K-SUBCONJUNTOS LIMITADOS

DE UM MONÓIDE LIVRE

ARNALDO MANDEL

DISSERTAÇÃO APRESENTADA AO

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

DA

UNIVERSIDADE DE SÃO PAULO

PARA OBTENÇÃO DO GRAU DE MESTRE

EM

MATEMÁTICA APLICADA

ORIENTADOR:

PROF. DR. IMRE SIMON

- SÃO PAULO, MAIO DE 1976 -

Aos meus pais

e à floresta

ÍNDICE

PRÓLOGO iv

ABSTRACT ix

CAPÍTULO I - CONCEITOS BÁSICOS E NOTAÇÃO 1

1. Algumas Convenções 1
2. Monóides 3
3. Monóides Livres 4
4. Semianéis 6
5. K-Subconjuntos 9

CAPÍTULO II - CONJUNTOS E K-SUBCONJUNTOS RECONHECÍVEIS 14

1. Σ-Autômatos e Conjuntos Reconhecíveis (Resumo) . . 14
   1.A. Forma Matricial de um Autômato 21
2. K-Subconjuntos Reconhecíveis 22
3. Operações com K-Subconjuntos Reconhecíveis 32

CAPÍTULO III - O CASO EM QUE K É UM CORPO 42

1. Idéias Gerais 42
2. O Teorema da Igualdade 43
3. O Teorema da Estrela 45
4. Matrizes de Hankel 50

CAPÍTULO IV - K-SUBCONJUNTOS LIMITADOS 63

1. Introdução 63
2. O monóide sintático de um K-Subconjunto de Σ^* . . . 64
3. Semianéis Limitadores 72
4. O caso K = N 80
   4.A. Autômatos Conexos 85
   4.B. O Teorema, Versão Combinatória 89
   4.C. O Teorema, Versão Algébrica 101
   4.D. Possibilidades de Extensão 105
   4.E. Construção de Exemplos 107
5. Subconjuntos Quase-Periódicos 111

BIBLIOGRAFIA 123

ÍNDICE DE DEFINIÇÕES 128

PRÓLOGO

A Teoria dos Autômatos Finitos surgiu na década de 50 como uma tentativa de criar um modelo matemático para o estudo do pensamento humano e ao mesmo tempo evidenciar certas estruturas úteis à construção de computadores.

Posteriormente, com a introdução por Chomsky das gramáticas e linguagens formais, a Teoria dos Autômatos foi parcialmente absorvida por estas. A partir daí, duas tendências distintas apareceram para o desenvolvimento da teoria:

A primeira, essencialmente algébrica, em que propriedades dos autômatos e conjuntos por eles reconhecidos eram relacionadas com propriedades de semigrupos a eles associados. Resultados fortes sobre semigrupos foram obtidos paralelamente.

A outra, dentro da Teoria de Linguagens Formais, onde os autômatos foram substituídos por estruturas mais sofisticadas de forma a se poder definir famílias maiores de linguagens. Dentro desse estudo, surgiu o método das séries formais, onde, em princípio, se associava uma multiplicidade a cada palavra produzida por uma gramática. Os passos iniciais neste sentido foram dados por Chomsky e Schutzenberger [CS1], [S3] e [S4]. Esse método enriqueceu a teoria com métodos algébricos que generalizaram algumas propriedades de operações com subconjuntos de um conjunto. Além disso, resultados anteriores foram generalizados e assuntos até então intratáveis tiveram campo aberto para se desenvolver. Um elemento unificador de vários desses resultados foi a introdução da multiplicidade em semianéis, e de K-Σ-autômatos como

a generalização natural de autômatos.

O primeiro tratamento sistemático dessa teoria na forma de livro é a obra recente de S. Eilenberg, "Automata, Languages and Machines" Vol. A [E1] que é a referência padrão no nosso trabalho. Muito do que aqui fizemos foi sugerido a partir da leitura desse livro e a ele nos referimos constantemente no texto. As citações são tantas que não colocamos em geral o indicador [E1], ficando subentendido que as referências a Eilenberg tem por fonte o livro citado.

O conteúdo e disposição do trabalho são o seguinte:

No *Capítulo* I são introduzidos os conceitos e notações básicos. Houve a preocupação de fixá-los, pois não existe ainda uma padronização neste sentido no campo, e além disso, isto permite a leitura do texto sem ter que recorrer a outras fontes para esse tipo de detalhe. Nos omitimos na definição e notação em objetos de presença usual em Matemática, por seu uso estar já padronizado. As três primeiras secções são necessárias por todo o texto. As duas últimas são referidas a partir de meados da secção II.2.

No *Capítulo* II são apresentados os fatos básicos da Teoria dos Autômatos Finitos e um tratamento extensivo das séries formais (também chamadas K-subconjuntos) reconhecíveis. O tratamento dado é basicamente o de Eilenberg, com pequenas diferenças devidas a preferirmos a apresentação matricial de K-Σ-autômatos e a não nos restringirmos a semianéis comutativos. É importante notar que um autômato finito (Σ-autômato) é uma abstração de algoritmos que utilizam uma memória fixa e instruções de desvio somente. A passagem para K-Σ-autômatos se faz permitindo, dentro das instruções, a execução de certas operações aritméticas em quantidade limi

tada.

O *Capítulo* III particulariza os K-subconjuntos para o caso em que o semianel é um corpo. Três resultados são apresentados:

— O Teorema da Igualdade, de Eilenberg - Schutzenberger, que permite a decisão algorítmica de certas questões concernentes a K-Σ-autômatos, fundamentalmente, a decisão quanto à igualdade do comportamento de dois K-Σ-autômatos dados.

— O Teorema da Estrela, de Jacob, que generaliza uma propriedade bem conhecida de autômatos finitos, dando informação sobre o suporte de K-subconjuntos reconhecíveis. Apresentamos uma demonstração consideravelmente mais simples que a original.

— O Teorema de Fliess sobre matrizes de Hankel, que dá uma caracterização algébrica de K-subconjuntos reconhecíveis, com importantes consequências. Esse resultado permitiu-nos construir um exemplo que prova uma conjectura de Eilenberg; além disso, combinando-o com o Teorema da Igualdade, obteremos um resultado que encontrará aplicação no Capítulo IV.

O *Capítulo* IV consiste essencialmente de resultados novos. A partir da relevância na teoria de N-subconjuntos e M-subconjuntos reconhecíveis de imagem finita e da tentativa de aplicar os métodos algébricos da Teoria de Autômatos Finitos, fomos levados a definir K-subconjuntos limitados, aqueles cujos monóides sintático é finito. Várias caracterizações e propriedades desses K-subconjuntos são apresentadas. Uma destas é a de que todo K-subconjunto limitado é reconhecível e de imagem finita. Como a recíproca vale para alguns semianéis particulares, tentamos verificar se essa era uma propriedade de semianéis. Não conseguimos uma resposta para isso, e por isto estudamos a classe dos semianéis com essa propriedade ("limitadores"), a qual se mostrou bem

ampla. Na secção 4 deste capítulo encontra-se a parte mais importante desta dissertação. Alí estudamos a possibilidade de decidir efetivamente se um N-subconjunto é limitado. Esse problema é reduzido ao de decidir se um conjunto finito de matrizes quadradas sobre N geram um monóide multiplicativo finito. Isso nos levou a caracterizar efetivamente matrizes periódicas com coeficientes em N e também a caracterizar submonóides finitos de $M_n(N)$. Estas caracterizações foram conseguidas por dois métodos essencialmente diferentes, um inteiramente combinatório e outro puramente algébrico. Obtivemos também uma forma canônica para matrizes periódicas em $M_n(N)$, bem como extensões dos resultados para semianéis graduados e corpos. Esses resultados foram obtidos com a forte colaboração do Prof. I. Simon. Por fim, a secção 5 apresenta os subconjuntos quase-periódicos de um monóide livre, isto é, aqueles que satisfazem $L^* = (1 \cup L)^n$ para algum $n \in N$. Alí enquadramos um trabalho isolado de I. Simon dentro da teoria que desenvolvemos. O problema de decidir se um Σ-autômato tem comportamento quase-periódico é reduzido ao de decidir se o monóide de um M-Σ-autômato é finito. Alguns resultados parciais são apresentados, mas os métodos da secção 4 não são suficientemente fortes para obter resultados análogos na 5, e assim, o problema de decidir se um conjunto é quase-periódico continua em aberto.

Os capítulos são denotados por números romanos. As secções e dentro de cada secção os teoremas, proposições, etc., são numerados sequencialmente. Para referências, por exemplo, a Proposição 4 da secção II.2 será referido pelo número 4 dentro da mesma secção, por 2.4 no resto do capítulo II e como Proposição II.2.4 em outros capítulos.

Ao final do trabalho encontram-se a bibliografia, onde procuramos colocar as fontes dos principais resultados que apresentamos e o índice de definições.

Agora cumpre agradecer à colaboração dada por algumas pessoas, e aqui me permitirei um tom mais pessoal.

Ao Professor Imre Simon, cuja orientação tem vindo durante toda minha formação acadêmica, dirigem-se os principais agradecimentos. Na realização deste trabalho sua colaboração foi intensiva, e, em muitos lugares onde se lê o formal "nós", seu significado é "Imre e eu", a não ser nas partes (que espero não hajam) onde ocorrem eventuais enganos.

Agradeço ao Professor Valdemar Waingort Setzer por ter dado o primeiro empurrão no meu encaminhamento para a área de Matemática Discreta.

Aos inúmeros amigos e colegas que em horas de aperto vieram dizer "não esquenta que tudo vai dar certo", meus reconhecimentos.

Agradeço ao Departamento de Matemática Aplicada pelas facilidades técnicas na execução deste trabalho, ao sr. João Baptista Esteves de Oliveira pela eficiente e ótima datilografia e ao sr. Armando Garcia Segura pelo esmerado serviço de impressão.

São Paulo, 17 de maio de 1976

A.M.

ABSTRACT.

Recognizable K-subsets of Σ^* are introduced and studied by means of K-Σ-automata along the lines of Eilenberg[E1]. This is done in chapters I and II.

Chapter III is dedicated to the special case when the coefficient semiring K is a field. Eilenberg-Schutzenberger's Equality Theorem [E1], Jacob's Star Theorem [J1] and Fliess'Theorem on Hankel Matrices [F2] are presented.We give a simplified proof of the Star Theorem, whichis a generalization of the "Pumping Lemma" for recognizable K-subsets. Based on Fliess'Theorem, we prove Eilenberg's conjecture that $Rec_N\Sigma$ is not closed by min and max, where $\min(A,B) = \sum \min(xA,xB)\underline{x}$ and $\max(A,B) = \sum \max(xA,xB)\underline{x}$. A consequence of Fliess'Theorem is the existence of reduced automata with a given behavior in $Rec_K\Sigma$. Using the Equality Theorem we present an effective construction of such a reduced automaton.

The last chapter introduces the syntatic monoid of a K-subset of Σ^*. Limited K-subsets are defined as those whose sintactic monoid is finite, and some properties of these are studied. In section IV.3 we investigate semirings for which any recognizable K-subset of finite image is limited. It is shown that these include any subsemiring of a field, and any finite semiring has this property. We leave open the question wheter all semirings have the above property.In section IV.4 limited N-subsets are studied. We show that it is decidable whether an N-Σ-automaton has a limited behavior.This is a consequence of our main theorem caracterizing effectively

finite submonoids of $M_n(N)$ generated by a finite set. Two entirely different proofs are presented: the first one, combinatorial, leading to a canonical form for periodic elements of $M_n(N)$ and using Ramsey's Theorem; the second, algebraic, uses McNaughton-Zalcstein's Theorem which answers Burnside's Problem for semigroups of matrices over a field. Each proof leads to a different algorithm and generalizes to a different direction. In section IV.5, quasi-periodic subsets of Σ^* are defined as those for wich $(1 \cup L)^n = L^*$ for some integer n, and the possibility of effectively deciding whether a given subset is quasi-periodic is studied by means of M-Σ-automata and limited M-subsets of Σ^*, as introduced by Simon [S6]. Partial results are presented.

Our main result can be stated as follows:

The semiring N_2 has as carrier $\{0,1,2\}$, sum $a \oplus_2 b = \min\{a+b,2\}$, product $a \otimes_2 b = \min\{ab,2\}$, defined in terms of the operations and order of N. Denote by ψ_2 the monoid epimorfism $\psi_2 : M_n(N) \to M_n(N_2)$ (multiplicative monoids) given by: $(A\psi_2)_{ij} = \min(A_{ij},2)$. An element m of a monoid is idempotent if $m = m^2$ and 2-potent if $m^2 = m^3$.

THEOREM 4.1' - Given a finite subset $X \subseteq M_n(N)$ the submonoid X^* of $M_n(N)$ generated by X is finite if and only if every idempotent of $X^*\psi_2$ is 2-potent as an element of $M_n(N)$.

A consequence of our combinatorial proof is that, given positive integers k, n, there only exists a finite number of finite submonoids of $M_n(N)$, generated by at most k elements.

Nome é nome; não precisa ter relação com o "nomado". *Quindim!*... Como sempre fui a botadeira de nomes lá do sítio, resolvo batizar o rinoceronte assim — e pronto!

Monteiro Lobato
"Emília no País da Gramática"

CAPÍTULO I

CONCEITOS BÁSICOS E NOTAÇÃO

1.1 - ALGUMAS CONVENÇÕES

No decorrer deste texto, não faremos distinção notacional entre um conjunto unitário e seu único elemento. Assim, geralmente escreveremos x no lugar de {x}, e consideraremos, para efeito de notação, $X \subseteq P(x)$, para todo conjunto X.

Dados conjuntos X, Y e uma função $f: X \to Y$, se $x \in X$, a imagem de x por f será denotada xf. Se $f: X \to Y$, $g: Y \to Z$, são funções, a composta $fg: X \to Z$ é definida, para todo $x \in X$, por:

$$x(fg) = (xf)g,$$

sendo, portanto desnecessário o uso de parênteses.

Uma *relação* $R: X \to Y$ é uma função de $P(X)$ em $P(Y)$ satisfazendo, para todo $A \subseteq X$:

$$AR = \bigcup_{x \in A} xR.$$

Claramente, R fica determinada pela sua restrição a X. Se $y \in xR$, escrevemos também xRy, que é a notação mais usada. Uma função $f: X \to Y$ pode ser naturalmente estendida a uma relação de X em Y. Também nesse caso, não faremos distinção entre esses dois objetos, e consideraremos funções co

mo relações particulares, em que a imagem de cada conjunto unitário é unitária.

Se $R: X \to Y$ é uma relação, a relação inversa $R^{-1}: Y \to X$ é definida, para cada $y \in Y$ por:

$$yR^{-1} = \{x \in X \mid xRy\}.$$

O conjunto de todas as relações de um conjunto X em si mesmo é denotado por Rel(X). A relação $1_X \in Rel(X)$ é definida, para todo x por: $x1_X = x$.

Se $R,S: X \to Y$ são relações, colocamos $R \subset S$ se para todo $x \in X$, $xR \subset xS$.

Uma *função parcial* é uma relação em que a imagem de cada conjunto unitário é um conjunto unitário ou vazio. Composição de relações está definida e é denotada como composição de funções.

Definições e propriedades gerais sobre relações de equivalência e relações de ordem podem ser encontrados no livro de Jacy Monteiro [M3].

Em particular, se $\sim$ é uma relação de equivalência sobre um conjunto X, denotaremos por $X/\sim$ o conjunto das classes de equivalência, também chamado *conjunto quociente*. Se $x \in X$, [x] denota a classe de equivalência de x (em geral, ficará subentendida qual a relação). A aplicação $\pi: X \to X/\sim$ dada por $x\pi = [x]$ é chamada *projeção canônica*. O *índice* de uma relação de equivalência é a cardinalidade do conjunto quociente.

A cardinalidade de um conjunto X será denotada $|X|$. O símbolo $|\ |$ será usado com outros significados, sendo que o contexto não deixará dúvidas.

Os símbolos N, Z, Q, R, C denotam os conjuntos dos números naturais, inteiros, racionais, reais e complexos.

Se n é um inteiro positivo, n denota o conjunto

$$\{1,2,\ldots,n\}.$$

A expressão "sse" será usada como abreviatura de "se e somente se".

1.2 - MONÓIDES

Um *semigrupo* é um conjunto não vazio dotado de uma operação binária associativa. Um *monóide* é um semigrupo em que existe um elemento neutro, denotado em geral por 1. Fatos em geral sobre monóides e semigrupos podem ser encontrados em Clifford & Preston [CP2] e Arbib [A1]. Apresentaremos aqui os resultados e conceitos que utilizaremos normalmente.

Dados monóides M_1 e M_2, um *morfismo* de M_1 em M_2 é uma função $\phi: M_1 \to M_2$ satisfazendo

a) $1\phi = 1$,

b) $\forall m,m' \in M_1$, $(mm')\phi = (m\phi)(m'\phi)$.

Um morfismo será denominado *monomorfismo*, *epimorfismo* ou *isomorfismo* se for respectivamente, uma função injetora, sobrejetora ou bijetora.

No que se segue, M é suposto um monóide.

Um subconjunto de M é um submonóide se for fechado em relação à operação de M e contiver o elemento neutro.

Se $A,B \subseteq M$, $AB = \{ab \mid a \in A, b \in B\}$. Isso transforma $P(M)$ em um monóide, com elemento neutro $\{1\}$. Se $A \subseteq M$, definimos $A^0 = \{1\}$, $A^n = A.A^{n-1}$, para $n > 0$. Em particular, se $m \in M$, está definido m^n, para todo $n \in N$.

Uma relação de equivalência ~ sobre M é uma *congruência* sse para todo $x,y,m \in M$, $x \sim y$ implica $mx \sim my$ e $xm \sim ym$. Neste caso, $M/\sim$ é um monóide com a operação $[x]\cdot[y] = [xy]$, denominado *monóide quociente* de M por ~ e a projeção canônica é um epimorfismo.

Se N é um monóide e $\phi: M \to N$ é um epimorfismo, a relação $\phi\phi^{-1} \in Rel(M)$ é uma congruência e $M/\phi\phi^{-1}$ é isomorfo a N. Se R,S são congruências sobre M, $R \subset S$ e $r: M \to M/R$, $s: M \to M/S$ são as projeções canônicas, então existe um epimorfismo $\phi: M/R \to M/S$ tal que $r\phi = s$. Em particular:

PROPRIEDADE 2.1 - Seja $\phi: M \to N$ um epimorfismo de monóides, $\sim$ uma congruência sobre M e suponhamos que para todo x,y em M, $x\phi = y\phi$ implica $x \sim y$. Então existe um epimorfismo $\psi: N \to M/\sim$ tal que o epimorfismo $\phi\psi: M \to M/\sim$ é a projeção canônica.

Dado um conjunto $A \subseteq M$, a relação $\sim_A$, dada por:

$x \sim_A y \iff$ para todo $u,v \in M$, $uxv \in A$ sse $uyv \in A$,

é uma congruência, denominada *congruência sintática* de A. O monóide quociente $M/\sim_A$ é denominado *monóide sintático* de A.

Ainda com $A \subset M$, o submonóide gerado por A, denotado A^*, é a intersecção de todos os submonóides de M contendo A. É claro que $A^* = \bigcup_{n \geq 0} A^n$. Em particular, $\emptyset^* = 1^* = 1$, e, para todo $A \subset M$, $(A^*)^* = A^*$; aliás, $A = A^*$ sse A for um submonóide de M. Também definimos $A^+ = AA^* = A^*A$; A^+ é o menor subsemigrupo de M contendo A. A operação unária $A \mapsto A^*$ é denominada *estrela*.

Para todo conjunto X, o conjunto Rel(X) é um monóide, com a operação de composição. O conjunto FP(X) das funções parciais de X em X é um submonóide de Rel(X), bem como o conjunto X^X das funções de X em X.

1.3 - MONÓIDES LIVRES

Dado um conjunto Σ, o *monóide livre* Σ^* gerado por Σ é definido da seguinte forma. Os elementos de Σ^* são as sequências finitas

(3.1) $$x = (\sigma_1, \sigma_2, \ldots, \sigma_n) \quad n \geq 0$$

de elementos de Σ. Em particular, temos a sequência vazia $()$. O inteiro n é o *comprimento* de x, e é denotado $|x|$. Se $y = (\tau_1, \tau_2, \ldots, \tau_m)$ é outro elemento de Σ^*, o produto xy é definido por concatenação

$$xy = (\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_m).$$

Esse produto é claramente associativo, e a sequência vazia é o neutro, sendo também denotado por 1. Temos então que $|1| = 0$ e $|xy| = |x| + |y|$.

Ao invés de escrevermos (σ), denotaremos esta sequência de comprimento 1 por σ. Dessa forma, (3.1) pode ser escrito

$$x = \sigma_1 \sigma_2 \ldots \sigma_n,$$

se $n > 0$. Devido a isso, o elemento x é dito uma *palavra*, cada $\sigma \in \Sigma$ é chamado *letra* e Σ é chamado *alfabeto*.

Com a convenção $(\sigma) = \sigma$, podemos considerar $\Sigma \subseteq \Sigma^*$. Daí se justifica a notação Σ^*, uma vez que este é o único submonóide do monóide livre contendo Σ.

Como toda estrutura algébrica livre, os monóides livres tem a seguinte propriedade fundamental:

PROPRIEDADE 3.1 - Seja Σ um alfabeto e M um monóide. Então toda função $\phi: \Sigma \to M$ se estende de forma única a um morfismo

$$\phi^*: \Sigma^* \to M.$$

Para demonstrar proposições sobre o monóide livre, e definirmos funções ou relações do monóide livre em algum conjunto, utilizaremos:

PRINCÍPIO DE INDUÇÃO PARA O MONÓIDE LIVRE: Seja Σ^* o monóide livre gerado por Σ e P uma propriedade monovalente de palavras. Se $P(x)$ é válida para toda palavra x de comprimento n e se para toda palavra y e letra σ, $P(y)$ válida implica $P(y\sigma)$ válida, então $P(x)$ é válida para toda palavra x de comprimento $\geq n$.

Se $x = x_1 x_2 \ldots x_n$, com $x, x_1, x_2, \ldots, x_n \in \Sigma^*$, dizemos que $x_1 x_2 \ldots x_n$ é uma *fatoração* de x.

Se $\Gamma \subset \Sigma$, definimos a aplicação $|\ |_\Gamma: \Sigma^* \to \mathbb{N}$ indutivamente por

$$|1|_\Gamma = 0$$

$$|x\sigma|_\Gamma = \begin{cases} |x|_\Gamma \text{ se } \sigma \notin \Gamma \\ |x|_\Gamma + 1 \text{ se } \sigma \in \Gamma \end{cases}$$

Em particular, $|x|_\Sigma = |x|$ e $|x|_\sigma$ denota o número de ocorrências da letra σ em x.

Vale a pena ainda frisar as seguintes propriedades:

Seja x uma palavra.

a) Para cada solução da equação

$$i_1+i_2+\ldots+i_k = |x|$$

em inteiros não negativos, existe uma única fatoração

$$x = x_1x_2\ldots x_k, \text{ com } |x_j| = i_j,\ j=1,2,\ldots,k.$$

b) Se $x = u_1v_1 = u_2v_2$ e $|u_1| \leq |u_2|$, então existe uma única palavra w tal que

$$u_1 = u_2w \text{ e } v_2 = wv_1$$

1.4 - SEMIANÉIS

Um *semianel* (com unidade) é um conjunto K, com dois elementos distinguidos e distintos 0 e 1, e duas operações binárias $+$ e $\cdot$, satisfazendo o seguinte:

a) $+$ é associativa, comutativa e tem 0 como elemento neutro

b) $\cdot$ é associativa e tem 1 como elemento neutro

c) $\cdot$ é distributiva à direita e à esquerda em relação a $+$

d) $0.k = k.0 = 0$, para todo $k \in K$.

Um semianel é dito *comutativo* se a operação $\cdot$ o for.

Em particular, todo anel com unidade é um semianel.

Subsemianéis, morfismos, somas diretas finitas e infinitas são definidos de maneira análoga à para anéis.

Seguem alguns exemplos de semianéis que não são anéis, alguns dos quais serão citados posteriormente:

R_+, Q_+, N, com as operações usuais.

O semianel de Boole, $B = \{0,1\}$, onde $1+1 = 1$ (de resto, as operações tem resultado determinado pelos axiomas).

$N = N \cup \infty$, onde as operações restritas a N são as usuais e

$$\infty + a = a + \infty = \infty \ , \ a \cdot \infty = \infty \cdot a = \infty \text{ se } a \neq 0 \text{ e } 0 \cdot \infty = \infty \cdot 0 = 0.$$

Ainda podemos estender a ordem de N, colocando, para todo $a \in N$, $a < \infty$.

$M = N \cup \infty$, com soma: $a \oplus b = \min(a,b)$ e produto $a \otimes b = a+b$, onde min e + são tomados em N.

Para cada $n \in N$, considere a função $\phi_n : N \cup \infty \to \{0,1,\ldots,n,\infty\}$, dada por:

$$x\phi_n = \begin{cases} x \text{ se } x \in \{0,1,\ldots,n,\infty\} \\ n \text{ caso contrário} \end{cases}$$

temos mais os semianéis:

$N_n = \{0,1,\ldots,n,\infty\}$, $a +_n b = (a+b)\phi_n$, $a \cdot_n b = (a \cdot b)\phi_n$ ($+$ e $\cdot$ são as operações de N).

$M_n = \{0,1,\ldots,n,\infty\}$, $a \oplus_n b = (a \oplus b)\phi_n$, $a \otimes_n b = (a \otimes b)\phi_n$ ($\oplus$ e $\otimes$ são as operações de M).

Ainda podemos apresentar:

$R = R_+ \cup \infty$, com operações análogas às de M.

Um semianel é *positivo* se ele satisfaz as seguintes condições para todos elementos x,y:

a) Se $x+y = 0$ então $x = y = 0$

b) Se $x \cdot y = 0$ então $x = 0$ ou $y = 0$.

Nenhum anel é positivo, e todos os semianéis apresentados acima são positivos. Se K é um semianel positivo, a aplicação $T: K \to B$, definida por

$$0T = 0, \quad xT = 1 \text{ se } x \neq 0$$

é um morfismo de semianéis. Observe o leitor que usaremos o

mesmo símbolo T com todos os semianéis positivos.

Dados conjuntos não vazios P,Q e um semianel K, uma aplicação A: P×Q → K é uma *matriz* P×Q com *coeficientes* em K. Em geral, no lugar da notação (p,q)A, usaremos a notação A_{pq}. Uma matriz 1×Q é chamada vetor linha e uma matriz Q×1 é denominada vetor coluna. Se A é um vetor linha, denotamos A_{1q} por A_q, e analogamente para vetores coluna. Observe que os dois tipos de vetores podem ser identificados com funções Q → K.

Para matrizes em $K^{P\times Q}$ definem-se da forma usual multiplicação por escalar (k∈K) e soma:

$$(kA)_{pq} = k\cdot A_{pq},\quad (Ak)_{pq} = A_{pq}\cdot k,$$

$$(A+B)_{pq} = A_{pq}+B_{pq}.$$

Se P,Q,R são conjuntos finitos, A é uma matriz P×Q, B é uma matriz Q×R, com coeficientes em K, o produto AB é uma matriz P×R definida por:

$$(AB)_{pr} = \sum_{q\in Q} A_{pq}\cdot B_{qr}.$$

Verifica-se imediatamente que se $A\in K^{P\times Q}$, $B\in K^{Q\times R}$, $C\in K^{R\times S}$, então,

$$(AB)C = A(BC).$$

Uma matriz P×Q é *quadrada* se P = Q. Vamos denotar por $M_Q(K)$ o conjunto das matrizes quadradas Q×Q → K. Se Q é finito, $M_Q(K)$ com as operações de soma e produto é um semianel. Existe um isomorfismo natural entre $M_1(K)$ e K, que a cada matriz associa seu único coeficiente. Por meio deste isomorfismo vamos identificar esses dois semianéis.

Quando nos referirmos a $M_Q(K)$ como monóide, estaremos subentendendo a operação de multiplicação.

Finalmente, uma observação: no estudo usual de matrizes, no lugar de conjuntos arbitrários P,Q, costuma-se utilizar conjuntos do tipo n. A razão de utilizarmos conjuntos arbitrários é, principalmente, de eliminar o que seria uma ordem irrelevante no conjunto dos estados de um autômato (ver Capítulo II). Mas, quando for conveniente, utilizaremos matrizes de $M_n(K)$, da forma apresentada por Hoffman e Kunze [HK1].

I.5 - K-SUBCONJUNTOS

Considere um conjunto X e um subconjunto A. Este fica determinado pela *função característica* $\chi_A: X \to \mathcal{B}$, onde $x\chi_A = 1$ sse $x \in A$. Em certos casos, a cada elemento do conjunto A associamos uma certa multiplicidade (como no conjunto de raízes de um polinômio), que é um número natural. Isto é feito por meio de uma generalização da função característica, e, por meio de operações convenientemente definidas, obtem-se uma álgebra de funções que lembra em vários aspectos uma álgebra booleana. A estrutura que permite essa generalização, unificando $\mathcal{B}$ e N é justamente a de semianel.

Seja K um semianel e X um conjunto. Um *K-subconjunto* de X é uma aplicação $A: X \to K$. Para cada $x \in X$, xA é sua *multiplicidade*. O conjunto $s(A) = \{x \in X \mid xA \neq 0\}$ é chamado *suporte* de A. O $\mathcal{B}$-subconjunto χ_A, dado por $x\chi_A = 1$ sse $x \in s(A)$ é chamado *$\mathcal{B}$-subconjunto característico* de A; se K é positivo, $\chi_A = A^T$. Como temos sempre a inclusão de conjuntos $\mathcal{B} \subset K$, χ_A pode ser interpretado como um K-subconjunto. Um K-subconjunto A é *não-ambíguo* se $A = \chi_A$; nesse caso, ele fica determinado pelo seu suporte, e temos $A = \chi_A = \chi_{s(A)}$.

O K-subconjunto vazio $\emptyset$ é definido por $x\emptyset = 0, \forall x \in X$.

Se $x \in X$, vamos indicar por $\underline{x}$ o K-subconjunto definido por:

$$y\underline{x} = \begin{cases} 1 \text{ se } y = x \\ \\ 0 \text{ se } y \neq x, \end{cases}$$

que será chamado de K-subconjunto *unitário*.

Também definimos o K-subconjunto não ambíguo X por $xX = 1$, para todo $x \in X$.

Se A,B são K-subconjuntos de X, $k \in K$, os K-subconjuntos kA, Ak, A+B e A∩B são definidos por:

$$x(kA) = k\cdot(xA) \quad , \quad x(Ak) = (xA)\cdot k,$$

$$x(A+B) = xA+xB \quad , \quad x(A\cap B) = xA\cdot xB.$$

Observe que $0A = A0 = \emptyset$.

Dada uma família indexada $\{A_i\}_{i\in I}$ de K-subconjuntos de X, podemos, sob certas condições, definir o K-subconjunto $\sum_{i\in I} A_i$ por:

$$x \sum_{i\in I} A_i = \sum_{i\in I} xA_i \tag{5.1}$$

Para isso, algumas condições devem ser satisfeitas para que a soma à direita, em (5.1) esteja bem definida. Eilenberg apresenta a noção de *semianel completo*, como sendo um semianel K, tal que para toda família $\{x_i\}_{i\in I}$ de elementos de K, está bem definido um elemento Σx_i, satisfazendo certas propriedades usuais. Por exemplo, B, N, M são semianéis completos. Para o nosso estudo, é mais conveniente restringir a definição em (5.1) para o caso em que a família $\{A_i\}$ é *localmente finita*, isto é, para cada $x \in X$, existe uma quantidade finita de índices, tais que $xA_i \neq 0$. Neste caso, a soma em (5.1) tem significado bem claro, e valem, entre outras, as propriedades

$$k \sum_{i\in I} A_i = \sum_{i\in I} kA_i,$$

$$\sum_{j\in J}\sum_{i\in I_j} A_i = \sum_{i\in I} A_i,$$

onde $\{I_j\}_{j\in J}$ é uma partição de I.

