para todo $g \in G$. Escrevemos $\mathcal{I}_\mu(\mathcal{T}) := \{A \in \mathscr{B} : \mu(T^g A \Delta A) = 0 \, \forall g \in G\}$. Se $\mathcal{T}$ é gerada por uma única transformação, então escrevemos $\mathcal{I}_\mu(T)$ ao invés de $\mathcal{I}_\mu(\mathcal{T})$.

Observação 2.14. Seja $\mathcal{I}(\mathcal{T}) := \{B \in \mathscr{B} : T^{-g}B = B \,\forall g \in G\}$. Então $\mathcal{I}(\mathcal{T}) = \mathcal{I}_\mu(\mathcal{T}) \mod \mu$, pois para cada $B \in \mathcal{I}_\mu(\mathcal{T})$ o conjunto $B' := \bigcup_{g\in G}\bigcap_{h\in G} T^{-(g+h)}B$ pertence a $\mathcal{I}(\mathcal{T})$ e $\mu(B\Delta B') = 0$.

Temos que $\mathcal{I}(\mathcal{T})$ e $\mathcal{I}_\mu(\mathcal{T})$ são σ-álgebras e que, uma função $\mathscr{B}$-mensurável f é $\mathcal{T}$-invariante ($\mathcal{T}$-invariante $\mod \mu$) se e somente se esta é $\mathcal{I}(\mathcal{T})$-mensurável ($\mathcal{I}_\mu(\mathcal{T})$-mensurável).

Para $n \in \mathbb{Z}_+$ seja

$$\Lambda_n := \{g = \sum_i g_i e_i \in G : |g_i| < n \,\forall i = 1, \ldots, d\} \quad \text{e} \quad \lambda_n := |\Lambda_n|.$$

E assim vamos ao Teorema, que é uma das partes principais da teoria ergódica.

Teorema 2.15 (Teorema ergódico de Birkhoff)**.** *Seja $(X, \mathscr{B}, \mu, \mathcal{T})$ um sistema dinâmico que preserva medida. Para cada $f \in L^1_\mu$ o limite*

$$\overline{f}(x) := \lim_{n\to\infty} \frac{1}{\lambda_n} \sum_{g\in\Lambda_n} f(T^g x) \tag{2.1}$$

existe μ-q.s. e está em L^1_μ. A função $\overline{f}$ é $\mathcal{T}$-invariante $\mod \mu$ *e para cada conjunto $A \in \mathcal{I}_\mu(\mathcal{T})$*

$$\int_A \overline{f}\mathrm{d}\mu = \int_A f\mathrm{d}\mu. \tag{2.2}$$

Declaremos a versão com semigrupos, como abaixo.

Teorema 2.16. *Se a G_+-ação em (X, μ) é ergódica, então para toda $f \in L^1(X, \mu)$ e para μ-quase todo $x \in X$ temos*

$$\lim_{N\to\infty} \frac{1}{\#\Lambda_N(G_+)} \sum_{g\in\Lambda_N(G_+)} f \circ T^g(x) = \int_X f\mathrm{d}\mu. \tag{2.3}$$

Este teorema é consequência do Teorema 2.15 anterior.

Quanto às ações de cardinalidade 1 (unicamente ergódicas), temos o fato abaixo (que, mais uma vez, afirmamos apenas para as ações de semigrupo).

Teorema 2.17. *Se uma G^+-ação por uma função contínua em um espaço métrico compacto é unicamente ergódica então para todo $f \in C(X)$*

$$\frac{1}{\#\Lambda_N(G_+)} \sum_{g\in\Lambda_N(G_+)} f \circ T^g \text{ converge uniformemente para } \int_X f \mathrm{d}\mu$$

quando $N \to \infty$, onde μ é uma medida boreliana de probabilidade única G^+-invariante.

A prova para este Teorema (para ações de cardinalidade 1) é feita de maneira análoga ao Teorema 2.6, aplicada com as devidas modificações para o presente caso. A recíproca do Teorema 2.17 é também verdadeira, mas não será necessária.

2.2.1.1 Demonstração do Teorema de Birkhoff

Como na página 26, observação 2.1.6 de Keller (1998), temos que é suficiente provar o Teorema de Birkhoff para $G = \mathbb{Z}^d_+$, por que o caso $G = \mathbb{Z}^d$ pode ser reduzido ao anterior.

Prova do Teorema 2.15:
Esta prova é feita em vários passos. Alguns deles independem da dimensão, outros são muito simples tanto para $d = 1$ quanto para $d > 1$. Para não sobrecarregar a prova com detalhes muito técnicos vamos fazer alguns passos somente para $d = 1$ primeiramente e depois escrever quais são as modificações necessárias para $d > 1$.

Vamos usar a seguinte notação: para $f : X \to \mathbb{R}$ mensurável seja

$$S_n f := \sum_{g\in\Lambda_n} f \circ T^g, \quad A_n f := \frac{1}{\lambda_n} S_n f$$
$$A^- := \liminf_{n\to\infty} A_n f, \quad A^+ := \limsup_{n\to\infty} A_n f.$$

Passo 1: Como $f = f^+ - f^-$, é suficiente provar o teorema para $0 \leq f \in L^1_\mu$. Para $i = 1, \ldots, d$ temos

$$\begin{aligned} A_n f \circ T^{e_i} &= A_n f - \frac{1}{n^d} \sum_{g\in\Lambda_{n,g_i}=0} f \circ T^g + \frac{1}{n^d} \sum_{g\in(\Lambda_n+e_i)/\Lambda_n} f \circ T^g \\ &\geq A_n f - \frac{1}{n} \left(\frac{1}{n^{d-1}} \sum_{g\in\Lambda_{n,g_i}=0} f \circ T^g \right). \end{aligned}$$

Se $d = 1$ (e assim $i = 1$), o termo em parêntese é igual a f. Se $d > 1$ aplicamos o teorema ergódico para $\mathbb{Z}_+^{d-1}$-ações para este termo e concluímos que esse converge quase sempre para valores finitos. Portanto, nos dois casos

$$A^+ f \circ T^{e_i} = \limsup_{n\to\infty} A_n f \circ T^{e_i} \geq \limsup_{n\to\infty} A_n f = A^+ f$$

μ-q.s. Assim como ao mesmo tempo $S_n f \circ T^{e_i} \leq S_{n+1} f$ logo

$$A^+ f \circ T^{e_i} = \limsup_{n\to\infty} \frac{1}{\lambda_n} S_n f \circ T^{e_i} \leq \limsup_{n\to\infty} \frac{(n+1)^d}{n^d} \frac{1}{\lambda_{n+1}} S_{n+1} f = A^+ f,$$

segue que

$$A^+ f \circ T^g = A^+ f \quad \mu\text{-q.s.} \tag{2.4}$$

para todo $g \in G$.

Passo 2: A ideia da prova é mostrar de forma direta que $A^- f \geq A^+ f$ μ-q.s. Veremos, no entanto, que essa abordagem ingênua não produz uma estimativa muito boa. Em vez disso vamos provar que

$$\int A^+ f \mathrm{d}\mu \leq \gamma_d \int f \mathrm{d}\mu$$

onde $\gamma_1 = 1$ e $\gamma_d = 2^d$ para $d > 1$. Para o caso $d = 1$ é fácil deduzir a partir disto no passo 3 que $\int A^+ f \mathrm{d}\mu \leq \int A^- f \mathrm{d}\mu$ e então $A^+ f = A^- f$ μ-q.s.

A ideia básica é decompor a soma $S_n f(x)$ em somas sobre os pequenos cubos Λ_k (uniformemente limitados em tamanho) de tal modo que a estimativa de f sob estes sub-cubos são próximas ou iguais a $A^+ f(x)$.

Para duas funções reais g, h em X seja $g \wedge h := \min\{g, h\}$ o ponto mínimo. Seja $r > 1$, $0 < \epsilon < 1$, e definamos $H = H_{r,\epsilon} := (A^+ f \wedge r)(1 - \epsilon)$. Então $0 \leq H < r$, e como $(A^+ f) \circ T^g = A^+ f$ pela equação (2.4), também $H \circ T^g = H$ para todo $g \in G$. A fim de realizar a decomposição mencionada acima, seja

$$\tau : X \to \mathbb{N}, \quad x \mapsto \min\{n \geq 1 : S_n f(x) \geq \lambda_n \cdot H(x)\}.$$

Observe que $\tau(x) < \infty$ para todo $x \in X$:

- se $A^+ f(x) = 0$, então $S_1 f(x) = f(x) \geq 0 = H(x)$ tal que $\tau(x) = 1$,

- se $0 < A^+f(x) < \infty$, então $A^+f(x) < H(x)$ tal que $\tau(x) < \infty$, e
- se $A^+f(x) = \infty$, então $A^+f(x) > r(1-\epsilon) = H(x)$ tal que $\tau(x) < \infty$.

A definição de τ sugere que os sub-blocos de Λ_n para os quais estamos olhando são da forma $\Lambda_{\tau(T^g x)} + g$ para um $g \in \Lambda_n$ arbitrário. Se τ é uniformemente limitada podemos realmente trabalhar com tais blocos. Caso contrário substituímos f por uma função $\tilde{f}$ próxima de f tal que associada a $\tilde{\tau}$ é limitada. Mais precisamente, para $M > 0$ considere $\tilde{f} := f + H \cdot 1_{\{r>M\}}$ e $\tilde{\tau}(x) := \min\{n \geq 1 : S_n\tilde{f}(x) \geq \lambda_n \cdot H(x)\}$. Observe que

- se $\tau(x) > M$, então $S_1\tilde{f}(x) = \tilde{f}(x) \geq H(x)$, i.é, $\tilde{\tau}(x) = 1 \leq M$, e
- se $\tau(x) \leq M$, então $S_{\tau(x)}\tilde{f}(x) \geq S_{\tau(x)}f(x) \geq \lambda_{\tau(x)}H(x)$, i.é, $\tilde{\tau}(x) \leq \tau(x) \leq M$.

Então $\tilde{\tau} \leq M$. Suponhamos agora que para cada $x \in X$ há algum conjunto $\Lambda'_n(x) \subseteq \Lambda_n$ com a propriedade que $(\Lambda_{\tilde{\tau}(T^g x)} + g : g \in \Lambda'_n(x))$ é a família de "cubos" dois a dois disjuntos contidos em Λ_n tais que

$$\sum_{g\in\Lambda'_n(x)} |\Lambda_{\tilde{\tau}(T^g x)}| \geq \gamma_d^{-1}(n-M)^d. \tag{2.5}$$

Esta condição sugere que a união destes cubos cubra aproximadamente uma fração γ_d^{-1} de Λ_n pelo menos. Para um d qualquer esta família é dada pelo Lema 2.18 abaixo; no caso $d = 1$ o conjunto $\Lambda'_n(x)$ é simplesmente todos os inteiros $\tau_k(x) \in \Lambda_{n-M}$ definidos recursivamente por

$$\tau_0 = 0 \quad \text{e} \quad \tau_{k+1} = \tau_k + \tilde{\tau} \circ T^{\tau_k} \quad \text{para } k \geq 0.$$

Em vista da definição de $\tilde{\tau}$ e da $\mathcal{T}$-invariância de H podemos estimar

$$\begin{aligned} S_n\tilde{f}(x) &\geq \sum_{h\in\Lambda'_n(x)} \sum_{g\in\Lambda_{\tilde{\tau}(T^h x)}+h} (\tilde{f}\circ T^g)(x) = \sum_{h\in\Lambda'_n(x)} \sum_{g\in\Lambda_{\tilde{\tau}(T^h x)}} (\tilde{f}\circ T^g)(T^h x) \\ &= \sum_{h\in\Lambda'_n(x)} (S_{\tilde{\tau}(T^h x)}\tilde{f})(T^h x) \geq \sum_{h\in\Lambda'_n(x)} \lambda_{\tilde{\tau}(T^h x)} \cdot H(T^h x) \\ &= \sum_{h\in\Lambda'_n(x)} |\Lambda_{\tilde{\tau}(T^h x)}| \cdot H(x) \geq \gamma_d^{-1}(n-M)^d \cdot H(x). \end{aligned}$$

