Representação de Sistemas Dinâmicos Fechados de Memória Finita com Restrições Periódicas

Daniel P. B. Chaves e Cecilio Pimentel

***Resumo*— Sistemas dinâmicos simbólicos de memória finita com restrições periódicas (PFT, do inglês periodic shift of finite type) formam a classe (na teoria de dinâmica simbólica) utilizada para modelar conjuntos de seqüências com restrição empregadas tanto para correção de erros quanto para codificação de linha. Neste trabalho a teoria de dinâmica simbólica é empregada como ferramenta matemática para abordar o problema da representação de seqüências de símbolos que podem ser modeladas como PFTs. Utilizando a teoria algébrica de linguagens, apresentaremos um novo procedimento para gerar grafos determinísticos com um número mínimo de vértices que apresentam a linguagem de um PFT irredutível.**

***Palavras-Chave*— Dinâmica simbólica, grafos direcionados, códigos de linha, sistemas com restrição.**

***Abstract*— Periodic shifts of finite type (PFT) is the symbolic dynamical system applied to study sets of sequences that have both error control and line coding properties. In this work the theory of symbolic dynamics is applied as a mathematical tool for studying the presentation of sequences that form a PFT. A new procedure is proposed to generate the minimal deterministic presentation of an irreducible PFT, based on algebraic language theory.**

***Keywords*— Symbolic dynamics, directed graphs, line codes, constrained systems.**

I. INTRODUÇÃO

Em sistemas de comunicação e gravação empregam-se os códigos corretores de erro (CCE) para correção de um número determinado de erros introduzidos pelo canal. Alguns destes sistemas também empregam os códigos de linhas (CL), que restringem as possíveis seqüências de saída, adequando-as às características do canal e, portanto, reduzindo a chance de ocorrências de erros.

Exemplos de sistemas que apresentam restrições são o MTR(j) - *maximum transition run* - que restringe o número máximo de 1's consecutivos a j e o RLL(d,k) - *run-length limited* - que restringe o número mínimo de 0's consecutivos a d e o máximo a k. Em sistemas que empregam codificação conjunta CL/CCE, pode-se propor um codificador que corrige um número determinado de erros e satisfaz as restrições do canal. Mas na prática as propriedades de correção e restrição de seqüências são obtidas pela concatenação de um codificador CCE e um CL. A concatenação não pode ser realizada de forma arbitrária, pois as operações realizadas por um codificador (na codificação ou decodificação) podem restringir o desempenho do outro [1].

Em [2], Wijngaarden e Immink propuseram um esquema de concatenação que codifica uma seqüência sem restrição em uma com restrição onde um conjunto definido de posições de bits na seqüência são reservados para bits de paridade do CCE. Os bits nessas posições podem ser modificados arbitrariamente sem violar a restrição, portanto são chamadas posições sem restrição. Assim, os bits de paridade do código CCE podem ser inseridos nas posições sem restrição da seqüência de saída do CL sem violarem a restrição do canal.

O conjunto de seqüências de saída geradas pelo esquema de codificação conjunta proposto por Wijngaarden e Immink pode ser modelado empregando os PFT, como proposto em [3]. Definido o PFT associado ao conjunto de seqüências restritas, através da especificação de um conjunto finito de palavras indexadas proibidas (seção II-B), pode-se construir um grafo determinístico que represente esse conjunto. O grafo obtido é utilizado em algoritmos para determinação de codificadores CL/CCE [4].

Neste artigo apresentamos um procedimento para construção de grafos determinísticos e reduzidos que representam o conjunto de seqüências restritas. Tendo como particularidade a geração de uma apresentação determinística e reduzida. Enquanto que outros procedimentos [5],[3] requerem a posterior aplicação de algoritmos para redução de estados, e em alguns casos determinização da apresentação inicial.

II. CONCEITOS E DEFINIÇÕES

A. Dinâmica simbólica e linguagens formais

Apresentamos nesta seção uma introdução aos conceitos de Dinâmica Simbólica [6],[7],[1] e Teoria de Linguagens Formais [8], [9]. Primeiramente, denotamos por $\mathcal{A}^{\mathbb{Z}}$ o conjunto de todas as seqüências bi-infinitas de símbolos em um alfabeto $\mathcal{A}$ e chamamos estas seqüências de *pontos* em $\mathcal{A}^{\mathbb{Z}}$. Uma seqüência finita de símbolos sobre $\mathcal{A}$ é chamada de *palavra*. O comprimento de uma palavra w é denotada por $|w|$. Para todo $x \in \mathcal{A}^{\mathbb{Z}}$ e $i \leq j$, denota-se a palavra em x, da coordenada i a j por $x_{[i,j]} = x_i x_{i+1} \ldots x_j$. Se $i > j$, define-se $x_{[i,j]} = \varepsilon$. Pode-se definir um sistema simbólico fechado, X, a partir de um conjunto $\mathcal{F}$ de palavras sobre $\mathcal{A}$ como: X é o conjunto de pontos em $\mathcal{A}^{\mathbb{Z}}$ que não possuem palavras no *conjunto de palavras proibidas* $\mathcal{F}$.

A *linguagem* de X, denotada por L, é o conjunto de todas as palavras que ocorrem em pontos de X, incluindo a palavra vazia, i.e. possui a propriedade $\varepsilon\ w = w\ \varepsilon = w$. Na prática os sistemas simbólicos fechados de maior interesse são os *irredutíveis*, sendo aqueles que para quaisquer $u, v \in L$, existe um w, tal que, $uwv \in L$.

Daniel P. B. Chaves, Departamento de Telemática, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, E-mail: ddselec@oi.com.br. C. Pimentel, Grupo de Pesquisa em Comunicações - CODEC, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, C.P. 7800 - Recife - PE, 50711-970, E-mail: cecilio@ufpe.br. Este trabalho recebeu suporte parcial do CNPq, No. 301253/2004-8, e da FACEPE, Processo BPD-0032-3.04/06.

Seja $G = (\mathcal{V}, \mathcal{E}, \mathcal{L})$ um grafo com conjunto de vértices $\mathcal{V}$, conjunto de ramos $\mathcal{E}$ e função de rotulação $\mathcal{L} : \mathcal{E} \to \mathcal{A}$. Definimos as funções $i : \mathcal{E} \to \mathcal{V}$ e $t : \mathcal{E} \to \mathcal{V}$ representando o vértice inicial e terminal de um ramo, respectivamente. X é um conjunto de seqüências obtidas concatenando-se os rótulos dos ramos percorridos por caminhos em G. Diz-se, então, que G é uma apresentação de X. Um grafo G é irredutível se para qualquer par de vértices $I, J \in \mathcal{V}$ existe um caminho entre I to J. Dado um vértice $I \in \mathcal{V}$ para o qual nenhum ramo inicia em I ou nenhum ramo termina em I; este pode ser removido juntamente com os ramos $e \in \mathcal{E}$, $t(e) = I$ ou $i(e) = I$. Um grafo que não permite tal eliminação de vértices é dito *essencial*. O contexto à direita de um vértice $I \in \mathcal{V}$, denotado por $\mathsf{F}(I)$, é o conjunto de todas as palavras que podem ser geradas por caminhos em G começando em I. Uma apresentação é *reduzida* se $\mathsf{F}(I) = \mathsf{F}(J)$ implica que $I = J$. Um grafo G é chamado *determinístico* se para todo $e_1, e_2 \in \mathcal{E}$, $i(e_1) = i(e_2)$ e $\mathcal{L}(e_1) = \mathcal{L}(e_2)$, então $e_1 = e_2$. O Shannon cover é definido como uma apresentação reduzida, irredutível e determinística, sendo isomorfas quaisquer apresentações que satisfaçam tais condições [6, Proposição 3.3.17].

