Universidade Estadual de Londrina

LUCAS MORENO LUNA

TRANSDUTORES E APLICAÇÕES NAS FRAÇÕES CONTINUADAS

Londrina
2020

LUCAS MORENO LUNA

TRANSDUTORES E APLICAÇÕES NAS FRAÇÕES CONTINUADAS

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Estadual de Londrina, como requisito parcial para a obtenção do Título de MESTRE em Matemática Aplicada e Computacional.

Orientador: Prof. Dr. Túlio Oliveira de Carvalho

Londrina
2020

Catalogação elaborada pela Divisão de Processos Técnicos da Biblioteca Central da Universidade Estadual de Londrina

Dados Internacionais de Catalogação -na-Publicação (CIP)

L961 Luna, Lucas Moreno.
Transdutores e Aplicações nas Frações Continuadas /
Lucas Moreno Luna. – Londrina, 2020.
54 f.

Orientador: Túlio Oliveira de Carvalho.
Dissertação (Mestrado em Matemática Aplicada e Computacional) – Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática Aplicada e Computacional, 2020.

Inclui Bibliografia.

1. Autômatos - Tese. 2. Transdutores - Tese. 3. Frações Continuadas - Tese. I. Carvalho, Túlio Oliveira de. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática Aplicada e Computacional. III. Título.

CDU 51

LUCAS MORENO LUNA

TRANSDUTORES E APLICAÇÕES NAS FRAÇÕES CONTINUADAS

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Estadual de Londrina, como requisito parcial para a obtenção do Título de MESTRE em Matemática Aplicada e Computacional.

BANCA EXAMINADORA

Prof. Dr. Túlio Oliveira de Carvalho
Universidade Estadual de Londrina – UEL

Prof. Dr. Marcus Vinicius Araújo Lima
Universidade Federal de São Carlos - UNESP

Prof. Dr. Paulo Antonio Liboni Filho
Universidade Estadual de Londrina - UEL

Londrina, 9 de outubro de 2020.

Dedico este trabalho a todos que passaram por 2020.
Número par, ano ímpar.

AGRADECIMENTOS

Agradeço ao meu orientador, Prof. Túlio de Oliveira Carvalho, por toda paciência, dedicação e pelo apoio que tive em um momento bastante obscuro de minha vida.

À CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, Código de Financiamento 001, pelo apoio financeiro cedido para o desenvolvimento dos meus estudos.

Agradeço, de modo geral, a todos os que, direta ou indiretamente, me ajudaram.

LUNA, Lucas Moreno. **Transdutores de Raney e Aplicações nas Frações Continuadas.** 2020. 54 f. Dissertação (Mestrado em Matemática Aplicada e Computacional) – Universidade Estadual de Londrina, Londrina, 2020.

RESUMO

Esta dissertação apresenta os conceitos fundamentais da estrutura de um transdutor, em especial do transdutor de Raney e a forma como estes atuam sobre a representação de um número real por frações continuadas sob certas aplicações de Möbius. São apresentadas as estruturas matemáticas essenciais para a construção dos transdutores de Raney, como o monóide das palavras finitas, o conjunto das matrizes duplamente balanceadas com entradas inteiras, a definição da representação de um número real por frações continuadas regulares, algumas relações entre estas representações e as matrizes duplamente balanceadas. Ao final, expõem-se exemplos de operações de multiplicação por inteiros que esses transdutores realizam sobre as representações em frações continuadas regulares de números irracionais.

Palavras-chave: Transdutor. Frações Continuadas. Transformações De Möbius. Autômatos. Teoria Dos Números.

LUNA, Lucas Moreno. **Transdutor and Applications in Continued Fractions.** 2020. 54 p. Dissertação (Mestrado em Matemática Aplicada e Computacional) – Universidade Estadual de Londrina, Londrina, 2020.

ABSTRACT

This monograph presents the fundamental concepts on the structure of a transducer, especially the Raney transducer, and the form which they allow for the computation the continued fraction representation of the image of numbers under certain Möbius maps. The essential mathematical structures for the construction of the Raney transducers are presented, such as the monoid of finite words on an alphabet, the set of doubly balanced integer matrices, the representation of real numbers by regular continued fraction expansions, some relationships between these representations and the doubly balanced matrices. We conclude with examples of multiplication operations by integers that these transducers perform on the regular continued fraction representation of irrational numbers.

Keywords: Transducer. Continued Fractions. Möbius Maps. Automata. Number Theory.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A teoria dos autômatos é uma área da matemática relativamente recente, ligada à Álgebra e à Teoria de Computação. Com o avanço da tecnologia relacionada a computadores, esta teoria vem ganhando utilizações em inúmeros campos. Os textos [2, 6] são boas referências que trata destes objetos do ponto de vista matemático.

Esta dissertação tem como objetivo mostrar a construção de uma família de autômatos com interessantes aplicações à Teoria de Números. Trata-se de uma classe de autômatos que possuem um número finito de configurações, ou *estados*, chamados de transdutores de Raney. Sua estrutura foi originalmente estudada em [4].

Um transdutor pode ser interpretado como uma maquina que lê e escreve informações, podendo mudar de estado conforme lê a informação. Ele é um caso particular de um autômato de finitos estados de duas fitas. Pelo fato de que o transdutor de Raney tem a mesma natureza para a fita de entrada e a de saída, e como qualquer estado de um transdutor de Raney pode ser visto como um estado inicial, podemos trabalhar com uma definição mais enxuta de transdutor, a qual é introduzida na seção 1 do capítulo 5.

É interessante citar que os transdutores de Raney mostram como podemos enxergar a representação em frações continuadas de um número real por um produto infinito de matrizes 2×2 com entradas inteiras não-negativas e assim, possibilitando um estudo de como a fração continuada deste número se modifica sob a ação de transformações de Möbius, que também sejam representáveis por matrizes sobre os inteiros.

Estruturamos este trabalho a fim de construir os elementos necessários para a construção dos transdutores de Raney $\mathcal{T}_{n,v}$.

No capítulo 2 são abordados os conceitos introdutórios acerca do conjunto das palavras em $\{L, R\}$, que é a "linguagem" das fitas dos transdutores de Raney. Neste capítulo é estudado o cone $\mathcal{C}_2$, que funcionará como uma representação dos números reais utilizada pelo transdutor de Raney. A relação entre estes dois conjuntos é vista com mais detalhes na seção 3 do capítulo 4.

O capítulo 3 trata dos fundamentos para a representação de um número real por frações continuadas regulares, como elas convergem para o número em questão. Mais detalhes sobre as frações continuadas, bem como suas vantagens em relação à representação por decimais pode ser encontradas em [3].

O capítulo 4 trata do semigrupo de matrizes 2×2 não singulares balanceadas com entradas inteiras não negativas, bem como suas fatorações, as relações entre estas matrizes e os vetores de $\mathcal{C}_2$. Definem-se ainda as matrizes duplamente balanceadas, que serão os estados dos transdutores de Raney.

Por fim, no capítulo 5 é visto de fato como podemos trabalhar as matrizes duplamente balanceadas de forma que atuem como estados de um transdutor, definindo assim, os transdutores

de Raney, além de trabalharmos dois exemplos de transdutores de Raney: $\mathcal{T}_{2,1}$ e $\mathcal{T}_{3,1}$.

Caso seja conhecida a representação de um número real ξ por continuadas, os trandutores de Raney são uma ferramenta matemática para encontrar a representação em frações continuadas da imagem de ξ por uma transformação de Möbius f_M, fixada, cuja matriz M relacionada possui entradas inteiras. Este caso geral segue da análise aqui exposta, assim como em [4], e constitui um algoritmo mais claro em relação ao exposto em [1].

Podemos concluir que para o caso da multiplicação de um número real por um outro número real seria necessário um transdutor com infinitos estados, demonstrando que esta "simples" operação não pode ser realizada por um autômato finito.

Os transdutores de Raney podem ser utilizados como ferramenta de estudo acerca das representações dos números reais por frações continuadas, e nos permite um outro olhar sobre como representamos os números reais, constituindo assim, um interessante exemplo introdutório de assuntos de Teoria dos Números e de Teoria dos Autômatos.

2 PRELIMINARES

2.1 MONÓIDES E ISOMORFISMOS

Definição 2.1. *Dado um conjunto não-vazio A, uma* **operação binária associativa** *em A é uma função $* : A \times A \to A$ tal que $*(a, b) = a * b$, com $(a, b) \in A \times A$ e satisfazendo a seguinte propriedade:*

- *dados $a, b, c \in A$, $((a * b) * c) = (a * (b * c))$.*

Caso exista um elemento $e \in A$ tal que, para todo $a \in A$, vale $a * e = e * a = a$, dizemos que a operação $*$ possui um **elemento neutro**.

Caso existam dois elementos neutros e_1 e e_2 de uma operação binária $*$ em A, vale que $e_1 = e_1 * e_2 = e_2$, ou seja, o elemento neutro de uma operação binária é único.

Definição 2.2. *O par $(A, *)$, onde A é um conjunto não-vazio e $*$ é uma operação binária associativa é chamado um* **semigrupo**. *Caso $*$ possua um elemento neutro, $(A, *)$ é dito um* **monoide**.

Definição 2.3. *Um* **homomorfismo** *do semigrupo $(A, *)$ no semigrupo $(B, \star)$ é uma aplicação $\Phi : A \to B$ tal que, para todo $a, b \in A$, vale $\Phi(a * b) = \Phi(a) \star \Phi(b)$.*

Se $(A, *)$ é um monoide, e Φ é um homomorfismo, então $\Phi : A \to B$ leva o elemento neutro de A no elemento neutro de B, uma vez que, para todo $a \in A$,

$$\Phi(a) = \Phi(a * \epsilon) = \Phi(a) \star \Phi(\epsilon) \ ,$$

e o elemento neutro é único. Dizemos que Φ é um **isomorfismo** de monoides (semigrupos), quando Φ é um homomorfismo bijetivo.

Definição 2.4. *Em $\mathbb{R}^2$, denotamos por $\mathcal{C}_2$ o cone formado por todos os vetores $x = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix}$ satisfazendo $\xi_1, \xi_2 \geq 0$ e $\xi_1 + \xi_2 > 0$. Definimos a relação de equivalência $\sim$ em $\mathcal{C}_2$ da seguinte forma: dados $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ e $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, temos $x \sim y$ quando $x_1 y_2 = x_2 y_1$. Em $\mathcal{C}_2/\sim$, definimos a operação: $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 y_2 + x_2 y_1 \\ x_2 y_2 \end{pmatrix}$, no caso em que $x_2 + y_2 > 0$. Quando $x_2 = y_2 = 0$, vale que $\begin{pmatrix} x_1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.*

Proposição 2.5. *Sejam $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ e $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ vetores em $\mathcal{C}_2$. Se $x \sim y$ então existe $\alpha \in \mathbb{R}^+$ tal que $x = \alpha y$.*

Demonstração. Se $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \sim \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, então $x_1 y_2 = x_2 y_1$. Como $y \in \mathcal{C}_2$, então necessariamente ou $y_1 \neq 0$, ou $y_2 \neq 0$. Caso $y_1 \neq 0$, suponha que $x_1 = 0$. Então $x_2 y_1 = 0$ implicaria $x \notin \mathcal{C}_2$. Com isto, $x_1 \neq 0$ e $x_2 = \dfrac{x_1 y_2}{y_1}$. Logo $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ \frac{x_1 y_2}{y_1} \end{pmatrix} = \begin{pmatrix} \frac{x_1}{y_1} \cdot y_1 \\ \frac{x_1}{y_1} \cdot y_2 \end{pmatrix} = \dfrac{x_1}{y_1} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$. Analogamente, caso $y_2 \neq 0$, então $x_2 \neq 0$ e $x_1 = \dfrac{x_2 y_1}{y_2}$. Logo $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{x_2 y_1}{y_2} \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{x_2}{y_2} \cdot y_1 \\ \frac{x_2}{y_2} \cdot y_2 \end{pmatrix} = \dfrac{x_2}{y_2} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$.

Em ambos os casos, existe $\alpha \in \mathbb{R}^+$ tal que $x = \alpha y$. □

Proposição 2.6. *O conjunto $(\mathcal{C}_2/\!\sim, \oplus)$ é um monoide, com o elemento neutro $e = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.*

Demonstração. Basta mostrar que $\oplus$ é associativa:

$$\begin{aligned}
&\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \left[\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right] = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} y_1 z_2 + y_2 z_1 \\ y_2 z_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 y_2 z_2 + x_2 y_1 z_2 + x_2 y_2 z_1 \\ x_2 y_2 z_2 \end{pmatrix} = \begin{pmatrix} x_1 y_2 + x_2 y_1 \\ x_2 y_2 \end{pmatrix} \oplus \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \\
&= \left[\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right] \oplus \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}
\end{aligned}$$

□

Denotamos por $\overline{\mathbb{R}}_+$ o conjunto $\mathbb{R}_+ \cup \{\infty\}$ dos números reais não-negativos unido a $\{\infty\}$. A operação de adição usual em $\mathbb{R}_+$ se estende a $\overline{\mathbb{R}}_+$ com a regra $\infty + a = a + \infty = \infty$, $\forall a \in \overline{\mathbb{R}}_+$.

Proposição 2.7. *O monoide $(\mathcal{C}_2/\!\sim, \oplus)$ é isomorfo ao monoide $\left(\overline{\mathbb{R}}_+, +\right)$, onde $+$ é a operação de adição em $\overline{\mathbb{R}}_+$.*

Demonstração. Basta notar que a função $T : \mathcal{C}_2/\!\sim \to \overline{\mathbb{R}}_+$ definida por

$$T \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{cases} \frac{x_1}{x_2}, & \text{se } x_2 \neq 0 \\ \infty, & \text{se } x_2 = 0 \end{cases}$$

é um isomorfismo. Mostraremos inicialmente que T está bem definida.

Dado $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \sim \begin{pmatrix} \overline{x}_1 \\ \overline{x}_2 \end{pmatrix} \in \mathcal{C}_2/\!\sim$, temos $x_1 \overline{x}_2 = x_2 \overline{x}_1$. Logo $x_2 = 0 \iff \overline{x}_2 = 0$ e, consequentemente $T \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \infty \iff T \begin{pmatrix} \overline{x}_1 \\ \overline{x}_2 \end{pmatrix} = \infty$. Caso $x_2 \neq 0$, vale que $\overline{x}_2 \neq 0$ e $\dfrac{x_1}{x_2} = \dfrac{\overline{x}_1}{\overline{x}_2}$. Portanto $T \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = T \begin{pmatrix} \overline{x}_1 \\ \overline{x}_2 \end{pmatrix}$.

Note que T leva o elemento neutro $\epsilon = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ de $(\mathcal{C}_2/\sim, \oplus)$ no elemento neutro de $\left(\overline{\mathbb{R}}_+, +\right)$, pois $T(\epsilon) = T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \dfrac{0}{1} = 0$ é o elemento neutro do monoide $\left(\overline{\mathbb{R}}_+, +\right)$.

Mostraremos agora que T é um homomorfismo. De fato, dados $x, y \in \mathcal{C}_2/\sim$, com $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ e $x_2, y_2 > 0$, temos

$$T(x \oplus y) = T\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = T\begin{pmatrix} x_1y_2 + x_2y_1 \\ x_2y_2 \end{pmatrix} = \frac{x_1y_2 + x_2y_1}{x_2y_2}$$
$$= \frac{x_1}{x_2} + \frac{y_1}{y_2} = T\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + T\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = T(x) + T(y).$$

Caso $x_2 = 0$ ou $y_2 = 0$, temos $x_2y_2 = 0$, logo $T(x \oplus y) = T\begin{pmatrix} x_1y_2 + x_2y_1 \\ 0 \end{pmatrix} = \infty = T(x) + T(y)$.

Por fim, mostraremos que T é uma bijeção.

(1) T é injetiva, pois se $T(x) = T(y)$, então temos dois casos:

- $T(x) = T(y) = \infty \implies x_2 = y_2 = 0 \implies x_1y_2 = x_2y_1 = 0$;
- $T(x) = \dfrac{x_1}{x_2} = \dfrac{y_1}{y_2} = T(y) \implies x_1y_2 = x_2y_1$;

e em ambos os casos, $x \sim y$, ou $x = y$ em $\mathcal{C}_2/\sim$.

(2) T é sobrejetiva, pois dado $a \in \overline{\mathbb{R}}_+$ temos que se $a = \infty$, então $T^{-1}(a) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathcal{C}_2/\sim$.

Por outro lado, se $a \neq \infty$, $\begin{pmatrix} a \\ 1 \end{pmatrix} \in \mathcal{C}_2/\sim$ é tal que $T\begin{pmatrix} a \\ 1 \end{pmatrix} = \dfrac{a}{1} = a$.

□

2.2 TRANSFORMAÇÕES DE MÖBIUS

Nesta seção iremos abordar algumas propriedades da transformação de Möbius restrita à reta estendida, e com coeficientes inteiros não negativos.

Denotamos por $\mathbb{M}_2(\mathbb{Z}_+)$ o conjuntos das matrizes $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ onde $a, b, c, d \in \mathbb{Z}_+$. O conjunto das matrizes não singulares em $\mathbb{M}_2(\mathbb{Z}_+)$ é um semigrupo, que denotamos por $\mathcal{S}_{\mathbb{Z}_+}$. De fato, como $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{S}_{\mathbb{Z}_+}$, $\mathcal{S}_{\mathbb{Z}_+}$ é um monoide.

Definição 2.8. *Dados $a, b, c, d \in \mathbb{Z}_+$, com $ad - bc \neq 0$, a função $f : \overline{\mathbb{R}}_+ \to \overline{\mathbb{R}}_+$ tal que*

$$f(x) = \frac{ax + b}{cx + d}$$

é chamada de transformação de Möbius associada à matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Denotamos por $Mb(\mathbb{Z}_+)$ o semigrupo das transformações de Möbius.

Observação 2.1. Vale que:

- caso $c \neq 0$, tem-se que $f\left(\frac{-d}{c}\right) = \infty$ e $f(\infty) = \frac{a}{c}$.
- caso $c = 0$, temos que $f(\infty) = \infty$.

Proposição 2.9. *O monoide $(\mathcal{S}_{\mathbb{Z}_+}, \cdot)$ das matrizes $\mathcal{S}_{\mathbb{Z}_+}$ munido da operação de multiplicação é homomorfo ao monoide $(Mb(\mathbb{Z}_+), \circ)$ das transformações de Möbius munido da operação de composição de funções.*

Demonstração. Temos que, dadas duas transformações de Möbius $f, g : \overline{\mathbb{R}}_+ \to \overline{\mathbb{R}}_+$, com $f(x) = \frac{a_1 x + b_1}{c_1 x + d_1}$ e $g(x) = \frac{a_2 x + b_2}{c_2 x + d_2}$, a composta $f \circ g$ é dada por

$$\begin{aligned}(f \circ g)(x) &= \frac{a_1 \frac{a_2 x + b_2}{c_2 x + d_2} + b_1}{c_1 \frac{a_2 x + b_2}{c_2 x + d_2} + d_1} = \frac{a_1(a_2 x + b_2) + b_1(c_2 x + d_2)}{c_1(a_2 x + b_2) + d_1(c_2 x + d_2)} \\ &= \frac{(a_1 a_2 + b_1 c_2)x + (a_1 b_2 + b_1 d_2)}{(c_1 a_2 + d_1 c_2)x + (c_1 b_2 + d_1 d_2)}. \end{aligned} \tag{2.1}$$

Por outro lado, dadas duas matrizes $M, N \in \mathcal{S}_{\mathbb{Z}_+}$, com $M = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ e $N = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ temos que

$$M \cdot N = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix} \tag{2.2}$$

Como $\det(M) \neq 0$ e $\det(N) \neq 0$, vale que $\det(M \cdot N) = \det(M)\det(N) \neq 0$, logo $(f \circ g) \in Mb(\mathbb{Z}_+)$.

