Banco de Filtros e Wavelets Cíclicos sobre Corpos de Característica Dois

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

***Resumo*— Este artigo apresenta a teoria dos bancos de filtros e wavelets cíclicos definidos sobre corpos finitos de característica dois. A condição de reconstrução perfeita para bancos de filtros cíclicos e a transformada wavelet cíclica sobre esses corpos são introduzidas. Exemplos e aplicações na área de códigos corretores de erros são apresentados.**

***Palavras-Chave*— Banco de filtros cíclico, wavelets cíclicas, corpo finito, reconstrução perfeita, característica dois.**

***Abstract*— This paper presents the theory of cyclic filter banks and wavelets defined on finite fields with characteristic two. The perfect reconstruction condition for cyclic filter banks and the discrete cyclic wavelet transform over theses fields are introduced. Examples and applications in the field of error control codes are presented.**

***Keywords*— Cyclic filter banks, cyclic wavelets, finite fields, perfect reconstruction, characteristic two.**

I. INTRODUÇÃO

A teoria de sinais e sistemas sobre o corpo dos complexos é bem estabelecida [1]-[3]. Nesse cenário, os sistemas baseados em estruturas cíclicas são de interesse especial em Engenharia. A principal vantagem de tais sistemas é o comprimento finito das seqüências presentes no mesmo, o que simplifica a questão do armazenamento em computadores digitais. Exemplos de tais sistemas incluem os códigos cíclicos [4],[5], os bancos de filtros cíclicos [6],[7] e sistemas baseados na transformada discreta de Fourier [8].

Estruturas sobre corpos finitos tem se tornado atrativas no sentido em que podem ser armazenadas em máquinas digitais, sem os problemas de quantização causados por operações de ponto flutuante. Muitas ferramentas em Engenharia têm surgido para essas estruturas [9]-[13]. Em particular, corpos finitos de característica dois ganham destaque pela simplicidade de adaptação à representação binária usada em computadores digitais.

Existem, na literatura, trabalhos sobre bancos de filtros e wavelets definidos sobre corpos finitos [14],[15]. Embora em alguns desses trabalhos, corpos de característica dois sejam abordados, não há referências a estruturas cíclicas sobre esses corpos. Além disso, o problema da reconstrução perfeita não é abordado, uma questão importante para o estudo de bancos de filtros biortogonais.

Um sistema cíclico requer que suas entradas e saídas, chamadas seqüências cíclicas, apresentem um comprimento finito, aqui denotado por N. Nesse cenário, a operação de deslocamento no tempo é substituída pelo deslocamento cíclico no tempo. De forma análoga ao que ocorre na teoria clássica de sistemas lineares invariantes no tempo (LIT), um sistema cíclico LIT (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.

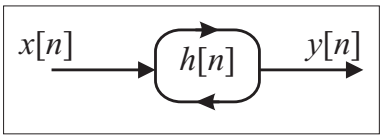

Fig. 1. Representação de um sistema CLIT.

Neste trabalho, $x[n]$ denota uma seqüência cíclica sobre um corpo finito de característica p, isto é, um vetor com N elementos de $GF(p^m)$, o corpo finito (campo de Galois) de ordem p^m. Duas operações básicas envolvendo tais seqüências são a convolução cíclica e a transformada de Fourier de corpo finito.

Definição 1: Se $x[n]$ é a entrada de um sistema CLIT com resposta ao impulso $h[n]$, então sua saída é dada por

$$y[n] = \sum_{r=0}^{N-1} x[r]h[((n-r))_N] = x[n] \circledN h[n], \qquad (1)$$

onde $\circledN$ denota convolução cíclica de comprimento N e $((j))_N$ indica $j(mod\ N)$.

Definição 2: As seqüências $x[n]$ e $X[k]$, $n, k = 0, 1, \ldots, N-1$, onde $x[n] \in GF(q)$ e $X[k] \in GF(q^s)$, formam um par da transformada de Fourier de corpo finito (TFCF), denotado por

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

se

$$X[k] \stackrel{\Delta}{=} \sum_{n=0}^{N-1} x[n]\alpha^{kn}, \qquad (2)$$

e

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

onde α é um elemento de ordem N em $GF(q^s)$ e $q = p^m$.