Se $\mathcal{A}$ e $\mathcal{B}$ são conjuntos de palavras com símbolos em um alfabeto $\mathcal{A}$, denota-se pela concatenação de $\mathcal{A}$ e $\mathcal{B}$ o conjunto $\mathcal{AB} = \{uv | u \in \mathcal{A} \text{ e } v \in \mathcal{B}\}$. Decorre da operação de concatenação entre conjuntos que $\mathcal{A}^+ = \bigcup_{i=1}^{\infty} \mathcal{A}^i$, onde $\mathcal{A}^1 = \mathcal{A}$ e para $n \geq 2$, $\mathcal{A}^n = \mathcal{A}^{n-1}\mathcal{A}$. O conjunto $\mathcal{A}^* = \varepsilon \cup \mathcal{A}^+$ recebe a denominação especial de *fechamento de Kleene*. Qualquer subconjunto de $\mathcal{A}^*$ é denominado uma *linguagem formal* (por simplicidade, iremos chamá-lo de linguagem). Assim, $\mathcal{A} \subseteq \mathcal{A}^*$ é uma linguagem. O *complemento* de $\mathcal{B}$ com relação a $\mathcal{A}$ é definido como $\mathcal{B}' = \{v | \ v \in \mathcal{A} \text{ e } v \notin \mathcal{B}\}$. O *conjunto de prefixos* de $\mathcal{A}$, representado por $\mathcal{P}(\mathcal{A})$, é definido como $\mathcal{P}(\mathcal{A}) = \{v | \ \exists \, u \in \mathcal{A}^*, \ vu \in \mathcal{A}\}$, e o *conjunto de sufixos* de $\mathcal{A}$, representado por $\mathcal{S}(\mathcal{A})$, é definido como $\mathcal{S}(\mathcal{A}) = \{v | \ \exists \, u \in \mathcal{A}^*, \ uv \in \mathcal{A}\}$. Definimos os conjuntos $\mathcal{AB}^{-1} = \{v | \ \exists \, u \in \mathcal{B}, \ vu \in \mathcal{A}\}$ e $\mathcal{B}^{-1}\mathcal{A} = \{v | \ \exists \, u \in \mathcal{B}, \ uv \in \mathcal{A}\}$, portanto, $\{111, 110, 000\}\{1\}^{-1} = \{11\}$ e $\{1\}^{-1}\{111, 110, 000\} = \{11, 10\}$.

B. Sistemas dinâmicos simbólicos fechados de memória finita com restrições variantes no tempo

O conceito de sistemas simbólicos dinâmicos de memória finita é estendido para o caso com restrições periódicas em [10]. Posteriormente, foi utilizado em [5] e [3] para determinação de apresentações determinísticas empregadas na construção de códigos que realizam codificação conjunta CL/CCE.

Determinado um inteiro positivo T, seja $\mathcal{F}$ uma coleção finita de palavras em $\mathcal{A}^*$, tal que, para cada $w_i \in \mathcal{F}$ é associado um inteiro k_i em $\{0, 1, \ldots, T-1\}$ que recebe o nome de *fase*. Descrevemos o conjunto $\mathcal{F}$ por $\mathcal{F} = \{(w_1, k_1), (w_2, k_2), \ldots, (w_n, k_n)\}$ e o chamamos de *conjunto proibido periódico*. As restrições associadas a uma fase k são escritas por $\mathcal{F}^{(k)} = \{w | \ (w, n) \in \mathcal{F} \text{ e } n = k\}$. Seja uma palavra finita w um fator de uma seqüência finita ou infinita x na coordenada i, portanto $w = x_{[i, i+|w|-1]}$, isto é representado por $w \prec_i x$, o contrário é representado por $w \not\prec_i x$. Escrevemos $w \prec x$ quando uma palavra w é um fator de uma seqüência x, sem considerar uma coordenada específica, o contrário é representado por $w \not\prec x$. Uma palavra w é um fator próprio de uma seqüência x, quando $w \prec x$ e $w \neq x$. Um PFT com período T e conjunto proibido periódico $\mathcal{F}$, representado por $\mathsf{X}_{\{\mathcal{F}, T\}}$, é definido a seguir.

Definição 1: Uma seqüência bi-infinita x pertence a $\mathsf{X}_{\{\mathcal{F}, T\}}$ se, e somente se, existe um inteiro $k \in \{0, \ldots, T-1\}$ tal que, para todo inteiro i, se $w \prec_i \sigma^k(x)$ então $w \notin \mathcal{F}^{(i \mod T)}$.

Para todo PFT é possível construir um grafo G que o apresente. G é dito *T-partite* se $\mathcal{V}$ pode ser dividido em T subconjuntos $D_0, \ D_1, \ldots, D_{T-1}$, tal que, qualquer ramo que parte de um vértice em D_i alcança um vértice em $D_{i+1 \mod T}$. Para $I, J \in \mathcal{V}$, o número de ramos que partem de I e alcançam J é A_{IJ}. A *matriz adjacência* de G é quadrada, de ordem $|\mathcal{V}|$ e é denotada por $A_G = [A_{IJ}]$. O *período de um vértice* I, representado por $\mathsf{per}(I)$, é o máximo divisor comum dos inteiros n para os quais $(A_G^n)_{II} > 0$. Caso este número não exista, então denota-se $\mathsf{per}(I) = \infty$. O *período de uma matriz* A, representado por $\mathsf{per}(A)$, é o máximo divisor comum dos números $\mathsf{per}(I)$ que são finitos, ou é ∞ se $\mathsf{per}(I) = \infty$ para todo I. O *período de um grafo* G, representado por $\mathsf{per}(G)$, é o período de A_G, *i.e*, $\mathsf{per}(G) \triangleq \mathsf{per}(A_G)$. Se G é irredutível, todos os estados têm o mesmo período [6, Lema 4.5.3], se $\mathsf{per}(A_G) = T$, então G é *T-partite* e os conjuntos $D_1, \ D_2, \ldots, \ D_{T-1}$ são as T *classes periódicas* do grafo.

Se o PFT é irredutível, podemos determinar seu Shannon cover aplicando métodos convencionais para construção de grafos determinísticos[10], [3]. Em nossa abordagem, sempre estaremos considerando o período como sendo o do Shannon cover, portanto, lembramos que parte dos resultados só são válidos para PFT irredutíveis.

Associado ao conceito de restrição por fase está o de linguagem por fase, que empregaremos para descrever as restrições de palavras em $\mathcal{A}^*$ para uma fase específica.

Definição 2: Seja $\mathcal{L}_x \subseteq \{0, \ldots, T-1\}$ o conjunto de deslocamentos de um ponto $x \in \mathcal{A}^{\mathbb{Z}}$ tal que $\forall i \in \mathbb{Z}$ e $\ell_x \in \mathcal{L}_x$ se $v \prec_i \sigma^{\ell_x}(x)$ então $v \notin \mathcal{F}^{(i \mod T)}$. Definimos uma linguagem associada com a fase k como $L^{(k)} = \{u \prec_j \sigma^{\ell_x}(x) | \ x \in \mathsf{X}_{\{\mathcal{F}, T\}}, \ \ell_x \in \mathcal{L}_x \text{ e } j \equiv k \mod T\}$.