Se A é um K-subconjunto de X, a família $\{(xA)\underline{x}\}_{x\in X}$ é localmente finita, e claramente:

$$A = \sum_{x\in X} (xA)\underline{x}. \tag{5.2}$$

No caso de K-subconjuntos de um monóide M, vamos introduzir um produto, que restrito aos unitários é a operação de M, e que dá a K^M uma estrutura de semianel, quando combinado com a soma já definida.

Definimos para $A,B\in K^M$ o produto AB por:

$$x(AB) = \sum_{yz=x} yA\cdot zB.$$

Isto nem sempre faz sentido, pois podemos ter infinitos pares (y,z) tais que x = yz. No caso em que o semianel é completo, não há restrições a fazer. Em outros casos, costuma-se restringir ao estudo de K-subconjuntos de suporte finito (anéis de grupo, por exemplo).

Uma outra possibilidade é a de nos restringirmos a monóides em que para toda palavra x existe um conjunto finito de pares (y,z) tais que x = yz. Isto é o que faremos aqui, trabalhando com monóides livres. Em desenvolvimentos da teoria além dos limites do nosso trabalho, utilizam-se também produtos diretos finitos de monóides livres.

No caso de um monóide livre Σ^*, a família dos seus K-subconjuntos é denotada $K\langle\langle\Sigma\rangle\rangle$, que com a soma e produto acima definidos tem uma estrutura de semianel. Devido à expansão (5.2), $K\langle\langle\Sigma\rangle\rangle$ é também chamado de semianel das *séries formais nas variáveis não comutativas* Σ, *com coeficien*

tes em K. No caso em que K é um anel, verifica-se imediatamente que $K\langle\langle\Sigma\rangle\rangle$ é um anel, e uma álgebra sobre K, se K for comutativo. Um elemento de $K\langle\langle\Sigma\rangle\rangle$ de suporte finito é chamado do *polinômio* em Σ; os polinômios formam um subsemianel de $K\langle\langle\Sigma\rangle\rangle$, denotado $K\langle\Sigma\rangle$. Observe que para todo $k\in K$, $A\in K\langle\langle\Sigma\rangle\rangle$, $kA = (k\underline{1})A$, onde $\underline{1}$ é o K-subconjunto unitário associado a $1\in\Sigma^*$. Em particular, $K\langle\Sigma\rangle$ é fechado por multiplicação por escalares de K (à esquerda e à direita).

Se K_1 é um subsemianel de K_2, consideraremos de forma natural $K_1\langle\langle\Sigma\rangle\rangle$ um subsemianel de $K_2\langle\langle\Sigma\rangle\rangle$.

Um K-subconjunto de Σ^* é dito *quase-inversível* se $1A = 0$. Se A é quase inversível, a família $\{A^n\}_{n\in\mathbb{N}}$ é localmente finita, e definimos:

$$A^+ = \sum_{n\geq 1} A^n \quad \text{e}$$

$$A^* = \sum_{n\geq 0} A^n = 1+A^+.$$

A série A^+ é chamada *quase-inversa* de A, e satisfaz a identidade:

$$A^+ = A+AA^+ = A+A^+A. \tag{5.3}$$

A razão deste nome é que quando K é um anel e A é quase-inversível, 1-A é inversível e sua inversa é $1+A^+$.

Dado $A\in K\langle\langle\Sigma\rangle\rangle$, sua *parte quase-inversível* $B\in K\langle\langle\Sigma\rangle\rangle$ é definida por:

$$xB = \begin{cases} xA \text{ se } x \neq 1 \\ 0 \text{ se } x = 1, \end{cases}$$

Então $A = (1A)\underline{1}+B$, e B é quase inversível.

Se $\phi: K_1 \to K_2$ é um morfismo de semianéis, e $A \in K_1\langle\langle\Sigma\rangle\rangle$, a função composta $A\phi$ é um K_2-subconjunto de Σ^*, e valem as seguintes propriedades, para todo $A, B \in K_1\langle\langle\Sigma\rangle\rangle$, $k \in K_1$:

$$(kA)\phi = k\phi A\phi,$$

$$(A+B)\phi = A\phi + B\phi,$$

$$(A \cap B)\phi = A\phi \cap B\phi,$$

$$(AB)\phi = A\phi B\phi.$$

Conforme observamos no início da secção, existe uma correspondência biunívoca que a cada $L \subseteq \Sigma^*$ associa

$$\chi_L \in B\langle\langle\Sigma\rangle\rangle.$$

Assinalamos as seguintes propriedades, válidas para todo $L, L' \subseteq \Sigma^*$:

(5.4) $$\chi_{L \cup L'} = \chi_L + \chi_{L'},$$

(5.5) $$\chi_{L \cap L'} = \chi_L \cap \chi_{L'},$$

(5.6) $$\chi_{LL'} = \chi_L \chi_{L'},$$

(5.7) $$\chi_{L^+} = \chi_L^+$$

(5.8) $$\chi_{L^*} = \chi_L^*$$

sendo as duas últimas para $L \subseteq \Sigma^+$.

Finalmente, um comentário relacionado com a secção anterior. Conforme observamos, um vetor em $K^{1\times Q}$ ou $K^{Q\times 1}$ pode ser considerado uma função de Q em K. Portanto, um vetor é também um K-subconjunto de Q! Além disso, as definições de de soma e multiplicação por escalar são concordantes para K^Q interpretado como conjunto de vetores linha, ou vetores coluna ou K-subconjuntos de Q. Por isso nos permitiremos tratar um vetor ora como vetor, ora como K-subconjunto.

- □ -

"Ele não o reconheceu; porque como as suas mãos estavam cobertas de pelo, pareceram-lhe todas semelhantes às do mais velho."

Gênese 27:23

CAPÍTULO II

CONJUNTOS E K-SUBCONJUNTOS RECONHECÍVEIS

II.1 - Σ-AUTÔMATOS E CONJUNTOS RECONHECÍVEIS (RESUMO)

Daqui em diante, Σ será suposto um conjunto finito não vazio.

Um Σ-*autômato* é uma quádrupla $A = (Q,I,F,E)$, onde

Q é um conjunto finito, de *estados*,
$I \subseteq Q$, é chamado conjuntos dos *estados iniciais*,
$F \subseteq Q$, é chamado conjunto dos *estados finais*,
E é uma aplicação $\Sigma \to Rel(Q)$.

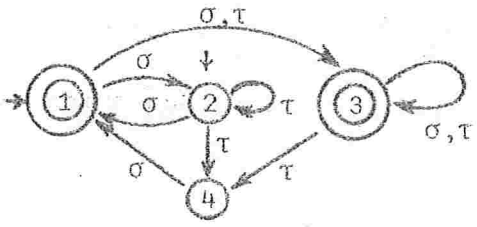
Denotamos por E^* a extensão de E a um morfismo $\Sigma^* \to Rel(Q)$, dado pela Propriedade I.3.1. Na descrição de um Σ-autômato substituiremos ocasionalmente a aplicação E pelo morfismo E^*. Isto tem a vantagem de permitir uma generalização da teoria para monóides não livres, mas não desenvolveremos este aspecto no nosso trabalho. Quando não houver possibilidade de confusão, omitiremos a referência ao alfabeto, dizendo simplesmente autômato.

Se p e q são estados e $q \in p\sigma E$, dizemos que a tripla (p,σ,q) é uma *aresta* de A, dirigida do *início*, p, ao *término* q, com *rótulo* σ.

Costuma-se representar graficamente um autômato do

seguinte modo: aos estados fazem-se corresponder pequenos círculos. Para cada par de estados p,q tal que existe uma aresta dirigida de p para q, coloca-se uma seta apontando do círculo correspondente a p para o círculo que corresponde a q. Essa seta é rotulada com todos os rótulos de arestas dirigidas de p para q. Coloca-se uma seta apontando para o círculo de cada estado inicial, e um círculo rodeando cada estado final. Por exemplo:

$A = (Q,I,F,E)$, $Q = \{1,2,3,4\}$, $I = \{1,2\}$, $F = \{1,3\}$, $\Sigma = \{\sigma,\tau\}$



P	1	2	3	4
pσE	{2,3}	1	3	1
pτE	3	{2,4}	{3,4}	∅

Uma *trilha* em A é uma sequência finita $T=a_1a_2\ldots a_n$ de arestas tal que o término de a_i é igual ao início de a_{i+1}, $i=1,\ldots,n-1$. Se para $1 \leq i \leq n$, $a_i=(p_{i-1},\sigma_i,p_i)$, dizemos que T vai de p_0 para p_n, *soletrando* $x = \sigma_1\sigma_2\ldots\sigma_n$. A palavra x é também chamada o *rótulo* de T. Se T é uma trilha de p para q soletrando x, denotamos:

$$T: p \xrightarrow{x} q,$$

e, eventualmente, omitiremos a referência ao rótulo de T. Para cada estado p, a sequência vazia de arestas é uma trilha de p para p soletrando 1, e é chamada *trilha trivial*. As trilhas são simplesmente palavras do monóide livre gerado pelas arestas de A, e nessa condição está claro o que é concatenação de trilhas. Porém, se $T: p \xrightarrow{x} q$ e $S: r \xrightarrow{y} s$ são trilhas, a concatenação TS será uma trilha sse $q = r$. Nesse caso, $TS: p \xrightarrow{xy} s$.

O *comportamento* do autômato $A = (Q,I,F,E)$ é o con-

junto $|A| = \{x \in \Sigma^* / IxE^* \cap F \neq \emptyset\}$. Um conjunto $L \subseteq \Sigma^*$ é *reconhecível* sse ele for o comportamento de algum autômato.

PROPOSIÇÃO 1.1 - Sejam p,q estados de $A = (Q,I,F,E)$, $x \in \Sigma^*$. Então:

a) $q \in pxE^*$ sse existe uma trilha de p para q soletrando x,

b) $x \in |A|$ sse existe uma trilha dum estado inicial para um estado final soletrando x.

DEMONSTRAÇÃO - Suponhamos que existe uma trilha $T: p \xrightarrow{x} q$, onde

$$T = (p_0=p,\sigma_1,p_1)(p_1,\sigma_2,p_2)\ldots(p_{n-1},\sigma_n,p_n=q), \text{ e } x = \sigma_1\sigma_2\ldots\sigma_n.$$

Pela definição de arestas, $p_i \in p_{i-1}\sigma E$, $i=1,2,\ldots,n$. Daí vem:

$$p_1 \in p_0\sigma E,$$

$$p_2 \in p_1\sigma_2 E \subset (p_0\sigma_1 E)\sigma_2 E = p_0\sigma_1 E\sigma_2 E,$$

e, prosseguindo sucessivamente,

$$p_n \in p_0\sigma_1 E\sigma_2 E\ldots\sigma_n E = p_0(\sigma_1\sigma_2\ldots\sigma_n)E^*,$$

portanto, $q \in pxE^*$.

Agora vamos provar que, dados p,x, se $q \in pxE^*$ então existe uma trilha $T: p \xrightarrow{x} q$. Isto será feito por indução, para todo $x \in \Sigma^*$: Se $|x| = 0$, $x = 1$ e $1E^* = 1_Q$. Mas $p1_Q = p$ e temos a trilha trivial $T: p \xrightarrow{1} p$. Se $x = y\sigma$ e $q \in pxE^* = pyE^*\sigma E$, então existe um estado r tal que $r \in pyE^*$ e $q \in r\sigma E$. Pela hipótese de indução, existe uma trilha $T: p \xrightarrow{y} r$, e temos também a aresta (r,σ,q). Então, $T(r,\sigma,q): p \xrightarrow{x} q$.

No caso em que $x \in |A|$, $IxE^* \cap F \neq \emptyset$, seja $q \in IxE^* \cap F$. Como $IxE^* = \bigcup_{p \in I} pxE^*$, existe $p \in I$ tal que $q \in pxE^*$. Segue, pela parte anterior, que existe uma trilha do estado inicial p para o estado final q soletrando x. Por outro lado, se existe tal trilha, $q \in pxE^* \cap F \subset IxE^* \cap F$. □

O *monóide do autômato* A, denotado M_A, é o submonói de de Rel(Q) gerado pelo conjunto $\{\sigma E/\sigma\in\Sigma\}$. Equivalentemente, M_A é a imagem de Σ^* pelo morfismo E^*.

Um autômato é *determinístico* se existe um único estado inicial, e, para cada letra σ, σE é uma função parcial. Nesse caso, xE^* é uma função parcial, para toda palavra x, isto é, $M_A\subseteq FP(Q)$. Isto significa que dado um estado p e uma palavra x, existe no máximo uma trilha soletrando x a partir de p. Um autômato determinístico é *completo* se σE é uma função para cada $\sigma\in\Sigma$.

Lembremos (ver I.2) que dado um conjunto $L\subset\Sigma^*$, a congruência sintática de L, definida por:

$$x\sim_L y \iff \text{para todo } u,v\in\Sigma^*,\ uxv\in L \text{ sse } uyv\in L.$$

PROPOSIÇÃO 1.2 - Seja $L\subseteq\Sigma^*$. São equivalentes:

a) L é reconhecível.
b) L é o comportamento de um autômato determinístico completo.
c) O monóide sintático M_L é finito.
d) Existe uma congruência de índice finito sobre Σ^* tal que L é união de classes de congruência..
e) Existe um monóide finito M e um epimorfismo
$$\phi:\Sigma^*\longrightarrow M \text{ tal que } L = L\phi\phi^{-1}.$$

(A equivalência entre (a) e (c) é devida a Myhill e aparece em Rabin and Scott [RS1]).

DEMONSTRAÇÃO - Provaremos de acordo com o esquema
$$(a)\Rightarrow(c)\Rightarrow(d)\Rightarrow(e)\Rightarrow(b)\Rightarrow(a).$$

(a) implica (c) - Seja $A=(Q,I,F,E)$ um autômato reconhecendo L. Considere o epimorfismo $E^*:\Sigma^*\to M_A$.
Se $xE^*=yE^*$, então para todo $u,v\in\Sigma^*$, $(uxv)E^*=(uyv)E^*$.
Portanto, $I(uxv)E^*=I(uyv)E^*$, donde $uxv\in L$ sse $uyv\in L$.

Segue que $x \sim_L y$, e pela Propriedade I-2.1, existe um epimorfismo $\phi: M_A \to M_L$. Como $M_A \subset Rel(Q)$ é finito, vem que M_L também é finito.

(c) implica (d) - Como M_L é finito, $\sim_L$ tem índice finito; além disso, a definição de $\sim_L$ implica que $x \in L$ sse $[x] \subseteq L$. Portanto, $L = \bigcup_{x \in L} [x]$.

(d) implica (e) - Seja $\sim$ uma congruência nas condições de (d). Então $M = \Sigma^*/\sim$ é um monóide finito. Se $\phi: \Sigma^* \to M$ é a projeção canônica, para todo x, $x\phi\phi^{-1} = [x]$. Mas como L é união de classes de $\sim$, $x \in L$ implica $[x] \subseteq L$. Portanto $x\phi\phi^{-1} \subseteq L$ para todo $x \in L$, donde $L\phi\phi^{-1} \subseteq L$. A inclusão $L \subseteq L\phi\phi^{-1}$ é trivial.

(e) implica (b) - Vamos definir o autômato $A = (M, 1, L\phi, E)$ onde para todo $m \in M$, $\sigma \in \Sigma$, $m\sigma E = m \cdot (\sigma\phi)$. Claramente, σE é uma função para cada letra σ, e temos um único estado inicial, logo A é determinístico completo. É imediato que, para todo $x \in \Sigma^*$ e $m \in M$,

$$m(xE^*) = m \cdot (x\phi),$$

donde

$$\begin{aligned} x \in |A| &\iff 1(xE^*) \cap L\phi \neq \emptyset \\ &\iff x\phi \in L\phi \\ &\iff x \in L\phi\phi^{-1} \\ &\iff x \in L, \end{aligned}$$

portanto $L = |A|$.

b) implica a) - Nada a demonstrar. □

Dado um autômato $A = (Q, I, F, E)$ reconhecendo L, podemos construir diretamente um autômato determinístico

$$A' = (Q', I', F', E)$$

reconhecendo L da seguinte forma:

$$Q' = P(Q), \quad I' = I (\in Q'), \quad F' = \{X \in Q' / X \cap F \neq \emptyset\}$$

e, para todo $\sigma \in \Sigma$, a relação $\sigma E \in Rel(Q)$ é interpretada como função de Q' em Q'. Esta construção será referida pelo nome de *construção dos subconjuntos*.

A família dos subconjuntos reconhecíveis de Σ^* é denotada $Rec\Sigma$. A seguinte proposição apresenta algumas propriedades básicas de $Rec\Sigma$.

PROPOSIÇÃO 1.3 - Sejam $A,B \in Rec\Sigma$. Então $A \cup B$, $A \cap B$, $\bar{A} = \Sigma^* - A$, AB, A^+ e A^* são reconhecíveis.

DEMONSTRAÇÃO - Com exceção da afirmativa referente ao complemento, todas essas propriedades serão demonstradas na secção 3, a partir de uma formulação mais geral.

Vamos demonstrar que se A é reconhecível, $\bar{A}$ também o é. Seja $A = (Q,q,F,E)$ um autômato determinístico completo reconhecendo A, que existe pela proposição anterior. Então, A é reconhecido por $\bar{A} = (Q,q,Q-F,E)$. Com efeito, como A é determinístico, xE^* é uma função para cada x e:

$$x \in |A| \iff qxE^* \cap F \neq \emptyset$$
$$\iff qxE^* \in F$$
$$\iff qxE^* \notin Q-F$$
$$\iff x \notin |A|. \qquad \square$$

O seguinte teorema mostra que todo conjunto reconhecível pode ser obtido a partir de um conjunto finito de palavras, por meio de um número finito de operações. Será também demonstrado em formulação mais geral na secção 3 (Teorema 3.11).

TEOREMA 1.4 - (Teorema de Kleene [K2])- $Rec\Sigma$ é a menor família de subconjuntos de Σ^* contendo os subconjuntos unitários e fechada por união, concatenação e estrela.

Para encerrar esta secção, vamos apresentar uma condição necessária para um conjunto ser reconhecível. Essa condição tem uma generalização parcial no Teorema III.3.1,e permite apresentar certos exemplos de conjuntos não reconhecíveis.

PROPOSIÇÃO 1.5 - Seja L um subconjunto reconhecível de Σ^*. Então, existe um inteiro positivo k tal que toda palavra $x \in L$, com $|x| \geq k$ pode ser fatorada na forma $x = uvw$, com $0 < |v| \leq k$, de modo que $uv^*w \subseteq L$.

DEMONSTRAÇÃO - Seja $A = (Q, I, F, E)$ um autômato reconhecendo L e seja $k = |Q|$. Se $x \in L$, existem um estado inicial p, um estado final q e uma trilha

$$T = (p_0 = p, \sigma_1, p_1) \ldots (p_{n-1}, \sigma_n, p_n = q) : p \xrightarrow{x} q.$$

Se $n = |x| \geq k$, a sequência de estados $p_0, p_1, \ldots, p_k$ contém alguma repetição. Sejam $0 \leq i < j \leq k$ tais que $p_i = p_j$. Então T pode ser fatorada na forma $T = T_1 T_2 T_3$, onde

$$T_1 : p_0 \xrightarrow{u} p_i, \quad u = \sigma_1 \ldots \sigma_i,$$
$$T_2 : p_i \xrightarrow{v} p_j, \quad v = \sigma_{i+1} \ldots \sigma_j,$$
$$T_3 : p_j \xrightarrow{w} p_n, \quad u = \sigma_{j+1} \ldots \sigma_n.$$

Como $0 < j \leq k$, $0 < |v| = j - i \leq k$. Além disso, $p_i = p_j$ implica que para todo $n \geq 0$, $T_1 T_2^n T_3$ é uma trilha de p para q soletrando $uv^n w$, Portanto $uv^n w \in L$, para todo $n \geq 0$, o que equivale à tese. □

Essa condição, embora necessária, não é suficiente para garantir que um subconjunto de Σ^* é reconhecível. Por exemplo, com $\Sigma = \{\sigma, \tau\}$, considere os conjuntos

(1.1) $$A = \{\sigma^n \tau^n / n \geq 0\},$$

(1.2) $$B = \{x \in \Sigma^* / |x|_\sigma = |x|_\tau\}.$$

Ambas não estão em Rec Σ , pois o subconjunto σ^* gera um conjunto infinito de classes de congruência, tanto para $\sim_A$ como para $\sim_B$. Portanto, M_A e M_B são infinitos. No entanto, B satisfaz a condição da Proposição 5, bastando tomar $k = 2$. Já, o conjunto A é o exemplo clássico de conjunto que não satisfaz a dita condição. Para isto basta verificar que dado $k \geq 0$, tomando-se $m \geq k/2$, $\sigma^m\tau^m \in A$, e para toda fatoração $\sigma^m\tau^m = uvw$, com $v \neq 1$, $uv^nw \notin A$, para todo $n > 1$.

II.1.A - FORMA MATRICIAL DE UM AUTÔMATO

Seja Q um conjunto finito e $f \in Rel(Q)$. Podemos representar f pela matriz $f' \in M_Q(\mathcal{B})$ do seguinte modo

$$f'_{pq} = \begin{cases} 1 \text{ se } q \in pf \\ \\ 0 \text{ caso contrário.} \end{cases}$$

Lembremos que o semianel $\mathcal{B} = \{0,1\}$, com $1+1 = 1$ (ver I.4).

Essa correspondência é biunívoca, pois dada uma matriz $A \in M_Q(\mathcal{B})$, existe uma única relação f tal que $f' = A$. Além disso, é fácil verificar que, para todo $f,g \in Rel(Q)$,

$$(fg)' = f' \cdot g', \tag{1.3}$$

onde do lado direito temos um produto de matrizes. Segue que a aplicação $':Rel(Q) \to M_Q(\mathcal{B})$ é um isomorfismo de monóides.

Considere agora um autômato $A = (Q,I,F,E)$. Vamos construir:

Um vetor linha $I' \in \mathcal{B}^{1\times Q}$, onde $I'_q = 1$ sse $q \in I$

Um vetor coluna $F' \in \mathcal{B}^{Q\times 1}$, onde $F'_q = 1$ sse $q \in F$

Uma aplicação $E':\Sigma \to M_Q(\mathcal{B})$, dada por $\sigma E' = (\sigma E)'$.

Em vista do morfismo (1.3), segue que para toda palavra x, $xE'^* = (xE^*)'$, onde $E'^*:\Sigma^* \to M_Q(\mathcal{B})$ é o morfismo que estende E'. Afirmamos então que:

$$|A| = \{x \in \Sigma^* / I'(xE'^*)F' = 1\}. \tag{1.4}$$

Com efeito, $I'(xE'^*)F'=1$ sse existem p,q tais que

$$I'_p = (xE'^*)_{pq} = F'_q = 1.$$

Isto equivale a dizer que $p \in I$, $q \in F$ e $q \in pxE^*$, o que pela Proposição 1 equivale a $x \in |A|$.

Por outro lado, revertendo-se essa construção, podemos concluir que um conjunto L é reconhecível sse existe um conjunto finito Q, um vetor linha $I \in \mathcal{B}^{1\times Q}$, um vetor coluna $F \in \mathcal{B}^{Q\times 1}$ e uma aplicação $E: \Sigma \to M_Q(\mathcal{B})$ tal que

$$L = \{x \in \Sigma^* / I(xE^*)F = 1\}.$$

Observe que, para todo semianel K, $\mathcal{B} \subset K$, como conjuntos. Então, podemos supor que os vetores I',F', e as matrizes $\sigma E'$ tem coeficientes em K. Só que nesse caso, nem sempre (1.4) será válido.

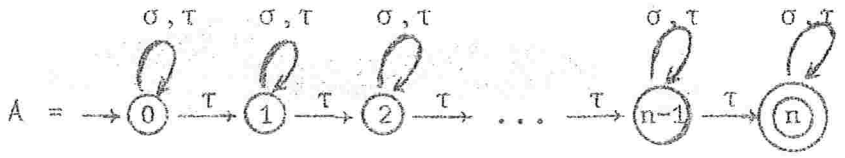
II.2 - K-SUBCONJUNTOS RECONHECÍVEIS

Na Teoria das Linguagens Formais (Salomaa [S1]) estudam-se subconjuntos de um monóide livre, ali chamados *linguagens*. Um dos mecanismos dessa teoria consiste nas gramáticas; certas classes de linguagens podem ser descritas por *gramáticas*, que são conjuntos de axiomas e regras de inferência que permitem demonstrar se uma palavra está numa linguagem. Acontece que conforme a gramática, para cada palavra pode existir um número diferente de demonstrações de que ela está na linguagem. A partir dessa observação, Chomsky e Schutzenberger [CS1] introduziram a idéia de associar a uma gramática não simplesmente um subconjunto de Σ^*, mas uma fun

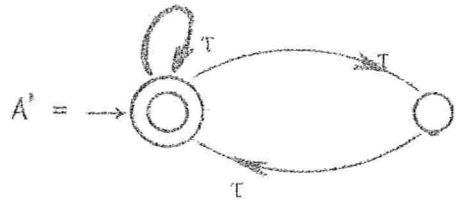
ção de Σ^* em N, cujo valor para cada palavra é o número de demonstrações naquela gramática que a palavra está na linguagem considerada (sendo 0 se a palavra não estiver).

No caso de conjuntos reconhecíveis, ocorre algo semelhante. Se um conjunto reconhecível A é dado por um autômato $\mathcal{A}$, sabemos que uma palavra $x \in A$ se e somente se existe em $\mathcal{A}$ uma trilha de um estado inicial para um estado final soletrando x. Assim, cada uma dessas trilhas pode ser considerada uma demonstração de que $x \in A$. Uma forma de estudarmos isto é associarmos ao autômato $\mathcal{A}$ uma função $\tilde{A}:\Sigma^* \to N$, dada por $x\tilde{A}$ = número de trilhas de um estado inicial para um final soletrando x.

Vários exemplos interessantes de funções podem ser definidas dessa forma:

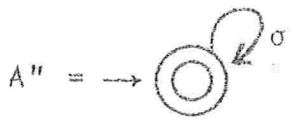


$$x\tilde{A} = \binom{|x|_\tau}{n} = \frac{r(r-1)\ldots(r-n+1)}{n!} \quad \text{onde } r = |x|_\tau$$



$\tau^n\tilde{A}'$ é o n-ésimo número de Fibonacci, a_n, dado por

$$a_0 = a_1 = 1, \quad a_n = a_{n-1} + a_{n-2} \text{ se } n \geq 2.$$



$$\sigma^n \tilde{A}'' = 1, \quad \forall n \in N.$$

Assim, A' e A'' tem o mesmo comportamento como reconhecedores de subconjuntos de Σ^* ($|A'| = |A''| = \Sigma^*$), porém a forma como o reconhecimento se processa, que é razoavelmente exposto por $\tilde{A}'$ e $\tilde{A}''$, é essencialmente diferente nos dois casos.

Um subconjunto $A \subseteq \Sigma^*$ fica perfeitamente determinado pela sua função característica χ_A. Assim, podemos substituir A pela função $\chi_A: \Sigma^* \to B$, sem perda de informação. Da mesma forma, na situação anterior, nada se perde substituindo-se o comportamento $|A|$ pela função $\tilde{A}$. O conceito que unificou propriedades de N e B de modo a estender o estudo de subconjuntos para funções foi o de semianel (I.4). Eilenberg introduziu a noção de K-subconjuntos (I.5), e outros semianéis mostraram ser relevantes no estudo de subconjuntos de Σ^* (por exemplo, N, R_+, e, de modo inesperado, M). Assim, cabe observar que o interesse fundamental da presença de semianéis na teoria é o de unificar uma série de resultados isolados. O estudo algébrico de semianéis não é, por enquanto, uma disciplina estabelecida.

A forma de estender a noção de subconjunto reconhecível para a de K-subconjunto reconhecível, de forma que possamos, por exemplo, estudar o número de trilhas num autômato é dada pela construção na subsecção 1.A.

A partir de agora, K é suposto um semianel e Σ^* o monóide livre gerado pelo alfabeto Σ.

Um K-Σ-*autômato* é uma quádrupla $A = (Q, I, F, E)$ onde:

Q é um conjunto finito de *estados*
$I \in K^{1 \times Q}$ é o *vetor inicial*
$F \in K^{Q \times 1}$ é o *vetor final*
$E: \Sigma \to M_Q(K)$ uma função.

Observe que mesmo em termos de definição, esta é quase uma reformulação da definição de Σ-autômato, pois I e F podem ser interpetrados como K-subconjuntos de Q, e teríamos os K-subconjuntos de estados iniciais e finais. Veremos adiante que a partir de E se estende a noção de aresta de Σ-autômato de forma bastante natural.

Quando não houver possibilidade de confusão, vamos nos referir a um K-Σ-autômato como K-autômato ou simplesmente autômato. A expressão Σ-autômato ficará reservada para os autômatos da secção 1.

Denotamos, como sempre, por $E^*: \Sigma^* \to M_Q(K)$ a extensão de E a um morfismo. Um K-Σ-autômato será as vezes descrito por uma quádrupla (Q,I,F,ϕ), onde $\phi: \Sigma^* \to M_Q(K)$ é um morfismo.

Vamos utilizar a notação $(xE^*)_{pq} = xE^*_{pq}$, com $p,q \in Q$. Essa eliminação de parênteses alivia certas expressões, e além disso, para cada $p,q \in Q$, podemos considerar E^*_{pq} como um subconjunto de Σ^*.

O *comportamento* de A é o K-subconjunto $|A|$ de Σ^* dado por

$$x|A| = IxE^*F, \quad \forall x \in \Sigma^*,$$

Um subconjunto de Σ^* é *reconhecível* sse ele for o comportamento de um K-Σ-autômato A, e nesse caso ele é *reconhecido* por A. A família dos K-subconjuntos reconhecíveis de Σ^* é denotada $\mathrm{Rec}_K\Sigma$.

Se K_1 é um subsemianel de K_2, todo K_1-Σ-autômato é um K_2-Σ-autômato. Segue que $\mathrm{Rec}_{K_1}\Sigma \subseteq \mathrm{Rec}_{K_2}\Sigma$. Veremos posteriormente que, em geral,

$$\mathrm{Rec}_{K_1}\Sigma \neq K_1\langle\langle\Sigma\rangle\rangle \cap \mathrm{Rec}_{K_2}\Sigma \tag{2.1}$$

Se $K_1 \subseteq K_2$ e $A \in K_1\langle\langle\Sigma\rangle\rangle \cap Rec_{K_2}\Sigma$ diremos que A é K_2-*reconhecível*. No caso $K_1 = K_2$, K_1-reconhecível equivale ao conceito de reconhecível.