A transformada de Fourier de corpo finito tem se mostrado uma excelente ferramenta de análise com diversas aplicações [9],[16]. Entretanto, para que esta transformada exista em um corpo de característica p, é necessário que $MDC(p, N) = 1$. Esta é uma das primeiras dificuldades de se definir wavelets cíclicas sobre corpos de característica dois, já que N deve ser par para um banco de filtros com dois canais.

Este artigo está organizado da seguinte forma: Na seção II é apresentada uma nova definição para a transformada Z cíclica inversa, a qual permite analisar vetores de qualquer comprimento em qualquer corpo finito. Na seção III é introduzida a nova teoria de banco de filtros com dois canais sobre corpos de característica dois; um método de projeto para banco de filtros cíclicos definidos sobre esses corpos é apresentado. Na seção IV, a transformada wavelet cíclica é introduzida e uma aplicação em codificação de canal é examinada. As conclusões do trabalho são apresentadas na seção V.

II. A Transformada Z cíclica

A *transformada Z cíclica* (TZC) é definida de modo a evitar o problema de existência que ocorre na TFCF.

Definição 3: Para uma seqüência $x[n]$, $n = 0, 1, \ldots, N-1$, de elementos de $GF(q)$, existe um polinômio $X(z)$, com coeficientes em $GF(q)$, que representa a TZC de $x[n]$, denotado por

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

se

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

e

$$x[n] = -\sum_{z \in GF(q^m)} X(z) z^n, \tag{5}$$

onde $q^m - 1 \geq N$.

Demonstração: Seja $s[n]$ a seqüência de N pontos, $n = 0, 1, \ldots, N-1$, dada por

$$s[n] = -\sum_{z \in GF(q^m)} X(z) z^n. \tag{6}$$

Substituindo $X(z)$ por (4), tem-se

$$s[n] = -\sum_{z \in GF(q^m)} \sum_{l=0}^{N-1} x[l] z^{n-l} \tag{7}$$

ou

$$s[n] = -\sum_{l=0}^{N-1} x[l] \sum_{z \in GF(q^m)} z^{n-l}. \tag{8}$$

O último somatório pode ser expresso por

$$\sum_{z \in GF(q^m)} z^{n-l} = \sum_{r=0}^{q^m-2} \gamma^{r(n-l)} \tag{9}$$

onde γ é um elemento primitivo de $GF(q^m)$. Se $q^m - 1 \geq N$, a expressão pode ser simplificada para

$$\sum_{z \in GF(q^m)} z^{n-l} = (q^m - 1)\delta[n-l]. \tag{10}$$

Levando em (8), o resultado é

$$s[n] = x[n]. \tag{11}$$

■

A TZC está associada com a aritmética polinomial módulo $(z^{-N} - 1)$ e não requer que $MDC(N, p) = 1$ para existir.

Algumas propriedades da TZC estão listadas na Tabela I.

TABELA I
PROPRIEDADES DA TRANSFORMADA Z CÍCLICA

Seqüência	Transformada	Propriedades
$x[n]$	$X(z)$	-
$y[n]$	$Y(z)$	-
$ax[n] + by[n]$	$aX(z) + bY(z)$	Linearidade
$x[((n-d))_N]$	$z^{-d}X(z)(mod\ (z^{-N}-1))$	Deslocamento no tempo
$nx[n]$	$-z\frac{d}{dz}X(z)$	Derivada formal em z
$x[n] \circledN y[n]$	$X(z)Y(z)(mod\ (z^{-N}-1))$	Convolução cíclica

III. Banco de Filtros com Dois Canais sobre Corpos de Característica Dois

A equação principal para banco de filtros é a condição de reconstrução perfeita (RP). Esta condição depende essencialmente da análise do sobreamostrador e do subamostrador cíclico.