Um conceito similar ao de coleção mínima de palavras proibidas de um SFT existe para um PFT, sendo chamado de *conjunto mínimo periódico de palavras proibidas* $\mathcal{O}$, contendo os elementos $(w, k) \in \mathcal{A}^* \times \{0, \ldots, T-1\}$, $w = w_0 w_1 \ldots w_n$, que não pertencem a linguagem $L^{(k)}$ mas com todos os fatores próprios $u \prec_i w$ pertencendo a linguagem $L^{(k+i \mod T)}$. Portanto, $(w, k) \in \mathcal{O}$ se, e somente se, $w \notin L^{(k)}$, $w_{[0, |w|-2]} \in L^{(k)}$ e $w_{[1, |w|-1]} \in L^{(k+1 \mod T)}$. Quando T é o período do Shannon cover, o conjunto $\mathcal{O}$ é único [10, Teorema 4]. O maior comprimento das palavras em $\mathcal{O}$ é dito a *memória* do PFT.

Exemplo 1: Como exemplo da dependência da linguagem com a fase, consideremos $\mathcal{O} = \{(101, 0), (111, 1)\}$ e $T = 2$. Observe que $11100 \in L^{(0)}$ e $1010 \in L^{(1)}$, no entanto, $1010 \notin L^{(0)}$ e $11100 \notin L^{(1)}$.

Motivados pela Definição 2, quando queremos enfatizar que $w \in L^{(k)}$ escrevemos (w, k). Se (w, k) não é definido, logo $w \notin L^{(k)}$, implicando que os elementos em $\mathcal{O}^{(k)}$ proíbem a ocorrência de w, o que não impede que $w \in L$, pois esta poderá pertencer a uma linguagem $L^{(j)}$ com $j \neq k$. Como uma extensão dessa definição, dizemos que (s, j) é um fator de (w, k) se $s \prec_t w$ e $j \equiv k + t \mod T$. Se $s \prec_0 w$ então (s, k) é um prefixo de (w, k) (prefixo próprio se $|s| < |w|$). Quando $s \prec_t w$ e $k+t+|s| \equiv k+|w| \mod T$ então $(s, k+t \mod T)$ é um sufixo de (w, k) (sufixo próprio se $t > 0$). Na próxima definição estenderemos o conceito de contexto à direita de uma palavra $w \in \mathcal{A}^*$ para um elemento (w, k).

Definição 3: O contexto à direita de $w \in L$ associado a uma fase k é $\mathsf{F}(w, k) = \{s|\ ws \in L^{(k)}\}$. O complemento do contexto à direita em relação a linguagem L é dado por $\mathsf{F}\,'(w, k) = L \backslash \mathsf{F}(w, k)$, ou $\mathsf{F}\,'(w, k) = \{s \in L|\ ws \notin L^{(k)}\}$.

Exemplo 2: Como exemplo do contexto à direita de uma palavra associado a uma fase, consideremos o conjunto $\mathcal{O}$ e período do Exemplo 1. Para $w = 1$, temos que $11 \in \mathsf{F}(1, 0)$ e $01 \in \mathsf{F}(1, 1)$, no entanto, $01 \notin \mathsf{F}(1, 0)$ e $11 \notin \mathsf{F}(1, 1)$.

Caso (w, k) não seja definido, então para todo $s \in L$ teremos que $ws \notin L^{(k)}$. Portanto, para todo $w \notin L^{(k)}$, segue da Definição 3 que $\mathsf{F}(w, k) = \emptyset$, implicando que $\mathsf{F}\,'(w, k) = L$.

Definição 4: Seja $(w, k) \in L \times \{0, \ldots, T-1\}$. Um conjunto $\mathcal{C}(w, k) \subseteq L \times \mathbb{N} \cup \{0\}$, chamado conjunto das restrições de (w, k), satisfaz as propriedades:

a. Seja $(u, j) \in \mathcal{C}(w, k)$. Se $u \prec_j s$, $s \in L$, então $ws \notin L^{(k)}$;
b. Seja $s \in L$ e $ws \notin L^{(k)}$, então existe $(u, j) \in \mathcal{C}(w, k)$ tal que $u \prec_j s$.

Quando $w \notin L^{(k)}$, definimos $\mathcal{C}(w, k) = (\varepsilon, 0)$.

Definimos a seguir um operador que quando aplicado ao conjunto das restrições de um elemento (w, k) determina o contexto à direita da palavra w, o que será demonstrado na proposição seguinte.

Definição 5: Seja $\mathcal{C}(w, k)$ o conjunto das restrições de $(w, k) \in L \times \{0, \ldots, T-1\}$. Se $w \in L^{(k)}$ então $[\mathcal{C}(w, k)] = \{s \in L|\ \exists (u, j) \in \mathcal{C}(w, k)$ tal que $u \prec_j s\}$, caso contrário $[\mathcal{C}(w, k)] = L$.

Proposição 1: Seja L a linguagem de um PFT. Se $w \in L$ então $[\mathcal{C}(w, k)] = \mathsf{F}'(w, k)$. Portanto, $[\mathcal{C}(w, k)] = [\mathcal{C}(w', j)]$ se, e somente se, $\mathsf{F}(w, k) = \mathsf{F}(w', j)$.

Demonstração: Se $w \notin L^{(k)}$ então $ws \notin L^{(k)}$ para todo $s \in L$, logo $\mathsf{F}'(w, k) = L$. Da Definição 5, se $w \notin L^{(k)}$ então $[\mathcal{C}(w, k)] = L$. A seguir consideramos que $w \in L$.

Se $s \in \mathsf{F}'(w, k)$ então $ws \notin L^{(k)}$, logo da Definição 4-b existe $(u, j) \in \mathcal{C}(w, k)$ tal que $u \prec_j s$ e, portanto, $s \in [\mathcal{C}(w, k)]$, conseqüentemente $\mathsf{F}'(w, k) \subseteq [\mathcal{C}(w, k)]$. De modo reverso, se $s \in [\mathcal{C}(w, k)]$, então pela Definição 5 existe $(u, j) \in \mathcal{C}(w, k)$ tal que $u \prec_j s$. Da Definição 4-a $ws \notin L^{(k)}$ e, portanto, $s \in \mathsf{F}'(w, k)$, logo $[\mathcal{C}(w, k)] \subseteq \mathsf{F}'(w, k)$.

Se $[\mathcal{C}(w, k)] = [\mathcal{C}(w', j)]$ então $\mathsf{F}'(w, k) = \mathsf{F}'(w', j)$, logo da Definição 3 concluímos que $\mathsf{F}(w, k) = \mathsf{F}(w', j)$. Se agora considerarmos que $\mathsf{F}(w, k) = \mathsf{F}(w', j)$, então $\mathsf{F}'(w, k) = \mathsf{F}'(w', j)$ e, portanto, $[\mathcal{C}(w, k)] = [\mathcal{C}(w', j)]$. ■

III. DETERMINAÇÃO DE PALAVRAS COM MESMO CONTEXTO À DIREITA

No caso de um PFT as restrições estão associadas a fases, portanto, geralmente dependem da fase escolhida como referência, *e.g.*, se a partir da fase 0 qualquer palavra w com $v \prec_i w$ e $v \in \mathcal{O}^{(i)}$ não pode ocorrer, em relação a fase j as palavras u com $v \prec_{(i-j \mod T)} u$ não poderão ocorrer. Logo, com relação a fase j o conjunto das restrições considerado é $\{(v, i-j \mod T)|\ (v, i) \in \mathcal{O}\}$.

A dependência das restrições com a fase torna a definição do contexto à direita de uma palavra w dependente não só desta e do conjunto $\mathcal{O}$, como também da fase. Assim, para representarmos as restrições de uma palavra w com relação a uma fase k, iremos dividir $\mathcal{C}(w, k)$ em dois subconjuntos, enquanto um depende dos sufixos de w e da fase k, o outro depende do comprimento de w e da fase k.