A função identidade $I : \overline{\mathbb{R}}_+ \to \overline{\mathbb{R}}_+$ onde $I(x) = x = \frac{1 \cdot x + 0}{0 \cdot x + 1}$ é uma transformação de Möbius, e I é o elemento neutro de $\circ$, já que , para toda $f \in Mb(\mathbb{Z}_+)$, vale que $f \circ I = I \circ f = f$. Portanto, $(Mb(\mathbb{Z}_+), \circ)$ é um monoide.

O homomorfismo natural $\Phi : \mathcal{S}_{\mathbb{Z}_+} \to Mb(\mathbb{Z}_+)$ associa $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{S}_{\mathbb{Z}_+}$ a $\Phi(A) = \Phi_A \in Mb(\mathbb{Z}_+)$ com $\Phi_A(x) = \frac{px + q}{rx + s}$, para todo $x \in \overline{\mathbb{R}}_+$.

Das equações 2.1 e 2.2, temos que $\Phi(M \cdot N) = \Phi \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix} = \Phi_{M \cdot N}$ onde $\Phi_{M \cdot N}(x) = \dfrac{(a_1a_2 + b_1c_2)x + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2)x + (c_1b_2 + d_1d_2)} = (\Phi_M \circ \Phi_N)(x)$. Portanto $\Phi(M \cdot N) = \Phi(M) \circ \Phi(N)$.

Como a matriz $Id_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o elemento neutro do monoide $(\mathcal{S}_{\mathbb{Z}_+}, \cdot)$, temos que $\Phi(Id_2) = \Phi_{Id_2} : \overline{\mathbb{R}}_+ \to \overline{\mathbb{R}}_+$ é a função tal que $\Phi_{Id_2}(x) = \dfrac{1 \cdot x + 0}{0 \cdot x + 1} = \dfrac{x}{1} = x = I(x)$, logo $\Phi(Id_2) = I$ é o elemento neutro do monoide $(Mb(\mathbb{Z}_+), \circ)$. Portanto a função Φ é um homomorfismo. □

Observação 2.2. O homomorfismo Φ definido acima é sobrejetor, mas não é injetor.

De fato, dada uma transformação de Möbius $f : \overline{\mathbb{R}}_+ \to \overline{\mathbb{R}}_+$, com $f(x) = \dfrac{ax + b}{cx + d}$, temos que $f = \Phi(M)$, com $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Porém, para qualquer k inteiro positivo, $\Phi(k \cdot M) = \Phi(M)$.

2.3 ALFABETOS E PALAVRAS

Uma estrutura de monoide pode ser construída de maneira bastante geral a partir de um conjunto não-vazio A.

Consideramos A um conjunto finito e não-vazio, o qual chamamos **alfabeto**. Chamaremos de **letras** os elementos de um alfabeto.

Uma **palavra** em A é uma sequência finita de letras, denotada por $a_1 \cdots a_n$, com $a_i \in A$. Se $w = a_1 \cdots a_n$, $n \in \mathbb{N}$ é chamado o **comprimento** da palavra w. Duas palavras $u = u_1 \cdots u_n$ e $v = v_1 \cdots v_m$ são iguais quando $m = n$ e $u_i = v_i$, para cada i, $1 \leq i \leq n$. Denotamos por A^n o conjunto de todas as palavras de tamanho n.

Consideramos também a palavra vazia, denotando-a por λ, com comprimento igual a zero, por definição. Definimos o conjunto

$$A^* = \cup_{n=1}^{\infty} A^n \cup \{\lambda\} .$$

A^* contém todas as palavras finitas de A e a palavra vazia.

Dadas as palavras $u = u_1u_2u_3 \cdots u_n$ e $v = v_1v_2v_3 \cdots v_m$, $m, n \in \mathbb{N}$, a **concatenação** é uma operação binária associativa definida por $uv = u_1u_2u_3 \cdots u_nv_1v_2v_3 \cdots v_m$. A palavra vazia λ é o elemento neutro da concatenação, ou seja, para toda sequência finita $u \in A^*$, vale $\lambda u = u\lambda = u$.

O conjunto A^* munido da operação concatenação é um monoide, chamado **monoide livre**[1].

[1] O termo *livre* faz alusão ao fato de que a concatenação não possui simplificações, que são vínculos entre os

Dado $u \in A^*$, denotamos por $|u|$ o comprimento de u.

Denotamos por $A^{\mathbb{N}}$ o conjunto das palavras infinitas em A.

É possível estender a operação de concatenação, com uma palavra infinita à direita do seguinte modo. Dada uma palavra finita $w = w_1w_2w_3\cdots w_k \in A^*$ e uma palavra infinita $a = a_1a_2a_3\cdots \in A^{\mathbb{N}}$, indicamos por wa a palavra infinita

$$wa = w_1w_2w_3\cdots w_ka_1a_2a_3\cdots \in A^{\mathbb{N}}\,.$$

Dada uma palavra V (finita ou infinita), dizemos que uma palavra $U \in A^*$ é **prefixo** de V se existir uma palavra W (finita ou infinita, dependendo de V) tal que $V = UW$. Neste caso, podemos definir a operação $V\backslash U$, chamada de **eliminação** do prefixo U, cujo resultado é W, ou seja, $V\backslash U = W$. Se $|W| > 0$, dizemos que U é **prefixo próprio** de V.

Neste trabalho, consideramos o alfabeto[2] $A = \{L, R\}$.

Usaremos a notação de potências para representar palavras com letras repetidas consecutivamente, ou seja, dado $n \in \mathbb{N}$

$$L^n = \underbrace{LLL\cdots L}_{n \text{ vezes}} \text{ e } R^n = \underbrace{RRR\cdots R}_{n \text{ vezes}}.$$

Quando estivermos nos referindo as palavras infinitas $LLL\cdots$ e $RRR\cdots$, utilizaremos a notação de potências juntamente com o símbolo ∞, de forma que $L^\infty = LLL\cdots$ e $R^\infty = RRR\cdots$.

Para cada $W \in \{L, R\}^*$, chamaremos de PROD(W) a matriz produto associada a W, ou seja, PROD : $\{L, R\}^* \to \mathcal{S}_{\mathbb{Z}_+}$ é a função tal que PROD$(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e para cada $W = W_1W_2\cdots W_k$, com $k \in \mathbb{N}$ e, para todo $1 \leq i \leq k$, $W_i \in \{L, R\}$, vale que

$$\text{PROD}(W) = \text{PROD}(W_1W_2\cdots W_k) = M_1 \cdot M_2 \cdot \cdots \cdot M_k,$$

$$\text{onde, para cada } 1 \leq i \leq k,\ M_i = \begin{cases} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, & \text{se } W_i = L; \\ \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, & \text{se } W_i = R. \end{cases}$$

Observação 2.3. Para simplificar as notações, usaremos o símbolo **L** quando nos referirmos a matriz PROD$(L) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ e **R** para a matriz PROD$(R) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, deste modo, o conjunto

elementos de A ou de A^*. As simplificações podem aparecer em grupos ou álgebras, por exemplo em $\mathbb{Z}_2 \times \mathbb{Z}_2$: $A = \{a, b\}$, e $ab = ba$, $a^2 = b^2 = e$.

[2]Associaremos adiante as letras L e R a certas transformações de Möbius. Em $\overline{\mathbb{R}}^+$, veremos que $L(1) < 1 < R(1)$, permitindo associar a ideia de mover para a esquerda e para a direita o ponto 1.

$\{\mathbf{L}, \mathbf{R}\} = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \subset \mathcal{S}_{\mathbb{Z}_+}$ é diferente de $\{L, R\}$. Da mesma forma, quando estivermos nos referindo a uma palavra $W \in \{L, R\}^*$ tal que $|W| = 1$, em outras palavras, uma palavra que possua apenas uma letra, usaremos $\mathbf{W}$ para nos referir a PROD(W).

Exemplo 1. Dado $n \in \mathbb{N}$ vale

- PROD$(L^n) = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$;
- PROD$(R^n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$;
- PROD$(L^n R^n) = \begin{pmatrix} 1 & n \\ n & n^2+1 \end{pmatrix}$;
- PROD$(R^n L^n) = \begin{pmatrix} n^2+1 & n \\ n & 1 \end{pmatrix}$.

2.4 BASES DE $\{L, R\}^{\mathbb{N}}$

Definição 2.10. *Dizemos que um conjunto finito $\mathcal{B} \subset \{L, R\}^*$ é uma* **base** *de $\{L, R\}^{\mathbb{N}}$ quando:*

(1) para todo $V \in \{L, R\}^{\mathbb{N}}$ existe uma palavra $B_k \in \mathcal{B}$ tal que B_k é prefixo de V;

(2) dadas quaisquer duas palavras $B_p, B_q \in \mathcal{B}$, temos que B_p não é prefixo de B_q.

Lema 2.11. *Dada $W \in \{L, R\}^{\mathbb{N}}$, se $\mathcal{B}$ é uma base, então existe uma única palavra $B \in \mathcal{B}$ tal que B é prefixo de W.*

Demonstração. Seja $W \in \{L, R\}^{\mathbb{N}}$ e $\mathcal{B}$ uma base de $\{L, R\}^{\mathbb{N}}$. Pela primeira propriedade da definição de base, existe uma palavra $B \in \mathcal{B}$ tal que B é prefixo de W. Já pela segunda propriedade, temos que para toda palavra $B' \in \mathcal{B}$, com $B' \neq B$, vale que B' não é prefixo de B, logo B' não é prefixo de W. Portanto B é a única palavra de $\mathcal{B}$ tal que B é prefixo de W. □

Definição 2.12. *Se $S = S_1 S_2 S_3 \cdots \in \{L, R\}^{\mathbb{N}}$ e $\mathcal{B}$ é uma base para $\{L, R\}^{\mathbb{N}}$, denotamos por $H(S, \mathcal{B})$ o prefixo de S que pertence à base $\mathcal{B}$.*

Definição 2.13. *Chamamos de* **ramo imediato** *de $W \in \{L, R\}^*$ toda palavra $V \in \{L, R\}^*$ tal que:*

(1) V não é um prefixo de W;

(2) se U é qualquer prefixo de V tal que $U \neq V$, então U é prefixo de W.

Exemplo 2. A palavra vazia λ não pode ser ramo imediato de nenhum $V \in \{L, R\}^*$, uma vez que λ é o elemento neutro da concatenação, então $\lambda V = V$, ou seja, λ é prefixo de qualquer palavra V. Logo se $U \in \{L, R\}^*$ é um ramo imediato de V, então $|U| \geq 1$.

Exemplo 3. Seja $V \in \{L, R\}^*$ um ramo imediato da palavra vazia λ. Se U é prefixo próprio de V, então U é prefixo de λ, o que implica em $U = \lambda$. Com isso, temos que V não possui prefixos próprios diferente de λ, o que torna necessário $|V| = 1$. Como L e R não são prefixos de λ, vale que L e R são ramos imediatos de λ. Temos portanto que o conjunto de todos os ramos imediatos de λ é $\{L, R\}$.

Proposição 2.14. *Seja $V \in \{L, R\}^*$. Se $U \in \{L, R\}^*$ é um ramo imediato de V, então $|U| \leq |V| + 1$.*

Demonstração. Sejam $U, V \in \{L, R\}^*$. Suponha que $|U| > |V| + 1$. Logo, podemos escrever U na forma $U = WU_1$, onde $U_1 \in \{L, R\}$ e $W \in \{L, R\}^*$ é prefixo próprio de U. De $|U| = |W| + 1 > |V| + 1$, tem-se que $|W| > |V|$. Portanto W não pode ser prefixo de V. Com isto, U não pode ser um ramo imediato de V, pois se fosse, W deveria ser prefixo de V. □

Observação 2.4. Uma consequência da Proposição 2.14 é o fato de que dado $V \in \{L, R\}^*$, o conjunto de todos os ramos imediatos de V é um conjunto finito.

Proposição 2.15. *Dados $U, V, W \in \{L, R\}^*$ temos que U é um ramo imediato de V se, e somente se, WU é um ramo imediato de WV.*

Demonstração. ($\Longrightarrow$) Se U é um ramo imediato de V então U não é prefixo de V, logo WU não é prefixo de WV. Se $X \in \{L, R\}^*$ é um prefixo próprio de WU, então X é prefixo de W ou W é prefixo de X. Se X é prefixo de W, então X é prefixo de WV. Caso W seja prefixo de X, então $X = WP$, onde $P \in \{L, R\}^*$ e $P \neq U$, já que X é prefixo próprio de WU. Logo P é prefixo próprio de U. Do fato de U ser ramo imediato de V, vale que P é prefixo de V. Portanto, $X = WP$ é prefixo de WV.

($\Longleftarrow$) Se WU é um ramo imediato de WV então WU não é prefixo de WV, logo U não é prefixo de V. Se $X \in \{L, R\}^*$ é um prefixo próprio de U, então WX é um prefixo próprio de WU, e como WU é ramo imediato de WV, vale que WX é prefixo de WV. Portanto X é prefixo de V. □

Definição 2.16. *Seja $A \in \{L, R\}$. Chamamos de* **transposto** *de A a letra $\mathfrak{p}(A) \in \{L, R\}$ tal que* $\mathfrak{p}(A) = \begin{cases} R & , se\ A = L; \\ L & , se\ A = R. \end{cases}$

Há um homomorfismo interessante no monoide $\{L, R\}^*$, a troca de duas letras, podendo ser generalizado para alfabetos quaisquer.

Definição 2.17. *Seja $V \in \{L, R\}^*$. Chamamos de* **função troca** *a função $\mathfrak{p} : \{L, R\}^* \to \{L, R\}^*$ tal que $\mathfrak{p}(\lambda) = \lambda$, e para toda palavra não vazia $V = V_1 V_2 \cdots V_m$, com $V_i \in \{L, R\}$ para cada $1 \leq i \leq m$, vale que $\mathfrak{p}(V) = \mathfrak{p}(V_1)\mathfrak{p}(V_2) \cdots \mathfrak{p}(V_m) \in \{L, R\}^*$.*

Proposição 2.18. *Sejam $P \in \{L, R\}$, $V \in \{L, R\}^*$ e $B = \{U_1, U_2, U_3, \cdots, U_k\} \subset \{L, R\}^*$ o conjunto de todos os ramos imediatos de V. Então o conjunto de todos os ramos imediatos de $PV \in \{L, R\}^*$ é igual a $B' = \{\mathfrak{p}(P), PU_1, PU_2, PU_3 \cdots PU_k\}$.*

Demonstração. Seja W um ramo imediato de PV. Do fato que P é um prefixo de PV, temos que se $|W| = 1$, então $W \neq P$. Como $\mathfrak{p}(P)$ não é prefixo de PV, vale que $W = \mathfrak{p}(P)$ é ramo imediato de PV. Se $|W| > 1$, então $W = QX$, com $Q \in \{L, R\}$, $X \in \{L, R\}^*$ e $X \neq \lambda$. Como Q é prefixo próprio de W, temos que Q deve ser prefixo de PV, logo $Q = P$ e $W = PX$. Com isso, temos que PX é um ramo imediato de PV. Pela Proposição 2.15, temos que X é ramo imediato de V, logo $X = U_i \in B$, para algum $1 \leq i \leq k$. Portanto $W = PU_i$. □

Teorema 2.19. *Seja $V = V_1V_2V_3 \cdots V_k \in \{L, R\}^*$, onde $V_i \in \{L, R\}$ para todo $1 \leq i \leq k$. O conjunto de todos os ramos imediatos de V é*

$$\mathcal{B} = \{\mathfrak{p}(V_1), V_1\mathfrak{p}(V_2), V_1V_2\mathfrak{p}(V_3), \cdots, V_1V_2V_3 \cdots V_{k-1}\mathfrak{p}(V_k), VL, VR\},$$

Demonstração. Provaremos por indução em $k = |V|$. Se $|V| = 1$, então $V = V_1$. O conjunto de todos os ramos imediatos de λ é igual a $\{L, R\}$. Agora como $V = V_1 = V_1\lambda$, pela Proposição 2.18 temos que o conjunto de todos os ramos imediatos de $V = V_1\lambda$ é igual a $\{\mathfrak{p}(V_1), V_1L, V_1R\}$.

Suponha que para todas as palavras $W = W_1W_2W_3 \cdots W_m$ com $|W| = m$, o conjunto de todos os ramos imediatos de W é igual a

$$\mathcal{B} = \{\mathfrak{p}(W_1), W_1\mathfrak{p}(W_2), W_1W_2\mathfrak{p}(W_3), \cdots, W_1W_2W_3 \cdots \mathfrak{p}(W_m), WL, WR\}.$$

Seja $V = V_1V_2V_3 \cdots V_mV_{m+1} \in \{L, R\}^*$ tal que $V_i \in \{L, R\}$, para todo $1 \leq i \leq m + 1$. Logo $|V| = m + 1$. Note que se tomarmos $U = V_2V_3 \cdots V_mV_{m+1} \in \{L, R\}^*$, temos que $|U| = m$. Pela hipótese de indução, vale que o conjunto de todos os ramos imediatos de $U = V_2V_3 \cdots V_mV_{m+1}$ é igual a

$$\mathcal{B}_1 = \{\mathfrak{p}(V_2), V_2\mathfrak{p}(V_3), V_2V_3\mathfrak{p}(V_4), \cdots, V_2V_3V_4 \cdots V_m\mathfrak{p}(V_{m+1}), UL, UR\}.$$

Por fim, como $V = V_1U$, segue da Proposição 2.18 que o conjunto de todos os ramos imediatos de $V = V_1U$ é igual a

$$\begin{aligned}\mathcal{B}_2 &= \{\mathfrak{p}(V_1), V_1\mathfrak{p}(V_2), V_1V_2\mathfrak{p}(V_3), \cdots, V_1V_2V_3 \cdots V_m\mathfrak{p}(V_{m+1}), V_1UL, V_1UR\} \\ &= \{\mathfrak{p}(V_1), V_1\mathfrak{p}(V_2), V_1V_2\mathfrak{p}(V_3), \cdots, V_1V_2V_3 \cdots V_m\mathfrak{p}(V_{m+1}), VL, VR\}\end{aligned}$$

□

Corolário 2.20. *A cardinalidade do conjunto de ramos imediatos de uma palavra $V \in \{L, R\}^*$ é $|V| + 2$.*

Exemplo 4. Seja $V = L^2R^3LR^2$. Temos então que, pelo Teorema 2.19, o conjunto de todos os ramos imediatos de V é igual a

$$\{R, LR, L^3, L^2RL, L^2R^2L, L^2R^4, L^2R^3L^2, L^2R^3LRL, L^2R^3LR^2L, L^2R^3LR^3\}.$$

Teorema 2.21. *Seja $V \in \{L, R\}^*$. O conjunto de todos os ramos imediatos de V é uma base de $\{L, R\}^{\mathbb{N}}$.*

Demonstração. Seja $k = |V|$. Provaremos por indução em k. Se $k = 0$, então $V = \lambda$, logo o conjunto de todos os ramos imediatos de V é o conjunto $\{L, R\}$, que é claramente uma base de $\{L, R\}^{\mathbb{N}}$.

Suponha que exista $m \in \mathbb{Z}_+$ tal que, para qualquer palavra $W \in \{L, R\}^*$ com $|W| = m$, o conjunto de todos os ramos imediatos de W seja uma base de $\{L, R\}^{\mathbb{N}}$.