PROPOSIÇÃO 2.1 - Um conjunto $L \subseteq \Sigma^*$ é reconhecível sse

$$\chi_L \in Rec_B\Sigma.$$

DEMONSTRAÇÃO - É dada pela construção na subsecção 1.A. □

Seja $A = (Q,I,F,E)$ um K-Σ-autômato. Uma tripla $(p,\sigma,q) \in Q\times\Sigma\times Q$ é uma *aresta* de A se $\sigma E_{pq} \neq 0$. O *peso* ρ é o K-subconjunto de $Q\times\Sigma\times Q$ dado por $(p,\sigma,q)\rho = \sigma E_{pq}$; observe que dado E, fica determinado ρ e vice-versa. O conceito de trilha e as observações sobre concatenação de trilhas vistas na secção 1 continuam válidas. Se $T = (p_0,\sigma_1,p_1)\ldots(p_{n-1},\sigma_n,p_n)$ é uma trilha, seu *peso* também denotado ρ, é definido por:

$$T\rho = \prod_{i=1}^{n} (p_{i-1},\sigma_i,p_i)\rho = \sigma_1 E_{p_0p_1}\sigma_2 E_{p_1p_2}\ldots\sigma_n E_{p_{n-1}p_n},$$

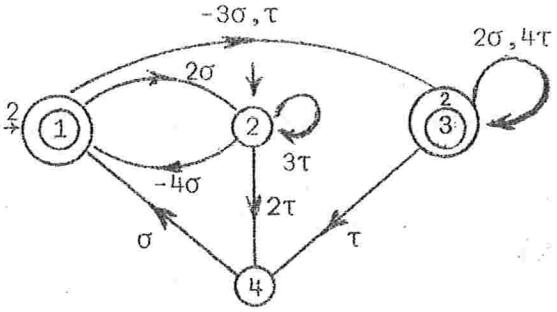
e denotamos

$$T:\ p_0 \xrightarrow{T\rho,x} p_n$$

onde x é a palavra soletrada por T. Eventualmente omitiremos $T\rho$ ou x ao utilizarmos o símbolo acima. Observe que a definição de peso de uma trilha é parte da extensão da função $\rho: Q\times\Sigma\times Q \to K$ a um morfismo do monóide livre $(Q\times\Sigma\times Q)^*$ ao monóide multiplicativo K. Para cada estado p, temos a trilha trivial $T:\ p \xrightarrow{1,1} p$.

Representamos pictorialmente um K-Σ-autômato de forma análoga a Σ-autômatos, isto é, com círculos para os estados e setas para as arestas. Coloca-se uma seta com rótulo I_p apontando para o círculo correspondente a p se $I_p \neq 0$. Se $F_p \neq 0$, o círculo p será assinalado como estado final, e en-

tre os dois círculos colocado o rótulo F_p. Em geral, se I_p ou $F_p = 1$, não colocamos explicitamente esse rótulo. Se (p,σ,q) é uma aresta com peso k, na seta correspondente colocamos o rótulo $k\sigma$, ou σ se $k = 1$. Por exemplo:



$$K = Z,\ Q = \{1,2,3,4\}$$

$$I = (2,1,0,0),\ F = \begin{pmatrix}1\\0\\2\\0\end{pmatrix}$$

$$\sigma E = \begin{pmatrix}0 & 2 & -3 & 0\\ -4 & 0 & 0 & 0\\ 0 & 0 & 2 & 0\\ 1 & 0 & 0 & 0\end{pmatrix} \qquad \tau E = \begin{pmatrix}0 & 0 & 1 & 0\\ 0 & 3 & 0 & 2\\ 0 & 0 & 4 & 1\\ 0 & 0 & 0 & 0\end{pmatrix}$$

Vamos dar agora uma interpretação para o comportamento de um K-Σ-autômato que mostrará que quando $K = N$ e A é um B-Σ-autômato interpretado como N-Σ-autômato, $\tilde{A} = |A|$.

PROPOSIÇÃO 2.2 - Sejam p,q estados do K-Σ-autômato (Q,I,F,E). Então, para toda palavra x,

$$xE^*_{pq} = \sum T\rho,$$

onde T percorre o conjunto de todas as trilhas de p para q que soletram x.

DEMONSTRAÇÃO - Por indução.

Se $x = 1$, trivial.

Se $x = y\sigma$, toda trilha $T: p \xrightarrow{x} q$ pode ser fatorada na forma $T = T_1(r,\sigma,q)$, onde $T_1: p \xrightarrow{y} r$, para algum estado r. Por outro lado, dada uma trilha $T_1: p \xrightarrow{y} r$, se (r,σ,q) é uma aresta, então $T_1(r,\sigma,q): p \xrightarrow{x} q$. Daí segue que

$$\{T/T: p \xrightarrow{x} q\} = \bigcup_{r/\sigma E_{rq} \neq 0} \{T(r,\sigma,q)/T: p \xrightarrow{y} r\}$$

Portanto,

$$xE^*_{pq} = \sum_{r\in Q} yE^*_{pr}\sigma E^*_{rq}$$

$$= \sum_{r/\sigma E_{rq}\neq 0} yE^*_{pr}\sigma E_{rq}$$

$$= \sum_{r/\sigma E_{rq}\neq 0} \left(\sum_{T:p\xrightarrow{y}r} T\rho \right)(r,\sigma,q)\rho \text{ (pela hipótese de indução)}$$

$$= \sum_{T:p\xrightarrow{x}q} T\rho. \qquad \square$$

COROLÁRIO 2.3 - Se $A = (Q,I,F,E)$ é um K-Σ-autômato, para toda palavra x,

$$x|A| = \sum_{p,q\in Q} \sum_{T:p\xrightarrow{x}q} (I_p T\rho F_q).$$

DEMONSTRAÇÃO - Fica a cargo do leitor. $\square$

Se $q\in A$, $\underline{\delta}^q$ é o vetor

$$\delta^q_p = \begin{cases} 1 \text{ se } p = q \\ 0 \text{ se } p \neq q \end{cases}$$

ficando o contexto encarregado de esclarecer se se trata de vetor linha ou vetor coluna; é simplesmente uma notação vetorial para os K-subconjuntos unitários de Q.

Um K-Σ-autômato é dito *normalizado* se existirem estados i,f, distintos tais que

$$I = \delta^i;\ F = \delta^f;\ \sigma E_{qi} = \sigma E_{fq} = 0,\ \forall q\in Q.$$

PROPOSIÇÃO 2.4 - Seja A um K-subconjunto reconhecível de Σ^*. Então, existe um autômato normalizado reconhecendo a parte quase-inversível de A.

DEMONSTRAÇÃO - Seja $A = (Q,I,F,E)$ um K-Σ-autômato reconhecendo A. Vamos construir $A' = (Q',I',F',E')$ da seguinte forma:

$Q' = Q \cup \{i,f\}$, onde i e f são elementos distintos e não estão em Q.

$I' = \delta^i$; $F' = \delta^f$;

E' é definido, para cada letra σ por:

$$\sigma E'_{pq} = \sigma E_{pq} \text{ se } p,q \in Q \tag{2.2}$$

$$\sigma E'_{iq} = (I\sigma E)_q \text{ se } q \in Q \tag{2.3}$$

$$\sigma E'_{qf} = (\sigma E F)_q \text{ se } q \in Q \tag{2.4}$$

$$\sigma E'_{if} = I\sigma E F \tag{2.5}$$

$$\sigma E'_{qi} = \sigma E'_{fq} = 0 \text{ para todo } q \in Q'. \tag{2.6}$$

É claro que A' é normalizado. Vamos demonstrar que $|A'|$ é a parte quase-inversível de A.

A partir de (2.6) segue imediatamente:

$$xE'^*_{qi} = 0, \ \forall q \in Q', \ \forall x \in \Sigma^+. \tag{2.7}$$

Afirmamos que, para todo $q \in Q$, e todo $x \in \Sigma^+$,

$$xE^*_{iq} = (IxE^*)_q, \tag{2.8}$$

o que segue por indução, lembrando que

$$(y\sigma)E'^*_{iq} = \sum_{r \in Q'} yE'^*_{ir}\sigma E'_{rq} = \sum_{r \in Q} yE'^*_{ir}\sigma E'_{rq},$$

por (2.6) e (2.7), e usando-se (2.3) para estabelecer a base.

Finalmente, se $x \in \Sigma^*$, calculemos $x|A'|$:

Se $x = 1$, $x|A'| = I'F' = \delta^i \delta^f = 0$, pois $i \neq f$.

Se $x = \sigma \in \Sigma$, $x|A'| = I'\sigma E'F' = \sigma E'_{if} = I\sigma EF = \sigma A$.

Se $|x| > 1$, $x = y\sigma$, com $y \in \Sigma$, e:

$$x|A'| = I'xE'^*F' = xE'^*_{if}$$

$$= \sum_{q \in Q'} yE'^*_{iq} \sigma E'_{qf}$$

$$= \sum_{q \in Q} yE'^*_{iq} \sigma E'_{qf} \quad \text{por (2.6) e (2.7)}$$

$$= \sum_{q \in Q} (IyE^*)_q (\sigma EF)_q \quad \text{por (2.4) e (2.8)}$$

$$= IyE^*\sigma EF$$

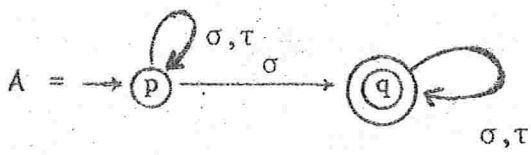
$$= IxE^*F$$

$$= xA.$$

Portanto, $|A'|$ é a parte quase-inversível de A. □

EXEMPLO: Considere o N-$\{\sigma,\tau\}$- autômato

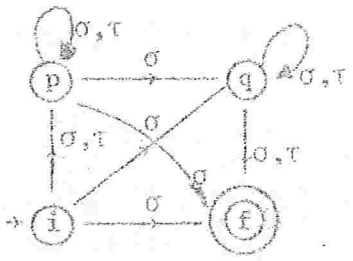
(2.9)



Dado $x \in \Sigma^*$, para cada fatoração da forma $x = uov$ temos uma trilha $p \xrightarrow{u} p \xrightarrow{\sigma} q \xrightarrow{v} q$. Portanto, existem exatamente $|x|_\sigma$ trilhas de p para q soletrando x, cada uma com peso 1. Pelo Corolário 3, como $I = \delta^p$, $P = \delta^q$, $x|A| = |x|_\sigma$ e

$$|A| = \sum_{x \in \Sigma^*} |x|_\sigma \underline{x}.$$

Aplicando-se a construção da Proposição 4 obtem-se:

$A' =$ 

e

$$|A'| = \sum_{x \in \Sigma^+} |x|_\sigma \underline{x}.$$

COROLÁRIO 2.5 - (Schutzenberger [S2]) - Um K-subconjunto quase-inversível A de Σ^* é reconhecível sse existe um natural n e um morfismo $\phi: \Sigma^* \to M_n(K)$ tal que $xA = x\phi_{1n}$, $\forall x \in \Sigma^+$.

DEMONSTRAÇÃO - Se A é reconhecível, seja $A' = (Q, \delta^i, \delta^f, E)$ um K-Σ-autômato normalizado reconhecendo A, e seja $n = |Q|$. Podemos então numerar $Q = \{q_1, \ldots, q_n\}$, onde $q_1 = i$, $q_n = f$. Definimos então ϕ por:

$$x\phi_{jk} = xE^*_{q_j q_k}$$

Verifica-se imediatamente que $x\phi_{1n} = xE^*_{if} = xA$.

Por outro lado, dado o morfismo ϕ nas condições acima, $(n, \delta^1, \delta^n, \phi)$ é um K-Σ-autômato que reconhece A. □

PROPOSIÇÃO 2.6 - Se $L \subseteq \Sigma^*$ é reconhecível, então a função característica χ_L é K-reconhecível para todo semianel K (aqui consideramos a inclusão de conjuntos $\mathcal{B} \subseteq K$).

DEMONSTRAÇÃO - Seja $A = (Q,I,F,E)$ um Σ-autômato determinístico (Proposição 1.2) reconhecendo L. Aplicando-se a construção da subsecção 1.A, tem-se $A' = (Q,I',F',E')$, onde para todo p,q,σ tem-se $I'_q, F'_q, \sigma E'_{pq} \in \mathcal{B}$, e verifica-se o seguinte:

(a) As trilhas de A' estão em correspondência biunívoca com as de A.

(b) Todas as trilhas em A' tem peso 1.

Como A é determinístico, $I = p$ e existe, para cada x, no máximo uma trilha soletrando x a partir de p. Mas o vetor inicial de A' é δ^p, donde:

$$x \in L \iff \text{existe em } A \text{ } T: p \xrightarrow{x} q, \text{ com } q \in F$$

$$\iff \text{existe em } A' \text{ } T: p \xrightarrow{x} q, \text{ com } F_q = 1.$$

Portanto, se $x \in L$, $x|A'| = \delta^p_p T_\rho F_q = 1$. Se $x \notin L$, ou não existe trilha a partir de p soletrando x em A ou existe $T: p \xrightarrow{x} q$, com $q \notin F$. Neste caso, $F_q = 0$ e em ambos os casos, $x|A'| = 0$. Portanto, $x|A'| = 1$ se $x \in L$ e $x|A'| = 0$ se $x \notin L$. Segue que $|A'| = \chi_L$. □

II.2.3 - OPERAÇÕES COM K-SUBCONJUNTOS RECONHECÍVEIS

O objetivo desta secção é demonstrar o Teorema de Kleene-Schutzenberger, que é a generalização para K-subconjuntos de Σ^* do Teorema 1.4. Desta forma, aplicando-se a Proposição 2.1, teremos como corolários a Proposição 1.3 e Teorema 1.4, via as identidades I (5.4)-(5.8).

No decorrer desta secção, salvo menção explícita,

suporemos A e A' K-subconjuntos reconhecíveis de Σ^*, sendo A reconhecido por $A = (Q,I,F,E)$ e A' por $A' = (Q',I',F',E')$ e $Q \cap Q' = \emptyset$. Nas proposições que envolvem construção de um autômato, apresentaremos esse autômato, e em geral deixaremos ao leitor a maçante, mas fácil, tarefa de demonstrar que o comportamento do autômato construído é o que é afirmado na proposição.

PROPOSIÇÃO 3.1 - Se $k \in K$, então kA e $Ak \in Rec_K^{\Sigma}$.

DEMONSTRAÇÃO - kA é reconhecido por (Q,kI,F,E) e Ak é reconhecido por (Q,I,Fk,E). □

PROPOSIÇÃO 3.2 - $A+A' \in Rec_K^{\Sigma}$.

DEMONSTRAÇÃO - A+A' é reconhecido por $A+A' = (Q \cup Q',J,G,H)$, onde:

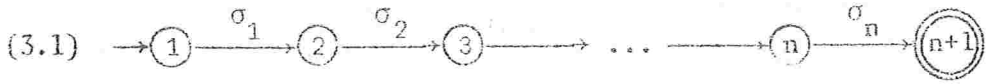
$$J_q = \begin{cases} I_q & \text{se } q \in Q \\ I'_q & \text{se } q \in Q' \end{cases} \quad ; \quad G_q = \begin{cases} F_q & \text{se } q \in Q \\ F'_q & \text{se } q \in Q' \end{cases}$$

$$\sigma H = \sigma E \oplus \sigma E', \text{ isto é, } \sigma H_{pq} = \begin{cases} \sigma E_{pq} & \text{se } p,q \in Q \\ \sigma E'_{pq} & \text{se } p,q \in Q' \\ 0 & \text{caso contrário.} \end{cases}$$ □

Observe que se K é um anel, $A-A' = A+(-1)A'$ é reconhecível pelas proposições acima.

COROLÁRIO 3.3 - Todo polinômio é reconhecível.

DEMONSTRAÇÃO - Se $x = \sigma_1\sigma_2\ldots\sigma_n \in \Sigma^*$, com $\sigma_i \in \Sigma$, $i=1,2,\ldots,n$, o K-subconjunto unitário $\underline{x}$ é reconhecido pelo K-Σ-autômato

(3.1) 

Aplicando-se as Proposições 1 e 2, obtem-se a tese. Em particular, se x=1, o autômato em (3.1) é → ⓞ □

COROLÁRIO 3.4 - Uma série é reconhecível sse sua parte quase inversível o é.

DEMONSTRAÇÃO - Se A é reconhecível, sua parte quase-inversível o é, pela Proposição 2.4.

Se $B \in Rec_K\Sigma$ é a parte quase-inversível de A, então,

$$A = (1A)\underline{1} + B \in Rec_K\Sigma \qquad \square$$

PROPOSIÇÃO 3.5 - $AA' \in Rec_K\Sigma$.

DEMONSTRAÇÃO - Seja $a = 1A$, $a' = 1A'$, B e B' respectivamente as partes quase inversíveis de A e A'. Então,

$$(3.2) \qquad AA' = (a\underline{1}+B)(a'\underline{1}+B') = aa'\underline{1} + aB' + Ba' + BB'.$$

Pelo que já foi demonstrado nesta secção,

$$aa'\underline{1} + aB' + Ba' \in Rec_K(\Sigma).$$

Portanto, para completar, basta mostrar que BB' é reconhecível. Para isso, sejam $\mathcal{B} = (R, \delta^i, \delta^f, H)$ e $\mathcal{B}' = (R', \delta^{i'}, \delta^{f'}, H')$ autômatos normalizados reconhecendo B e B' (Proposição 2.4), e podemos supor $R \cap R' = \emptyset$. Então, BB' é reconhecido por:

$$\mathcal{C} = (R \cup R' - i', \delta^i, \delta^{f'}, G),$$

onde

$$\sigma G_{pq} = \begin{cases} \sigma H_{pq} & \text{se } p,q \in R \\ \sigma H'_{pq} & \text{se } p,q \in R' \\ \sigma H^!_{i',q} & \text{se } p=f,\ q \in R'-i' \\ 0 & \text{caso contrário.} \end{cases}$$

Em outras palavras, $\mathcal{B}$ é obtido unindo-se $\mathcal{B}$ e $\mathcal{B}'$, identificando-se i' e f e mantendo-se todas as arestas com o mesmo peso. $\square$

Seria interessante se pudéssemos provar que $Rec_K\Sigma$ é fechado pela operação $\cap$. Porém, não conhecemos uma demons

tração disso válida para todo semianel K, nem sabemos se isto é válido. Acontece que, como veremos, $A \cap A'$ é reconhecível se K for comutativo. E os semianéis que têm mais importância até agora na teoria (N, R_+, M, B) são todos comutativos. Assim, Eilenberg de princípio define o conceito de K-subconjunto reconhecível supondo K comutativo; fica assim ressaltada a importância secundária por ele (e outros autores) atribuída aos semianéis como estrutura. O que apresentaremos é uma versão da propriedade referente à $\cap$, que pode ser encontrada em Fliess [Fl], onde a comutatividade do semianel é substituída por uma condição um pouco mais fraca. A partir de resultados do Capítulo IV (Proposição IV-2.6 e 3.2), pode-se provar que se K é finito, $Rec_K\Sigma$ é fechado por $\cap$, independentemente de sua estrutura.

PROPOSIÇÃO 3.6 - Se K_1 e K_2 são subsemianéis de K tais que todo elemento de K_1 comuta com todo elemento de K_2, $A \in Rec_{K_1}\Sigma$, $A' \in Rec_{K_2}\Sigma$, então $A \cap A' \in Rec_K\Sigma$. Em particular, se A' é não ambíguo e $s(A')$ é reconhecível, então

$$A \cap A' \in Rec_{K_1}\Sigma.$$

Finalmente, se K é comutativo, $Rec_K\Sigma$ é fechado por $\cap$.

DEMONSTRAÇÃO - Podemos supor que A é um K_1-autômato e A' é um K_2 autômato. Então $A \cap A'$ é reconhecido por $A \cap A' = (R, J, G, H)$, onde:

$$R = Q \times Q'; \quad J_{(q,q')} = I_q \cdot I'_{q'}, \quad G_{(q,q')} = F_q \cdot F'_{q'};$$

$$\sigma H_{(p,p')(q,q')} = \sigma E_{pq} \cdot \sigma E'_{p'q'}.$$

Com efeito, para todo $x \in \Sigma^*$, $p,q \in Q$, $p',q' \in Q'$,

$$xH^*_{(p,p')(q,q')} = xE^*_{pq}\, xE'^*_{p'q'}.$$

Isto se verifica por indução em x, lembrando que para todo $y, \sigma, yE'^*_{p'r'} \in K_2$, $\sigma E^*_{rq} \in K_1$, e portanto comutam.

Assim, para todo x,

$$x|A\cap A'| = \sum_{(p,p'),(q,q')} J(p,p')\,xH^*(p,p')(q,q')\,G(q,q') =$$

$$= \sum_{p,p',q,q'} I_p I'_{p'}\,xE^*_{pq}\,xE'^*_{p'q'}\,F_p F'_{p'} =$$

$$= \sum_{p,q,p',q'} (I_p\,xE^*_{pq}F_q)(I'_{p'}\,xE'^*_{p'q'}F'_{p'}) \quad \text{(usando a comutatividade)}$$

$$= \left(\sum_{p,q} I_p\,xE^*_{pq}F_q\right)\left(\sum_{p',q'} I'_{p'}\,xE'^*_{p'q'}F'_{q'}\right) =$$

$$= xA\cdot xA' =$$

$$= x(A\cap A').$$

Se A' é não ambíguo, e s(A') é reconhecível, a Proposição 2.6 nos mostra $A' = \chi_{s(A')}$ é também um K_1-subconjunto reconhecível, reconhecido por um autômato onde os coeficientes são zeros e 1's. Portanto, podemos construir $A\cap A'$ da forma acima. □

PROPOSIÇÃO 3.7 - Se A é quase-inversível, A^+ e A^* são reconhecíveis.

DEMONSTRAÇÃO - Seja (P,δ^i,δ^f,H) uma autômato normalizado reconhecendo A (Proposição 2.4). O autômato $(P-f,\delta^i,\delta^f, M)$, onde

$$\sigma M_{pq} = \begin{cases} \sigma H_{pq} & \text{se } q \neq i \\ \sigma H_{pf} & \text{se } q = f \end{cases}$$

reconhece A^*; A^+ é portanto reconhecível pelo Corolário 4. □

COROLÁRIO 3.8 - Se L é um subconjunto reconhecível de Σ^*, L^* e L^+ são também reconhecíveis.

DEMONSTRAÇÃO - Se $L \subseteq \Sigma^+$, $\chi_L \in Rec_{\mathcal{B}}\Sigma$ é quase-inversível, donde $\chi_L^+ = \chi_{L^+}$ e $\chi_L^* = \chi_{L^*}$ são reconhecíveis. Pela Proposição 2.1, L^+ e L^* são reconhecíveis. Se $1 \in L$,

$$L^+ = L^* = 1 \cup (L-1)^+,$$

sendo portanto reconhecíveis. □

PROPOSIÇÃO 3.9 - Seja $\phi: K \to K_1$ um morfismo de semianéis. Se $A \in Rec_K\Sigma$, então $A\phi \in Rec_{K_1}\Sigma$.

DEMONSTRAÇÃO - $A\phi$ é o comportamento do K_1-autômato (Q, J, G, H) onde

$$J_q = I_q\phi; \quad G_q = F_q\phi \quad \text{e} \quad \sigma H_{pq} = \sigma E_{pq}\phi \qquad \square$$

COROLÁRIO 3.10 - Se K é um semianel positivo e $A \in Rec_K\Sigma$ então $s(A)$ é um subconjunto reconhecível de Σ^*.

DEMONSTRAÇÃO - Como K é positivo, podemos aplicar o morfismo $T: K \to \mathcal{B}$, e pela Proposição 9, $AT \in Rec_{\mathcal{B}}\Sigma$. Pela Proposição 2.1, $s(AT) = s(A)$ é reconhecível. □

Um subsemianel de $K\langle\langle\Sigma\rangle\rangle$ é *racionalmente fechado* se contém o quase-inverso de todos os seus elementos quase-inversíveis. É imediato que a intersecção de qualquer família de subsemianéis racionalmente fechados é um subsemianel com a mesma propriedade. O subsemianel $Rat_K\Sigma$ dos K-subconjuntos *racionais* é o menor subsemianel racionalmente fechado de $K\langle\langle\Sigma\rangle\rangle$ que contém os polinômios, $K\langle\Sigma\rangle$. Observe que se $A \in Rat_K\Sigma$, $k \in K$, então $kA = (k1)A \in Rat_K\Sigma$, pois $k1 \in K\langle\Sigma\rangle$.

TEOREMA 3.11 - (Kleene-Schutzenberger [S2]) - Seja K um semianel e Σ um alfabeto, Então as famílias de K-subconjuntos reconhecíveis e racionais de Σ^* são idênticas.

DEMONSTRAÇÃO - As Proposições 2 e 5 mostram que $Rec_K\Sigma$ é um subsemianel, a Proposição 7 mostra que é racionalmente fechado, e o Corolário 3 que $K<\Sigma>\subseteq Rec_K\Sigma$. Portanto, $Rat_K\Sigma\subseteq Rec_K\Sigma$.

Para mostrarmos a inclusão inversa, seja $A\in Rec_K\Sigma$, reconhecido por $A = (Q,I,F,E)$. Vamos demonstrar que A é racional.

Redenominando os estados, podemos supor $Q = n$. Considere os autômatos $A_i = (Q,\delta^i,F,E)$, $i=1,\ldots,n$ e seja $A_i = |A_i|$. Claramente, $A = \sum_i I_i A_i$, portanto, se mostrarmos que cada A_i é racional, seguirá que A é racional.

Para isso, em primeiro lugar, vamos observar o seguinte: fixados i,j, E_{ij} é uma aplicação $\Sigma \to K$, dado por

$$\sigma \longrightarrow \sigma E_{ij}$$

e como $\Sigma\subseteq\Sigma^*$, E_{ij} pode ser considerado um K-subconjunto de Σ^*, onde $xE_{ij} = 0$ se $x\notin\Sigma$.

Vamos provar que para cada i vale

$$A_i = \sum_j E_{ij}A_j + (1A_i)\underline{1}. \tag{3.3}$$

Para isso, vamos calcular xA_i, para cada $x\in\Sigma$. Se $x = 1$, como $1E_{ij} = 0$, vem

$$1A_i = 1\left(\sum_j E_{ij}A_j + (1A_i)\underline{1}\right).$$

Se $x \neq 1$, $x = \sigma y$. Nesse caso, lembremos que para todo j e todo w,

$$wA_j = \delta^j wE^*F = (wE^*F)_j.$$

Então,

$$
\begin{aligned}
xA_i &= \delta^i x E^* F \\
&= \delta^i \sigma E y E^* F \\
&= \sum_i (\delta^i \sigma E)_j (y E^* F)_j \\
&= \sum_j \sigma E_{ij} y A_j \\
&= \sigma y \sum_i E_{ij} \cdot A_j \\
&= x\left(\sum_j E_{ij} A_j + (1A_j)\cdot \underline{1}\right).
\end{aligned}
$$

Portanto, o vetor $(A_1, A_2, \ldots, A_n) \in K\langle\langle\Sigma\rangle\rangle^{n\times 1}$ é uma solução do sistema de equações lineares:

$$
\begin{aligned}
X_1 &= E_{11}X_1 + E_{12}X_2 + \ldots + E_{1n}X_n + T_1 \\
X_2 &= E_{21}X_1 + E_{22}X_2 + \ldots + E_{2n}X_n + T_2 \\
&\vdots \\
X_n &= E_{n1}X_1 + E_{n2}X_2 + \ldots + E_{nn}X_n + T_n
\end{aligned}
$$

onde $T_i = (1A_i)\underline{1}$. Observe que os coeficientes E_{ij} são polinômios quase-inversíveis (como K-subconjuntos de Σ^*), e $T = (T_1, \ldots, T_n)$ é um vetor de polinômios em $K\langle\Sigma\rangle$. O teorema segue das proposições adiante.

PROPOSIÇÃO 3.12 - Seja E uma matriz $n\times n$ de K-subconjuntos quase-inversíveis de Σ^* e T um vetor $n\times 1$ de $K\langle\langle\Sigma\rangle\rangle$. Então existe no máximo um vetor $X \in K\langle\langle\Sigma\rangle\rangle^{n\times 1}$ satisfazendo

$$X = EX + T \tag{3.4}$$

DEMONSTRAÇÃO - Suponhamos que X e Y sejam soluções de (3.4),

e vamos provar que $X = Y$. Para isso vamos mostrar que para toda palavra x e todo $i \in n$, $xX_i = xY_i$.

Se $x = 1$,

$$1X_i = 1(EX)_i + 1T_i$$

$$= 0 + 1T_i \qquad ((EX)_i \text{ é quase-inversível})$$

$$= 1(EY)_i + 1T_i$$

$$= 1Y_i$$

Se $x = \sigma y$, supondo, por indução, $yX_i = yY_i$ para todo i,

$$xX_i = x(EX)_i + xT_i$$

$$= x\left(\sum_j E_{ij}X_j\right) + xT_i$$

$$= \sum_j \left(\sum_{uv=x} uE_{ij}vX_j\right) + xT_i \text{ e como } uE_{ij} = 0 \text{ se } |u| \neq 1,$$

$$= \sum_j \sigma E_{ij} yX_j + xT_i$$

$$= \sum_j \sigma E_{ij} yY_j + xT_i$$

$$= x\sum_j E_{ij}Y_j + xT_i$$

$$= x\left((EY)_i + T_i\right)$$

$$= xY_i \qquad \square$$

PROPOSIÇÃO 3.13 - Nas condições da proposição anterior, o sistema tem solução e se para todo i, j, E_{ij}, T_i são K-subconjuntos racionais de Σ^*, então a solução de (3.4) é um vetor de K-subconjuntos racionais.

DEMONSTRAÇÃO - Vamos provar por indução em n.

Se $n = 1$, o sistema tem uma simples equação

(3.5) $$X = EX + T.$$

Como E é quase-inversível, $X = E^*T$ é a solução de (3.5), pois $EE^*T+T = (E^+\underline{1})T = E^*T$. Se E e T são racionais, claramente $E^*T \in Rat_K\Sigma$.

Suponhamos $n > 1$. Temos então que

$$X_n = E_{nn}X_n + C + T_n,$$

onde $C = E_{n1}X_1 + \ldots + E_{n(n-1)}X_{n-1}$.

Isto é um caso particular de (3.5), portanto

(3.6) $$X_n = E^*_{nn}(C+T_n)$$

Então podemos substituir X_n nas outras equações de (3.4), e obtemos o sistema de $n-1$ equações e $n-1$ incógnitas

(3.7) $$X' = E'X' + T',$$

onde

(3.8) $E'_{ij} = E_{ij} + E_{in}E^*_{nn}E_{nj}$ é quase-inversível e

(3.9) $$T'_i = T_i + E_{in}E^*_{nn}T_n.$$

Pela hipótese de indução, (3.7) tem solução. Completando com X_n calculado a partir de (3.6), temos que (3.3) tem solução.

Ainda, como os E_{ij}, T_i são racionais, (3.8) e (3.9) mostra que os E'_{ij}, T'_j também o são. Portanto, $X_i \in Rat_K\Sigma$, $1 \le i \le n-1$, pela hipótese de indução. A expressão (3.6) mostra que $X_n \in Rat_K\Sigma$. □

"Quero ficar no teu corpo
feito tatuagem..."

F.B.de Hollanda

CAPÍTULO III

O CASO EM QUE K É UM CORPO

III.1 - IDÉIAS GERAIS

No caso em que o semianel de coeficientes é um corpo, técnicas de álgebra linear podem ser aplicadas às matrizes e vetores que ocorrem nos K-Σ-autômatos. Com isso obtem-se resultados particulares, em alguns casos muito fortes. Neste capítulo apresentaremos três deles. Alguns desses resultados tem aplicação para semianéis que são subsemianéis de um corpo. Entre esses destaca-se de forma especial N.

Na secção 2, apresentaremos o teorema da Igualdade, devido a Eilenberg e Schutzenberger [E1], que tem como consequência a possibilidade de decisão algorítmica quanto a igualdade de K-subconjuntos reconhecíveis.

O conteúdo da secção 3 é o Teorema da Estrela, trabalho de Jacob [J1] , [J2] e que é uma generalização parcial da Proposição II.1.5. Apresentaremos aí uma simplificação considerável da demonstração original.

Finalmente, a secção 4 contém o resultado fundamental de Fliess [F1], [F2], sobre matrizes de Hankel, generalizando resultados da Análise clássica para séries racionais. Consiste numa caracterização algébrica de K-subconjuntos re

conhecíveis, com importantes consequências teóricas, desenvolvidas nos trabalhos citados. Além disso, permitiu-nos construir um exemplo pedido por Eilenberg em seu livro. Uma combinação com o Teorema da Igualdade permitiu-nos obter uma construção efetiva do autômato reduzido, apresentado por Schtzenberger e construído também na demonstração de Fliess.

No decorrer deste capítulo, K será suposto um corpo (comutativo).