Definição 6: Seja $\mathcal{A} \subseteq L \times \{0 \ldots T-1\}$. Definimos a representação da expansão do conjunto $\mathcal{A}$ para um período T por $< \mathcal{A} >= \{(s, j)|\ (s, j \mod T) = (s, i)$ para todo $(s, i) \in \mathcal{A}$ e $j \geq 0\}$.

Definição 7: Seja w uma palavra da linguagem de um PFT. Se $w \in L^{(k)}$ então $\mathcal{C}^d_{\mathcal{O}}(w, k) = \{(s, 0)|\ s \in L^{(k+|w| \mod T)}$ e $\exists p \in \mathcal{S}(w) \backslash \{\varepsilon\}$ para o qual $ps \in \mathcal{O}^{(k+|w|-|p| \mod T)}\}$ e $\mathcal{C}^i_{\mathcal{O}}(w, k) = \{(s, j)|\ (s, j) = (s, i-k-|w| \mod T)$ para algum $(s, i) \in \mathcal{O}\}$. Se $w \notin L^{(k)}$ definimos $\mathcal{C}^d_{\mathcal{O}}(w, k) = \mathcal{C}^i_{\mathcal{O}}(w, k) = (\varepsilon, 0)$. Definimos $\mathcal{C}_{\mathcal{O}}(w, k) = \mathcal{C}^d_{\mathcal{O}}(w, k) \cup < \mathcal{C}^i_{\mathcal{O}}(w, k) >$ como o conjunto de todas as restrições indexadas de (w, k).

Lema 2: Se $\mathcal{C}_{\mathcal{O}}(w, k) = \mathcal{C}_{\mathcal{O}}(u, j)$ então $\mathcal{C}^d_{\mathcal{O}}(w, k) = \mathcal{C}^d_{\mathcal{O}}(u, j)$ e $\mathcal{C}^i_{\mathcal{O}}(w, k) = \mathcal{C}^i_{\mathcal{O}}(u, j)$.

Demonstração: Suponha que existe $(s, 0) \in \mathcal{C}^d_{\mathcal{O}}(w, k)$, tal que $(s, 0) \in \mathcal{C}^i_{\mathcal{O}}(u, j)$. Como $(s, 0) \in \mathcal{C}^d_{\mathcal{O}}(w, k)$, então $ps \in \mathcal{O}^{(k+|w|-|p| \mod T)}$, onde $p \in \mathcal{S}(w) \backslash \{\varepsilon\}$. Assim, $(ps, -|p| \mod T) \in \mathcal{C}^i_{\mathcal{O}}(w, k)$, portanto, temos que $(ps, -|p| \mod T) \in \mathcal{C}^i_{\mathcal{O}}(u, j)$ e por suposição que $(s, 0) \in \mathcal{C}^i_{\mathcal{O}}(u, j)$, por conseqüência $s \in \mathcal{O}^{(|u|+j \mod T)}$ é um fator de $ps \in \mathcal{O}^{(|u|+j-|p| \mod T)}$, mas, como todo fator próprio de $(ps, |u|+j-|p| \mod T)$ pertence a linguagem, isto é uma contradição.

De forma análoga, se supusermos que $(s, 0) \in \mathcal{C}^d_{\mathcal{O}}(u, j)$ e $(s, 0) \in \mathcal{C}^i_{\mathcal{O}}(w, k)$, concluiremos que isto é uma contradição. Portanto, se $\mathcal{C}_{\mathcal{O}}(w, k) = \mathcal{C}_{\mathcal{O}}(u, j)$, então $(s, 0) \in \mathcal{C}^d_{\mathcal{O}}(w, k)$ se, e somente se $(s, 0) \in \mathcal{C}^d_{\mathcal{O}}(u, j)$. ■

Exemplo 3: Considere um PFT dado pelo conjunto $\mathcal{O} = \{(11, 0), (1, 2), (01, 3)\}$ e com período $T = 5$. Então para $(w, k) = (1, 0)$ teremos $\mathcal{C}^d_{\mathcal{O}}(1, 0) = \{(1, 0)\}$ e $\mathcal{C}^i_{\mathcal{O}}(1, 0) = \{(1, 1),\ (01, 2),\ (11, 4)\}$, para $(w, k) = (0, 3)$ teremos $\mathcal{C}^d_{\mathcal{O}}(0, 3) = \{(1, 0)\}$ e $\mathcal{C}^i_{\mathcal{O}}(0, 3) = \{(11, 1), (1, 3),\ (01, 4)\}$. Observamos que $[\mathcal{C}^d_{\mathcal{O}}(1, 0)] = [\mathcal{C}^d_{\mathcal{O}}(0, 3)]$, contudo a seqüência $001011 \in [\mathcal{C}_{\mathcal{O}}(0, 1)]$ pois $11 \prec_4 001011$, no entanto, $001011 \notin [\mathcal{C}_{\mathcal{O}}(0, 3)]$, pois não há fatores do conjunto $< \mathcal{C}^i_{\mathcal{O}}(0, 3) >$ em 001011. Portanto, $[\mathcal{C}_{\mathcal{O}}(1, 0)] \neq [\mathcal{C}_{\mathcal{O}}(0, 3)]$.

Na próxima proposição demonstraremos que $\mathcal{C}_{\mathcal{O}}(w, k)$ é um possível conjunto das restrições para uma palavra $w \in L^{(k)}$.

Proposição 3: Seja $w \in L^{(k)}$, em que L é a linguagem de $X_{\{\mathcal{O}, T\}}$, então $[\mathcal{C}(w, k)] = [\mathcal{C}_{\mathcal{O}}(w, k)]$.

Demonstração: Para todo $s \in [\mathcal{C}_{\mathcal{O}}(w, k)]$ há um fator $u \prec_j s$ tal que $(u, j) \in \mathcal{C}^d_{\mathcal{O}}(w, k) \cup < \mathcal{C}^i_{\mathcal{O}}(w, k) >$. Se $(u, j) \in < \mathcal{C}^i_{\mathcal{O}}(w, k) >$ então $(u, j + k + |w| \mod T) \in \mathcal{O}$ e portanto $ws \notin L^{(k)}$. No entanto, se $(u, j) \in \mathcal{C}^d_{\mathcal{O}}(w, k)$ então existe $p \in \mathcal{S}(w) \backslash \{\varepsilon\}$ tal que $pu \in \mathcal{O}^{(k+|w|-|p| \mod T)}$, como $pu \prec_{|w|-|p|} ws$ então $ws \notin L^{(k)}$. Logo, $[\mathcal{C}_{\mathcal{O}}(w, k)] \subseteq [\mathcal{C}(w, k)]$.

