DECOMPOSIÇÃO DE WAVELETS SOBRE CORPOS FINITOS

H.M. de Oliveira, T.H. Falk, R.F.G. Távora

Resumo - Este trabalho introduz fundamentos de wavelets sobre campos de Galois. Wavelets ortogonais padrões sobre Corpos Finitos, as *FF*-Wavelets (do inglês *Finite Field Wavelets*), são derivadas, incluindo a *FF*-Haar e a *FF*-Daubechies. *FF*-wavelets não–ortogonais, como as *B*-Splines sobre GF(*p*) também são investigadas. Alguns exemplos da Análise Multiresolucional (AMR) sobre corpos finitos e condições matriciais sobre os coeficientes do filtro suavizador da AMR para garantir a nulidade de momentos de uma wavelet são mostrados. Um novo algoritmo rápido para o cálculo de *FF*-Wavelets, baseado na decomposição bifásica, é introduzido. As Transformadas de Pacotes Wavelets sobre corpos finitos são também consideradas. Uma aplicação demonstra o potencial uso das *FF*-wavelets em projetos de esquemas de multiplex por seqüência multinível de espalhamento espectral (Mux por divisão em códigos).

Palavras-Chave: Wavelets sobre Corpos Finitos (*FF*-Wavelets), *FF*-Haar, *FF*-Daubechies, Seqüências de espalhamento espectral, CDM.

Abstract - This paper introduces some foundations of wavelets over Galois fields. Standard orthogonal finite-field wavelets (*FF*-Wavelets) including *FF*-Haar and *FF*-Daubechies are derived. Non-orthogonal *FF*-wavelets such as *B*-splines over GF(*p*) are also considered. A few examples of multiresolution analysis over finite fields as well as conditions for the coefficients of the smoothing filter to achieve vanishing moments are presented. A new fast algorithm to compute *FF*-wavelets, based on a two-phase decomposition is introduced. Wavelet packed transforms over finite fields are also considered. An application of *FF*-wavelets to design multiplex schemes with spread-spectrum sequences is presented.

Keywords: Finite field Wavelets, *FF*-Haar, *FF*-Daubechies, Spread-spectrum sequences, CDM.

1. INTRODUÇÃO

A primeira menção sobre wavelets aparece na tese de doutorado de Alfred Haar em 1909, onde se fala em análise escalonada. No início da década de 80, Jean P. Morlet (Elf Acquitaine) e Alex Grossmann (Université de Marseille) introduziram o conceito de wavelets [1,2] (Morlet recebeu o prêmio *Reginald Fessenden Award* 1997).

Desde a sua introdução, as transformadas de Wavelet (Contínuas e Discretas) revelaram-se como uma poderosa ferramenta em Ciência e Engenharia. Na análise de sinais e sistemas, elas têm demonstrado superioridade em relação à análise de Fourier clássica em diversas situações [3, 4, 5, 6].

As wavelets se desenvolveram nos campos da Matemática, Engenharia, na Física Quântica e hoje a teoria wavelet têm se proliferado em uma larga gama de aplicações: visão computacional e humana [7, 8], geologia sísmica, radar/sonar, computação gráfica [4], predição de terremotos e maremotos, turbulência, fractais, bancos de filtros, distinção celular (células normais *vs* patológicas), modelos para trato auditivo, processamento de imagens (e.g. reconstrução de imagens em alta resolução, compressão de imagens [9] — vide padrão JPEG 2000 http://www.jpeg2000.org), descontaminação de sinais (*denoising*) [10, 11], detecção de rupturas e bordas, tons musicais, neurofisiologia, detecção de curtos eventos patológicos (e.g. crises epilépticas) e análise de sinais biomédicos (eletrocardiogramas [12], mamografias [13], eletroencefalogramas etc.) [14, 15], espalhamento em banda larga, modelagem de sistemas lineares, Séries temporais [16, 17], modelagem geométrica, reconhecimento de alvos, Óptica [18], análise de transitório e falhas em linhas de potência, Metalurgia (rugosidade de superfícies), visualização volumétrica, previsão de comportamento de mercados financeiros, solução de equações diferenciais ordinárias e parciais, não sendo esta lista nem de longe exaustiva.

A Transformada de Wavelet consiste essencialmente numa decomposição do sinal em um conjunto de funções base, todas derivadas de uma única wavelet protótipo (wavelet-mãe) por sucessivos escalonamentos (dilatações e compressões) e translações (deslocamentos no tempo) [19, 20]. As transformadas de wavelet discretas sofrem dilatações e translações discretas (inteiras), sendo o caso diádico o mais utilizado.

