Banco de Filtros e Wavelets para Sistemas Cíclicos sobre Corpos Finitos

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

***Resumo*— Este artigo apresenta uma abordagem para sinais e sistemas de comprimento finito, denominados aqui como sinais e sistemas cíclicos. A Transformada de Fourier em Corpo Finito e a transformada Z cíclica são apresentadas nesse contexto. Os sistemas subamostrador e sobreamostrador são definidos para sinais cíclicos. É mostrada a estrutura de banco de filtros cíclicos e, a partir destas, as séries wavelet para sinais cíclicos. Exemplos e aplicações em corpos finitos são apresentados.**

***Palavras-Chave*— Corpo finito, banco de filtros cíclicos, wavelets cíclicas, transformada Z cíclica, TFCF, sistemas cíclicos.**

***Abstract*— This paper presents a framework to deal with cyclic and finite length signals and systems. The finite field Fourier transform and the cyclic Z transform are presented in this context. The downsampler and upsampler systems are defined for cyclic signals. The structure of cyclic filter banks is shown and wavelet series for cyclic signals are constructed. Examples and applications in finite fields are presented.**

***Keywords*— Finite fields, cyclic filter banks, cyclic wavelets, cyclic Z transform, FFFT, cyclic systems.**

I. INTRODUÇÃO

A teoria de sinais e sistemas sobre o corpo dos complexos encontra-se bem estabelecida [1]-[3]. Sinais e sistemas são quase sempre analisados e simulados em máquinas digitais que utilizam aritmética de ponto flutuante, o que leva a aproximações de números reais, podendo acarretar em erros de quantização [1]. Estruturas sobre corpos finitos [4] vêm se tornando atrativas, no sentido de que as mesmas podem ser armazenadas em máquinas e processadores digitais, evitando erros de quantização e arredondamento causados por operações com ponto flutuante. Muitas ferramentas de engenharia vêm emergindo para estruturas definidas sobre corpos finitos [5]-[9].

Sistemas baseados nas chamadas estruturas cíclicas são de especial interesse em engenharia, uma vez que apresentam comprimento finito, como por exemplo os códigos cíclicos [10] e sistemas baseados na DFT, o que facilita sua implementação [1], [5].

Formalmente, um sistema é dito *cíclico* se suas entradas e saídas são blocos de comprimento fixo, *N*, denominados *sinais cíclicos*. Nesse cenário, a operação de deslocamento é substituída pelo deslocamento circular ou cíclico. De forma análoga aos sistemas lineares e invariantes no tempo, um sistema *cíclico linear invariante no tempo* (CLIT) também pode ser caracterizado por sua resposta ao impulso, $h[n]$ (Figura 1).

G. J. 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, E-mails: gilsonjr@gmail.com, ricardo@ufpe.br.

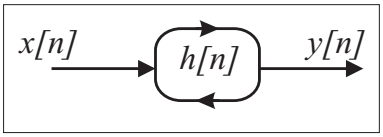

Fig. 1. Diagrama ilustração de um sistema CLIT.

A notação indicada a seguir é utilizada neste trabalho:

$N \rightarrow$ Comprimento do sinal;
$n \rightarrow$ Índice de variável no domínio do tempo;
$k \rightarrow$ Índice de variável no domínio da freqüência;
$\alpha \rightarrow$ Elemento de GF(p^m) (Campo de Galois de ordem p^m) com ordem *N*.

Dessa forma, um sinal cíclico $x[n]$ é um vetor com *N* elementos em GF(p^m). Toda notação de deslocamento se refere a deslocamento cíclico. Os sinais cíclicos também podem ser vistos como sinais infinitos com período N. A saída de um sistema CLIT é dada por

$$y[n] = \sum_{j=0}^{N-1} x[j]h[n-j] = x[n] \circledN h[n], \tag{1}$$

onde $\circledN$ denota convolução cíclica de comprimento N.

As seqüências $x[n]$ e $X[k]$, $n, k = 0, 1, \ldots, N-1$, onde $x[n], X[k] \in GF(p^m)$, formam um par da transformada de Fourier em corpo finito (TFCF), denotado por

$$x[n] \overset{\mathcal{F}}{\longleftrightarrow} X[k],$$

se

$$X[k] \triangleq \sum_{n=0}^{N-1} x[n]\alpha^{kn}, \tag{2}$$

e

$$x[n] = N^{-1}(mod\ p) \sum_{k=0}^{N-1} X[k]\alpha^{-kn}. \tag{3}$$

A TFCF possui propriedades análogas às da DFT [1], [5].