III.2 - O TEOREMA DA IGUALDADE

TEOREMA 2.1 - Um K-Σ-autômato $A = (Q, I, F, E)$ tem comportamento $|A| = \emptyset$ sse $x|A| = 0$ para toda palavra x com comprimento menor que $|Q|$.

DEMONSTRAÇÃO - Seja $n = |Q|$. Então $K^{1\times Q}$ é um espaço vetorial sobre K, de dimensão n. Para cada $i \geq 0$, seja V_i o subespaço de $K^{1\times Q}$ gerado pelo conjunto

$$Y_i = \{IvE^* / |x| \leq i\}. \tag{2.1}$$

Vamos definir

$$W = \{X \in K^{1\times Q} / XF = 0\}. \tag{2.2}$$

Por hipótese, $IxE^*F = 0$ para todo x tal que $|x| < n$. Logo, para todo $i < n$, $V_i \subseteq W$. Temos portanto a seguinte sequência de subespaços

$$V_0 \subseteq V_1 \subseteq \ldots \subseteq V_{n-1} \subseteq W. \tag{2.3}$$

Podemos supor $I \neq 0$ e $F \neq 0$, pois nesses casos é imediato que $|A| = \emptyset$. Portanto, $\dim V_0 = 1$, $\dim W = n-1$. Como temos n subespaços V_i em (2.3), as inclusões não podem ser todas próprias, donde, para um certo $0 \leq j < n-1$, $\dim V_j = \dim V_{j+1}$ e daí vem $V_j = V_{j+1}$. Vamos mostrar que $V_k = V_j$, para todo $k \geq i$.

Por construção, se $k \geq j$, $V_j \subseteq V_k$.

Seja então $k > j$, e vamos supor, por indução, que $V_{k-1} = V_j$. Mas V_k é gerado por Y_k, e claramente vale

$$Y_k = \{X(\sigma E)/X \in Y_{k-1}, \sigma \in \Sigma\}.$$

Como $Y_{k-1} \subset V_{k-1} = V_j$, $Y_k \subset V_{j+1}$. Mas pela escolha de j, $V_{j+1} = V_j$, donde $Y_k \subseteq V_j$, e segue que $V_k \subseteq V_j$.

Dessa forma, para todo $k \geq 0$, $V_k \subseteq V_j \subseteq W$, o que implica $Y_k \subseteq W$, para todo $k \geq 0$. Por (2.1) e (2.2), isso se traduz em

$$IxE^*F = 0, \ \forall x \in \Sigma^*,$$

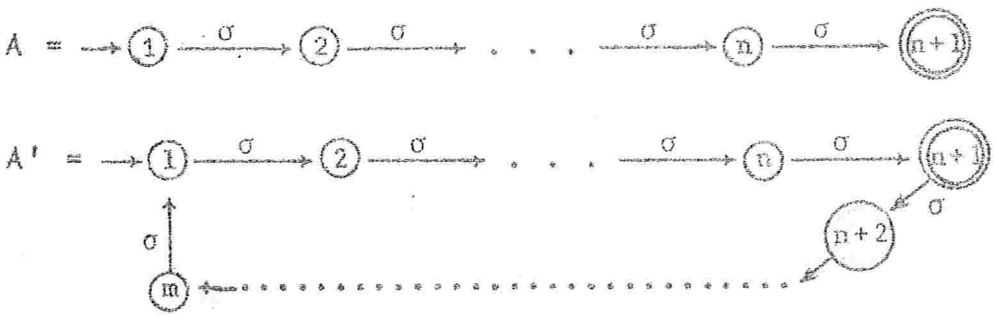
donde $|A| = \mathcal{A}$. □

TEOREMA 2.2 (Teorema da Igualdade) - Sejam A e A' K-Σ-autômatos com n e n' estados respectivamente. Então $|A| = |A'|$ sse $x|A| = x|A'|$ para toda palavra x tal que $|x| < n+n'$.

DEMONSTRAÇÃO - Aplicando-se as construções das Proposições II.3.1 e II.3.2, obtemos um autômato reconhecendo $|A| - |A'|$, com n+n' estados. A tese é, então, consequência do Teorema 1. □

Este exemplo mostra que a limitação é a melhor possível.

Sejam $0 < n < m$ inteiros, $\Sigma = \sigma$, A e A' representados graficamente por:



Então, $|A| = \sigma^n$, $|A'| = \sum_{k\geq 0} \sigma^{n+mk}$ e, para todo $r < n+m$, $\sigma^r|A| = \sigma^r|A'|$.

Como corolário do Teorema da Igualdade vem:

TEOREMA 2.3 - Dados K-Σ-autômatos A e A', é decidível se

$$|A| = |A'|.$$

Em particular, como $N \subseteq Q$, o problema de igualdade de N-subconjuntos reconhecíveis é decidível. Como consequência, podemos, por exemplo, decidir se um N-Σ-autômato reconhece um N-subconjunto não ambíguo.

Com efeito, dado um N-Σ-autômato A reconhecendo A, pelo Corolário II.3.10, s(A) é reconhecível, e a Proposição II.2.5, nos dá a construção efetiva de um N-Σ-autômato A' reconhecendo $\chi_{s(A)}$. Aí, basta aplicar o Teorema 2 para decidir se $|A| = |A'|$.

III.3 - O TEOREMA DA ESTRELA

TEOREMA 3.1 - Seja A um K-subconjunto reconhecível de Σ^*, com suporte infinito. Então existe um inteiro k tal que toda palavra $x \in s(A)$, com $|x| > k$, pode-se fatorar na forma

$$x = uvw, \text{ com } v \neq 1$$

de modo que o K-subconjunto de σ^*

$$\sum_{n\geq 0} (uv^n wA)\underline{\sigma}^n$$

é reconhecível e tem suporte infinito.

Este teorema é devido a Jacob [J1].

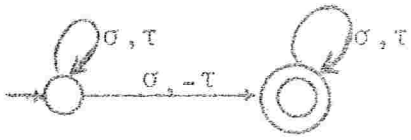
Antes de apresentarmos uma demonstração desse teorema, queremos tecer alguns comentários:

Sabemos que se S é um semianel positivo, todo S-subconjunto de Σ^* tem suporte reconhecível. Dessa forma, temos uma condição que permite provar que alguns S-subconjuntos não são reconhecíveis. Por exemplo, as séries formais

$$A = \sum_{n\geq 0} n\sigma^n\tau^n \tag{3.1}$$

$$B = \sum_{x\in\Sigma^*} (|x|_\sigma - |x|_\tau)^2 \underline{x} \tag{3.2}$$

sobre $\Sigma = \{\sigma,\tau\}$ não são N-subconjuntos reconhecíveis, pois seus suportes não são conjuntos reconhecíveis (Cap.I,(1.1) e (1.2)).No entanto, o Z-Σ-autômato



reconhece $C = \Sigma(|x|_\sigma - |x|_\tau)\underline{x}$, donde $B = C \cap C \in Rec_Z\Sigma$. Isto mostra que

$$B \in N\langle\langle\Sigma\rangle\rangle \cap Rec_Z\Sigma - Rec_N\Sigma,$$

sendo um exemplo da situação referida em II(2.1).

Podemos levantar a mesma questão para a série A. O Teorema 1 permite-nos provar que ela não é um Q-subconjunto reconhecível, não estando portanto em $Rec_Z\Sigma$. Com efeito, para todo inteiro positivo k, e toda fatoração $\sigma^k\tau^k = uvw$, a série $\sum(uv^nwA)\underline{\sigma}^n$ é um polinômio.

A demonstração de Jacob do Teorema 1 divide-se em duas partes. A primeira consiste num teorema sobre matrizes, de demonstração extremamente técnica, e que faz o papel da descoberta da subtrilha fechada na proposição II.1.6 (é o Teorema 2). Não repetiremos a demonstração aqui, e referi-

mos o leitor ao trabalho original para isso. De posse desse teorema, completaremos a demonstração, com uma simplificação da prova original.

Para nomenclatura e resultados sobre espaços vetoriais e transformações lineares, utilizaremos o livro de Hoffman e Kunze [HK1]. Usaremos também sua notação, em particular, a imagem de v pela aplicação linear T será indicada T(v) ou Tv quando não houver possibilidade de confusão.

Seja V um espaço vetorial sobre K, de dimensão finita n. Uma transformação $T \in L(V,V)$ é dita *pseudo-regular* se V pode ser decomposto na soma direta $E_1 \oplus E_2$ de subespaços invariantes sobre T de forma que

$T|_{E_1}$ é inversível e

$T|_{E_2}$ é a aplicação nula.

Uma matriz é pseudo-regular se for semelhante à soma direta de uma matriz inversível e uma matriz nula.

TEOREMA 3.2 - Seja V um espaço vetorial sobre K, de dimensão finita n, Σ um alfabeto finito e $\phi:\Sigma^* \to L(V,V)$ um morfismo de monóides. Então, existe um inteiro k, dependendo somente de n e $|\Sigma|$, tal que toda palavra x, com $|x|>k$, e $x\phi \neq 0$ pode ser fatorada $x = uvw$, com $v \neq 1$ de modo que $v\phi$ seja uma transformação pseudo-regular.

DEMONSTRAÇÃO DO TEOREMA 1 - Seja $A \in Rec_K \Sigma$ e suponhamos que A é reconhecido por $A = (Q,I,F,E)$. Podemos supor $Q = n$, para algum n, redenominando eventualmente os estados.

Seja $x \in \Sigma^*$, e $x = uvw$ uma fatoração. Considere o K-σ-autômato $A' = (n, IuE^*, wE^*F, E')$ onde $\sigma E' = vE^*$. É imediato que

$$A' = \sum (uv^t wA)\sigma^t$$

portanto essa série é reconhecível.

Seja agora k dado pelo Teorema 2 para $V=K^{n\times 1}$ e $\phi=E^*$, onde identificamos cada transformação linear com sua representação na base canônica. Seja $x\in s(A)$, com $|x| > k$; então, $IxE^*F \neq 0$, donde $xE^* \neq 0$, assim, pelo Teorema 2, $x = uvw$, onde $v \neq 1$ e $T = vE^*$ é pseudo-regular.

Então, $V = V_1 \oplus V_2$, onde

$$T_1 = vE^*|_{V_1} \text{ é inversível e}$$

$$T_2 = vE^*|_{V_2} \text{ é nula.}$$

Esta decomposição induz uma decomposição $V^* = V_2^0 \oplus V_1^0$ do espaço dual V^*, onde V_i^0 é o anulador de V_i, $i=1,2$. Considere os vetores $J = IuE^*$, $G = wE^*F$, e seja $\psi: K^{1\times n} \to V^*$ o isomorfismo que ao vetor L associa o funcional linear $L\psi$, tal que $(L\psi)(X) = LX$ (produto vetor linha por vetor coluna).

Podemos então escrever de forma única,

$$G = G_1 + G_2$$

$$J = J_1 + J_2$$

onde $G_1 \in V_1$, $G_2 \in V_2$, $J_1\psi \in V_2^0$ e $J_2\psi \in V_1^0$. Dessa forma, para todo inteiro r,

$$uv^r wA = I(uv^r wE^*)F$$

$$= JT^r G$$

$$= J_1 T_1^r G_1 + J_2 T_2^r G_2$$

$$= J_1 T_1^r G_1 \qquad \text{pois } T_2 = 0.$$

Queremos provar que $uv^r wA \neq 0$ para uma infinidade de inteiros r. Isto segue do seguinte lema:

LEMA 3.3 - Seja V um espaço vetorial de dimensão finita n sobre K, $T:V \to V$ uma aplicação linear inversível, f um funcional linear não nulo sobre V. Seja $v \in V$, tal que $f(v) \neq 0$. Então

$$f(T^m v) \neq 0,$$

para uma infinidade de inteiros m.

DEMONSTRAÇÃO - Suponhamos que a tese seja falsa. Então, existe $m_0 \geq 0$ tal que

(3.1) $$f(T^{m_0} v) \neq 0 \quad \text{e} \quad f(T^m v) = 0, \ \forall m > m_0$$

Seja $w = T^{m_0} v$. Então (3.1) se transforma em:

(3.2) $$w \neq 0 \quad \text{e}$$

(3.3) $$f(T^m w) = 0, \ \forall m \geq 1.$$

Considere agora o espaço T-cíclico gerado por w, isto é, o subespaço V' de V gerado pelos vetores $\{T^m w / m \geq 0\}$. Seja $r = \dim V'$ e

$$\chi_T(X) = \sum_{i=0}^{r} a_i X^i$$

o polinômio característico de $T' = T|_{V'}$. Como T é inversível, T' também o é, logo $a_0 = \det(T') \neq 0$. Lembrando que para todo k, $T'^k w = T^k w$ e $\chi_{T'}(T') = 0$, vem:

$$0 = \chi_{T'}(T')(w) = \sum_{i=0}^{r} a_i T'^i(w) = \sum_{i=0}^{r} a_0 T^i w$$

donde

$$\sum_{i=1}^{r} a_i T^i w = -a_0 w$$

portanto,

$$\sum_{i=1}^{r} a_i f(T^i w) = f\left(\sum_{i=1}^{r} a_i T^i w\right)$$

$$= f(-a_0 w)$$

$$= -a_0 f(w)$$

$$\neq 0,$$

contradizendo (3.3). □

III.4 - MATRIZES DE HANKEL

Dado um K-subconjunto A de Σ^*, a *Matriz de Hankel* $H(A)$: $\Sigma^* \times \Sigma^* \to K$ é definida por

$$H(A)_{v,w} = vwA.$$

A matriz $H(A)$ fornece uma caracterização poderosa dos K-subconjuntos reconhecíveis. No caso em que Σ é unitário, a relação entre matrizes de Hankel e séries racionais são clássicas (ver por exemplo Gantmacher [G1]). O que apresentaremos é a generalização de Fliess de trabalhos de Schutzenberger [S3], Heller [H1] e [H2], Carlyle e Paz [CP1], para um alfabeto qualquer.

Como K é um corpo, $K\langle\langle\Sigma\rangle\rangle$ é um espaço vetorial.

Para cada $w \in \Sigma^*$, definem-se o K-subconjuntos:

$$\text{a } \textit{coluna } C_w = \sum (vwA)\underline{v},$$

$$\text{a } \textit{linha } L_w = \sum (wvA)\underline{v},$$

ou seja, C_w e L_w são a coluna e a linha do índice w de $H(A)$.

O *posto* de $H(A)$ é a dimensão de seu espaço linha, o qual é igual à dimensão do espaço coluna. É resultado da teoria elementar de determinantes (v. Hoffman & Kunze [HK1] que o posto é:

finito, igual a zero se $A = \emptyset$.

finito, igual a um inteiro $n > 0$ se $H(A)$ contém uma submatriz quadrada inversível de ordem n e toda submatriz quadrada de ordem maior que n é singular.

infinito, caso contrário.

Este teorema é devido a Fliess [F1] e [F2].

TEOREMA 4.1 - Seja K um corpo e A um K-subconjunto não nulo de Σ^*. Uma condição necessária e suficiente para que A seja reconhecível é que $H(A)$ tenha posto finito n. Nesse caso, existe um K-Σ-autômato com n estados reconhecendo A, e qualquer K-Σ-autômato que reconheça A tem pelo menos n estados.

DEMONSTRAÇÃO - A condição é necessária:

Seja $A = (Q, I, F, E)$ tal que $|A| = A$. Considere a família $T = \{T_q\}_{q \in Q}$ de K-subconjuntos de Σ^* definidos por:

$$wT_q = (wE^*F)_q$$

Seja $v \in \Sigma^*$ e consideremos a linha L_v. Para todo $w \in \Sigma^*$,

$$wL_v = vwA = IvE^*wE^*F = \sum_{q \in Q} (IvE^*)_q (wE^*F)_q = \sum_{q \in Q} (IvE^*)_q wT_q .$$

Segue que

$$L_v = \sum_{q \in Q} (IvE^*)_q T_q .$$

Portanto, o conjunto finito T gera o espaço-linha de $H(A)$.

donde esse espaço tem dimensão finita $n \leq |T| = |Q|$.

A condição é suficiente:

Seja $A \neq 0$ tal que $H(A)$ tem posto finito n. Então, existem conjuntos $D = \{d_1,\ldots,d_n\}$ e $G = \{g_1,\ldots,g_m\}$ de palavras, tal que a submatriz $G\times D$ de $H(A)$, B, é inversível.

Isto significa que as colunas C_{d_i} são linearmente independentes, portanto geram o espaço-coluna. Assim, para cada $w\in\Sigma^*$, existe um único vetor coluna $m(w) = (m_1(w), \ldots, m_n(w))$ tal que

$$C_w = \sum_{i=1}^{n} C_{d_i} m_i(w).$$

Em outras palavras, para todo $v,w\in\Sigma^*$,

$$vwA = \sum_{i=1}^{n} vd_iA\ m_i(w). \tag{4.1}$$

Vamos definir agora duas aplicações $\mu,\chi:\Sigma^* \to M_n(K)$ por:

$$w\mu_{ij} = m_i(wd_j), \tag{4.2}$$

$$w\chi_{ij} = g_iwd_jA, \tag{4.3}$$

Essas aplicações estão ligadas por

$$v\chi w\mu = vw\chi. \tag{4.4}$$

Para provarmos isto, calculemos:

$$\begin{aligned}(v\chi w\mu)_{ij} &= \sum_k v\chi_{ik} w\mu_{kj} \\ &= \sum_k g_i vd_kA\ m_k(wd_j) \\ &= g_i vwd_jA \quad \text{por (4.1)} \\ &= vw\chi_{ij}.\end{aligned}$$

Em particular, $1\chi w\mu = w\chi$, e como $1\chi = B$, que é inversível,

$$w\mu = (1\chi)^{-1} w\chi .$$

Mas então, μ é um morfismo, pois

$$\begin{aligned} v\mu w\mu &= (1\chi)^{-1} v\chi w\mu \\ &= (1\chi)^{-1} vw\chi \\ &= vw\mu . \end{aligned}$$

Considere agora o K-Σ-autômato $A = (n, I, F, \mu)$, onde

$$I_i = d_i A \quad \text{e} \quad F = m(1).$$

Vamos mostrar que $|A| = A$.

Seja $w \in \Sigma^*$. Então,

$$\begin{aligned} w|A| &= Iw\mu F \\ &= \sum_j (Iw\mu)_j F_j \\ &= \sum_j \left(\sum_k d_k A \; m_k(wd_j) \right) m_j(1) \\ &= \sum_j wd_j A \; m_j(1) \\ &= wA . \end{aligned}$$

Portanto A é reconhecido por um K-Σ-autômato com posto de $H(A)$ estados. □

Sobre essa demonstração temos alguns comentários a fazer. Dizemos que dois autômatos $A = (Q, I, F, E)$ e $A' = (Q, I', F', E')$ são *isomorfos* se existe uma matriz inversível $P \in M_Q(K)$ tal que $I' = IP$, $F' = P^{-1}F$ e $wE'^* = P^{-1} wE^* P$, $\forall w \in \Sigma^*$.

Verifica-se imediatamente que isto define uma rela

ção de equivalência em qualquer conjunto de K-Σ-autômatos tal que todos os membros de cada classe reconhecem o mesmo K-subconjunto de Σ^*.

a) Vamos mostrar que, a menos de isomorfismo ,o autômato que se obtem na demonstração é único. Para isso, considere D,G,m(w),I,F,χ,μ,A, como na demonstração e mais conjuntos $D' = \{d'_1,\ldots,d'_n\}$, $G' = \{g'_1,\ldots,g'_n\}$ de palavras tais que a submatriz $G'\times D'$ de $H(A)$ é inversível. De modo análogo à demonstração, obtemos vetores m'(w),I',F', e aplicações χ' e μ'.

Seja P a matriz inversível que transforma a base ordenada $(C_{d_1},\ldots,C_{d_n})$ do espaço coluna em $(C_{d'_1},\ldots,C_{d'_n})$ por

$$C_{d'_i} = \sum_j C_{d_j} P_{ji} \qquad i=1,\ldots,n$$

e Q a matriz inversível que transforma a base do espaço-linha $(L_{g_1},\ldots,L_{g_n})$ em $(L_{g'_1},\ldots,L_{g'_n})$ por

$$L_{g'_i} = \sum_j Q_{ij} L_{g_j} \qquad i=1,\ldots,n.$$

Seja $w\in\Sigma^*$. Calculemos

$$\begin{aligned}
w\chi'_{ij} &= g'_i w d'_j A \\
&= w d'_j L_{g'_i} \\
&= \sum_k Q_{ik} w d'_j L_{g_k} \\
&= \sum_k Q_{ik} g_k w d'_j A \\
&= \sum_k Q_{ik} g_k w C_{d'_j} \\
&= \sum_{k,\ell} Q_{ik} g_k w C_{d_\ell} P_{\ell j} \\
&= \sum_{k,\ell} Q_{ik} g_k w d_\ell P_{\ell j} \\
&= (Qw\chi P)_{ij} \quad ,
\end{aligned}$$

donde

$$w\chi' = Qw\chi P.$$

Portanto,

$$\begin{aligned} w\mu' &= (1\chi')^{-1} w\chi \\ &= P^{-1}(1\chi)^{-1} w\chi P \\ &= P^{-1} w\mu P. \end{aligned}$$

Agora,

$$\begin{aligned} I_i' &= d_i' A \\ &= 1C_{d_i'} \\ &= \sum_j 1C_{d_j} P_{ji} \\ &= \sum_j d_j A\ P_{ji} \\ &= IP. \end{aligned}$$

Finalmente, lembrando que $F = m(1)$ é o único vetor satisfazendo

$$C_1 = \sum_j C_{d_j} F_j,$$

vem:

$$\begin{aligned} C_1 &= \sum_j C_{d_j'} F_j' \\ &= \sum_{j,k} C_{d_k} P_{kj} F_j' \\ &= \sum_k C_{d_k} P_{kj} F_j' \\ &= \sum_k C_{d_k} (PF')_k \end{aligned}$$

donde

$$F = PF'.$$

b) Da mesma forma que usamos o espaço coluna de $H(A)$, com a

expressão (4.1), poderíamos construir o autômato a partir do espaço linha, com os mesmos conjuntos D e G. Assim, poderíamos obter, para cada palavra w um vetor linha m'(w) tal que

$$L_w = \sum_i L_{g_i} m'_i(w),$$

e um autômato $A' = (n, I', F', \mu')$, onde

$$I' = m'(1), \quad F'_i = g_i A$$

e o morfismo μ' dado por

$$(w\mu')_{ij} = m'_j(g_i w).$$

Este morfismo satisfaz

$$w\mu' w\chi = vw\chi,$$

onde χ é a aplicação definida no teorema.

Verifica-se que A e A' são isomorfos, sendo a ligação feita pela matriz $B = 1\chi$.

c) Em vista das observações anteriores, chamamos de *autômato reduzido* de A qualquer autômato com posto de $H(A)$ estados.

d) Schutzenberger [S3] dá uma construção completamente diferente para um autômato reduzido.

Dados $A, B \in N\langle\langle\Sigma\rangle\rangle$, definem-se os N-subconjuntos

$$\min(A,B) = \sum \min(xA, xB)\underline{x}, \quad \text{e}$$

$$\max(A,B) = \sum \max(xA, xB)\underline{x}.$$

Em seu livro, Eilenberg conjectura que $Rec_N\Sigma$ não é fechado por min e max. A conjectura se baseia no seguinte: na mesma secção do livro encontra-se provado (por redução ao Problema de Correspondência de Post) que dados N-Σ-autômatos A e B, é indecidível se $|A| \leq |B|$, isto é, se $x|A| \leq x|B|$

para toda palavra x. Mas $|A| \leq |B|$ é equivalente a

$$\max(|A|,|B|) = |B|$$

e,ainda equivalente a $\min(|A|,|B|) = |A|$. Portanto, se pudéssemos construir, por exemplo, em N-Σ-autômato reconhecendo $\max(|A|,|B|)$ a decisão quanto à igualdade poderia ser feita, pelo Teorema da Igualdade. Assim, uma eventual prova de que max(A,B) é reconhecível, não poderia ser construtiva, e em Teoria de Autômatos isto até agora não existe.

O exemplo que vamos mostrar é aplicação imediata da condição necessária do Teorema 1 e prova a conjectura de Eilenberg.

Considere os N-subconjuntos de $\{\sigma,\tau\}$

$$A = \Sigma |x|_\sigma \underline{x} \quad \text{e}$$

$$B = \Sigma |x|_\tau \underline{x},$$

reconhecíveis, por II.(2.9). Vamos mostrar que max(A,B) não é Q-reconhecível, portanto, não é N-reconhecível podendo-se provar o mesmo de modo análogo para min(A,B).

Temos que $C = \max(A,B) = \Sigma \max(|x|_\sigma, |x|_\tau)\,\underline{x}$.

Para cada inteiro positivo n, considere a seguinte submatriz de $H(C)$:

$M =$

	1	τ	τ^2	...	τ^j	...	τ^n
1	0	1	2	...	j	...	n
σ	1	1	2	...	j	...	n
σ^2	2	2	2	...	j	...	n
.	.	.	.		.		.
.	.	.	.		.		.
.	.	.	.		.		.
σ^i	i	i	i	..	max(i,j)	..	n
.	.	.	.		.		.
.	.	.	.		.		.
.	.	.	.		.		.
σ^n	n	n	n	...	n	...	n

Vamos mostrar que det $M \neq 0$. Para isso, vamos aplicar sucessivamente, para $i=0,1,\ldots,n-1$ a operação elementar de linhas substituição de $L_{\sigma^{n-i}}$ por $L_{\sigma^{n-i}} - L_{\sigma^{n-i-1}}$. Obtemos

$$M' = \begin{array}{c|cccccccc} & 1 & \tau & \tau^2 & \cdots & \tau^j & \cdots & \tau^n \\ \hline 1 & 0 & 1 & 2 & \cdots & j & \cdots & n \\ \sigma & 1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ \sigma^2 & 1 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots \\ \sigma^i & 1 & 1 & 1 & \cdots & \begin{cases} 1 \text{ se } i>j \\ 0 \text{ se } i\leq j \end{cases} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots \\ n & 1 & 1 & 1 & & 1 & & 0 \end{array}$$

Desenvolvendo pela última coluna vem

$$\det(M') = (-1)^{n+1} n = \det(M),$$

portanto M é inversível. Assim, para cada $n > 0$, existe uma submatriz inversível de ordem $>n$ em $H(C)$, donde $H(C)$ tem posto infinito, e pelo teorema, $C \notin Rec_Q \Sigma$. Como $Rec_N \Sigma \subseteq Rec_Q \Sigma$, C não é N-reconhecível.

Uma outra forma de provarmos que $\min(A,B) \notin Rec_Q \Sigma$ é lembrando que $\max(A,B) = A+B-\min(A,B)$. Assim, se $\min(A,B)$ fosse reconhecível, como $Rec_Q \Sigma$ é um anel, $\max(A,B)$ o seria, em contradição com o que demonstramos.

Finalmente, por meio de uma combinação feliz entre o Teorema 2.2 e o Teorema 1, obtemos a possibilidade de uma construção efetiva de um autômato reduzido, com comportamento idêntico ao de um autômato dado.

PROPOSIÇÃO 4.2 - Seja A um K-Σ-autômato com k estados e comportamento $A \neq \emptyset$, e $X = \{x \in \Sigma^* \mid |x| \leq 3k-3\}$. Então, existem conjuntos $D, G \subseteq X$, $|D| = |G| = r$, onde r = posto $H(A)$,

tais que a submatriz G×D de $H(A)$ é inversível.

DEMONSTRAÇÃO - Seja H_i a submatriz $X_i \times X_i$ de $H(A)$, onde $X_i = \{x \in \Sigma^* \mid |x| \leq i\}$, e n_i = posto H_i, $i \geq 0$. Se $n_m = 0$, então $H_m = 0$, portanto para toda palavra $w \in X_m$,

$$0 = (H_m)_{w,1} = wA$$

Pelo Teorema 2.1, segue que $A = \emptyset$, o que não é nosso caso. Portanto, $n_m \geq 1$. Podemos também supor $m > 1$, caso contrário obviamente A é reduzido.

Considere a sequência:

$$1 \leq n_m \leq n_{2m-2} \leq n_{2m-1} \leq n_{2m} \leq n_{2m+1} \leq \ldots \leq n_{3m-2} \leq r \leq m$$

onde $n_i \leq n_j$ se $i < j$, pois H_i é submatriz de H_j, $n_i < r$ porque H_i é submatriz de $H(A)$ e $r \leq m$ vale pelo Teorema 1. As desigualdades não podem ser todas estritas, e, em particular, existe $2m-2 \leq \ell \leq 3m-3$ tal que $n_\ell = n_{\ell+1} = n$.

É claro que $n \leq r$. Sejam $D = \{d_1, \ldots, d_n\}$, $G = \{g_1, \ldots, g_n\}$, tais que $D, G \subseteq X_\ell$ e a submatriz G×D de H_ℓ é inversível (isto existe porque posto $H_\ell = n$). Então, como posto de $H_{\ell+1} = n$, as colunas $\{C_{d_i}\}$ formam uma base do espaço coluna de $H_{\ell+1}$.

Segue que para todo w, $|w| \leq \ell+1$, existe um vetor $m(w) \subseteq K^{n \times 1}$ tal que

$$C_w = \sum_i C_{d_i} m_i(w) \qquad \text{(colunas restritas a } X_{\ell+1})$$

o que significa que, para todo v tal que $|v| \leq \ell+1$,

$$vwA = \sum_i vd_iA \; m_i(w), \tag{4.5}$$

Vamos construir um autômato $A' = (n, I, F, E)$ por:

$$I_i = d_iA; \; F_i = m_i(1); \; \sigma E_{ij} = m_i(\sigma d_j)$$

(como $|d_j| \leq \ell$, $\sigma d_j \in X_{\ell+1}$ e $m(\sigma d_j)$ está definido).

Agora, para $x \in X_{\ell+1}$ vem que $(IxE^*)_j = xd_jA$. Com efeito, se $x = 1$ isto é imediato; indutivamente: se $x = y\sigma$,

$$\begin{aligned}(IxE^*)_j &= (IyE^*\sigma E^*)\\ &= \sum_i (IyE^*)_i \sigma E_{ij}\\ &= \sum_i yd_iA\, m_i(\sigma d_j) \quad \text{(por hipótese de indução)}\\ &= y\sigma d_jA \quad \text{por (4.5)}\\ &= xd_jA.\end{aligned}$$

Assim,

$$\begin{aligned}x|A'| &= IxE^*F\\ &= \sum_j xd_jA\, m_j(1)\\ &= xA \quad \text{por (4.5)},\end{aligned}$$

para todo x tal que $|x| \leq \ell+1$. Como $\ell+1 \geq 2m-1$, vem que

$$x|A'|_k = xA$$

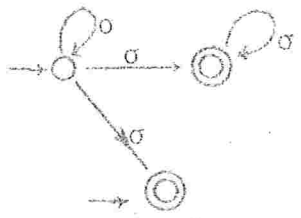
para todo x tal que $|x| \leq 2m-1$. Como A tem m estados e A' tem $n \leq m$ estados, pelo Teorema da Igualdade (teorema (2.2)) vem que $|A'| = A$. Assim, pelo Teorema 1, devemos ter $n \geq r$. Portanto $n = r$. □

Vamos apresentar dois exemplos de autômatos reduzidos, sobre Q (eles serão Z-autômatos, na verdade).

EXEMPLO 4.1 - Considere o N-subconjunto de σ^*:

$$A = \sum_{n\geq 0} (n+1)\underline{\sigma}^n.$$

Ele é o comportamento do N-autômato



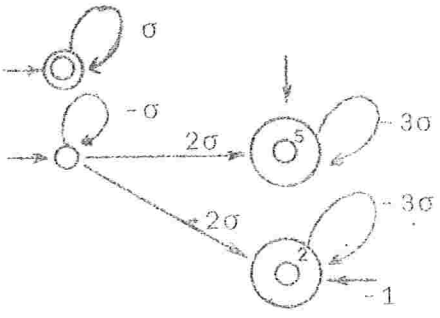
e pode-se verificar que nenhum N-autômato com dois estados reconhece A.