Um dos métodos de construção de wavelets ortogonais, desenvolvido por Mallat e Meyer, é a Análise de Multiresolução (AMR) [21]. Este método permite construir a maioria das wavelets ortogonais. A AMR está intimamente relacionada com o algoritmo piramidal usado na decomposição e reconstrução de wavelets [22].

Adota-se o símbolo := para denotar "igual por definição". Como usual, Wavelets são denotadas por $\psi(.)$ e as funções de escala por $\phi(.)$. Suas respectivas transformadas de Fourier são $\Psi(w)$ e $\Phi(w)$, respectivamente. Z denota o conjunto dos inteiros.

Desde a sua introdução em 1989 a representação AMR vem se consolidando como um método de processamento de sinais, provendo uma ênfase local nas características importantes de um sinal [17]. Este processo é baseado em um par de filtros com coeficientes $\{g_k\}$ e $\{h_k\}$, associados às funções $\psi(.)$ e $\phi(.)$, respectivamente.

A equação $\phi(t) = \sqrt{2} \sum_{n \in Z} h_n \phi(2t - n)$, que é conhecida como a *equação de dilatação* ou de *refinamento*, constitui a principal relação da multiresolução [7, 19]. Definindo o

Os autores são do CODEC – Grupo de Pesquisas em Comunicações, Departamento de Eletrônica e Sistemas – CTG – Universidade Federal de Pernambuco, Caixa Postal 7800, 50711-970, Recife–PE, Brasil. E-mails: hmo@npd.ufpe.br, tiagofalk@go.com, r_tavora@hotmail.com.

Editores responsáveis: Antonio Sérgio B. Sombra, Ricardo M. C. de Souza e M. Gerken. Data de recebimento: 31/Dez/2001; data de revisão: 15/Mar/2002, data de aceitação: 8/Abr/2002.

espectro do filtro suavizador $\{h_k\}$ de acordo com $H(w) := \frac{1}{\sqrt{2}} \sum_{k \in Z} h_k e^{-jwk}$, as seguintes equações centrais (no domínio da freqüência) para a AMR podem ser demonstradas [17, 21]:

Relação de dupla-escala para a função de escala e para a wavelet.

$$\Phi(w) = H\left(\frac{w}{2}\right)\Phi\left(\frac{w}{2}\right)$$

$$\Psi(w) = G\left(\frac{w}{2}\right)\Phi\left(\frac{w}{2}\right),$$

onde $\Phi(w)$ é a transformada de Fourier da função de escala e $G(w) := \frac{1}{\sqrt{2}}\left(\sum_{k \in Z} g_k e^{-jwk}\right)$ é a função de transferência do filtro de detalhes. ❑

A comodidade básica da infra-estrutura da informação escalonável do futuro será certamente a informação representada na forma de alfabetos discretos. Tal representação da informação precisa ser transmitida, armazenada e manipulada sem erros e quase sempre com altos níveis de segurança. O processamento de dados discretos está no núcleo da infra-estrutura dos novos sistemas. O processamento de alfabetos finitos é um componente chave de códigos para controle de erro, códigos para segurança, acesso multi-usuário, codificação conjunta fonte-canal e muito mais.

A análise de Fourier também pode ser mapeada para uma análise sobre corpos finitos. Tal mapeamento ficou conhecido como Transformada de Fourier sobre Corpos Finitos (TFCF), introduzida em 1971 por Pollard [23]. Durante décadas, esta foi a única transformada definida sobre corpos finitos. Outra transformada sobre Corpos Finitos foi recentemente introduzida, a Transformada de Hartley sobre Corpos Finitos [24]. Esta transformada é definida sobre um corpo finito denominado de inteiros gaussianos GI(p^s), o qual é isomorfo a GF(p^{2s}) [24]. Novas transformadas numéricas sobre corpos finitos foram recentemente propostas as quais são atrativas para muitas aplicações devido a sua baixa complexidade computacional [25]. Isto permite inclusive a implementação de transformadas "livre de multiplicação" (vide *Rev. Soc. Bras. Telecom*., este número). Essas transformadas têm um papel importante em problemas relacionados a estruturas de corpo finito e com aritméticas de inteiros [26].