Uma outra transformada de interesse é a transformada Z cíclica sobre corpos finitos, que pode ser vista como uma notação polinomial do sinal ou do sistema, notação bastante utilizada em códigos cíclicos [10]. Para a seqüência $x[n]$, $n = 0, 1, \ldots, N-1$, onde $x[n] \in GF(p^m)$, existe um polinômio $X(z)$, com coeficientes em $GF(p^m)$, na variável z^{-1}, o qual representa a transformada Z cíclica de $x[n]$, denotada por

$$x[n] \overset{Z}{\longleftrightarrow} X(z),$$

se

$$X(z) \triangleq \sum_{n=0}^{N-1} x[n]z^{-n}. \quad (4)$$

Então, mostra-se que

$$x[n] = N^{-1}(mod\ p)\sum_{z\in S} X(z)z^n, \quad (5)$$

onde $S = \{1,\ \alpha,\ \alpha^2, \ldots,\ \alpha^{N-1}\}$. Como o sistema é cíclico, a transformada Z está associada a aritmética polinomial módulo $(z^{-N}-1)$.

A TFCF se relaciona com a transformada Z cíclica por meio da seguinte relação:

$$X[k] = X(z)|_{z=\alpha^{-k}} = X(\alpha^{-k}), \quad (6)$$

para $k = 0, 1, \ldots, N-1$.

Este trabalho está organizado como descrito a seguir. Nas seções II e III são introduzidos, respectivamente, o subamostrador e o sobreamostrador cíclicos. Na seção IV, é mostrada uma forma eficiente de processar sinais subamostrados. A seção V apresenta duas identidades importantes para processamento multitaxa e as seções seguintes (VI e VII) descrevem as estruturas de banco de filtros e wavelets cíclicas. As conclusões sobre o trabalho são apresentadas na seção VIII.

II. Sistema Subamostrador ou Compressor Cíclico

O sistema da Figura 2 é um sistema subamostrador cíclico no tempo. A saída é denotada por $x_d[n] = x[Mn]$. Em sistemas não cíclicos, o sinal $x_d[n]$ tem comprimento M vezes menor que o comprimento de $x[n]$. Para sistemas cíclicos, o comprimento da saída é sempre N, porém, a mesma pode ser expressa de forma reduzida.

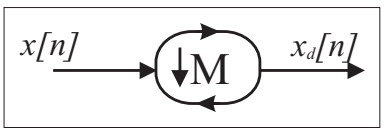

Fig. 2. Diagrama de um sistema subamostrador cíclico de parâmetro *M*.

Definição 1: Um sistema subamostrador M cíclico, com entrada $x[n]$ e saída $x_d[n] = x[Mn]$, existirá se M divide N.

Com essa definição, a saída de um subamostrador pode ser representada por um sinal cíclico de comprimento N/M.

Proposição 1: A saída de um subamostrador M, $x_d[n]$, apresenta período igual a N/M, ou seja,

$$x_d[n + N/M] = x_d[n]. \quad (7)$$

Demonstração: $x[n]$ tem período pelo menos N, por definição de sinal cíclico. Então, $x[n] = x[n+N]$, de modo que $x_d[n + N/M] = x[M(n + N/M)] = x[Mn + N] = x[Mn] = x_d[n]$. ■

Pode-se então representar a saída de um subamostrador M por um sinal cíclico de comprimento N/M.

Exemplo 1: Considere o sinal $x[n] = (1, 2, 3, 4, 5, 6)$ como entrada de um subamostrador com $M = 3$. Então $x_d[n] = x[3n] = (1, 4, 1, 4, 1, 4) = (1, 4)$, onde a última igualdade expressa a seqüência $x_d[n]$ em forma reduzida.

A. Análise do Subamostrador Cíclico

Para analisar a saída $x_d[n]$ do subamostrador cíclico, considera-se a seqüência $s_M[n]$ definida a seguir:

$$s_M[n] = \begin{cases} 1, & \text{se } n \equiv 0\ (mod\ M) \\ 0, & \text{caso contrário,} \end{cases} \quad (8)$$