Se considerarmos que $s \in [\mathcal{C}(w,k)]$, decorre da Definição 5 que existe $(u,j) \in \mathcal{C}(w,k)$ tal que $u \prec_j s$. Da Definição 4.a temos que $ws \notin L^{(k)}$, assim existe $v \in \mathcal{O}^{(k+t \mod T)}$ tal que $v \prec_t ws$. No entanto $v \not\prec_t w$ (pois $w \in L^{(k)}$). Caso $t \geq |w|$, então $s \in [< \mathcal{C}^i_{\mathcal{O}}(w,k) >]$ pois $(v, t-|w| \mod T) \in \mathcal{C}^i_{\mathcal{O}}(w,k)$. Se $t < |w|$, então existe $p \in \mathcal{S}(w) \backslash \{\varepsilon\}$ e $q \in \mathcal{P}(s) \backslash \{\varepsilon\}$ tal que $v = pq \in \mathcal{O}^{(k+|w|-|p| \mod T)}$, logo $s \in [\mathcal{C}^d_{\mathcal{O}}(w,k)]$. Concluímos que $[\mathcal{C}(w,k)] \subseteq [\mathcal{C}_{\mathcal{O}}(w,k)]$, e o resultado segue. ■

Como no caso de um SFT há uma forma recursiva para calcularmos os conjuntos $\mathcal{C}^d_{\mathcal{O}}(w,k)$. Para uma palavra não nula $w \in L^{(k)}$, $w = a_0 a_1 \ldots a_{n-1}$, o cálculo é realizado do prefixo de menor comprimento (a_0) para o de maior comprimento $a_0 \ldots a_{n-1}$, empregando a definição $\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(w,k)) = \{s \mid (s,0) \in \mathcal{C}^d_{\mathcal{O}}(w)\}$, temos que:

$$\begin{aligned}
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(a_0,k)) = a_0^{-1}\mathcal{O}^{(k)},\\
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(a_0a_1,k)) = a_1^{-1}\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(a_0,k)) \cup a_1^{-1}\mathcal{O}^{(k+1 \mod T)},\\
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(a_0 \ldots a_{n-1},k)) =\\
&a_{n-1}^{-1}\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(a_0 \ldots a_{n-2},k)) \cup a_{n-1}^{-1}\mathcal{O}^{(k+n-1 \mod T)}.
\end{aligned} \tag{1}$$

A prova desta relação é apresentada no topo da próxima pagina pelo desenvolvimento do conjunto $\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(w,k))$, a partir da descrição do conjunto $\mathcal{C}^d_{\mathcal{O}}(w,k)$ dada na Definição 7.

Exemplo 4: Seja $T = 3$ o período do Shannon cover de um PFT. Dados os conjuntos $\mathcal{O}^{(0)} = \{1111, 1011\}$, $\mathcal{O}^{(1)} = \emptyset$ e $\mathcal{O}^{(2)} = \{111, 1101\}$, segue o cálculo dos conjuntos $\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(w,k))$ para $(111,0)$ e $(110,2)$:

$$\begin{aligned}
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(1,0)) = 1^{-1}\mathcal{O}^{(0)} = \{111, 011\},\\
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(11,0)) = 1^{-1}\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(1,0)) \cup 1^{-1}\mathcal{O}^{(1)} = \{11\},\\
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(111,0)) = 1^{-1}\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(11,0)) \cup 1^{-1}\mathcal{O}^{(2)} = \{1, 11, 101\},\\
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(1,2)) = 1^{-1}\mathcal{O}^{(2)} = \{11, 101\},\\
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(11,2)) = 1^{-1}\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(1,2)) \cup 1^{-1}\mathcal{O}^{(0)} = \{1, 01, 111, 011\},\\
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(110,2)) = 1^{-1}\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(11,2)) \cup 1^{-1}\mathcal{O}^{(1)} = \{1, 11\}.
\end{aligned}$$

O Lema 4 nos permite concluir, para um PFT irredutível de linguagem L, que, para qualquer $w \in L^{(k)}$ e $(v,n) \in \mathcal{C}^i_{\mathcal{O}}(w,k)$ existe uma palavra uv em $[\mathcal{C}_{\mathcal{O}}(w,k)]$ que só possui $v \prec_{|u|} uv$ como fator proibido, onde $|u| \equiv n \mod T$. Portanto, quando consideramos a linguagem indexada $L^{(k)}$, o único fator proibido de (wuv, k) é $(v, |wu| + k \mod T)$, onde $(|wu| + k) - (k + |w|) \equiv n \mod T$. Assim, qualquer elemento em $\mathcal{C}^i_{\mathcal{O}}(w,k)$ é uma restrição não dispensável do conjunto $\mathcal{C}_{\mathcal{O}}(w,k)$, ou seja, retirá-la do conjunto $\mathcal{C}_{\mathcal{O}}(w,k)$ implica que a Proposição 1 não seria verificada.

Lema 4: Seja $X_{\{\mathcal{O},T\}}$ um PFT irredutível. Para qualquer $v = pa \in \mathcal{A}^*$, $a \in \mathcal{A}$, $v \in \mathcal{O}^{(n)}$ se, e somente se,

(i) $\forall s \prec_\ell v$, $s \in L^{(n+\ell \mod T)}$;

(ii) $wuv \notin L^{(k)}$ para todo $wup \in L^{(k)}$ em que $k + |wu| \equiv n \mod T$, qualquer $k \in \{0, \ldots, T-1\}$ e $w \in L^{(k)}$.

Demonstração: Chamaremos de $\mathcal{G}$ o Shannon cover de $X_{\{\mathcal{O},T\}}$ (a irredutibilidade de $X_{\{\mathcal{O},T\}}$ garante sua existência), $T = \mathrm{per}(A_{\mathcal{G}})$ e $D_0, \ldots, D_{T-1}$ as classes periódicas de $\mathcal{G}$. A implicação direta segue da definição dos elementos em $\mathcal{O}$ para afirmação (i). Para afirmação (ii), seja $k \in \{0, \ldots, T-1\}$ e $w \in L^{(k)}$, portanto, existe pelo menos um caminho ξ em $\mathcal{G}$ tal que $\mathcal{L}(\xi) = w$, $i(\xi) \in D_k$ e $t(\xi) \in D_{(k+|w| \mod T)}$. Tomemos um caminho π em $\mathcal{G}$ para o qual $\mathcal{L}(\pi) = p$ e $i(\pi) \in D_n$, como $p \in L^{(n)}$ então este caminho existe. Já que $\mathcal{G}$ é irredutível, existe um caminho ϕ em $\mathcal{G}$ para o qual $i(\phi) = t(\xi)$ e $t(\phi) = i(\pi)$, logo temos que $w\mathcal{L}(\phi)p \in L^{(k)}$ e $w\mathcal{L}(\phi)v \notin L^{(k)}$, uma vez que o vértice inicial do caminho com rótulo v em $w\mathcal{L}(\phi)v$ pertence à classe D_n. O que concluí a prova direta, pois, w é uma palavra qualquer em $L^{(k)}$ e π é qualquer caminho, tal que, $\mathcal{L}(\pi) = p$ e $i(\pi) \in D_n$.

Da afirmação (i), temos que $v_{[0,|v|-2]} \in L^{(n)}$ e $v_{[1,|v|-1]} \in L^{(n+1 \mod T)}$. Da afirmação (ii), temos que $v \notin L^{(n)}$. Portanto, pela definição dos elementos do conjunto $\mathcal{O}$, concluímos que $v \in \mathcal{O}^{(n)}$. ■

Os conjuntos $\mathcal{C}_{\mathcal{O}}(w,k)$ podem ser reduzidos pela eliminação de elementos $(s,k) \in \mathcal{C}_{\mathcal{O}}(w,k)$ que possuem prefixos próprios em $\mathcal{C}_{\mathcal{O}}(w,k)$, o que é justificado observando-se que para todo prefixo (s',k) de (s,k) temos que $[(s,k)] \subset [(s',k)]$, portanto concluímos que $[\mathcal{C}_{\mathcal{O}}(w,k)] = [\mathcal{C}_{\mathcal{O}}(w,k) \backslash \{(s,k)\}]$. Escreveremos $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)$ para indicar que eliminações deste tipo não podem ser realizadas no conjunto $\mathcal{C}_{\mathcal{O}}(w,k)$. Observamos que um elemento $(s,j) \in \mathcal{C}_{\mathcal{O}}(w,k)$ só poderá ter um fator próprio $(s',i) \in \mathcal{C}_{\mathcal{O}}(w,k)$ se $(s',i) \in \mathcal{C}^d_{\mathcal{O}}(w,k)$, ou seja $i = j = 0$, caso contrário $s' \in \mathcal{O}^{(i+k+|w| \mod T)}$ será um fator próprio de $s \in \mathcal{O}^{(j+k+|w| \mod T)}$, o que contradiz a definição dos elementos de $\mathcal{O}$.

