Decomposição em matrizes posto-1 com aplicações em algoritmos rápidos

G. Jerônimo da Silva Jr. e R. M. Campello de Souza

***Resumo*— Este trabalho apresenta o problema de decompor um conjunto de matrizes com elementos racionais como uma combinação linear do menor número possível de matrizes de posto um (posto-1) e como a solução desse problema é aplicada em transformadas rápidas. Um método para decompor uma matriz de posto r como a soma de uma matriz posto-1 mais uma matriz posto $r-1$ é introduzido. Um algoritmo que busca a melhor solução para o problema proposto é apresentado.**

***Palavras-Chave*— Decomposição de matrizes, posto-1, complexidade multiplicativa, algoritmos rápidos.**

***Abstract*— Let A denote a finite set of matrices with rational entries. This paper proposes the problem of expressing the elements of A as a linear combination of the least possible number of rank one matrices and shows how its solution can be applied in the construction of fast algorithms for discrete transforms. A method for expressing a matrix of rank r as the sum of a rank one matrix and a rank $(r-1)$ matrix is introduced. An algorithm that searches for the best solution for the proposed problem is presented.**

***Keywords*— Matrices decomposition, rank one, multiplicative complexity, fast algorithms.**

I. INTRODUÇÃO

A computação de uma transformada discreta linear (TDL) envolve a combinação linear de um número finito de variáveis de entrada. Representando as variáveis de entrada pelo vetor $\vec{x} \in \mathbb{R}^N$, as variáveis de saída pelo vetor transformado $\vec{y} \in \mathbb{R}^M$ e a matriz TDL por $\Psi = [\psi_{ij}]_{M\times N}$, $\psi_{ij} \in \mathbb{R}$, qualquer TDL pode ser representada como

$$\vec{y} \triangleq \Psi\vec{x}, \tag{1}$$

em que a m-ésima componente do vetor $\vec{y}$ é computada por

$$y_m = \sum_{n=1}^{N} x_n \psi_{mn}, \tag{2}$$

que totaliza MN multiplicações e $M(N-1)$ adições, computando diretamente por (2).

Filtros digitais, a transformada wavelet discreta [1], a transformada discreta de Hartley (DHT) [2] e a transformada discreta de Fourier (DFT) são exemplos de TDLs, as quais podem ser implementadas em um dispositivo eletrônico conhecido como processador digital de sinais (DSP) com diversas aplicações na engenharia [3]-[5].

Algoritmos rápidos para computar uma TDL são procedimentos que realizam a computação indicada em (1) com um número reduzido de multiplicações e adições, em comparação ao método direto de (2). Alguns algoritmos rápidos podem ser expressos na forma CBA, isto é, a matriz TDL é fatorada em $\Psi = CBA$, em que as matrizes A e C são matrizes racionais e a matriz B é diagonal; esse é o caso da transformada rápida de Fourier (FFT), para pequenos comprimentos, de Winograd [6].

O conceito de bases numéricas é útil para obtenção de algoritmos na forma CBA [7]. Sendo a matriz TDL formada pela base numérica $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_L\}$, isso significa que qualquer coeficiente da matriz TDL pode ser expresso por

$$\psi_{ij} = \sum_{l=1}^{L} a_{ij}^{(l)} \lambda_l, \tag{3}$$

em que $a_{mn}^{(l)} \in \mathbb{Q}$. Assim, a matriz TDL é dada por

$$\Psi = \sum_{l=1}^{L} \lambda_l A_l, \tag{4}$$

em que $A_l = [a_{ij}^{(l)}]_{M\times N}$ são matrizes com números racionais. Em [8], foi demonstrado que existe um algoritmo na forma CBA que implementa a transformada $\vec{y} = \Psi\vec{x}$ com K multiplicações se, e somente se, existe uma decomposição para o conjunto das matrizes A_l como combinação linear de K matrizes de posto um (posto-1), por meio do *Teorema da Complexidade Multiplicativa*. Considerando essa decomposição em matrizes posto-1 (DP1), então

$$A_l = \sum_{k=1}^{K} g_{lk} U_k, \tag{5}$$

em que U_k são matrizes posto-1 racionais e $G = [g_{ij}]_{(L\times K)}$ é a matriz de decomposição. Nesse caso, a matriz TDL é dada por