$n = 0, 1, \ldots, N-1$. Se $M|N$, essa seqüência pode ser representada de duas formas,

$$s_M[n] = \sum_{j=0}^{N/M-1} \delta[n - jM] \quad (9)$$

ou

$$s_M[n] = M^{-1}\sum_{j=0}^{M-1} \alpha^{-\frac{N}{M}jn}. \quad (10)$$

Amostrando a seqüência $x[n]$ chega-se à

$$x_s[n] = x[n]s_M[n], \quad (11)$$

cuja transformada Z cíclica pode ser obtida por meio de (9) como sendo

$$X_s(z) = \sum_{j=0}^{N/M-1} x[Mj]z^{-jM} = \sum_{j=0}^{N/M-1} x_d[j]z^{-jM}. \quad (12)$$

Alternativamente, partindo-se de (10), chega-se a

$$X_s(z) = M^{-1}\sum_{j=0}^{M-1} X(\alpha^{\frac{N}{M}j}z). \quad (13)$$

Utilizando as equações (4) e (7), chega-se à expressão da transformada Z do sinal $x_d[n]$,

$$X_d(z) = \sum_{j=0}^{M-1} z^{-\frac{N}{M}j} \sum_{n=0}^{N/M-1} x[Mn]z^{-n}. \quad (14)$$

De (9) e (12), pode-se escrever

$$X_d(z) = S_{\frac{N}{M}}(z)X_s(z^{\frac{1}{M}}), \quad (15)$$

onde $S_{\frac{N}{M}}(z) = \sum_{j=0}^{M-1} z^{-\frac{N}{M}j}$ é a transformada Z de $s_{\frac{N}{M}}[n]$. Usando (13) chega-se a uma expressão que só depende de $X(z)$,

$$X_d(z) = M^{-1}S_{\frac{N}{M}}(z)\sum_{j=0}^{M-1} X(\alpha^{\frac{N}{M}j}z^{\frac{1}{M}}). \quad (16)$$

Utilizando (6) para obter resultados no domínio da freqüência, chega-se a

$$X_s[k] = M^{-1}\sum_{j=0}^{M-1} X[k - \frac{N}{M}j] \quad (17)$$

e

$$X_d[k] = \begin{cases} \sum_{j=0}^{M-1} X[\frac{k}{M} - \frac{N}{M}j], & \text{se } M \text{ divide } k \\ 0, & \text{caso contrário.} \end{cases} \quad (18)$$

Essas propriedades funcionam também para sistemas cíclicos no corpo dos reais. Para isso, basta substituir α por $e^{j2\pi/N}$.

III. Sistema Sobreamostrador ou Expansor Cíclico

O sistema sobreamostrador cíclico, Figura 3, será definido de acordo com a Figura 4, ou seja, a saída do sistema em cascata subamostrador - sobreamostrador L resulta em $x_s[n]$ para uma entrada $x[n]$. Essa relação vale também para sistemas não cíclicos.

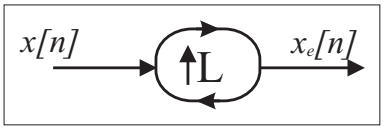

Fig. 3. Representação de um sistema sobreamostrador L cíclico no tempo.

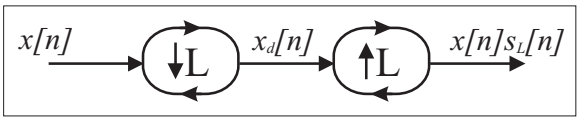

Fig. 4. O sistema sobreamostrador é definido de forma que o sistema em cascata subamostrador sobreamostrador, para uma entrada $x[n]$, resulta em $x[n]s_L[n]$, assim como em sistemas não cíclicos.

Assim, a definição de um sistema sobreamostrador cíclico é feita da seguinte forma:

***Definição** 2:* Um sistema sobreamostrador cíclico de parâmetro L existirá se L divide N, de tal forma que, para uma entrada $x[n]$, a saída $x_e[n]$ é dada por

$$x_e[n] = L^{-1} \sum_{j=0}^{N-1} x[j]\delta[n - jL]. \tag{19}$$

Pode-se fazer algumas observações sobre essa definição:

- Os sinais expandidos podem ter componentes não nulas apenas em valores de n que são múltiplos de L;
- Se o sinal $x[n]$ tem período N/L (foi resultado de uma compressão de L), então o sinal expandido é dado simplesmente por

$$x_e[n] = \begin{cases} x[n/L], & \text{se } L \text{ divide } n \\ 0, & \text{caso contrário.} \end{cases} \tag{20}$$

- A expansão de um sinal $x[n]$ que não possui período N/L, sofrerá perda de informação com a expansão pela sobreposição (*aliasing*). Isso não ocorre em sistemas não cíclicos.