Teorema 1: Em um corpo finito $GF(2^m)$, A TZC da saída do sobreamostrador cíclico (Figura 2), $X_e(z)$, é expressa em termos da TZC da entrada, $X(z)$, assumindo-se que a entrada tem período $N/2$, por

$$X_e(z) = \frac{X(z^2)}{1 + z^{-N}}, \tag{12}$$

onde a fração indica divisão polinomial.

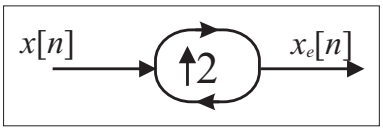

Fig. 2. Representação de um sistema sobreamostrador cíclico.

Demonstração: Se a entrada tem período $N/2$, então sua TZC é dada por

$$X(z) = \sum_{n=0}^{N-1} x[n] z^{-n} = (1 + z^{-N/2}) \sum_{n=0}^{N/2-1} x[n] z^{-n}, \tag{13}$$

com isso,

$$\frac{X(z)}{1 + z^{-N/2}} = \sum_{n=0}^{N/2-1} x[n] z^{-n}, \tag{14}$$

e como

$$X_e(z) = \sum_{n=0}^{N/2-1} x[n] z^{-2n}, \tag{15}$$

o resultado segue. ■

Teorema 2: Em um corpo $GF(2^m)$, A TZC da saída de um subamostrador cíclico, $X_d(z)$, e a TZC da saída do conjunto subamostrador-sobreamostrador cíclico, $X_s(z)$, podem ser expressas em termos da TZC de entrada, $X(z)$ (Figura 3), respectivamente, por

$$X_d(z) = (1 + z^{-N/2}) \left(z^{\frac{1}{2}} X'(z^{\frac{1}{2}}) + X(z^{\frac{1}{2}}) \right) \tag{16}$$

e

$$X_s(z) = zX'(z) + X(z), \tag{17}$$

onde $X'(z) = \frac{d}{dz}X(z)$ é a derivada formal de $X(z)$ [5].

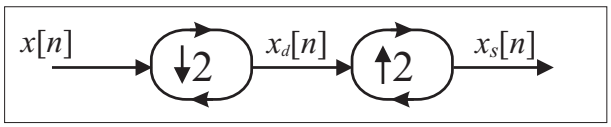

Fig. 3. Representação de um sistema subamostrador cíclico em cascata com um sobreamostrador cíclico.

Demonstração: Em $GF(2^m)$, a seqüência $x_s[n]$ pode ser expressa por

$$x_s[n] = (n+1)x[n] = nx[n] + x[n]. \tag{18}$$

Aplicando a TZC e usando a propriedade da derivada (Tabela I), obtêm-se que

$$X_s(z) = zX'(z) + X(z). \tag{19}$$

Como $X_d(z) = (1 + z^{-N/2})X_s(z^{\frac{1}{2}})$, a prova está completa. ■

Com essas novas relações, é possível estabelecer, pela primeira vez na literatura da área, a condição de reconstrução perfeita para banco de filtros com dois canais sobre corpos de característica dois.

Teorema 3: Em um corpo finito $GF(2^m)$, A condição RP, para banco de filtros com dois canais (Figura 4), é

$$\begin{bmatrix} H_0(z) & H_1(z) \\ H_0'(z) & H_1'(z) \end{bmatrix} \begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} (mod\ (z^{-N}+1)) = \begin{bmatrix} 0 \\ z^{-1} \end{bmatrix}. \tag{20}$$

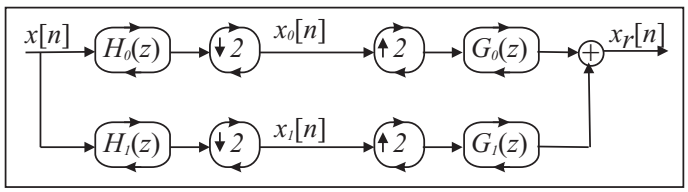

Fig. 4. Representação de um banco de filtros cíclico com dois canais.