Se considerarmos $A \in Q\langle\langle\sigma\rangle\rangle$ e construirmos parte da matriz de Hankel:

	1	σ	σ^2	σ^3	σ^4	σ^5	σ^6
1	1	2	3	4	5	6	7
σ	2	3	4	5	6	7	8
σ^2	3	4	5	6	7	8	9
σ^3	4	5	6	7	8	9	10
σ^4	5	6	7	8	9	10	11
σ^5	6	7	8	9	10	11	12
σ^6	7	8	9	10	11	12	13

verificamos que ela tem posto 2 e a submatriz $\{1,\sigma\} \times \{1,\sigma\}$ é inversível. Construindo-se o Q-autômato reduzido obtem-se

EXEMPLO 4.2 - Considere o Q-Σ-autômato com 4 estados



seu comportamento A é dado por:

$$\sigma^n A = \begin{cases} 4 \text{ se } n \text{ é par} \\ \\ -2 \text{ se } n \text{ é ímpar} \end{cases}$$

Construindo-se a submatriz $\{1,\sigma,\ldots,\sigma^8\}^2$ de $H(A)$, verifica-se que esta tem posto 2 e obtem-se o autômato reduzido,

a partir da submatriz inversível $\{1,\sigma\}\times\{1,\sigma\}$.

"I ask you, sweet child, has anyone ever seen a Great White Wooly Wugga-Wugga on the plains of Astrakhan?"

Leslie Charteris
"Enter the Saint"

CAPÍTULO IV

K-SUBCONJUNTOS LIMITADOS

IV.1 - INTRODUÇÃO

O conceito de K-subconjunto limitado, na forma como estudaremos neste capítulo, não ocorre na literatura. Nosso estudo foi motivado através de duas idéias distintas, e o conceito de "limitado" foi uma forma de unificar nosso estudo.

A primeira idéia surgiu da relevância que tem na teoria os K-subconjuntos reconhecíveis de imagem finita no caso particular dos semianéis N e M. Para o semianel N, nossa atenção foi chamada por um teorema de Eilenberg. O semianel M aparece no tratamento de uma questão na Teoria de Autômatos Finitos.

A segunda idéia consistiu na tentativa de generalizar o monóide sintático para K-subconjuntos de Σ^*. A generalização que apresentamos, bastante elementar, não generaliza completamente a propriedade fundamental vista na Proposição II.1.2, ou seja, a de que um subconjunto de Σ^* é reconhecível sse seu monóide sintático é finito. Aliás, o nosso monóide sintático de um K-subconjunto é finito somente se o dito K-subconjunto for reconhecível e de imagem finita. Ocor

re que nos dois semianéis citados acima vale a recíproca, isto é, todo K-subconjunto reconhecível de imagem finita tem o monóide sintático finito. Isto nos motivou a definir K-subconjunto limitado como aquele cujo monóide sintático é finito, o que permite também esperar uma relação com o estudo de autômatos por meio de semigrupos. As propriedades de K-subconjuntos limitados aparecem na secção 2.

Conforme observamos, quando K = N ou K = M, todo K-subconjunto reconhecível com imagem finita é limitado. É natural perguntar se isto vale para qualquer semianel. Não pudemos responder a essa pergunta mas, na secção 3, definindo semianéis limitadores como aqueles que tem a propriedade citada, pudemos provar que eles formam uma classe bastante ampla, incluindo por exemplo todos os corpos. Uma propriedade mais fraca dos semianéis limitadores é de que todo K-subconjunto não-ambíguo tem suporte reconhecível.

A secção 4 ocupa-se de questões particulares sobre N-subconjuntos limitados e tem sua introdução lá mesmo. Alí estão os principais resultados de nosso trabalho, entre os quais uma caracterização de submonóides finitos de $M_n(N)$ obtida por dois métodos inteiramente distintos.

Na secção 5 estudamos os subconjuntos L de Σ^* que tem a propriedade de, para algum $n \in N$, $(1 \cup L)^n = L^*$. Estes são chamados de quase-periódicos e a técnica apresentada numa tentativa de caracterizá-los efetivamente leva ao estudo de M-subconjuntos limitados de Σ^*.

Neste capítulo, K volta a simbolizar um semianel qualquer.

IV.2 - O MONÓIDE SINTÁTICO DE UM K-SUBCONJUNTO DE Σ^*

O monóide sintático é um instrumento fundamental no

estudo de conjuntos reconhecíveis. A razão básica está na Proposição II.1.2 que afirma que um subconjunto de Σ^* é reconhecível sse seu monóide sintático é finito.

Lembramos que se $L \subseteq \Sigma^*$, a congruência sintática $\sim_L$ é definida por

$$x \sim_L y \iff \forall u,v \in \Sigma^*,\ uxv \in L \text{ sse } uyv \in L.$$

O monóide sintático M_L é o quociente $\Sigma^*/\sim_L$.

Uma consequência imediata da definição de congruência sintática é:

(2.1) - Se $\phi: \Sigma^* \to M$ é um epimorfismo de monóides e $L\phi\phi^{-1} = L$, então existe um epimorfismo de M em M_L.

Em particular, temos

(2.2) - Se $A = (Q,I,F,E)$ é um Σ-autômato reconhecendo L, existe um epimorfismo $M_A \to M_L$, onde M_A é o submonóide de $Rel(Q)$, imagem de Σ^* por E^*.

Um estudo sistemático vem sendo feito, relacionando propriedades algébricas de semigrupos finitos com propriedades de linguagens reconhecíveis. Para isso ver Brzozowski & Simon [BS1], McNaughton & Papert [MP1], Schutzenberger [S5], Zalcstein [Z1], McNaughton [M2] e Simon [S7].

Uma vez que K-subconjuntos reconhecíveis são uma generalização de conjuntos reconhecíveis, poder-se-ia esperar uma generalização razoável do monóide sintático. Uma possibilidade é o que faremos a seguir.

Dado um K-subconjunto A de Σ^*, a *congruência sintática* $\sim_A$ de A sobre Σ^* é definida por

(2.3) $$x \sim_A y \iff \text{para todo } u,v \in \Sigma^*,\ uxvA = uyvA.$$

O *monóide sintático* M_A é o quociente $\Sigma^*/\sim_A$. O *re-*

presentador de A é o K-subconjunto $\tilde{A}$ de M_A definido por

$$[x]\tilde{A} = xA.$$

É claro que $\tilde{A}$ está bem definido, e, se $\pi_A:\Sigma^* \to M_A$, é a projeção canônica,

$$A = \pi_A\tilde{A}.$$

Dado um K-Σ-autômato $A = (Q,I,F,E)$ o *monóide de* A, denotado M_A é o submonóide de $M_Q(K)$ imagem de Σ^* por E^*; M_A é gerado por $\{\sigma E/\sigma\in\Sigma\}$.

Deve estar claro que se A é não-ambíguo, $\sim_A = \sim_{s(A)}$ e $M_A = M_{s(A)}$.

A seguinte proposição generaliza (2.1) e (2.2).

PROPOSIÇÃO 2.1 - Seja M um monóide, A um K-subconjunto de Σ^*. Se $\phi:\Sigma^* \to M$ é um epimorfismo e existe um K-subconjunto A de M tal que $A = \phi A'$, então existe um epimorfismo $\psi:M \to M_A$, tal que $A' = \psi\tilde{A}$. Em particular, se A é reconhecido por $A = (Q,I,F,E)$, existe um epimorfismo $M_A \to M_A$.

DEMONSTRAÇÃO - Se $x,y\in\Sigma^*$ e $x\phi = y\phi$, então para todo $u,v\in\Sigma^*$,

$$uxvA = (uxv)\phi A' = (u\phi)(x\phi)(v\phi)A' = (u\phi)(y\phi)(v\phi)A' = (uyv)\phi A' = uyvA,$$

donde $x\sim_A y$. Pela Proposição I.2.1, existe um epimorfismo $\psi: M\to M_A$, tal que $\phi\psi = \pi_A$.

Dado $x\in M$, se $y\in\Sigma^*$ é tal que $y\phi = x$, temos que

$$x\psi\tilde{A} = y\phi\psi\tilde{A} = yA = y\phi A' = xA',$$

portanto

$$A' = \psi\tilde{A}.$$

No caso de A, temos $E^*:\Sigma^* \to M_A$ e A' definido para cada elemento xE^* de M_A por

$$xE^*A' = IxE^*F. \qquad \square$$

A definição de congruência sintática feita aqui para K-subconjuntos de Σ^* pode ser feita para K-subconjuntos de um monoide qualquer. Não nos preocupamos aqui com esta possibilidade de generalização.

Recordemos que, por definição, um K-subconjunto de Σ^* é uma função $\Sigma^* \to K$. Assim, está claro o significado da imagem de um K-subconjunto A, $\mathrm{Im}\, A = \{xA/x \in \Sigma^*\}$.

A generalização do monóide sintático que apresentamos não leva em conta nenhum aspecto da estrutura do semianel. Com efeito, se A é um K-subconjunto e ϕ é uma aplicação de K num semianel K' que é injetora restrita à imagem de A, claramente, $M_A = M_{A\phi}$. Além disso, o monóide sintático de um K-subconjunto não reflete sua estrutura de modo tão bom quanto ao monóide sintático de um subconjunto de Σ^*.

PROPOSIÇÃO 2.2 - Seja A um K-subconjunto de σ^* com imagem infinita. Então a congruência $\sim_A$ é trivial e $M_A = \sigma^*$.

DEMONSTRAÇÃO - Sejam $0 \leq n < m$ inteiros. Afirmamos que σ^n e σ^m não são congruentes módulo $\sim_A$. Se isso não acontecesse, para todo $r \geq 0$ teríamos $\sigma^n\sigma^r \sim_A \sigma^m\sigma^r$, isto é, $\sigma^{n+r}A = \sigma^{m+r}A$. Mas então a sequência $\{\sigma^k A\}_{k\geq n}$ seria periódica, com período $\leq m-n$, e teria, portanto, uma quantidade finita de termos distintos. Daí teríamos $\mathrm{Im}\, A = \{\sigma^k A/k<m\}$ finita, contradizendo a hipótese. □

Assim, com alfabeto unitário, para K-subconjuntos com imagem infinita, o monóide sintático não traz informação útil. Com alfabeto maiores, podem ocorrer monóides sintáticos não isomorfos, mas eles serão infinitos sempre que a imagem do K-subconjunto for infinita (Proposição 3), e com estrutura independente do K-subconjunto ser ou não reconhecível.

Vamos então restringir-nos ao K-subconjuntos cujo

monóide é finito. O que se segue mostra que eles têm relação íntima com conjuntos reconhecíveis.

Um K-subconjunto de Σ^* é *limitado* sse seu monóide sintático é finito. A família dos K-subconjuntos limitados é denotada $\mathrm{Lim}_K\Sigma$, veremos adiante que $\mathrm{Lim}_K\Sigma$ *não* é um subsemianel de $K\langle\langle\Sigma\rangle\rangle$.

PROPOSIÇÃO 2.3 - Seja $A\in\mathrm{Lim}_K\Sigma$. Valem as seguintes propriedades:

(a) A é reconhecível $(\mathrm{Lim}_K\Sigma\subseteq\mathrm{Rec}_K\Sigma)$
(b) Im A é finita
(c) Para todo $k\in K$, o conjunto $kA^{-1} = \{x\in\Sigma^*/xA=k\}$ é reconhecível
(d) $A = k_1A_1+k_2A_2+\ldots k_nA_n$, com $k_i\in K$, $i=1,\ldots,n$, cada $A_i\in\mathrm{Rec}_K\Sigma$, não-ambíguo, de suporte reconhecível, e $A_i\cap A_j = 0$ se $i\neq j$.

DEMONSTRAÇÃO - (a)-Considere o K-Σ-autômato $A = (M,\delta^1,F,\mu)$, onde

$$F_a = a\tilde{A},\ \forall a\in M, \quad \text{e}$$

$$(2.3)\qquad x\mu_{ab} = \begin{cases} 1 \text{ se } a\cdot(x\pi_A) = b \\ 0 \text{ caso contrário} \end{cases} \qquad \forall x\in\Sigma^*,\ a,b\in M.$$

Verifica-se imediatamente que μ é um morfismo.

Assim, para todo $x\in\Sigma^*$,

$$\begin{aligned} x|A| &= \delta^1 x\mu F \\ &= \delta^{x\pi_A F} \\ &= x\pi_A\tilde{A} \\ &= xA, \end{aligned}$$

portanto A é reconhecível.

(b)- Como $A = \pi_{\tilde{A}}\tilde{A}$ e $\tilde{A}$ têm por domínio o conjunto finito M, Im A = Im $\tilde{A}$ é finita.

(c) Seja $k \in K$. Se $k \notin$ Im A, $kA^{-1} = \emptyset$ que é reconhecível. Caso contrário, considere o B-Σ-autômato $A_k = (M, \delta^1, F', \mu)$, onde μ é definido em (2.3) e

$$F'_a = 1 \text{ sse } a\tilde{A} = k.$$

Segue imediatamente que $x|A_k| = 1$ sse $xA = k$, donde $s(A) = kA^{-1}$. Pela Proposição II.2.1, s(A) é reconhecível.

(d) Podemos, em vista de (b), escrever

$$\text{Im } A = \{k_1, \ldots, k_n\}.$$

Por (c), k_iA^{-1} é um conjunto reconhecível, para cada i, e claramente

$$k_iA^{-1} \cap k_jA^{-1} = \emptyset, \text{ se } i \neq j. \tag{2.4}$$

Seja $A_i = \chi_{k_iA^{-1}} \in \text{Rec}_K\Sigma$, conforme a Proposição II.2.6. Então (2.4) se transforma em $A_i \cap A_j = 0$ se $i \neq j$ e verifica-se que

$$A = k_1A_1 + \ldots + k_nA_n. \qquad \square$$

Um K-Σ-*autômato determinístico* é da forma

$A = (Q, I, F, E)$, onde

(a) $I = \delta^q$ para algum $q \in Q$,

(b) Para todo $\sigma \in \Sigma$, $p, q \in Q$, $\sigma E_{pq} \in \{0,1\}$,

(c) Para todo $\sigma \in \Sigma$, $p \in Q$, existe no máximo um estado q tal que $\sigma E_{pq} = 1$.

As condições (b) e (c) são, conjuntamente, equivalentes a

(b') Para todo $x \in \Sigma^*$, $p, q \in Q$, $xE^*_{pq} \in \{0,1\}$,

(b') Para todo $x \in \Sigma^*$, $p \in Q$, existe no máximo um estado q tal que $xE^*_{pq} = 1$.

PROPOSIÇÃO 2.4 - Um K-subconjunto de Σ^* é limitado sse for reconhecido por um autômato determinístico.

DEMONSTRAÇÃO - Se $A \in Lim_K \Sigma$, o autômato reconhecendo A construído na demonstração da Proposição 3 (a) é determinístico.

Se A é um autômato determinístico reconhecendo A, (b') mostra que $M_A \subset M_Q(B)$ (inclusão de conjuntos), portanto é finito. Pela Proposição 1, M_A é imagem homomórfica de M_A, logo M_A é finita. □

Um fato usado na demonstração acima é um método básico, que vale a pena ser ressaltado:

LEMA 2.5 - Seja A um K-Σ-autômato, reconhecendo A. Se M_A é finito então A é limitado.

PROPOSIÇÃO 2.6 - Dados $A, A' \in Lim_K \Sigma$, $k \in K$, os K-subconjuntos kA, Ak, A+A' e A∩A' são limitados.

DEMONSTRAÇÃO - Sejam $A = (Q, I, F, E)$ e $A' = (Q', I', F', E')$, com $Q \cap Q' = \emptyset$, autômatos determinísticos reconhecendo A e A'.

O autômato determinístico $Ak = (Q, I, Fk, E)$ reconhece Ak e $kA = (Q, I, kF, E)$ reconhece kA, mesmo quando K não é comutativo.

Para A+A' temos o autômato A+A', construído na Proposição II.3.2. É imediato da construção que

$$M_{A+A'} = M_A \times M_{A'} .$$

Como A e A' são determinísticos, seus monóides são finitos, donde $M_{A+A'}$ é finito. Pelo Lema 5, A+A' é limitado.

Finalmente, o autômato $A \cap A'$ construído na Proposição II.3.6 é determinístico e reconhece $A \cap A'$ mesmo se K não for comutativo. □

Cabe aqui observar que nem sempre o produto de K-subconjutos limitados é limitado. Por exemplo, se considerarmos o N-subconjunto de Σ^*.

$$\sum_{x \in \Sigma^*} \underline{x},$$

reconhecido pelo autômato determinístico:

o N-subconjunto $A^2 = \sum (|x|+1)\underline{x}$ não tem imagem finita, portanto não é limitado.

PROPOSIÇÃO 2.7 - Seja A um K-subconjunto de Σ^*. São equivalentes:

(a) A é limitado.

(b) Im A é finita e, para todo $k \in K$, o conjunto, kA^{-1} é reconhecível.

(c) $A = k_1A_1 + \ldots K_nA_n$, $k_i \in K$, $A_i \in Rec_K\Sigma$, não-ambíguos, com suporte reconhecível, e $k_i \neq k_j$, $s(A_i) \cap s(A_j) = \emptyset$ se $i \neq j$.

(d) $A = k_1A_1 + \ldots k_mA_m$, $k_i \in K$, $A_i \in Rec_K\Sigma$, não-ambíguos, com suporte reconhecível.

(e) $A = k_1A_1 + \ldots k_nA_n$, $k_i \in K$, $A_i \in Lim_K\Sigma$.

(f) A é o comportamento de um K-Σ-autômato de suspense.

DEMONSTRAÇÃO - (a) implica (b), Proposição 3.

(b) implica (c), ver demonstração da Proposição 3 (d).

(c) implica (d), nada a demonstrar.

(d) implica (e). Como cada A_i é não-ambíguo, $M_{A_i} = M_{s(A_i)}$, e como $s(A_i)$ é reconhecível, M_{A_i} é finito. Então cada A_i é limitado.

(e) implica (a). Aplica-se indutivamente a Proposição 6.
(a) equivale a (f). Proposição 4. □

IV.3 - SEMIANÉIS LIMITADORES

A Proposição 2.7 diz, entre outras coisas, que se A é limitado então Im A é finita e A é reconhecível. É uma questão relevante saber se todo K-subconjunto reconhecível de imagem finita é limitado. Não pudemos provar que isto vale para todo semianel K, nem encontramos um contra-exemplo. O que faremos agora é estudar a classe dos semianéis para os quais essa recíproca é válida.

Chamamos um semianel K de *limitador* se todo K-subconjunto reconhecível de Σ^* com imagem finita é limitado, qualquer que seja o alfabeto finito Σ.

PROPOSIÇÃO 3.1 - Todo subsemianel de umsemianel limitador é um semianel limitador.

DEMONSTRAÇÃO - Imediata a partir da caracterização na Proposição 2.7 (d). □

PROPOSIÇÃO 3.2 - Se K é finito, então K é limitador e

$$\mathrm{Lim}_K\Sigma = \mathrm{Rec}_K\Sigma.$$

DEMONSTRAÇÃO - Seja $A \in \mathrm{Rec}_K\Sigma$. Como K é finito Im A é finita. Se A é um K-Σ-autômato reconhecendo A , M_A é um monóide de matrizes com coeficientes em K, portanto, é finito. Pelo Lema 2.5, A é limitado. Segue que K é limitador e $\mathrm{Rec}_K\Sigma \subseteq \mathrm{Lim}_K\Sigma$. A igualdade decorre da Proposição 2.3, (a). □

Uma consequência desta proposição e da Proposição 2.6 é que se K é finito, $\mathrm{Rec}_K\Sigma$ é fechado em relação à operação $\cap$.

PROPOSIÇÃO 3.3 - Um semianel é limitador sse todo subsemia-

nel finitamente gerado o for.

DEMONSTRAÇÃO - A parte "só se" fica por conta da Proposição 1.

Se todo subsemianel finitamente gerado de K é limitador, considere um K-subconjunto A,reconhecido por A=(Q,I,F,E), com imagem finita. Seja K_1 o subsemianel de K gerado por todos os coeficientes em I,F e das matrizes σE. Então, A é um K_1-Σ-autômato, e $A \in Rec_{K_1}\Sigma$. Como K_1 é finitamente gerado, A é limitado. □

PROPOSIÇÃO 3.4 - Dado $A \in Rec_K\Sigma$ com imagem finita, se existir um semianel limitador K_1 e um morfismo $\psi: K \to K_1$, que seja injetor restrito à imagem de A, então A é limitado. Portanto, se para todo subconjunto finito $F \subseteq K$ existe um semianel K_1 e $\psi: K \to K_1$ injetor restrito a F então K é limitador.

DEMONSTRAÇÃO - Seja Im $A = \{k_1, \ldots, k_n\}$. O K_1-subconjunto $A\psi$ é reconhecível (Proposição II.3.9),e Im $A\psi = \{k_1\psi, \ldots, k_n\psi\}$ é finita. Como K_1 é limitador, $A\psi$ é limitado , portanto $A\psi = k_1\psi A_1 + \ldots + k_n\psi A_n$, conforme a Proposição 2.7, com $s(A_i) \cap s(A_j) = \emptyset$ se $i \neq j$. Observe que, como $\psi|_{Im\,A}$ é injetora, $k_i\psi \neq k_j\psi$ se $i \neq j$. Como $s(A_i)$ é reconhecível

$$A'_i = \chi_{s(A_i)} \in Rec_K\Sigma.$$

É imediato que $A = k_1A'_1 + \ldots + k_nA'_n$, e é limitado, pela Proposição 2.7. □

Apresentamos aqui alguns exemplos de semianéis limitadores infinitos:

Z - Se $F \subset Z$ é finito, tomando-se $p = \max\{|x| \mid x \in F\}$, o epimorfismo canônico $Z \to Z_{2p+1}$ é injetor restrito a F. Aplicando-se a Proposição 4, vem que Z é limitador.

N - (ver secção I.4). Se $F \subset N$ é finito, seja

$$n = \max\{x \in F / x \neq \infty\}.$$

O morfismo $\phi_n : N \to N_n$ definido por

$$x\phi_n = \begin{cases} x \text{ se } x \neq n \text{ ou } x = \infty \\ \\ n \text{ caso contrário.} \end{cases}$$

é injetor restrito a F. Novamente, pela Proposição 4, N é limitador.

R - (ver secção I.4). Seja K um subsemianel de R, gerado pelo conjunto finito $\{k_1, \ldots, k_n\}$. Os elementos de K são somas de produtos dos k_i. Mas a soma em R é definida por

$$a \oplus b = \min(a,b),$$

portanto, os elementos de K são produtos dos k_i. Mas o produto em R é a soma de $R_+ \cup \infty$. Chamemos de α o menor entre os k_i não nulos.

Seja agora $F \subset K$, finito e n um inteiro maior que todos os membros de $F - \infty$. Seja

$$K_n = \{x \in K / x \leq n \text{ ou } x = \infty\}.$$

Qualquer soma dos k_i com mais de n/α parcelas tem valor maior que n, portanto, K_n é finito. Vamos dar a K_n uma estrutura de semianel por:

$$a \oplus b = \min(a,b)$$

$$a \otimes b = \begin{cases} a+b \text{ se } a+b \in K_n \\ \\ n \text{ caso contrário.} \end{cases}$$

O epimorfismo $\phi_n : K \to K_n$ definido pela expressão (3.1) é injetor restrito a F. Aplicando-se a Proposição 4, K é limitador, e pela Proposição 3, R é limitador.

M - é um subsemianel de R, e pela Proposição 1 é limitador.

PROPOSIÇÃO 3.5 - Todo corpo (comutativo) K é limitador.

DEMONSTRAÇÃO - Seja $A \in Rec_K \Sigma$ com imagem finita. Voltemos a demonstração do Teorema III.4.1.Para todo $x \in \Sigma^*$, a matriz $x\chi \in (ImA)^{n \times n}$, onde n é o posto da matriz de Hankel $H(A)$, portanto, temos um conjunto finito de matrizes $x\chi$. Como $x\mu = (1\chi)^{-1} x\chi$, existe uma quantidade finita de matrizes $x\mu$, e o autômato A, construído nesse teorema,reconhecendo A, tem o monóide finito. Pelo Lema 2.5, A é limitado. □

Observe que isto dá outra demonstração de que Z é limitador.

Ainda no caso de corpos, temos uma caracterização de K-subconjuntos limitados em termos da matriz de Hankel.

Utilizaremos a notação do Teorema III.4.1.

PROPOSIÇÃO 3.6 - Seja K um corpo, A um K-subconjunto de Σ^*. São equivalentes:

(a) A é limitado
(b) $H(A)$ tem uma quantidade finita de colunas distintas
(c) $H(A)$ tem uma quantidade finita de linhas distintas
(d) $H(A)$ tem posto finito e uma quantidade finita de entradas $H(A)_{vw}$ distintas.

DEMONSTRAÇÃO - (a) implica (b). Como A é limitado, $H(A)$ tem posto finito n e existem conjuntos

$$D = \{d_1, \ldots, d_n\}, \quad G = \{g_1, \ldots, g_n\}$$

de palavras como no Teorema III.4.1. Toda coluna C_w é univocamente determinada pelo vetor $m(w)$, que satisfaz

$$g(w) = Bm(w)$$

onde $B_{ij} = g_i d_j A$ e $g(w)$ é o vetor coluna $(g_1 wA, \ldots, g_n wA)$. Co

mo B é inversível, existe uma correspondência biunívoca entre os vetores m(w) e g(w). Mas os coeficientes de g(w) estão em Im A que é finita. Portanto, existe uma quantidade finita desses vetores e consequentemente de colunas distintas.

(b) implica (c). Sejam $d_1,\ldots,d_k$ palavras tais que para todo $w\in\Sigma^*$, $C_w = C_{d_i}$ para algum i. Então toda linha L_w fica determinada pelo vetor $d(w) = (wd_1A,..,wd_kA)$. Mas, $wd_iA = 1C_{wd_i} = 1C_{d_j} = d_jA$ para algum j. Portanto, os coeficientes dos vetores d(w) são extraídos do conjunto $\{d_1A,\ldots,d_kA\}$ logo existe um número finito de d(w)'s. Portanto, número finito de linhas.

(c) implica (d). Se $H(A)$ tem número finito de linhas distintas, claramente tem posto finito. Ainda, se $g_1,\ldots,g_r$ são tais que $L_{g_1},\ldots,L_{g_r}$ são representantes de todas as linhas, para todo v,w, $H(A)_{vw} = vwA = 1L_{vw} = 1L_{g_1} = g_iA$, para algum i. Portanto, as entradas de $H(A)$ são $\{g_1A,\ldots,g_nA\}$.

(d) implica (a). Se $H(A)$ tem posto finito, A é reconhecível. Como $H(A)$ tem número finito de entradas, Im A é finita. Já que K é limitador (Proposição 5), A é limitado. □

PROPOSIÇÃO 3.7 - Se K é limitador e $A\in K\langle\langle\Sigma\rangle\rangle$ é não-ambíguo, então A é reconhecível sse s(A) é uma linguagem reconhecível.

DEMONSTRAÇÃO - Se s(A) é reconhecível, A é reconhecível, pela Proposição II.2.6. Se A é não-ambíguo, Im $A\subseteq\{0,1\}$ é finita, e sendo A reconhecível, como K é limitador, A é limitado. Pela Proposição 2.7, $A = 1A_1+0A_2 = A_1$, com $s(A_1)$ e $s(A_2)$ reconhecíveis. Então s(A) é reconhecível. □

PROPOSIÇÃO 3.8 - Se K é limitador e K_1 um subsemianel de K, então, $\mathrm{Lim}_K\Sigma\cap K_1\langle\langle\Sigma\rangle\rangle = \mathrm{Lim}_{K_1}\Sigma$.

DEMONSTRAÇÃO - Dado $A\in \mathrm{Lim}_K\Sigma\cap K_1\langle\langle\Sigma\rangle\rangle$, todo K-Σ-autômato de-

terminístico que reconhece A é um K_1-Σ-autômato determinístico. □

PROPOSIÇÃO 3.9 - Se K_1 e K_2 são semianéis limitadores, a soma direta $K_1 \oplus K_2$ é um semianel limitador.

DEMONSTRAÇÃO - Seja A um $K_1 \oplus K_2$-subconjunto reconhecível de Σ^*, de imagem finita. Considere os subsemianéis de $K_1 \oplus K_2$, $K_1' = K_1 \oplus 0$ e $K_2' = 0 \oplus K_2$, que são, respectivamente, isomorfos a K_1 e K_2, portanto limitadores. Sejam

$$\phi_i : K_1 \oplus K_2 \to K_i', \quad i=1,2$$

as projeções canônicas. Então, $A = A\phi_1 + A\phi_2$. Como A é reconhecível de imagem finita, $A\phi_1$ e $A\phi_2$ também o são, e como K_1' e K_2' são limitadores, $A\phi_1$ e $A\phi_2$ são limitados. Portanto, a soma A também o é. □

COROLÁRIO 3.10 - Se $\{K_i\}_{i\in I}$ é uma família qualquer de semianéis limitadores, a soma direta $\oplus_{i\in I} K_i$ também é um semianel limitador.

DEMONSTRAÇÃO - Basta observar que todo subsemianel finitamente gerado de $\oplus_{i\in I} K_i$ é subsemianel de uma soma $\oplus_{i\in J} K_i'$, onde $J \subset I$ é finito e K_i' é um subsemianel de K_i. Basta agora aplicar as Proposições 1, 9 e 3. □

Para a próxima propriedade de semianéis limitadores precisaremos de um resultado de Fliess [F1].

Considere um conjunto finito Q e um semianel K. A aplicação

$$\phi : M_Q(K)\langle\langle\Sigma\rangle\rangle \to M_Q(K\langle\langle\Sigma\rangle\rangle)$$

que a $A \in M_Q(K)\langle\langle\Sigma\rangle\rangle$ associa $A\phi$ dado por

$$x(A\phi)_{pq} = (xA)_{pq}, \quad \forall x \in \Sigma^*, \ p,q \in Q$$

é um isomorfismo de semianéis.

PROPOSIÇÃO 3.11 - (Fliess [F1])- A restrição do isomorfismo

acima a $\mathrm{Rec}_{M_Q(K)}\Sigma$ é um isomorfismo entre $\mathrm{Rec}_{M_Q(K)}\Sigma$ e $M_Q(\mathrm{Rec}_K\Sigma)$.

PROPOSIÇÃO 3.12 - Seja K um semianel limitador e Q um conjunto finito. Então o semianel $M_Q(K)$ é limitador.

DEMONSTRAÇÃO - Seja $A \in \mathrm{Rec}_{M_Q(K)}\Sigma$ com imagem finita. Para cada $p,q \in Q$, o K-subconjunto de Σ^* A_{pq} definido por

$$xA_{pq} = (xA)_{pq}$$

tem imagem finita, e pela Proposição 11, é reconhecível. Portanto, como K é limitador, cada A_{pq} é limitado. Por meio do monomorfismo $\phi: K \to M_Q(K)$ dado por $k\phi = k \cdot I_Q$, onde I_Q é a matriz identidade, temos que cada $A_{pq}\phi$ é um $M_Q(K)$-subconjunto de Σ^*.

Considere agora a família $\{e^{pq}\}_{p,q \in Q} \subset M_Q(K)$ dada por

$$e^{pq}_{ij} = \begin{cases} 1 \text{ se } i=p \text{ e } j=q \\ \\ 0 \text{ caso contrário.} \end{cases}$$

Então,

$$A = \sum_{p,q} e^{pq}(A_{pq}\phi),$$

e é limitado pela Proposição 2.7. □

COROLÁRIO 3.13 - Se K é um corpo, G um grupo finito tal que $\mathrm{car}K \nmid |G|$ então o anel de grupo KG é limitador.