A. Análise do Sobreamostrador Cíclico

O sinal $x_e[n]$ pode ser analisado a partir da definição da transformada Z cíclica, Equação (4), e da definição 2 (19). Tem-se

$$X_e(z) = L^{-1}X(z^L). \tag{21}$$

Passando para o domínio de Fourier,

$$X_e[k] = L^{-1}X[Lk]. \tag{22}$$

Conclui-se que uma compressão no tempo gera uma expansão na freqüência e uma expansão no tempo gera uma compressão na freqüência, semelhante ao caso de sistemas não cíclicos.

IV. Convolução Cíclica de Sinais Subamostrados

Os sinais de saída de um sistema subamostrador tem comprimento $R = N/M$ e também são cíclicos. Observando o que acontece quando se convolui um sinal $x[n]$, de período R, com um outro $y[n]$, de período N, tem-se

$$x[n] \circledN y[n] = \sum_{j=0}^{N-1} x[j]y[n-j] = \sum_{j=0}^{R-1}\sum_{m=0}^{M-1} x[j]y[n-j-mR],$$

ou

$$x[n] \circledN y[n] = \sum_{j=0}^{R-1} x[j] \sum_{m=0}^{M-1} y[n-j-m\frac{N}{M}]. \tag{23}$$

Definindo a representação reduzida de $y[n]$ de período R por

$$y_R[n] = \sum_{m=0}^{M-1} y[n-mR], \tag{24}$$

observa-se que $y_R[n]$ tem período R. Pode-se então simplificar a expressão da convolução cíclica para

$$x[n] \circledN y[n] = \sum_{j=0}^{R-1} x[j]y_R[n-j] = x[n] \circledR y_R[n]. \tag{25}$$

A computação da representação reduzida (24) não possui multiplicações. Isto reduz a complexidade computacional multiplicativa da convolução cíclica envolvendo um sinal reduzido.

Supõe-se agora que ambos os sinais, $x[n]$ e $y[n]$, são reduzidos de período R. Utilizando a expressão (24) para calcular a representação reduzida de $y[n]$ e sabendo que $y[n] = y[n+mR]$, chega-se a

$$y_R[n] = \sum_{m=0}^{M-1} y[n-mR] = My[n]. \tag{26}$$

A expressão da convolução para sinais reduzidos pode ser encontrada substituindo (26) em (25), resultando em

$$x[n] \circledN y[n] = Mx[n] \circledR y[n]. \tag{27}$$

V. Trocando a Posição do Filtro com o Subamostrador/Sobreamostrador

Para o estudo de banco de filtros algumas relações básicas são necessárias, as quais são válidas para sinais não cíclicos, mas que precisam ser demonstradas para sistemas cíclicos.

A. Primeira Identidade Nobre

***Proposição** 2:* Os sistemas (a) e (b) da Figura 5 são equivalentes.

Demonstração: Partindo do sistema (a), utilizando a propriedade da convolução,

$$W(z) = X(z)H(z^M)$$

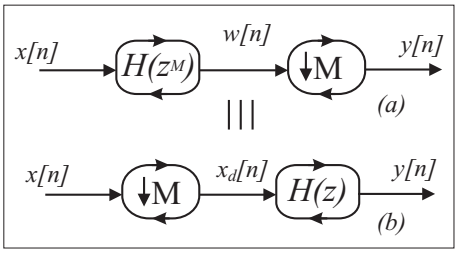

Fig. 5. Primeira identidade nobre - Os sistemas (a) e (b) são equivalentes.

e

$$Y(z) = W_d(z) = M^{-1} S_{\frac{N}{M}}(z) \sum_{j=0}^{M-1} X(\alpha^{\frac{N}{M}j} z^{\frac{1}{M}}) H(\alpha^{Nj} z).$$

Como $\alpha^{Nj} = 1$, pode-se retirar $H(z)$ do somatório e portanto

$$Y(z) = H(z) M^{-1} S_{\frac{N}{M}}(z) \sum_{j=0}^{M-1} X(\alpha^{\frac{N}{M}j} z^{\frac{1}{M}}) = H(z) X_d(z),$$

que é a relação entrada/saída para o sistema (b). ■

B. Segunda Identidade Nobre

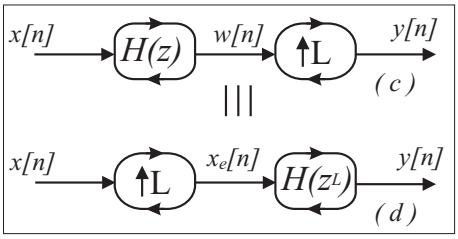

Fig. 6. Segunda identidade nobre - Os sistemas (c) e (d) são equivalentes.