Demonstração: Para o banco de filtros da Figura 4, utilizando o Teorema 2, pode-se escrever

$$\begin{aligned} &[z(H_0(z)X(z))' + H_0(z)X(z)]\,G_0(z) + \\ &[z(H_1(z)X(z))' + H_1(z)X(z)]\,G_1(z) = X(z) \end{aligned} \tag{21}$$

ou ainda,

$$\begin{aligned} X(z)\,&[z(G_0(z)H_0'(z) + G_1(z)H_1'(z)) + \\ &H_0(z)G_0(z) + H_1(z)G_1(z)] + \\ zX'(z)&[H_0(z)G_0(z) + H_1(z)G_1(z)] = X(z). \end{aligned} \tag{22}$$

Para que ocorra a reconstrução perfeita, as componentes $X'(z)$ devem ser anuladas. Assim

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 0 \tag{23}$$

e

$$\begin{aligned} &z[G_0(z)H_0'(z) + G_1(z)H_1'(z)] + \\ &H_0(z)G_0(z) + H_1(z)G_1(z) = 1. \end{aligned} \tag{24}$$

Substituindo (23) em (24), tem-se as duas condições RP,

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 0 \tag{25}$$

e

$$G_0(z)H_0'(z) + G_1(z)H_1'(z) = z^{-1}. \tag{26}$$

■

A. Projeto de Banco de Filtros Cíclicos com Dois Canais sobre $GF(2^m)$

Definição 4: O *filtro produto binário* é definido por

$$P_b(z) \triangleq H_0(z)H_1(z)(mod\ (z^{-N}+1)). \tag{27}$$

Por meio do Teorema 3, pode-se escrever que

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = P_b'(z)^{-1} \begin{bmatrix} H_1'(z) & H_1(z) \\ H_0'(z) & H_0(z) \end{bmatrix} \begin{bmatrix} 0 \\ z^{-1} \end{bmatrix}; \tag{28}$$

simplificando o resultado, os filtros de síntese podem ser expressos por

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = z^{-1}P_b'(z)^{-1}(mod\ (z^{-N}+1)) \begin{bmatrix} H_1(z) \\ H_0(z) \end{bmatrix}. \tag{29}$$

Desde que a derivada do filtro produto binário, $P_b'(z)$, seja não nula e que

$$MDC(P_b'(z), z^{-N}+1) = 1, \tag{30}$$

é possível obter os filtros de síntese satisfazendo à condição RP.

Proposição 1: Um método de projeto de banco de filtros cíclicos com dois canais sobre $GF(2^m)$:

- Escolher um filtro $P_b(z)$ satisfazendo (30);
- Fatorar $P_b(z)$ em $H_0(z)H_1(z)$;
- Utilizar

$$G_0(z) = z^{-1}P_b'(z)^{-1}H_1(z)(mod\ (z^{-N}+1)) \tag{31}$$

e

$$G_1(z) = z^{-1}P_b'(z)^{-1}H_0(z)(mod\ (z^{-N}+1)), \tag{32}$$

para encontrar $G_0(z)$ e $G_1(z)$.

Exemplo 1: Considere os seguintes filtros de análise, projetados para $N = 8$ sobre um corpo de característica dois:

$$H_0(z) = 1 + z^{-1}$$

e

$$H_1(z) = 1 + z^{-2} + z^{-3}.$$

O filtro produto binário é dado por

$$P_b(z) = H_0(z)H_1(z)(mod\ (z^{-8}+1)) = 1 + z^{-1} + z^{-2} + z^{-4},$$

e sua derivada,

$$P_b'(z) = z^{-2}.$$

Os filtros de síntese podem ser obtidos pelas expressões (31) e (32). Os resultados são