Seja $V \in \{L, R\}^*$ tal que $|V| = m+1$, ou seja, $V = V_1V_2 \cdots V_mV_{m+1}$, com $V_i \in \{L, R\}$, para todo $1 \leq i \leq m + 1$. Sejam também $Y = Y_1Y_2Y_3 \cdots \in \{L, R\}^{\mathbb{N}}$, com $Y_i \in \{L, R\}$, para todo $i \in \mathbb{N}$. Seja $Z \in \{L, R\}^{\mathbb{N}}$ tal que $Z = Y_2Y_3Y_4 \cdots \in \{L, R\}^{\mathbb{N}}$. Ou seja, $Y = Y_1Z$. Da mesma forma, seja a palavra $U = V_2V_3 \cdots V_mV_{m+1} \in \{L, R\}^*$ tal que $V = V_1U$.

Então, pela hipótese de indução, o conjunto $\mathcal{B} = \{B_1, B_2, \cdots B_{m+2}\} \subset \{L, R\}^*$ de todos os ramos imediatos de U é base de $\{L, R\}^*$.

Pelo Lema 2.11, existe um único $B_j \in \mathcal{B}$ tal que B_j é prefixo de Z, em outras palavras, $Z = B_jP$, para alguma $P \in \{L, R\}^{\mathbb{N}}$. Pela proposição 2.18, o conjunto de todos os ramos imediatos de $V = V_1U$ é $\mathcal{B}' = \{\mathfrak{p}(V_1), V_1B_1, V_1B_2, \cdots, V_1B_{m+1}\}$. Se $Y_1 = \mathfrak{p}(V_1)$, então $\mathfrak{p}(V_1) \in \mathcal{B}'$ é prefixo de Y. Se $Y_1 = V_1$, então $Y = V_1Z = V_1B_jP$, logo $V_1B_j \in \mathcal{B}'$ é prefixo de Y.

Dados $B_p, B_q \in B$, temos que B_p não é prefixo de B_q, logo V_1B_p não é prefixo de V_1B_q. Vale também que, para qualquer $1 \leq i \leq m + 1$, $\mathfrak{p}(V_1)$ não é prefixo de V_1B_i e V_1B_i não é prefixo de $\mathfrak{p}(V_1)$. Portanto, $\mathcal{B}'$ é uma base de $\{L, R\}^{\mathbb{N}}$. □

3 FRAÇÕES CONTINUADAS

O objetivo deste capítulo é apresentar uma forma de representar os números reais utilizando frações continuadas regulares. Primeiramente vamos definir a função piso. Dado um número real x, o maior inteiro que seja menor do que ou igual a x é denotado por $\lfloor x \rfloor$. Em outras palavras, a função piso é a função que leva o número real x no inteiro $\lfloor x \rfloor = \max_{m \in \mathbb{Z}} \{m : m \leq x\}$.

Definimos recursivamente $\theta_n \in \mathbb{R}$ da seguinte forma: $\theta_0 = x$, e $a_0 = \lfloor \theta_0 \rfloor$. Se $\theta_n \notin \mathbb{Z}$, então $\theta_{n+1} = \dfrac{1}{\theta_n - a_n}$, e $a_{n+1} = \lfloor \theta_{n+1} \rfloor$ para todo $n \in \mathbb{Z}_+$.

Se existir n tal que $\theta_n = a_n$, então

$$x = \theta_0 = [a_0; a_1, a_2, \cdots, a_n] \stackrel{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}.$$

Se não, denotamos

$$x = [a_0; a_1, a_2, a_3 \cdots] \stackrel{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}.$$

Explicaremos o sentido da última notação mais adiante. A representação de x definida acima é chamada de **representação por frações continuadas regulares**, ou, mais brevemente, representação por frações continuadas.

Note que, se a representação por frações continuadas de x for finita, então x é claramente racional. Reciprocamente, se $x \in \mathbb{Q}$ podemos utilizar o algoritmo de Euclides para encontrar os coeficientes da representação por frações continuadas. Se $x = \dfrac{p}{q}$, onde $p \in \mathbb{Z}$, $q \in \mathbb{N}$, então:

$$\begin{aligned}
p &= a_0 q + r_1 && 0 \leq r_1 < q \\
q &= a_1 r_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= a_2 r_2 + r_3 && 0 \leq r_3 < r_2 \\
&\vdots && \vdots \\
r_{n-2} &= a_{n-1} r_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n a_n
\end{aligned}$$

Logo, temos que

$$x = \frac{p}{q} = a_0 + \frac{r_1}{q} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}}$$
$$= \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}} = [a_0; a_1, a_2, \cdots, a_n].$$

Seja $x = [a_0; a_1, a_2, \cdots]$. Sejam $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}$, com $mdc(p_n, q_n) = 1$ tais que $\frac{p_n}{q_n} = [a_0; a_1, a_2, \cdots, a_n]$, com $n \geq 0$. Chamaremos a fração $\frac{p_n}{q_n}$ de ***n*-ésima reduzida** da fração continuada de x.

Proposição 3.1. *Dada uma sequência (finita ou infinita)* $t_0, t_1, \cdots \in \mathbb{R}$ *tal que* $t_k > 0$*, para todo* $k \geq 1$*, definimos as sequências* (x_m) *e* (y_m) *de forma que* $x_0 = t_0$*,* $y_0 = 1$*,* $x_1 = t_0 t_1 + 1$*,* $y_1 = t_1$*,* $x_{m+2} = t_{m+2} x_{m+1} + x_m$*,* $y_{m+2} = t_{m+2} y_{m+1} + y_m$*, para todo* $m \geq 0$*.*

Temos então

$$[t_0; t_1, t_2, \cdots, t_n] = t_0 + \cfrac{1}{t_1 + \cfrac{1}{t_2 + \ddots + \cfrac{1}{t_n}}} = \frac{x_n}{y_n}, \text{ para todo } n \geq 0.$$

Além disso, $x_{n+1} y_n - x_n y_{n+1} = (-1)^n$*, para todo* $n \geq 0$*.*

Demonstração. Faremos a prova por indução em n. Para $n = 0$ temos $[t_0] = t_0 = \frac{t_0}{1} = \frac{x_0}{y_0}$. Para $n = 1$, temos $[t_0; t_1] = t_0 + \frac{1}{t_1} = \frac{t_0 t_1 + 1}{t_1} = \frac{x_1}{y_1}$ e, para $n = 2$, temos

$$[t_0; t_1, t_2] = t_0 + \frac{1}{t_1 + \frac{1}{t_2}} = t_0 + \frac{t_2}{t_1 t_2 + 1} = \frac{t_0 t_1 t_2 + t_0 + t_2}{t_1 t_2 + 1}$$
$$= \frac{t_2(t_0 t_1 + 1) + t_0}{t_2 t_1 + 1} = \frac{t_2 x_1 + x_0}{t_2 y_1 + y_0} = \frac{x_2}{y_2}.$$

Suponha que a afirmação seja válida para n. Temos então

$$[t_0; t_1, t_2, \cdots, t_n, t_{n+1}] = \left[t_0; t_1, t_2, \cdots, t_n + \frac{1}{t_{n+1}}\right] = \frac{\left(t_n + \frac{1}{t_{n+1}}\right) x_{n-1} + x_{n-2}}{\left(t_n + \frac{1}{t_{n+1}}\right) y_{n-1} + y_{n-2}}$$
$$= \frac{t_{n+1}(t_n x_{n-1} + x_{n-2}) + x_{n-1}}{t_{n+1}(t_n y_{n-1} + y_{n-2}) + y_{n-1}} = \frac{t_{n+1}x_n + x_{n-1}}{t_{n+1}y_n + y_{n-1}} = \frac{x_{n+1}}{y_{n+1}}.$$

Mostraremos, por indução, a segunda afirmação. Temos $x_1y_0 - x_0y_1 = (t_0t_1 + 1) - t_0t_1 = 1 = (-1)^0$ e, se $x_{n+1}y_n - x_ny_{n+1} = (-1)^n$ para algum valor de n, então

$$x_{n+2}y_{n+1} - x_{n+1}y_{n+2} = (t_{n+2}x_{n+1} + x_n)y_{n+1} - (t_{n+2}y_{n+1} + y_n)x_{n+1}$$
$$= -(x_{n+1}y_n - x_ny_{n+1}) = -(-1)^n = (-1)^{n+1}.$$

□

Corolário 3.2. *Seja $x = [a_0; a_1, a_2, \cdots]$ um número real, $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{Z}_+}$ uma sequência de números reais, de forma que $\frac{p_n}{q_n} = [a_0; a_1, a_2, \cdots, a_n]$ é a n-ésima reduzida da fração continuada de x. As sequências (p_n) e (q_n) satisfazem as recorrências*

$$p_{n+2} = a_{n+2}p_{n+1} + p_n \qquad e \qquad q_{n+2} = a_{n+2}q_{n+1} + q_n$$

para todo $n \geq 0$, com $p_0 = a_0$, $p_1 = a_0a_1 + 1$, $q_0 = 1$ e $q_1 = a_1$. Além disso,

$$p_{n+1}q_n - p_nq_{n+1} = (-1)^n$$

para todo $n \geq 0$.

Demonstração. As sequências (p_n) e (q_n) definidas pelas recorrências acima satisfazem, pela Proposição 3.1, as igualdade $\frac{p_n}{q_n} = [a_0; a_1, a_2, \cdots, a_n]$ e $p_{n+1}q_n - p_nq_{n+1} = (-1)^n$, para todo $n \geq 0$.

Como $p_{n+1}q_n - p_nq_{n+1} = (-1)^n$ para todo $n \in \mathbb{Z}_+$, temos que os p_n, q_n dados pelas recorrências acima são primos entre si. Além disso, também segue da recorrência que $q_n > 0$, para todo $n \in \mathbb{Z}_+$. Esses fatos implicam que $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{Z}_+}$ é a sequência de reduzidas da fração continuada de x. □

Corolário 3.3. *Temos, para todo $n \in \mathbb{Z}_+$,*

$$x = \frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}} \quad e \quad \theta_n = \frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}}$$

Demonstração. A primeira igualdade segue da Proposição 3.1 pois $x = [a_0; a_1, a_2, \cdots, a_{n-1}, \theta_n]$

e a segunda é consequência direta da primeira. □

Proposição 3.4. *Temos*

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\theta_{n+1} + \beta_{n+1})q_n^2}$$

onde

$$\beta_{n+1} = \frac{q_{n-1}}{q_n} = [0; a_n, a_{n-1}, a_{n-2}, \cdots, a_2, a_1].$$

Em particular

$$\frac{1}{(a_{n+1}+2)q_n^2} < \left| x - \frac{p_n}{q_n} \right| = \frac{1}{(\theta_{n+1} + \beta_{n+1})q_n^2} < \frac{1}{a_{n+1}q_n^2}.$$

Demonstração. Pelo Corolário 3.3 temos

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{\theta_{n+1}p_n + p_{n-1}}{\theta_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{(\theta_{n+1}q_n + q_{n-1})q_n} = \frac{-(p_nq_{n-1} - p_{n-1}q_n)}{(\theta_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{-(-1)^{n-1}}{(\theta_{n+1}q_n + q_{n-1})q_n} = \frac{(-1)^n}{\left(\theta_{n+1} + \dfrac{q_{n-1}}{q_n}\right)q_n^2} = \frac{(-1)^n}{(\theta_{n+1} + \beta_{n+1})q_n^2}. \end{aligned}$$

Em particular,

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{(\theta_{n+1} + \beta_{n+1})q_n^2},$$

e, como $\lfloor \theta_{n+1} \rfloor = a_{n+1}$ e $0 < \beta_{n+1} < 1$, segue que $a_{n+1} < \theta_{n+1} + \beta_{n+1} < a_{n+1} + 2$, o que implica a última afirmação.

A expansão de β_{n+1} como fração continuada segue de

$$\frac{q_{n-1}}{q_n} = \frac{q_{n-1}}{a_nq_{n-1} + q_{n-2}} \implies \frac{q_{n-1}}{q_n} = \frac{1}{a_n + \dfrac{q_{n-2}}{q_{n-1}}}$$

aplicado recursivamente. □

Observação 3.1. Do fato que q_n é estritamente crescente, segue da Proposição 3.4 que

$$\lim_{n\to\infty} \frac{p_n}{q_n} = x,$$

o que dá sentido à igualdade $x = [a_0; a_1, a_2, \cdots]$ quando a fração continuada de x é infinita.

Observação 3.2. A Proposição 3.4 implica que, para todo θ irracional, a desigualdade $\left| \theta - \dfrac{p}{q} \right| < \dfrac{1}{q^2}$ tem infinitas soluções racionais $\dfrac{p}{q}$. Este fato é conhecido como *Teorema de Dirichlet*.

É interessante notar que, se $\theta = \dfrac{r}{s} \in \mathbb{Q}$, a desigualdade $\left| \theta - \dfrac{p}{q} \right| < \dfrac{1}{q^2}$ tem apenas um número finito de soluções racionais $\dfrac{p}{q}$. De fato, $\left| \dfrac{r}{s} - \dfrac{p}{q} \right| < \dfrac{1}{q^2}$ equivale a $|qr - ps| < \dfrac{s}{q}$, o que

implica em $q \leq s$.

A seguinte proposição mostra que os convergentes pares formam uma sequência crescente, e que os convergentes ímpares formam uma sequência decrescente. Além disso todos os convergentes ímpares são maiores do que todos os convergentes pares.

Proposição 3.5. *Para todo $k \geq 0$, temos*

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq x \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}.$$

Demonstração. Para todo $n \leq 0$, temos que

$$\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} = \frac{a_{n+2}p_{n+1} + p_n}{a_{n+2}q_{n+1} + q_n} - \frac{p_n}{q_n} = \frac{a_{n+2}(p_{n+1}q_n - p_nq_{n+1})}{q_n(a_{n+2}q_{n+1} + q_n)} = \frac{(-1)^n q_{n+2}}{q_{n+2}q_n}$$

é positivo para n par e negativo para n ímpar. Além disso, para todo $n \geq 0$, temos que $x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\theta_{n+1}q_n + q_{n-1})q_n}$ é positivo para n par e negativo para n ímpar. □

Proposição 3.6. *Sejam $a_0, a_1, \cdots, a_n$ inteiros com $a_k > 0$, para todo $k \geq 1$, e seja $\left(\frac{p_k}{q_k}\right)_{k\geq 0}$ a sequência de reduzidas da fração continuada $[a_0; a_1, a_2, \cdots, a_n]$. Então o conjunto dos números reais cuja representação por frações continuadas começa com $a_0, a_1, a_2, \cdots, a_n$ é o intervalo*

$$\begin{aligned} I(a_0, a_1, \cdots, a_n) &= \left\{\frac{p_n}{q_n}\right\} \cup \{[a_0, a_1, \cdots, a_n, \theta], \theta > 1\} \\ &= \begin{cases} \left[\frac{p_n}{q_n}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}}\right) & \text{, se } n \text{ é par} \\ \left(\frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{p_n}{q_n}\right] & \text{, se } n \text{ é ímpar.} \end{cases} \end{aligned}$$

Além disso, a função $G : (1, +\infty) \to I(a_0, a_1, \cdots, a_n)$ dada por $G(\theta) = [a_0; a_1, a_2, \cdots, a_n, \theta]$ é monótona, sendo crescente para n ímpar e decrescente para n par.

Demonstração. Note que $G(\theta) = [a_0; a_1, a_2, \cdots, a_n, \theta] = \frac{\theta p_n + p_{n-1}}{\theta q_n + q_{n-1}} = \frac{p_n}{q_n} + \frac{(-1)^n}{(\theta q_n + q_{n-1})q_n}$, e portanto G é crescente para n ímpar e decrescente para n par. Assim, como $G(1) = \frac{p_n + p_{n-1}}{q_n + q_{n-1}}$ e $\lim_{\theta \to +\infty} G(\theta) = \frac{p_n}{q_n}$, temos

$$G((1, +\infty)) = \begin{cases} \left(\frac{p_n}{q_n}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}}\right) & \text{, se } n \text{ é par} \\ \left(\frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{p_n}{q_n}\right) & \text{, se } n \text{ é ímpar.} \end{cases}$$

Portanto

$$\begin{aligned} I(a_0, a_1, \cdots, a_n) &= \left\{\frac{p_n}{q_n}\right\} \cup \{[a_0, a_1, \cdots, a_n, \theta], \theta > 1\} \\ &= \left\{\frac{p_n}{q_n}\right\} \cup G((1, +\infty)) \\ &= \begin{cases} \left[\dfrac{p_n}{q_n}, \dfrac{p_n + p_{n-1}}{q_n + q_{n-1}}\right) & \text{, se } n \text{ é par} \\ \left(\dfrac{p_n + p_{n-1}}{q_n + q_{n-1}}, \dfrac{p_n}{q_n}\right] & \text{, se } n \text{ é ímpar.} \end{cases} \end{aligned}$$

□

Proposição 3.7. *Dados inteiros $a_0, a_1, a_2, \cdots$ com $a_k > 0$, para todo $k \geq 1$, existe um único número real θ cuja representação por frações continuadas é $[a_0; a_1, a_2, \cdots]$.*

Demonstração. Considere as sequências (p_n) e (q_n) definidas pelas recorrências

$$p_{n+2} = a_{n+2}p_{n+1} + p_n \qquad \text{e} \qquad q_{n+2} = a_{n+2}q_{n+2} + q_n$$

para todo $n \geq 0$, com $p_0 = a_0$, $p_1 = a_0a_1 + 1$, $q_0 = 1$ e $q_1 = a_1$. Temos, como na Proposição 3.5,

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}, \forall k \geq 0.$$

Assim, considerando os intervalos fechados $I_k = \left[\dfrac{p_{2k}}{q_{2k}}, \dfrac{p_{2k+1}}{q_{2k+1}}\right]$, temos $I_{k+1} \subset I_k$, para todo $k \geq 0$, e portanto, como

$$|I_k| = \frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = \frac{p_{2k+1}q_{2k} - p_{2k}q_{2k+1}}{q_{2k+1}q_{2k}} = \frac{(-1)^{2k}}{q_{2k+1}q_{2k}} = \frac{1}{q_{2k+1}q_{2k}}$$

tende a 0 quando k tende a infinito, existe $\theta \in \mathbb{R}$ tal que

$$\bigcap_{k \geq 0} I_k = \{\theta\}.$$

Como, para todo $k \geq 0$,

$$[a_0; a_1, a_2, \cdots, a_{2k}] = \frac{p_{2k}}{q_{2k}} \leq \theta \leq \frac{p_{2k+1}}{q_{2k+1}} = [a_0; a_1, a_2, \cdots, a_{2k}, a_{2k+1}]$$

e, da Proposição 3.6, $[a_0; a_1, a_2, \cdots, a_{2k}]$ e $[a_0; a_1, a_2, \cdots, a_{2k}, a_{2k+1}]$ pertencem a $I(a_0, a_1, a_2, \cdots, a_{2k})$, que é um intervalo, segue que $\theta \in I(a_0, a_1, a_2, \cdots, a_{2k})$, e portanto a fração continuada de θ começa com $a_0, a_1, a_2, \cdots, a_{2k}$, para todo $k \geq 0$, donde a representação por frações continuadas de θ é $[a_0; a_1, a_2, \cdots]$.

Note que, como a representação por frações continuadas de θ é infinita, θ é irracional. □

$\theta : \mathbb{R} \times \mathbb{Z}_+ \to \mathbb{R}$ de forma que $\theta(x,k) = \theta_x(k) = [x_k; x_{k+1}, x_{k+2}, \cdots]$. Como $\sum_{n=0}^{\infty} x_n$ diverge, temos que $\sum_{n=k}^{\infty} x_n$ também diverge, para todo $k \in \mathbb{Z}_+$. Logo $\theta_x(k)$ está bem definida.