Então, observando que $H \leq r$,

$$S_n f = S_n(\tilde{f} - H1_{\{r>M\}}) \geq \gamma_d^{-1}(n-M)^d \cdot H - rS_n 1_{\{1>M\}}. \tag{2.6}$$

Dividindo essa inequação por λ_n e passando o limite $n \to \infty$ temos que $A^- f \geq \gamma_d^{-1} H - rA^+ 1_{\{r>M\}} = \gamma_d^{-1}(1-\epsilon)(A^+ f \wedge r) - rA^+ 1_{\{r<M\}}$. A esperança agora é que $A^+ 1_{\{r>M\}}$ seja pequeno porque $\mu\{\tau < M\}$ é pequeno se M é grande o suficiente. Mas este termo é do mesmo tipo que o termo $A^+ f$ que queremos estimar. Mais ainda, não fizemos o uso da $\mathcal{T}$-invariância de mu ainda, e este é exatamente o ponto onde temos que usar isto. Em vez de estimar as médias do caminho $A_n 1_{\{r>M\}}(x)$ integramos a inequação (2.6) e observamos que $\mathcal{T}\mu = \mu$:

$$\int f \mathrm{d}\mu = \frac{1}{n^d} \int S_n f \mathrm{d}\mu \geq \gamma_d^{-1} \left(\frac{n-M}{n}\right)^d \int H \mathrm{d}\mu - r\mu\{\tau > M\}.$$

No limite $n \to \infty$ isto fica

$$\int f \mathrm{d}\mu + r\mu\{\tau > M\} \geq \gamma_d^{-1} \int H \mathrm{d}\mu.$$

Como $\lim_{M\to\infty} \mu\{\tau > M\} = 0$ e como $H = (1-\epsilon)(A^+ f \wedge r)$, temos

$$\gamma_d \int f \mathrm{d}\mu \geq (1-\epsilon) \inf(A^+ f \wedge r) \mathrm{d}\mu.$$

Passando $\epsilon \to 0$ e então com $r \to \infty$, usando o Teorema da convergência monótona, segue que

$$\int A^+ f \mathrm{d}\mu \leq \gamma_d \int f \mathrm{d}\mu. \tag{2.7}$$

Passo 3 (somente para o caso $d = 1$): Aqui derivamos a convergência quase certa em (2.1) para estimar (2.7). Nossa primeira observação é que para $f(0 \leq f \leq M)$ limitada temos $A^- f = -A^+(-f) = M - A^+(M-f)$ tal que

$$\int A^- f \mathrm{d}\mu = M - \int A^+(M-f) \mathrm{d}\mu \geq M - \int (M-f) \mathrm{d}\mu = \int f \mathrm{d}\mu$$

por (2.7) temos $\gamma_1 = 1$. Por um argumento de truncamento simples esta inequação se estende para $f \geq 0$ ilimitada: Seja $M > 0$. Então

$$\int A^- f \mathrm{d}\mu \geq \int A^-(f \wedge M) \mathrm{d}\mu \geq \int f \wedge M \mathrm{d}\mu \nearrow \int f \mathrm{d}\mu$$

com $M \to \infty$ e pelo Teorema da convergência monótona, logo para qualquer $f \geq 0$ mensurável

$$\int A^- f \mathrm{d}\mu \geq \int f \mathrm{d}\mu \geq \int A^+ f \mathrm{d}\mu. \tag{2.8}$$

Como $A^- f \leq A^+ f$ segue que $\overline{f} = A^- f = A^+ f$ μ-q.s.

Passo 4: Vamos provar as afirmações restantes do Teorema. Para a L^1_μ-convergência de $A_n f$ para $\overline{f}$ é suficiente mostrar que a sequência $(A_n f)_n$ é uniformemente integrável (ver a seção A.4.21 de Keller (1998)): como $A_n f - r = A_n(f-r) \leq A_n((f-r)^+)$ onde $A_n((f-r)^+) \geq 0$, temos $(A_n f - r)^+ \leq A_n((f-r)^+)$ tal que

$$\int (A_n f - r)^+ \mathrm{d}\mu \leq \int A_n((f-r)^+)\mathrm{d}\mu = \int (f-r)^+ \mathrm{d}\mu,$$

e isto tende a zero com $r \to \infty$.

A $\mathcal{T}$-invariância mod μ de $\overline{f}$ segue de (2.4), e (2.2) é uma consequência direta da $\mathcal{T}$-invariância de μ: se $A \in \mathcal{I}_\mu(\mathcal{T})$, então

$$\int_A \overline{f} \mathrm{d}\mu = \lim_{n\to\infty} \frac{1}{\lambda_n} \int_A S_n f \mathrm{d}\mu = \lim_{n\to\infty} \frac{1}{\lambda_n} \sum_{g\in\Lambda_n} \int_{T^{-g}A} f \circ T^g \mathrm{d}\mu = \int_A f \mathrm{d}\mu.$$

Isto encerra a prova para o teorema ergódico para o caso $d = 1$.Temos que algumas modificações são necessárias para provarmos o caso $d > 1$:

1. uma escolha diferente para os cubos na inequação (2.5), e
2. uma nova demonstração para $A^+ f = A^- f$ μ-q.s. no Passo 3.

Começaremos com o primeiro ponto. No caso $d > 1$, o cubo Λ_n já não pode mais ser preenchido sem buracos utilizando os cubos $\Lambda_{\tau(T^h x)} + h$ como no caso unidimensional. O Lema seguinte nos dá um preenchimento bom (mas ainda fragmentado):

Lema 2.18. *Dados inteiros positivos $n > M$ e uma função $\ell : \Lambda_n \to \{1, \ldots, M\}$, há um conjunto $\Lambda'_n \subseteq \Lambda_n$ tal que $(\Lambda_{\ell(g)} + g : g \in \Lambda'_n)$ é uma família de "cubos" dois a dois disjuntos contidos em Λ_n e*

$$\sum_{g\in\Lambda'_n} |\Lambda_{\ell(g)}| \geq 2^{-d}(n-M)^d. \tag{2.9}$$

Prova. Seja $\mathcal{D}_M$ uma coleção maximal de conjuntos disjuntos da forma $\Lambda_M + g$ com $\ell(g) = M$ e $g \in \Lambda_{n-M}$. Quando $\mathcal{D}_M, \ldots, \mathcal{D}_i$ foram construídos para $i > 1$, seja $\mathcal{D}_{i-1}$ uma coleção maximal de conjuntos da forma $\Lambda_{i-1} + g$ com $\ell(g) = i - 1$ e $g \in \Lambda_{n-M}$, para o qual todos os conjuntos em $\mathcal{D}_{i-1} \cup \cdots \cup \mathcal{D}_M$ são disjuntos. Seja

$$\Lambda'_n := \{g \in \Lambda_{n-M} : \Lambda_{\ell(g)} + g \in \mathcal{D}_1 \cup \cdots \cup \mathcal{D}_M\}.$$

Observe que os conjuntos $D_g := \Lambda_{\ell(g)}, g \in \Lambda'_n$, são conjuntos dois a dois disjuntos de Λ_n. Tome qualquer $h \in \Lambda_{n-M}$. Pela maximalidade de $\mathcal{D}_{\ell(h)}$ existe algum $j \geq \ell(h)$ e $\Lambda_j + g \in \mathcal{D}_j$ com $(\Lambda_{\ell(g)} + g) \cap (\Lambda_{\ell(h)} + h) \neq \varnothing$. Então $\ell(g) = j \geq \ell(h)$ e $\Lambda_{\ell(g)} \supseteq \Lambda_{\ell(h)}$. Então $h \in \tilde{D}_g := g + \Lambda_{\ell(g)} - \Lambda_{\ell(g)}$, e portanto $\Lambda_{n-M} \subseteq \cup_{g \in \Lambda'_n} \tilde{D}_g$. Agora (2.9) segue da inequação $|\tilde{D}_g| \leq 2^d \cdot |D_g|$. □

Lema 2.19. *Seja* $\mathcal{T} = \{T^g : g \in G\}$, $F := \{f \in L^2_\mu : f \circ T = f \, \forall T \in \mathcal{T}\}$ *e* $N := \{h - h \circ T : h \in L^2_\mu, T \in \mathcal{T}\}$. *Então* $F = N^\perp$.

Prova. Para mostrar $F \subseteq N^\perp$, seja $f \in F$, $h \in L^2_\mu$ e $T \in \mathcal{T}$. Então

$$\langle f, h - h \circ T\rangle = \langle f, h\rangle - \langle f \circ T, h \circ T\rangle = \langle f, h\rangle - \langle f, h\rangle = 0,$$

i.é, $f \in M^\perp$.

Para a inclusão inversa seja $f \in N^\perp$. Então $\langle f, f - f \circ T\rangle = 0$ tal que $\langle f, f\rangle = \langle f \circ T, f\rangle$. Segue que

$$\|f - f \circ T\|^2 = \langle f, f - f \circ T\rangle - \langle f \circ T, f\rangle + \langle f \circ T, f \circ T\rangle = -\|f\|^2 + \|f\|^2 = 0,$$

i.é, $f \in F$. □

Continuação da demonstração do teorema ergódico para $d > 1$:

Para $f \in L^1_\mu$ seja $\Delta f := A^+ f - A^- f$. Devemos mostrar que $\Delta f = 0$ μ-q.s. Para este fim decompomos f em uma soma de funções do espaço F ou N do lema anterior mais um pequeno termo restante. Seja $\epsilon > 0$.

1. $f = u_1 + r_0$ onde $u_1 \in L^2_\mu$ e $\inf |r_0| \mathrm{d}\mu < \epsilon$. Isto é possível porque L^2_μ é $\|\cdot\|_1$-denso em L^1_μ.

2. $u_1 = f_1 + u_2 + \cdots + u_k + r_1$ para algum $k \geq 2$ onde $f_1 \in F$, $u_j = h_j - h_j \circ T^{g_j} \in N$, $g_j \in G$ $(j = 2, \ldots, k)$ e $\int |r_1| \mathrm{d}\mu \leq \|r_1\|_2 < \epsilon$, veja o Lema anterior.

3. $h_j = f_j + r_j$ onde f_j é limitada e $\int |r_j| \mathrm{d}\mu < \frac{\epsilon}{2k}$ $(j = 2, \ldots, k)$. Por exemplo, podemos escolher $f_j = h_j \cdot 1_{\{|h_j| \leq M\}}$ para um $M > 0$ suficientemente grande.

Seja $R := r_0 + r_1 + \sum_{j=2}^{k}(r_j - r_j \circ T^{g_j})$. Então $\int |R| \mathrm{d}\mu < 3\epsilon$ e

$$f = f_1 + \sum_{j=2}^{k}(f_j - f_j \circ T^{g_j}) + R$$

tal que

$$\Delta f \leq \Delta f_1 + \sum_{j=2}^{k} \Delta(f_j - f_j \circ T^{g_j}) + \Delta R.$$

Agora $\Delta f_1 = A^+ f_1 - A^- f_1 = f_1 - f_1 = 0$, e para $j = 2, \ldots, k$ observamos que

$$\begin{aligned} |A_n(f_j - f_j \circ T^{g_j})| &= \left| \frac{1}{\lambda_n} \sum_{g \in \Lambda_n} f_j \circ T^g - \frac{1}{\lambda_n} \sum_{g \in \Lambda_n + g_j} f_j \circ T^g \right| \\ &\leq \frac{1}{\lambda_n} \sum_{g \in \Lambda_n \Delta(\Lambda_n + g_j)} |f_j \circ T^g| \\ &\leq \frac{1}{\lambda_n} \cdot 2d|g_j| n^{d-1} \cdot \|f_j\|_\infty \\ &= 2dn^{-1}|g_j| \|f_j\|_\infty, \end{aligned}$$

tal que $A^-(f_j - f_j \circ T^{g_j}) = A^+(f_j - f_j \circ T^{g_j}) = 0$ e assim $\Delta(f_j - f_j \circ T^{g_j}) = 0$. Segue que

$$0 \leq \Delta f \leq \Delta R = A^+ R - A^- R \leq 2A^+ |R|.$$

Em vista de (2.7) isto implica que

$$\int \Delta f \mathrm{d}\mu \leq 2 \int A^+ |R| \mathrm{d}\mu \leq 2\gamma_d \int |R| \mathrm{d}\mu \leq 2\gamma_d \cdot 3\epsilon.$$

Como $\epsilon > 0$ é arbitrário, concluímos que $\int \Delta f \mathrm{d}\mu = 0$ e assim $\Delta f = 0$ μ-q.s. $\square$

3 O PROBLEMA DA PERSISTÊNCIA DE SLOANE

Neste capítulo veremos a formalização do problema da persistência, bem como uma formulação mais geral, como veremos na seção seguinte.