$$\Psi = \sum_{k=1}^{K} \beta_k U_k, \tag{6}$$

em que o vetor formado pelas constantes β_k, denotado por $\vec{\beta}$, se relaciona com o vetor formado pela base numérica λ_l, denotado por $\vec{\lambda}$, por

$$\vec{\beta} = G^T\vec{\lambda}. \tag{7}$$

Em [8], os autores usaram métodos heurísticos para resolver a DP1 e encontrar a FFT com o menor número de multiplicações possível na forma CBA, de acordo com a mínima complexidade multiplicativa calculada por Heideman [9]. Entretanto, quando a soma dos postos das matrizes iniciais

G. Jerônimo da Silva Jr. e R. M. Campello de Souza, Grupo de Processamento de Sinais, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, Brasil, E-mails: gilson.silvajr@ufpe.br, ricardo@ufpe.br.

é um valor relativamente alto (a partir de 20), o método heurístico torna-se inviável.

Nesse artigo, é proposto um algoritmo sistemático de busca para encontrar a melhor DP1 para um conjunto de matrizes racionais. A próxima seção apresenta resultados básicos sobre matrizes posto-1. A Seção III apresenta novos resultados sobre a DP1 e um algoritmo para encontrá-la é descrito na Proposição 2. A Seção IV apresenta um breve estudo sobre a complexidade da busca do algoritmo rápido em comparação com o método descrito em [8] e mostra uma aplicação. As conclusões do trabalho são apresentadas na Seção V.

II. PRELIMINARES

Teorema 1: Uma matriz U é posto-1 se, e somente se, pode ser fatorada como um produto de uma matriz coluna, denotada por $\vec{u}$, por uma matriz linha, denotada por $\vec{v}^T$, isto é, $U = \vec{u}\vec{v}^T$. Essa fatoração não é única.

Demonstração: Seja a primeira linha não nula da matriz U $(m \times n)$ igual $\vec{v}^T$. Como U é posto-1, todas as m linhas de U são proporcionais a $\vec{v}^T$. Seja a i-ésima linha de U igual a $\mu_i \vec{v}^T$, em que μ_i é um escalar, então

$$U = \begin{bmatrix} \mu_1 \vec{v}^T \\ \mu_2 \vec{v}^T \\ \vdots \\ \mu_m \vec{v}^T \end{bmatrix} = \begin{bmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_m \end{bmatrix} \vec{v}^T.$$

Definindo a matriz coluna

$$\vec{u} = \begin{bmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_m \end{bmatrix},$$

tem-se que $U = \vec{u}\vec{v}^T$. Por outro lado, se $U = \vec{u}\vec{v}^T$ então todas as colunas são proporcionais a $\vec{u}$ e todas as linhas são proporcionais a $\vec{v}^T$ o que significa que a matriz U é posto-1. Essa fatoração não é única, pois, para qualquer escalar não nulo $\alpha \neq 1$, $U = (\alpha\vec{u})(\alpha^{-1}\vec{v}^T)$ representa outra fatoração. ■

Exemplo 1: A matriz posto-1

$$U = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ -2 \\ -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \\ 2 \\ 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 \end{bmatrix}.$$

Esse resultado é importante, pois, a implementação da TDL $\vec{y} = \beta U \vec{x}$, em que β é um escalar e U é uma matriz posto-1 racional, é realizada por meio de $\vec{y} = \vec{u}[\beta(\vec{v}^T\vec{x})]$, com uma única multiplicação não trivial, considerando as multiplicações por constantes racionais como triviais [3], [9].

III. DP1 PARA UM CONJUNTO DE MATRIZES

Para um conjunto de L matrizes $(m \times n)$, A_l, $l = 1, 2, \ldots, L$, denotado por $\{A_l\}_{l=1}^L$, em que posto$(A_l) = r_l$, o problema da DP1 é obter o menor conjunto de matrizes posto-1 que geram as matrizes $\{A_l\}_{l=1}^L$. Na pior das hipóteses, é possível resolver o problema da DP1 individualmente para cada matriz A_l, o que significa que existe um conjunto de $d = \sum_{l=1}^L r_l$ matrizes posto-1 que geram o conjunto de matrizes A_l. Entretanto, dependendo das matrizes A_l, é possível gerar o conjunto de matrizes com um número menor que d de matrizes posto-1. Isso motiva a definição a seguir.