4 MATRIZES BALANCEADAS

4.1 MATRIZES LINHA BALANCEADAS E COLUNA BALANCEADAS

Dado $n \in \mathbb{N}$, denotamos por $\mathcal{D}_n$ o conjunto das matrizes $M \in \mathcal{S}_{\mathbb{Z}_+}$ tais que $det(M) = n$. Dizemos que uma matriz $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{D}_n$ tem a

(a) **primeira linha dominante** caso $a \geq c$ e $b \geq d$;

(b) **segunda linha dominante** caso $c \geq a$ e $d \geq b$;

(c) **primeira coluna dominante** caso $a \geq b$ e $c \geq d$;

(d) **segunda coluna dominante** caso $b \geq a$ e $d \geq c$.

Caso a matriz $M \in \mathcal{D}_n$ não tenha a primeira ou a segunda linha dominante, dizemos que ela é **linha balanceada**, e caso não tenha coluna dominante, dizemos que ela é **coluna balanceada**.

Chamamos de $\mathcal{LB}_n$ o conjunto das matrizes $M \in \mathcal{D}_n$ tais que M seja linha balanceada, $\mathcal{CB}_n$ o conjunto das matrizes de $\mathcal{D}_n$ que são coluna balanceada e $\mathcal{DB}_n$ o conjunto das matrizes $M \in \mathcal{D}_n$ que são linha e coluna balanceadas, em outras palavras, $\mathcal{DB}_n = \mathcal{LB}_n \cap \mathcal{CB}_n$.

Chamaremos $\mathcal{DB}_n$ das matrizes $M \in \mathcal{D}_n$ **duplamente balanceadas**.

Proposição 4.1. *Seja $M \in \mathcal{D}_n$. M possui a:*

- *primeira linha dominante se, e somente se, M possuir um* **fator $\mathbf{R}$ à esquerda***, ou seja, se existir uma matriz $M' \in \mathcal{D}_n$ tal que $M = \mathbf{R} \cdot M'$;*
- *segunda linha dominante se, e somente se, M possuir um* **fator $\mathbf{L}$ à esquerda***, ou seja, se existir uma matriz $M' \in \mathcal{D}_n$ tal que $M = \mathbf{L} \cdot M'$;*
- *primeira coluna dominante se, e somente se, M possuir um* **fator $\mathbf{L}$ à direita***, ou seja, se existir uma matriz $M' \in \mathcal{D}_n$ tal que $M = M' \cdot \mathbf{L}$;*
- *segunda coluna dominante se, e somente se, M possuir um* **fator $\mathbf{R}$ à direita***, ou seja, se existir uma matriz $M' \in \mathcal{D}_n$ tal que $M = M' \cdot \mathbf{R}$.*

Demonstração. Provaremos o primeiro caso. Seja $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{D}_n$ uma matriz que possua a primeira linha dominante, ou seja, existem $u, v \in \mathbb{Z}_+$ tais que $a = c + u$ e $b = d + v$.

Logo $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c+u & d+v \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} u & v \\ c & d \end{pmatrix} = \mathbf{R} \cdot \begin{pmatrix} u & v \\ c & d \end{pmatrix}$. Note que a matriz $M' = \begin{pmatrix} u & v \\ c & d \end{pmatrix}$ pertence a $\mathcal{D}_n$, já que $u, v, c, d \in \mathbb{Z}_+$ e, do fato de $M \in \mathcal{D}_n$, vale que $n = \det(M) = \det(\mathbf{R} \cdot M') = \det(\mathbf{R}) \cdot \det(M') = \det(M')$.

Os demais casos são demonstrados analogamente. □

Observação 4.1. Do fato de uma matriz $M \in \mathcal{D}_n$ não poder ter a primeira e a segunda linha dominante, temos que os conjuntos $\mathbf{R}\mathcal{D}_n = \{M \in \mathcal{D}_n : M = \mathbf{R} \cdot M', \text{com } M' \in \mathcal{D}_n\}$, $\mathbf{L}\mathcal{D}_n = \{M \in \mathcal{D}_n : M = \mathbf{L} \cdot M', \text{com } M' \in \mathcal{D}_n\}$ e $\mathcal{LB}_n$ são dois a dois disjuntos e $\mathcal{D}_n = \mathbf{R}\mathcal{D}_n \cup \mathbf{L}\mathcal{D}_n \cup \mathcal{LB}_n$.

Analogamente os conjuntos $\mathcal{D}_n\mathbf{R} = \{M \in \mathcal{D}_n : M = M' \cdot \mathbf{R}, \text{com } M' \in \mathcal{D}_n\}$, $\mathcal{D}_n\mathbf{L} = \{M \in \mathcal{D}_n : M = M' \cdot \mathbf{L}, \text{com } M' \in \mathcal{D}_n\}$ e $\mathcal{CB}_n$ são dois a dois disjuntos e $\mathcal{D}_n = \mathcal{D}_n\mathbf{R} \cup \mathcal{D}_n\mathbf{L} \cup \mathcal{CB}_n$.

Lema 4.2. $\mathcal{LB}_1 = \mathcal{CB}_1 = \{Id_2\}$.

Demonstração. Seja $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{D}_1$. Se M for linha balanceada, então não é possível que $a < c$ e $d < b$, pois caso ocorresse, teríamos $ad < cb$ e $ad - cb < 0$, o que não é verdade, uma vez que $ad - cb = 1$.

Logo, $a > c$ e $d > b$. Tome $a = c + k$ e $d = b + k'$, para $k, k' \in \mathbb{N}$. Logo $1 = \det(M) = ad - bc = (c + k)(b + k') - cb = ck' + bk + kk'$. Como $kk' \geq 1$, vale que $ck' + bk = 0$, o que implica em $c = 0$ e $b = 0$, consequentemente, $kk' = 1$. Por fim, podemos concluir que $k = k' = 1$.

Portanto $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c+k & b \\ c & b+k' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id_2$.

Analogamente pode se mostrar que $\mathcal{CB}_1 = \{Id_2\}$. □

4.2 Fatoração de Matrizes $\mathcal{D}_n$

Lema 4.3. *Seja* $S : \mathcal{S}_{\mathbb{Z}_+} \to \mathbb{N}$ *a função onde* $S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + b + c + d$. *Sejam* $n \in \mathbb{N}$, $M, N \in \mathcal{D}_n$.

(a) Se $N \notin \mathcal{LB}_n$ *então* $S(M \cdot N) > S(M)$.

(b) Se $M \notin \mathcal{CB}_n$ *então* $S(M \cdot N) > S(N)$.

Demonstração. Sejam $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ e $N = \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix}$, com $M, N \in \mathcal{S}_{\mathbb{Z}_+}$. Logo

$$\begin{aligned} S(M \cdot N) &= S\begin{pmatrix} m_{11}n_{11} + m_{12}n_{21} & m_{11}n_{12} + m_{12}n_{22} \\ m_{21}n_{11} + m_{22}n_{21} & m_{21}n_{12} + m_{22}n_{22} \end{pmatrix} \\ &= (m_{11} + m_{21})(n_{11} + n_{12}) + (m_{12} + m_{22})(n_{21} + n_{22}). \end{aligned}$$

- Caso $N \notin \mathcal{LB}_n$, seja $min_{\mathcal{L}}(N) = \min\{n_{11} + n_{12}, n_{21} + n_{22}\}$. Note que $min_{\mathcal{L}}(N) \geq 1$, já que $min_{\mathcal{L}}(N) = 0 \implies \det(N) = 0$. De $N \notin \mathcal{LB}_n$ vale que N possui a primeira ou

a segunda linha dominante. Em ambos os casos, vale que

$$\begin{aligned} S(M \cdot N) &= (m_{11} + m_{21})(n_{11} + n_{12}) + (m_{12} + m_{22})(n_{21} + n_{22}) \\ &> (m_{11} + m_{21})min_{\mathcal{L}}(N) + (m_{12} + m_{22})min_{\mathcal{L}}(N) \\ &= (m_{11} + m_{12} + m_{21} + m_{22})min_{\mathcal{L}}(N) \\ &= S(M) \cdot min_{\mathcal{L}}(N) \\ &\geq S(M). \end{aligned}$$

- Caso $M \notin \mathcal{CB}_n$, seja $min_{\mathcal{C}}(M) = \min\{m_{11}+m_{21}, m_{12}+m_{22}\}$. Note que $min_{\mathcal{C}}(M) \geq 1$, já que $min_{\mathcal{C}}(M) = 0 \implies \det(M) = 0$. De $M \notin \mathcal{CB}_n$ vale que M possui a primeira ou a segunda coluna dominante. Em ambos os casos, vale que

$$\begin{aligned} S(M \cdot N) &= (m_{11} + m_{21})(n_{11} + n_{12}) + (m_{12} + m_{22})(n_{21} + n_{22}) \\ &> min_{\mathcal{C}}(M)(n_{11} + n_{12}) + min_{\mathcal{C}}(M)(n_{21} + n_{22}) \\ &= min_{\mathcal{C}}(M)(n_{11} + n_{12} + n_{21} + n_{22}) \\ &= min_{\mathcal{C}}(M) \cdot S(N) \\ &\geq S(N). \end{aligned}$$

□

Corolário 4.4. *A função $S : \mathcal{S}_{\mathbb{Z}_+} \to \mathbb{N}$ tem como mínimo global o valor 2 e satisfaz $S^{-1}(2) = \{Id_2\}$.*

Demonstração. Seja $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_{\mathbb{Z}_+}$. Temos que $a, b, c, d \geq 0$ e $ad - bc \neq 0$. Logo $a \geq 1$ e $d \geq 1$. Com efeito, $S(M) = a + b + c + d \geq 2$. Suponha que $S(M) = 2$. Logo $a + b + c + d = 2$. De $a \geq 1$ e $d \geq 1$, temos que $a = d = 1$ e $c = d = 0$. Portanto $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id_2$. □

Teorema 4.5. *Cada matriz $M \in \mathcal{D}_n$ possui uma única fatoração $M = \text{PROD}(W) \cdot Q$, onde $W \in \{L, R\}^*$ e $Q \in \mathcal{LB}_n$. Analogamente, cada matriz $M \in \mathcal{D}_n$ possui uma única fatoração $M = Q' \cdot \text{PROD}(W')$, onde $W' \in \{L, R\}^*$ e $Q' \in \mathcal{CB}_n$.*

Demonstração. Faremos a demonstração para o caso da fatoração $M = \text{PROD}(W) \cdot Q$, onde $W \in \{L, R\}^*$ e $Q \in \mathcal{LB}_n$. Seja $M \in \mathcal{D}_n$. Pela Observação 4.1, M pertence a apenas um dos seguintes conjuntos: $\mathcal{LB}_n$, $\mathbf{L}\mathcal{D}_n$ ou $\mathbf{R}\mathcal{D}_n$.

Caso $M \in \mathcal{LB}_n$, então $M = Id_2 \cdot M = \text{PROD}(\lambda) \cdot M$. Suponha que existam $W' \in \{L, R\}^*$ e $Q' \in \mathcal{LB}_n$ tais que $M = \text{PROD}(W') \cdot Q'$.

Suponha que $W' \neq \lambda$. Temos então que existe $p \in \mathbb{N}$ tal que $W' = W'_1 W'_2 \cdots W'_p$, com $W'_i \in \{L, R\}$, para todo $1 \leq i \leq p$. Logo $M = \text{PROD}(W') \cdot Q' = \mathbf{W}'_1 \cdot \mathbf{W}'_2 \cdot \cdots \cdot \mathbf{W}'_p \cdot Q'$. Como

$W_1' \in \{L, R\}$, vale apenas um dos dois casos: $M \in \mathbf{L}\mathcal{D}_n$ ou $M \in \mathbf{R}\mathcal{D}_n$. Absurdo já que pela Observação 4.1, temos que $(\mathbf{L}\mathcal{D}_n \cup \mathbf{R}\mathcal{D}_n) \cap \mathcal{LB}_n = \emptyset$. Portanto, $W' = \lambda$ e consequentemente $Q' = M$.

Caso $M \notin \mathcal{LB}_n$, pela Observação 4.1 vale que ocorre apenas um dos casos a seguir: $M \in \mathbf{L}\mathcal{D}_n$ ou $M \in \mathbf{R}\mathcal{D}_n$. Isso implica que existe um único $W_1 \in \{L, R\}$ e uma única matriz $M_1 \in \mathcal{D}_n$ tal que $M = \mathbf{W}_1 \cdot M_1$.

Note que $M_1 \in \mathcal{D}_n$, logo podemos repetir em M_1 a análise feita em M. Se $M_1 \in \mathcal{LB}_n$, então existe uma única palavra $W = W_1 \in \{L, R\}^*$ e uma matriz $Q = M_1 \in \mathcal{LB}_n$ tais que $M = \text{PROD}(W) \cdot Q = \mathbf{W}_1 \cdot M_1$. Caso $M_1 \notin \mathcal{LB}_n$, então existe um único $W_2 \in \{L, R\}$ e uma única matriz $M_2 \in \mathcal{D}_n$ tal que $M_1 = \mathbf{W}_2 \cdot M_2$. Logo $M = \mathbf{W}_1 \cdot M_1 = \mathbf{W}_1 \cdot \mathbf{W}_2 \cdot M_2$. Note que, nestas condições, existe uma única palavra $W = W_1W_2 \in \{L, R\}^*$ e uma única matriz $M_2 \in \mathcal{D}_n$ tais que $M = \text{PROD}(W) \cdot M_2$.

Por fim, mostraremos que se repetirmos o processo feito anteriormente k-vezes, para algum $k \in \mathbb{N}$, encontraremos uma matriz $M_k \in \mathcal{LB}_n$. Suponha que para todo $k \in \mathbb{N}$, existe $M_k \notin \mathcal{LD}_n$ e $W_1, W_2, \cdots, W_k \in \{L, R\}$ tais que $M = \mathbf{W}_1 \cdot \mathbf{W}_2 \cdot \cdots \cdot \mathbf{W}_k \cdot M_k$. Como $\mathbf{L} \notin \mathcal{CB}_n$ e $\mathbf{R} \notin \mathcal{CB}_n$, podemos usar item (b) do Lema 4.3,

$$\begin{aligned} M &= \mathbf{W}_1 \cdot \mathbf{W}_2 \cdot \cdots \cdot \mathbf{W}_k \cdot M_k \\ S(M) &= S(\mathbf{W}_1 \cdot \mathbf{W}_2 \cdot \cdots \cdot \mathbf{W}_k \cdot M_k) \\ S(M) &= g_1 + s(\mathbf{W}_2 \cdot \cdots \cdot \mathbf{W}_k \cdot M_k) \\ &\vdots \\ S(M) &= g_1 + g_2 + \cdots + g_k + s(M_k) \end{aligned}$$

onde $g_i \in \mathbb{N}$ para todo $1 \leq i \leq k$. Absurdo, uma vez que $S(M)$ é um número natural e a soma do segundo membro da equação diverge quando $k \to \infty$.

Em outras palavras, para cada matriz $M \in \mathbf{L}\mathcal{D}_n \cup \mathbf{R}\mathcal{D}_n$, existe uma única palavra $W = W_1W_2 \cdots W_l \in \{L, R\}^*$ com exatamente $l \in \mathbb{N}$ letras e uma única matriz $M_l \in \mathcal{LB}_n$ tal que $M = \text{PROD}(W) \cdot M_l$.

A demonstração do caso $M = Q' \cdot \text{PROD}(W')$ com $W \in \{L, R\}^*$ e $Q' \in \mathcal{CB}_n$ é análoga à anterior. □

Corolário 4.6. *Para cada matriz $M \in \mathcal{D}_1$ existe uma única palavra $W \in \{L, R\}^*$ tal que $M = \text{PROD}(W)$.*

Demonstração. Seja $M \in \mathcal{D}_1$. Pelo Teorema 4.5 existe uma única palavra $W \in \{L, R\}^*$ e uma única matriz $Q \in \mathcal{LB}_1$ tal que $M = \text{PROD}(W) \cdot Q$. Já pelo Lema 4.2, $\mathcal{LB}_1 = \{Id_2\}$.

Portanto $Q = Id_2$ e $M = \text{PROD}(W)$. □

Corolário 4.7. *O monoide $(\{L, R\}^*, *)$ das palavras em $\{L, R\}$ com a operação de concatenação é isomorfo ao monoide $(\mathcal{D}_1, \cdot)$ das matrizes em $\mathcal{D}_1$ com a operação de multiplicação.*

Demonstração. Segue diretamente do Corolário 4.6 e da definição de PROD que a função PROD : $\{L, R\}^* \to \mathcal{D}_1$ é um isomorfismo. □

Corolário 4.8. *Cada matriz $M \in \mathcal{LB}_n$ possui uma única fatoração $M = Q \cdot \text{PROD}(W)$, onde $W \in \{L, R\}^*$ e $Q \in \mathcal{DB}_n$. Analogamente, cada matriz $M' \in \mathcal{CB}_n$ possui uma única fatoração $M' = \text{PROD}(W') \cdot Q'$, onde $W' \in \{L, R\}^*$ e $Q' \in \mathcal{DB}_n$.*

Demonstração. Faremos a demonstração para o caso da fatoração $M = Q \cdot \text{PROD}(W)$, onde $W \in \{L, R\}^*$ e $Q \in \mathcal{DB}_n$.

Seja $M \in \mathcal{LB}_n$. Pelo Teorema 4.5, existe uma única palavra $W \in \{L, R\}^*$ e uma única matriz $Q \in \mathcal{CB}_n$ tais que $M = Q \cdot \text{PROD}(W)$.

Suponha que $Q \notin \mathcal{LB}_n$. Logo, pela Observação 4.1, vale que ocorre apenas um dos casos a seguir: $Q \in \mathbf{L}\mathcal{D}_n$ ou $Q \in \mathbf{R}\mathcal{D}_n$. Em outras palavras, existe um único $V \in \{L, R\}$ e uma matriz $Q_1 \in \mathcal{D}_n$ tais que $Q = \mathbf{V} \cdot Q_1$. Sendo assim, temos que $M = Q \cdot \text{PROD}(W) = \mathbf{V} \cdot Q_1 \cdot \text{PROD}(W) \in \mathbf{L}\mathcal{D}_n \cup \mathbf{R}\mathcal{D}_n$, o que é absurdo, pois pela Observação 4.1, $\mathcal{LB}_n$, $\mathbf{L}\mathcal{D}_n$ e $\mathbf{R}\mathcal{D}_n$ são dois a dois disjuntos.

Vale então que $Q \in \mathcal{LB}_n$. Portanto $Q \in \mathcal{LB}_n \cap \mathcal{CB}_n = \mathcal{DB}_n$

A demonstração do caso $M' = \text{PROD}(W') \cdot Q'$, com $M' \in \mathcal{CB}_n$, $W' \in \{L, R\}^*$ e $Q' \in \mathcal{DB}_n$ é análoga à anterior. □

4.3 Decomposição dos Vetores de $\mathcal{C}_2$ associados a números racionais

Definição 4.9. *Seja $M \in \mathcal{D}_n$, $n > 0$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Chamaremos de $r : \mathcal{D}_n \to \mathbb{R}^2$ a função que leva M no vetor $r(M) = \begin{pmatrix} d-b \\ a-c \end{pmatrix}$.*

Se $M \in \mathcal{LB}_n$, do fato que $ad - bc = n > 0$, então não pode ocorrer que $a < c$ e $d < b$. Portanto, necessariamente $a > c$ e $d > b$, e assim $r(M) = \begin{pmatrix} d-b \\ a-c \end{pmatrix} \in \mathcal{C}_2$.