3.1 Função de Sloane e persistência

Sejam n um número natural e q um inteiro com $q > 1$. A expansão de n na base q é dada por

$$n = [d_1 d_2 d_3 \cdots d_k]_q = \sum_{j=1}^{k} d_j q^{k-j}, \tag{3.1}$$

onde cada dígito $d_j \in \{0, 1, \ldots, q-1\}$ (e $d_1 \neq 0$ quando $n \geq 1$).

Definição 3.1. Sejam n um número natural e q um inteiro com $q > 1$, onde $n = [d_1 d_2 d_3 \cdots d_k]_q$. A função

$$\begin{aligned} S_q : \mathbb{Z}_+ &\to \mathbb{Z}_+ \\ n &\mapsto S_q(n) = \prod_{j=1}^{k} d_j \end{aligned}$$

é chamada de função de Sloane na base q.

Claramente esta função pode ser iterada, isto é, podemos fazer $S_q(S_q(n))$ e assim por diante. Logo, dado $n \in \mathbb{Z}_+$, podemos considerar uma órbita da função de Sloane como

$$n, S_q(n), S_q^2(n), S_q^3(n), \ldots, S_q^m(n), \ldots$$

Observação 3.2. Se n é um inteiro tal que $0 \leq n \leq q$, então $S_q(n) = n$.

Exemplo 3.3. Vamos tomar o exemplo de 2^{15} na base 3, isto é, $n = 2^{15}$ e $q = 3$. Temos que (utilizando a multiplicação na base $q = 3$)

$$\begin{aligned}
2_3^{15} &= 2 \cdot 2 \cdot 2^{13} = (11_3 \cdot 2) \cdot 2^{12} = (22_3 \cdot 2) \cdot 2^{11} \\
&= (121_3 \cdot 2) \cdot 2^{10} = (1012_3 \cdot 2) \cdot 2^9 = (2101_3 \cdot 2) \cdot 2^8 \\
&= (11202_3 \cdot 2) \cdot 2^7 = (100111_3 \cdot 2) \cdot 2^6 \\
&= (200222_3 \cdot 2) \cdot 2^5 = (1101221_3 \cdot 2) \cdot 2^4 = (2210212_3 \cdot 2) \cdot 2^3 \\
&= (12121201_3 \cdot 2) \cdot 2^2 = (102020102_3 \cdot 2) \cdot 2 = 211110211_3 \cdot 2 = 1122221122_3.
\end{aligned}$$

$$S([1122221122]_3) = \prod_{j=1}^{10} d_j = 1012_3$$

e

$$S([1012]_3) = S(S([1122221122]_3)) = S^2([1122221122]_3) = \prod_{j=1}^{4} d_j = 0$$

pois o segundo dígito é zero.

Vamos a uma proposição que garantirá que uma órbita da função de Sloane se estabiliza depois de um número finito de iterações.

Proposição 3.4. *Se $n \in \mathbb{N}$ e $q \in \mathbb{Z}_+$, então $S_q(n) < n$ para todo $n \geq q$.*

Prova. Escrevamos n da forma

$$n = [d_1 d_2 d_3 \cdots d_k]_q = \sum_{j=1}^{k} d_j q^{k-j}.$$

Note que $k > 1$ por hipótese, já que $n \geq q$ o que implica n ter pelo menos dois dígitos. Temos

$$S_q(n) = d_1 \prod_{j=2}^{k} d_j < d_1 (q-1)^{k-1} < n.$$

□

Da Proposição anterior temos algumas consequências interessantes.

Corolário 3.5. *Sejam $n \in \mathbb{N}$ e $q \in \mathbb{Z}_+$. Logo n é um ponto fixo de $S_q(n)$ se e somente se $k = 1$.*

Corolário 3.6. *Sejam N e q em $\mathbb{Z}_+$. Então existe um número mínimo $\nu_q(n) \in \mathbb{Z}_+$ tal que $S_q^i(n) = S_q^{\nu_q(n)}$ para todo $i \geq \nu_{q(n)}$.*

Prova. Pela proposição 3.4, deduzimos que a sequência $(S_q^i(n))_{i\geq 0}$ é decrescente. Como ela é limitada inferiormente por 0, deduzimos que ela é convergente. Como $(S_q^i(n))$ está em $\mathbb{Z}_+$ para todo $i \geq 0$, obtemos o resultado. □

Sloane perguntou em (SLOANE, 1973) (e vimos isto também na Seção 3) se esse número mínimo de passos até um ponto fixo é uniformemente limitado. O número $\nu_q(n)$ é conhecido como persistência (ou persistência multiplicativa) de n na base q. Vimos na seção 3 que as evidências numéricas para $\nu_q(n)$ foram coletadas para alguns valores de q, na qual vimos também que para $q = 2$, para qualquer $n \geq 0$ temos $S_2(n) \in \{0, 1\}$ e $\{0, 1\}$ são pontos fixos de S_2. O problema da persistência pode ser sistematizado como abaixo.

Problema 1. Para um dado $q > 2$, existe um número positivo $B(q)$ tal que $\nu_q(n) \leq B(q)$ para todo n?

Considerando $B(q) = \sup_n \nu_q(n)$ como um elemento de $\mathbb{Z}_+ \cup \infty$.

Problema 2. Qual é o comportamento de $B(q)$ visto como uma função de q? Mais precisamente, podemos perguntar

(a) A resposta ao Problema 1 é positiva para todos, ou todos, exceto alguns valores finitos, ou para um valor finito de q?

(b) Qual é o comportamento assintótico de $B(q)$ quando $q \to \infty$?

Vamos relembrar alguns fatos sobre o problema da persistência em várias bases:

(a) Na base $q = 2$ (binária) todo número inteiro positivo tem persistência no máximo 1, e zero caso for de um único digito.

(b) Na base $q = 3$, nenhum número com persistência maior do que 3 foi encontrado.

(c) Na base decimal $q = 10$ o número 68889 tem persistência multiplicativa 7, porque sob a função de Sloane S_{10} temos

$$68889 \mapsto 27648 \mapsto 2688 \mapsto 768 \mapsto 336 \mapsto 54 \mapsto 20 \mapsto 0.$$

Este é o menor número com persistência 7.
Ainda na base decimal, o número $n = 277777788888899$ tem persistência multiplicativa 11. É o menor número para com persistência 11.
Está conjecturado que $\nu_{10}(n) \leq 11$ para todo $n \in \mathbb{N}$. Isto foi checado para todos os n até 10^{233}.

3.2 Algumas conjecturas

Na literatura existem várias conjecturas:

Conjectura 1. Existe um inteiro positivo $k_0(q)$ tal que, para todo $k \geq k_0(q)$, a expansão na base q de qualquer produto de k dígitos maiores do que 1 para a base q tem pelo menos um dígito igual a zero.

Assim que um produto de dígitos se torna divisível por q, um zero aparece como seu dígito mais à direita quando escrito na base q e, portanto, a próxima iteração da função Sloane produz 0 como resultado. Esta observação trivial permite que nos concentremos apenas nos produtos que não são divisíveis pela base q. O efeito disso será dramático quando $q = 4$. As duas conjecturas a seguir estão implícitas na Conjectura 1.

No caso da base $q = 3$, os únicos valores diferentes de zero e de um assumidos pela função de Sloane são potências de 2. Em outras palavras, só precisamos investigar a órbita de 1 sob a função duplicadora $x \mapsto 2 \cdot x$.

Conjectura 1a. Existe um inteiro positivo $k_{3,2}$ tal que, para todo $k \geq k_{3,2}$, a expansão na base 3 de 2^k tem pelo menos um dígito igual a zero.

Tal afirmação é uma reminiscência de uma conjectura de Erdös no sentido de que sempre há um 2 entre os dígitos na base 3 de 2^k para todo k suficientemente grande (FARIA; TRESSER, 2013, Página 5).

No caso da base $q = 4$, em princípio todos os produtos da forma $2^m \cdot 3^n$ tem de ser examinados, já que são os resultantes da segunda iteração, i.é, dado um número $(1222333113)_4$ a multiplicação dos seus dígitos é igual a $(2^3 \cdot 3^4)_4$. Mas como a base 4 divide $2^m \cdot 3^n$ assim que $m \geq 2$ (isto é, $(2^2)_4 = (10)_4$ e assim o número terá um zero), temos somente que considerar: (a) potências de 3 ou (b) produtos na forma $2 \cdot 3^m$. Em outras palavras, precisamos considerar as órbitas de 1 e 2 sob a função triplicadora $x \mapsto 3 \cdot x$.

Conjectura 1b. Existe um inteiro positivo $k_{4,3}$ tal que, para todo $k \geq k_{4,3}$, a expansão na base 4 de 3^k e $2 \cdot 3^k$ tem pelo menos um dígito igual a zero.

Existe uma evidência computacional em favor destas conjecturas. Provar estas conjecturas certamente é o suficiente para resolver o problema da persistências nas bases citadas.

3.3 Uma estimativa para a persistência no caso da base ternária

Queremos estabelecer uma estimativa em $\nu_3(n)$, para isto vamos primeiro demonstrar alguns resultados preliminares.

Lema 3.7. *A equação $x^a - 2^b = 1$ possui uma única solução em que a e b são inteiros maiores que 1, e x é um primo ímpar, a qual é dada por $x = b = 3 e\ a = 2$.*

Prova. Temos que

$$2^b = x^a - 1 = (x-1)(x^{a-1} + x^{a-2} + x^{a-3} + \cdots + x + 1)$$

disto temos que ambos os termos $(x-1)$ e $(x^{a-1} + x^{a-2} + x^{a-3} + \cdots + x + 1)$ são potências de 2. Logo existe um h tal que

$$x - 1 = 2^h$$
$$(x^{a-1} + x^{a-2} + x^{a-3} + \cdots + x + 1) = 2^{b-h}.$$

Afirmação 1: Não existe solução se $h > 1$.

De fato, se $h > 1$, então $x \geq 5$ e $x + 1$ não é uma potência de 2. Além do mais $a - 1$ deve ser impar já que $(x^{a-1} + x^{a-2} + x^{a-3} + \cdots + x + 1)$ é par e x é ímpar. Também $(x^a - 1)$ não pode ser uma potência de 2 já que $x + 1$ divide $(x^{a-1} + x^{a-2} + x^{a-3} + \cdots + x + 1)$ pois $(a - 1)$ é ímpar. Isso é um absurdo, logo temos a Afirmação 1.

Afirmação 2: Não existe solução para $h = 1$ onde $a > 2$.

De fato a é par, já que da Afirmação 1 temos que $a - 1$ é ímpar, então $2^b = 3^a - 1 = (3^{\frac{a}{2}} - 1)(3^{\frac{a}{2}} + 1)$. Mas para $a > 2$, $\frac{a}{2} \geq 2$ ambos $(3^{\frac{a}{2}} - 1)$ ou $(3^{\frac{a}{2}} + 1)$ não são potências de 2. □

Observação 3.8. O Lema anterior é um caso restrito do problema de E. Catalan (1844) diz que 8 e 9 (2^3 e 3^2 são os únicos inteiros consecutivos positivos que são potências de inteiros menores que estes, algebricamente temos que $x^a - y^b = 1$, $a > 1$, $b > 1$ implicam que $a = y = 2$, $b = x = 3$. O problema foi resolvido por Mihailescu (2004).

Proposição 3.9. *Se $n > 3$, então pelo menos um dígito na expansão na base 3 de 2^n não é igual a 2.*

Prova. Suponhamos, por contradição, que a expansão na base ternária de 2^n tem exatamente $k > 1$ dígitos (o que é garantido pelo fato que $n > 3$), todos iguais a 2, isto é $2^n = [d_1 d_2 \dots d_k]_3$ com $d_j = 2$, $j = 1, \dots, k$. Então $2^n = 3^k - 1$ e assim a equação $x^a - 2^b = 1$ teria uma solução $x = 3$, $a = k > 1$ e $b = n > 3$, o que contradiz o Lema 3.7.