Definição 1: O grau de um conjunto de matrizes $\{A_l\}_{l=1}^L$, posto$(A_l) = r_l$, é dado por $d = \sum_{l=1}^L r_l$.
Assim, o que se deseja é encontrar o conjunto de menor grau, K, de matrizes posto-1, $\{U_k\}_{k=1}^K$, que geram as matrizes $\{A_l\}_{l=1}^L$ através de uma combinação linear, isto é

$$A_l = \sum_{k=1}^K g_{lk} U_k,$$

em que g_{lk} são escalares. Definindo a matriz DP1 por $G = [g_{ij}]$ $(L \times K)$, deseja-se, a partir de $\{A_l\}_{l=1}^L$, obter as K matrizes posto-1 $\{U_k\}_{k=1}^K$ e a matriz G com o menor valor de K.

A solução do problema parte de um conjunto inicial de matrizes $\{A_l\}_{l=1}^L$, de grau d, e procura obter um novo conjunto de matrizes com menor grau que gera o conjunto inicial. A definição a seguir é útil quando existe uma ou mais matrizes posto-1 no conjunto $\{A_l\}_{l=1}^L$.

Definição 2: Uma matriz posto-1 U reduz uma matriz A de posto r se A pode ser expressa como

$$A = \alpha U + B, \tag{8}$$

em que $\alpha \neq 0$ é um escalar, chamado de *coeficiente de redução*, e B é uma matriz, chamada de *matriz reduzida*, que satisfaz posto$(B) = r - 1$. Se tal expressão não existe, então U não reduz A.

Um problema que decorre dessa definição é como descobrir se uma dada matriz posto-1 U reduz uma matriz A dada. Um teorema, apresentado sem demonstração, referenciando os trabalhos de Householder e Wedderburn [10], resolve essa questão. O teorema é apresentado a seguir com sua demonstração.

Teorema 2: Seja $U = \vec{u}\vec{v}^T$ uma matriz posto-1 $(m \times n)$ e seja A uma matriz $(m \times n)$ de posto r e α um escalar não nulo. A matriz $B = A - \alpha U$ tem posto $r - 1$ se, e somente se, existem matrizes colunas $\vec{x}$ e $\vec{y}$ tais que $\vec{u} = A\vec{x}$, $\vec{v}^T = \vec{y}^T A$ e $\alpha^{-1} = \vec{y}^T A \vec{x}$.

Demonstração: Supondo inicialmente que $B = A - \alpha U$ tem posto $r - 1$, então a matriz coluna $\vec{u}$ deve ter a forma $\vec{u} = A\vec{x}$, para algum $\vec{x}$, caso contrário, isso significa que as colunas não nulas de U não podem ser geradas pelo espaço das colunas de A e, portanto, é linearmente independente das colunas de A, o que significa que a dimensão do espaço gerado pelas colunas de $B = A - \alpha U$ é $r + 1$, o que é absurdo pois B tem posto $r - 1$. Assim $\vec{u} = A\vec{x}$. Aplicando o mesmo argumento para a matriz linha $\vec{v}^T$ e as linhas de U, chega-se a conclusão que $\vec{v}^T = \vec{y}^T A$. Assim

$$B = A - \alpha A\vec{x}\vec{y}^T A. \tag{9}$$

Tomando $\vec{z}$ como um vetor do núcleo das colunas de B que não pertence ao núcleo das colunas de A (esse vetor existe desde que posto de B é menor do que posto de A) e aplicando à direita de B, tem-se

$$B\vec{z} = A\vec{z} - \alpha A\vec{x}(\vec{y}^T A\vec{z}) = \vec{0},$$

o que implica que

$$A(\vec{z} - (\vec{y}^T A\vec{z})\alpha\vec{x}) = \vec{0},$$

e então

$$\vec{x} = ((\vec{y}^T A\vec{z})\alpha)^{-1}\vec{z},$$

o que significa que $\vec{x}$ pertence ao núcleo de B. Aplicando $\vec{x}$ à direita em (9), tem-se