***Proposição** 3:* Os sistemas (c) e (d) da Figura 6 são equivalentes.

Demonstração: Partindo do sistema (c),

$$W(z) = X(z) H(z)$$

e

$$Y(z) = W_e(z) = L^{-1} W(z^L) = L^{-1} X(z^L) H(z^L),$$

o que implica

$$Y(z) = X_e(z) H(z^L),$$

que é a relação entrada/saída para o sistema (d). ■

VI. Banco de Filtros em Sistemas Cíclicos

Considere a estrutura da Figura 7, um banco de filtros cíclicos (BFC) de M canais que recupera exatamente o sinal de entrada após a síntese, uma característica chamada de reconstrução perfeita [2], [3].

***Proposição** 4:* Para um banco de filtros cíclicos de M canais, como mostrado na Figura 7, se a chamada relação de reconstrução perfeita (28) é satisfeita, ou seja, se

$$\sum_{j=0}^{M-1} H_j(\alpha^{\frac{N}{M}m} z) G_j(z) = M\delta[m], \qquad (28)$$

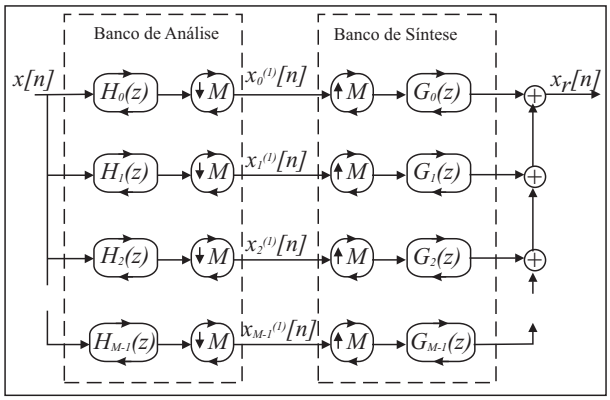

Fig. 7. Estrutura de um banco de filtros cíclicos de M canais, ilustrando o banco de análise e de síntese.

então, $x_r[n] = x[n]$.

Demonstração: Para a j-ésima linha da estrutura, chamando a saída do filtro $G_j(z)$ de $y_j[n]$, temos a seguinte equação de saída da linha j:

$$Y_j(z) = G_j(z)(H_j(z)X(z))_s.$$

Considerando as expressões (16) e (21),

$$Y_j(z) = G_j(z) M^{-1} \sum_{m=0}^{M-1} H_j(\alpha^{\frac{N}{M}m} z) X(\alpha^{\frac{N}{M}m} z).$$

Somando todas as M saídas da estrutura temos o sinal recuperado, denotado por $x_r[n]$. Então

$$X_r(z) = \sum_{j=0}^{M-1} Y_j(z) =$$

$$M^{-1} \sum_{j=0}^{M-1} G_j(z) \sum_{m=0}^{M-1} H_j(\alpha^{\frac{N}{M}m} z) X(\alpha^{\frac{N}{M}m} z) =$$

$$M^{-1} \sum_{m=0}^{M-1} X(\alpha^{\frac{N}{M}m} z) \sum_{j=0}^{M-1} H_j(\alpha^{\frac{N}{M}m} z) G_j(z).$$

Substituindo o último somatório pela relação de reconstrução perfeita (28), a expressão de $X_r(z)$ se reduz a

$$X_r(z) = M^{-1} \sum_{m=0}^{M-1} X(\alpha^{\frac{N}{M}m} z) M\delta[m] =$$

$$\sum_{m=0}^{M-1} X(\alpha^{\frac{N}{M}m} z)\delta[m] = X(z).$$

■

A reconstrução perfeita pode também ser analisada no domínio da freqüência por (6). A Equação (28) torna-se