Proposição 4.10. *Dado $M \in \mathcal{D}_n$, vale que $r(M \cdot \mathbf{L}) = \mathbf{L}^{-1} \cdot r(M)$ e $r(M \cdot \mathbf{R}) = \mathbf{R}^{-1} \cdot r(M)$.*

Demonstração. Basta notar que, dado $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{D}_n$, temos:

$$r(M \cdot \mathbf{L}) = r\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = r\begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix} = \begin{pmatrix} d-b \\ a+b-(c+d) \end{pmatrix}$$
$$= \begin{pmatrix} d-b \\ -(d-b)+a-c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} d-b \\ a-c \end{pmatrix} = \mathbf{L}^{-1} \cdot r(M)$$

e

$$r(M \cdot \mathbf{R}) = r\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = r\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} c+d-(a+b) \\ a-c \end{pmatrix}$$
$$= \begin{pmatrix} d-b-(a-c) \\ a-c \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} d-b \\ a-c \end{pmatrix} = \mathbf{R}^{-1} \cdot r(M).$$

□

Corolário 4.11. *Dado $M \in \mathcal{D}_n$ e $W \in \{L, R\}^*$, tem-se que*

$$r(M \cdot \text{PROD}(W)) = (\text{PROD}(W))^{-1} \cdot r(M).$$

Demonstração. Seja $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{D}_n$. Claramente a equação acima é válida para a palavra vazia $W = \lambda$. Seja $k \in \mathbb{N}$ e uma palavra não-vazia $W = W_1W_2W_3 \cdots W_k \in \{L, R\}^*$, onde $W_i \in \{L, R\}$, para todo $1 \leq i \leq k$. Provaremos por indução em k que

$$r(M \cdot \text{PROD}(W_1W_2 \cdots W_k)) = (\text{PROD}(W_1W_2 \cdots W_k))^{-1} \cdot r(M). \tag{4.1}$$

Para $k = 1$, a equação (4.1) é verdadeira, pois segue diretamente da proposição anterior. Suponha que a equação (4.1) seja verdadeira para algum $k = m \in \mathbb{N}$. Como $M \in \mathcal{D}_n$ e $\mathbf{W}_1 \in \mathcal{D}_1$, tome $M' = M \cdot \mathbf{W}_1 \in \mathcal{D}_n$. Logo

$$\begin{aligned}
r(M \cdot \text{PROD}(W_1 \cdots W_{m+1})) &= r(M \cdot \mathbf{W}_1 \cdot \mathbf{W}_2 \cdot \cdots \cdot \mathbf{W}_{m+1}) \\
&= r(M \cdot \mathbf{W}_1 \cdot \text{PROD}(W_2 \cdots W_{m+1})) \\
&= r(M' \cdot \text{PROD}(W_2 \cdots W_{m+1})) \\
&\overset{\text{Hip.Ind.}}{=} (\text{PROD}(W_2 \cdots W_{m+1}))^{-1} \cdot r(M') \\
&= (\text{PROD}(W_2 \cdots W_{m+1}))^{-1} \cdot r(M \cdot \mathbf{W}_1) \\
&\overset{\text{Prop.4.10}}{=} (\text{PROD}(W_2 \cdots W_{m+1}))^{-1} \cdot \mathbf{W}_1^{-1} \cdot r(M) \\
&= (\mathbf{W}_1 \cdot \text{PROD}(W_2 \cdots W_{m+1}))^{-1} \cdot r(M) \\
&= (\text{PROD}(W_1W_2 \cdots W_{m+1}))^{-1} \cdot r(M).
\end{aligned}$$

Portanto a equação (4.1) é verdadeira para todo $k \in \mathbb{N}$. □

Lema 4.12. *Seja $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathcal{C}_2$, onde $a > 0$ e $b > 0$.*

(a) Se $a > b$, então existem únicos $r_a \in \mathbb{R}$ e $k_a \in \mathbb{N}$ tais que $\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{R}^{k_a} \cdot \begin{pmatrix} r_a \\ b \end{pmatrix}$ e $0 < r_a \leq b$.

Caso $a, b \in \mathbb{N}$, vale que $r_a \in \mathbb{N}$ e $\text{mdc}(r_a, b) = \text{mdc}(a, b)$.

(b) Se $a < b$, então existem únicos $r_b \in \mathbb{R}$ e $k_b \in \mathbb{N}$ tais que $\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{L}^{k_b} \cdot \begin{pmatrix} a \\ r_b \end{pmatrix}$ *e* $0 < r_b \leq a$.

Caso $a, b \in \mathbb{N}$, vale que $r_b \in \mathbb{N}$ e $\text{mdc}(a, r_b) = \text{mdc}(a, b)$.

Demonstração. Vamos provar o item (a). Seja $\gamma : \mathbb{N} \to \mathbb{R}$, com $\gamma(k) = a - kb$ e $A = \gamma^{-1}(\mathbb{R}_+^*)$, ou seja, $A = \{k \in \mathbb{N} : \gamma(k) > 0\}$.

Temos que A não é vazio, pois de $a > b$, vale que $1 \in A$, já que $\gamma(1) = a - b > 0$.

Do fato de $b > 0$, existe $\overline{k} \in \mathbb{N}$ tal que $\overline{k}b > a$. Com isso, vale que para todo número natural $k \geq \overline{k}$, temos $\gamma(k) = a - kb \leq a - \overline{k}b < 0$. Em outras palavras, se $k \in \mathbb{N}$ e $k \geq \overline{k}$ então $k \notin A$. Logo $\overline{k}$ é um limitante superior de A.

Como A é um subconjunto de $\mathbb{N}$ não-vazio e limitado, A possui elemento máximo. Tome $k_a = \max A$ e $r_a = \gamma(k_a) = a - k_a b$. Temos que $r_a > 0$, pois $k_a \in A$. Do fato de k_a ser o elemento máximo de A, vale que $k_a + 1 \notin A$, ou seja, $\gamma(k_a + 1) = a - (k_a + 1)b = a - k_a b - b = r_a - b \leq 0$. Logo, $0 < r_a \leq b$. Como $a = k_a b + r_a$, temos

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} k_a b + r_a \\ b \end{pmatrix} = \begin{pmatrix} 1 & k_a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} r_a \\ b \end{pmatrix} = \mathbf{R}^{k_a} \cdot \begin{pmatrix} r_a \\ b \end{pmatrix}.$$

No caso particular em que $a, b \in \mathbb{N}$, temos que $r_a = a - k_a b \in \mathbb{N}$ e $\text{mdc}(a, b) = \text{mdc}(k_a b + r_a, b) = \text{mdc}(r_a, b)$.

Podemos fazer um raciocínio análogo para o item (b), tomando a função $\gamma : \mathbb{N} \to \mathbb{R}$, com $\gamma(k) = b - ka$. □

Proposição 4.13. *Para cada vetor* $\begin{pmatrix} a \\ b \end{pmatrix}$ *com $a, b \in \mathbb{N}$, existe uma única palavra $W \in \{L, R\}^*$ e um único $g \in \mathbb{N}$ tal que*

$$\begin{pmatrix} a \\ b \end{pmatrix} = \text{PROD}(W) \cdot \begin{pmatrix} g \\ g \end{pmatrix}.$$

Vale também que g é o máximo divisor comum entre a e b.

Demonstração. Como $a, b \in \mathbb{N}$, temos que ocorre apenas um dos seguintes casos: $a = b$, $a > b$ ou $a < b$. Caso $a = b$, vale que $g = \text{mdc}(a, b) = a$ e $W = \lambda$.

Suponha que $a > b$. Usando o item (a) do Lema 4.12 obtemos $r_1 \in \mathbb{R}$ e $k_1 \in \mathbb{N}$ de modo que $\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{R}^{k_1} \cdot \begin{pmatrix} r_1 \\ b \end{pmatrix}$, com $0 < r_1 \leq b$. Note que, como $a, b \in \mathbb{N}$, tem-se que $r_1 \in \mathbb{N}$ e $\text{mdc}(r_1, b) = \text{mdc}(a, b)$. Caso $r_1 = b$, temos que $W = R^{k_1}$ e $g = b$. Caso $r_1 < b$, do item (b) do Lema 4.12 temos que existem $k_2 \in \mathbb{N}$ e $r_2 \in \mathbb{R}$ tais que $\begin{pmatrix} r_1 \\ b \end{pmatrix} = \mathbf{L}^{k_2} \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, onde vale $0 < r_2 \leq r_1$. Como $r_1, b \in \mathbb{N}$, temos que $r_2 \in \mathbb{N}$ e $\text{mdc}(r_1, r_2) = \text{mdc}(r_1, b) = \text{mdc}(a, b)$. Logo, $\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{R}^{k_1} \cdot \begin{pmatrix} r_1 \\ b \end{pmatrix} = \mathbf{R}^{k_1} \cdot \mathbf{L}^{k_2} \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \text{PROD}(R^{k_1} L^{k_2}) \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, com $0 < r_2 \leq r_1 < b$.

Podemos repetir esse processo de intercalar os itens (a) e (b) do Lema 4.12 até encontrarmos um índice $j \in \mathbb{N}$ tal que $r_j = r_{j-1}$, pois cada resto será um número natural e não existe uma sequência infinita estritamente decrescente de números naturais.

Portanto, temos que $\begin{pmatrix} a \\ b \end{pmatrix} = \text{PROD}(W) \cdot \begin{pmatrix} r_j \\ r_j \end{pmatrix}$, onde $W = U_1^{k_1} U_2^{k_2} \cdots U_j^{k_j} \in \{L, R\}^*$ de forma que $U_i = \begin{cases} R & \text{, se } i \text{ é ímpar;} \\ L & \text{, se } i \text{ é par.} \end{cases}$ e $r_j = \text{mdc}(r_j, r_j) = \text{mdc}(a, b) = g$.

O caso $b > a$ pode ser demonstrado analogamente, apenas mudando a ordem de aplicação dos itens do Lema 4.12. □

Definição 4.14. *Dado o vetor $x = \begin{pmatrix} a \\ b \end{pmatrix}$ com $a, b \in \mathbb{N}$, chamaremos a palavra W encontrada na Proposição 4.13 de* **palavra geradora** *de x. Dada uma matriz $M = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \in \mathcal{LB}_n$, do fato que $xz - wy = n > 0$, temos que $z > y$ e $x > w$. Em outras palavras, $z - y, x - w \in \mathbb{N}$. Portanto, podemos encontrar a palavra geradora do vetor $r(M) = \begin{pmatrix} z - y \\ x - w \end{pmatrix}$.*

Observação 4.2. Chamaremos de W_M a palavra geradora do vetor $r(M)$.

4.4 Relações entre as palavras de $\{L, R\}^{\mathbb{N}}$ e os vetores de $\mathcal{C}_2$

Definição 4.15. *Dado um vetor $x = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathcal{C}_2$ e uma palavra infinita $U = U_1 U_2 U_3 \cdots \in \{L, R\}^{\mathbb{N}}$ dizemos que x* **aceita** *U quando existir uma sequência de vetores $(x_n)_{n \in \mathbb{Z}_+}$ de $\mathcal{C}_2$ tais que $x_0 = x$ e, para todo $i \in \mathbb{N}$, vale que $x_{i-1} = \text{PROD}(U_i) \cdot x_i$.*

Exemplo 5. Dado um número real $\xi > 0$, o vetor $\begin{pmatrix} 0 \\ \xi \end{pmatrix}$ aceita apenas a palavra infinita L^∞, já que $\begin{pmatrix} 0 \\ \xi \end{pmatrix} = \mathbf{L} \cdot \begin{pmatrix} 0 \\ \xi \end{pmatrix}$, mas para qualquer vetor $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathcal{C}_2$ vale que $\mathbf{R} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a + b \\ b \end{pmatrix}$ e como $a + b > 0$, não é possível que $\begin{pmatrix} 0 \\ \xi \end{pmatrix} = \mathbf{R} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$. Portanto, para que o vetor $\begin{pmatrix} 0 \\ \xi \end{pmatrix}$ aceite uma palavra infinita $W \in \{L, R\}^{\mathbb{N}}$ é necessário que W não possua nenhuma letra R.

Analogamente temos que o vetor $\begin{pmatrix} \xi \\ 0 \end{pmatrix}$ aceita apenas a palavra infinita $R^\infty \in \{L, R\}^{\mathbb{N}}$.

Exemplo 6. Considere um vetor $x = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathcal{C}_2$ tal que $a, b \in \mathbb{N}$, e $\text{mdc}\{a, b\} = g$. Da Proposição 4.13 tem-se que $x = \begin{pmatrix} a \\ b \end{pmatrix} = \text{PROD}(W) \cdot \begin{pmatrix} g \\ g \end{pmatrix}$ onde W é a palavra geradora de x.

Considerando que $\begin{pmatrix} g \\ g \end{pmatrix} = \mathbf{L} \cdot \begin{pmatrix} g \\ 0 \end{pmatrix} = \mathbf{R} \cdot \begin{pmatrix} 0 \\ g \end{pmatrix}$ e o exemplo anterior, podemos concluir que as duas únicas palavras infintas que o vetor $x = \begin{pmatrix} a \\ b \end{pmatrix}$, $a, b \in \mathbb{N}$ pode aceitar são WLR^∞ e WRL^∞.

Proposição 4.16. *Sejam $x \in \mathcal{C}_2$ e $W = W_1W_2W_3\cdots \in \{L, R\}^{\mathbb{N}}$. Temos que x aceita W se, e somente se, existir uma sequência de vetores $(x_n)_{n\in\mathbb{Z}_+}$ de $\mathcal{C}_2$ tais que $x_0 \sim x$ e, para todo $i \in \mathbb{N}$, vale que $x_{i-1} \sim \text{PROD}(W_i) \cdot x_i$, onde $\sim$ é a relação de equivalência da Definição 2.4.*

Demonstração. Se existe uma sequência de vetores $(x_n)_{n\in\mathbb{Z}_+}$ tal que $x_0 \sim x$ e, para todo $i \in \mathbb{N}$, vale que $x_{i-1} \sim \text{PROD}(W_i) \cdot x_i$, então pela Proposição 2.5 temos que, para todo $n \in \mathbb{Z}_+$, existem $\alpha_n \in \mathbb{R}$ tais que $x = \alpha_0 \cdot x_0$ e, para todo $i \in \mathbb{N}$, $x_{i-1} = \alpha_i \cdot \text{PROD}(W_i) \cdot x_i$. Defina a sequência $(\hat{x}_n)_{n\in\mathbb{Z}_+}$ onde, para cada $n \in \mathbb{Z}_+$, $\hat{x}_n = \prod_{k=0}^{n} \alpha_k \cdot x_n$. Logo $\hat{x}_0 = \alpha_0 \cdot x_0 = x$ e para todo $i \in \mathbb{N}$,

$$\begin{aligned}\hat{x}_{i-1} &= \prod_{k=0}^{i-1} \alpha_k \cdot x_{i-1} = \prod_{k=0}^{i-1} \alpha_k \cdot (\alpha_i \cdot \text{PROD}(W_i) \cdot x_i) = \prod_{k=0}^{i} \alpha_k \cdot \text{PROD}(W_i) \cdot x_i \\ &= \text{PROD}(W_i) \cdot \left(\prod_{k=0}^{i} \alpha_k \cdot x_i \right) = \text{PROD}(W_i) \cdot \hat{x}_i\end{aligned}$$

Portanto x aceita a palavra W. A recíproca é claramente verdadeira. □

Dado um vetor $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathcal{C}_2$ com $x_2 \neq 0$, existe uma relação entre uma palavra $W \in \{L, R\}^{\mathbb{N}}$ aceita por x e a representação do número $\frac{x_1}{x_2} \in \mathbb{R}$ por frações continuadas.

Teorema 4.17. *Seja $x = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \in \mathcal{C}_2$ tal que $\xi = \frac{\xi_1}{\xi_2} \in \mathbb{R}$ é um número irracional cuja representação por frações continuadas seja $\xi = [a_0; a_1, a_2, a_3 \cdots]$.*

- *Se $\xi_1 > \xi_2$, então x aceita apenas a palavra infinita $R^{a_0}L^{a_1}R^{a_2}\cdots$;*
- *Se $\xi_1 < \xi_2$, então x aceita apenas a palavra infinita $L^{a_1}R^{a_2}L^{a_3}\cdots$.*

Demonstração. Suponha que $\xi_1 > \xi_2 > 0$. Defina a sequência de vetores $(x_n)_{n\in\mathbb{Z}_+}$ de $\mathcal{C}_2$ de forma que $x_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$, onde

$$a_n = \begin{cases} \theta_\xi(n) & \text{, se } n \text{ é par;} \\ 1 & \text{, se } n \text{ é ímpar;} \end{cases} \text{ e } b_n = \begin{cases} 1 & \text{, se } n \text{ é par;} \\ \theta_\xi(n) & \text{, se } n \text{ é ímpar.} \end{cases}$$

Do fato de $\xi = \dfrac{\xi_1}{\xi_2} = \theta_\xi(0)$, vale que $x = \begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix} \sim \begin{pmatrix}\theta_\xi(0)\\ 1\end{pmatrix} = \begin{pmatrix}a_0\\ b_0\end{pmatrix} = x_0$. Mostraremos agora que, para todo $i \in \mathbb{N}$, vale que $x_{i-1} \sim \mathbf{U}_i^{a_{i-1}} \cdot x_i$, com $U_i = \begin{cases} L & \text{, se } i \text{ é par;} \\ R & \text{, se } i \text{ é impar.}\end{cases}$

Como $\xi_1 > \xi_2 > 0$, pelo item (a) do Lema 4.12, existem únicos $k_0 \in \mathbb{N}$ e $r_0 \in \mathbb{R}$ tais que $x = \begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix} = \mathbf{R}^{k_0} \cdot \begin{pmatrix}r_0\\ \xi_2\end{pmatrix} = \begin{pmatrix}k_0\xi_2 + r_0\\ \xi_2\end{pmatrix}$, com $0 < r_0 \leq \xi_2$. Como $\xi = \dfrac{\xi_1}{\xi_2}$ é irracional, temos que $r_0 \neq \xi_2$. Com isso, temos que $\dfrac{\xi_1}{\xi_2} = \dfrac{k_0\xi_2 + r_0}{\xi_2} = k_0 + \dfrac{r_0}{\xi_2} = a_0 + \dfrac{1}{\theta_\xi(1)}$, o que implica em $k_0 - a_0 = \dfrac{1}{\theta_\xi(1)} - \dfrac{r_0}{\xi_2} \in \mathbb{Z} \cap (-1, 1) = \{0\}$. Logo $k_0 = a_0$ e $\dfrac{1}{\theta_\xi(1)} = \dfrac{r_0}{\xi_2}$. Com efeito, vale que $x_0 \sim x = \begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix} = \mathbf{R}^{a_0} \cdot \begin{pmatrix}r_0\\ \xi_2\end{pmatrix} \sim \mathbf{R}^{a_0} \cdot \begin{pmatrix}1\\ \theta_\xi(1)\end{pmatrix} = \mathbf{R}^{a_0} \cdot \begin{pmatrix}a_1\\ b_1\end{pmatrix} = \mathbf{U}_1^{a_0} \cdot x_1$.

