UM ALGORITMO RÁPIDO PARA A TRANSFORMADA WAVELET EM CORPOS FINITOS

R.G.F. Távora, H.M. de Oliveira, R.M. Campello de Souza

CODEC- DES- UFPE
C.P. 7800, 50.711-970 Recife - PE BRASIL
Emails: {Ricardo,hmo}@npd.ufpe.br, rgtavora@bol.com.br

Resumo Uma nova versão da Transformada Wavelet foi recentemente definida, a Transformada Wavelet em Corpos Finitos (TWCF). Esta transformada apresenta uma estrutura cíclica e pode ser definida no domínio freqüencial através da Transformada de Fourier em Corpos Finitos. O potencial desta ferramenta é promissor considerando a forma com que surgiram aplicações para a Transformada Wavelet Discreta em diversas áreas da Engenharia Elétrica. Um fator decisivo para o emprego eficiente desta ferramenta é a existência de algoritmos rápidos para o cálculo da mesma. Neste trabalho, um novo algoritmo rápido para a TWCF, com base na Transformada de Fourier em Corpos Finitos, é proposto.

1. INTRODUÇÃO

A Transformada Wavelet Discreta (TWD), que está associada à técnica de filtragem por sub-bandas, é uma ferramenta relativamente recente no campo do processamento digital de sinais. Recentemente a Transformada Wavelet em Corpos Finitos foi proposta por Caire *et al.* [1]. Nenhuma aplicação ainda foi proposta para esta nova ferramenta. Entretanto é promissor o emprego desta ferramenta em áreas que utilizam a Transformada de Fourier em Corpos Finitos (TFCF), como em Códigos Algébricos e em Criptografia, assim como aconteceu para a Transformada Wavelet Discreta que tem aplicações em várias áreas [2, 3, 4, 5] onde a Transformada de Fourier é usada. Um fator decisivo para a aplicação destas transformadas discretas é a existência de algoritmos rápidos para o cálculo das mesmas. Neste trabalho a TWCF é definida, explicitando sua estrutura cíclica. O projeto dos filtros g e h (passa-altas e passa-baixas respectivamente) é abordado e um novo algoritmo rápido para o cálculo da TWCF usando a TFCF é apresentado.

2. A TRANSFORMADA WAVELET CíCLICA

As condições necessárias obtidas na análise no domínio da freqüência para a geração dos filtros em Quadratura Espelhada (QMF) [6] (filtros passa-altas g e passa-baixas h) não são sempre suficientes, e outras condições devem ser impostas para garantir a reconstrução perfeita [7]. No entanto, quando as seqüências analisadas são periódicas, estas condições são também suficientes [1]. Neste caso, as matrizes H^j e G^j, na escala j, obtidas para os filtros, são matrizes circulantes,

$$G^j = \begin{bmatrix} g_0^j & g_1^j & g_2^j & \cdots & g_{N_j-1}^j \\ g_{N_j-2}^j & g_{N_j-1}^j & g_0^j & \cdots & g_{N_j-3}^j \\ g_{N_j-4}^j & g_{N_j-3}^j & g_{N_j-2}^j & \cdots & g_{N_j-5}^j \\ \vdots & \vdots & \vdots & & \vdots \\ g_2^j & g_3^j & g_4^j & \cdots & g_1^j \end{bmatrix},$$

e

$$H^j = \begin{bmatrix} h_0^j & h_1^j & h_2^j & \cdots & h_{N_j-1}^j \\ h_{N_j-2}^j & h_{N_j-1}^j & h_0^j & \cdots & h_{N_j-3}^j \\ h_{N_j-4}^j & h_{N_j-3}^j & h_{N_j-2}^j & \cdots & h_{N_j-5}^j \\ \vdots & \vdots & \vdots & & \vdots \\ h_2^j & h_3^j & h_4^j & \cdots & h_1^j \end{bmatrix},$$

logo esta transformada é cíclica. As matrizes G^j e H^j são completamente definidas pela primeira linha. A dizimação está embutida nas matrizes com deslocamentos cíclicos duplos das linhas. A aplicação recursiva destes filtros implementa um algoritmo de Análise de Multiresolução (AM) para o caso de seqüências c^j e d^j de período igual aos seus comprimentos (N_{j+1}). Além das condições para geração serem mais simples para a Transformada Wavelet Cíclica, a análise no domínio freqüencial em Corpos Finitos só é possível com a utilização da TFCF, que também é cíclica. Logo a definição da TWCF é feita para o caso cíclico.