$$B\vec{x} = \vec{0} = A\vec{x} - \alpha A\vec{x}\vec{y}^T A\vec{x}$$

e

$$\alpha A\vec{x}\vec{y}^T A\vec{x} = A\vec{x},$$

aplicando $\vec{y}^T$ à esquerda, tem-se

$$\alpha(\vec{y}^T A\vec{x})(\vec{y}^T A\vec{x}) = \vec{y}^T A\vec{x}$$

e

$$\alpha = (\vec{y}^T A\vec{x})^{-1}. \tag{10}$$

Supondo agora que $\vec{u} = A\vec{x}$, $\vec{v}^T = \vec{y}^T A$ e (10) são relações válidas por hipótese, então (9) também é válida. Considere o vetor $\vec{z}$ que pertence ao núcleo das colunas de A, então $A\vec{z} = \vec{0}$, e por (9), $B\vec{z} = \vec{0}$. Portanto, $\vec{z}$ também pertence ao núcleo de B e $\dim N(B) \geq \dim N(A)$. Seja $\vec{\omega}$ um vetor que pertence ao núcleo das colunas de B, por (9), tem-se

$$B\vec{\omega} = \vec{0} = A\vec{\omega} - \alpha A\vec{x}\vec{y}^T A\vec{\omega},$$

$$A(\vec{\omega} - \alpha(\vec{y}^T A\vec{\omega})\vec{x}) = \vec{0},$$

pois o termo $(\vec{y}^T A\vec{\omega}) = k_\omega$ é um escalar, o que significa que $\vec{\omega} - \alpha k_\omega \vec{x}$ pertence ao núcleo de A. Mas $\vec{u} = A\vec{x} \neq \vec{0}$, o que significa que $\vec{x}$ não pertence ao núcleo das colunas de A. Assim, todo $\vec{z}$ pode ser escrito como $\vec{z} = \vec{\omega} - \alpha k_\omega \vec{x}$ e, portanto, $\vec{\omega} = \vec{z} + \alpha k_\omega \vec{x}$, o que significa que $\dim N(B) = \dim N(A) + 1$ e, pelo teorema do núcleo e da imagem [11], $\text{posto}(A) = \text{posto}(B) + 1$. ■

Aplicando o Teorema 2 na Definição 2, chega-se ao resultado apresentado a seguir.

Corolário 1: Uma matriz posto-1 $U = \vec{u}\vec{v}^T$ reduz a matriz A de posto r se, e somente se, existem $\vec{u} = A\vec{x}$, $\vec{v}^T = \vec{y}^T A$ e $\alpha = (\vec{y}^T A\vec{x})^{-1}$ não nulos.

Teorema 3: O coeficiente de redução α e a matriz reduzida B, obtidos através da redução da matriz A pela matriz posto-1 $U = \vec{u}\vec{v}^T$, são únicos.

Demonstração: Pelo Corolário 1, $\alpha^{-1} = (\vec{y}^T A\vec{x})$, em que $\vec{x}$ e $\vec{y}$ são vetores solução dos sistemas de equações $A\vec{x} = \vec{u}$ e $A^T\vec{y} = \vec{v}$, respectivamente. Sendo $\vec{x}_0$ e $\vec{y}_0$ vetores solução dos respectivos sistemas, a solução geral é dada por $\vec{x} = \vec{x}_0 + N_A\vec{r}$ e $\vec{y} = \vec{y}_0 + \bar{N}_A\vec{s}$, respectivamente, em que N_A é o núcleo de A, $\bar{N}_A$ é o núcleo de A^T e $\vec{r}$ e $\vec{s}$ são vetores arbitrários. Então, os valores possíveis para α^{-1} são da forma

$$\begin{aligned}\alpha^{-1} &= (\vec{y}_0 + \bar{N}_A\vec{s})^T A(\vec{x}_0 + N_A\vec{r}) \\ &= (\vec{y}_0^T + \vec{s}^T\bar{N}_A^T)A\vec{x}_0 \\ &= \vec{y}_0^T A\vec{x}_0,\end{aligned}$$

que não depende de $\vec{r}$ nem $\vec{s}$. Assim, para qualquer $\vec{x}$ e $\vec{y}$ escolhidos, o valor de α é único. Como a matriz reduzida $B = A - \alpha U$, então ela é única. ■

Teorema 4: Se a matriz posto-1 U reduz a matriz A de posto r, por meio de (8) com $\text{posto}(B) = \text{posto}(A) - 1$, então U não reduz a *matriz reduzida* B.