O potencial das transformadas discretas clássicas (DFT, DCT, DWT etc.) já encontra-se firmemente estabelecido. Embora discretizadas no domínio da variável, as amplitudes assumidas pelos coeficientes pertencem a um corpo infinito. Elas podem portanto ser encaradas como "Transformadas analógicas" (algo análogo, como por exemplo, ao sistema de Pulsos Modulados em Amplitude, PAM). Já as transformadas definidas sobre corpos finitos são discretas e têm coeficientes que assumem valores num alfabeto finito, de modo que podem ser interpretadas como "Transformadas Digitais". Da mesma forma que os sistemas digitais têm se mostrado atrativos comparados aos analógicos, as transformadas digitais podem constituir uma abordagem potente. É natural então pensar em uma possível análise de wavelets sobre Corpos Finitos (TWCF, *Transformada de Wavelet sobre Corpos Finitos*) que apresente vantagens em relação à análise de Fourier clássica sobre Corpos Finitos, em algumas situações. Este tema fascinante tem sido relativamente pouco explorado. O principal resultado foi estabelecido por Caire e colaboradores [27]. Em 1995, alguns desenvolvimentos foram apresentados durante o ISIT'95, Simpósio Internacional de Teoria da Informação do IEEE [28, 29]. Porém o tema ainda desperta muito interesse [30] e expectativas [31]. Fica óbvio que dúvidas a respeito de um tema tão pouco explorado surjam, como: Existem TWCF de interesse? Que propriedades serão mantidas? Existem aplicações para a TWCF e quais seus potenciais? Este trabalho visa responder algumas destas perguntas.

No caso de wavelets "convencionais", a transformada pode ser calculada com base nos filtros suavizador e de detalhes, sem explicitar a forma de onda da wavelet e da função de escala. Bancos de filtros em corpos finitos foram bem abordados no artigo [32], tratando inclusive de wavelets. Uma das questões interessantes consiste em definir as "formas de onda" das wavelets em corpos finitos, baseadas em propriedades de escalonamento e translação.

Seja p um primo tal que $p \equiv \pm 1 \pmod 8$, condição necessária para que 2 seja um resíduo quadrático do corpo finito GF(p) [33]. A wavelet-mãe será definida como um vetor de comprimento N:

$$\underline{\psi}_{1,0} = (\psi_{1,0}(0), \psi_{1,0}(1), \psi_{1,0}(2), ..., \psi_{1,0}(N-1)),$$

onde cada componente de ψ pertence ao corpo de extensão GF(p^s) onde s é um inteiro, $s \geq 1$.

Inicialmente serão tratadas wavelets sobre Corpos Finitos primos. Seja N um inteiro e $D(N)$ o conjunto dos divisores de N. O escalonamento sobre corpos finitos não pode ser tomado como um número real, $a \in \Re$, como usualmente se faz, mas sim como um inteiro divisor do comprimento (N).

Propõe-se então as seguintes operações:

1) Escalonamento ($\underline{\psi}_{j,0}$):

$\psi_{j,0}(i) = \psi_{1,0}(ji)$, $\forall\, j \in D(N/2) := \{ j \text{ tal que } j \mid N/2\}$.

2) Translações ($\underline{\psi}_{j,k}$):

$$\psi_{j,k}(i) = \psi_{j,0}\left(i + \frac{Nk \pmod N}{j}\right), \forall\, k = 0,1,...N\text{-}1.$$

As funções wavelet:

$\underline{\psi}_{j,k} = (\psi_{j,k}(0), \psi_{j,k}(1), \psi_{j,k}(2), ..., \psi_{j,k}(N-1))$, são versões escalonadas e/ou transladadas da wavelet-mãe $\underline{\psi}_{1,0}$.

Propriedade 1. $\sum_{i=0}^{N-1} \psi_{j,k}(i) \equiv 0 \pmod p, \forall\, j,k.$ ❑

Definição 1. Seja $\underline{v} = (v_0, v_1, ..., v_{N-1})$ um sinal-vetor de comprimento N sobre um Campo de Galois GF(p), de característica $p \neq 2$. $\underline{\psi}_{j,k}$ são as funções wavelet sobre GF(p^s), $s \geq 1$. A transformada de Wavelet sobre Corpos Finitos (TWCF) do sinal $\underline{v}$ será definida como: $TWCF(j,k) := \sum_{i=0}^{N-1} v_i \psi_{j,k}(i) \pmod p$, o que é denotado por $TWCF(j,k) = \langle \underline{v}, \underline{\psi}_{j,k} \rangle$. ❑

2. DECOMPOSIÇÃO DE HAAR SOBRE CORPOS FINITOS

Na análise de sinais constante por partes, as bases de Haar podem ser mais adequadas [7, 34]. A wavelet de Haar é definida pela relação:

$$\psi^{(H)}(t) := \begin{cases} -\frac{1}{\sqrt{2}} & -1 < t \le 0 \\ \frac{1}{\sqrt{2}} & 0 < t \le 1 \\ 0 & \text{caso contrário} \end{cases} . \ \square$$

Nesta seção apresenta-se uma construção generalizada das bases ortogonais de Haar. Assume-se que $p \equiv \pm 1$ (*mod* 8) e que N é uma potência de dois.