3. A TRANSFORMADA WAVELET EM CORPOS FINITOS

Seja $F = GF(p^r)$, onde p é primo, $N = 2^n$ e $\alpha \in GF(p^r)$ um elemento de ordem 2^{n-1}. Para projetar transformadas em Corpos Finitos deve-se construir seqüências $\{g^j, h^j \in F\} | \, j = 1, 2, ..., n\}$ que satisfaçam às condições para a reconstrução perfeita, i.e. [1]

$$G^* G + H^* H = I, \quad HG^* = 0, \tag{1}$$

onde I denota a matriz identidade. Define-se:

$$\gamma^m = TFCF(g^m),\ m = 0, 1,$$
$$\eta^m = TFCF(h^m),\ m = 0, 1.$$

Então estas condições podem ser transferidas para o domínio freqüencial [1], resultando em

$$\begin{array}{c} \gamma^0_{-k}\gamma^0_k + \gamma^1_{-k}\gamma^1_k = \frac{1}{N'}, \\ \eta^m_k = (-1)^m v_k \gamma^{1-m}_{-k}\ , m = 0, 1. \end{array} \tag{2}$$

Logo, dadas duas seqüências γ e η, que satisfaçam à equação (2), deseja-se construir seqüências $\{g^j, h^j | j = 1, 2, ...n\}$ que especifiquem um esquema AM. Seqüências g^j e h^j que permitem uma reconstrução perfeita podem ser obtidas através de

$$\begin{array}{c} g^j_{2l+m} = TDF^{-1}[\{\gamma^m(\alpha^{2^{j-1}k}) | k = 0, 1, ..., 2^{n-j} - 1\}]_l\ , \\ h^j_{2l+m} = TDF^{-1}[\{\eta^m(\alpha^{2^{j-1}k}) | k = 0, 1, ..., 2^{n-j} - 1\}]_l\ , \end{array} \tag{3}$$

para $l = 0, 1, ..., 2^{n-j} - 1$, e $m = 0, 1$.

Pode-se mostrar [1] que G^j e H^j satisfazem à equação (1) para cada j.

Um exemplo para a TWCF é apresentado a seguir. Considerando o caso em que

$$h_k = (-1)^k g_{(1-k)} \pmod N,\ k = 0, 1, ..., N-1\,.$$

Seja $F = GF(2^q + 1)$ tal que $2^q + 1$ é um primo de Fermat. Neste caso pode-se definir a transformada para todos os casos $n \leq q + 1$. Tem-se $\alpha = \alpha_0^{2(q-n+1)}$, onde α_0 é um elemento primitivo de F. Por exemplo, em $GF(17)$, definindo os filtros no domínio da freqüência:

$$\eta^0 = \{\ 1\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0\ \},$$
$$\eta^1 = \{\ 16\quad 6\quad 6\quad 6\quad 6\quad 6\quad 6\quad 6\ \},$$

pode-se verificar facilmente que para qualquer inteiro k

$$\eta^0_k\eta^0_{-k} + \eta^1_k\eta^1_{-k} = 1/N',$$

onde $N' = 9$. Usando o núcleo $\zeta = 9 \in GF(17)$, e calculando o filtro h a partir da transformada inversa de Fourier em $GF(17)$, e aplicando a relação $h_k = (-1)^k g_{(1-k)} \pmod N$, obtém-se $h = \{3, 2, 14, 2, 14, 2, 14, 2, 14, 2, 14, 2, 14, 2, 14, 2\}$, e $g = \{15, 3, 15, 14, 15, 14, 15, 14, 15, 14, 15, 14, 15, 14, 15, 14\}$. A partir de g e da equação (3) pode-se calcular as demais seqüências:

$$g^2 = \{13, 16, 13, 6, 13, 6, 13, 6\},$$
$$h^2 = \{16, 4, 6, 4, 6, 4, 6, 4\},$$
$$g^3 = \{9, 11, 9, 5\},$$
$$h^3 = \{11, 8, 5, 8\}.$$