Demonstração: Se U reduz B, então existe $\alpha_1 \neq 0$ e B_1 tais que $B = \alpha_1 U + B_1$ com $\text{posto}(B_1) = \text{posto}(B) - 1$. Substituindo em (8), tem-se

$$A = (\alpha + \alpha_1)U + B_1,$$

o que significa que $\text{posto}(A) \leq \text{posto}(B_1) + 1 = \text{posto}(B)$ e, portanto, contradiz $\text{posto}(A) = \text{posto}(B) + 1$. Logo, U não reduz B. ■

Definição 3: Seja $\mathbf{A} = \{A_l\}_{l=1}^L$ um conjunto de matrizes não nulas e seja U uma matriz posto-1. O conjunto $\mathbf{A}$ é dito ser *redutível* por U com *redutibilidade* R se U reduz R matrizes de $\mathbf{A}$. Se U não reduz nenhuma matriz de $\mathbf{A}$, então o conjunto $\mathbf{A}$ é dito ser *irredutível* por U.

Sem perda de generalidade, o conjunto de matrizes $\{A_l\}_{l=1}^L$ pode ser organizado pelo posto das matrizes, de forma que $r_l \leq r_{l+1}$. Nesse caso, se a matriz A_1 é posto-1 e o conjunto $\{A_l\}_{l=2}^L$ é redutível por A_1, então, pode-se obter um novo conjunto irredutível a A_1 que gera o conjunto $\{A_l\}_{l=2}^L$, conforme a proposição a seguir.

Proposição 1: Seja um conjunto de matrizes $\{A_l\}_{l=2}^L$, de grau d, redutível pela matriz posto-1 A_1 com redutibilidade R, em que as R matrizes redutíveis são dadas por

$$A_l = \alpha_l A_1 + B_l,$$

para $l = 2, 3, \ldots, R+1$, com $\text{posto}(B_l) = \text{posto}(A_l) - 1$ e as matrizes $\{A_l\}_{l=R+2}^L$ são irredutíveis a A_1. Então, $\{A_l\}_{l=1}^L$ pode ser escrito como combinação[1] de $\{A_1 \cup \mathbf{B}\}$ por

$$\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_{R+1} \\ A_{R+2} \\ \vdots \\ A_L \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots 0 \\ \alpha_2 & 1 & \cdots & 0 & 0 & \cdots 0 \\ \vdots & & & & & \\ \alpha_{R+1} & 0 & \cdots & 1 & 0 & \cdots 0 \\ 0 & 0 & \cdots & 0 & 1 & \cdots 0 \\ \vdots & & & & & \\ 0 & 0 & \cdots & 0 & 0 & \cdots 1 \end{bmatrix}}_{T} \begin{bmatrix} A_1 \\ B_2 \\ \vdots \\ B_{R+1} \\ A_{R+2} \\ \vdots \\ A_L \end{bmatrix},$$

em que o conjunto de matrizes $\mathbf{B} = \{\{B_l\}_{l=2}^{R+1} \cup \{A_l\}_{l=R+2}^L\}$ é irredutível por A_1 e possui grau $d - R$. A matriz T ($L \times L$) é chamada de *matriz transformação*.

[1] Ambos os conjuntos estão representados como vetores de matrizes.

Generalizando a proposição, se A_1 reduz A_l por $A_l = \alpha_l A_1 + B_l$, com posto(B_l) = posto$(A_l) - 1$, a matriz transformação é dada por $T = [t_{ij}]_{(L\times L)}$, em que

$$t_{ij} = \begin{cases} 1, & \text{se } i = j, \\ \alpha_i, & \text{se } j = 1, i > 1 \text{ e } A_1 \text{ reduz } A_i, \\ 0, & \text{outros casos.} \end{cases} \tag{11}$$

O novo conjunto de matrizes $\{C_l\}_{l=1}^{L}$ irredutível por A_1 é dado por

$$C_l = \begin{cases} A_1, & \text{se } l = 1, \\ B_l, & \text{se } l > 1 \text{ e } A_1 \text{ reduz } A_l, \\ A_l, & \text{outros casos.} \end{cases} \tag{12}$$

Entretanto, algumas das matrizes $C_l = B_l$ podem ser nulas. Se a matriz B_n é nula, pode-se remover C_l do conjunto de matrizes e remover a n-ésima coluna de T. Removendo todas as z matrizes nulas do conjunto $\{C_l\}_{l=1}^{L}$ e as respectivas colunas em T, tem-se o novo conjunto reduzido $\{D_l\}_{l=1}^{L-z}$ e a matriz transformação reduzida T_D $(L \times (L - z))$.