A definição de anel de grupo e os Teoremas de Maschke e Wedderburn podem ser encontrados em Curtis & Reiner [CR1].

DEMONSTRAÇÃO - Pelos teoremas de Maschke e Wedderburn, KG é

isomorfo à soma direta de anéis de matrizes sobre o fecho algébrico de K. Este fecho é limitador, pela Proposição 5, e pela Proposição 12, cada anel de matrizes é limitador. O resultado segue então do Corolário 10. □

O que apresentamos nesta secção consiste essencialmente na busca de propriedades de semianéis limitadores e na tentativa de encontrar algum semianel sem essa propriedade. Isso equivaleria a apresentar um K-subconjunto reconhecível A, com imagem finita tal que kA^{-1} não fosse reconhecível para algum $k \in K$. Não conseguimos esse exemplo, mas, em contrapartida, mostramos que os semianéis limitadores formam uma classe bem ampla.

Outra possibilidade que levamos em conta neste trabalho é a de que todo semianel é limitador. Acontece que, para provarmos isto, caso seja verdade, a única técnica de que dispomos é a de mostrar que toda série formal reconhecível, com imagem finita, é reconhecida por um K-Σ-autômato cujo monóide é finito. Mas temos exemplos de K-Σ-autômatos muito simples, com monóide infinito, que sugerem que essa construção pode depender muito da estrutura do semianel. Por exemplo, considere o Z-σ-autômato $A_a = (2, I, F, E)$, onde

$$I = (-1\ 1),\quad F = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\quad E = \begin{pmatrix} 1 & a-1 \\ 0 & a \end{pmatrix},\quad a \in Z, |a| > 1.$$

Para todo $n \geq 0$,

$$\sigma^n E^* = \begin{pmatrix} 1 & a^n - 1 \\ 0 & a^n \end{pmatrix},$$

portanto M_A é infinito. Mas $\sigma^n |A_a| = 1$, para todo n.

Uma outra forma de tentarmos provar que todo semianel é limitador envolveria uma classificação completa dos semianéis, o que foge do escopo deste trabalho.

IV.4 - O CASO K=N

Os N-subconjuntos de Σ^* foram o ponto de partida da teoria, que levou à generalização para semianéis. Eles foram introduzidos por Chomski e Schutzenberger [CS1], como método para o estudo de linguagens formais. Muitos resultados apresentados nesta dissertação para semianéis quaisquer, e às vezes, para certas classes particulares (anéis ou corpos), são generalização de resultados obtidos inicialmente para N, Z ou Q.

Eilenberg faz um estudo sistemático de $Rec_N\Sigma$ nas secções VI-9 a 12 de seu livro. Nesse estudo ocorre o conceito de N-subconjunto *cotado* ("bounded"), sendo que $A \in N\langle\langle\Sigma\rangle\rangle$ é cotado se existe um natural p tal que $xA \leq p$, para toda palavra x. Isso, para o semianel N é equivalente ao conceito de N-subconjunto de imagem finita. Os N-subconjuntos cotados reconhecíveis (portanto, limitados, pois N é limitador) têm um papel especial na teoria geral em vista do seguinte resultado (Eilenberg [E1], teorema IV.11.1):

TEOREMA - Se A,B são N-subconjuntos reconhecíveis de Σ^* e B é cotado, então o N-subconjunto

$$A-B = \sum \max(xA-xB,0)x$$

é reconhecível.

Observe que a hipótese "cotado" não pode ser totalmente eliminada, pois, se considerarmos as séries em $Rec_N\{\sigma,\tau\}$:

$$A = \sum |x|_\sigma \underline{x}, \quad B = \sum |x|_\tau \underline{x},$$

temos que:

$$C = A \cap A + B \cap B = \sum (|x|_\sigma^2 + |x|_\tau^2)x$$

e

$$D = 2(A \cap B) = \sum 2|x|_\sigma |x|_\tau x$$

são reconhecíveis, mas

$$E = C \dot{-} D = \sum (|x|_\sigma - |x|_\tau)^2 x$$

tem suporte $\{x/|x|_\sigma \neq |x|_\tau\} \notin Rec\Sigma$, portanto, não é reconhecível, pois N é positivo e pelo Corolário II.3.10, todo N-subconjunto reconhecível tem suporte reconhecível.

A demonstração do teorema acima depende de resultados profundos sobre relações racionais e de uma construção que permite a partir de um N-autômato dado obter outro com o mesmo comportamento, em que os vetores iniciais e finais são N-subconjuntos não-ambíguos do conjunto de estados, e todas as arestas tem peso 1. Como não vamos utilizar esses resultados no que se segue, não os reproduzieremos aqui.

Quando trabalhamos com N em problemas discretos, questões de decidabilidade tornam-se relevantes. Um problema que motivou nosso estudo e que enfocaremos aqui é o seguinte:

(4.1) "Dado um N-autômato, pode-se decidir efetivamente se seu comportamento é um N-subconjunto limitado?"

A resposta que obtivemos é afirmativa, e é um corolário da nossa caracterização (Teorema 1) de monóides finitamente gerados de matrizes com coeficientes em N que são finitos.

Inicialmente, na subsecção A, provaremos que o problema de decidir se um N-autômato tem comportamento limitado se reduz ao problema de decidir se um dado conjunto finito de matrizes quadradas em $M_Q(N)$ geram um submonóide finito de $M_Q(N)$.

Assim teremos a seguinte questão:

(4.2) "Dado um conjunto finito de matrizes em $M_Q(N)$, é decidível se ele gera um submonóide finito?"

e a resposta afirmativa à (4.2) implica na resposta afirmativa para (4.1).

Para enunciar nosso resultado fundamental, vamos relembrar que N_2 é o semianel cujo conjunto suporte é $\{0,1,2\}$, com soma $a \oplus_2 b = \min\{a+b,2\}$ e produto $a \otimes_2 b = \min\{ab,2\}$, definidos a partir das operações e ordem de N. A aplicação $\phi_2: N \to N_2$ dada por $a\phi_2 = \min\{a,2\}$ é um morfismo de semianéis. Para todo conjunto finito Q, a aplicação $\psi_2: M_Q(N) \to M_Q(N_2)$ dada por $(A\psi_2)_{pq} = A_{pq}\phi_2$ é um morfismo de monóides. Além disso, valem as inclusões de conjuntos $N_2 \subset N$ e $M_Q(N_2) \subset M_Q(N)$.

Para todo monóide um elemento m é *idempotente* sse $m = m^2$. Dizemos que m é *periódico* sse o submonóide $m^* = \{m^k / k \in N\}$ é finito. Isto equivale a dizer que existem naturais $i<j$ tais que $m^i = m^j$ e também equivale à existência de $k>0$ tal que m^k é idempotente (ver Clifford & Preston, [CP2]). Um *monóide* é *periódico* se todos os seus elementos o são; claramente, todo monóide finito é periódico.

O resultado principal desta secção pode agora ser enunciado:

TEOREMA 4.1 - Um submonóide M de $M_Q(N)$ finitamente gerado é finito sse todo elemento de $M\psi_2$ que é idempotente como matriz em $M_Q(N_2)$ é periódico com matriz em $M_Q(N)$.

Apresentaremos duas demonstrações distintas para o Teorema 1, uma puramente combinatória e outra inteiramente algébrica.

Na subsecção B daremos a demonstração combinatória. Essa demonstração é feita em duas etapas. Primeiro daremos

uma caracterização de matrizes periódicas em $M_Q(N)$ que tem como corolários a existência de uma forma canônica para estas matrizes e a caracterização de matrizes idempotentes em $M_Q(N)$. Isto será feito construindo-se um N-σ-autômato associado a uma matriz dada e trabalhando-se com as arestas desse autômato. Em seguida demonstraremos o Teorema 1 utilizando o clássico Teorema de Ramsey. Combinando-se a caracterização de matrizes periódicas com o Teorema 1, teremos então um processo efetivo para decidir a questão (4.2), e portanto a questão (4.1).

A utilização do Teorema de Ramsey na segunda etapa de nossa demonstração acentua seu caráter combinatório. Esse teorema que é generalização do "Princípio da Casa do Pombo" de Dirichlet , foi descoberto por Ramsey [R1], que o utilizou como lema para obter resultados em Lógica. Sua demonstração foi aperfeiçoada por Erdös e Szekeres [ES1], que lhe deram um contexto combinatório mais coerente. Esse teorema determina, para cada tripla (m,n,k) de naturais um natural R(m,n,k) com uma certa propriedade. Acontece que o valor mínimo ρ(m,n,k) para o qual esta propriedade continua válida só é conhecido para poucas triplas, sendo sua determinação a fonte de uma área, atualmente muito ampla, em Combinatória, a dos problemas extremos. Maiores detalhes históricos e técnicos podem ser encontrados em Feofiloff [F0].

A subsecção C apresenta a demonstração algébrica do Teorema 1, e tem como consequência outro processo de decisão para (4.2). A demonstração também será feita por etapas. Na primeira, caracterizaremos matrizes periódicas sobre um corpo de característica 0 em função de seu polinômio minimal. Em seguida, mostraremos que uma matriz $A \in M_Q(N)$ é periódica sse $A\psi_2$ é periódica em $M_Q(N)$. Em terceiro lugar, provaremos que um submonóide finitamente gerado de $M_Q(N)$ é periódico sse ele satisfaz as condições do Teorema 1. O passo

final é dado com o Teorema de McNaughton-Zalcstein [MZ1] que afirma que "todo monóide periódico de matrizes com coeficientes num corpo é localmente finito". (Um monóide é localmente finito se todos os seus monóides finitamente gerados são finitos).

Este teorema que citamos tem uma história interessante. O Problema de Burnside para grupos é a questão sobre se todo grupo periódico é localmente finito. Este problema tem uma generalização óbvia para semigrupos (monóides). O problema geral para semigrupos foi respondido negativamente em 1944 por Morse e Hedlund [MH] enquanto que o problema para grupos só foi respondido, também negativamente, em 1968 por Novikov e Adjan [NA1]. Porém, é já um resultado clássico, devido a Schur [S2] (ver também [CR1], 36.1), o de que o problema tem resposta afirmativa para grupos de matrizes sobre os complexos. Este resultado foi estendido recentemente por Kaplansky [K1] para matrizes com coeficientes num corpo qualquer, e, como o resultado original, depende fortemente da Teoria de Representações. A demonstração de McNaughton e Zalcstein que generaliza Kaplansky para semigrupos de matrizes depende fortemente do resultado de Kaplansky-Schur.

Estas citações "folclóricas" fornecem um sabor especial ao nosso resultado, uma vez que ele tem demonstrações essencialmente diferentes nos seus métodos. São poucos, por enquanto, os resultados conhecidos onde a possibilidade de troca entre métodos algébricos e combinatórios existem; como exemplo temos a teoria de Krohn-Rhodes [KR1] de decomposição de semigrupos e certos resultados da Teoria dos Grafos (ver Biggs [B2]). Isto dá um encorajamento para uma pesquisa no sentido de obter maior interligação entre esses dois ramos da Matemática.

Na subsecção D apresentamos duas direções distintas para as quais nossas demonstrações se generalizam, com

processos de decisão correspondente. A demonstração combinatória generaliza-se para semianéis graduados, que ali definiremos e a demonstração algébrica para qualquer subsemianel de um corpo.

Finalmente na subsecção E apresentamos uma construção de exemplos não triviais de N-autômatos de comportamento limitados.

Cabe ainda uma observação. No seu trabalho, Eilenberg, ao tratar de N-subconjuntos cotados reconhecíveis, apresenta uma caracterização desses N-subconjuntos. Esta caracterização, no entanto, não é efetiva, ou seja, não dá um algoritmo para decidir (4.1):

PROPOSIÇÃO 4.2 - Um N-subconjunto reconhecível A de Σ^* é cotado sse existe um natural p tal que A é soma de p N-subconjuntos não-ambíguos reconhecíveis.

DEMONSTRAÇÃO - A parte "se" é trivial. A implicação contrária se consegue, observando que, se A é cotado, tomando-se $p = \max \operatorname{Im} A$, pela Proposição 2.7,

$$A = \sum_{1 \le i \le p} i A_i ,$$

onde os A_i são não-ambíguos, reconhecíveis e tem suportes disjuntos dois a dois. Definindo-se para cada $1 \le i \le p$,

$$A'_i = \sum_{j \ge i} A_i ,$$

temos que cada A'_i é não-ambíguo e $A = A'_1 + \ldots + A'_p$. □

IV.4.A) - AUTÔMATOS CONEXOS

Seja K um semianel. Lembramos que todo vetor com coeficientes em K é também um K-subconjunto, portanto tem sentido falarmos no seu suporte.

Um K-Σ-autômato $A = (Q,I,F,E)$ é dito

(a) *Acessível* se para todo $q \in Q$, existe $p \in s(I)$, tal que existe uma trilha de p para q.

(b) *Coacessível* se para todo $q \in Q$, existe $p \in s(F)$, tal que existe uma trilha de q para p.

(c) *Conexo* se for acessível e coacessível.

LEMA 4.3 - Dado um K-Σ-autômato com comportamento não vazio, existe um K-Σ-autômato conexo com o mesmo comportamento, que pode ser construído efetivamente.

DEMONSTRAÇÃO - Seja $A = (Q,I,F,E)$ e $n = |Q|$.

Vamos construir duas sequências de subconjuntos de Q, $\{P_i\}_{i=0}^{n}$, $\{R_i\}_{i=0}^{n}$ da seguinte forma:

$$P_0 = s(I);\ \text{para } i>0,\ P_i = P_{i-1} \cup \{q \in Q / \sigma E_{pq} \neq 0 \text{ para algum } \sigma \in \Sigma,\ p \in P_{i-1}\};$$

$$R_0 = s(F);\ \text{para } i>0,\ R_i = R_{i-1} \cup \{q \in Q / \sigma E_{qp} \neq 0 \text{ para algum } \sigma \in \Sigma,\ p \in R_{i-1}\}.$$

Como $|A| \neq 0$, $P_0 \neq \emptyset$. Além disso temos que

$$P_0 \subseteq P_1 \subseteq \ldots \subseteq P_n \subseteq Q$$

e como $|Q| = n$, as inclusões não podem ser todas próprias portando existe $j<n$ tal que $P_j = P_{j+1} = P$. Vamos provar que se $p \in Q$ é tal que existe $p \in s(I)$ e uma trilha de p para q, então $q \in P$.

Da definição da sequência $\{P_i\}$, verifica-se imediatamente que $P_i = \{q \in Q /$ existe uma trilha de comprimento $\leq i$ de algum $p \in s(I)$ até q$\}$. Suponhamos que a nossa afirmativa acima fosse falsa, isto é, que existisse $p \in s(I)$, $q \in Q$, uma trilha $T: p \rightarrow q$ e que $q \notin P$. Então poderíamos escolher p,q e T de de forma que T tenha comprimento mínimo, nessas condições.

Como $P = P_i$, devemos ter $|T| > i$. Mas então, se (r,σ,q) é a última aresta de T, temos que $T = T_1(r,\sigma,q)$, onde $T_1 : p \to r$. Como $|T_1| < |T|$, $r \in P = P_i$. Mas daí, como (r,σ,q) é uma aresta, vem que $q \in P_{i+1}$. Como $P_{i+1} = P$, isso é uma contradição.

De forma análoga, determinamos $R \subseteq Q$ tal que

$$R = \{q \in Q / \exists p \in s(F) \text{ tal que existe } T: q \to p\}.$$

Considere agora $A' = (Q', I', F', E')$:

$$Q' = P \cap R,\quad I' = I|_{Q'},\quad F' = F|_{Q'},\quad \sigma E' = \sigma E|_{Q' \times Q'},\quad \forall \sigma \in \Sigma$$

Como $|A| \neq 0$, existe ao menos uma trilha de $s(I)$ para $s(F)$, pelo Corolário II.2.3, donde $Q' \neq 0$ e A' é um K-Σ-autômato. Pela construção, toda trilha em A' é uma trilha em A, com o mesmo peso, e além disso, A' é conexo. Agora, se uma trilha $T: p \to q$ em A é tal que $I_p T \rho F_q \neq 0$, todos os seus estados devem estar em Q'. Assim, T é uma trilha em A' e $I'_p T \rho F'_q = I_p T \rho F_q$. Pelo Corolário II.2.3, $|A'| = |A|$. □

LEMA 4.4 - Se K é um semianel positivo e $A = (Q,I,F,E)$ é um K-Σ-autômato, então:

(a) A é acessível sse $\forall q \in Q$, $\exists x \in \Sigma^*$ tal que $(IxE^*)_q \neq 0$;

(b) A é coacessível sse $\forall q \in Q$, $\exists x \in \Sigma^*$ tal que $(xE^*F)_q \neq 0$.

DEMONSTRAÇÃO - Vamos demonstrar (a), sendo que (b) é análoga. Se A é acessível e $q \in Q$, existe $p \in s(I)$ e uma trilha $T: p \to q$. Seja x o rótulo de T. Então $xE^*_{pq} = T\rho + \sum T'\rho$, onde T' percorre as outras trilhas $T': p \xrightarrow{x} q$ (Proposição II.2.2). Como K é positivo, $xE^*_{pq} \neq 0$, e como $p \in s(I)$, $I_p xE^*_{pq} \neq 0$. Agora,

$$(IxE^*)_q = \sum_{r \in Q} I_r xE^*_{rq} = I_p xE^*_{pq} + \sum_{r \neq p} I_r xE^*_{rq} \neq 0,$$

ainda porque K é positivo.

Por outro lado, se para todo $q \in Q$ existe x tal que $(IxE^*)_q \neq 0$, então, dados q e x nessas condições,

$$0 \neq (IxE^*)_q = \sum_p I_p xE^*_{pq}.$$

Portanto, existe p tal que $I_p \neq 0$ e $xE^*_{pq} \neq 0$. Pela Proposição II.2.2, existe uma trilha soletrando x, de $p \in s(I)$, para q. Logo, A é acessível. □

O Teorema III.2.1, ou a construção do Lema 3 (quando $Q' = \emptyset$) permite-nos decidir efetivamente se um N-Σ-autômato tem comportamento $\emptyset$. Assim, daqui por diante, suporemos que os N-Σ-autômatos tem comportamento não vazio.

LEMA 4.5 - Seja A um N-Σ-autômato conexo. Então $|A|$ é limitado sse M_A é um monóide finito.

DEMONSTRAÇÃO - Se M_A é finito, $|A|$ é limitado, pelo Lema 2.5. Se M_A é infinito, dado $n \in N$, existem estados p,q e uma palavra $x \in \Sigma^*$ tais que $xE^*_{pq} > n$ (caso contrário, $M_A \leq M_Q(N_n)$, que é finito). Como A é conexo e N é positivo, pelo Lema 4 existem palavras u e v tais que $(IuE^*)_q > 0$ e $(vE^*F)_q > 0$. Logo:

$$\begin{aligned} uxv|A| &= IuE^*xE^*vE^*F \\ &= \sum_{r,s} (IuE^*)_r (xE^*)_{rs} (vE^*F)_s \\ &\geq (IuE^*)_p xE^*_{pq} (vE^*F)_p \\ &> n \end{aligned}$$

e $|A|$ não é cotado, portanto não é limitado. □

LEMA 4.6 - Se existe algoritmo para decidir se um subconjunto finito de $M_Q(N)$ gera um submonóide finito (para todo Q) então existe um algoritmo para decidir se um N-Σ-autômato tem comportamento limitado (para qualquer alfabeto finito Σ).

DEMONSTRAÇÃO - Suponhamos que exista um algoritmo A para de

cidir se um conjunto de matrizes gera um monóide finito (4.2). Seja A um N-Σ-autômato. Podemos decidir se $|A| = \emptyset$, pelo Teorema III.2.1. Se $|A| \neq \emptyset$, podemos construir efetivamente A' conexo tal que $|A'| = |A|$ (Lema 3). Aplicando-se A, podemos decidir se $M_{A'}$ (gerado por $\{\sigma E/\sigma \in \Sigma\}$) é finito. Pelo Lema 5, isto decide se $|A'| = |A|$ é limitado.

□

IV.4.B) - O TEOREMA, VERSÃO COMBINATÓRIA

Vamos definir alguns conceitos úteis sobre K-Σ-autômatos, que serão utilizados também na secção 5. Para isso, seja $A = (Q,I,F,E)$ um K-Σ-autômato.

Começamos pela relação $\to$ sobre Q, definida por

$p \to q$ sse existe uma trilha de p para q.

Esta relação é reflexiva e transitiva. Vamos também definir a relação $\leftrightarrows$ por:

$$p \leftrightarrows q \text{ sse } p \to q \text{ e } q \to p$$

Esta é uma relação de equivalência. As classes de equivalência de $\leftrightarrows$ são chamadas *componentes fortemente conexas* de A (por analogia com o conceito do mesmo nome para grafos dirigidos, ver Harary [H1]), ou *componentes fortes*.

Dizemos que uma componente forte C *contém* uma aresta (p,σ,q) se $p,q \in C$. Toda componente forte que não seja um conjunto unitário contém necessariamente uma aresta. Uma componente forte é *trivial* se não contiver nenhuma aresta.

Se $T = (p_0,\sigma_1,p_1)\ldots(p_{n-1},\sigma_n,p_n)$ é uma trilha, definimos

$QT = \{p_0,p_1,\ldots,p_n\}$, o conjunto dos estados de T e

$eT = \{(p_0,\sigma_1,p_1),\ldots,(p_{n-1},\sigma_n,p_n)\}$, o conjunto das arestas de T.

Uma componente forte C *contém* uma trilha T se QT⊆C. Observe que se a trilha tem só uma aresta, esta idéia de "contém" concorda com o que definimos acima.

Um *caminho* é uma trilha $P=(p_0,\sigma_1,p_1)\ldots(p_{n-1},\sigma_n,p_n)$ tal que $p_i \neq p_j$ se $i \neq j$. Em particular, uma trilha trivial é também um caminho. É imediato que se P é um caminho, seu comprimento é $\leq |Q|-1$ e $|P| = |eP|$. Portanto existe um número finito de caminhos em A.

LEMA 4.7 - Se $p \to q$, então existe um caminho de p para q.

DEMONSTRAÇÃO - Como $p \to q$, existe alguma trilha de p para q. Seja P uma trilha de comprimento mínimo nessas condições. Afirmamos que P é um caminho. Com efeito, se isso não acontecesse, na sua sequência de estados ocorreria uma repetição $p_i = p_j$, com $i < j$. Daí, P poderia ser fatorada como $P_1P_2P_3$, com $P_1: p \to p_i$; $P_2: p_i \to p_j$ e $P_3: p_j \to q$, e como $i < j$, $|P_2| \geq 1$. Mas então, P_1P_3 seria uma trilha de p para q, com comprimento menor do que o de P, o que contradiria a escolha de P. □

Um *circuito* é uma trilha não trivial.

$$S = (p_0,\sigma_1,p_1)\ldots(p_{n-1},\sigma_n,p_n)$$

tal que

(a) $(p_1,\sigma_2,p_2)\ldots(p_{n-1},\sigma_n,p_n)$ é um caminho (eventualmente trivial)

(b) $p_0 = p_n$.

É imediato que $|S| = |QS| = |eS|$.

Dado um circuito, com a notação acima, para cada $0 \leq i < n$, $S_i = (p_1,\sigma_{i+1},p_{i+1})\ldots(p_{n-1},\sigma_n,p_n)(p_0,\sigma_1,p_1)\ldots\ldots(p_{i-1},\sigma_i,p_i)$ é também um circuito e é chamado *rotação* de S *a partir de* p_i. Se T é uma rotação de S é imediato que

(a) S é uma rotação de T

(b) $Q\Gamma = QS$ e $e\Gamma = eS$

(c) Se K é comutativo, $T\rho = S\rho$.

Além disso, se S e T são circuitos e $eS = eT$, então T é uma rotação de S.

Agora estamos aptos a caracterizar matrizes quadradas sobre N que são periódicas.

Seja Q um conjunto finito e $A \in M_Q(N)$. Vamos construir o autômato de A, cujas arestas e trilhas nos darão as informações necessárias sobre o comportamento das potências de A. Esse autômato é o N-σ-autômato $A_A = (Q,0,0,E)$, onde 0 é o vetor nulo e $\sigma E = A$ (na verdade, os vetores iniciais e finais são irrelevantes aqui). Evidentemente, $M_{A_A} = A^* \subseteq M_Q(N)$ e $\sigma^r E^*_{pq} = A^r_{pq}$.

Para ficar mais claro o enunciado adiante, vamos supor Q totalmente ordenado.

TEOREMA 4.8 - Seja $A \in M_Q(N)$ e A_A como acima. São equivalentes:

(a) A é periódica

(b) Em A_A não ocorre

(b.1) Um circuito com peso > 1, ou

(b.2) Dois circuitos S_1 e S_2, com $eS_1 \neq eS_2$ tais que exista um caminho de $p_1 \in QS_1$ para $p_2 \in QS_2$.

(c) Existe uma matriz de permutação π tal que $\pi^{-1} A \pi$ se escreve na forma de blocos

$$\begin{pmatrix} B_{11} & B_{12} & B_{13} \\ 0 & B_{22} & B_{23} \\ 0 & 0 & B_{33} \end{pmatrix} \tag{4.3}$$

onde B_{11} e B_{33} são triangulares superiores com dia-

gonal nula e B_{22} é uma matriz de permutação, onde alguns dos blocos podem ser vazios.

Sobre a condição (c) é importante o seguintes esclarecimento: a conjugação por uma matriz de permutação equivale a uma ordenação dos estados, na qual se baseia a forma gráfica dos blocos. Uma forma de enunciarmos o resultado sem referência a π é dizer que existe uma partição

$$Q = Q_1 \cup Q_2 \cup Q_3$$

(algumas partes podendo ser vazias), definindo os blocos B_{ij} como restrições $Q_i \times Q_j$ de A, e substituindo a afirmativa sobre B_{11} e B_{33} pela de que essas matrizes são nilpotentes.

DEMONSTRAÇÃO - (a) implica (b). Vamos mostrar que se (b.1) ou (b.2) não for satisfeita, A não é periódica. Para isso vamos provar que para todo $m \geq 0$ existem $p,q \in Q$ e $r \in N$ tais que $A^r_{pq} > m$.

Suponhamos que (b.1) não é satisfeita e existe um circuito

$$S: p \xrightarrow{\sigma^r} p,$$

com $Sp \geq 2$. Então, para todo n,

$$S^m: p \xrightarrow{\sigma r^m} p \quad e \quad S^m p = (Sp)^m \geq 2^m.$$

Vem daí que para todo m, $A^{rm}_{pp} \geq 2^m > m$, donde A não é periódica.

Suponhamos agora que (b.2) não é satisfeita. Então existem circuitos S_1 e S_2, com $eS_1 \neq eS_2$, $p_i \in QS_i$ $i=1,2$, e $P: p_1 \rightarrow p_2$. Substituindo eventualmente cada S_i por uma rotação, podemos supor $S_i: p_i \rightarrow p_i$.

Seja $m > 0$. Vamos mostrar que $A^{mn_1 n+r}_{p_i q_i} > m$, do que resultará que A não é periódica.

Existem m+1 pares (a,b) de naturais tais que a+b=m. Para cada par, $S_1^{an_2} p S_2^{bn_1}$ é uma trilha de p_1 para p_2 sole-

trando σ^d, onde $d = an_2n_1+r+bn_1n_2 = mn_1n_2+r$. Além disso, como $eS_1 \neq eS_2$, a pares distintos correspondem trilhas distintas. Portanto existem pelo menos m+1 trilhas de p_1 para p_2 soletrando σ^d. Segue que

$$A^{mn_1n_2+r}_{p_iq_i} = \sum T\rho \geq m+1.$$

(b) implica (c). Seja A tal que A_A satisfaça (b.1) e (b.2). Por (b.1) todo circuito tem peso 1. Seja agora C um componente forte não trivial. Então existe uma aresta (p,σ,q) contida em C (pode ser $p = q$). Pela definição de componente forte, existe uma trilha de q para p e pelo Lema 7, existe um caminho $P:q \to p$. Então, $S=(p,\sigma,q)P$ é um circuito. Seja agora (p',σ,q') uma aresta em C e suponhamos que $(p',\sigma,q') \notin S$. Pela mesma razão acima, existe um caminho $P':q' \to p'$ tal que $S' = (p',\sigma,q')P'$ é um circuito. Mas, $p,p' \in C$, logo $p \to p'$ e existe um caminho $T: p \to p'$ (Lema 7). Como $eS' \neq eS$, isso contradiz (b.2). Portanto, toda aresta contida em C é uma aresta de S. Segue que se $p \in C$, existe um único $q \in C$ tal que (p,σ,q) é uma aresta, isto é, $A_{pq} \neq 0$ e como $S\rho = 1$, devemos ter $(p,\sigma,q)\rho = A_{pq} = 1$.

Sejam:

$Q_2 = \{p \in Q / [p]$ é uma componente forte não trivial$\}$,

$Q_1 = \{p \in Q / p \to q$ para algum $p \in Q_2\}$,

$Q_3 = Q - Q_1 \cup Q_2$.

B_{ij} a restrição de A a $Q_i \times Q_j$, $i,j \in 3$.

Se $Q_2 \neq \emptyset$, as considerações acima mostram que B_{22} é uma matriz de permutação, pois se $p \in Q_2$, existe um único $q \in [p] \subseteq Q_2$ tal que $A_{pq} \neq 0$, e nesse caso $A_{pq} = 1$ e também, se considerarmos o circuito $S: p \to p$ tal que $QS = [p]$, veremos que existe um único $r \in [p]$ tal que $A_{rp} = 1$. Além disso, se $[p] \neq [q]$, não podemos ter $A_{pq} \neq 0$, pois teríamos a aresta

(p,σ,q), que combinada com os circuitos em $[p]$ e em $[q]$ seria uma contradição com (b.2).

Se $Q_1 \neq \emptyset$, a relação $\rightarrow$ restrita a Q_1 é uma ordem parcial, pois se $p \rightarrow q$ e $q \rightarrow p$ com $p \neq q$, temos que $[p] = [q]$ é não trivial e $p \in Q_2$. Além disso, não existe aresta (p,σ,q) com p em Q_1, pela mesma razão. Mas então, $\rightarrow$ pode ser imerso numa ordem total $\leq_1$ em Q (ver por exemplo Berge [B1]), isto é, existe uma ordem $\leq_1$ tal que $p \rightarrow q$ implica $p \leq_1 q$. Assim, se considerarmos B_{11} com a ordem $\leq_1$ associada a Q_1, temos que $(B_{11})_{pq} = 0$ se $q \leq p$, o que mostra que B_{11} é triangular superior com diagonal nula. Da mesma forma, se $Q_3 \neq \emptyset$, obtem-se uma ordem $\leq_3$ e prova-se a afirmativa sobre B_{33}.

Supondo que $Q_1 \neq \emptyset$ e $Q_2 \neq \emptyset$, se $p \in Q_2$ e $q \in Q_1$ não podemos ter $A_{pq} \neq 0$. Caso contrário, como $q \rightarrow r$ para algum $r \in Q_2$, temos a trilha $T: q \rightarrow r$ donde $(p,\sigma,q)T: p \rightarrow t$. Por (b.2) não podemos ter $[r] \neq [p]$, logo $[r] = [p]$. Daí vem $r \rightarrow p$, e pela transitividade, $q \rightarrow p$. Mas então, $p \rightarrow q$ e $q \rightarrow p$, donde $q \in [p]$ e deveríamos ter $q \in Q_2$, o que é uma contradição. Portanto, para todo $q \in Q_1$ e $q \in Q_2$, $A_{pq} = 0$, donde $B_{21} = 0$.

Se B_{31} ou B_{32} não fossem nulas, teríamos $A_{pq} \neq 0$ para algum $q \in Q_3$, $p \in Q_1 \cup Q_2$. Isso implicaria em $q \rightarrow r$, para algum $r \in Q_2$ o que contraria a construção de Q_3. Daqui segue a forma de blocos (4.3), onde a matriz π corresponde a qualquer permutação que ordene Q, colocando $p < q$ se $p \in Q_i$, $q \in Q_j$ com $i < j$ e restrita a Q_1 e Q_3 induza respectivamente as ordens $\leq_1$ e $\leq_3$.