Suponha agora que existe $m \in \mathbb{N}$ tal que $x_{m-1} \sim \mathbf{U}_m^{a_{m-1}} \cdot x_m$. Primeiramente, suponha que m é par. Logo, $x_m = \begin{pmatrix}a_m\\ b_m\end{pmatrix} = \begin{pmatrix}\theta_\xi(m)\\ 1\end{pmatrix}$. Pelo item (a) do Lema 4.12, temos que existem $k_m \in \mathbb{N}$ e $r_m \in \mathbb{R}$ tais que $\begin{pmatrix}\theta_\xi(m)\\ 1\end{pmatrix} = \mathbf{R}^{k_m} \cdot \begin{pmatrix}r_m\\ 1\end{pmatrix}$, onde $0 < r_m \leq 1$. Do fato de ξ ser irracional, vale que para todo $n \in \mathbb{Z}_+$, $\theta_\xi(n)$ é irracional, logo $r_m < 1$. Com efeito, $\theta_\xi(m) = a_m + \dfrac{1}{\theta_\xi(m+1)} = k_m + r_m$, o que implica em $a_m - k_m = r_m - \dfrac{1}{\theta_\xi(m+1)}$. Logo $a_m = k_m$ e $r_m = \dfrac{1}{\theta_\xi(m+1)}$. Com isso, temos $x_m = \begin{pmatrix}\theta_\xi(m)\\ 1\end{pmatrix} = \mathbf{R}^{a_m} \cdot \begin{pmatrix}r_m\\ 1\end{pmatrix} \sim \mathbf{R}^{a_m} \cdot \begin{pmatrix}1\\ \theta_\xi(m+1)\end{pmatrix} = \mathbf{U}_{m+1}^{a_m} \cdot x_{m+1}$. Caso m seja ímpar, por um raciocínio análogo, tem-se que $x_m = \begin{pmatrix}1\\ \theta_\xi(m)\end{pmatrix} \sim \mathbf{L}^{a_m} \cdot \begin{pmatrix}\theta_\xi(m+1)\\ 1\end{pmatrix} = \mathbf{U}_{m+1}^{a_m} \cdot x_{m+1}$. Pela Proposição 4.16 temos, portanto, que x aceita a palavra $U = U_1^{a_0}U_2^{a_1}U_3^{a_2}\cdots = R^{a_0}L^{a_1}R^{a_2}\cdots$.

Considere agora uma palavra $V = V_1V_2V_3\cdots \in \{L, R\}^{\mathbb{N}}$, tal que $V_i \in \{L, R\}$ para todo $i \in \mathbb{N}$. Podemos escrever $U = R^{a_0}L^{a_1}R^{a_2}\cdots$ de forma que $U = \overline{U}_1\overline{U}_2\overline{U}_3\cdots$, com $\overline{U}_i \in \{L, R\}$, para todo $i \in \mathbb{N}$. Suponha que V é diferente de U. Logo, existe um índice $p \in \mathbb{N}$ tal que $V_p \neq \overline{U}_p$. Tome p_0 o menor índice p que satisfaz $V_p \neq \overline{U}_p$. Caso x aceite V, temos que existem $v_{p_0} = \begin{pmatrix}\gamma_1\\ \gamma_2\end{pmatrix}, \overline{x}_{p_0} = \begin{pmatrix}\sigma_1\\ \sigma_2\end{pmatrix} \in \mathcal{C}_2$ tais que

$$x = \text{PROD}(V_1V_2\cdots V_{p_0}) \cdot v_{p_0} = \text{PROD}(\overline{U}_1\overline{U}_2\cdots\overline{U}_{p_0}) \cdot \overline{x}_{p_0}$$
$$\mathbf{V}_{p_0} \cdot v_{p_0} = \overline{\mathbf{U}}_{p_0} \cdot \overline{x}_{p_0}.$$

Sem perda de generalidade, suponha $\mathbf{V}_{p_0} = \mathbf{R}$. Temos então que $\overline{\mathbf{U}}_{p_0} = \mathbf{L}$ e

$$\mathbf{V}_{p_0} \cdot v_{p_0} = \mathbf{R} \cdot \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} \gamma_1 + \gamma_2 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \sigma_1 + \sigma_2 \end{pmatrix} = \mathbf{L} \cdot \begin{pmatrix} \sigma_1 \\ \sigma_2 \end{pmatrix} = \overline{\mathbf{U}}_{p_0} \cdot \overline{x}_{p_0},$$

o que implica em $\gamma_1 = \sigma_2 = 0$ e $v_{p_0} = \begin{pmatrix} 0 \\ \gamma_2 \end{pmatrix}$. Note que

$$x = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} = \text{PROD}(V_1 V_2 \cdots V_{p_0}) \cdot \begin{pmatrix} 0 \\ \gamma_2 \end{pmatrix} \sim \text{PROD}(V_1 V_2 \cdots V_{p_0}) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} q_1 \\ q_2 \end{pmatrix}$$

onde $q_1, q_2 \in \mathbb{Z}_+$ Absurdo, pois $\xi = \dfrac{\xi_1}{\xi_2}$ é irracional.

Por fim, analisaremos o caso em que $0 < \xi_1 < \xi_2$. Pelo item (b) do Lema 4.12, existem únicos $k' \in \mathbb{N}$ e $r' \in \mathbb{R}$ tais que $x = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} = \mathbf{L}^{k'} \cdot \begin{pmatrix} \xi_1 \\ r' \end{pmatrix}$, com $0 < r' \leq \xi_1$. Como $\xi = \dfrac{\xi_1}{\xi_2}$ é um número irracional, vale que $0 < r' < \xi_1$. Note que $\xi = \dfrac{\xi_1}{\xi_2} < 1$, ou seja, $\xi = \dfrac{\xi_1}{\xi_2} = a_0 + \dfrac{1}{\theta_\xi(1)} = \dfrac{\xi_1}{k'\xi_1 + r'}$ e, com isso, $a_0 = \dfrac{\xi_1}{k'\xi_1 + r'} - \dfrac{1}{\theta_\xi(1)}$. Logo $a_0 = 0$ e $\theta_\xi(1) = \dfrac{k'\xi_1 + r'}{\xi_1} = k' + \dfrac{r'}{\xi_1} = a_1 + \dfrac{1}{\theta_\xi(2)}$, o que implica em $k' = a_1$ e $\theta_\xi(2) = \dfrac{\xi_1}{r'}$. Note que $\theta_\xi(2) = \dfrac{\xi_1}{r'} = [a_2; a_3, a_4, \cdots]$ é irracional e $\xi_1 > r' > 0$, logo podemos aplicar a primeira parte deste Teorema, ou seja, o vetor $\begin{pmatrix} \xi_1 \\ r' \end{pmatrix}$ aceita apenas a palavra $R^{a_2} L^{a_3} R^{a_4} \cdots$. Como a decomposição $x = \mathbf{L}^{a_1} \cdot \begin{pmatrix} \xi_1 \\ r' \end{pmatrix}$, onde $0 < r' < \xi_1$, é única, temos portanto que x aceita apenas a palavra $L^{a_1} R^{a_2} L^{a_3} R^{a_4} \cdots$. □

4.5 MATRIZES DUPLAMENTE BALANCEADAS

Definição 4.18. *Dado $n \in \mathbb{N}$, uma tripla ordenada (g, s, s') de números inteiros não negativos é chamada de* **$(*, n)$-tripla** *caso $g \cdot (s + s' + g) = n$. Dado $M \in \mathcal{D}_n$, dizemos que a $(*, n)$-tripla (g, s, s')* **está associada a** *M se existir uma palavra $W \in \{L, R\}^*$ tal que $M \cdot \text{PROD}(W) = \begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix}$.*

Proposição 4.19. *Dado $M \in \mathcal{D}_n$. $r(M) = \begin{pmatrix} g \\ g \end{pmatrix}$ se, e somente se, $M = \begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix}$, onde (g, s, s') é uma $(*, n)$-tripla.*

Demonstração. ($\Longrightarrow$) Seja $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Se $r(M) = \begin{pmatrix} g \\ g \end{pmatrix}$, então $d - b = a - c$. Sejam

$g = d - b = a - c$, $s = b$ e $s' = c$.

Logo $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c + (a-c) & b \\ c & b + (d-b) \end{pmatrix} = \begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix}$. Do fato de $M \in \mathcal{D}_n$, tem-se que $\det(M) = (s'+g)(s+g) - ss' = g(s + s' + g) = n$.

($\Longleftarrow$) Se $M = \begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix}$, então $r(M) = \begin{pmatrix} g \\ g \end{pmatrix}$. □

Teorema 4.20. *Para cada $M \in \mathcal{LB}_n$ existe uma única $(*, n)$-tripla associada a M. A $(*, n)$-tripla associada a M satisfaz a equação*

$$M \cdot \text{PROD}(W_M) = \begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix}.$$

Demonstração. Seja $M \in \mathcal{LB}_n$. Do fato de W_M ser a palavra geradora de $r(M)$, temos que $r(M) = \text{PROD}(W_M) \cdot \begin{pmatrix} g \\ g \end{pmatrix}$, com g sendo o máximo divisor comum das entradas de $r(M)$. Pelo Corolário 4.11, temos que $r(M \cdot \text{PROD}(W_M)) = (\text{PROD}(W_M))^{-1} \cdot r(M) = \begin{pmatrix} g \\ g \end{pmatrix}$. Pela Proposição 4.19, vale que $M \cdot \text{PROD}(W_M) = \begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix}$, onde (g, s, s') é uma $(*, n)$-tripla. Logo (g, s, s') está associada a M. Suponha que (g_1, s_1, s_1') seja uma $(*, n)$-tripla associada a M. então existe uma palavra $W_1 \in \{L, R\}^*$ tal que $M \cdot \text{PROD}(W_1) = \begin{pmatrix} s_1' + g_1 & s_1 \\ s_1' & s_1 + g_1 \end{pmatrix}$. Pelo Corolário 4.11, $(\text{PROD}(W_1))^{-1} \cdot r(M) = r(M \cdot \text{PROD}(W_1)) = \begin{pmatrix} g_1 \\ g_1 \end{pmatrix}$. Com efeito, temos que $\text{PROD}(W_1) \cdot \begin{pmatrix} g_1 \\ g_1 \end{pmatrix} = r(M) = \text{PROD}(W_M) \cdot \begin{pmatrix} g \\ g \end{pmatrix}$. Pela Proposição 4.13, temos que $W_1 = W_M$ e $g_1 = g$, o que implica em $s_1 = s$ e $s_1' = s'$. Podemos concluir portanto que (g, s, s') é a única $(*, n)$-tripla associada a M. □

O teorema a seguir nos diz que a quantidade de elementos de matrizes duplamente balanceadas de $\mathcal{D}_n$ pode ser calculado encontrando todas as possíveis $(*, n)$-triplas.

Teorema 4.21. *Para cada $(*,n)$-tripla (g, s, s') existe uma única matriz $Q \in \mathcal{DB}_n$ à qual (g, s, s') está associada. As matrizes $M \in \mathcal{LB}_n$ às quais (g, s, s') também está associada são da forma $M = Q \cdot \text{PROD}(U)$, onde U é um prefixo de W_Q. Neste caso, temos $W_Q = UW_M$.*

Demonstração. Seja (g, s, s') uma $(*, n)$-tripla. Como $\begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix} \in \mathcal{LB}_n$, pelo Corolário 4.8, existe uma única palavra $W \in \{L, R\}^*$ e uma única matriz $Q \in \mathcal{DB}_n$ tais que $\begin{pmatrix} s' + g & s \\ s' & s + g \end{pmatrix} = Q \cdot \text{PROD}(W)$. Logo a $(*, n)$-tripla (g, s, s') está associada a matriz Q.

Pelo Teorema 4.20, $Q \cdot \text{PROD}(W_Q) = \begin{pmatrix} s'+g & s \\ s' & s+g \end{pmatrix}$. Portanto $W = W_Q$.

Seja $M \in \mathcal{LB}_n$ tal que a $(*, n)$-tripla (g, s, s') está associada a M. Então, pelo Teorema 4.20, $M \cdot \text{PROD}(W_M) = \begin{pmatrix} s'+g & s \\ s' & s+g \end{pmatrix}$, logo $M \cdot \text{PROD}(W_M) = Q \cdot \text{PROD}(W_Q)$. Pelo Corolário 4.8, temos que M pode ser fatorada em $M = Q_1 \cdot \text{PROD}(U)$, onde $Q_1 \in \mathcal{DB}_n$ e $U \in \{L, R\}^*$. Logo $Q \cdot \text{PROD}(W_Q) = Q_1 \cdot \text{PROD}(U) \cdot \text{PROD}(W_M) = Q_1 \cdot \text{PROD}(UW_M)$ o que, ainda pelo Corolário 4.8, implica em $Q = Q_1$ e $W_Q = UW_M$. Portanto $M = Q \cdot \text{PROD}(U)$, em que U é um prefixo de W_Q. □

Corolário 4.22. *Se $M \in \mathcal{LB}_n$ e $V \in \{L, R\}^*$, então $M \cdot \text{PROD}(V) \in \mathcal{LB}_n$ se, e somente se, V é um prefixo de W_M.*

Demonstração. Seja $Q \in \mathcal{DB}_n$ a matriz tal que a $(*)$-tripla associada a Q seja a mesma de M. Pelo Teorema 4.21, temos que $M = Q \cdot \text{PROD}(U)$, onde $W_Q = UW_M$. Sendo assim, V é um prefixo de W_M se, e somente se, UV é um prefixo de W_Q. Pelo Teorema 4.21, $Q \cdot \text{PROD}(UV) \in \mathcal{LB}_n$ se, e somente se, UV é um prefixo de W_Q. Como $M \cdot \text{PROD}(V) = Q \cdot \text{PROD}(UV)$, vale que $M \cdot \text{PROD}(V) \in \mathcal{LB}_n$ se, e somente se, V é um prefixo de W_M. □

Corolário 4.23. *Se p é primo, então $\mathcal{DB}_p$ possui p elementos.*

Demonstração. As $(*, p)$-triplas devem satisfazer $g(s + s' + g) = p$. Do fato de $g, s, s' \in \mathbb{Z}_+$, considerando que p é primo, então $g = 1$ e $s + s' = p - 1$. Sendo assim, existem exatamente p $(*, p)$-triplas. Pelo Teorema 4.21, existem portanto p matrizes em $\mathcal{DB}_p$. □

Exemplo 7. Para determinar todas as matrizes de $\mathcal{DB}_6$, primeiramente é necessário encontrar todas as $(*, n)$-triplas para $n = 6$. Ou seja, devemos encontrar todas as triplas $(g, s, s') \in \mathbb{Z}_+^3$ tais que $g(s+s'+g) = 6$. Note que g deve ser um divisor de 6, ou seja, $g \in \{1, 2, 3, 6\}$. Vamos analisar quais valores g pode assumir:

- Se $g = 1$, temos $1 \cdot (s + s' + 1) = 6$, ou seja, $s + s' = 5$. Com isso, temos as $(*)$-triplas $(1, 0, 5)$, $(1, 1, 4)$, $(1, 2, 3)$, $(1, 3, 2)$, $(1, 4, 1)$ e $(1, 5, 0)$;
- Se $g = 2$, temos $2 \cdot (s + s' + 2) = 6$, ou seja, $s + s' = 1$. Com isso, temos as $(*)$-triplas $(2, 0, 1)$ e $(2, 1, 0)$;
- Se $g = 3$ ou $g = 6$, temos que a equação $g(s + s' + g) = 6$ não possui soluções para $s, s' \in \mathbb{Z}_+$.

Existem exatamente 8 $(*, n)$-triplas para $n = 6$. Logo o número de matrizes que pertencem a $\mathcal{DB}_6$ é igual a 8. Para cada $(*, n)$-tripla (g, s, s'), seja $M = \begin{pmatrix} g+s' & s \\ s' & g+s \end{pmatrix}$. Pelo Teorema 4.21, temos que existe uma única matriz $Q \in \mathcal{DB}_n$ tal que $Q \cdot \text{PROD}(U) = M$, com U sendo um prefixo de W_Q.

Para a $(*, n)$-tripla $(1, 0, 5)$, temos que $M = \begin{pmatrix} 6 & 0 \\ 5 & 1 \end{pmatrix} \in \mathcal{D}_6\mathbf{L}$. Logo $M = M' \cdot \mathbf{L}$, para alguma $M' \in \mathcal{D}_6$. Com efeito, $M' = M \cdot \mathbf{L}^{-1} = \begin{pmatrix} 6 & 0 \\ 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 4 & 1 \end{pmatrix} \in \mathcal{D}_6\mathbf{L}$. Podemos repetir o processo até encontrar a matriz duplamente balanceada $Q = \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix}$. Note que $r(Q) = \begin{pmatrix} 1 \\ 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \text{PROD}(L^5) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, logo $W_Q = L^5$. Mais ainda, $M = \begin{pmatrix} 6 & 0 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix} = Q \cdot \text{PROD}(L^5)$.

Repetindo o processo para as demais $(*, n)$-triplas, concluímos que

$$\mathcal{DB}_6 = \left\{ \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \right\}.$$

Observação 4.3. Se $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ é duplamente balanceada, então $A' = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ e $\begin{pmatrix} d & b \\ c & a \end{pmatrix}$ também são duplamente balanceadas.

5 TRANSDUTORES

Definição 5.1. *Um* **transdutor** *é uma tripla ordenada* $\mathcal{T} = (A, Q, \mathcal{F})$ *definida por um alfabeto* A*, um conjunto finito* Q *chamado de estados e uma família* $\mathcal{F}$ *de funções indexadas em* Q *onde cada função* $\rho_q : \beta_q \to Q \times A^*$ *de* $\mathcal{F}$ *é definida de forma que* $\beta_q \subset A^*$ *é uma base para o monoide livre* A^**, para todo estado* $q \in Q$*.*

Definição 5.2. *Seja* $\mathcal{T} = (A, Q, \mathcal{F})$ *um transdutor. Dado* $q \in Q$*, seja* $V \in \beta_q$ *e* $\rho_q(V) \in Q \times A^*$*. Chamaremos de* $\sigma_q(V)$ *e* $\delta_q(V)$ *a primeira e a segunda coordenadas do vetor* $\rho_q(V)$*, respectivamente. Em outras palavras, as funções* $\sigma_q : \beta_q \to Q$ *e* $\delta_q : \beta_q \to A^*$ *são tais que* $\rho(V) = (\sigma_q(V), \delta_q(V))$*, para todo* $V \in \beta_q$*.*

Definição 5.3. *Seja* $\mathcal{T} = (A, Q, \mathcal{F})$ *um transdutor. Para qualquer estado* $q \in Q$*, podemos definir a função* $\Psi_q : \{L, R\}^{\mathbb{N}} \to \{L, R\}^{\mathbb{N}}$*, da seguinte forma: Seja* $S \in \{L, R\}^{\mathbb{N}}$ *uma palavra infinta e sejam* $S_0, S_1, S_2, \cdots$*,* $q_0, q_1, q_2, \cdots$*,* $V_0, V_1, V_2, \cdots$*, e* $W_1, W_2, W_3, \cdots$*, definidos por* $S_0 = S$*,* $q_0 = q$ *e, para cada* $i = 0, 1, 2, \cdots$*,* $V_i = H(S_i, \beta_{q_i})$*,* $S_{i+1} = S_i \backslash V_i$*,* $q_{i+1} = \sigma_{q_i}(V_i)$ *e* $W_{i+1} = \delta_{q_i}(V_i)$*. Por fim, defina* $\Psi_q(S)$ *sendo a palavra infinita formada pela concatenação* $W_1 W_2 W_3 \cdots$*.*

Exemplo 8. Seja $\mathcal{T} = (A, Q, \mathcal{F})$ o transdutor tal que $A = \{L, R\}$, $Q = \{a, b, c\}$ e $\mathcal{F} = \{\rho_a, \rho_b, \rho_c\}$ de forma que $\rho_a = \{(R, a, L), (LL, b, L), (LR, c, R)\}$, $\rho_b = \{(R, c, R), (L, b, L)\}$ e $\rho_c = \{(R, c, R), (L, c, R)\}$. Veja Figura 5.1.