Quando a matriz A_1 possui posto $r > 1$, ela pode ser expressa como a soma de uma matriz posto-1 com uma matriz de posto $r - 1$. Esse passo é chamado de *fragmentação* da matriz A_1. Nesse caso, se $A_1 = \alpha U + B_1$, com posto$(B_1) = r - 1$, o conjunto de matrizes $\mathbf{A}$ é escrito como

$$\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_L \end{bmatrix} = \underbrace{\begin{bmatrix} \alpha & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}}_{F} \begin{bmatrix} U \\ B_1 \\ A_2 \\ \vdots \\ A_L \end{bmatrix},$$

em que o conjunto de matrizes $\mathbf{B} = \{\{U, B_1\} \cup \{A_l\}_{l=2}^{L}\}$ possui grau d e gera o conjunto $\mathbf{A}$. A matriz F $(L \times (L + 1))$ é chamada de *matriz fragmentação* de A_1 em relação ao conjunto $\mathbf{A}$ e é dada por

$$F = \begin{bmatrix} \alpha & \\ 0 & I_L \\ \vdots & \\ 0 & \end{bmatrix}. \tag{13}$$

Considerando a notação de vetores matriciais, se $\mathbf{A} = F\mathbf{B}$, por meio de uma fragmentação de A_1, e $\mathbf{B} = T_D\mathbf{D}$, por meio de uma redução por U, então $\mathbf{A} = (FT_D)\mathbf{D}$. Nesse caso, o conjunto $\mathbf{A}$, de grau d é escrito como combinação do conjunto $\mathbf{D}$, com grau $d - R_1$, em que R_1 é a redutibilidade de A_1 em relação ao conjunto $\{\mathbf{A} - \{A_1\}\}$. Esse processo pode ser repetido de forma recursiva a $\mathbf{D}$ até que o conjunto de matrizes resultante tenha apenas matrizes posto-1. Isso motiva o algoritmo DP1 para um conjunto de matrizes apresentado a seguir.

Proposição 2 (DP1 para um conjunto de matrizes): Para um conjunto de matrizes $\mathbf{A} = \{A_l\}_{l=1}^{L}$, a DP1 é obtida por meio de:

- Inicializar a matriz DP1 $G = I_L$ e o conjunto de matrizes $\mathbf{U} = \{A_l\}_{l=1}^{L}$, de tamanho inicial $S = L$, e $t = 1$.
- Enquanto $t < S$ ou posto$(U_S) > 1$, fazer: permutar a matriz de menor posto de $\{U_l\}_{l=t}^{S}$ com U_t e, sendo P a matriz permutação, atualizar $G \leftarrow GP$.
  - Se U_t é posto-1, reduzir o conjunto $\{U_l\}_{l=t+1}^{S}$ por U_t, obtendo a matriz transformação reduzida T_D $((S - t + 1) \times (S - z - t + 1))$ e o novo conjunto reduzido $\{D_l\}_{l=t+1}^{S-z}$ irredutível a U_t (utilizando (11), (12) e removendo as z matrizes nulas e respectivas colunas de T). Atualizar as matrizes $U_l \leftarrow D_l$, para $l = t + 1, t + 2, \ldots, S - z$, a matriz DP1
  $$G \leftarrow G \begin{bmatrix} I_{t-1} & O \\ O & T_D \end{bmatrix},$$
  em que O representa uma matriz nula, e os parâmetros $S \leftarrow S - z$ e $t \leftarrow t + 1$.
  - Se U_t não é posto-1, então toma-se a matriz posto-1 U que reduz U_t com máxima redutibilidade em relação ao conjunto $\{U_l\}_{l=t+1}^{S}$, com matriz de fragmentação F dada por (13) e atualizam-se as matrizes $U_{l+1} \leftarrow U_l$, para $l = S, S - 1, \ldots, t$, a matriz $U_t \leftarrow U$, a matriz DP1
  $$G \leftarrow G \begin{bmatrix} I_{t-1} & O \\ O & F \end{bmatrix},$$
  e o parâmetro $S \leftarrow S + 1$.