$$\sum_{j=0}^{M-1} H_j[k - \frac{N}{M}m] G_j[k] = M\delta[m]. \qquad (29)$$

***Exemplo** 2:* Considere o corpo GF(2^4), com $N = 15$, $M = 3 \equiv 1(mod\ 2)$ e α um elemento de ordem 15, raiz

do polinômio primitivo sobre GF(2), $\pi(x) = x^4 + x + 1$. Utilizando (29), escolhe-se os filtros sem sobreposição:
$H_0[k] = (1,1,1,0,1,0,0,0,1,0,0,0,0,0,0,0) = G_0[k]$,
$H_1[k] = (0,0,0,0,0,1,0,1,0,0,0,0,1,0,1,1) = G_1[k]$,
$H_2[k] = (0,0,0,1,0,0,1,0,0,0,1,1,0,1,0,0) = G_2[k]$.
A Equação (29) é facilmente verificada, pois, $H_i[k]G_i[k] = H_i[k]$ e $H_i[k-5m]G_i[k] = 0$, para $m \neq 0(mod\ 3)$. Além disso, $H_0[k] + H_1[k] + H_2[k] = 1$, para $k = 0, 1, \ldots, N-1$. Logo, essa estrutura é um banco de filtros com reconstrução perfeita (Figura 7, com $M = 3$). Para o sinal de entrada $x[n] = (1,0,0,1,1,1,0,0,0,1,1,1,1,0,0)$, a saída do banco de análise resulta em
$x_0^{(1)}[n] = (0,0,0,0,0,0)$,
$x_1^{(1)}[n] = (0,0,1,1,0)$,
$x_2^{(1)}[n] = (1,1,1,0,1)$.
Aplicando esses valores nas entradas do banco de síntese, verifica-se que ocorre a reconstrução perfeita de $x[n]$ na saída.

A. Banco de Filtros Cíclicos de Dois Canais

Banco de filtros de dois canais são as estruturas mais simples e mais utilizadas na teoria de banco de filtros para sistemas não cíclicos. A grande vantagem é a simplificação computacional para o projeto dos bancos. A estrutura de dois canais está apresentada na Figura 8.

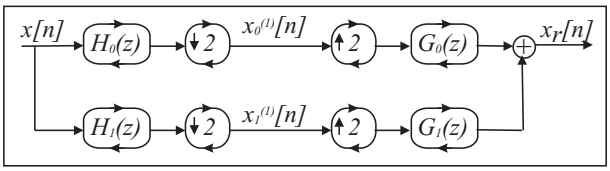

Fig. 8. Estrutura de um banco de filtros de dois canais.

Escrevendo a Equação (28) em forma matricial com $M = 2$, tem-se

$$\begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix} \begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix}. \quad (30)$$

Definindo a matriz modulação $\mathbf{H}_m(z)$ como

$$\mathbf{H}_m^T(z) = \begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix}, \quad (31)$$

resulta em

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = 2\Lambda^{-1}(z) \begin{bmatrix} H_1(-z) \\ -H_0(-z) \end{bmatrix}, \quad (32)$$

onde $\Lambda(z) = det(\mathbf{H}_m(z))$.

B. Projeto de Banco de Filtros Cíclicos

O método apresentado para o projeto consiste em restringir $\Lambda(z) = \beta z^l$. Isto faz com que sempre se encontre solução para $\Lambda^{-1}(z)(mod\ z^{-N} - 1)$. A constante β não nula pode variar, assim como o valor de l, o qual tem a restrição de ser ímpar. Adotando $\beta = 2$ e substituindo em (32), resulta em

$$G_0(z) = z^{-l} H_1(-z) \quad (33)$$

e

$$G_1(z) = -z^{-l} H_0(-z). \quad (34)$$

Com esses dois resultados, a equação matricial (30) reduz-se a

$$H_0(z)G_0(z) + H_0(-z)G_0(-z) = 2. \quad (35)$$

Definindo o filtro produto

$$P(z) = H_0(z)G_0(z) \quad (36)$$

e substituindo em (35), tem-se

$$P(z) + P(-z) = 2. \quad (37)$$

O polinômio $P(z)$ contém apenas potências ímpares de z^{-1} e o termo independente é a unidade. Assim, pode-se propor um método de projeto para banco de filtros cíclicos.

***Proposição** 5:* Um método para projeto de banco de filtros cíclicos:

- Escolher um filtro $P(z)$ satisfazendo (37);
- Fatorar $P(z)$ em $H_0(z)G_0(z)$;
- Utilizar as equações (33) e (34) para encontrar $H_1(z)$ e $G_1(z)$.

VII. Wavelets Cíclicas sobre Corpos Finitos

As expressões da série wavelet cíclica sobre corpos finitos podem ser obtidas por iterações de banco de filtros de dois canais, estruturas conhecidas como *Octave-Band* (divide o sinal em oitavas, no caso de sistemas não cíclicos), como mostra a Figura 9.