Portanto pelo menos um dígito na expansão na base 3 de 2^n não é igual a 2. □

O seguinte resultado tem demonstração imediata.

Corolário 3.10. *Se $n > 3$ temos que $S_3(2^n) \leq 2^{k-1}$.*

□

Seja x um número real. O inteiro n tal que $n \leq x < n+1$ será denotado por $\lfloor x \rfloor$. O inteiro k tal que $k - 1 < x \leq k$ será denotado por $\lceil x \rceil$. Temos $\lceil x \rceil = \lfloor x \rfloor + 1$. Denotaremos $\{x\} = x - \lfloor x \rfloor$ e a chamamos de parte fracionária de x.

Por exemplo, dado 3,067 temos que $\lfloor 3,99 \rfloor = 3$ e $\lceil 3,01 \rceil = 4$.

Seja $N \in \mathbb{Z}_+$ que tem k dígitos em uma base q. Como $q^{k-1} \leq N < q^k$ deduzimos que

$$k = \lfloor \log_q N \rfloor + 1.$$

Vamos utilizar esta fórmula na demonstração abaixo.

Proposição 3.11. *Para todo $n \geq 1$ temos que $\nu_3(n) \leq 2 + 3 \log_3 \log_3 n$.*

Prova. Seja $n > 3$ dado e suponhamos que $S_3(n) \neq 0$, caso contrário não há o que provar. Então, suponhamos $n_1, n_2, \ldots, n_m$ tais que

(i) $n_j > 3$ para $j = 1, 2, \ldots, m$;

(ii) $S_3(n) = 2^{n_1}$;

(iii) $S_3(2^{n_j}) = 2^{n_{j+1}}$ para $j = 1, 2, \ldots, m-1$;

(iv) m é maximal com as propriedades acima.

Pelo Corolário 3.10 temos que a sequência $n_1, n_2, \ldots, n_m$ é decrescente, pois $S_3(n_j) = 2^{n_{j+1}} \leq S_3(2^{n_{j+1}}) = 2^{n_{j+2}}$. Como m é o último valor desta sequência $j = 1, 2, \ldots, m-1$, e $n_m > 3$, do Corolário 3.10 temos que $S_3(2^{n_m}) = 2^k$ onde $n_m \leq k$, assim os únicos valores para $S_3(2^{n_m})$ são, 0,1,2,2^2 e 2^3. Isto implica que

$$\nu_3(n) \leq 3 + m$$

onde, como vimos m é o número de iterações até n ser igual a 0,1,2,2^2 e 2^3, o número 3 vem do fato que se $S_3(2^{n_m}) = 2^3 = 22$, $S_3^2(2^{n_m}) = 2^2 = 11$ e $S_3^3(2^{n_m}) = 1$ então o número máximo de iterações restantes é 3. Como m é um número desconhecido, vamos encontrar um limite razoável para este.

Seja k_j denotando o número de dígitos da expansão na base ternária de n_j, para $j = 1, 2, \ldots, m$. Como $n_j > 3$ deduzimos da Proposição 3.9 e do Corolário 3.10 que $S_3(2^{n_j}) = 2^{n_{j+1}} \leq 2^{k_j - 1}$. Mas vimos também que $k_j = 1 + \lfloor \log_3 2^{n_j} \rfloor = 1 + \lfloor n_j \log_3 2 \rfloor$. Portanto temos que

$$S_3(2^{n_j}) = 2^{n_{j+1}} \leq 2^{k_j - 1} \Leftrightarrow n_{j+1} \leq k_j - 1 = \lfloor n_j \log_3 2 \rfloor \leq n_{j+1} \leq \alpha n_j$$

onde $\alpha = \log_3 2$, para $j = 1, 2, \ldots, m-1$. Isto implica que

$$n_m \leq \alpha n_{m-1} \leq \alpha^2 n_{m-2} \leq \alpha^3 n_{m-3} \leq \cdots \leq \alpha^{m-1} n_1.$$

Como $n_m > 3$ e do fato anterior temos a desigualdade

$$3 < n_m \leq \alpha^{m-1} n_1.$$

Temos também que $n_1 \leq \log_3 n$ pois n_1 é o número de 2 que aparecem na expansão de n na base 3. Extraindo o logaritmo de base três da inequação acima e lembrando que $0 < \alpha < 1$ e $\log_3 \alpha < 0$ temos

$$\begin{aligned}
\log_3 3 < \log_3 n_m &\leq \log_3 \alpha^{m-1} n_1 \\
1 < \log_3 \alpha^{m-1} + \log_3 n_1 &< \log_3 \alpha^{m-1} + \log_3 \log_3 n \\
-m \log_3 \alpha &< -1 - \log_3 \alpha + \log_3 \log_3 n \\
-m &> \frac{-1 - \log_3 \alpha + \log_3 \log_3 n}{\log_3 \alpha} \\
m &< 1 + \frac{(\log_3 \log_3 n) - 1}{\log_3 \alpha^{(-1)}} \\
m &< 1 + \frac{\log_3 \log_3 n}{\log_3 \alpha^{(-1)}} - \frac{1}{\log_3 \alpha^{(-1)}} < 1 + 3 \log_3 \log_3 n - 2.
\end{aligned}$$

Isto demonstra que $\nu_3(n) \leq 2 + 3 \log_3 \log_3 n$. □

4 PROPRIEDADES DA PERSISTÊNCIA NA BASE TERNÁRIA

Nesta seção, estudaremos propriedades aritméticas e de medida da função de Sloane em base 3.

4.1 Periodicidade da cauda de uma expansão ternária

Observando as expansões na base ternária de sucessivas potências de dois, temos que para todo $k \geq 1$ o dígito $k \geq 1$ mais a direita destas potências exibem um comportamento periódico, como na Figura 1. Nosso objetivo aqui é calcular o período mínimo. Esta periodicidade é mais geral: os últimos k dígitos de expansão na base q de p^n formam uma sequência periódica, para todo $1 < p < q$. Este fato é uma consequência simples da aritmética modular, e chamamos isso de periodicidade da cauda.

Vamos relembrar alguns fatos da aritmética modular. Se $q > 1$ é um inteiro, então o conjunto de todos os restos, ou resíduos, $r \in \{0, 1, 2, \ldots, q-1\}$ módulo q que são relativamente primos com q e formam um grupo multiplicativo (sob a multiplicação módulo q). Este grupo é o grupo de unidades da operação multiplicação no conjunto $\mathbb{Z}_q^*$, já que um elemento é uma unidade se e somente se tem inverso multiplicativo, e este tem inverso multiplicativo se e somente é coprimo com q. O grupo de unidades do grupo multiplicativo $(\mathbb{Z}_q^*, \cdot)$ é denotado como U_q (lembremos também que as unidades da operação multiplicação de um anel formam um grupo). O grupo U_q tem ordem $\phi(q)$, onde ϕ é a função totiente de Euler, isto é, $\phi(q)$ é o número de inteiros positivos menores do que ou iguais a q que são relativamente primos com q.

Definição 4.1. Um inteiro g é dito uma raiz primitiva módulo m se a classe residual, ou de restos, módulo m tem ordem $\phi(q)$, simbolicamente $\mathrm{ord}_m g = \phi(m)$.

Em particular se existe uma raiz primitiva, então o grupo U_m é cíclico, já que é gerado pela raiz primitiva g que tem ordem $\phi(q)$.

Lembremos também que dado $n = p_1^{e_1} \dots p_r^{e_r}$ com primos distintos $p_1, p_2, \dots, p_r$ e $e_1, e_2, \dots, e_r \in \mathbb{Z}_+$. Então

$$\phi(n) = \prod_{k=1}^{r} p_k^{e_k - 1}(p_k - 1) = n \cdot \prod_{k=1}^{r} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

onde a notação significa que o produto é estendido para todos os primos que dividem n.

Para um estudo estruturado de aritmética modular, sugerimos os Capítulos 2, 3 e 4 do livro Domingues e Iezzi (2003), Santos (1998) capítulos 2 e 6, LeVeque (1977) capítulos 3 e 4, e Ireland, Rosen e Rosen (1982) capítulos 3 e 4.

Vamos agora analisar as raízes primitivas módulo p^t, onde p é um número primo ímpar e $t \geq 1$ inteiro. As duas proposições seguintes são clássicas e podem ser vistas também na página 122 e 123 de Santos (1998).

Proposição 4.2. *Se a for uma raiz primitiva módulo p, p primo ímpar, com $a^{p-1} \not\equiv 1 \pmod{p^2}$, então*

$$a^{\phi(p^{t-1})} \not\equiv 1 \pmod{p^t} \tag{4.1}$$

para todo $t \geq 2$.

Prova. Demonstraremos (4.1) por indução em t. Para $t = 2$ temos

$$a^{\phi(p^{2-1})} = a^{\phi(p)} = a^{p-1} \not\equiv 1 \pmod{p^2}$$

uma vez que estamos admitindo $a^{p-1} \not\equiv \pmod{p^2}$.

Como hipótese de indução, assumimos (4.1) como verdade para t e vamos provar que esta congruência continua válida quando substituímos t por $t+1$. Como o $\text{mdc}\,(a, p) = 1$ (a é uma raiz primitiva) temos que $\text{mdc}\,(a, p^{t-1}) = 1$ e assim pelo Teorema de Euler

$$a^{\phi(p^{t-1})} \equiv 1 \pmod{p^{t-1}}.$$

Esta congruência nos garante a existência de um número n tal que

$$a^{\phi(p^{t-1})} = 1 + np^{t-1} \tag{4.2}$$

o que iria contradizer nossa hipótese de indução. Sabendo $p \nmid n$, elevamos ambos os membros da equação (4.2) à potência p.

$$\begin{aligned}
[a^{\phi(p^{t-1})}]^p = a^{p\phi(p^{t-1})}] &= (1 + np^{t-1})^p \\
&= \sum_{i=0}^{p} \binom{p}{i} (np^{t-1})^i \\
&= \binom{p}{0} + \binom{p}{1} np^{t-1} + \binom{p}{2} n^2 p^{2(t-1)} + \sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i \\
&= 1 + np^t + \frac{p(p-1)}{2} n^2 p^{2t-2} + S \\
&= 1 + np^t + \frac{p-1}{2} n^2 p^{2t-1} + S.
\end{aligned}$$

Mas, sendo $3t - 3 = t + 2t - 3 \geq t + 1$ para $t \geq 2$, todo termo da soma

$$S = \sum_{i=3}^{p} \binom{p}{i} (np^{t-1})^i$$

possui uma potência de p maior do que ou igual a p^{t+1}.

Como $2t - 1 \geq t + 1$, para $t \geq 2$, a sequência de igualdades acima nos garante, módulo p^{t+1}, que

$$a^{p\phi(p^{t-1})} = a^{\phi(p^t)} \equiv 1 + np^t \pmod{p^{t+1}}.$$

Esta congruência nos garante que

$$a^{\phi(p^t)} \not\equiv 1 \pmod{p^{t+1}}$$

uma vez que $p \nmid n$. Mas isto é (4.1) com $t + 1$ no lugar de t, o que conclui a demonstração. □

Proposição 4.3. *Se p é um número primo ímpar, então uma raiz primitiva módulo p é também raiz primitiva módulo p^t, para todo $t \geq 1$ se, e somente se, $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

Prova. Seja a uma raiz primitiva módulo p e vamos supor que A também seja uma raiz primitiva módulo p^t, para $t \geq 1$. Neste caso teremos, em particular, que a é raiz primitiva módulo p^2 e isto implica que

$$a^{p-1} \not\equiv 1 \pmod{p^2}$$

pois, caso contrário, teríamos uma contradição, uma vez que $p-1 < p(p-1) = \phi(p^2)$.

Provaremos agora a recíproca, i.é, vamos admitir que a seja uma raiz primitiva módulo p para a qual $a^{p-1} \not\equiv 1 \pmod{p^2}$. Devemos mostrar que a é também uma raiz primitiva módulo p^t para todo $t \geq 2$.