Exemplo 5: Os conjuntos $\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(w,k))$ calculados no Exemplo 4 possuem os seguintes conjuntos $\mathcal{R}(\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k))$ correspondentes:

$$\begin{aligned}
&\mathcal{R}(\tilde{\mathcal{C}}^d_{\mathcal{O}}(1,0)) = \{111, 011\},\\
&\mathcal{R}(\tilde{\mathcal{C}}^d_{\mathcal{O}}(11,0)) = \{11\},\\
&\mathcal{R}(\tilde{\mathcal{C}}^d_{\mathcal{O}}(111,0)) = \{1\},\\
&\mathcal{R}(\tilde{\mathcal{C}}^d_{\mathcal{O}}(1,2)) = \{11, 101\},\\
&\mathcal{R}(\tilde{\mathcal{C}}^d_{\mathcal{O}}(11,2)) = \{1, 01, 011\},\\
&\mathcal{R}(\tilde{\mathcal{C}}^d_{\mathcal{O}}(110,2)) = \{1\}.
\end{aligned}$$

Mostraremos que elementos em $L \times \{0, \ldots, T-1\}$ com o mesmo contexto à direita possuem conjuntos $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)$ iguais, dado que o PFT é irredutível.

Teorema 5: Seja $w \in L^{(k)}$ e $w' \in L^{(j)}$. A igualdade $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k) = \tilde{\mathcal{C}}_{\mathcal{O}}(w',j)$ é verificada se, e somente se, $F(w,k) = F(w',j)$.

Demonstração: Se $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k) = \tilde{\mathcal{C}}_{\mathcal{O}}(w',j)$ então $[\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)] = [\tilde{\mathcal{C}}_{\mathcal{O}}(w',j)]$, o que das Proposições 1 e 3 implica que $F(w,k) = F(w',j)$.

Para provarmos a recíproca, inicialmente demonstraremos que se $F(w,k) = F(w',j)$ então $\tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k) = \tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)$ e usaremos isto para provar que $\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k) = \tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$. Seja $(v,n) \in \tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k)$. Supondo que $v = pa$, $a \in \mathcal{A}$, para todo $up \in F(w,k)$, tal que $|u| \equiv n \mod T$, temos que $upa = uv \notin F(w,k)$, logo a igualdade $F(w,k) = F(w',j)$ implica que $uv \notin F(w',j)$. Da definição dos elementos do conjunto $\tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k)$, para todo fator próprio $s \prec_\ell v$ de v existe u', tal que $|u'| \equiv n + \ell \mod T$, satisfazendo $u's \in F(w,k)$ e, portanto, $u's \in F(w',j)$, implicando que $s \in L^{(n+j+|w'|+\ell \mod T)}$. Assim, a partir do Lema 4 temos que $v \in \mathcal{O}^{(n+j+|w'| \mod T)}$,

$$
\begin{aligned}
&\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(a_0\ldots a_{n-1},k))\\
&=\bigcup_{i=1}^{n}(a_{n-i}\ldots a_{n-1})^{-1}\mathcal{O}^{(k+n-i \mod T)}\\
&=\left(\bigcup_{i=2}^{n}(a_{n-i}\ldots a_{n-1})^{-1}\mathcal{O}^{(k+n-i \mod T)}\right)\cup a_{n-1}^{-1}\mathcal{O}^{(k+n-1 \mod T)}\\
&=\left(\bigcup_{i=2}^{n}a_{n-1}^{-1}(a_{n-i}\ldots a_{n-2})^{-1}\mathcal{O}^{(k+n-i \mod T)}\right)\cup a_{n-1}^{-1}\mathcal{O}^{(k+n-1 \mod T)}\\
&=a_{n-1}^{-1}\left(\bigcup_{i=2}^{n}(a_{n-i}\ldots a_{n-2})^{-1}\mathcal{O}^{(k+n-i \mod T)}\right)\cup a_{n-1}^{-1}\mathcal{O}^{(k+n-1 \mod T)}\\
&=a_{n-1}^{-1}\mathcal{R}(\mathcal{C}^d_{\mathcal{O}}(a_0\ldots a_{n-2},k))\cup a_{n-1}^{-1}\mathcal{O}^{(k+n-1 \mod T)}.
\end{aligned}
$$

---

logo $(v,n)\in\tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)$, de onde concluímos que $\tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k)\subseteq\tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)$. Supondo que $(v,n)\in\tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)$, podemos concluir de forma semelhante que $\tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)\subseteq\tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k)$.

Dadas as igualdades $F(w,k)=F(w',j)$ e $\tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k)=\tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)$, demonstraremos que a hipótese $\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k)\neq\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$ gera uma contradição. Assim, seja $\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k)\neq\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$ e s um dos elementos entre os de menor comprimento em $\{u|\ (u,0)\in(\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k)\backslash\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j))\cup(\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)\backslash\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k))\}$. Iremos supor, sem perda de generalidade, que $(s,0)\in\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k)$ e portanto que $s\in[\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)]$. Existe $v=ps$ tal que $v\in\mathcal{O}^{(k+|w|-|p| \mod T)}$ e $p\in\mathcal{S}(w)\backslash\{\varepsilon\}$, portanto, se considerarmos que $s\in[<\tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)>]=[<\tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k)>]$, então existe $s'\prec_{|p+t|}v$ para algum $(s',t)\in\tilde{\mathcal{C}}^i_{\mathcal{O}}(w,k)$, isto implica que $s'\in\mathcal{O}^{(k+|w|+t \mod T)}$ é um fator de $v\in\mathcal{O}^{(k+|w|-|p| \mod T)}$, o que é uma contradição. Logo, podemos afirmar que $s\notin[<\tilde{\mathcal{C}}^i_{\mathcal{O}}(w',j)>]$. Nos limitando aos elementos de $\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$, temos três casos a considerar (i) $s\notin[\{(u,0)|\ (u,0)\in\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$ e $|u|>|s|\}]$, uma vez que $u\not\prec_0 s$ para qualquer u tal que $|u|>|s|$; (ii) $s\notin[\{(u,0)|\ (u,0)\in\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$ e $|u|=|s|\}]$, já que por hipótese $(s,0)\notin\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$; (iii) $s\notin[\{(u,0)|\ (u,0)\in\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$ e $|u|<|s|\}]$, pois da definição da palavra s, temos que $\{(u,0)\in\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k)|\ |u|<|s|\}=\{(u,0)\in\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)|\ |u|<|s|\}$ implicando que não há $(v,0)\in\tilde{\mathcal{C}}^d_{\mathcal{O}}(w',j)$ tal que $v\not\prec_0 s$. Logo, $s\notin[\tilde{\mathcal{C}}_{\mathcal{O}}(w',j)]$ e, portanto, da Proposição 1, concluímos que $F(w,k)\neq F(w',j)$, o que contradiz a hipótese de (w,k) e (w',j) terem o mesmo contexto à direita. ∎

IV. CONSTRUÇÃO DE UMA APRESENTAÇÃO REDUZIDA

Nesta seção proporemos um método para gerar uma apresentação $G=(\mathcal{V},\mathcal{E},\lambda)$ de um PFT irredutível a partir de um conjunto mínimo periódico de palavras proibidas $\mathcal{O}$. Começamos por definir o conjunto $\mathcal{V}$, que tem como elementos as classes de equivalência provenientes da partição de $\mathcal{W}\cup\mathcal{O}$, sendo $\mathcal{W}$ definido a seguir.