Definição 2. A wavelet-mãe de Haar em GF(p) (*FF*-Haar) é definida de acordo com:

$$\psi_{1,0}(i) = \begin{cases} 1 & se\ 0 \le \frac{i}{N} < \frac{1}{2} \\ p-1 & se\ \frac{1}{2} \le \frac{i}{N} < 1 \\ 0 & caso\ contrário. \end{cases}$$

$$\text{i.e., } \psi_{1,0}(i) = \begin{cases} (p-1)^{\left\lfloor \frac{i \,(mod\ N)}{N/2} \right\rfloor} & se\ 0 \le \frac{i}{N} < 1 \\ 0 & caso\ contrário \end{cases} . \ \square$$

Exemplo 1. Considerando a *FF*-Haar, N=8, sobre GF(p). Os possíveis fatores de escalonamento $j \in D(4)=\{1,2,4\}$. Portanto:

j =1 $\underline{\psi}_{1,0} = (1,\ 1,\ 1,\ 1,\ p-1,\ p-1,\ p-1,\ p-1)$

j =2 $\underline{\psi}_{2,0} = (1,\ 1,\ p-1,\ p-1,\ 0,\ 0,\ 0,\ 0)$

j =4 $\underline{\psi}_{4,0} = (1,\ p-1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0)$.

Translações de tais seqüências são permitidas, e.g., $\underline{\psi}_{2,1} = (0,\ 0,\ 0,\ 0,\ 1,\ 1,\ p-1,\ p-1)$.

Propriedade 2. Dada uma versão escalonada da wavelet-mãe $\underline{\psi}_{j,0}$, o número de diferentes translações possíveis da wavelet $\underline{\psi}_{j,k}$ é numericamente igual a j.

Prova. As versões transladadas diferentes e possíveis são obtidas para k=0 até k=j-1. ❑

2.1 NORMALIZAÇÃO DE ENERGIA

Para garantir uma transformada isométrica, deve-se introduzir um fator de normalização. Como N é uma potência de dois e j pertence a $D(N/2)$, N/j também será uma potência de dois.

Supondo $p \equiv \pm 1$ (*mod* 8), então $\sqrt{\frac{N}{j}} \in$ GF(p). Pode-se, em conseqüência, definir a transformada normalizada por:

$$TWCF(j,k) = \frac{1}{\sqrt{\left(\frac{N}{j}\right)}\ (mod\ p)} \sum_{i=0}^{N-1} v_i \psi_{j,k}(i)\ (mod\ p) .$$

O número total de wavelets distintas será $\sum_{j \in D(N/2)} j$. Considerando um subconjunto $S \subseteq D(N/2)$ tal que $\sum_{j \in S \subseteq D(N/2)} j = N$-1, quando N=2^m, então $D(N/2)$={1,2, 4, 8,...2^{m-1}} e $\sum_{j \in D(N/2)} j = \sum_{j=1}^{m-1} 2^j = N-1$.

Todos os valores de $j \in D(N/2)$ serão usados como versões escalonadas da wavelet-mãe. Essas formas de onda, em conjunto com o sinal[1] (1 1 1 1 ... 1) geram N sinais ortogonais entre si, sobre GF(p) e de comprimento N, i.e., foram geradas as bases ortogonais de Haar. Apesar do escalonamento j=0 não ter significado, por convenção e conveniência adota-se $\underline{\psi}_{0,0}$ para denotar a seqüência "toda um".

Exemplo 2. À esquerda tem-se a *FF*-Haar sobre GF(7) e a direita tem-se a Wavelet *FF*-Haar normalizada sobre GF(7).