$$G_0(z) = z^{-1} + z^{-2} + z^{-7}$$

e

$$G_1(z) = 1 + z^{-7}.$$

No domínio do tempo, tem-se

$$h_0[n] = [1\ 1\ 0\ 0\ 0\ 0\ 0\ 0],$$

$$h_1[n] = [1\ 0\ 1\ 1\ 0\ 0\ 0\ 0],$$

$$g_0[n] = [0\ 1\ 1\ 0\ 0\ 0\ 0\ 1]$$

e

$$g_1[n] = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 1].$$

Para uma entrada $x[n] \in GF(2^4)$ dada por

$$x[n] = [\alpha\ \alpha^2\ 0\ 0\ 0\ 0\ 0\ 0],$$

onde $\alpha \in GF(2^4)$. As saídas do banco de análise são

$$x_0[n] = [\alpha\ \alpha^2\ 0\ 0]$$

e

$$x_1[n] = [\alpha\ \alpha\ \alpha^2\ 0].$$

A seqüência de entrada é recuperada na estrutura de síntese do banco de filtros.

Exemplo 2: Considere-se $N = 8$ e o filtro produto binário dado por

$$\begin{aligned} P_b(z) &= 1 + z^{-1} + z^{-3} + z^{-4} + z^{-5} + z^{-6} \\ &= (1 + z^{-1})(1 + z^{-3} + z^{-5}). \end{aligned}$$

Sua derivada formal é

$$P_b'(z) = z^{-2}(1 + z^{-1} + z^{-2})^2,$$

satisfazendo $MDC(P_b'(z), z^{-8} + 1) = 1$ e

$$P_b'(z)P_b'(z)(mod\ (z^{-8} + 1)) = 1,$$

o que significa que $P_b'(z)^{-1}(mod\ (z^{-8} + 1)) = P_b'(z)$. Dessa forma, os filtros podem ser projetados utilizando a Proposição 1, com fatoração escolhida para $P_b(z)$ dada por

$$H_0(z) = 1 + z^{-1},$$

$$H_1(z) = 1 + z^{-3} + z^{-5}.$$

Os filtros de síntese podem ser obtidos pelas expressões (31) e (32). Os resultados são

$$\begin{aligned} G_0(z) &= z^{-1}P_b'(z)^{-1}H_1(z)(mod\ (z^{-8} + 1)) \\ &= z^{-3} + z^{-4} + z^{-5} + z^{-6} + z^{-7} \end{aligned}$$

e

$$\begin{aligned} G_1(z) &= z^{-1}P_b'(z)^{-1}H_0(z)(mod\ (z^{-8} + 1)) \\ &= 1 + z^{-3} + z^{-4} + z^{-5} + z^{-6} + z^{-7}. \end{aligned}$$

IV. A Transformada Wavelet Cíclica sobre Corpos de Característica Dois

As expressões da *transformada wavelet cíclica* (TWC) podem ser obtidas através de banco de filtros cíclicos estruturados em árvore logarítmica, análogo ao caso não cíclico (*discrete wavelet transform* [3]). As equações de análise da TWC são

$$X_0^{(J)}[l] = \sum_{n=0}^{N-1} x[n]h_0^{(J)}[((2^J l - n))_N] \tag{33}$$

e

$$X_1^{(j)}[l] = \sum_{n=0}^{N-1} x[n]h_1^{(j)}[((2^j l - n))_N], \tag{34}$$

onde $j = 1, 2, \ldots, J$, $l = 0, 1, \ldots, (N/2^j) - 1$ e J é o máximo valor de j tal que 2^j divide N. As seqüências $h_0^{(J)}[n]$ and $h_1^{(j)}[n]$ são obtidas através de suas TZC, expressas pelas equações

$$H_0^{(J)}(z) \triangleq H_0(z)^{2^J - 1}(mod\ (z^{-N} + 1)) \tag{35}$$

e

$$H_1^{(j)}(z) \triangleq H_1(z)^{2^{(j-1)}} H_0(z)^{2^{(j-1)} - 1}(mod\ (z^{-N} + 1)) \tag{36}$$