Seja

$$k = \mathrm{ord}_{p^t} a$$

precisamos mostrar que

$$k = \phi(p^t).$$

Como $\phi(p^t) = p^{t-1}(p-1)$ temos que

$$n(p-1) | p^{t-1}(p-1) \quad \Rightarrow \quad n | p^{t-1}.$$

Logo, $n = p^h$, $h \leq t-1$. Portanto, $k = p^h \phi(p) = p^h(p-1)$.

Precisamos mostrar que $h = t-1$. Vamos supor que $h < t-1$, isto é, $h \leq t-2$. Neste caso, teríamos

$$k = p^h(p-1) | p^{t-2}(p-1) = \phi(p^{t-1}).$$

Isto nos diz que $\phi(p^{t-1})$ é um múltiplo de k e, portanto,

$$a^{\phi(p^{t-1})} \equiv 1 \pmod{p^t}.$$

Mas isto contradiz o Teorema 4.2 anterior. Logo $h = t-1$ então $n = p^{t-1}$ que implica

$$k = p^{t-1}\phi(p) = p^{t-1}(p-1) = \phi(p^t).$$

□

Lema 4.4. *Seja p e q inteiros tais que $1 < p < q$ e p é um raiz primitiva módulo q. Então os resíduos p^n módulo q, $n = 0, 1, 2, \ldots$ formam uma sequência periódica com um período mínimo igual a $\phi(q)$.*

Prova. Por hipótese, $p \in U_q$ é uma raiz primitiva, logo, está gera o grupo U_q (como vimos no capítulo 2). Portanto, pelo Teorema de Euler temos $p^{\phi(q)} \equiv 1 \pmod{q}$ e os elementos $1, p, p^2, \ldots, p^{\phi(q)-1}$ são incongruentes módulo q (devido a cardinalidade de U_q). Como $p^n \in \mathbb{Z}$, então podemos multiplicar $p^{\phi(q)} \equiv 1 \pmod{q}$ e assim obtemos $p^{n+\phi(q)} \equiv p^n \pmod{q}$ para todo n, logo a sequência p^n é de fato periódica, com período mínimo $\phi(q)$.

□

Figura 1 – Algumas potências de dois calculadas na base ternária

n	2^n em base 3																												
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	1	
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	2	
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	1		
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	0	2		
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1		
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	2	2		
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	2	2	1	
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	1	0	2	1	2	
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	1	2	1	2	0	1	
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	2	0	1	0	2
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	1	1	1	0	2	1	1
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	2	2	2	1	1	2	2
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2	2	2	2	0	0	2	1
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	1	2	2	2	1	0	1	1	2
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	2	2	1	2	1	0	0	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	1	2	2	0	1	2	0	0	2
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	0	2	1	1	0	1	0	1	1	
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	2	1	1	1	2	2	0	2	0	2	2	
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	2	2	0	0	0	2	1	1	1	1	2	1	
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	2	1	0	0	1	2	0	0	0	0	1	2	
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	2	0	1	0	1	0	0	0	1	0	1
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	1	0	2	0	2	0	0	0	2	0	2
26	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	0	0	0	2	1	1	1	1	0	0	1	1	1	1	
27	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	2	2	2	2	0	0	2	2	2	2	
28	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	0	1	0	0	2	2	2	1	0	1	2	2	2	1	
29	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	2	0	1	2	2	1	2	1	0	2	2	1	2	
30	0	0	0	0	0	0	0	0	0	0	2	2	0	2	2	1	1	1	0	2	2	0	1	2	1	2	2	0	1	
31	0	0	0	0	0	0	0	0	0	1	2	1	1	2	1	2	2	2	1	2	1	1	0	2	0	2	1	0	2	
32	0	0	0	0	0	0	0	0	1	0	2	0	0	2	0	2	2	2	0	1	2	2	1	1	1	1	2	1	1	
33	0	0	0	0	0	0	0	0	2	1	1	0	1	1	1	2	2	1	1	0	2	2	0	0	0	0	1	2	2	
34	0	0	0	0	0	0	0	1	1	2	2	1	0	0	0	2	1	2	2	1	2	1	0	0	0	1	0	2	1	
35	0	0	0	0	0	0	1	0	0	2	1	2	0	0	1	2	0	2	2	0	1	2	0	0	0	2	1	1	2	
36	0	0	0	0	0	0	2	0	1	2	0	1	0	1	0	1	1	2	1	1	0	1	0	0	1	2	0	0	1	
37	0	0	0	0	0	1	1	1	0	1	0	2	0	2	1	0	0	1	2	2	0	2	0	1	0	1	0	0	2	
38	0	0	0	0	0	2	2	2	0	2	1	1	1	1	2	0	1	0	2	1	1	1	0	2	0	2	0	1	1	
39	0	0	0	0	1	2	2	1	1	2	0	0	0	0	1	0	2	1	1	2	2	2	1	1	1	1	0	2	2	
40	0	0	0	1	0	2	2	0	0	1	0	0	0	0	2	1	2	0	0	2	2	1	2	2	2	2	1	2	1	
41	0	0	0	2	1	2	1	0	0	2	0	0	0	1	2	0	1	0	1	2	2	0	2	2	2	2	0	1	2	
42	0	0	1	2	0	1	2	0	1	1	0	0	1	0	1	0	2	1	0	2	1	1	2	2	2	1	1	0	1	
43	0	1	0	1	1	0	1	0	2	2	0	0	2	0	2	1	1	2	1	2	0	0	2	2	1	2	2	0	2	
44	0	2	0	2	2	0	2	1	2	1	0	1	1	1	2	0	0	2	0	1	0	1	2	2	0	2	1	1	1	
45	1	1	1	2	1	1	2	0	1	2	1	0	0	0	1	0	1	1	0	2	1	0	2	1	1	1	2	2	2	

Fonte: Elaborado pelo autor

Dados inteiros $k \geq 1$ e $n \geq 0$, seja $r_n(k)$ denotando o resíduo de 2^n módulo 3^k.

Proposição 4.5. *Para cada $k \geq 1$, a sequência $r_n(k)$, $n = 0, 1, \ldots$, é periódica com período mínimo $2 \cdot 3^{k-1}$.*

Prova. Para ver que 2 é uma raiz primitiva de 3^k, vamos inicialmente demonstrar que 2 é uma raiz primitiva de 3^2. Temos que 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7 e 2^8 são os resíduos 2, 4, 8, 7, 5, 1, 2 e 4. Desta forma $U_9 = \langle 2 \rangle$. Também vale que $2^{3-1} \not\equiv 1 \pmod{3^2}$, logo pela Proposição 4.3, temos que 2 é uma raiz primitiva de 3^k com $k \geq 1$.

Então, pelo Lema 4.4 anterior, tomando $p = 2$ e $q = 3^k$ temos que a sequência $n = 0, 1, 2, \ldots$ forma uma sequência com período igual a $\phi(3^k)$.

Desta forma

$$\phi(3^k) = 3^k - 3^{k-1} = 3^{k-1}(3-1) = 2 \cdot 3^{k-1}$$

como queríamos.

□

4.2 A função $T_{p,q}$ e sua medida invariante

Sejam dois inteiros $1 < p < q$ e considere a sequência p^n, com $n = 0, 1, 2, 3, \ldots$, escrita na base q, isto é

$$p^n = [d_{1,n} d_{2,n} \ldots d_{k_n,n}]_q = \sum_{i=1}^{k_n} d_{i,n} q^{k_n - i}, \tag{4.3}$$

onde $0 \leq d_{i,n} \leq q-1$ e $d_{1,n} \neq 0$, e onde o número de dígitos k_n é dado, como vimos por

$$k_n = 1 + \lfloor \log_q p^n \rfloor = 1 + \lfloor n \log_q p \rfloor = \lceil n \log_q p \rceil.$$

Se adicionarmos um "ponto decimal" na frente da expansão (4.3) de p^n anterior, temos o número

$$x_n = \frac{p^n}{q^{k_n}} = [0, d_{1,n} d_{2,n} \ldots d_{k_n,n}]_q \in \Delta_q \quad \text{onde} \quad \Delta_q = [\frac{1}{q}, 1] \subset \mathbb{R}. \tag{4.4}$$

Notemos que $x_0 = [0,1]_q = \dfrac{1}{q}$ e que k_n é o único inteiro tal que $\frac{p^n}{q^{k_n}}$ pertence a Δ_q.

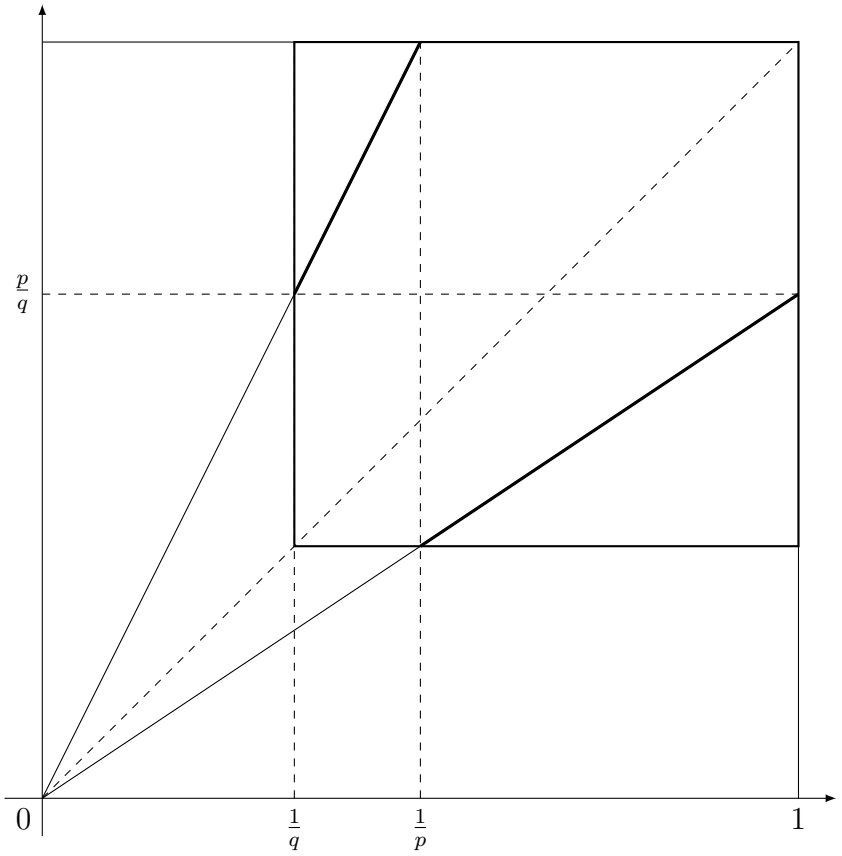
Agora, a observação crucial é que a sequência (x_n) é definida é precisamente a órbita de $x_0 = 1/q$ sob a função afim definida por partes como

$$T_{p,q} : \Delta_q \to \Delta_q$$
$$x \mapsto T_{p,q}(x) = \begin{cases} px, & \text{se } \frac{1}{q} \leq x < \frac{1}{p} \\ \frac{p}{q}x, & \text{se } \frac{1}{p} \leq x \leq 1 \end{cases} \tag{4.5}$$

Esta função construída a partir de duas funções lineares na reta real: uma expandindo (multiplicando por $p > 1$), e outra contraindo (multiplicando por $p/q < 1$), vejamos a figura 2.

Veremos no próximo teorema que, através da identificação dos pontos finais do intervalo Δ_q, a função definida por partes $T_{p,q}$ torna-se um homeomorfismo com o círculo $\mathbb{S}^1$ (BOSHERNITZAN, 1993), (LIOUSSE, 2004).
Um exemplo seria aplicar a função com $p = 3$ e $q = 10$, teríamos então uma função constituída por duas partes, como exemplifica a figura 2 abaixo.

Figura 2 – A representação da função $T_{p,q}$, que é um pedaço da função do círculo construída com duas funções lineares, uma expandindo e outra contraindo



Fonte: (FARIA; TRESSER, 2013)

Lema 4.6. *Sejam $n = 0, 1, 2, \ldots$, dois inteiros $1 < p < q$ e considere a sequência p^n, com $n = 0, 1, 2, 3, \ldots$, escrita na base q. Então*

$$x_n := \frac{p^n}{q^{k_n}} = [0, d_{1,n}d_{2,n}\cdots d_{k_n,n}]_q = T^n_{p,q}(x_0)$$

onde $x_0 = [0, 1]_q = 1/q$.