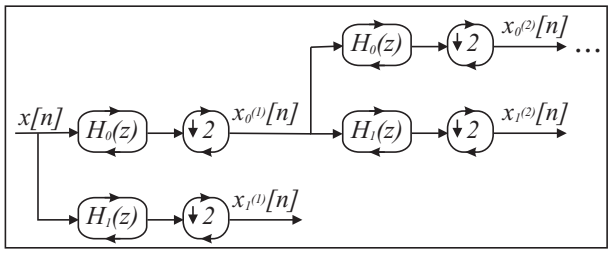

Fig. 9. BFC de análise *Octave-Band* (resulta nas séries wavelet cíclicas sobre corpos finitos).

Como existe compressão por 2 somente se o comprimento do bloco é par, então existirá saída no estágio j, $x_1^{(j)}[n]$ e $x_0^{(j)}[n]$, se 2^j divide N. O sinal original é recuperado utilizando a estrutura de síntese, mostrada na Figura 10.

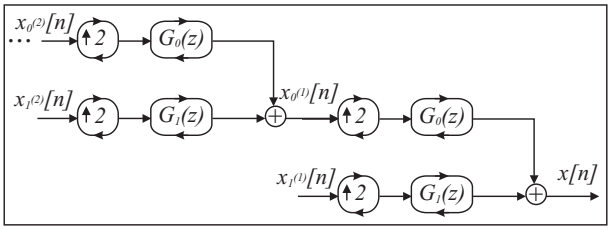

Fig. 10. BFC de sintese *Octave-Band*.

A partir da Figura 9, pode-se utilizar a primeira identidade nobre para colocar todos os subamostradores nas extremidades da direita. Assim, definindo

$$H_0^{(j)}(z) = \prod_{i=0}^{j-1} H_0(z^{2^i}) = H_0^{(j-1)}(z) H_0(z^{2^{j-1}}) \qquad (38)$$

e

$$H_1^{(j)}(z) = H_1(z^{2^{j-1}}) \prod_{i=0}^{j-2} H_0(z^{2^i}) = H_0^{(j-1)}(z) H_1(z^{2^{j-1}}), \qquad (39)$$

$j = 1, 2, \ldots, J$, em que J é o maior número tal que $2^J | N$, os sinais nas saídas do estágio j são

$$x_i^{(j)}[l] = \sum_{n=0}^{N-1} x[n] h_i^{(j)}[2^j l - n], \qquad (40)$$

$i = 0, 1$.

A expressão de síntese pode ser encontrada, utilizando a segunda identidade nobre para colocar os sobreamostradores na extrema esquerda. Definindo

$$G_0^{(j)}(z) = \prod_{i=0}^{j-1} G_0(z^{2^i}) = G_0^{(j-1)}(z) G_0(z^{2^{j-1}}) \qquad (41)$$

e

$$G_1^{(j)}(z) = G_1(z^{2^{j-1}}) \prod_{i=0}^{j-2} G_0(z^{2^i}) = G_0^{(j-1)}(z) G_1(z^{2^{j-1}}), \qquad (42)$$

pode-se escrever a expressão de saída no domínio Z,

$$X(z) = \sum_{j=1}^{J} 2^{-j} X_1^{(j)}(z^{2^j}) G_1^{(j)}(z) + 2^{-J} X_0^{(J)}(z^{2^j}) G_0^{(J)}(z). \qquad (43)$$

Considerando a transformada Z inversa de (43), encontra-se a expressão de síntese para J estágios,

$$x[n] = \sum_{j=1}^{J} \sum_{l=0}^{N/2^j-1} x_1^{(j)}[l] g_1^{(j)}[n - 2^j l] + \sum_{l=0}^{N/2^J-1} x_0^{(J)}[l] g_0^{(J)}[n - 2^J l]. \qquad (44)$$

***Exemplo** 3:* Considere o corpo GF(7^2), $N = 7^2 - 1 = 48$, e o elemento primitivo α, raiz do polinômio $\pi(x) = x^2 + x + 3$. Utilizando o método de projeto da proposição 5, considere $P(z) = (1 + z^{-1})^4 R(z)$.