Com isso, $\mathbf{A} = G\mathbf{U}$, em que G é a matriz DP1 e $\mathbf{U}$ é um conjunto de matrizes posto-1.

O algoritmo proposto converge, pois o valor máximo para S é o grau de $\mathbf{A}$. Em algumas situações, a maior redutibilidade pode aparecer em mais de uma matriz posto-1. Nesse caso, pode-se avaliar os conjuntos resultantes e escolher aquele que contém a matriz posto-1 com máxima redutibilidade. Entretanto, tais verificações aumentam a complexidade computacional da DP1.

IV. Complexidade da DP1 e resultados

A parte mais complexa computacionalmente na Proposição 2 é a procura da matriz posto-1 com máxima redutibilidade (MMR). Mesmo assumindo que todas as matrizes são de números racionais, existem infinitas matrizes que podem reduzir U_t, pelo Corolário 1.

A busca pela MMR consiste em procurar diferentes vetores $\vec{x}$ e $\vec{y}^T$ não nulos, com coeficientes 1, -1 e 0, tais que $\vec{u} = U_t\vec{x}$, $\vec{v}^T = \vec{y}^T U_t$, $\vec{y}^T U_t \vec{x} \neq 0$ e $U = \vec{u}\vec{v}^T$ com máxima redutibilidade ao conjunto $\{U_l\}_{l=t+1}^{S}$.

A quantidade de vetores possíveis para $\vec{u}$ é igual à quantidade de vetores possíveis para $\vec{v}$. Se a matriz U_t possui posto r_t, considerando a combinação de uma base com coeficientes 1, -1 e 0, existem $3^{r_t} - 1$ vetores não nulos possíveis para cada, totalizando $(3^{r_t} - 1)^2$ matrizes diferentes que podem reduzir U_t.

Deve-se testar se cada matriz U reduz a matriz U_l, $l \geq t$. Pelo Corolário 1, haverá solução se existirem $\vec{x}$ e $\vec{y}$ não nulos tais que

$$U_t\vec{x} = \vec{u}, \tag{14}$$

$$U_t^T\vec{y} = \vec{v} \tag{15}$$

e $\vec{y}^T U_l \vec{x} \neq 0$. As equações (14) e (15) são sistemas de equações lineares. Esse teste deve ser feito para $S - t$ matrizes.

A quantidade de testes necessários, μ, é dada por

$$\mu = (S_1 - 1)(3^{r_1} - 1)^2 + \ldots + (S_N - 1)(3^{r_N} - 1)^2,$$

em N valores de t. Como $t \le d$, então $S_l \le d$ e $r_l \le \min(m,n) = \rho$ (considerando que as matrizes são $m \times n$). Então

$$\mu \le (d-1)d(3^\rho - 1)^2,$$

e a complexidade da DP1 para um conjunto de matrizes de grau d é dada por $O(d^2 3^{2\rho})$.

Exemplo 2: Considere implementar uma multiplicação pelo número complexo $c = a + jb$, com a, b e a/b números não racionais. Sendo a entrada $x_r + jx_i$, a saída é calculada por

$$\begin{bmatrix} y_r \\ y_i \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} x_r \\ x_i \end{bmatrix},$$

inicialmente com 4 multiplicações e duas adições. A matriz TDL pode ser escrita como

$$\Psi = a\underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{A_1} + b\underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{A_2}.$$