Prova. Vamos mostrar que $x_n = T^n_{p,q}(x_0)$ para todo $n \geq 0$. Vamos aplicar a indução sobre n.

Se $n = 0$ então temos que $T^0_{p,q}(x_0) = x_0 \in \Delta_q$.

Suponha válido para n, i. é, $T_{p,q}^n(x_0) = x_n$ e demonstremos que $x_{n+1} = T^{n+1}(x_0)$. Vale

$$T_{p,q}^{n+1}(x_0) = T_{p,q}(T_{p,q}^n(x_0)) = T_{p,q}(x_n)$$

temos então dois casos a considerar:

- Se $\frac{1}{q} \leq x_n < \frac{1}{p}$ então $T_{p,q}(x_n) = px_n = \frac{p^{n+1}}{q^{k_n}} = x_{n+1}$.
- Se $\frac{1}{p} \leq x_n \leq 1$ então $T_{p,q}(x_n) = \frac{p}{q}x_n = \frac{p^{n+1}}{q^{k_n+1}}$. Como $T_{p,q}(x_n)$ pertence a Δ_q, então $k_n = k_{n+1}$ (pois k_{n+1} é o único inteiro tal que $\frac{x_{n+1}}{q^{k_{n+1}}}$ pertence a Δ_q. Portanto $T_{p,q}(x_n) = x_{n+1}$

O que demonstra o resultado. □

Teorema 4.7. *A função $T_{p,q} : \Delta_q \to \Delta_q$ é topologicamente conjugada à rotação de ângulo $\alpha = \log_q p$ no círculo $\mathbb{S}^1$. A conjugação é, em particular, Lipschitz e diferenciável, exceto em um único ponto. Além disso, $T_{p,q}$ tem uma medida invariante absoluta contínua dada por*

$$d_\mu(x) = \frac{\mathrm{d}x}{x \log q}.$$

Prova. Vamos escrever $T := T_{p,q}$ na demonstração. Relembremos que

$$k_n = \lceil n\alpha \rceil = 1 + \lfloor n\alpha \rfloor = 1 + n\alpha - \{n\alpha\}.$$

Logo

$$T^n(x_0) = \frac{p^n}{q^{\lceil n\alpha \rceil}} = \frac{p^n}{q^{1+n\alpha-\{n\alpha\}}} = \frac{1}{q^{1-\{n\alpha\}}} \left(\frac{p}{q^\alpha}\right)^n = q^{\{n\alpha\}-1}$$

pois $\frac{p}{q^\alpha} = 1$. Vamos definir

$$\begin{aligned} h : [0,1] &\to \Delta_q \\ t &\mapsto h(t) = q^{t-1} = \frac{1}{q}\exp(t \ln q), \end{aligned} \tag{4.6}$$

vemos que

$$h(\{n\alpha\}) = \frac{1}{q}\exp(\{n\alpha\} \cdot \ln q) = T^n(x_0).$$

Seja $a \in \mathbb{R}$ e $R_a : [0,1] \to [0,1)$ a função definida por $R_a(x) = x + a \pmod 1$. Observe que para todo inteiro $n \geq 0$, tomando $a = \alpha$, temos que $R_\alpha^n(0) = \{n \cdot \alpha\}$ e

temos $h(R_\alpha^n(0)) = h(\{n\alpha\}) = T^n(x_0)$ que é o mesmo que dizer que h leva a órbita de 0 sob a rotação $R_\alpha : t \mapsto t + \alpha \pmod 1$ sobrejetivamente na órbita de x_0 sob T. Isso sugere que:

Afirmação: T é conjugado a R_α^n por h, i.é $h \circ R_\alpha = T \circ h$.

Para ver isto, seja $t \in [0, 1]$ e daí temos duas possibilidades

(i) Se $0 \leq t < 1-\alpha$ então $0 \leq t+\alpha < 1$, deste modo a função piso de $\lfloor t+\alpha \rfloor = 0$. Logo $R_\alpha(t) = t + \alpha \pmod 1 = \{t + \alpha\} = t + \alpha - \lfloor t + \alpha \rfloor = t + \alpha + 0 = t + \alpha$ e assim

$$h \circ R_\alpha(t) = h(R_\alpha(t)) = h(t + \alpha) = q^{(t+\alpha)-1} = q^{\log_q p} h(t) = ph(t).$$

Temos que $h(t) \in \Delta_q$, o fato que $0 \leq t < 1-\alpha$ implica $h(0) \leq h(t) < h(1-\alpha)$ e assim

$$q^{-1} \leq h(t) < q^{(1-\alpha)-1} \quad \Rightarrow \quad \frac{1}{q} \leq h(t) < \frac{1}{p} \quad \Rightarrow \quad T(h(t)) = ph(t).$$

Portanto

$$h \circ R_\alpha(t) = ph(t) = T \circ h(t).$$

(ii) Se $1 - \alpha \leq t \leq 1$ então $1 \leq t + \alpha \leq 1 + \alpha$ e assim $R_\alpha(t) = t + \alpha - \lfloor t + \alpha \rfloor = t + \alpha - 1$. Logo

$$h \circ R_\alpha(t) = q^{t+\alpha-2} = q^{\log_q p - 1} h(t) = \frac{p}{q} h(t) = T \circ h(t).$$

A última igualdade vale pois $1 - \alpha \leq t \leq 1$ implica $h(1-\alpha) \leq h(t) < h(1)$ e assim

$$q^{(1-\alpha)-1} \leq h(t) \leq q^{1-1} \quad \Rightarrow \quad \frac{1}{p} \leq h(t) \leq 1 \quad \Rightarrow \quad T(h(t)) = \frac{p}{q} h(t).$$

Destes dois casos segue então que $h \circ R_\alpha = T \circ h$, como queríamos demonstrar.

Temos que a função h é um homeomorfismo devido à sua definição, na equação (4.6), isto pois é uma composição de funções homeomorfas. Também h é um difeomorfismo analítico com o intervalo aberto $(0, 1)$. Das afirmações anteriores

temos que h é um homeomorfismo com o círculo $\mathbb{S}^1$ que é diferenciável em todos os pontos, exceto em um ponto, o qual não existe a derivada.

A medida invariante absoluta μ para T em Δ_q pode ser obtida de maneira simples pela medida imagem[1] da medida de Lebesgue λ no intervalo $[0,1]$ via h. Para isto, se $E \subseteq \Delta_q$ é Borel mensurável, a medida imagem nos dá que

$$\mu(E) = \lambda(h^{-1}(E)).$$

Temos que $h^{-1} : \Delta_q \to [0,1]$ e que, dado um conjunto $E \subseteq \Delta_q$ mensurável. Note que se $t \in h^{-1}(E)$ então existe $x \in E \subseteq \Delta_q$ tal que $t = h^{-1}(x)$. Desta forma, de $t = h^{-1}(x)$ temos que $\mathrm{d}t = (h^{-1})'(x)\mathrm{d}x$ com $x \in E \subset \Delta_q$, assim

$$\mu(E) = \lambda(h^{-1}(E)) = \int_{h^{-1}(E)} \mathrm{d}t = \int_E (h^{-1})'(x)\mathrm{d}x.$$

Da equação (4.6) temos

$$h^{-1}(x) = \frac{\ln qx}{\ln q},$$

então

$$\mathrm{d}\mu(x) = (h^{-1})'(x)\mathrm{d}x = \frac{1}{x \ln q}\mathrm{d}x,$$

como queríamos demonstrar.

□

4.3 Um resultado da densidade de números com zeros em sua expansão

Para provar o primeiro Corolário do Teorema 4.7 anterior, relembraremos a definição de densidade inferior de um subconjunto dos inteiros.

Definição 4.8. A densidade inferior D^- (respectivamente superior D^+) de um subconjunto $A \subseteq \mathbb{Z}_+$ é dada pela equação

$$D^-(A) = \liminf_{n\to\infty} \frac{1}{n}\#(A \cap [1,n])$$

[1] Conhecida em inglês como *pushforward measure*.

$$\left(\text{ respectivamente } D^+(A) = \limsup_{n\to\infty} \frac{1}{n}\#(A \cap [1,n]) \right).$$

A definição anterior pode ser encontrada na página 58 de Viana e Oliveira (2014).

Definição 4.9. Seja $A \subseteq \mathbb{Z}_+$. Se as densidades inferior e superior são iguais, então dizemos que A tem uma densidade assintótica $D(A) = D^+(A) = D^-(A)$.

Teorema 4.10. *Se $1 < p < q$ são tais que $\log_q p$ é irracional, então o conjunto $A = \{n \in \mathbb{Z}_+ : S_q(p^n) = 0\}$ tem densidade assintótica igual a 1.*

Prova. Inicialmente tomemos $T = T_{p,q}$, μ a medida criada no Teorema 4.7 e $x_n = T^n(x_0)$.
É conhecido que a rotação no círculo é unicamente ergódica se, e somente se, o ângulo é um número irracional. Vimos que T é uma função Lipschitziana (logo contínua) e conjugada com uma rotação irracional no círculo $\mathbb{S}^1$, logo T também é unicamente ergódica.

Para cada $j \geq 1$, seja $B_j \subseteq \Delta_q$ o conjunto de todos os pontos x cuja expansão na base q tenha pelo menos um dígito 0 entre seus primeiros j dígitos. Então B_j é uma união finita de intervalos e vamos encontrar sua medida.
O conjunto B_j é a união de todos os conjuntos $[a_1 \dots a_k 0]$ com $2 \leq k \leq j-1$ e $a_1, \dots, a_k$ pertencem à $\{1, 2, \dots, q-1\}$ e $[a_1 \dots a_k 0]$ é conjunto dos x em Δ_q cuja expansão na base q, começa com $a_1 \dots a_k 0$, isto é

$$x = \frac{a_1}{q} + \frac{a_2}{q^2} + \cdots + \frac{a_k}{q^k} + \sum_{i=k+2}^{\infty} \frac{b_i}{q^i} \quad \text{onde } b_i \in \{0, 1, ..., q-1\}.$$

Observe que a medida de Lebesgue de cada $[a_1 \dots a_k 0]$ é $\frac{1}{q^{k+1}}$, logo a medida de todos os conjuntos $[a_1 .....a_k 0]$, $a_i \in \{1, ..., q-1\}$ é $\frac{(q-1)^k}{q^{k+1}}$.
Como dois conjuntos quaisquer distintos $[a_1 .....a_k 0]$, $2 \leq k \leq j-1$, $a_i \in \{1, 2, ..., q-1\}$ não se intersectam ou se intersectam num conjunto de medida de Lebesgue 0, deduzimos que

$$\lambda(B_j) = \frac{(q-1)}{q^2} + \frac{(q-1)^2}{q^3} \cdots \frac{(q-1)^{j-1}}{q^j} = \frac{(q-1)}{q^2}(1 + r + ...r^{j-2})$$

onde $r = \frac{(q-1)}{q} = 1 - \frac{1}{q}$. Isso implica que

$$\lambda(B_j) = \frac{(q-1)}{q^2}(1 - r^{j-1})(1 - r) = |\Delta_q| \left(1 - \left(1 - \frac{1}{q}\right)^{j-1}\right).$$

e assim

$$\lambda(B_j) = |\Delta_q| \left[1 - \left(1 - \frac{1}{q}\right)^{j-1}\right].$$

Então

$$\lim_{j\to\infty} \lambda(B_j) = \lim_{j\to\infty} |\Delta_q| \left[1 - \left(1 - \frac{1}{q}\right)^{j-1}\right] = |\Delta_q| \cdot 1 = |\Delta_q|.$$