Definição 8: Dado o conjunto $\mathcal{O}$ associado a um PFT, definimos o conjunto $\mathcal{W}=\bigcup_{k=0}^{T-1}\mathcal{W}^{(k)}$, onde:

$$\mathcal{W}^{(k)}=\{(u,k)|\ u\in\mathcal{P}(w\mathcal{A}^{-1}),\ \forall\ (w,k)\in\mathcal{O}^{(k)}\}$$

se $\mathcal{O}^{(k)}\neq\emptyset$, ou $\mathcal{W}^{(k)}=\{(\varepsilon,k)\}$ se $\mathcal{O}^{(k)}=\emptyset$.

A partição do conjunto $\mathcal{W}\cup\mathcal{O}$ é determinada pela relação de equivalência: $(w,k)\sim(u,j)$ se, e somente se, $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)=\tilde{\mathcal{C}}_{\mathcal{O}}(u,j)$. Portanto, $(w,k)\sim(u,j)$ se, e somente se, $F(w,k)=F(u,j)$, justificado pelo Teorema 5. Decorre dessa relação que o conjunto $\mathcal{O}$ forma uma classe, já que para todo $(v,k)\in\mathcal{O}$ e $x\in L$ temos que $vx\notin L^{(k)}$.

A partir de um conjunto $\mathcal{V}$, iremos determinar o conjunto de ramos e seus rótulos. Seja $C_i,C_j\in\mathcal{V}$ e $C_i\neq\mathcal{O}$, criaremos um ramo de C_i para C_j com rótulo a, se para algum dos $(w,k)\in C_i$ o mais longo sufixo de (wa,k) em $\mathcal{W}\cup\mathcal{O}$ pertence a C_j. Descrevemos com maior precisão o método de determinação dos ramos na próxima definição.

Definição 9: Seja $C_i\in\mathcal{V}\backslash\{\mathcal{O}\}$ e $(w,k)\in C_i$. A relação $\delta:\mathcal{V}\backslash\{\mathcal{O}\}\times\mathcal{A}\cup\{\varepsilon\}\rightarrow\mathcal{V}$ é definida como

$$\delta(C_i,a)=\{\mathcal{Q}|\ (v,k+r \mod T)\in\mathcal{Q},\ a\in\mathcal{A}\cup\{\varepsilon\} \text{ e } v=wa_{[r,|wa|-1]} \text{ é o mais longo sufixo de } (wa,k) \text{ tal que } (v,k+r \mod T)\in\mathcal{W}\cup\mathcal{O}\}.$$

A partir da Definição 9, observamos que não há ramos partindo da classe $\mathcal{O}$. Tendo definido o conjunto de vértices, os ramos e seus rótulos, seguiremos demonstrando que G é uma apresentação determinística e reduzida de um PFT irredutível especificado por um conjunto mínimo periódico de palavras proibidas $\mathcal{O}$ e período T. Nos próximos dois lemas apresentaremos algumas propriedades dos conjuntos $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)$ que nos permitirão concluir que G é um grafo determinístico.

Lema 6: Para todo $w\in L^{(k)}$ e $u\in L^{(j)}$, se $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)=\tilde{\mathcal{C}}_{\mathcal{O}}(u,j)$ então $\tilde{\mathcal{C}}_{\mathcal{O}}(wa,k)=\tilde{\mathcal{C}}_{\mathcal{O}}(ua,j)$.

Demonstração: Pelo Teorema 5, $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)=\tilde{\mathcal{C}}_{\mathcal{O}}(u,j)$ se, e somente se, $F(w,k)=F(u,j)$. Logo $waz\in L^{(k)}$ se, e somente se, $waz\in L^{(j)}$, portanto $F(wa,k)=F(ua,j)$, ou $\tilde{\mathcal{C}}_{\mathcal{O}}(wa,k)=\tilde{\mathcal{C}}_{\mathcal{O}}(ua,j)$. ∎

Lema 7: Seja $w\in L^{(k)}$. Se (v,ℓ) é o mais longo sufixo de (w,k) em $\mathcal{W}$, então $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k)=\tilde{\mathcal{C}}_{\mathcal{O}}(v,\ell)$.

Demonstração: Supondo que $v=w_{[r,|w|-1]}$, então o comprimento de v é $|v|=|w|-r$. Logo, a partir da equação $\ell\equiv k+r \mod T$, temos que $|v|+\ell\equiv|w|-r+k+r\equiv|w|+k \mod T$, portanto $\mathcal{C}^i_{\mathcal{O}}(w,k)=\mathcal{C}^i_{\mathcal{O}}(v,\ell)$.

Observemos que $\mathcal{C}^d_{\mathcal{O}}(v,\ell)\subseteq\mathcal{C}^d_{\mathcal{O}}(w,k)$, pois (v,ℓ) é uma sufixo de (w,k). Para a demonstração da inclusão reversa, consideremos que $(s,0) \in \tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k)$, logo existe $p = w_{[i,|w|-1]}$ tal que $ps \in \mathcal{O}^{(k+i \mod T)}$, portanto $(p, k+i \mod T)$ é um sufixo de (w,k) em $\mathcal{W}$. Uma vez que (v,ℓ) é o mais longo sufixo de (w,k) em $\mathcal{W}$, então $(p, k+i \mod T)$ também é um sufixo de (v,ℓ), o que implica que $(s,0) \in \mathcal{C}^d_{\mathcal{O}}(v,\ell)$. Se $(s',0)$ é um prefixo de $(s,0)$ contido em $\mathcal{C}^d_{\mathcal{O}}(v,\ell)$, então $(s',0) \in \mathcal{C}^d_{\mathcal{O}}(w,k)$ implicando que $(s,0) \notin \tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k)$, o que é uma contradição. Logo, temos que $\tilde{\mathcal{C}}^d_{\mathcal{O}}(w,k) \subseteq \tilde{\mathcal{C}}^d_{\mathcal{O}}(v,\ell)$. Concluímos que $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k) = \tilde{\mathcal{C}}_{\mathcal{O}}(v,\ell)$. ■

Proposição 8: O grafo G é determinístico.

Demonstração: Para $C_i \neq \mathcal{O}$ e $(w,k),(u,j) \in C_i$, consideremos (w',k') e (u',j') os mais longos sufixos de (wa,k) e (ua,j) em $\mathcal{W} \cup \mathcal{O}$, respectivamente. Do Lema 6 $\tilde{\mathcal{C}}_{\mathcal{O}}(wa,k) = \tilde{\mathcal{C}}_{\mathcal{O}}(ua,j)$, então para $(w',k') \in C_t$ e $(u',j') \in C_\ell$ temos que $C_t = C_\ell$, pois do Lema 7 decorre a igualdade $\tilde{\mathcal{C}}_{\mathcal{O}}(w',k') = \tilde{\mathcal{C}}_{\mathcal{O}}(u',j')$. ■

Como apresentada na Definição 9 a relação δ é uma função, a Proposição 8 nos permite concluir que esta função é bem definida.