Aplicando a Proposição 2, inicialmente $U_1 = A_1$, $U_2 = A_2$, $G = I_2$, $t = 1$ e $S = 2$. Como U_1 possui o menor posto igual a 2, a primeira etapa é procurar a MMR. Após alguns testes, uma possível MMR com redutibilidade 2 (máxima possível) é

$$U = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix},$$

Como $\alpha = 1$ e

$$B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix},$$

então

$$G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$U_3 \leftarrow U_2$, $U_2 \leftarrow B$, $U_1 \leftarrow U$ e $S = 3$. O próximo passo é reduzir $\{U_2, U_3\}$ por U_1, que resulta na transformação

$$\begin{bmatrix} U_1 \\ U_2 \\ U_3 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}}_{T} \begin{bmatrix} U_1 \\ U_2 \\ B_3 \end{bmatrix},$$

com

$$B_3 = \begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix}.$$

Em seguida, $U_3 \leftarrow B_3$, $t = t + 1 = 2$ e $G \leftarrow GT$, resultando em

$$G = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

Os passos seguintes não alteram G nem $\mathbf{U}$. Com isso, a matriz Ψ é escrita por (6) com (7), nesse caso

$$\begin{bmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}}_{T} \begin{bmatrix} a \\ b \end{bmatrix},$$

são pré calculados e a matriz Ψ pode ser colocada na forma CBA, pelo Teorema 1 em [8],

$$\Psi = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

A computação de $\vec{y} = CBA\vec{x}$ é feita com 4 adições e 3 multiplicações. Variando a MMR inicial, é possível encontrar outras construções mais eficientes, em termo de número de adições, como em [3, p. 3], mas todas com 3 multiplicações.

A técnica apresentada na Proposição 2 foi utilizada para encontrar um algoritmo para computar a parte real da DFT de 11 pontos utilizando o mesmo computador e mesma ferramenta computacional (Scilab) que o método em [8]. A Proposição 2 encontrou um algoritmo na forma CBA com 10 multiplicações em cerca de 3 segundos, enquanto que a técnica apresentada em [8] gastou cerca de 2 horas para encontrar um algoritmo com 12 multiplicações.

V. Conclusões

Neste trabalho, o problema da decomposição de um conjunto finito de matrizes por meio de matrizes de posto-1 foi introduzido. Uma técnica sistemática de solução para esse problema considerando um conjunto de matrizes racionais, consistindo de um procedimento iterativo em que os postos das matrizes dadas são sistematicamente reduzidos, foi proposta. Definições e teoremas utilizados para o desenvolvimento da técnica foram introduzidos. O procedimento apresentou um melhor desempenho, na busca por algoritmos rápidos para computação da DFT, do que o apresentado em [8].

Referências

[1] G. Strang and T. Nguyen, *Wavelets and Filter Banks*. Wellesley - Cambridge Press, 1997.

[2] R. N. Bracewell, "Discrete Hartley transform," *J. Opt. Soc. Am.*, vol. 73, no. 12, pp. 1832–1835, Dec 1983.

[3] R. E. Blahut, *Fast Algorithms for Signal Processing*, 2nd ed. New York: Cambridge University Press, 2010.

[4] A. V. Oppenheim, R. W. Schafer, and J. R. Buck, *Discrete-Time Signal Processing*, 3rd ed. New Jersey: Prentice Hall, 2010.

[5] U. Meyer-Baese, *Digital Signal Processing with Field Programmable Gate Arrays*, 4th ed., ser. Signals and Communication Technology. Springer, 2014.

[6] S. Winograd, "On computing the discrete Fourier transform," *Mathematics of Computation*, vol. 32, pp. 175–199, Jan. 1978.

[7] G. J. da Silva Jr., "A teoria da complexidade aritmética aplicada à otimização de transformadas lineares," tese de doutorado, Universidade Federal de Pernambuco - UFPE, Recife - PE, 2012.

[8] G. J. da Silva Jr. and R. M. Campello de Souza, "Transformada rápida de Fourier otimizada," in *XXIX Simpósio Brasileiro de Telecomunicações (SBrT2011)*, Curitiba - PR, outubro 2011, pp. 1–5.

[9] M. T. Heideman, *Multiplicative Complexity, Convolution, and the DFT*. New York: Springer-Verlag, 1988.

[10] M. T. Chu, R. E. Funderlic, and G. H. Golub, "A rank-one reduction formula and its applications to matrix factorizations," *SIAM Review*, vol. 37, no. 4, pp. 512–530, 1995. [Online]. Available: http://dx.doi.org/10.1137/1037124

[11] G. Strang, *Linear Algebra and its Applications*, 2nd ed. Elsevier Inc, Academic Press Inc, 1980.