Sejam G e H as matrizes 2-circulantes geradas pelas linhas g e h respectivamente, e G^T e H^T suas respectivas transpostas. Pode-se verificar que $GH^T = HG^T = 0$ e $H^TG + G^TH = \frac{1}{N'}I$.

4. UM ALGORITMO RÁPIDO PARA A TWCF BASEADO NA TFCF

A TWCF de comprimento N pode ser calculada pela aplicação sucessiva dos operadores G e H, de acordo com

$$(Gx)_k = \sum_{l=0}^{N-1} g_{l-2k}x_l,$$
$$(Hx)_k = \sum_{l=0}^{N-1} h_{l-2k}x_l.$$

Sejam c e d as seqüências dadas por $c_k = (Hx)_k$ e $d_k = (Gx)_k$. Estes somatórios equivalem, cada um, a uma correlação seguida de uma subamostragem e podem ser calculados através da TFCF de comprimento N, pelo teorema da convolução. Dessa forma pode-se empregar os algoritmos rápidos existentes para a TFCF [8]. Neste caso, se a transformada dos filtros h e g forem pré-calculadas, são necessárias uma TFCF direta e duas TFCF inversas de comprimento N, além de 2N multiplicações no domínio freqüencial. No entanto, este cálculo pode ser mais eficiente. Calculando a TFCF da seqüência c usando como núcleo um elemento ζ de ordem $N/2$, tem-se

$$\begin{array}{c} C(i) = \sum_{k=0}^{N/2-1} c(k)\zeta^{ik} = \\ = \sum_{k=0}^{N/2-1}\sum_{j=0}^{N-1} h(j-2k)x(j)\zeta^{ik} = \\ = \sum_{j=0}^{N-1} x(j) \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik}. \end{array}$$

O somatório interno pode ser calculado de forma separada para os casos em que j é par ou ímpar, introduzindo novas seqüências $\{\widetilde{h}^0\}$ e $\{\widetilde{h}^1\}$ expressas por

$$\{\widetilde{h}^0\} = \{\ h(0)\quad h(-2)\quad h(-4)\quad \cdots\quad h(2)\ \}\ ,$$
$$\{\widetilde{h}^1\} = \{\ h(1)\quad h(-1)\quad h(-3)\quad \cdots\quad h(3)\ \}.$$

Logo, para j par:

$$S = \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik} = \sum_{k=0}^{N/2-1} \widetilde{h}^0(k)\zeta^{ik}\zeta^{ij/2} = \widetilde{\eta}^0(i)\zeta^{ij/2},$$

onde $\widetilde{\eta}^0(i) = TFCF(\widetilde{h}^0(k))$.

Para j ímpar :

$$\begin{array}{c} S = \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik} = \\ = \sum_{k=0}^{N/2-1} \widetilde{h}^1(k)\zeta^{ik}\zeta^{i(j-1)/2} = \\ = \widetilde{\eta}^1(i)\zeta^{i(j-1)/2}, \end{array}$$

onde $\widetilde{\eta}^1(i) = TFCF(\widetilde{h}^1(k))$. Por outro lado,

$$\begin{array}{c} \sum_{j=0}^{N-1} x(j) \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik} = \\ = \sum_{j=0}^{N/2-1} x(2j)S + \sum_{j=0}^{N/2-1} x(2j+1)S. \end{array}$$

Substituindo a expressão de S, tem-se

$$C(i) = \sum_{j=0}^{N/2-1} x(2j)\widetilde{\eta}^0(i)\zeta^{ij} + \sum_{j=0}^{N/2-1} x(2j+1)\widetilde{\eta}^1(i)\zeta^{ij}.$$