Essa é a construção de Daubechies D_2, utilizada para construir banco de filtros para sistemas não cíclicos sobre o corpo dos reais. O polinômio $R(z) = (a + bz^{-1} + az^{-2}z)z^3$ apresenta solução única para a e b para $P(z)$ satisfazer (37). A solução em GF(49) é $a = 3$ e $b = 2$, ou seja,
$P(z) = (1 + z^{-1})^4 (3 + 2z^{-1} + 3z^{-2}) z^3$.
Escolhendo
$H_0(z) = 4 + 2z^{-1} + 2z^{-47}$,
$G_0(z) = 5 + 4z^{-1} + 5z^{-2} + 5z^{-46} + 4z^{-47}$,
e utilizando as equações (33) e (34), com $l = 1$, chega-se a
$H_1(z) = 4 + 2z^{-1} + 2z^{-45} + 4z^{-46} + 2z^{-47}$,
$G_1(z) = 2 + 5z^{-1} + 2z^{-2}$. Se
$x[n] = (0, 1, 2, 3, 4, 5, 6, 0, 1, 2, \ldots, 4, 5) = n(mod\ 7)$ é a entrada do banco com quatro estágios (quatro é o número máximo de estágios para $N = 48$), obtém-se os resultados:
$x_1^{(1)}[l] = (5, 0, 0, \ldots, 0, 6)$,
$x_1^{(2)}[l] = (4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5)$,
$x_1^{(3)}[l] = (0, 0, 0, 0, 0, 1)$,
$x_1^{(4)}[l] = (5, 0, 6)$,
$x_0^{(4)}[l] = (5, 2, 4)$.
Utilizando o banco de síntese para D_2 em $GF(7)$, recupera-se exatamente o sinal original de comprimento $N = 48$.

VIII. Conclusões e Sugestões

Dois novos sistemas cíclicos foram definidos, o subamostrador e o sobreamostrador cíclico, os quais foram utilizados para definir as estruturas de *banco de filtros cíclicos* (BFC). Um método de projeto de BFC foi proposto. A série wavelet cíclica foi apresentada, utilizando estruturas BFC. As estruturas BFC e as séries wavelet cíclicas constituem novas ferramentas que podem ser utilizadas na análise de sinais sobre corpos finitos e sobre o corpo dos complexos. Para corpos finitos destacam-se aplicações na análise e geração de códigos de bloco [11]. Para o corpo dos complexos, estão sendo estudadas aplicações de BFC em processamento de imagem, esteganografia e marca d'agua.

Agradecimentos

Os autores agradecem ao Prof. Dr. Hélio M. de Oliveira por suas valorosas sugestões ao presente trabalho.

Referências

[1] A. V. Oppenheim and R. W. Schafer, *Discrete-time Signal Processing*, Prentice Hall, Upper Saddle River, New Jersey, 1999.

[2] G. Strang and T. Nguyen, *Wavelets and Filter Banks*, Wellesley Cambridge, USA, 1997.

[3] M. Vetterli and J. Kovacevic , *Wavelets and Subband Coding*, Prentice Hall, Upper Saddle River, New Jersey, 1995.

[4] R. J. McEliece, *Finite Field for Computer Scientists and Engineers*, KAP, Norwell, Massachusetts, 1987.

[5] J. M. Pollard, *The Fast Fourier Transform in a Finite Field*, Math Comput., Vol. 25, No 114, pp. 365-374, Apr. 1971.

[6] G. Caire and R. L. Grossman, *Wavelet Transforms Associated with Finite Cyclic Groups*, IEEE Transaction on Information Theory, Vol 39, No 4, pp. 1157-1166, July 1993.

[7] T. Cooklev, A. Nishihara and M. Sablatash, *Theory of Filter Banks over Finite Fields*, 1994 IEEE Asia-Pacific Conference on Circuits and Systems, pp. 260-265, Taipei, Taiwan, Dec. 1994.

[8] H. M. de Oliveira, T. H. Falk e R. F. G. Távora, *Decomposição de Wavelets sobre Corpos Finitos*, Revista da Sociedade Brasileira de Telecomunicações, Vol 17, No 1, pp. 38-47, 2002.

[9] F. Fekri, S. W. McLaughlin, R. M. Mersereau and R. W. Schafer *Block Error Correcting Codes Using Finite-Field Wavelet Transforms*, IEEE Transactions on Signal Processing, Vol. 54, NO. 3, March 2006.

[10] S. Lin and D. J. Costello, Jr., *Error Control Coding*, 2a. ed., Prentice Hall, 2004.

[11] G. J. da Silva Jr., R. M. Campello Souza e H. M. de Oliveira, *Códigos de Bloco Lineares Baseados em Banco de Filtros e Wavelets Cíclicos Sobre Corpos Finitos*, XXV Simpósio Brasileiro de Telecomunicações - SBrT, Recife - PE, Brazil, setembro 2007 (aceito para apresentação).