Seja $C_i \neq \mathcal{O}$, uma palavra u é dita definida por C_i se, e somente se, existe um caminho partindo de C_i com rótulo u. O que nos leva a uma natural modificação do domínio da função δ para grafos determinísticos, de $\mathcal{V} \times \mathcal{A} \cup \{\varepsilon\}$ para $\mathcal{V} \times \mathcal{A}^*$. Para qualquer $C_i \in \mathcal{V}\backslash\{\mathcal{O}\}$ e $u \in \mathcal{A}^*$, caso o estado $\mathcal{O}$ seja alcançado a partir de C_i por um prefixo próprio de u, então u não é definida por C_i, pois $\mathcal{O}$ não possui ramos partindo deste; caso contrário, $\delta(C_i,u)$ é o estado alcançado a partir de C_i por u.

No próximo teorema empregaremos este conceito para concluir que G é uma apresentação de $X_{\{\mathcal{O},T\}}$. Por G ser determinístico, para qualquer palavra u definida por um vértice C_i há um único caminho π em G tal que $\lambda(\pi) = u$ e $i(\pi) = C_i$, portanto, se $\delta(C_i,u) = \mathcal{O}$ então $u \notin F(C_i)$, pois não há ramos partindo de $\mathcal{O}$ e portanto este não pertence a componente essencial de G.

Lema 9: Seja $(w,k) \in C_i$ e $C_i \neq \mathcal{O}$. Se u é definido por C_i, então o mais longo sufixo de (wu,k) contido em $\mathcal{W} \cup \mathcal{O}$ pertence a $\delta(C_i,u)$.

Demonstração: Realizaremos uma prova por indução no comprimento de u. Inicialmente, se $u = \varepsilon$ então a afirmação é satisfeita. Portanto, iremos supor que o lema é satisfeito para algum $|u| = r > 0$. Seja $x = ua$ uma palavra definida por C_i, $a \in \mathcal{A}$, portanto, existe um ramo partindo do vértice $\delta(C_i,u)$ com rótulo a para o vértice $\delta(\delta(C_i,u),a)$. Da hipótese indutiva o mais longo sufixo de (wu,k) em $\mathcal{W} \cup \mathcal{O}$ pertence a $\delta(C_i,u)$ e $\delta(C_i,u) \subseteq \mathcal{W}$.

Seja $(u',k') \in \delta(C_i,u)$ o mais longo sufixo de (wu,k) em $\mathcal{W}$ e seja $v = u'a_{[t,|u'a|-1]}$, tal que $(v, k'+t \mod T)$, o mais longo sufixo de $(u'a,k')$ em $\mathcal{W} \cup \mathcal{O}$. Consideremos que $v'a = wua_{[t',|ua|-1]}$ seja um sufixo de (wua,k) em $\mathcal{W} \cup \mathcal{O}$. Então $(v', t'+k \mod T)$ é um sufixo de (wu,k) em $\mathcal{W} \cup \mathcal{O}$, portanto $(v', t'+k \mod T)$ é um sufixo de (u',k'), implicando que $(v'a, t'+k \mod T)$ é um sufixo de $(u'a,k')$. Assim, concluímos que $(v, k'+t \mod T)$ é o mais longo sufixo de (wua,k) em $\mathcal{W} \cup \mathcal{O}$. ■

Teorema 10: A componente essencial de G é uma apresentação reduzida do PFT.

Demonstração: Seja x uma palavra não nula e $C_i \in \mathcal{V}\backslash\{\mathcal{O}\}$, tal que $x \in F(C_i)$, $(w,k) \in C_i$ e $\delta(C_i,x) \neq \mathcal{O}$. Considerando que (wx,k) possui fatores em $\mathcal{O}$, seja $v = wx_{[t,|v|+t-1]}$ o fator de (wx,k) em $\mathcal{O}$ que inicia no menor coeficiente t de wx. Então, do Lema 9 temos que $\delta(C_i, wx_{[0,t+|v|-1]}) = \mathcal{O}$, logo $x \notin F(C_i)$, o que é uma contradição. Isso implica que $F(C_i) \subseteq F(w,k)$. Reciprocamente, seja $x \in F(w,k)$, então (wx,k) não possui fatores em $\mathcal{O}$. Se $(w,k) \in C_i$, então, para todo prefixo x' de x temos que $\delta(C_i,x') \neq \mathcal{O}$, logo $x \in F(C_i)$. Isso implica que $F(w,k) \subseteq F(C_i)$. Assim, concluímos que $F(C_i) = F(w,k)$ para qualquer $(w,k) \in C_i$.

Dada uma palavra $w \in L^{(k)}$ e sendo (w',k') seu mais longo sufixo em $\mathcal{W}$ (como $w \in L^{(k)}$, (w,k) não possui fatores em $\mathcal{O}$), a partir do Lema 7 e do Teorema 5, concluímos que $F(w,k) = F(w',k') = F(C_i)$, tal que $(w',k') \in C_i$. Uma vez que $F(\varepsilon,k) = L^{(k)}$ e para qualquer palavra $x \in L$ temos que $x \in L^{(j)}$ para alguma fase $j \in \{0,\ldots,T-1\}$, concluímos que $\bigcup_{C_i \in \mathcal{V}\backslash\{\mathcal{O}\}} F(C_i) = L$. Portanto, o subgrafo de G com conjunto de vértices $\mathcal{V}\backslash\{\mathcal{O}\}$ é uma apresentação do PFT, logo, a componente essencial de G também é uma apresentação do PFT. Para demonstração que G é uma apresentação reduzida, sejam $C_i, C_\ell \in \mathcal{V}\backslash\{\mathcal{O}\}$ tal que $F(C_i) = F(C_\ell)$, se $(w,k) \in C_i$ e $(u,j) \in C_\ell$ então, do Teorema 5, temos que $\tilde{\mathcal{C}}_{\mathcal{O}}(w,k) = \tilde{\mathcal{C}}_{\mathcal{O}}(u,j)$, logo $C_i = C_\ell$, o que implica que a componente essencial é reduzida. ■

REFERÊNCIAS

[1] D. P. B. Chaves, "Representação de sistemas dinâmicos simbólicos de memória finita usando grafos," Master's thesis, UFPE, September 2006.

[2] A. Wijngaarden and K. S. Immink, "Maximum run-length limited codes with error control properties," *IEEE J. Select. Areas Commun.*, vol. 19, pp. 602–611, April 2001.

[3] M.-P. Béal, M. Crochemore, and G. Fici, "Presentations of constrained systems with unconstrained positions," *IEEE Trans. Inform. Theory*, vol. 51, pp. 1891–1900, May 2005.

[4] B. H. Marcus, R. M. Roth, and P. H. Siegel, "Constrained systems and coding for recording channels," in *Handbook of Coding Theory* (V. S. Pless and W. Huffman, eds.), vol. 2, pp. 1635–1764, Eds. Amsterdam:Elsevier, 1999.

[5] J. C. de Souza, B. H. Marcus, R. New, and B. A. Wilson, "Constrained systems with unconstrained positions," *IEEE Trans. Inform. Theory*, vol. 48, pp. 866–879, April 2002.

[6] D. Lind and B. H. Marcus, *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, 1995.

[7] M.-P. Béal and D. Perrin, "Symbolic dynamics and finite automata," in *Handbook of formal languages, vol. 2: linear modeling: background and application*, pp. 463–505, Springer-Verlag New York, 1997.

[8] M. V. Lawson, *Finite Automata*. Chapman & Hall/CRC, 2004.

[9] S. Eilenberg, *Automata, Languages, and Machines*, vol. A. Academic Press, 1974.

[10] B. Moision and P. H. Siegel, "Periodic-finite-type shift spaces," in *Proc. IEEE Int. Symp. Inform. Theory*, (Washington, DC), p. 65, June 2001.