(1 1 1 1 1 1 1 1)	(1 1 1 1 1 1 1 1)
(1 1 1 1 6 6 6 6)	(6 6 6 6 1 1 1 1)
(1 1 6 6 0 0 0 0)	(4 4 3 3 0 0 0 0)
(0 0 0 0 1 1 6 6)	(0 0 0 0 4 4 3 3)
(1 6 0 0 0 0 0 0)	(5 2 0 0 0 0 0 0)
(0 0 1 6 0 0 0 0)	(0 0 5 2 0 0 0 0)
(0 0 0 0 1 6 0 0)	(0 0 0 0 5 2 0 0)
(0 0 0 0 0 0 1 6)	(0 0 0 0 0 0 5 2).

Fica claro que :

$$\sum_{i=0}^{N-1} \psi_{j,k}(i) \equiv 0\ (mod\ p),$$

$$\sum_{i=0}^{N-1} \psi^2_{j,k}(i) \equiv 1\ (mod\ p) \quad \text{e}$$

$$\sum_{i=0}^{N-1} \psi_{j,k}(i)\psi_{j',k'}(i) \equiv 0\ (mod\ p), \forall j \ne j' \text{ or } k \ne k'.$$

Se N não for uma potência de dois, wavelets não-ortogonais são geradas, e.g., N=24 sobre GF(7). Neste exemplo, $D(12)=\{1, 2, 3, 4, 6, 12\}$.

 # de versões transladadas

j=0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 **1**

j=1
1 1 1 1 1 1 1 1 1 1 1 1 6 6 6 6 6 6 6 6 6 6 6 6 **1**

j=4
1 1 1 6 6 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 **4**

j=6
1 1 6 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 **6**

j=12
1 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 **12**

24

Estas wavelets não são mais ortogonais, por exemplo, $\langle \underline{\psi}(2,1), \underline{\psi}(6,0) \rangle \ne 0\ (mod\ p)$. As wavelets duais podem ser facilmente derivadas.

2.2 DECOMPOSIÇÃO PIRAMIDAL DE HAAR

Uma das ferramentas mais poderosas proveniente da teoria de wavelets é a decomposição de dados via algoritmo de filtragem piramidal [4, 20, 35].

Exemplo 3. Considerando um filtro de dois elementos (1, 1), a decomposição *FF*-Haar sobre GF(7) resulta em filtros passa-baixa e passa-alta com coeficientes, respectivamente:

[1] Este sinal desempenha o papel da função de escala para a *FF*-Haar. Note que o valor médio não é nulo.

h= [5 5] h^* = [5 5]
g= [2 5] g^* = [5 2].

O processo de filtragem é exatamente idêntico ao caso convencional, exceto pelo fato que as operações são tomadas *mod p*. ❑

3. *B*-SPLINES SOBRE CORPOS FINITOS

Splines são famílias de curvas obtidas por combinações lineares de bases polinomiais. Abaixo um exemplo de wavelet gerada a partir de *B*-splines [7, 19]. A seguinte relação geral de auto-recursão pode ser demonstrada:

Proposição 1. (Relação geral de dupla escala para *B*-splines) [19]:

$$N_m(t) = \sum_{n=0}^{m} 2^{-m+1} \binom{m}{n} N_m(2t-n). \quad ❑$$

Desta forma, segue-se que:

$$N_1(t) = N_1(2t) + N_1(2t-1)$$

$$N_2(t) = \frac{1}{2}N_1(2t) + N_1(2t-1) + \frac{1}{2}N_1(2t-2)$$

$$N_3(t) = \frac{1}{4}N_3(2t) + \frac{3}{4}N_3(2t-1) + \frac{3}{2}N_3(2t-2) + \frac{1}{4}N_3(2t-3)\cdots$$

(e assim por diante).

Uma *B*-spline pode ser portanto utilizada como função de escala $\phi(t) = N_m(t)$, obedecendo a uma equação de escala dupla explicitada pela relação de auto-recursão dada acima. Os coeficientes são exatamente os coeficientes h_m não nulos da AMR *B*-spline. Uma wavelet simples, não-ortogonal, como a *n*-cardinal *B*-Spline, $n<p+1$, pode também ser derivada sobre corpos finitos, GF(p), onde $p \equiv \pm 1$ (*mod* 8).

Um filtro de (n+2) elementos é dado por:

$$(2^n)^{-1}\binom{n+1}{k} \ (mod\ p),\ k=0,1,2,...,n+1,$$

permanecendo a relação com a definição clássica da *B*-Spline. O fator de normalização é dado por: $\sqrt{2}.(mod\ p).2^{-1}$. Como exemplos de *B*-Splines sobre corpos finitos é possível citar a *B*-Spline quadrática sobre GF(7) (2-cardinal *B*-spline) com coeficientes dos filtros dada por [3 2 2 3] ou [4 5 5 4].