(c) implica (a). Suponhamos que $\pi^{-1}A\pi$ se escreva na forma (4.3). Então, para todo $n \geq 0$,

$$\pi^{-1}A^n\pi = (\pi^{-1}A\pi)^n = \begin{pmatrix} B_{11}^n & C_n & D_n \\ 0 & B_{22}^n & E_n \\ 0 & 0 & B_{33}^n \end{pmatrix}$$

onde C_n, D_n e E_n são matrizes, cuja expressão em termos dos blocos originais é irrelevante.

Como B_{11} e B_{33} são triangulares superiores com diagonal nula, elas são nilpotentes. Assim, se $m=\max(|Q_1|,|Q_2|)$, $B_{11}^m = B_{33}^m = 0$. Como B_{22} é matriz de permutação, existe r tal que $B_{22}^r = I_{Q_2}$, a matriz identidade. Se n é tal que $nr \geq m$, então:

$$H = \pi^{-1}A^{nr}\pi = \begin{pmatrix} 0 & C_{nr} & D_{nr} \\ 0 & I & E_{nr} \\ 0 & 0 & 0 \end{pmatrix}$$

Portanto,

$$H^2 = \begin{pmatrix} 0 & C_{nr} & C_{nr} E_{nr} \\ 0 & I & E_{nr} \\ 0 & 0 & 0 \end{pmatrix}$$

e $H^2 = H^3$. Segue que $\pi^{-1}A^{2nr}\pi = \pi^{-1}A^{3nr}\pi$, donde $A^{2nr}=A^{3nr}$, portanto, A é periódica. □

COROLÁRIO 4.9 - Uma matriz $A \in M_Q(N)$ é idempotente sse existe uma matriz de permutação π tal que $\pi^{-1}A\pi$ é da forma em blocos

$$(4.4) \qquad \begin{pmatrix} 0 & B & BC \\ 0 & I & C \\ 0 & 0 & 0 \end{pmatrix}$$

onde I é uma matriz identidade (alguns blocos podem ser vazios).

DEMONSTRAÇÃO - Se $\pi^{-1}A\pi$ é da forma (4.4) é imediato que A é idempotente. Por outro lado, se A é idempotente, é, em particular, periódica, e existe π tal que $\pi^{-1}A\pi$

é da forma (4.3). Mas então $(\pi^{-1}A\pi)^2 = \pi^{-1}A\ \pi$, e calculando, a partir da forma em blocos, temos

$$B_{11}^2 = B_{11}$$
$$B_{33}^2 = B_{33}$$
$$B_{22}^2 = B_{22}$$
$$B_{11}B_{12} + B_{12}B_{22} = B_{12}$$
$$B_{11}B_{13} + B_{12}B_{23} + B_{13}B_{33} = B_{13}$$
$$B_{22}B_{23} + B_{23}B_{33} = B_{23}$$

Como B_{11} é nilpotente, $B_{11}^2 = B_{11}$ implica $B_{11} = 0$, e analogamente, $B_{33} = 0$; e como B_{22} é matriz de permutação, $B_{22}^2 = B_{22}$ implica $B_{22} = I$. Aplicando-se esses resultados obtemos também $B_{13} = B_{12}B_{23}$. □

COROLÁRIO 4.10 - É decidível se uma matriz $A \in M_Q(N)$ é periódica.

DEMONSTRAÇÃO - Dada a matriz A, os caminhos e circuitos de A_A são em número finito, e podem ser enumerados; assim, podemos testar as condições (b.1) e (b.2) (não nos preocupamos aqui com a eficiência do algoritmo resultante. □

COROLÁRIO 4.11 - Se $A \in M_Q(N_2)$ é idempotente e além disso é um elemento periódico de $M_Q(N)$, então:

(a) Existe uma matriz de permutação π tal que $\pi^{-1}A\pi$ é da forma em blocos

$$\begin{pmatrix} 0 & B & C \\ 0 & I & D \\ 0 & 0 & 0 \end{pmatrix}$$

onde I é uma matriz identidade.

(b) $A^2 = A^3$ em $M_Q(N)$.

DEMONSTRAÇÃO - Como A, como matriz sobre N é periódica, pelo Teorema 8, existe π tal que $\pi^{-1}A\pi$ é da forma (4.3). Mas $\pi, \pi^{-1} \in M_Q(N_2)$ e o produto $\pi^{-1}A\pi$ dá o mesmo resultado seja sobre N ou N_2 (observe que este produto corresponde a uma ordenação de Q). Aplicando-se a mesma técnica do Corolário 9, obtem-se que A é da forma citada. □

COROLÁRIO 4.12 - Sejam $A, B \in M_Q(N)$ e suponhamos que para todo

$$p,q \in Q,\ A_{pq} \leq 1 \text{ implica } B_{pq} \leq A_{pq}.$$

Então, se A é periódica, B também o é.

DEMONSTRAÇÃO - Considere os autômatos A_A e A_B. A hipótese implica que toda aresta de A_B é uma aresta de A_A. Além disso, todo circuito de A_B é um circuito de A_A e como A_A satisfaz (b.1), esses circuitos têm peso 1. Além disso, como em A_A não existem caminhos ligando circuitos com conjuntos distintos de arestas, não existem tais caminhos em B, e B satisfaz (b.2). Pelo Teorema 8, B é periódica. □

Agora estamos quase em condições de demonstrar o Teorema 1, precisando ainda do Teorema de Ramsey ([R1], ver também Ryser [R2]), que enunciaremos aqui numa forma que nos será útil.

TEOREMA DE RAMSEY [R1] - Dados inteiros positivos m,n,k, existe um inteiro R(m,n;k) tal que para todo conjunto X com pelo menos R(m,n,k) elementos, e toda partição da família de subconjuntos de X com k elementos em m partes $X_1, \ldots, X_m$ (algumas eventualmente vazias), existe um subconjunto X de Y com n elementos e uma parte X_i tal que todos os subconjuntos de Y com k elementos estão contidos em X_i.

Este Teorema é um dos clássicos da Combinatória, e a aplicação que vamos dar é semelhante a uma aplicação para

semigrupos finitos, que pode ser vista em [M2].

Repetimos aqui o enunciado do Teorema 1, numa forma mais forte. Para isso, vamos definir: um elemento a de um monóide é *2-potente* se $a^2 = a^3$.

TEOREMA 4.1' - Um submonóide M de $M_Q(N)$ finitamente gerado é finito sse todo elemento $M\psi_2$ que é idempotente como matriz em $M_Q(N_2)$ é 2-potente como matriz em $M_Q(N)$.

DEMONSTRAÇÃO - Suponhamos que M seja finito, e seja $B \in M\psi_2$, idempotente em $M_Q(N_2)$. Então, existe $A \in M$ tal que $A\psi_2 = B$. Como M é finito, A é periódica, logo, pelo Corolário 11, B é 2-potente em $M_Q(N)$.

Suponhamos agora que $M = X^*$, onde X é um subconjunto finito de $M_Q(N)$ e M satisfaz as condições do teorema. Seja Σ um alfabeto com $|\Sigma| = |X|$ e $\phi: \Sigma^* \to X$ uma bijeção. Então ϕ se estende a um morfismo $\phi^*: \Sigma^* \to M_Q(N)$ e $M = \{x\phi^*/x \in \Sigma^*\}$. Para mostrarmos que M é finito, vamos mostrar que existe um inteiro α tal que para todo $m \in M$, existe $x \in \Sigma^*$ com $|x| < \alpha$ tal que $m = x\phi^*$ (isto implica que $|M| \leq (|\Sigma|^{\alpha} - 1)/(|\Sigma| - 1)$). Tomemos

$$\alpha = R(n,4,2),$$

dado pelo Teorema de Ramsey, onde $n = |M\psi_2|$.

Seja x uma palavra tal que $|x| \geq \alpha$. Vamos mostrar que existe uma palavra y, com $|y| < |x|$ tal que $y\phi^* = x\phi^*$. Aplicando-se sucessivamente este resultado, pode-se obter uuma palavra z, $|z| < \alpha$ e tal que $z\phi^* = x\phi^*$.

Suponhamos então $r = |x|$ e que $x = \sigma_1\sigma_2 \ldots \sigma_r$, com $\sigma_i \in \Sigma$, $\forall i \in r$. Vamos repartir os subconjuntos de r com 2 elementos em n partes disjuntas, $\{P_m | m \in M\psi_2\}$ da seguinte forma

$$P_m = \left\{\{i,j\}/i<j \text{ e } (\sigma_i\sigma_{i+1}\ldots\sigma_{j-1})\phi^*\psi_2 = m\right\}.$$

Como $r \geq \alpha$, existem $i \leq j < k < \ell \leq r$ tais que todos os subconjuntos com 2 elementos de $\{i,j,k,\ell\}$ estão no mesmo P_m para algum m.

Fazendo:

$$x_0 = \sigma_1 \cdots \sigma_{i-1}$$
$$x_1 = \sigma_i \cdots \sigma_{j-1}$$
$$x_2 = \sigma_j \cdots \sigma_{k-1}$$
$$x_3 = \sigma_k \cdots \sigma_{\ell-1}$$
$$x_4 = \sigma_\ell \cdots \sigma_r,$$

temos, denotando $\xi = \phi^*\psi_2$, entre outras igualdades, que

$$m = x_1\xi = x_2\xi = (x_1x_2)\xi = x_3\xi$$

pois, $\{i,j\},\{j,k\},\{i,k\},\{k,\ell\} \in P_m$.

Mas, $m = (x_1x_2)\xi = x_1\xi x_2\xi = m^2$, portanto m é idempotente em $M_Q(N_2)$. Pela hipótese, m é 2-potente em $M_Q(N)$, portanto periódico, e pelo Corolário 11, existe uma matriz de permutação π tal que

$$\pi^{-1}m\pi = \begin{pmatrix} 0 & C & D \\ 0 & I & B \\ 0 & 0 & 0 \end{pmatrix}.$$

Mas então, para cada x_i, i=1,2,3,

$$\pi^{-1}(x_i\phi^*)\pi = \begin{pmatrix} 0 & C_i & D_i \\ 0 & I & E_i \\ 0 & 0 & 0 \end{pmatrix},$$

pois $m = x_i\xi$.

Daí vem

$$\pi^{-1}(x_1x_2x_3)\phi^*\pi = \pi^{-1}(x_1\pi^*)\pi\cdot\pi^{-1}(x_2\phi^*)\pi\cdot\pi^{-1}(x_3\phi^*)\pi =$$

$$= \begin{pmatrix} 0 & C_1 & D_1 \\ 0 & I & E_1 \\ 0 & 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & C_2 & D_2 \\ 0 & I & E_2 \\ 0 & 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & C_3 & D_3 \\ 0 & I & E_3 \\ 0 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & C_1 & C_1E_3 \\ 0 & I & E_3 \\ 0 & 0 & 0 \end{pmatrix}$$

$$= \pi^{-1}(x_1\phi^*)\pi\cdot\pi^{-1}(x_3\phi^*)\pi$$

$$= \pi^{-1}(x_1x_3)\phi^*\pi,$$

portanto

$$(x_1x_2x_3)\phi^* = (x_1x_3)\phi^*.$$

Segue que

$$x = (x_0x_1x_2x_3x_4)\phi^* = (x_0x_1x_3x_4)\phi^*.$$

e como $j < k$, $|x_2| > 0$, donde $|x_0x_1x_3x_4| < |x|$. Isto completa a demonstração. □

Observe que se na demonstração tomássemos

$$\alpha = R(|M_Q(N_2)|,4,2),$$

no lugar do valor que tomamos, obteríamos um limitante superior para o número de elementos de qualquer submonóide finito de $M_Q(N)$ com k geradores, a saber $(k^\alpha-1)/(k-1)$. Isto implica que *dados* $n,k \in N$ *existe apenas um número finito de semigrupos (abstratos) com* k *geradores, que tem uma representação fiel em* $M_n(N)$.

COROLÁRIO 4.13 - Dado um subconjunto finito X de $M_Q(N)$, é decidível se X^* é um monóide finito.

DEMONSTRAÇÃO - "Basta" construir a imagem $X^*\psi_2$, que, utilizando a notação do teorema, é igual a

$$\{x\phi^*\psi_2 / x\in\Sigma^* \text{ e } |x| \leq |M_Q(N_2)| = 3^{|D|^2}\},$$

selecionarmos os idempotentes, e verificarmos se eles são 2-potentes como elementos de $M_Q(N)$. Uma outra possibilidade bem curiosa é a seguinte: calcula-se

$$\alpha = R(3^{|Q|^2},4,2), \quad \beta = (|X|^\alpha-1)/(|X|-1),$$

sendo α dado pelo Teorema de Ramsey efetivamente, e, sendo I_Q a matriz de identidade, verifica-se se para algum $n \leq \beta$, $(I_Q \cup X)^n = (I_Q \cup X)^{n+1}$. As limitações apresentadas implicam que X^* é finito sse essa igualdade ocorrer, para algum $n \leq \beta$. □

IV.4.c) - O TEOREMA, VERSÃO ALGÉBRICA

Seja K um corpo de característica zero.

O *polinômio ciclotômico* Φ_d, onde d é um inteiro positivo, é definido por

$$\Phi_d(X) = \Pi(X-\xi),$$

onde ξ percorre o conjunto das raízes primitivas d-ésimas da unidade.

São clássicos os seguintes fatos (ver por exemplo McCarthy [M1]):

(a) Se $a \neq b$, $\Phi_a \neq \Phi_b$,

(b) Os coeficientes de Φ_d são inteiros, para todo d,

(c) Φ_d é irredutível em $Q[X]$, para todo d,

(d) $X^n-1 = \prod_{d/n} \Phi_d(X)$.

(e) O grau de $\Phi_d(x)$ é $\phi(d)$, onde ϕ é a função de Euler.

PROPOSIÇÃO 4.14 - Seja K um corpo de característica zero e $A \in AGM_Q(K)$. Então A é periódica sse seu polinômio minimal for da forma

$$m_A = X^r P \tag{4.5}$$

onde P é um produto de polinômios ciclotômicos distintos.

DEMONSTRAÇÃO - Se A é periódica, existem naturais $p < q$ tais que $A^p = A^q$. Segue que A é raíz do polinômio $X^p(X^{q-p}-1)$, portanto, m_A, que é um divisor deste polinômio, tem que ser da forma (4.5), por (d).

Se o polinomio minimal $m_A(X) = X^r \Phi_{d_i} \ldots \Phi_{d_k}$, tomando-se para n o mínimo múltiplo comum de $d_i \ldots d_k$, vem que

$$m_A / X^r(X^n-1),$$

portanto, $A^r = A^{r+n}$ e A é periódica. □

COROLÁRIO 4.15 - É decidível se $A \in AGM_Q(K)$ é periódica.

DEMONSTRAÇÃO - Observe que "decidível" aqui subentende que as operações com elementos de K são realizáveis algoritmicamente. Um possível processo de decisão seria calcular o polinômio característico de A, verificar se suas raízes são 0 e raízes da unidade somente, e em seguida testar um número finito de candidatos até obter m_A. No entanto, apresentaremos aqui um resultado mais interessante, que dá outro método. □

Seja $n = |Q|$. Sabe-se que o grau de $m_A(X)$ é $\leq n$. Seja $D_n = \{d \in \mathbb{N} / \phi(d) \leq n\}$. Por propriedades conhecidas da função de Euler, D_n é finito. Para cada subconjunto B de D_n, seja

$$\bar{B} = \sum_{x \in B} \phi(x).$$

Considere agora o conjunto $F_n = \{B \subseteq D_n / \tilde{B} \leq n\}$. A Proposição 13 nos diz que se A é uma matriz periódica, existe $B \in F_n$, $r \leq n - \tilde{B}$ tal que

$$m_A(X) = X^r \prod_{d \in B} \Phi_d,$$

e nesse caso, se $m = m.m.c.B$, $A^{m+r} = A^r$.

Vamos definir $f: N \to N$ por: $nf = \max\{m.m.c.B / B \in F_n\}$. Observe que f é uma função computável de n, e vale o seguinte: Se A é periódica, existem inteiros $r < p \leq nf$, com $r \leq n$, tais que $A^r = A^{r+p}$. Isto implica também que se A é periódica, A^* tem no máximo $nf + n$ elementos.

Observe que como $M_Q(N) \subseteq M_Q(Q)$, a Proposição 14 também caracteriza matrizes periódicas em $M_Q(N)$. Vamos voltar agora a N, com uma demonstração mais algébrica do Corolário 4.12, cujo enunciado aqui repetimos.

COROLÁRIO 4.12 - Sejam $A, B \in M_Q(N)$ e suponhamos que para todo $p,q \in A$, $A_{pq} \leq 1$ implica $B_{pq} \leq A_{pq}$.

Então, se A é periódica, B também o é.

DEMONSTRAÇÃO - Vamos provar para o caso em que existe um único par (p,q) tal que $A_{pq} \neq B_{pq}$. O resultado geral segue deste indutivamente.

Seja então (p,q) tal que $A_{pq} \neq B_{pq}$.

CASO 1: $A_{pq} = 1$. Então, $B_{pq} = 0$, e para todo r,s, vale que $B_{rs} \leq A_{rs}$. Mas daí, para todo $k \geq 0$, $B^k_{rs} \leq A^k_{rs}$, donde segue que

$$\{B^k_{rs} / k \in N, r,s \in Q\}$$

é finito, portanto B é periódica.

CASO 2: $A_{pq} = a \geq 2$. Considere a matriz $A' \in M_Q(N[X])$, obtida de A substituindo-se a entrada (p,q) pela variá

vel X. Então para todo $k\in N$, $r,s\in Q$, $A^k_{rs} = P_{r,s,k}(X)\in N[X]$. Afirmamos que, como A é periódica, o conjunto de polinômios $P = \{P_{r,s,k}(X)\}$ é finito. Com efeito, $A^k_{rs} = P_{r,s,k}(a)$. Como A é periódica, $\{A^k_{rs}\}$ é um conjunto finito, portanto $\{P_{r,s,k}(a)\}$ é finito. Mas se P fosse infinito, existiria uma sequência $\{L_1, L_2, \ldots\}$ infinita de elementos de P tais que, ou $L_i(1) < L_{i+1}(1)$, para todo i, ou grau $L_i <$ grau L_{i+1} para todo i. Em ambos os casos, a sequência $\{L_i(a)\}_{i\in N}$ teria infinitos termos, contradizendo o fato de A ser periódica.

Mas se $B_{pq} = b$, para todo $k\in N$, $r,s\in Q$, $B^k_{rs} = P_{r,s,k}(b)$, e como P é finito, $\{B^k_{rs}/k\in N,\ r,s\in Q\}$ é finito. Portanto, B é periódica. □

A seguinte proposição tem aplicação na secção 5, cujos métodos foram o ponto de partida para esta secção.

PROPOSIÇÃO 4.16 - Sejam M,S semigrupos (ou monóides), S periódico, e $\phi: M \to S$ um morfismo. Então M é periódico sse todo $m\in M$, cuja imagem $m\phi$ é idempotente, é periódico.

DEMONSTRAÇÃO - A parte "só se" é trivial. Suponhamos então que M e ϕ satisfaçam a condição, e seja $m\in M$. Vamos mostrar que m é periódico.

Com efeito, como S é periódico, existe $k>0$ tal que $(m\phi)^k$ é idempotente. Portanto, m^k é periódico, e existem inteiros p e q tais que $m^{kp} = m^{kq}$. Segue que m é periódico. □

Combinando-se o Corolário 12 com a Proposição 16, vem que:

(4.6) "Um submonóide M de $M_Q(N)$ é periódico sse todo elemento de $M\psi_2$ que é idempotente como matriz em $M_Q(N_2)$ é periódico como matriz em $M_Q(N)$."

Para isso, basta observar que $M_Q(N_2)$ é um monóide finito, portanto periódico; de resto aplica-se o Corolário

12 da mesma forma que no início da demonstração do Teorema 1'.

A passagem de (4.6) para o Teorema 1 é imediata via:

TEOREMA DE McNAUGHTON-ZALCSTEIN [MZ1] - Todo semigrupo periódico de matrizes quadradas sobre um corpo é localmente finito.

IV.4.D) - POSSIBILIDADES DE ESTENSÃO

As duas demonstrações que apresentamos para o Teorema 1 são fundadas em conceitos intrinsecamente diferentes, e como tal trazem possibilidades de generalização completamente distintas.

O Lema 5, que diz que um N-autômato conexo tem comportamento limitado sse seu monóide é finito, continua válido se substituirmos N por um semianel graduado. Um semianel K é *graduado* se existe uma função $\gamma: K \to R_+$ satisfazendo o seguinte:

(a) $0\gamma = 0$

(b) $1\gamma = 1$

e para todo $x,y \in K$:

(c) $x\gamma > 1$ se $x \neq 0,1$

(d) $(x+y)\gamma \geq x\gamma + y\gamma$

(e) $(xy)\gamma \geq x\gamma y\gamma$.

Por exemplo, para todo alfabeto Σ, o semianel $N\langle\Sigma\rangle$ é graduado, com γ dado por

$$\left(\sum_i \alpha_i \underline{x}_i\right)\gamma = \sum \alpha_i |x_i| .$$

Ainda neste caso, todo método da subsecção B pode

ser aplicado, obtendo-se uma caracterização análoga para matrizes periódicas, e o mesmo processo de decisão. As modificações essenciais consistem em substituir o peso ρ pela função $\rho\gamma$ em certos contextos e substituir a função $\phi_2: N \to N_2$ por $\phi_2': K \to N_2$, dada por

$$x\phi_2' = \begin{cases} 0 \text{ se } x = 0 \\ 1 \text{ se } x = 1 \\ 2 \text{ caso contrário.} \end{cases}$$

Já a demonstração algébrica necessita de um ponto de partida distinto. Ela se generaliza para qualquer subsemianel de um corpo em certos aspectos, a partir das seguintes observações:

(a) - O Lema 5 deixa de ter validade no caso geral. O exemplo III.4.2 mostra um Q-σ-autômato conexo, reconhecendo um Q-subconjunto limitado, cujo monóide é infinito. Porém, a Proposição 3.5 mostra que se K é um corpo, um K-subconjunto é limitado sse o monóide de seu autômato reduzido é finito; mas, dado um K-autômato A, a Proposição III.4.2 mostra que é possível construir um K-autômato reduzido reconhecendo $|A|$ efetivamente.

(b) - Assim, no caso de um corpo, o problema de decidir se um K-subconjunto reconhecível é limitado é também equivalente a decidir se um subconjunto finito de $M_Q(K)$ gera um submonóide finito.

(c) - A Proposição 14 caracteriza matrizes periódicas em corpos de característica 0. Para corpos de característica $p > 0$ pode-se sem dificuldade obter uma classificação dos polinômios minimais de matrizes periódicas em $M_Q(K)$, e estes formam certamente um conjunto finito. Assim, é decidível em qualquer ca

so se uma matriz é periódica.

(d) - O Teorema de McNaughton-Zalcstein permite estabecer o seguinte algoritmo para decidir-se um subconjunto finito X de $M_Q(K)$ gera um submonóide X^*, finito. Observe que

$$X^* = \bigcup_{n\geq 0} X^n$$

e que X^* é finito sse, para algum n,

$$X^* = \bigcup_{0\leq k\leq n} X^n$$

(1) - Faça $n = 1$

(2) - Se $X^n \subseteq \bigcup_{0\leq k<n} X^k$, então $X^* = \bigcup_{0\leq k<n} X^n$

(3) - Caso contrário, verifique se todos elementos de $X^n - \bigcup_{0\leq k<n} X^n$ são periódicos. Se algum não for, X^* é infinito. Pare.

(4) Faça $n \leftarrow n+1$ e volte para (2).

O Teorema de McNaughton-Zalcstein garante que o algoritmo termina sempre.

(e) - Se K é um corpo de característica $p > 0$ e todas entradas das matrizes em X são elementos algébricos sobre o corpo primo GF(p), o problema torna-se trivial, pois teremos $X^* \subseteq M_Q(K')$ onde $K' \subseteq K$ é uma extensão finita de GF(p). Assim, X^* será finito.

IV.4.E) - CONSTRUÇÃO DE EXEMPLOS

É interessante ver-se alguns exemplos não triviais de N-Σ-autômatos que reconhecem N-subconjuntos limitados. Não triviais significa conexos e sem ser determinísticos, ou seja, com monóide finito, formado por matrizes razoavelmente com-

plicadas. Vamos apresentar uma construção para isso.

O *reverso* de uma palavra x, denotado $\overleftarrow{x}$ é definido indutivamente por $\overleftarrow{1} = 1$ e $\overleftarrow{(y\sigma)} = \sigma\overleftarrow{y}$. Vale imediatamente

$$\overleftarrow{(xy)} = \overleftarrow{y}\,\overleftarrow{x}.$$

O reverso de um conjunto $L \subseteq \Sigma^*$ é $\overleftarrow{L} = \{\overleftarrow{x}/x \in L\}$. O reverso de um K-subconjunto (K é um semianel qualquer) A é $\overleftarrow{A}$, dado por $x\overleftarrow{A} = \overleftarrow{x}A$. Se A é o complemento de $A = (Q,I,F,E)$ e K é comutativo, verifica-se que $\overleftarrow{A}$ é reconhecido por

$$\overleftarrow{A} = (Q,F^t,I^t,\overleftarrow{E}),$$

onde B^t indica a transposta da matriz B e $\sigma\overleftarrow{E} = (\sigma E)^t$, $\forall \sigma \in \Sigma$.

Um N-subconjunto não-ambíguo P de Σ^* é dito um *prefixo* se, para todo $x \in s(P)$ e todo $y \neq 1$, $xyP = 0$. Ele é um *sufixo* se para todo $x \in s(P)$ e todo $y \neq 1$, $yxP = 0$.

Se $A = (Q,\delta^P,F,E)$ é um N-Σ-autômato determinístico conexo em que $F_q = 0$ ou 1, para cada $q \in Q$, e tal que não existe aresta com início em $s(F)$ (o que equivale a dizer que $FoE = 0$, $\forall \sigma \in \Sigma$), então afirmamos que $|A|$ é um prefixo. Deixamos a demonstração a cargo do leitor. Logo, $|\overleftarrow{A}|$ é um sufixo.

Seja S um sufixo. Se $1S = 1$, então, para todo $x \in \Sigma^+$, $xS = 0$, donde $S = 1$, e a mesma coisa vale para prefixo.

PROPOSIÇÃO 4.17 - Se S é um sufixo e $S \neq 1$ então S^* é não-ambíguo.

DEMONSTRAÇÃO - Seja $x \in \Sigma^*$. Então, $xS^* = \Sigma\, x_1Sx_2S\ldots x_nS$, onde a soma é sobre todas fatorações $x = x_1x_2\ldots x_n$, $x_i \neq 1$, para todos os valores de n. Suponhamos que $x \in s(S^*)$. Então, para alguma fatoração, $x_1Sx_2S\ldots x_nS \neq 0$. Como S é não ambíguo, $x_1Sx_2S\ldots x_nS = 1$. Considere alguma outra fatoração $x = y_1y_2\ldots y_m$ distinta da vista acima. Seja r o menor índice $\leq \min(n,m)$ tal que $x_r \neq y_r$ e $w = x_{r+1}\ldots x_n = y_{r+1}\ldots y_m$. Então, $x = x_1\ldots x_rw = y_1\ldots y_rw$. Podemos supor $|x_r| > |y_r|$ (o caso con

trário é análogo), donde $x_r = zy_r$, com $z \neq 1$. Mas como S é um sufixo, se $y_r S = 1$, teríamos $x_r = 0$, o que é uma contradição com a escolha da fatoração $x_1 x_2 \ldots x_n$. Portanto, $xS^* = 1$, e S^* é não-ambíguo □

A partir de $\hat{A}$ construído acima reconhecendo um sufixo S, podemos contruir A' reconhecendo S^* da seguinte forma:

$$A' = (Q - s(F), \delta^p, \delta^p, E'),$$

onde

$$\sigma B'_{qt} = \begin{cases} \sigma \hat{E}_{qt} & \text{se } q \neq p \\ (F^t \sigma \hat{E})_t & \text{se } q = p. \end{cases}$$

Fica a cargo do distinto leitor o seguinte:

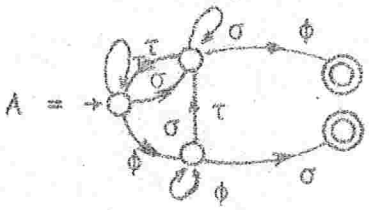
(1) $|A'| = S^*$

(2) A' é conexo e contém uma única componente forte.

Em geral, A' não é determinístico.

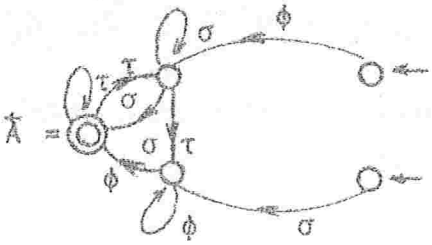
Em vista de (1) e (2), $M_{A'}$ é finito, pois A' é conexo e $|A'|$ tem imagem finita.

Por exemplo, se partimos de

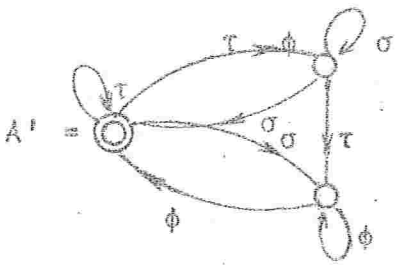


$\Sigma = \{\sigma, \tau, \phi\}$

obtemos



e



Um N-Σ-autômato é *acíclico* se não tiver circuitos. Se $A = (Q,I,F,E)$ é acíclico, para todo x tal que $|x| \geq |Q|$, $xE^* = 0$, portanto M_A é finito.

Sejam $Q \cap R = \emptyset$ e $\mu: \Sigma \to M_Q(N)$, $\chi: \Sigma \to M_R(N)$ e $\psi: \Sigma \to N^{Q \times R}$ aplicações. Definimos a soma ligada

$$\mu +_\psi \chi: \Sigma \to M_{Q \cup R}(N)$$

por

$$\sigma(\mu +_\psi \chi) = \begin{matrix} \\ Q \\ R \end{matrix} \begin{matrix} \begin{matrix} Q & \quad R \end{matrix} \\ \begin{pmatrix} \sigma\mu & \sigma\psi \\ 0 & \sigma\chi \end{pmatrix} \end{matrix}$$

Considere $A = (Q,I,F,E)$ e $A' = (Q',I',F',E')$, com $Q \cap Q' = \emptyset$. Seja $\psi: \Sigma \to N^{Q \times Q'}$ uma aplicação. Definimos

$$A +_\psi A' = (Q\ Q', J, G, E +_\psi E'),$$

onde

$$J_q = \begin{cases} I_q & \text{se } q \in Q \\ I'_q & \text{se } q \in Q' \end{cases} \qquad G_q = \begin{cases} F_q & \text{se } q \in Q \\ F'_q & \text{se } q \in Q' \end{cases}$$

Se ψ é a função nula, $A +_\psi A' = A + A'$ (ver II.3.2). Sejam A e A' N-Σ-autômatos, e suponhamos que M_A e $M_{A'}$ são finitos. Deixamos a cargo do leitor a verificação de que:

(a) $M_{A+A'}$ é finito (ver Proposição 2.6)

(b) Se A ou A' é acíclico, então para todo ψ, $M_{A+_\psi A'}$ é

finito (basta provar que $M_{A+_\psi A'}$ é periódico e aplicar o Teorema de McNaughton-Zalcstein)

(c) Se A e A' são conexos, para toda ψ, $A+_\psi A'$ é conexo.