Logo, em relação ao estado $a \in Q$, a função $\Psi_a : \{L, R\}^{\mathbb{N}} \to \{L, R\}^{\mathbb{N}}$ é tal que para qualquer $x \in \{L, R\}^{\mathbb{N}}$, tem-se

$$\Psi_a(x) = \begin{cases} L^\infty & \text{, se } x = R^\infty \text{ ou } x = R^{k_0} L^\infty, \text{ com } k_0 \in \mathbb{Z}_+; \\ L^k R^\infty & \text{, se } x = VLRU, \text{ com } U \in \{L, R\}^{\mathbb{N}}, V = R^{k_1} L^{k_2} \text{ tais que } k_1 + k_2 = k. \end{cases}$$

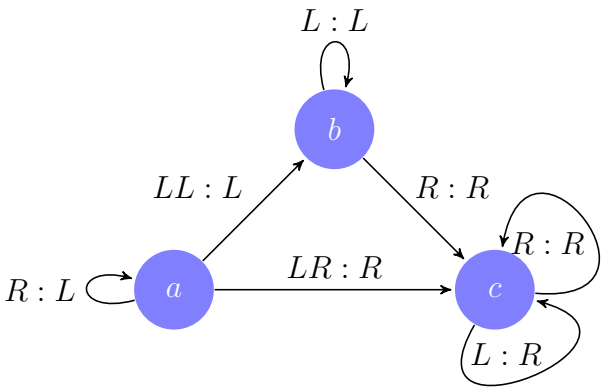

Figura 5.1: Diagrama do transdutor do Exemplo 8.

Por exemplo, no caso em que $x = R^3L^4R^2L^3\cdots \in \{L,R\}^{\mathbb{N}}$, podemos calcular $\Psi_a(x) = \delta_a(R)^3\delta_a(LL)\delta_b(L)^2\delta_b(R)\delta_c(R)\delta_c(L)^3\cdots = L^3LL^2RRR^3\cdots = L^6R^\infty$. Podemos fatorar x de forma que $x = R^3L^4R^2L^3\cdots = R^3L^3LRRL^3\cdots = VLRU$, com $V = R^3L^3$ e $U = RL^3\cdots$.

5.1 Matrizes Duplamente Balanceadas como Estados de um Transdutor

Definição 5.4. *Para cada matriz $M \in \mathcal{LB}_n$ denotamos por $\mathcal{B}_M$ o conjunto de todos os ramos imediatos da palavra W_M.*

Observação 5.1. Segue do Teorema 2.21 que, para toda matriz $M \in \mathcal{LB}_n$, $\mathcal{B}_M$ é uma base de $\{L,R\}^{\mathbb{N}}$.

Exemplo 9. Para $M = \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix} \in \mathcal{LB}_6$, temos que $r(M) = \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \mathbf{L}^2 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \text{PROD}(L^2) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, logo $W_M = L^2$. Pelo Teorema 2.19, o conjunto de todos os ramos imediatos de L^2 é $\mathcal{B}_M = \{R, LR, L^2R, L^3\}$.

Teorema 5.5. *Seja $M \in \mathcal{LB}_n$. Para cada palavra $B \in \mathcal{B}_M$, $M \cdot \text{PROD}(B)$ pertence a $\mathbf{L}\mathcal{LB}_n$ ou a $\mathbf{R}\mathcal{LB}_n$ se a última letra de B for L ou R, respectivamente. Mais ainda, existe uma única palavra não-vazia $V \in \{L,R\}^*$ e uma única matriz $M' \in \mathcal{DB}_n$ tal que $M \cdot \text{PROD}(B) = \text{PROD}(V) \cdot M'$.*

Demonstração. Sejam $M \in \mathcal{LB}_n$ e W_M a palavra geradora de $r(M)$. Pelo Teorema 4.20, existe uma única $(*,n)$-tripla (g,s,s') tal que $M \cdot \text{PROD}(W_M) = \begin{pmatrix} s'+g & s \\ s' & s+g \end{pmatrix}$.

Se $|W_M| = 0$, então $W_M = \lambda$ e $\mathcal{B}_M = \{L,R\} = \{W_ML, W_MR\}$.

No caso em que $|W_M| = j \geq 1$, podemos escrever $W_M = W_1W_2W_3\cdots W_j$, onde $W_i \in \{L,R\}$, para cada $i \in \mathbb{N}$, com $i \leq j$. Neste caso, pelo Teorema 2.19, vale que

$$\mathcal{B}_M = \{\mathfrak{p}(W_1), W_1\mathfrak{p}(W_2), W_1W_2\mathfrak{p}(W_3), \cdots, W_1W_2\cdots W_{j-1}\mathfrak{p}(W_j), W_ML, W_MR\}\ .$$

Temos que, independente do valor de $|W_M|$, dado $B \in \mathcal{B}_M$, ocorre um dos seguintes casos: $B = W_ML$, $B = W_MR$ ou existe $l \in \mathbb{N}$, com $l \leq |W_M|$ tal que $B = W_1W_2\cdots W_{l-1}\mathfrak{p}(W_l)$.

Caso $B = W_ML$, temos

$$M \cdot \text{PROD}(B) = M \cdot \text{PROD}(W_ML) = M \cdot \text{PROD}(W_M) \cdot \mathbf{L} = \begin{pmatrix} g+s' & s \\ s' & g+s \end{pmatrix} \cdot \mathbf{L}$$

$$= \begin{pmatrix} g+s'+s & s \\ s'+g+s & g+s \end{pmatrix} = \mathbf{L} \cdot \begin{pmatrix} g+s'+s & s \\ 0 & g \end{pmatrix} \in \mathbf{L}\mathcal{LB}_n.$$

Caso $B = W_M R$, temos

$$M \cdot \text{PROD}(B) = M \cdot \text{PROD}(W_M R) = M \cdot \text{PROD}(W_M) \cdot \mathbf{R} = \begin{pmatrix} g+s' & s \\ s' & g+s \end{pmatrix} \cdot \mathbf{R}$$
$$= \begin{pmatrix} g+s' & g+s'+s \\ s' & g+s'+s \end{pmatrix} = \mathbf{R} \cdot \begin{pmatrix} g & 0 \\ s' & g+s'+s \end{pmatrix} \in \mathbf{R}\mathcal{CB}_n.$$

Os casos anteriores abrangem o caso em que $|W_M| = 0$. Considere $|W_M| = j \geq 1$. Vamos analisar o caso em que $B = W_1 W_2 \cdots W_{l-1} \mathfrak{p}(W_l)$, para algum $l \in \mathbb{N}$ com $l \leq j$.

Para cada $k \in \mathbb{N}$, com $k \leq j$, vamos definir $U_k \in \{L, R\}^*$ de forma que $U_1 = \lambda$ e $U_k = W_1 W_2 \cdots W_{k-1}$, quando $k \neq 1$. Analogamente, seja $Z_k \in \{L, R\}^*$, de forma que $Z_j = \lambda$ e $Z_k = W_{k+1} W_{k+2} \cdots W_j$, quando $k \neq j$.

Note que, para qualquer $k \in \mathbb{N}$ com $k \leq j$, podemos decompor $W_M = U_k W_k Z_k$. Desta forma, considerando que $B = W_1 W_2 \cdots W_{l-1} \mathfrak{p}(W_l)$ para algum $l \in \mathbb{N}$, com $l \leq j$, temos que $B = U_l \mathfrak{p}(W_l)$.

Considere a decomposição $W_M = U_l W_l Z_l$.

Escrevendo $\text{PROD}(Z_l) = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathcal{D}_1$, temos $(\text{PROD}(Z_l))^{-1} = \begin{pmatrix} w & -y \\ -z & x \end{pmatrix}$.

Note que $M \cdot \text{PROD}(W_M) = M \cdot \text{PROD}(U_l W_l Z_l) = M \cdot \text{PROD}(U_l) \cdot \text{PROD}(W_l) \cdot \text{PROD}(Z_l)$, o que implica em

$$M \cdot \text{PROD}(U_l) = M \cdot \text{PROD}(W_M) \cdot (\text{PROD}(Z_l))^{-1} \cdot (\text{PROD}(W_l))^{-1} .$$

Caso $W_l = R$, temos que

$$M \cdot \text{PROD}(U_l) = M \cdot \text{PROD}(W_M) \cdot (\text{PROD}(Z_l))^{-1} \cdot \mathbf{R}^{-1}$$
$$= \begin{pmatrix} g+s' & s \\ s' & g+s \end{pmatrix} \cdot \begin{pmatrix} w & -y \\ -z & x \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} gw + s'w - sz & -gw - gy - s'w - s'y + sz + sx \\ s'w - gz - sz & -s'w - s'y + gz + gx + sz + sx \end{pmatrix}$$

Como $M \cdot \text{PROD}(U_l)$ não possui entradas negativas, temos que $s'w - gz - sz \geq 0$ e do fato que $\text{PROD}(Z_l) \in \mathcal{D}_1$, vale que $w \geq 0$, $z \geq 0$ e $z + w > 0$. Como $g > 0$, temos que $gz + gw > 0$ e com isso, $-sz + s'w + gw > 0$. Além disto, observando a segunda entrada na primeira linha:

$$-gw - gy - s'w - s'y + sz + sx \geq 0 \;\Rightarrow\; sx - gy - s'y \geq gw + s'w - sz > 0 .$$

Portanto

$$\begin{aligned} M \cdot \text{PROD}(B) &= M \cdot \text{PROD}(U_l \mathfrak{p}(W_l)) = M \cdot \text{PROD}(U_l L) = M \cdot \text{PROD}(U_l) \cdot \mathbf{L} \\ &= \begin{pmatrix} gw + s'w - sz & -gw - gy - s'w - s'y + sz + sx \\ s'w - gz - sz & -s'w - s'y + gz + gx + sz + sx \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -gy - s'y + sx & -gw - gy - s'w - s'y + sz + sx \\ -s'y + gx + sx & -s'w - s'y + gz + gx + sz + sx \end{pmatrix} \\ &= \mathbf{L} \cdot \begin{pmatrix} -gy - s'y + sx & -gy - s'y + sx - (-sz + s'w + gw) \\ gx + gy & gx + gy + (gz + gw) \end{pmatrix} \in \mathbf{L}\mathcal{CB}_n. \end{aligned}$$

Por fim, caso $W_l = L$, seja novamente $\text{PROD}(Z_l) = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. Logo $M \cdot \text{PROD}(U_l) = M \cdot \text{PROD}(W_M) \cdot (\text{PROD}(Z_l))^{-1} \cdot \mathbf{L}^{-1} = \begin{pmatrix} gw + gy + s'w + s'y - sz - sx & -gy - s'y + sx \\ s'w + s'y - gz - gx - sz - sx & -s'y + gx + sx \end{pmatrix}$ não possui entradas negativas. Com efeito, $-gy - s'y + sx \geq 0$. Do fato que $g > 0$ e $x + y > 0$, vale que $gx + gx > 0$ e $-s'y + sx + gx > 0$. Logo,

$$\begin{aligned} M \cdot \text{PROD}(B) &= M \cdot \text{PROD}(U_l \mathfrak{p}(W_l)) = M \cdot \text{PROD}(U_l R) = M \cdot \text{PROD}(U_l) \cdot \mathbf{R} \\ &= \begin{pmatrix} gw + gy + s'w + s'y - sz - sx & -gy - s'y + sx \\ s'w + s'y - gz - gx - sz - sx & -s'y + gx + sx \end{pmatrix} \cdot \mathbf{R} \\ &= \begin{pmatrix} gw + gy + s'w + s'y - sz - sx & gw + s'w - sz \\ s'w + s'y - gz - gx - sz - sx & s'w - gz - sz \end{pmatrix} \\ &= \mathbf{R} \cdot \begin{pmatrix} gz + gw + (gx + gy) & gz + gw \\ s'w - gz - sz - (-s'y + gx + sx) & s'w - gz - sz \end{pmatrix} \in \mathbf{R}\mathcal{CB}_n \end{aligned}$$

Pelo Corolário 4.8, cada matriz $M_1 \in \mathcal{CB}_n$ pode ser decomposta de maneira única na forma $M_1 = \text{PROD}(V') \cdot M'$, em que $V' \in \{L, R\}^*$ e $M' \in \mathcal{DB}_n$. Portanto em todos os casos existe uma palavra não vazia $V \in \{L, R\}^*$ e uma matriz $M' \in \mathcal{DB}_n$ tal que $M \cdot \text{PROD}(B_k) = \text{PROD}(V) \cdot M'$. □

Observação 5.2. Segue do Corolário 4.22 que os elementos de $\mathcal{B}_M$ são minimais, na ordem parcial de comprimento, no sentido que se $V \in \{L, R\}^*$ é um prefixo próprio de $B_j \in \mathcal{B}_M$, então $M \cdot \text{PROD}(V)$ não possui um fator L ou R à esquerda.

Note que, em relação ao Teorema 5.5, dada uma matriz $M \in \mathcal{DB}_n$ e uma palavra $V \in \mathcal{B}_M$, podemos definir as funções $\sigma : \mathcal{DB}_n \times \{L, R\}^* \to \mathcal{DB}_n$ e $\delta : \mathcal{DB}_n \times \{L, R\}^* \to \{L, R\}^*$ tais que $\sigma(M, V) = \sigma_M(V)$ e $\delta(M, V) = \delta_M(V)$ satisfazem a equação

$$M \cdot \text{PROD}(V) = \text{PROD}(\delta_M(V)) \cdot \sigma_M(V).$$

Logo podemos enxergar as matrizes duplamente balanceadas de $\mathcal{D}_n$ como os estados de um transdutor onde a família de funções $\mathcal{F}$ é tal que suas funções $\rho_M : \mathcal{B}_M \to \mathcal{D}_n \times \{L, R\}^*$ são definidas por $\rho_M(V) = (\sigma_M(V), \delta_M(V))$.

5.2 TRANSDUTORES DE RANEY

Definição 5.6. *Para cada inteiro positivo v tal que seu quadrado é um divisor de n, chamaremos de* **transdutor de Raney** *a tripla ordenada $\mathcal{T}_{n,v} = (\{L, R\}, Q_{n,v}, \mathcal{F}_{n,v})$, onde $Q_{n,v}$ é o conjunto de todas as matrizes $M \in \mathcal{DB}_n$ tais que o máximo divisor comum dos elementos de M é v e $\mathcal{F}_{n,v}$ é o conjunto de todas as funções $\rho_M : \mathcal{B}_M \to Q_{n,v} \times \{L, R\}^*$ onde para cada $V \in \mathcal{B}_M$ tem-se $\rho_M(V) = (\sigma_M(V), \delta_M(V))$ de forma que $M \cdot \text{PROD}(V) = \text{PROD}(\delta_M(V)) \cdot \sigma_m(V)$.*

Observação 5.3. Para cada $M \in Q_{n,v}$, cada uma das palavras $\mathcal{B}_j \in \mathcal{B}_M$ é não vazia, já que $\mathcal{B}_j$ é um ramo imediato de W_M. Pelo Teorema 4.8, $\sigma_M(V)$ e $\delta_M(V)$ são unicamente determinados por M e V. Pelo Teorema 5.5, a palavra $\delta_M(V)$ é não vazia. Logo as funções σ_M e δ_M estão bem definidas. Podemos concluir que $\mathcal{T}_{n,v}$ satisfaz as condições da Definição 5.1, isto é, um transdutor de Raney é um transdutor.

Lema 5.7. *Seja $x \in \mathcal{C}_2$. Seja $W_1, W_2, \cdots, W_k, \cdots$ uma sequência em $\{L, R\}^*$. Se para cada $k \geq 1$ existir um vetor $x_k \in \mathcal{C}_2$ tal que $x = \text{PROD}(W_1 W_2 \cdots W_k) \cdot x_k$, então x aceita a palavra infinita formada pela concatenação $W_1 W_2 W_3 \cdots \in \{L, R\}^{\mathbb{N}}$.*

Demonstração. Basta tomar a sequência x_k para $k \in \mathbb{Z}_+$, de forma que $x_0 = x$. Note que para todo $i \in \mathbb{N}$, temos que

$$\begin{aligned} x = \text{PROD}(W_1 W_2 \cdots W_{i-1}) \cdot x_{i-1} &= \text{PROD}(W_1 W_2 \cdots W_{i-1} W_i) \cdot x_i \\ \text{PROD}(W_1 W_2 \cdots W_{i-1}) \cdot x_{i-1} &= \text{PROD}(W_1 W_2 \cdots W_{i-1}) \cdot \text{PROD}(W_i) \cdot x_i \\ x_{i-1} &= \text{PROD}(W_i) \cdot x_i \end{aligned}$$

o que implica em x aceitar a palavra infinta $W_1 W_2 W_3 \cdots \in \{L, R\}^{\mathbb{N}}$. □

Teorema 5.8. *Seja $\mathcal{T}_{n,v}$ um transdutor de Raney. Para cada $M \in Q_{n,v}$, vale que Ψ_M possui a seguinte propriedade: Seja $S \in \{L, R\}^{\mathbb{N}}$. Se o vetor $x \in \mathcal{C}_2$ aceita a palavra infinita S, então o vetor $M \cdot x$ aceita a palavra $\Psi_M(S)$.*

Demonstração. Suponha que $x \in \mathcal{C}_2$ aceita a palavra infinita $S \in \{L, R\}^{\mathbb{N}}$ e $M \in Q_{n,v}$. Então temos que $S_0 = S$, $M_0 = M$, $V_0 = H(S_0, \mathcal{B}_{M_0}) = H(S, \mathcal{B}_M)$. Temos também que $S_0 = V_0 S_1$. Seja $k_0 = |V_0|$. Logo $k_0 \geq 1$. Seja $S = S^{(1)} \cdots S^{(k)} \cdots$. De x aceitar S, existe uma sequência $x^{(0)}, x^{(1)}, \cdots x^{(k)}, \cdots$ de vetores de $\mathcal{C}_2$ tais que $x^{(0)} = x$ e para todo $k \geq 0$, $x^{(k)} = S^{(k+1)} x^{(k+1)}$. Logo $\text{PROD}(S^{(1)} \cdots S^{(k_0)}) \cdot x^{(k_0)} = (\text{PROD}(V_0)) x^{(k_0)}$. Seja $x_1 = x^{(k_0)}$. Então $Mx = (M \cdot \text{PROD}(V_0)) \cdot x_1 = (\text{PROD}(\delta_{M_0}(V_0)) \cdot \sigma_{M_0}(V_0)) x_1 = (\text{PROD}(W_1) \cdot M_1) \cdot x_1$. Note que $M_1 \in Q_{n,v}$, $x_1 \in \mathcal{C}_2$ e $x_1 \sim S_1$.

Agora se $Mx = (\text{PROD}(W^{(1)} \cdots W^{(k)}) \cdot M^{(k)})x^{(k)}$, com $M^{(k)} \in Q_{n,v}$, $x^{(k)} \in \mathcal{C}_2$ e $x^{(k)} \sim S^{(k)}$. Seguindo um raciocínio análogo ao anterior, é possível mostrar que $M^{(k)}x^{(k)} = (\text{PROD}(W^{(1)} \cdots W^{(k+1)}) \cdot M^{(k+1)})x^{(k+1)}$, onde $M^{(k+1)} \in Q_{n,v}, x^{(k+1)} \in \mathcal{C}_2$ e $x^{(k+1)} \sim S^{(k+1)}$. Logo, por indução em k, temos que para qualquer $k \in \mathbb{N}$, existe um vetor $x^{(k)} \in \mathcal{C}_2$ e uma matriz $M^{(k)} \in Q_{n,v}$ tais que $Mx = (\text{PROD}(W^{(1)} \cdots W^{(k)})) \cdot M^{(k)}x^{(k)}$.

Do fato que $M^{(k)}x^{(k)} \in \mathcal{C}_2$, podemos aplicar o Lema 5.7 para concluir que Mx aceita a palavra $W^{(1)}W^{(2)} \cdots = \Phi_M(S)$. □

5.3 EXEMPLOS DE TRANSDUTORES DE RANEY

Exemplo 10. Dado $n \in \mathbb{N}$ e um irracional $x = [x_0; x_1, x_2, x_3, x_4, \cdots] \in \mathbb{R}^+$, temos que pelo isomorfismo definido pela Proposição 2.7 existe um vetor $X = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathcal{C}_2$ tal que $\frac{a}{b} = x$. Em contrapartida, um resultado imediato do Teorema 4.17 garante que X aceita a palavra $R^{x_0}L^{x_1}R^{x_2}L^{x_3}R^{x_4} \cdots \in \{L, R\}^{\mathbb{N}}$.