onde

$$h_i^{(j)}[n] \overset{Z}{\longleftrightarrow} H_i^{(j)}(z). \tag{37}$$

A equação de síntese da TWC é

$$\begin{aligned} x[n] = &\sum_{j=1}^{J} \sum_{l=0}^{N/2^j - 1} X_1^{(j)}[l] g_1^{(j)}[((n - 2^j k))_N] \\ &+ \sum_{l=0}^{N/2^J - 1} X_0^{(J)}[l] g_0^{(J)}[((n - 2^J k))_N], \end{aligned} \tag{38}$$

onde as seqüências $g_0^{(J)}[n]$ e $g_1^{(j)}[n]$ são obtidas através de suas TZC, expressas pelas equações

$$G_0^{(J)}(z) \triangleq G_0(z)^{2^j - 1}(mod\ (z^{-N} + 1)) \tag{39}$$

e

$$G_1^{(j)}(z) \triangleq G_1(z)^{2^{(j-1)}} G_0(z)^{2^{(j-1)} - 1}(mod\ (z^{-N} + 1)), \tag{40}$$

onde

$$g_i^{(j)}[n] \overset{Z}{\longleftrightarrow} G_i^{(j)}(z). \tag{41}$$

A. Representação Reduzida

Na computação dos coeficientes da TWC, é necessário a convolução cíclica de seqüências com períodos (comprimentos) diferentes. Para simplificar a computação, a seguinte relação pode ser utilizada.

Definição 5: A *representação reduzida* da seqüência $h[n]$ é

$$h_R[n] \triangleq \sum_{m=0}^{M-1} h[((n - mR))_N], \tag{42}$$

uma seqüência cíclica de $R = N/M$ pontos ou uma seqüência cíclica de N pontos com período R.

Lema 1: Se $x[n]$ tem período $R = N/M$, então

$$x[n] \textcircled{N} h[n] = x[n] \textcircled{R} h_R[n] \quad (43)$$

Demonstração: Se $x[n]$ tem período $R = N/M$, então

$$x[n] \textcircled{N} h[n] = \sum_{j=0}^{N-1} x[(j)_R] h[((n-j))_N] = \sum_{j=0}^{R-1} \sum_{m=0}^{M-1} x[j] h[((n-j-mR))_N], \quad (44)$$

ou

$$x[n] \textcircled{N} h[n] = \sum_{j=0}^{R-1} x[j] \sum_{m=0}^{M-1} h[((n-j-mR))_N], \quad (45)$$

e assim

$$x[n] \textcircled{N} y[n] = \sum_{j=0}^{R-1} x[j] h_R[((n-j))_R] = x[n] \textcircled{R} h_R[n]. \quad (46)$$

■

Exemplo 3: Considere o banco de filtros projetado no exemplo 1 para fazer uma estrutura de análise TWC com dois estágios. A seqüência a ser analisada é

$$x[n] = [1\ 1\ 0\ 0\ 0\ 1\ 0\ 1].$$

No primeiro estágio, é feita a convolução cíclica de comprimento oito seguida de subamostragem, resultando em

$$x_0^{(1)}[n] = (x[n] \textcircled{8} h_0[n]) \downarrow 2 = [0\ 1\ 0\ 1]$$

e

$$x_1^{(1)}[n] = (x[n] \textcircled{8} h_1[n]) \downarrow 2 = [0\ 0\ 1\ 0],$$

ambas seqüências cíclicas de quatro pontos. No segundo estágio, a convolução cíclica de oito pontos pode ser feita utilizando-se o Lema 1 por meio de

$$x_0^{(2)}[n] = (x_0^{(1)}[n] \textcircled{4} h_{04}[n]) \downarrow 2$$

e

$$x_1^{(2)}[n] = (x_0^{(1)}[n] \textcircled{4} h_{14}[n]) \downarrow 2,$$

onde, por (42),

$$h_{04}[n] = [1\ 1\ 0\ 0]$$

e

$$h_{14}[n] = [1\ 0\ 1\ 1].$$

Assim, os resultados são

$$x_0^{(2)}[n] = [1\ 1]$$

e

$$x_1^{(2)}[n] = [0\ 0].$$

B. Aplicações em Códigos Corretores de Erros

Banco de filtros cíclicos e wavelets podem ser utilizados para análise, geração, codificação e decodificação de códigos de bloco. Cada filtro cíclico constitui, per si, um código cíclico. Existem publicações utilizando banco de filtros e wavelets sobre corpos finitos para aplicações em códigos corretores de erros considerando corpos $GF(p^m)$, com p ímpar [14],[17]. A inclusão de corpos de característica dois amplia, de modo significativo, o escopo dessas aplicações e consolida, definitivamente, uma nova área de estudo conectando códigos corretores de erros à teoria de sinais e sistemas.