4. CONDIÇÕES PARA ANULAR MOMENTOS DE UMA WAVELET

No caso contínuo, Wavelets $\psi(t)$ com uma maior regularidade podem ser obtidas impondo a nulidade para os primeiros momentos de $\psi(.)$, o que significa transições mais suaves na passagem de um subespaço ao próximo subespaço da AMR. Para wavelets de uma mesma família, um dos parâmetros importantes é o número de momentos nulos. Como versar estas condições para wavelets em um corpo finito? Esta seção trata de Wavelets contínuas, estabelecendo resultados que sejam mais simples de "transferir" para um corpo finito. Lembrando a relação de dupla-escala $\Psi(w) = \frac{1}{\sqrt{2}} G\left(\frac{w}{2}\right)\Phi\left(\frac{w}{2}\right)$, a anulação dos momentos de $\psi(t)$ tem implicações sobre o filtro $G(.)$.

Por exemplo,

$$\Psi^{(1)}(w)|_{w=0} = 0 \Rightarrow$$

$$2\sqrt{2}\Psi^{(1)}(w) = G\left(\frac{w}{2}\right)\Phi^{(1)}\left(\frac{w}{2}\right) + G^{(1)}\left(\frac{w}{2}\right)\Phi\left(\frac{w}{2}\right) = 0 \text{ em } w=0.$$

Assim,

$$\Psi^{(1)}(w)|_{w=0} = 0 \Rightarrow$$

$$G(0)\Phi^{(1)}(0) + G^{(1)}(0)\Phi(0) = 0 \quad \therefore G(0)=0.$$

No caso geral, anular os N primeiros momentos de $\psi(t)$, m=0,1,...,*N-1* implica em

$$\Psi^{(m)}(w)|_{w=0} = 0 \Rightarrow G^{(m)}(0)=0 \quad m=0,1,2,...,N-1.$$

(Nota: não confundir com o N, comprimento de ψ para a TWCF).

Pelas condições QMF [21, 35] isto implica em $H^{(m)}(\pi)=0$ para m=0,1,...,*N-1*.

Quando os N primeiros momentos são nulos, então:

$H(\pi)=0$ e $G(0)=0$;
$H'(\pi)=0$ e $G'(0)=0$;
$H''(\pi)=0$ e $G''(0)=0$;
⋮
$H^{(N-1)}(\pi)=0$ e $G^{(N-1)}(0)=0$.

Um caso de particular interesse é quando o filtro $H(.)$ possui apenas L elementos não nulos, i.e.,

$$H(w) = \left(\sum_{k=0}^{L-1} h_k e^{-jwk}\right).$$

As condições sobre a nulidade dos primeiros N momentos podem ser expressas em termos dos coeficientes do filtro H:

i) $H(\pi)=0 \Leftrightarrow H(0)=\sqrt{2}$ (normalização)

$$\sum_{k=0}^{L-1}(-1)^k h_k = 0 \Leftrightarrow \sum_{k=0}^{L-1} h_k = \sqrt{2},$$

ii) $H^{(1)}(\pi)=0$ (Nulidade do primeiro momento)

$$\sum_{k=0}^{L-1}(-1)^k k h_k = 0,$$

iii) $H^{(2)}(\pi)=0$ (Nulidade do segundo momento)

$$\sum_{k=0}^{L-1}(-1)^k k(k+1) h_k = 0,$$

iv) $H^{(3)}(\pi)=0$ (Nulidade do terceiro momento)

$$\sum_{k=0}^{L-1}(-1)^k k(k+1)(k+2) h_k = 0,$$

e assim por diante.

Condições equivalentes, expressas em termos do filtro G, são:

i) $G(0)=0$ (normalização)

$$\sum_{k=0}^{L-1} g_k = 0,$$

ii) $G^{(1)}(0)=0$ (Nulidade do primeiro momento)

$$\sum_{k=0}^{L-1} k g_k = 0,$$

iii) $G^{(2)}(0)=0$ (Nulidade do segundo momento)

$$\sum_{k=0}^{L-1} k(k+1) g_k = 0,$$

iv) $G^{(3)}(0)=0$ (Nulidade do terceiro momento)

$$\sum_{k=0}^{L-1} k(k+1)(k+2) g_k = 0,$$

e assim por diante.