Por outro lado

$$\mu(B_j) = \int_{B_j} \frac{\mathrm{d}x}{x \ln q}.$$

Como $\lambda(B_j)$ tende para $\lambda(\Delta_q)$ quando j tende para o infinito, deduzimos que $\mu(B_j)$ tende para

$$\int_{\Delta_q} \frac{\mathrm{d}x}{x \ln q} = 1.$$

Note que se $x_n \in B_j$ para algum n com $k_n \geq j$, então $S_q(p^n) = 0$, i.é $n \in A$. Como B_j é uma união finita de intervalos e μ é uma medida regular de Borel, podemos encontrar uma função contínua $f_j : \Delta_q \to \mathbb{R}$ tal que $0 \leq f_j \leq \chi_{B_j}$ em todo ponto e

$$\int_{\Delta_q} f_j \mathrm{d}\mu \geq \mu(B_j) - \frac{1}{2j}. \tag{4.7}$$

Em particular, para todo $N \geq 1$ temos

$$\frac{1}{N} \sum_{n=0}^{N-1} \chi_{B_j} \circ T^n(x_0) \geq \frac{1}{N} \sum_{n=0}^{N-1} f_j \circ T^n(x_0). \tag{4.8}$$

Usando (4.7) e o fato que T é unicamente ergódica deduzimos, pelo Teorema 2.6, que a soma $\sum_{n=0}^{N-1} f_j \circ T^n(x_0)$ converge para a integral $\int_{\Delta_q} f_j \mathrm{d}\mu$, logo

$$\frac{1}{N} \sum_{n=0}^{N-1} f_j \circ T^n(x_0) \geq \int_{\Delta_q} f_j \mathrm{d}\mu - \frac{1}{2j} \geq \mu(B_j) - \frac{1}{j}, \tag{4.9}$$

para um N suficientemente grande. Então, combinando (4.8) e (4.9) temos que

$$\frac{1}{N}\sum_{n=0}^{N-1}\chi_{B_j}(x_n) \geq \mu(B_j) - \frac{1}{j}. \tag{4.10}$$

para todos N suficientemente grandes. Escrevendo $A_j = \{n \in \mathbb{Z}_+ : x_n \in B_j\}$, temos que

$$\begin{aligned} D^-(A_j) &= \liminf_{N\to\infty} \frac{1}{N}\#(A_j \cap [1,N]) \\ &= \liminf_{N\to\infty} \frac{1}{N}\sum_{i=0}^{N-1}\chi_{A_j\cap[1,N]}(x_n) \\ &= \liminf_{N\to\infty} \frac{1}{N}\sum_{n=0}^{N-1}\chi_{B_j}(x_n). \end{aligned}$$

e assim provamos que

$$D^-(A_j) \geq \mu(B_j) - \frac{1}{j}.$$

Como todos menos um número finito de elementos de A_j pertencem a A, segue que $D^-(A) \geq \mu(B_j) - \frac{1}{j}$ para todo j, como queríamos. Fazendo j tender para infinito, deduzimos que que $D^-(A) = 1$. Como $D^-(A) \leq D^+(A) \leq 1$. Deduzimos que $D(A) = 1$ o que completa a demonstração. □

Vamos a outra consequência do Teorema 4.7, que no caso é uma fórmula para encontrar um dígito da expansão de p^n na base q.

Corolário 4.11. *Sejam $\alpha = \log_q p$ e k_n é a quantidade de dígitos da expansão de p^n na base q. Então, para todo $j = 1, 2, ..., k_n$ o dígito $d_{j,n}$ da expansão de*

$$p^n = [d_{1,n}d_{2,n}\ldots d_{j,n}\ldots d_{k_n,n}]_q,$$

é dado pela fórmula

$$d_{j,n} = \lfloor q\{q^{j+\{n\alpha\}-2}\}\rfloor \tag{4.11}$$

Prova. Vamos denotar $T = T_{p,q}$. Como $d_{j,n}$ é também o j-ésimo dígito de $x_n = T^n(x_0)$ após a vírgula podemos seguir o seguinte raciocínio: 1) multiplicamos x_n por q^{j-1} logo o primeiro número após a vírgula será o dígito $d_{j,n}$; 2) tomamos somente a parte fracionária do número anterior; 3) multiplicamos por q deixando somente o

dígito $d_{j,n}$ do lado esquerdo da vírgula; 4) tomamos somente a parte inteira sem a fracionária do número, que será $d_{j,n}$. Da ideia anterior temos a fórmula

$$d_{j,n} = \lfloor q\{q^{j-1}x_n\}\rfloor. \tag{4.12}$$

Pelo Teorema 4.7 temos que

$$x_n = T^n(x_0) = h \circ R_\alpha^n(0) = h(\{n\alpha\}) = q^{\{n\alpha\}-1}. \tag{4.13}$$

Substituindo x_n da equação (4.12) em (4.13) obtemos a fórmula (4.11) que queríamos. □

Ter uma fórmula explícita para os $d_{j,k}$ dígitos é realmente divertido, porém, na prática ela não é tão útil. Isso se dá pois para valores grandes de n, calcular $d_{j,n}$ depende do conhecimento dos primeiros n dígitos de $\alpha = \log_q p$.

Faria e Tresser (2013) nos dizem que para as bases 3, 4, 5 e 10 tem-se boas evidências computacionais sugerindo a validade da conjectura baixo, que é uma forma mais forte da Conjectura 1a.

Conjectura 2. Se q não é uma potência de p, e $p^n = [d_{1,n}...d_{j,n}..d_{k_n,n}]_q$, então para cada $d = 0, 1, \ldots, q-1$, temos

$$\lim_{n\to\infty} \frac{1}{k_n} \#\{1 \le j \le k_n : d_{j,n} = d\} = \frac{1}{q}.$$

O que aconteceria se q fosse uma potência de p? Se $q = p^k$ para algum $k \ge 1$, então para todo $n \ge 1$ a expansão de p^{nk} na base q consiste de dígitos 1 seguidos por n zeros. Isto mostra que a hipótese que q não é uma potência de p é de fato realmente necessária.

5 AS $\mathbb{Z}^d$-AÇÕES ERGÓDICAS PARA A PERSISTÊNCIA DE NÚMEROS COM BASE MAIOR DO QUE 3

Neste capítulo vamos discutir os resultados para bases maiores que 3. O sistema dinâmico que utilizaremos será mais geral, mas baseado, no do capítulo 4. Também generalizaremos o resultado da densidade.

5.1 Sobre ações abelianas de grupo e sua relação com a função de Sloane

Sejam $2 = p_1 < p_2 < \cdots < p_m \leq q-1$ a lista de todos os primos menores que q. Se n é um inteiro positivo com $S_q(n) \neq 0$ podemos escrever

$$S_q(n) = \prod_{i=1}^{m} p_i^{n_i}, \tag{5.1}$$

onde

$$(n_1, n_2, \ldots, n_m) \in \mathbb{Z}_+^m = (\mathbb{Z}_+)^m \subset \mathbb{Z}^m.$$

Isso vale pois $S_q(n)$ resulta em uma multiplicação de dígitos menores que q, logo os dígitos são decompostos em primos menores que q.
Desta forma a equação anterior (5.1) fica similar a expansão de p^n na base q que vimos na seção 4.2.

Utilizando a mesma notação da seção 4.2, seja o intervalo, em destaque

$$\Delta_q = [q^{-1}, 1] \equiv \mathbb{S}^1,$$

e consideremos os homeomorfismos (que são funções definidas por partes)

$$T_{p_i,q} : \Delta_q \to \Delta_q$$
$$x \mapsto T_{p_i,q}(x) = \begin{cases} p_i x, & \text{se } \dfrac{1}{q} \leq x < \dfrac{1}{p_i} \\ \\ \dfrac{p_i}{q} x, & \text{se } \dfrac{1}{p_i} \leq x \leq 1 \end{cases} \qquad (i = 1, 2, \ldots, m). \tag{5.2}$$

Denotaremos $PL^+(\Delta)$ como o grupo de todos os homeomorfismos (afins por partes) de um intervalo $\Delta \subset \mathbb{R}$ qualquer. Assim as funções anteriores estão no grupo $PL^+(\Delta_q)$.

Lema 5.1. *O grupo $G_q \subset PL^+(\Delta_q)$ gerado por $\{T_{p_i} : i = 1, 2, \ldots, m\}$ é abeliano.*

Prova. Seja o homeomorfismo construído na demonstração do Teorema 4.7, por comodidade vamos reescrevê-lo abaixo

$$h : [0,1] \to \Delta_q$$
$$t \mapsto h(t) = q^{t-1} = \frac{1}{q} \exp(t \ln q).$$

Também seja

$$R_{\alpha_i} : [0,1] \to \mathbb{S}^1$$
$$x \mapsto R_{\alpha_i}(x) = x + \alpha_i \pmod 1$$

a rotação onde o ângulo é $\alpha_i = \log_q p_i$.
Então para cada i temos que $T_{p_i} = h \circ R_{\alpha_i} \circ h^{-1}$.
Como quaisquer duas rotações no círculo são comutativas, temos que

$$R_{\alpha_i} \circ R_{\alpha_j} = R_{\alpha_j} \circ R_{\alpha_i}$$

o que implica

$$T_{p_i} \circ T_{p_j} = T_{p_j} \circ T_{p_i}.$$

Portanto G_q é abeliano. □

Uma conclusão que podemos retirar do lema acima é que existe um homomorfismo, bem definido, da forma

$$\begin{aligned} T^{\mathbf{n}} : \mathbb{Z}^m &\to G_q \\ \mathbf{n} &\mapsto T^{\mathbf{n}} = T_{p_1}^{n_1} \circ T_{p_2}^{n_2} \circ \cdots \circ T_{p_m}^{n_m} \in G_q \end{aligned}$$

onde $\mathbf{n} = (n_1, n_2, \ldots, n_m) \in \mathbb{Z}^m$.
A sobrejetividade existe, mas a injetividade nem sempre já que a composição de funções é comutativa. A conclusão é que $\mathbb{Z}^m$ age no círculo de modo especial como um grupo de homeomorfismos (definidos por partes, que são as funções T_{p_i,n_i}) com o círculo.

Para ver a relevância, ou utilidade, desta função anterior (que é uma ação) para o estudo da função Sloane na base q vamos organizar as notações baseadas na seção 4.2.

Seja $x_0 = [0,1]_q = \frac{1}{q} \in \Delta_q$. Então, para cada $\mathbf{n} \in \mathbb{Z}_+^m$, temos

$$T^{\mathbf{n}}(x_0) = \frac{{p_1}^{n_1} {p_2}^{n_2} \cdots {p_m}^{n_m}}{q^{k(\mathbf{n})}}, \tag{5.3}$$

onde $k(\mathbf{n})$ é o número de dígitos da expansão na base q do numerador, dada por

$$k(\mathbf{n}) = \left\lceil \sum_{i=1}^{m} n_i \log_q p_i \right\rceil = \left\lceil \sum_{i=1}^{m} n_i \alpha_i \right\rceil.$$

Como restringimos mais o $\mathbf{n}$ para valores positivos, vemos que toda a gama de valores assumidos pela função de Sloane está contida em uma única órbita da ação do semigrupo $\mathbb{Z}_+^m \subset \mathbb{Z}_+$.

5.2 Primeiro resultado da densidade para números com base maior do que 4

Voltemos as nossas investigações da função de Sloane.

Definição 5.2. Dado um inteiro positivo N, e seja Λ_N denotando o "cubo" $\Lambda_N = \{\mathbf{n} \in \mathbb{Z}_m : |n_i| \leq N,\ i = 1, 2, \ldots, m\}$, e seja $\Lambda_N^+ = \Lambda_N \cap \mathbb{Z}_+^m$. A densidade assintótica

inferior de um subconjunto $A \subseteq \mathbb{Z}_+^m$ é definida como

$$D^-(A) = \liminf_{N\to\infty} \frac{1}{N^m} \#(A \cap \Lambda_N^+).$$

A densidade assintótica superior é definida como

$$D^+(A) = \limsup_{N\to\infty} \frac{1}{N^m} \#(A \cap \Lambda_N^+).$$

Notemos que

$$\begin{aligned}\Lambda_N^+ &= \Lambda_N \cap \mathbb{Z}_+^m \\ &= \{\mathbf{n} \in \mathbb{Z}^m,\, N \in \mathbb{Z}_+ : |n_i| \leq N \text{ e } n_i \geq 0,\, i = 1, \ldots, m\} \\ &= \{\mathbf{n} \in \mathbb{Z}_+^m,\, N \in \mathbb{Z}_+ : n_i \leq N,\, i = 1, \ldots, m\}.\end{aligned}$$

Sempre temos que $0 \leq D^-(A) \leq D^+(A) \leq 1$ (isso é importante para interpretar o resultado, como vimos no caso da seção 4.3). Quando $D^-(A) = D^+(A)$, este valor comum é chamado de densidade assintótica de A e é denotada por $D(A)$.