Definindo agora as expressões $\{x^0\}$ e $\{x^1\}$ dadas por

$$\begin{array}{l} \{x^0\} = \{\ x(0) \quad x(-2) \quad x(-4) \quad \cdots \quad x(2)\ \}\,, \\ \{x^1\} = \{\ x(1) \quad x(-1) \quad x(-3) \quad \cdots \quad x(3)\ \}, \end{array}$$

tem-se

$$C(i) = \sum_{j=0}^{N/2-1} x^0(j)\widetilde{\eta}^0(i)\zeta^{ij} + \sum_{j=0}^{N/2-1} x^1(j)\widetilde{\eta}^1(i)\zeta^{ij}.$$

Sejam $\{X^0\}$ e $\{X^1\}$ as $TFCF$ de $\{x^0\}$ e $\{x^1\}$, respectivamente. Logo os valores de $C(i)$ podem ser calculados de acordo com

$$C(i) = X^0(i)\widetilde{\eta}^0(i) + X^1(i)\widetilde{\eta}^1(i).$$

Finalmente $c(k) = TFCF^{-1}(C(i))$.

O cálculo efetuado para a seqüência $\{d\}$ é análogo. Sejam

$$\begin{array}{c} \{\widetilde{g}^0\} = \{\ g(0) \quad g(-2) \quad g(-4) \quad \cdots \quad g(2)\ \}, \\ \{\widetilde{g}^1\} = \{\ g(1) \quad g(-1) \quad g(-3) \quad \cdots \quad g(3)\ \}, \\ \widetilde{\gamma}^0(i) = TFCF(\widetilde{g}^0(k)), \\ \widetilde{\gamma}^1(i) = TFCF(\widetilde{g}^1(k)). \end{array}$$

Tem-se

$$D(i) = TFCF(d(k))$$

e

$$D(i) = X^0(i)\widetilde{\gamma}^0(i) + X^1(i)\widetilde{\gamma}^1(i).$$

Logo, são necessárias duas $TFCF$ diretas e duas $TFCF$ inversas de comprimento $N/2$. O número de multiplicações no domínio freqüencial é $2N$.

Pode-se observar também que $\widetilde{\eta}^0(i) = \widetilde{\gamma}^1(i)$, e $\widetilde{\eta}^1(i) = -\widetilde{\gamma}^0(i)$.

Logo

$$C(i) = X^0(i)\widetilde{\gamma}^1(i) - X^1(i)\widetilde{\gamma}^0(i).$$

Observando que as expressões de $C(i)$ e $D(i)$ possuem a mesma estrutura de uma multiplicação complexa, elas podem ser calculadas por [8, pag. 73]

$$\begin{bmatrix} C(i) \\ D(i) \end{bmatrix} = \\ = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} X^0(i) & & \\ & X^1(i)-X^0(i) & \\ & & X^0(i)+X^1(i) \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \widetilde{\gamma}^1(i) \\ \widetilde{\gamma}^0(i) \end{bmatrix}.$$

Dessa forma, reduz-se o número de multiplicações no domínio da freqüencial de $2N$ para $3N/2$. A figura 1 ilustra o esquema do cálculo da TWCF pelo algoritmo descrito.

5. CONCLUSÕES

O algoritmo proposto reduz a complexidade para o cálculo da TFCF, especialmente quando os filtros são definidos na freqüência e possuem poucos elementos nulos. Uma outra alternativa para reduzir a complexidade do cálculo da transformada consiste no uso de filtros com poucos coeficientes não nulos. Para isso, deve-se projetar os filtros no domínio do tempo, o que é mais difícil que no domínio freqüencial. Se as linhas das matrizes H^j e G^j possuírem no máximo M elementos não nulos, então o j-ésimo estágio da decomposição precisará de no máximo $MN2^{1-j}$ multiplicações e $(M-1)N2^{1-j}$ adições. Logo a decomposição completa precisará de no máximo uma ordem de $(2M-1)N\sum_{j=0}^{n-1} 2^{-j} = 2(2M-1)(N-1)$ operações, em comparação com $O(N\log_2(N))$ do algoritmo proposto usando a TFCF.