As condições de nulidade dos primeiros N momentos de um filtro $H(w)$ com apenas L coeficientes (L par) não nulos podem ser escritas de forma matricial:

$$\begin{vmatrix} 1 & -2 & 3 & -4 & \cdots & (L-1) \\ -1.2 & 2.3 & -3.4 & 4.5 & \cdots & -(L-1)L \\ 1.2.3 & -2.3.4 & 3.4.5 & -4.5.6 & \cdots & (L-1)L(L+1) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1.2.3....(N-1) & \cdots & \cdots & \cdots & \cdots & (L-1)L(L+1)...(L+N-3) \end{vmatrix} \begin{vmatrix} h_1 \\ h_2 \\ h_3 \\ \vdots \\ h_{L-1} \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{vmatrix}$$

A relação matricial acima pode ser simplificada obtendo-se uma nova matriz de nulidade de momentos:

$$\begin{vmatrix} 1 & -2 & 3 & -4 & 5 & \cdots & (L-1) \\ -1 & 3 & -6 & 10 & -15 & \cdots & -(L-1)L/2 \\ 1 & -4 & 10 & -20 & 35 & \cdots & (L-1)L(L+1)/6 \\ -1 & 5 & -15 & 35 & -70 & \cdots & -(L-1)L(L+1)(L+2)/24 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & \cdots & \cdots & \cdots & \cdots & \dfrac{(L-1)L(L+1)...(L+N-3)}{(N-1)!} \end{vmatrix} \begin{vmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \\ \vdots \\ h_{L-1} \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{vmatrix}$$

A relação de normalização introduzida, conduzindo a uma matriz $N\times L$ (completa) de nulidade de momentos, $[\Xi] := (\Xi_{i,j})$:

$$[X].[h]=[0],$$

ou seja,

$$\begin{vmatrix} 1 & -1 & 1 & -1 & 1 & \cdots & -1 \\ 0 & 1 & -2 & 3 & -4 & \cdots & (L-1) \\ 0 & -1 & 3 & -6 & 10 & \cdots & -(L-1)L/2 \\ 0 & 1 & -4 & 10 & -20 & \cdots & (L-1)L(L+1)/6 \\ 0 & -1 & 5 & -15 & 35 & \cdots & -(L-1)L(L+1)(L+2)/24 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & -1 & \pm N & & & \cdots & \dfrac{(L-1)L(L+1)...(L+N-3)}{(N-1)!} \end{vmatrix} \begin{vmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ \vdots \\ h_{L-1} \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix}$$

Os elementos da matriz de nulidade de momentos podem ser gerados de forma recursiva:

4.1 REGRA DE GERAÇÃO RECURSIVA

Regra 1. $\Xi_{1j} = (-1)^{(i+j)}$

Regra 2. $\Xi_{i1} = \delta_{i,1}$

Regra 3. $\Xi_{i+1\,j} = -\left(\Xi_{ij} + \Xi_{i+1\,j-1}\right)$, $1\le i<N$ e $1<j\le L$ ❑

Isto implica, por exemplo, que:

$$\Xi_{2j} = (-1)^j.(j-1),$$

$$\Xi_{i2} = (-1)^i.1.$$

Como exemplo, um filtro de Daubechies com 4 coeficientes não nulos para gerar a wavelet D_4 (denotada como $\text{ø}_{2N}^{(Dau)}$ ou db2), com N=2 momentos nulos, é expresso por: $H(w) = \left(\sum_{k=0}^{3} h_k e^{-jwk}\right)$,

com $[\,h_0\;\; h_1\;\; h_2\;\; h_3\,] = \left[\dfrac{1+\sqrt{3}}{4\sqrt{2}}\;\; \dfrac{3+\sqrt{3}}{4\sqrt{2}}\;\; \dfrac{3-\sqrt{3}}{4\sqrt{2}}\;\; \dfrac{1-\sqrt{3}}{4\sqrt{2}}\right]$.

Da matriz simplificada, obtém-se

$$\begin{vmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -2 & 3 \end{vmatrix} \begin{vmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \end{vmatrix}.$$

$$\text{❶}\quad h_0 - h_1 + h_2 - h_3 = 0,$$

$$\text{❷}\quad h_1 - 2h_2 + 3h_3 = 0.$$

Duas equações complementares (no caso geral, N equações) provém da condição de normalização e das condições de ortogonalidade.

$$h_0^2 + h_1^2 + h_2^2 + h_3^2 = 1,$$

$$h_0 h_2 + h_1 h_3 = 0.$$

Para anular os momentos de uma wavelet definida sobre um corpo finito, propõe-se usar a relação envolvendo a matriz completa de nulidade de momentos. Define-se a matriz considerando os elementos $\Xi_{i,j}$ como elementos do corpo finito GF(p).