Um método simples de gerar códigos de bloco é utilizar a estrutura de síntese da TWC, como mostra o exemplo na Figura 5. O símbolo de "terra" significa um sinal de entrada

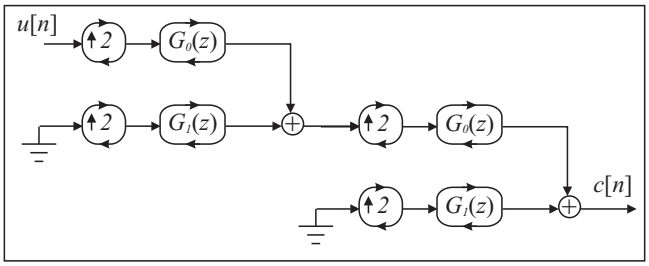

Fig. 5. Um exemplo de síntese da TWC com dois estágios, estrutura para gerar códigos de bloco.

nulo. Para cada mensagem $u[n]$, o codificador gera uma palavra código $c[n]$ com comprimento quatro vezes maior. A estrutura de análise da TWC pode ser utilizada para detecção de erros.

Exemplo 4: Usando a estrutura da Figura 5 projetada para $N = 8$, pode-se escrever, utilizando a equação de síntese da TWC (38),

$$c[n] = u[0] g_0^{(2)}[n] + u[1] g_0^{(2)}[(n-4)_8],$$

onde a TZC de $g_0^{(2)}[n]$ é obtida por (39). Por meio do banco de filtros do exemplo 1, tem-se

$$G_0^{(2)}(z) = G_0(z)^3 (mod\ (z^{-8}+1)) = 1 + z^{-1} + z^{-4} + z^{-6} + z^{-7}.$$

Assim

$$g_0^{(2)}[n] = [1\ 1\ 0\ 0\ 1\ 0\ 1\ 1],$$

e

$$\begin{bmatrix} c[0] \\ c[1] \end{bmatrix} = [u[0]\ u[1]] \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix},$$

o que define um código de bloco linear binário $C(8,2,5)$. Existe um código de Goppa com esses parâmetros [5]. A estrutura da Figura 6 é utilizada para detecção de erros. As seqüências $\tilde{c}[n]$ e $\tilde{u}[n]$ são as palavras código e mensagem possivelmente corrompidas, respectivamente. As seqüências $s^{(1)}[n]$ e $s^{(2)}[n]$ são síndromes utilizadas para detecção de erros [4].

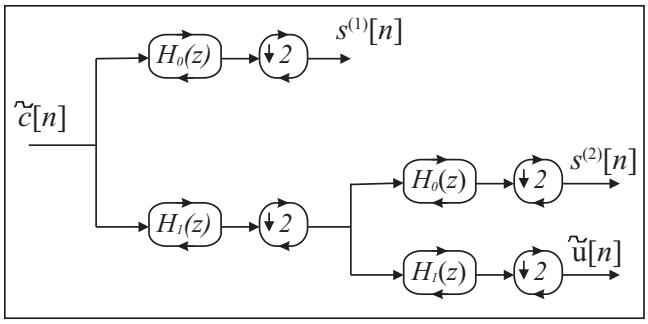

Fig. 6. Um exemplo de análise da TWC com dois estágios, estrutura para detectar erros.