Proposição 5.3. *Se a base q não é um número primo, então o conjunto*

$$A = \{\boldsymbol{n} = (n_1, n_2, \ldots, n_m) \in \mathbb{Z}_+^m : S_q(p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}) = 0\}$$

tem densidade assintótica igual a 1.

Prova. Por hipótese, temos que q não é primo, logo podemos escrevê-lo como fatores primos

$$q = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

onde cada $a_i \geq 0$.

Se $\mathbf{n} \in \mathbb{Z}_+^m$ é tal que $n_i \geq a_i$ para todo i, então q divide $p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$, e portanto

$$S_q(p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}) = 0$$

já que vai ser combinação da base, pois só mudamos o expoente dos fatores primos. Isso mostra que o conjunto dos múltiplos da base está contido em A, i.é, $\{\mathbf{n} \in \mathbb{Z}_+^m : n_i \geq a_i \text{ para todo } i\} \subseteq A$. Temos que

$$A \cap \Lambda_N^+ = \{\mathbf{n} \in \mathbb{Z}_+^m,\, N \in \mathbb{Z}_+ : n_i \leq N \text{ e } S_q(p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}) = 0\}.$$

Então, para todo N suficientemente grande temos que

$$\#(A \cap \Lambda_N^+) \geq \prod_{i=1}^{m}(N - a_i + 1),$$

e portanto

$$D^-(A) \geq \lim_{N\to\infty} \frac{1}{N^m} \prod_{i=1}^{m}(N - a_i + 1) = 1$$

o que prova que $D(A) = D^-(A) = 1$. □

5.3 Segundo resultado da densidade para números com base maior do que 4

Para um segundo resultado da densidade, que será uma generalização do primeiro, utilizaremos o grupo G_q e sua ação no círculo. Na verdade, utilizaremos certos subgrupos de G_q, que acabam sendo grupos abelianos livres.

Dados inteiros positivos ordenados $1 \leq i_1 < i_2 < \cdots < i_k \leq m$, vamos denotar o subgrupo de G_q gerado por $\{T_{p_{i_1}}, T_{p_{i_2}} \ldots, T_{p_{i_k}}\}$ por $G(i_1, i_2, \ldots, i_k)$. Temos também que $\alpha_i = \log_q p_i$ é o ângulo da rotação para T_{p_i} que usamos no Lema 5.1.

Lema 5.4. *Se os números $1, \alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ são racionalmente independentes, i.é, são linearmente independentes no conjunto dos racionais, então $G(i_1, i_2, \ldots, i_k)$ é um grupo abeliano livre de ordem k. Mais ainda, a ação no círculo $\Delta_q \equiv \mathbb{S}^1$ é unicamente ergódica.*

Prova. Suponhamos que $(n_1, n_2, \ldots, n_k) \in \mathbb{Z}^k$ de modo que

$$T_{p_{i_1}}^{n_1} \circ T_{p_{i_2}}^{n_2} \circ \cdots \circ T_{p_{i_k}}^{n_k} = Id.$$

Como cada T_{p_i} é conjugada com a rotação R_{α_i} pela mesma função, temos que

$$R_{\alpha_{i_1}}^{n_1} \circ R_{\alpha_{i_2}}^{n_2} \circ \cdots \circ R_{\alpha_{i_k}}^{n_k} = Id.$$

Mas então $n_1\alpha_{i_1} + n_2\alpha_{i_2} + \cdots + n_k\alpha_{i_k} \equiv 0 \pmod 1$. Podemos reescrever a expressão anterior como, existe $N \in \mathbb{Z}$ tal que

$$n_1\alpha_{i_1} + n_2\alpha_{i_2} + \cdots + n_k\alpha_{i_k} = N.$$

Pela hipótese da independência (linear) racional, isto implica que

$$n_1 = n_2 = \cdots = n_k = N = 0.$$

Então não há nenhuma relação não-trivial em $G(i_1, i_2, \ldots, i_k)$, o que implica que o grupo é abeliano livre. Mais ainda, um dos α_{i_j} deve ser irracional. Digamos que α_{i_1} é irracional; então $T_{p_{i_1}}$, sendo conjugada a uma rotação irracional, é unicamente ergódica. Isto pois cada uma das funções $T_{p_{i_k}}$ conjugadas pela rotação irracional com mesmo homeomorfismo, é diferenciável em todos os pontos, exceto um. Desta forma há somente uma medida invariante e assim cada uma das funções $T_{p_{i_k}}$ é unicamente ergódica, o que implica a ação no grupo todo ser unicamente ergódica.

Portanto, a ação de $G(i_1, i_2, \ldots, i_k)$ no círculo é unicamente ergódica. □

Vamos agora demonstrar o segundo resultado da densidade. Este segundo resultado, na verdade, generaliza a Proposição 5.3, a qual era para uma base q não prima, já que agora consideraremos q primo.
As hipóteses do próximo Teorema foram feitas de modo que a demonstração fique parecida com a prova do Teorema 4.10, mudando o necessário.

Teorema 5.5. *Seja $1 \leq i_1 < i_2 < \cdots < i_k \leq m$ escolhidos de forma que os números $1, \alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ são racionalmente independentes. Então para todo divisor d de q, o conjunto*

$$A = \left\{(n_1, n_2, \ldots, n_k) \in \mathbb{Z}_+^k : S_q(p_{i_1}^{n_1} p_{i_2}^{n_2} \cdots p_{i_k}^{n_k} \cdot d) = 0\right\}$$

tem densidade assintótica igual a 1.

Prova. Temos que pelo Lema 5.4, a ação de grupo $G = G(i_1, i_2, \ldots, i_k) \cong \mathbb{Z}^k$ no círculo $\Delta_q \equiv \mathbb{S}^1$ é unicamente ergódica; a medida invariante única é a medida μ, como foi construída no Teorema 4.7.
Fixemos o divisor d para a base q. Estamos interessados em uma órbita particular (isto é, uma iteração das funções com um valor inicial em particular) para o semigrupo $G^+ \cong \mathbb{Z}_+^k$, chamando este ponto de $w_0 = \frac{d}{q} \in \Delta_q$.
Para cada $\mathbf{n} \in \mathbb{Z}_+^k$, escrevamos $w_{\mathbf{n}} = T^{\mathbf{n}}(w_0)$. Também, denotemos por $\ell(\mathbf{n})$ o número de dígitos da expansão na base q do número $p_{i_1}^{n_1} p_{i_2}^{n_2} \cdots p_{i_k}^{n_k} \cdot d$. Assim como

na equação (5.3) temos

$$w_{\mathbf{n}} = \frac{p_{i_1}^{n_1} p_{i_2}^{n_2} \cdots p_{i_k}^{n_k} \cdot d}{q^{\ell(\mathbf{n})}}. \tag{5.4}$$

Como na prova do Teorema 4.10 para cada $j \geq 1$, seja $B_j \subseteq \Delta_q$ o conjunto de todos os pontos x em que a expansão na base q tenha pelo menos um dígito 0 nos seus primeiros j dígitos. Como vimos anteriormente, $\lim_{j\to\infty} \mu(B_j) = 1$.
Seja $f_j : \Delta_q \to \mathbb{R}$ (como na demonstração do Teorema 4.7), logo cada f_j é contínua e $0 \leq f_j \leq \chi_{B_j}$, e

$$\int_{\Delta_q} f_j \mathrm{d}\mu \geq \mu(B_j) - \frac{1}{2j}. \tag{5.5}$$

Da equação (5.4) temos que

$$S_q(p_{i_1}^{n_1} p_{i_2}^{n_2} \cdots p_{i_k}^{n_k} \cdot d) = 0 \quad \Leftrightarrow \quad T^{\mathbf{n}}(w_0) = w_{\mathbf{n}} \in B_j \text{ para algum } j \leq \ell(\mathbf{n}).$$

Isso nos diz que $\mathbf{n} \in A$ se, e somente se, $w_{\mathbf{n}} \in B_j$ para algum $j \leq k_{\mathbf{n}}$.
Analogamente, como fizemos na demonstração do Teorema 4.10, para cada $j \leq 1$ definamos $A_j = \{\mathbf{n} \in \mathbb{Z}_+^k : w_{\mathbf{n}} \in B_j\}$.
Notemos que todos, menos um número finito de elementos de A_j, pertencem a A. Então, a fim de provar que $D(A) = 1$, é suficiente mostrar que $\lim_{j\to\infty} D^-(A_j) = 1$.
Como a ação de G^+ no círculo é unicamente ergódica, combinando o Teorema 2.17 com a equação (5.5) isto implica que, para cada j fixo e para todo N suficientemente grande,

$$\frac{1}{\#\Lambda_N^+} \sum_{\mathbf{n}\in\Lambda_N^+} f_j \circ T^{\mathbf{n}}(w_0) \geq \int_{\Delta_q} f_j \mathrm{d}\mu - \frac{1}{2j} \geq \mu(B_j) - \frac{1}{j}.$$

Como $f_j \leq \chi B_j$, segue que

$$\frac{1}{\#\Lambda_N^+} \sum_{\mathbf{n}\in\Lambda_N^+} \chi B_j(w_{\mathbf{n}}) \geq \mu(B_j) - \frac{1}{j},$$

para todo N suficientemente grande. Fazendo $N \to \infty$, isto mostra que

$$D^-(A_j) \geq \mu(B_j) - \frac{1}{j}$$

para todo j, e portanto $\lim_{j\to\infty} D^-(A_j) = 1$ como queríamos. □

REFERÊNCIAS

BOSHERNITZAN, M. D. Dense orbits of rationals. *Proceedings of the American Mathematical Society*, American Mathematical Society, v. 117, n. 4, p. 1201–1203, 1993. Disponível em: <https://doi.org/10.1090/S0002-9939-1993-1134622-6>. 42

DOMINGUES, H.; IEZZI, G. *Álgebra Moderna: Edição Reformulada.* [S.l.]: Atual, 2003. ISBN 9788535704013. 36

EINSIEDLER, M.; WARD, T. *Ergodic Theory: with a view towards Number Theory.* [S.l.]: Springer London, 2010. (Graduate Texts in Mathematics). ISBN 9780857290212. 13, 14, 15

FARIA, E. de; TRESSER, C. *On Sloane's persistence problem.* 2013. 5, 6, 11, 30, 43, 50

IRELAND, K.; ROSEN, M. M.; ROSEN, M. *A Classical Introduction to Modern Number Theory.* [S.l.]: Springer-Verlag, 1982. (Graduate texts in mathematics). ISBN 9783540906254. 36

KELLER, G. *Equilibrium States in Ergodic Theory.* [S.l.]: Cambridge University Press, 1998. (London Mathematical Society Student Texts). 20, 24

KUEHN, C. *An Introduction to Rotation Theory.* Society for Industrial and Applied Mathematics, 2007. Disponível em: <https://dsweb.siam.org/Education/an-introduction-to-rotation-theory>. 14

LEVEQUE, W. *Fundamentals of Number Theory.* [S.l.]: Addison-Wesley, 1977. 36

LIOUSSE, I. Pl homeomorphisms of the circle which are piecewise c 1 conjugate to irrational rotations. *Bulletin Brazilian Mathematical Society*, v. 35, p. 269–280, 07 2004. 42

MIHAILESCU, P. Primary cyclotomic units and a proof of catalan's conjecture. *Journal fur die Reine und Angewandte Mathematik*, p. 167–195, 01 2004. 32

SANTOS, J. D. *Introdução à Teoria dos Números.* [S.l.]: IMPA, 1998. (Coleção Matemática Universitária). 36

SLOANE, N. The persistence of a number. *Journal of Recreational Mathematics*, v. 6, p. 97–98, 01 1973. 10, 29

VIANA, M.; OLIVEIRA, K. *Fundamentos da Teoria Ergódica*. SBM, 2014. (Coleção Fronteiras da Matemática). Disponível em: <http://w3.impa.br/~viana/out/OV3.pdf>. 14, 47

WALTERS, P. *An Introduction to Ergodic Theory*. [S.l.]: Springer New York, 2000. (Graduate Texts in Mathematics). ISBN 9780387951522. 15, 16