Uma possível aplicação para a TWD é a compressão de imagens. Um esquema proposto por Ingrid et al. [9], utiliza a TWD com técnica de pré-codificação e de fatoração ('lifting'), para permitir o mapeamento de seqüências de Z^N em Z^N, onde Z^N denota seqüências de comprimento N com elementos inteiros, evitando assim os erros de arredondamento. Este esquema pode ser então aplicado à compressão de imagens sem perda. A TWCF parece ser mais apropriada para esta aplicação, uma vez que imagens com componentes em Z^N possuem TWCF também com componentes em Z^N, sem que seja necessário qualquer pré-codificação.

6. REFERÊNCIAS

[1] CAIRE, G.; GROSSMAN, R. L.; POOR, H. V. Wavelet Transforms Associated with Finite Cyclic Groups. *IEEE Transactions on Information Theory*, v. 39, n. 4, julho 1993.

[2] LEARNED, R. E.; KRIM, H.; CLAUS, B. Wavelet-Packet Based Multiple Access Communication. *SPIE International Symposium*, julho 1994.

[3] LINDSEY, A. R.; DILL, J. C. Wavelet Packet Modulation: A Generalized Method for Orthogonal Multiplexed Communications.

[4] VILLASENOR, J.; BELTZER, B.; LIAO, J. Wavelet Filter Evaluation for Image Compression. *IEEE Trans. on Image Processing*, v. 2, p. 1053–1060, agosto 1995.

[5] COIFMAN, R.; MEYER, Y.; QUAKE, S.; WICKHAUSER, V. Signal Processing and Compression with Wavelet Packets. Numerical Algorithms Research Groups, Yale University, 1990.

[6] VAIDYANATHAN, P. P. Quadrature Mirror Filters, M-band Extensions and Perfect-Reconstruction Techniques. *ASSP Magazine*, v. 4, n. 3, p. 4–20, julho 1987.

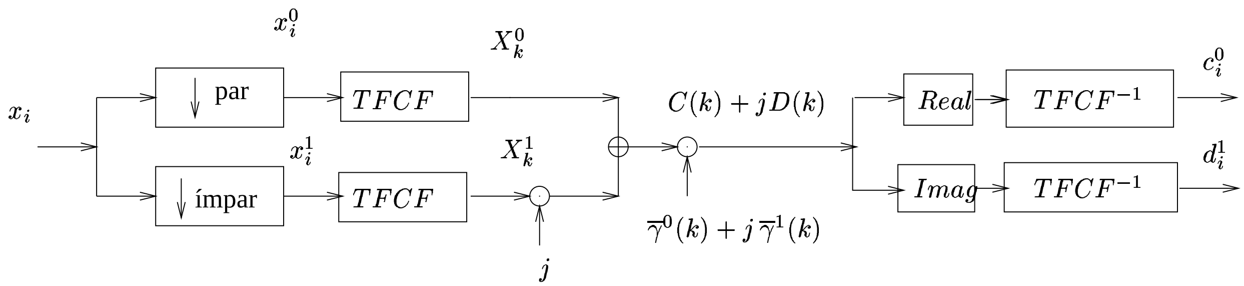

Figura 1: Esquema da cálculo da TWCF pela decomposição bifásica.

[7] DAUBECHIES, I. Ten Lectures on Wavelets. SIAM, 1992.

[8] BLAHUT, R. E. Fast Algorithms for Digital Signal Processing. Addison-Wesley, 1985.

[9] CALDERBANK, A. R.; DAUBECHIES, I.; SWELDENS, W.; YEO, B. Wavelet Transforms that Map Integers to Integers. *Appl. Comput. Harmon. Anal.*, v. 5, n. 3, p. 332–369, 1998.