V. Conclusões

Esse trabalho apresenta novas ferramentas para processamento de sinais em corpos finitos. Inicialmente, a transformada Z cíclica (TZC) foi introduzida, possibilitando a análise de seqüências cíclicas de comprimento par, definidas sobre corpos de característica dois. A TZC foi então utilizada para construir a (nova) teoria de banco de filtros e wavelets cíclicos sobre esses corpos. Uma nova condição de reconstrução perfeita foi obtida e um novo método de projeto de banco de filtros cíclicos biortogonais foi proposto. Um exemplo de aplicação das novas ferramentas, na área de codificação de canal, foi apresentado. A possibilidade de utilização de corpos de característica dois expande significativamente o campo de aplicações das técnicas de processamento de sinais sobre estruturas algébricas finitas. Os códigos Reed-Solomon (utilizados em CDs) [4],[5], o atual padrão de cifragem de dados, o cripto-sistema de chave secreta Rijndael [18] e a grande maioria dos sistemas de comunicação digital utiliza corpos de característica dois e podem ser agora analisados com essas ferramentas.

Agradecimentos

Os autores agradecem ao Prof. Dr. Hélio M. de Oliveira por suas valorosas sugestões ao presente trabalho. O primeiro autor agradece ao CNPq.

Referências

[1] A. V. Oppenheim, A. S. Willsky, and S. H. Nawab, *Signals and Systems*, 2nd ed. Prentice Hall, 1996.

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

[3] M. Vetterli and J. Kovacevic, *Wavelets and Subband Coding*. Prentice Hall, 1995.

[4] S. Lin and D. J. Costello, *Error Control Coding*, 2nd ed. Prentice Hall, 2004.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1988.

[6] P. Vaidyanathan and A. Kirac, "Theory of cyclic filter banks," in *ICASSP '97: Proceedings of the 1997 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '97)-Volume 3*. Washington, DC, USA: IEEE Computer Society, 1997, p. 2449.

[7] G. J. da Silva Jr. and R. M. C. de Souza, "Banco de filtros e wavelets para sistemas cíclicos sobre corpos finitos," *XXV Simpósio Brasileiro de Telecomunicações - SBrT 2007*, Setembro 2007, em CD.

[8] A. V. Oppenheim, R. W. Schafer, and J. R. Buck, *Discrete-Time Signal Processing*, 2nd ed. Prentice Hall, 1999.

[9] J. M. Pollard, "The fast Fourier transform in a finite field," *Math Comput.*, vol. 25, no. 114, pp. 365–374, Apr 1971.

[10] G. Caire, R. L. Grossman, and H. V. Poor, "Wavelet transforms associated with finite cyclic groups," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1157–1166, July 1993.

[11] T. Cooklev, A. Nishihara, and M. Sablatash, "Theory of filter banks over finite fields," *IEEE Asia-Pacific Conference on Circuits and Systems*, pp. 260–265, Dec 1994.

[12] R. M. C. de Souza, H. M. de Oliveira, and A. N. Kauffman, "Trigonometry in finite fields and a new Hartley transform," *Proc. of the IEEE Int. Symp. on Info. Theory*, p. 293, Aug. 1998.

[13] M. M. C. de Souza, H. M. de Oliveira, R. M. C. de Souza, and M. M. Vasconcelos, *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2004, vol. 3124, ch. The Discrete Cosine Transform over Prime Finite Fields, pp. 482–487.

[14] 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, pp. 991–1004, March 2006.

[15] F. Fekri, R. M. Mersereau, and R. W. Schafer, "Theory of paraunitary filter banks over fields of characteristic two," *IEEE Transactions on Information Theory*, vol. 48, no. 11, pp. 2964–2979, November 2002.

[16] H. M. de Oliveira, J. P. C. L. Miranda, and R. M. C. de Souza, "Spread-spectrum based on finite field Fourier transforms," *Proc. of the ICSECIT (Int. Conf. on System Engineering, Comm. and. Info. Technol.)*, pp. 1–5, 2001.

[17] G. J. da Silva Jr., R. M. C. de Souza, and 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 2007*, Setembro 2007, em CD.

[18] J. Daemen and V. Rijndael, *The Design of Rijndael*. Springer, 2002.