IV.5 - CONJUNTOS QUASE-PERIÓDICOS

Considere um conjunto $L \subseteq \Sigma^*$. Temos que

$$L^* = \bigcup_{n \geq 0} L^n.$$

Como $(1 \cup L)^n = 1 \cup L \cup \ldots \cup L^n$, vem que $(1 \cup L)^n \subseteq (1 \cup L)^{n+1}$, para todo n, e vale também

$$L^* = \bigcup_{n \geq 0} (1 \cup L)^n.$$

Um subconjunto L de Σ^* é dito *quase-periódico* se, para algum $n \geq 0$,

$$L^* = (1 \cup L)^n.$$

Isto porque neste caso $(1 \cup L)^{n+1} = (1 \cup L)^n$, e $1 \cup L$ é um elemento periódico de $P(\Sigma^*)$.

Nesta secção estudaremos a possibilidade de decidir se um conjunto reconhecível é quase-periódico, a partir de um autômato que o reconhece. A técnica utilizada consiste em construir um M-Σ-autômato A' a partir do autômato dado A tal que o M-subconjunto reconhecido por A' é limitado sse o conjunto $|A|$ é quase-periódico. Esse M-autômato A' tem um papel importante, análogo ao da N-Σ-autômato conexo na secção anterior: $|A'|$ é limitado sse M_A, é finito. A partir daí, o problema torna-se semelhante ao do capítulo anterior. As idéias aqui são devidas ao Prof. I.Simon [S6] e a J.A.Brzozowski, tendo inspirado o método utilizado na secção anterior. O que apresentaremos são resultados parciais, por falta de um resultado análogo ao do Teorema de McNaughton-Zalcstein, ou de uma generalização razoável de nossa demonstração combinatória.

Antes disso, veremos alguns exemplos de conjuntos

que são quase-periódicos e de alguns que não o são.

Qualquer subsemigrupo de Σ^* é um conjunto quase-periódico. Por outro lado, qualquer subconjunto finito de Σ^* contendo uma palavra não vazia não é quase-periódico. Um exemplo não trivial de conjuntos não quase-periódicos é o seguinte:

Um conjunto $S \subseteq \Sigma^*$ satisfazendo $S^* = S$ é um submonóide de Σ^* (e é também chamado *estrela* por Brzozowski [B1]). Um conjunto R tal que $R^* = S$ é um *gerador* de S. Para toda estrela S,

$$R = (S-1) - (S-1)^2 \tag{5.1}$$

é um gerador e está contido em todos os outros geradores de S; R é chamado *gerador minimal* de S. A expressão (5.1) mostra que se S é reconhecível, seu gerador minimal também o é.

TEOREMA 5.1 - (Simon [S6] - Se R é o gerador minimal de uma estrela S contendo uma palavra não vazia, então R não é quase-periódico.

Voltemos agora ao nosso problema, ou seja, o de decidir se um dado autômato reconhece um conjunto quase-periódico. Em primeiro lugar, vamos estabelecer algumas idéias sobre M.

O semianel M tem como conjunto suporte $\mathbb{N} \cup \infty$, a soma $\oplus$ definida por $a \oplus b = \min\{a,b\}$ e o produto $a \otimes b = a+b$, onde para ∞ se observa que

$$a < \infty, \ \forall a \in \mathbb{N}, \ \infty + a = a + \infty = \infty, \ \forall a \in M.$$

Observamos que ∞ é o neutro para $\oplus$ ou seja, é o 0 do semianel e 0 o neutro para $\otimes$ ou seja, o 1 do semianel. Ao trabalharmos com M, operaremos geralmente sobre $\mathbb{N} \cup \infty$ usando min e +, e fazendo diretamente uma tradução da notação usada anteriormente. Assim, quando falarmos em 0 e 1 estare-

mos nos referindo aos elementos de N. Em particular a Proposição II.2.2 se transforma em:

PROPOSIÇÃO 5.2 - Seja $A = (Q,I,F,E)$ um M-Σ-autômato. Então, para todo $p,q \in Q$, $xE^*_{pq} = \min\{T\rho / T : p \xrightarrow{x} q\}$, sendo ∞ se não houver trilha de p para q soletrando x, e se

$$T = (p_0,\sigma_1,p_1)\ldots(p_{n-1},\sigma_n,p_n),$$

então

$$T\rho = (p_0,\sigma_1,p_1)\rho + \ldots + (p_{n-1},\sigma_n,p_n)\rho.$$

Vamos agora construir um M-Σ-autômato associado a um conjunto reconhecível.

Seja L um conjunto reconhecido pelo Σ-autômato $A = (P,J,G,H)$. O M-Σ-autômato $A_L = (Q,I,F,E)$ é definido por

$$Q = P \cup p_0, \text{ onde } p_0 \notin P$$

$$I_p = F_p = \delta_p^{p_0} = \begin{cases} 0 \text{ se } p = p_0 \\ \infty \text{ caso contrário} \end{cases}$$

$$\sigma E_{pq} = \begin{cases} 0 \text{ se } p,q \in P \text{ e } q \in p\sigma H \text{ ou se } p = p_0 \text{ e } q \in J\sigma H \\ 1 \text{ se } q = p_0 \text{ e } p\sigma H \cap G \neq \emptyset \text{ ou } p = q = p_0 \text{ e } J\sigma H \cap G \neq \emptyset \\ \infty \text{ nos outros casos.} \end{cases}$$

Valem os seguintes fatos:

(a) Toda aresta de A é uma aresta de A_L, com peso 0.

(b) Uma aresta de A_L tem peso 1 sse seu estado terminal é p_0.

(c) O peso de uma trilha é o número de arestas de peso 1, que nela ocorrem, portanto, o número de ocorrências de p_0 como término de uma aresta na trilha.

(e) $x|A_L| = xE^*_{p_0p_0}$ e é finito sse existe uma trilha:

$$T: p_0 \xrightarrow{x} p_0$$

PROPOSIÇÃO 5.3 - Sejam L,A e A' como acima. Então $x|A_L| = 1$ sse $x \in L-1$.

DEMONSTRAÇÃO - Como $I_{p_0} = F_{p_0} = 0$, $1|A_L| = 0$. Se $x \neq 1$, suponhamos que $x \in L$. Então, existem $p \in J$, $q \in G$ e uma trilha $T: p \xrightarrow{x} q$ em A (Proposição II.1.1). Seja

$$T = (p_1 = p, \sigma_1, p_2) \ldots (p_{n-1}, \sigma_{n-1}, p_n = q).$$

Se $x = \sigma_1$, então $p_2 = q \in p\sigma E$, donde $J\sigma E \cap G \neq \emptyset$ e $\sigma E_{p_0 p_0} = 1$. Portanto, (p_0, σ, p_0): $p_0 \xrightarrow{x} p_0$ com peso 1, e não existe trilha não trivial terminando em p_0 com peso 0. Pela Proposição 2 $x|A_L| = 1$.

Se $|x| > 1$, como $p_{n-1}\sigma_{n-1}H \cap G \neq \emptyset$ (pois contêm p_n), temos em A_L a aresta $(p_{n-1}, \sigma_{n-1}, p_0)$ com peso 1, e como

$$p_2 \in p_1\sigma_1 H \subset J\sigma_1 H,$$

existe em A_L a aresta (p_0, σ_1, p_2) com peso 0. Todas outras arestas de T são arestas de A_L com peso 0. Então,

$$T' = (p_0, \sigma_1, p_2)(p_2, \sigma_2, p_3) \ldots (p_{n-1}, \sigma_{n-1}, p_0): p_0 \longrightarrow p_0 \text{ e } T\rho = 1.$$

Portanto $x|A_L| = 1$.

Da mesma foram, dado $T: p_0 \xrightarrow{x} p_0$, com $T\rho = 1$, podemos reverter o argumento, encontrando uma trilha conveniente em A e mostrando que $x \in L$. □

COROLÁRIO 5.4 - Ainda com as mesmas hipóteses:

$$x|A_L| = \begin{cases} \min\{n \mid x \in (1 \cup L)^n\} & \text{se } x \in L^* \\ \infty & \text{caso contrário.} \end{cases}$$

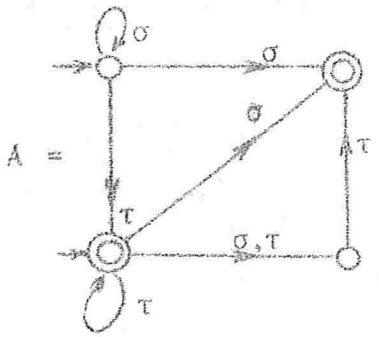
DEMONSTRAÇÃO - Se $x|A_L| = n < \infty$, existe uma trilha $T: p_0 \xrightarrow{x} p_0$, com peso n. Podemos então decompor $T = T_1 \ldots T_n$,

onde cada T_i: $p_0 \to p_0$ com peso 1. Sendo x_i a palavra soletrada por T_i, $x_i \in L-1$ pela Proposição 3, logo $x = x_1 \ldots x_n \in (1 \cup L)^n$, e $x \in L^*$. Segue que $x|A_L| = n \geq \min\{m / x \in (1 \cup L)^m\}$.

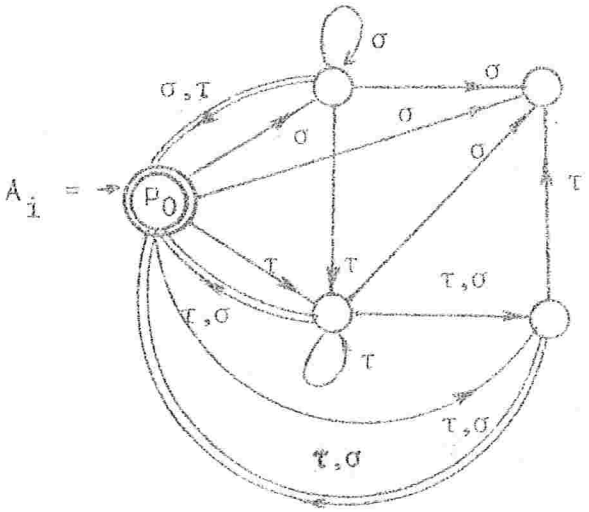
Por outro lado, se $x \in L^*$, então $x \in (1 \cup L)^n$ para algum n mínimo. Portanto, $x = x_1 x_2 \ldots x_n$, com $x_i \in L-1$, $i=1,\ldots,n$. Então, para cada x_i temos uma trilha T_i: $p_0 \xrightarrow{x_i} p_0$ com peso 1 em A_L, pela Proposição 3. Segue que $T = T_1 \ldots T_n$: $p_0 \xrightarrow{x} p_0$ com peso n. Portanto, $x|A_L| \leq T\rho = \min\{m / x \in (1 \cup L)^m\}$. □

Vejamos um exemplo:

Dado o autômato



que reconhece $L = \sigma^+ \cup \sigma^* \tau^+ (1 \cup \sigma \cup \sigma\tau)$, construímos:



onde as arestas indicadas por uma seta simples tem peso 0, e as indicadas por seta dupla $\Longrightarrow$ tem peso 1.

Observe que ele não é coacessível.

Chega agora o resultado que liga o conceito de conjuntos quase-periódicos com o de M-subconjuntos limitados. Para efeito de notação, lembremos que M_m é o semianel

$$M_m = \{0,1,\ldots,m,\infty\},$$

$\oplus$ como em M e $\otimes$ dado por a

$$a \otimes b = \begin{cases} a+b \text{ se } a+b \in M_m \\ m \text{ caso contrário.} \end{cases}$$

Vale para todo m, a inclusão de conjuntos $M_m \subset M$.

PROPOSIÇÃO 5.5 - São equivalentes:

(a) L é quase-periódico,

(b) M_{A_L} é finito,

(c) $|A_L|$ é limitado.

DEMONSTRAÇÃO - (a) implica (b): Seja n mínimo tal que $(1uL)^n = L^*$. Vamos mostrar que $M_{A_L} \subset M_Q(M_{n+1})$. Para isso, sejam

$$p,q \in Q, \quad x \in \Sigma^*.$$

Se $xE^*_{pq} = \infty$, nada a demonstrar. Senão $xE^*_{pq} = k < \infty$, e existe uma trilha $T: p \xrightarrow{x} q$ com peso k, e nenhuma trilha com peso $< k$ (Proposição 2). Podemos então decompor $T = T_1 T_2 \ldots T_k T_{k+1}$, onde $0 \leq i \leq k$, T_i termina em p_0 e tem peso 1 e $T_{k+1}: p_0 \xrightarrow{x} q$, com peso 0. Mas, daí, $T' = T_2 \ldots T_k: p_0 \xrightarrow{u} p_0$ e como T tem peso mínimo, T' tem peso k-1 que é mínimo entre as trilhas $p_0 \xrightarrow{u} p_0$. Portanto, $x|A_L| = k-1 \leq n$, pelo Corolário 4. Portanto, $T_p = k \leq n+1$, donde $xE^*_{pq} \in M_{m+1}$. O resultado segue, uma vez que $M_Q(M_{m+1})$ é finito.

(b) implica (c). Lema 2.5.

(c) implica (a). Como $|A_L|$ é limitado, tem imagem finita. Tomando-se $n = \max(\mathrm{Im}\,|A_L| - \infty)$, pelo Corolário 4, para todo $x \in \Sigma^*$, se $x \in L^*$, $x \in (1 \cup L)^n$. Portanto $L^* = (1 \cup L)^n$. □

Desta forma o problema de decidir se um conjunto reconhecível é quase-periódico se transforma num problema de decidir se um certo monóide finitamente gerado de matrizes sobre M é finito. Porém, a família de submonóides de $M_Q(M)$ que são da forma M_{A_L} é bem restrita, pois os geradores satisfazem certas condições especiais, conforme a construção. Assim, poderia haver algum algoritmo especial para esta classe de monóides, ainda que o problema geral seja indecidível. Não investigaremos isto aqui.

Note bem a semelhança entre o que se segue e algumas etapas das demonstrações do Teorema 4.1.

PROPOSIÇÃO 5.5 - Seja $A = (Q, I, F, E)$ um M-Σ-autômato. São equivalentes:

(a) M_A é finito

(b) $\forall q \in Q,\ \exists m \in \mathbb{N},\ \forall x \in \Sigma^*,\ x \in E^*_{qq} \in M_m$

(c) $\exists m \in \mathbb{N},\ \forall q \in Q,\ \forall x \in \Sigma^*,\ x \in E^*_{qq} \in M_m$

DEMONSTRAÇÃO - É claro que (a) implica (b) e (b) implica (c).

Para provarmos que (c) implica (a), seja k um inteiro tal que $\sigma E_{pq} \in M_k$ para todo σ, p, q.

Se $k = 0$, $xE^*_{pq} \subseteq M_0$ para todo x, p, q.

Se $k > 0$, vamos mostrar que

$$M_A \subseteq M_Q(M_{(m+k)|Q|}). \tag{5.2}$$

Para isso, sejam $p, q \in Q$ e $x \in \Sigma^*$. Se $xE^*_{pq} = \infty$, não há nada a demonstrar, portanto, podemos supor que exista uma trilha $T: p \xrightarrow{x} q$, como peso igual a xE^*_{pq}. Então, podemos fatorar

$$T = A_1T_1A_2T_2\ldots A_nT_n,$$

para algum $n < |Q|$, onde cada T_i é uma trilha fechada e

$$A_1A_2\ldots A_n$$

é um caminho de p para q (donde $|A_1A_2\ldots A_n| < |Q|$). (Para provar isso, basta considerar todas as trilhas de $p \longrightarrow q$ e seguir por indução do comprimento).

Segue que

$$T\rho = \sum A_i\rho + \sum T_i\rho$$

e como $A_i\rho \leq k|A_i|$ e $T_i\rho \leq m$, segue que

$$T\rho \leq \sum |A_i| + mn$$

$$< k|Q| + m|Q| = (k+m)|Q|.$$

Portanto, $xE^*_{pq} \subset M_{(k+m)|Q|}$, e M_A é finito. □

Vamos agora caracterizar as matrizes em $M_Q(M)$ que são periódicas. Para isso, dada uma matriz $A \in M_Q(M)$ construímos o M-σ-autômato A_A de forma análoga à secção anterior, $A_A = (Q,\infty,\infty,E)$ onde ∞ indica o vetor cujas componentes são ∞, e $\sigma E = A$. Assim, para todo $r \in \mathbb{N}$, $p,q \in Q$, $\sigma^r E^*_{pq} = A^r_{pq}$, e $M_{A_A} = \{A^n \mid n \geq 0\}$.

TEOREMA 5.6 (Simon [S6]) - Seja $A \in M_Q(M)$. Então A é periódica se e somente se cada componente fortemente conexa não trivial de A_A contêm um circuito de peso 0.

DEMONSTRAÇÃO - A condição é necessária:

Suponhamos que existe uma componente forte C, que não contenha nenhum circuito de peso 0. Segue que toda trilha com peso 0 contida em C tem comprimento $< |C|$, portanto, toda trilha contida em C, com comprimento $> n|C|$, onde

$n \in N$, tem peso $\geq n$. Como C é não trivial, existe um circuito

$$S: p \xrightarrow{\sigma^r} p$$

contido em C, com $0 < r \leq |C|$. Segue que para todo natural n, existe uma trilha

$$S^n: p \xrightarrow{\sigma^{rn|C|}} p,$$

com peso $\geq rn$. Portanto, $\sigma^{rn|C|}E^*_{pq} < \infty$. Assim, para todo n, temos a palavra $\sigma^{rn|C|}$ tal que

$$n \leq rn \leq \sigma^{rn|C|}E^*_{pp} < \infty$$

portanto, $A^{rn|C|}_{pp} \notin M_{n-1}$, e pela Proposição 5, A não é periódica.

A condição é suficiente. Para mostrar que M_A é finito, basta, pela Proposição 5, mostrar que dado $q \in Q$, existe $m \in N$ tal que para todo $n \geq 0$, $\sigma^n E^*_{qq} \in M_m$.

Seja C a componente forte de A_A contendo q. Se C é trivial, basta tomar $m = 0$. Se C é não trivial, existe um circuito G contido em C, com peso 0,

$$G: p \xrightarrow{\sigma^r} p,$$

onde $p \in C$ e $0 < r \leq |C|$. Desta forma, $\sigma^{nr}E^*_{pp} = 0$, para todo $n \in N$.

Como $q \in C$, existem caminhos

$$G_1: p \xrightarrow{\sigma^{r_1}} p \quad \text{e} \quad G_2: p \xrightarrow{\sigma^{r_2}} q,$$

e como G_1 e G_2 estão contidos em C, $0 \leq r_1, r_2 \leq |C|$.

Segue que o conjunto

$$R = \{x \in \Sigma^* / xE^*_{qq} < \infty\}$$

é infinito. Observe que o que buscamos é um natural m tal que $xE^*_{qq} \leq m$, para todo $x \in R$.

Se considerarmos o M-σ-autômato $A' = (Q, \delta^q, \delta^q, E)$, segue imeditamente que $R = s(|A'|)$ (lembremos que em $M = \delta^q_p = 0$ se $p = q$ e ∞ caso contrário). Como M é positivo, pelo Corolário II.3.10, R é reconhecível.

Seja A um Σ-autômato determinístico, com a estados, reconhecendo R, e seja

$$m = 4|C|ak,$$

onde k é um natural tal que $\sigma E \in M_Q(M_k)$. Vamos provar que $\sigma^n E^*_{qq} \leq m$, para todo n tal que $\sigma^n \in R$.

Se $n \leq 4|C|a$, não há nada a demonstrar, pois toda trilha de comprimento n tem peso $\leq nk$. Se $n \leq 4|C|a$, vamos relembrar que A tem que ser da forma:

para algum ℓ, onde os estados finais não foram assinalados. Como $n > a$ e $\sigma^n \in |A|$, existe um inteiro α, $\ell \leq \alpha \leq a$, tal que o estado α é final. Mas então, fazendo $\pi = a-\ell+1$, é claro que $\sigma^{\alpha+\gamma\pi} \in |A| = R$, para todo natural γ, e, em particular $n = \alpha+\beta\pi$, para algum $\beta \in N$.

Como:

$$\beta = \frac{n-\alpha}{\pi} > \frac{4|C|a-a}{a} = 4|C|-1,$$

existem inteiros não negativos γ, δ, tal que $\delta < r = |G|$ e

$$\beta - r_1 - r_2 = \gamma r + \delta.$$

Portanto,

$$n = \alpha + \beta\pi = \alpha + (r_1 + r_2 + \gamma r + \delta)\pi$$

$$= \alpha + \delta\pi + (r_1 + r_2 + \gamma r)\pi.$$

Agora, $z = \sigma^{\alpha+\delta\pi} \in R$. Seja então $T_i : q \xrightarrow{z} q$, com peso mínimo. Então, $T_1\rho \leq (\alpha+\delta\pi)k \leq (a+ra)k \leq 2|C|ak$.

Portanto,

$$T_1(G_1G^{\gamma}G_2)^{\pi} : q \xrightarrow{\sigma^n} q$$

e

$$[T_1(G_1G^{\gamma}G_2)^{\pi}]\rho = T_1\rho + \pi \cdot G_2\rho + \gamma\pi \cdot G\rho$$

$$\leq 2|C|ak + ar_1k + ar_2k + 0$$

$$\leq 4|C|ak = m,$$

e $\sigma^n E^*_{qq} \leq m$, como afirmamos. □

COROLÁRIO 5.7 - Um subconjunto reconhecível σ^* (alfabeto unitário) contendo alguma palavra não vazia é quase-periódico sse for infinito.

DEMONSTRAÇÃO - Se L é infinito, reconhecível, tomando-se o σ-autômato determinístico conexo A que reconhece L, é imediato que ele contém um circuito. Construindo-se A_L a partir de A, obtem-se uma única componente forte, onde o circuito original de A tem peso 0. □

O Teorema 6 tem consequências análogas às do Teorema 4.8.

COROLÁRIO 5.8 - É decidível se uma matriz em $M_Q(M)$ é periódica.

COROLÁRIO 5.9 - Sejam $A, B \in M_Q(M)$ e suponhamos que para todo $p,q \in Q$,

$$A_{pq} = \infty \text{ implica } B_{pq} = \infty$$

e

$$A_{pq} = 0 \text{ implica } B_{pq} = 0.$$

Então, se A é periódica, B também o é.

Os Corolários 8 e 9 tem demonstrações análogas aos Corolários 4.10 e 4.12.

COROLÁRIO 5.10 - Dado um M-Σ-autômato A, é possível decidir se M_A é periódico.

DEMONSTRAÇÃO - Análoga à do Teorema 4.1, versão algébrica, bastando substituir $\phi_2 : N \to N_2$ por

$$\phi' : M \to M_1$$

dada por

$$x\phi' = \begin{cases} x \text{ se } x \in M_1 \\ 1 \text{ caso contrário.} \end{cases} \qquad \square$$

Assim, o problema de decidir se um conjunto reconhecível é quase-periódico é deixado na dependência de uma resposta afirmativa ao problema de Burnside para matrizes com coeficiente em M; porém lembramos que os dois problemas não são (até prova em contrário) equivalentes.

BIBLIOGRAFIA

ADJAN, S.I. -

ver [NA1]

ARBIB, M.A. -

[A1] "Algebraic Theory of Machines,Languages and Semigroups", (ed.) Academic Press, N.Y.,1968.

BERGE, C. -

[B1] "Theorie des Graphes et ses Applications",Dunod, Paris, 1958.

BIGGS, N. -

[B2] "Algebraic Graph Theory", Cambridge University Press, London, 1974.

BRZOZOWSKI, J.A. -

[B3] Roots of Star Events, JACM, 14:3 (July 1967), pp. 466-477.

[BS1] (com SIMON,I.) -

Caracterization of Locally Testable Events, Discrete Math., 4 (1973), pp. 243-271.

CARLYLE, J.W. (com PAZ, A.) -

[CP1] Realizations by sthocastic finite automata,J. Computer Systems Sc., 5, 1971, pp. 26-40.

CLIFFORD, A.H. (com PRESTON, G.B.) -

[CP2] "The Algebraic Theory of Semigroups", vol. 1; Amer. Math. Soc., Providence (R.I.), 1967.

CURTIS, C.W. (com REINER, I.) -

[CR1] "Representation Theory of Finite Groups and Associative Algebras", Pure and Applied Mathematics, XI, Interscience, N.Y., 1963.

CHOMSKY, N.(com SCHUTZENBERGER, M.P.) -

[CS1] The Algebric Theory of Context - Free Languages in "Computer Programming and Formal Languages", (P.Brafford e D.Hirschberg ed.), pp. 118-161, North Holland, Amsterdam, 1963.

EILENBERG, S. -

[E1] "Automata, Languages and Machines", Academic Press, Vol. A (1974),New York.

ERDOS, P. (com SZEKERES, G.) -

[ES1] A Combinatorial problem in Geometry, Compositio Matematika, 2, (1935), pp. 463-470.

FEOFILOFF, P. -

[F0] Sobre os números de Ramsey, Dissertação de Mestrado, DMA-IME-USP, 1974.

FLIESS, M. -

[F1] Sur Certaines Familles de Series Formelles, Thèse Sc. Math., Univ. Paris VII,Paris,(1972).

[F2] Matrices de Hankel, J.Math.Pures Appl., 53, (1974).

GANTMACHER F.R. -

[G1] "Théorie des matrices", vol. 2, Dunod, Paris, 1966.

HARARY, F. -

[H1] "Graph Theory", Addison-Wesley, Reading,Mass., (1971).

HEDLUND, G. -

ver [MH1].

HELLER, A. -

[H2] On Stochastic Processes Derived from Markov

Chains, Ann.Math.Statistics,36,(1965),pp.1.286-1.291.

HOFFMAN, K. (com KUNZE, R.) -

[HK1] "Álgebra Linear", Ed.Polígono, São Paulo, (1971).

JACOB, G. -

[J1] Representations et Substituitions Matricielles dans la Theorie Algebrique des Transductions, Thèse Sc.Math., Univ. Paris VII, Paris, (1975).

[J2] Un Théorème de factorisation des produits d'endomorphismes de K^n. A aparecer no J. of Algebra.

KAPLANSKY, I. -

[K1] "Fields and Rings", 2nd ed., The Univ. of Chicago Press, Chicago and London, 1972.

KLEENE, S.C. -

[K2] Representation of Events in Nerve Nets "Automata Studies" (C.E.Shanon & J.McCarthy edit.) pp. 3-40, Princeton Univ.Press, Princeton, (N.J.), 1956.

KROHN, K. (com RHODES, J.L.) -

[KR1] Algebraic Theory of Machines I, Prime Decomposition Theorem for Finite Semigroups and Machines, Trans. Amer. Math. Soc., 116, (1965), pp. 450-464.

KUNZE R. -

ver [HK1].

Mc CARTHY, P.J. -

[M1] "Algebraic Extensions of Fields", Blaisdell, Waltham, Mass., 1966.

Mc NAUGHTON, R. -

[M2] Algebraic Decision Procedures for local testability, Math.Sys. Th., 8, (1974), pp. 60-76.

[MP1] (com PAPERT, S.) - "Counter-Free Automata", Research Monograph N.65, The MIT Press, Cambridge, Mass., 1971.

[MZ1] (com ZALCSTEIN,Y.) - The Burnside Problem for Semi-

groups, J.of Algebra, 34, (1975), pp.292-299.

MONTEIRO, L.H.J. -

[M3] "Elementos de Álgebra", Ao Livro Técnico S.A. Rio de Janeiro, 1971.

MORSE, M. (com HEDLUND, G.) -

[MH1] Unending Chess, Symbolic Dinamics and a Problem on Semigroups, Duke Math. J., 11, (1944) pp. 1-15.

NOVIKOV, P.S. (com ADJAN, S.I.) -

[NA1] Infinite Periodic Groups I, II, III;Math USSR Izv, 2 (1968), pp.209-236; 241-279; 665-685.

PAPERT, S. -

ver [MP1].

PAZ, A. -

ver [CP1].

PRESTON, G.B. -

ver [CP2].

RAMSEY, F.P. -

[R1] On a problem of formal logic. Proc.London Math. Soc., 2nd series, 30, (1930), pp. 264-286.

RABIN, M.O. (com SCOTT, D.) -

[RS1] Finite Automata and their Decision Problems, IBM J. Research Develop. 3,(1959),pp.114-125.

REINER, I.

ver [CR1].

RHODES, J.L.

ver [KR1].

RYSER, H.J. -

[R2] "Combinatorial Mathematics", Math. Ass.of America, John Wiley & Sons, Inc., 1963.

SALOMAA, A. -

[S1] "Formal Languages", Acad.Press, N.Y. and London, 1973.

SCHUR, I. -

[S2] Über Gruppen Periodischer Substitionen, Sitzungsbericht Preuss. Akad.Wiss, (1911). pp. 619-627.

SCHUTZENBERGER, M.P. -

[S3] On the Definition of a Family of Automata, Inf. and Control, 4, (1961), pp.245-270

[S4] Certain Elementary Families of Automata. Proc. Symp. Math. Theory of Automata, N.Y., 1962.pp. 139-153.

[S5] On Finite Monoids Having Only Trivial Subgroups. Inf. and Control, 8, (1965), pp.190-194. ver também [CS1].

SCOTT, D.

ver [RS1].

SIMON, I. -

[S6] On Limited Events, Mineografado no DMA, IME-USP, fevereiro, 1974.

[S7] Piecewise Testable Events In "Automata Theory and Formal Languages 2nd GI Conference", (H. Brakhage ed.), Lecture Notes in Computer Science 33, Springer-Verlag, Berlin, 1975, pp. 214-222.
ver também [BS1].

SZEKERES, G. ver [ES1].

ZALCSTEIN, Y. -

[Z1] Locaĺy Testable Languages, J. of Comp.and Sys. Sc., 6, (1972), pp. 151-167.
ver também [MZ1].

ÍNDICE DE DEFINIÇÕES

acíclico. 110
alfabeto. 5
aresta. 14
— início. 14
— término 14
autômato. 14
— completo. 17
— determinístico. 17

B-subconjunto característico. 9

caminho 90
circuito. 90
coluna. 50
componente forte. 99
— trivial 99
comprimento 5
congruência 3
— sintática 4
— — de K-subconjunto. 65
conjunto quociente. 2
construção dos subconjuntos 19
cotado. 80

2-potente 98

epimorfismo 3
estados 14
— finais. 14
— iniciais. 14
estrela 4

família localmente finita 10
fatoração 5
função característica 9
função parcial. 2

gerador 112
— mínimal 112
gramática 22

idempotente 82
índice. 2
isomorfismo 3

K-Σ-autômato. 24
— acessível 86
— aresta. 26
— coacessível 86
— conexo. 86
— comportamento 15
— determinístico. 69
— estados 24
— isomorfos 53
— monóide 66
— normalizado 28
— reduzido. 56
K-subconjunto 9
— congruência sintática 65
— limitado. 68
— monóide sintático 65
— não-ambíguo 9
— racional. 37
— reconhecível. 25
— unitário. 10
K-reconhecível. 26

letra 5
linguagem 22
linha 50

matriz. 8
— de Hankel 50
— — posto 51
— quadrada. 8
monomorfismo. 3
monóide 3
— de autômato 17
— de K-Σ-autômato 66
— livre 15
— quociente 3
— periódico 82
— sintático 4
— — de K-subconjunto. 65
morfismo. 3
multiplicidade. 9

palavra 5
parte quase-inversível. 12
periódico 82
peso. 26
polinômio 12
— ciclotômico 101
prefixo 108
projeção canônica 2
pseudo-regular. 47

quase-inversa 12
quase-inversível. 12
quase-periódico 111

racionalmente fechado 37
reconhecível. 16,24
relação 1
reverso 108
rotação 90
rótulo. 14

semianel. 6
— completo. 10
— comutativo. 6
— graduado. 105
— limitador 72
— positivo. 7
semigrupo 3
série formal. 11
Σ-autômato. 14
— comportamento 15
soletrar. 15
sufixo. 109
suporte 9

trilha. 15
— rótulo. 15
— trivial 15

vetor final 24
vetor inicial 24