Caso estejamos interessados em descobrir a representação por fração continuada de nx, podemos utilizar o isomorfismo e calcular $NX \in \mathcal{C}_2$, onde $N = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, uma vez que pelo isomorfismo Φ da Proposição 2.9, vale $nx = \dfrac{nx + 0}{0x + 1} = \Phi(N)(x)$. Em particular, se $n \in \mathbb{N}$ é primo ou se escreve como produto de primos com potência no máximo 1, podemos construir e utilizar o transdutor de Raney $\mathcal{T}_{n,1}$ para encontrar NX.

Vamos analisar o caso em que $n = 2$. Note que $Q_{2,1} = \mathcal{DB}_2 = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \right\}$. Para simplificar, chamaremos de $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ e $A' = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. As palavras geradoras de $r(A) = \begin{pmatrix} 1-0 \\ 2-0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ e $r(A') = \begin{pmatrix} 2-0 \\ 1-0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ são $W_A = L$ e $W_{A'} = R$, respectivamente. Temos então que o conjunto dos ramos imediatos de W_A é $\mathcal{B}_A = \{R, LR, LL\}$ e o conjunto dos ramos imediatos de W_B é $\mathcal{B}_{A'} = \{L, RL, RR\}$. O Teorema 2.21 garante que $\mathcal{B}_A$ e $\mathcal{B}_{A'}$ são bases de uma palavra infinita.

O Teorema 5.5 garante que para cada palavra $B \in \mathcal{B}_A$ existe uma única palavra não-vazia $W \in \{L, R\}^*$ e uma única matriz $U \in \mathcal{DB}_2$ tais que $A \cdot \text{PROD}(B) = \text{PROD}(W) \cdot U$. Analogamente para cada $B \in \mathcal{B}_{A'}$, existe uma única palavra não vazia $W \in \{L, R\}^*$ e uma única matriz $U \in \mathcal{DB}_2$ tais que $A' \cdot \text{PROD}(B) = \text{PROD}(W) \cdot U$.

Com efeito, podemos calcular W e U, obtendo assim as igualdades abaixo:

$$A\mathbf{R} = \mathbf{R}^2A, \quad A\mathbf{LR} = \mathbf{RL}A', \quad A\mathbf{L}^2 = \mathbf{L}A;$$
$$A'\mathbf{L} = \mathbf{L}^2A', \quad A'\mathbf{RL} = \mathbf{LR}A, \quad A'\mathbf{R}^2 = \mathbf{R}A'.$$

Estas, por sua vez, são as bases da função ρ_A e $\rho_{A'}$, sendo que as três primeiras nos

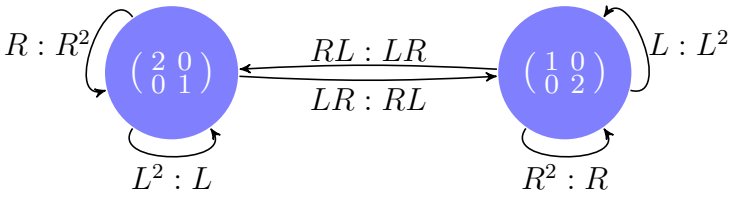

Figura 5.2: Diagrama do transdutor de Raney $\mathcal{T}_{2,1}$.

fornece a regra de $\rho_A : \mathcal{B}_A \to \{L, R\}^* \times \mathcal{DB}_2$, já que $\rho_A(R) = (R^2, A)$, $\rho_A(LR) = (RL, A')$ e $\rho_A(L^2) = (L, A)$. As três últimas equações fornecem a regra de $\rho_{A'} : \mathcal{B}_{A'} \to \{L, R\}^* \times \mathcal{DB}_2$, pois $\rho_{A'}(L) = (L^2, A')$, $\rho_{A'}(RL) = (LR, A)$ e $\rho_{A'}(R^2) = (R, A')$.

É possível construir um diagrama para representar o transdutor $\mathcal{T}_{2,1}$: os círculos em azul representam os estados de $\mathcal{DB}_2 = \{A, A'\}$ e para cada estado $q \in \{A, A'\}$, cada flecha que sai de q representa a imagem de ρ_q por algum elemento de $\mathcal{B}_q$ (veja Figura 5.2).

Por exemplo, tome a razão aurea $\phi = \dfrac{1+\sqrt{5}}{2} = [1; 1, 1, 1, 1, 1, \cdots] = [1; \overline{1}]$. O Teorema 4.17 garante que palavra infinita $S = RLRLRLRL\cdots \in \{L, R\}^{\mathbb{N}}$ é tal que o vetor $\begin{pmatrix} \phi \\ 1 \end{pmatrix} \in \mathcal{C}_2$ a aceita. Vamos encontrar uma representação por frações continuadas do número $2\phi = 1 + \sqrt{5}$.

O teorema 5.8 garante que o vetor $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \phi \\ 1 \end{pmatrix} = \begin{pmatrix} 2\phi \\ 1 \end{pmatrix}$ aceita a palavra infinita $\Psi_A(S)$. Vamos calcula-la.

Neste caso, seguindo a Definição 5.3, temos que $S_0 = S = RLRLRLRLRLRL\cdots$, o estado inicial é $q_0 = A$, a palavra da base $\mathcal{B}_A$ que é prefixo de S é $V_0 = H(S_0, \beta_{q_0}) = H(S, \mathcal{B}_A) = R$.

Logo , no estado A, a primeira palavra de S que $\mathcal{T}_{2,1}$ "lê" é $V_0 = R$. Assim que é "lida", do fato que $\rho_A(R) = (R^2, A)$, temos que $W_1 = \delta_{q_0}(V_0) = \delta_A(R) = R^2$ e $q_1 = \sigma_{q_0}(V_0) = \sigma_A(R) = A$, o que na prática significa que $\mathcal{T}_{2,1}$ "escreve" $W_1 = R^2$ e permanece no estado A.

Agora temos que $S_1 = S_0 \backslash V_0 = S \backslash R = LRLRLR\cdots$ e a palavra da base $\mathcal{B}_A$ que é prefixo de $S_1 = LRLRLRLR\cdots$ é $V_1 = H(S_1, \beta_{q_1}) = H(S_1, \mathcal{B}_A) = LR$. Já que $\rho_A(LR) = (RL, A')$, temos que $W_2 = \delta_{q_1}(V_1) = \delta_A(LR) = RL$ e $q_2 = \sigma_{q_1}(V_1) = \sigma_A(LR) = A'$. Ou seja, $\mathcal{T}_{2,1}$ "lê" $V_1 = LR$, "escreve" $W_2 = RL$ e muda para o estado A'.

Continuando os passos, temos que $S_2 = S_1 \backslash V_1 = S_1 \backslash LR = LRLRLR\cdots$, $V_2 = H(S_2, \mathcal{B}_{A'}) = L$, logo temos que no estado A', $\mathcal{T}_{2,1}$ "lê" L. De $\rho_{A'}(L) = (L^2, A')$, vale que $W_3 = L^2$ e $q_3 = A'$, em outras palavras, $\mathcal{T}_{2,1}$ "escreve" L^2 e continua no estado A'.

Por fim, repetindo os passos, podemos verificar que $S_3 = S_2 \backslash V_2 = RLRLRL\cdots$, $V_3 = H(S_3, \mathcal{B}_{A'}) = RL$, $\rho_{A'}(RL) = (LR, A)$, $W_4 = LR$ e $q_4 = A$. Note que a partir deste passo, o transdutor começará a se repetir, uma vez que $q_4 = A = q_0$ e a $S_4 = S_3 \backslash V_3 = S_3 \backslash RL = RLRLRL\cdots = S_0$. Logo, para todo $i \in \mathbb{Z}^+$, $S_{4+i} = S_i$, $V_{4+i} = V_i$, $q_{4+i} = q_i$ e $W_{5+i} = W_{1+i}$.

Podemos concluir que $\Psi_A(U) = W_1W_2W_3W_4W_5W_6\cdots = W_1W_2W_3W_4W_1W_2\cdots =$

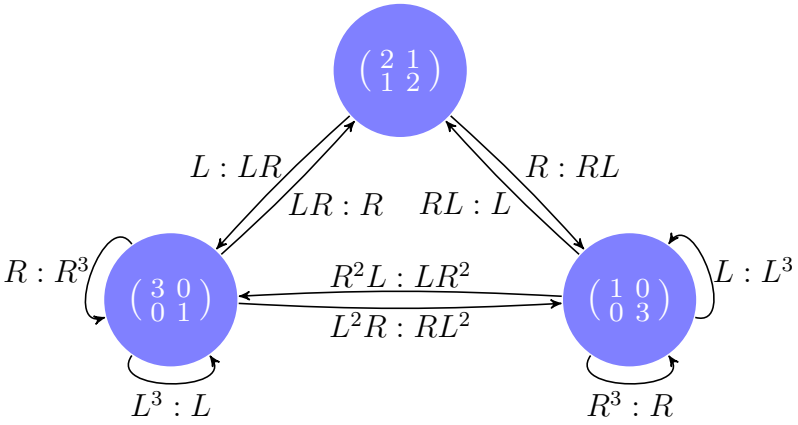

Figura 5.3: Diagrama do Transdutor de Raney $\mathfrak{T}_{3,1}$.

$R^2RLL^2LRR^2RL\cdots = R^3L^4R^4L^4R^4L^4R^4\cdots$, o que implica na representação de $1+\sqrt{5}$ por frações continuadas ser $[3;4,4,4,4,4,4,\cdots] = [3;\overline{4}]$.

Exemplo 11. Seja $e = \lim\limits_{n\to\infty}\left(1+\dfrac{1}{n}\right)^n \approx 2,718281828$. Escrevendo e na forma de fração continuada, temos $e = [2;1,2,1,1,4,1,1,6,1,1,8,1,\cdots] = [2;\overline{1,2n,1}]$, que é uma fração continuada polinomial periódica. Sabe-se que o número e é transcendente, e pertence à classe dos *números de Hurwitz* [5].

Vamos determinar a fração continuada do número $a = \dfrac{2e+1}{1+2e}$. Podemos escrever a como a imagem de e pela transformação de Möbius associada à matriz $M = \begin{pmatrix}2&1\\1&2\end{pmatrix}$, ou seja $a = \Phi(M)(e)$. Pelo Teorema 4.17, o vetor $x = \begin{pmatrix}e\\1\end{pmatrix} \in \mathcal{C}_2$ aceita apenas a palavra $S = R^2L^1R^2L^1R^1L^4R^1L^1R^6L^1R^1L^8R^1\cdots$. Note que $M \in \mathcal{DB}_3$ e o máximo divisor comum dos elementos de M é 1, logo, $M \in Q_{3,1}$.

Vamos construir o transdutor de Raney $\mathfrak{T}_{3,1} = \{\{L,R\}, Q_{3,1}, \mathcal{F}_{3,1}\}$. Temos que $Q_{3,1} = \left\{\underbrace{\begin{pmatrix}2&1\\1&2\end{pmatrix}}_{A}, \underbrace{\begin{pmatrix}3&0\\0&1\end{pmatrix}}_{B}, \underbrace{\begin{pmatrix}1&0\\0&3\end{pmatrix}}_{B}\right\} = \mathcal{DB}_3$. A família $\mathcal{F}_{3,1}$ pode ser representada por um diagrama conforme a Figura 5.3.

Com efeito, pelo Teorema 5.8, o vetor $Mx = \begin{pmatrix}2&1\\1&2\end{pmatrix}\cdot\begin{pmatrix}e\\1\end{pmatrix} = \begin{pmatrix}2e+1\\e+2\end{pmatrix}$ aceita a palava $\Psi_M(S)$.

Aplicando Ψ_M em S, tem-se

$$\begin{aligned}\Psi_M(S) &= \Psi_M(R^2L^1R^2L^1R^1L^4R^1L^1R^6L^1R^1L^8R^1\cdots)\\ &= \Psi_M((R)(RL)(R)(RL)(R)(L)(L)(L)(L)(RL)(R^3)(R^2L)(R)(L^3)(L^3)(L^2R)\cdots)\\ &= \delta_A(R)\delta_C(RL)\delta_A(R)\delta_C(RL)\delta_A(R)\delta_C(L)^4\delta_C(RL)\delta_A(R)\delta_C(R^3)\delta_C(R^2L)\\ &\quad\cdot\delta_B(R)\delta_B(L^3)^2\delta_B(L^2R)\cdots\\ &= (RL)(L)(RL)(L)(RL)(L^3)(L^3)(L^3)(L^3)(L)(RL)(R)(LR^2)(R^3)(L)(L)(RL^2)\cdots\\ &= RL^2RL^2RL^{14}RLRLR^5L^2RL^2\cdots\end{aligned}$$

Assim, a fração continuada do número $\dfrac{2e+1}{e+2}$ é igual a $[1,2,1,2,1,14,1,1,1,5,2,1\cdots]$. Perron provou que este é também um número de Hurwitz [5], no sentido de que existem polinômios $q_1, q_2, \cdots, q_n$ tais que

$$\frac{2e+1}{e+2} = [a_0; a_1, \cdots, a_k, \overline{q_1(j), \cdots, q_n(j)}]_{j=0}^{\infty}.$$

Exemplo 12. Vamos encontrar agora a representação por frações continuadas do número real $\beta = \dfrac{-5\cdot\sqrt{5}+6}{2\cdot\sqrt{5}-2}$. Escrevendo β como a imagem de $\sqrt{5}$ pela transformação de Möbius associada à matriz $M = \begin{pmatrix}-5 & 6\\ 2 & -2\end{pmatrix}$, como $\det(M) = -2$, é necessário tomarmos alguns passos para encontrar um problema que seja equivalente e com uma matriz $\overline{M} \in \mathcal{DB}_2$.

Note que $\begin{pmatrix}-5 & 6\\ 2 & -2\end{pmatrix}\cdot\begin{pmatrix}\sqrt{5}\\ 1\end{pmatrix} = \begin{pmatrix}6 & -5\\ -2 & 2\end{pmatrix}\cdot\begin{pmatrix}1\\ \sqrt{5}\end{pmatrix}$, ou seja, podemos reescrever $\beta = \dfrac{6\cdot\dfrac{1}{\sqrt{5}}-5}{-2\cdot\dfrac{1}{\sqrt{5}}+2}$ como imagem de $\dfrac{1}{\sqrt{5}}$ pela transformação de Möbius associada à matriz $\begin{pmatrix}6 & -5\\ -2 & 2\end{pmatrix}$, cujo determinante é igual a 2.

Agora basta encontrar um problema equivalente com uma matriz $\overline{M}$ que possui as entradas todas não negativas. Note que $\begin{pmatrix}1\\ \sqrt{5}\end{pmatrix}$ aceita apenas a palavra $L^2R^4L^4R^4L^4\cdots$, logo

$$\begin{pmatrix}6 & -5\\ -2 & 2\end{pmatrix}\cdot\begin{pmatrix}1\\ \sqrt{5}\end{pmatrix} = \begin{pmatrix}6 & -5\\ -2 & 2\end{pmatrix}\cdot\mathbf{L}^2\cdot\begin{pmatrix}1\\ \sqrt{5}-2\end{pmatrix} = \begin{pmatrix}-4 & -5\\ 2 & 2\end{pmatrix}\cdot\begin{pmatrix}1\\ \sqrt{5}-2\end{pmatrix}.$$

Por fim, note que $\begin{pmatrix}-4 & -5\\ 2 & 2\end{pmatrix}$ pode ser reescrita por $\mathbf{R}^{-3}\cdot\begin{pmatrix}2 & 1\\ 2 & 2\end{pmatrix}$, com efeito, tem-

se como $\beta = \dfrac{-5\cdot\sqrt{5}+6}{2\cdot\sqrt{5}-2} = \dfrac{-4\cdot\dfrac{1}{\sqrt{5}-2}-5}{2\cdot\dfrac{1}{\sqrt{5}-2}+2}$, vale que $\beta+3 = \dfrac{-4\cdot\dfrac{1}{\sqrt{5}-2}-5}{2\cdot\dfrac{1}{\sqrt{5}-2}+2}+3 = \dfrac{-4\cdot\dfrac{1}{\sqrt{5}-2}-5}{2\cdot\dfrac{1}{\sqrt{5}-2}+2}+3\cdot\dfrac{2\cdot\dfrac{1}{\sqrt{5}-2}+2}{2\cdot\dfrac{1}{\sqrt{5}-2}+2} = \dfrac{2\cdot\dfrac{1}{\sqrt{5}-2}+1}{2\cdot\dfrac{1}{\sqrt{5}-2}+2}$, o que significa que podemos escrever $\beta+3$ como a imagem de $\dfrac{1}{\sqrt{5}-2}$ pela transformação de Möbius associada à matriz $\begin{pmatrix}2&1\\2&2\end{pmatrix}$. Por $\begin{pmatrix}2&1\\2&2\end{pmatrix} = \mathbf{L}\cdot\mathbf{R}\cdot\begin{pmatrix}2&0\\0&1\end{pmatrix}$, vale que $\begin{pmatrix}\beta\\1\end{pmatrix} \sim \mathbf{R}^{-3}\cdot\mathbf{L}\cdot\mathbf{R}\cdot\begin{pmatrix}2&0\\0&1\end{pmatrix}\cdot\begin{pmatrix}1\\\sqrt{5}-2\end{pmatrix}$, ou seja, a matriz $\overline{M} = \begin{pmatrix}2&0\\0&1\end{pmatrix}$ é a matriz procurada. Do vetor $\begin{pmatrix}1\\\sqrt{5}-2\end{pmatrix}$ aceitar apenas a palavra $R^4L^4R^4L^4\cdots$ e pelo Transdutor de Raney $\Upsilon_{2,1}$, temos que $\begin{pmatrix}2&0\\0&1\end{pmatrix}\cdot\begin{pmatrix}1\\\sqrt{5}-2\end{pmatrix}$ aceita apenas a palavra $\Psi_{\overline{M}}(R^4L^4R^4L^4\cdots) = \delta_{\overline{M}}(R^2)\delta_{\overline{M}}(R^2)\delta_{\overline{M}}(L^2)\delta_{\overline{M}}(L^2)\cdots = R^8L^2R^8L^2R^8L^2\cdots$.

Podemos concluir que $\beta+3$ aceita apenas a palavra $LR^9L^2R^8L^2R^8L^2R^8L^2\cdots$, em outras palavras, $\beta+3 = [0;1,9,2,\overline{8,2}]$. Isso significa que a representação por frações continuadas de β é $[-3;1,9,2,\overline{8,2}]$.

REFERÊNCIAS

Referências Bibliográficas

[1] HALL, M. On the sum and product of continued fractions. *Ann. Math. 48* (1947), 966–993.

[2] HOPCROFT, J. E., MOTWANI, R., AND ULLMAN, J. D. *Introduction to automata theory, Languages, and Computation*. Addison-Wesley, Reading, MA, 2001.

[3] MARTINEZ, F. E. B., DE A. MOREIRA, C. G. T., SALDANHA, N. C., AND TENGAN, E. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA, Rio de Janeiro, RJ, 2018.

[4] RANEY, G. N. On continued fractions and finite automata. *Am. Math. Monthly 68* (1961), 552–557.

[5] STAMBUL, P. A generalization of Perron's theorem about hurwitzian numbers. *Acta Arith. 80* (1997), 141–148.

[6] TAO, R. *Finite Automata and Application to Cryptography*. Springer, Switzerland, 2008.