5. *FF*-DAUBECHIES WAVELETS SOBRE CORPOS FINITOS PRIMOS

A wavelet ortogonal mais importante da teoria de wavelets é a wavelet de Daubechies [17, 36]. (I. Daubechies recebeu o IEEE *Info. Theory Soc. Jubilee Medal*). Deseja-se encontrar uma decomposição wavelet ortogonal similar sobre GF(p). São empregadas wavelets diádicas derivadas de uma wavelet-mãe

$$\psi(.):\ \psi_{j,k}(i) := (\sqrt{2})^j \psi(2^j i - k).$$

A Análise Multiresolucional é gerada pela função de escalonamento $\phi(.)$ tal que: $\phi_{j,k}(i) \equiv (2)^{j/2}\phi(2^j i - k)$, de modo que: $\phi_{1,k}(i) \equiv \sqrt{2}.\phi(2i-k)\ (mod\ p)$.

Uma multiresolução ortogonal sobre GF(p) é gerada por $\phi(.)$ que preserva a:

Dilatação ou Equação de Refinamento.

$$\phi(i) \equiv \sqrt{2}\ (mod\ p).\sum_{k=0}^{N-1} h_k \phi(2i-k)\ (mod\ p).$$

A *FF*-wavelet deve satisfazer:

$$\psi(i) \equiv \sqrt{2}\ (mod\ p).\sum_{k=0}^{N-1} g_k \phi(2i-k)\ (mod\ p).$$

Os filtros h e g são Filtros Espelhados em Quadratura (QMF, do inglês *Quadrature Mirror Filters*) de comprimento $N=2^n$ e a multiresolução é realizada em n passos.

Requerimento dos Filtros para a Multiresolução.

$$\sum_{k=0}^{N-1} h_k \equiv \sqrt{2}\ (mod\ p), \qquad \sum_{k=0}^{N-1} g_k \equiv 0\ (mod\ p).$$

$$g_k \equiv (-1)^k h_{N-1-k}\ (mod\ p),$$

$$\sum_{k=0}^{N-1} h_k h_{k+2m} \equiv 0\ (mod\ p),\ m\neq 0.\ ❑$$

Exemplo 4. Considerando uma *FF*-Daubechies de comprimento N=4 (db2) sobre GF(97). A análise multiresolucional pode ser realizada com o auxílio dos seguintes filtros:

Suavidade (passa - baixa) h = [92, 47, 12, 57]
Detalhes (passa - alta) g = [57, 85, 47, 5].

Os filtros são tais que:

$$\forall k=0,..,3\ \ g_k \equiv (-1)^k h_{3-k}\ \ (mod\ 97).$$

Ainda mais:

$$\sum_{k=0}^{3} h_k \equiv 14\ (mod\ 97),\quad \sum_{k=0}^{3} g_k \equiv 0\ (mod\ 97)$$

$$\sum_{k=0}^{3} h_k h_{k+2} \equiv 0\ (mod\ 97).\ ❑$$

A nulidade dos dois momentos desta wavelet pode ser verificada através da congruência:

$$\begin{vmatrix} 1 & 96 & 1 & 96 \\ 0 & 1 & 95 & 3 \end{vmatrix} \cdot \begin{vmatrix} 92 \\ 47 \\ 12 \\ 57 \end{vmatrix} \equiv \begin{vmatrix} 0 \\ 0 \end{vmatrix} \ (mod\ 97).$$

A tabela abaixo especifica os coeficientes dos filtros passa-baixa para uma AMR via db2 sobre GF(p), para p=23, 47,71, 73 e 97. Na tabela 2, apresentam-se os coeficientes para as wavelets de Daubechies db3 sobre os corpos finitos p=31, 41, 79, 281, 359, 431 e 449.

Corpo	Coeficientes de db2 sobre GF(p)			
GF(p)	$h_0\equiv$	$h_1\equiv$	$h_2\equiv$	$h_3\equiv$
GF(23)	21	14	11	18
GF(47)	29	19	45	8
GF(71)	66	69	11	8
GF(73)	58	50	72	7
GF(97)	97	47	12	57

Tabela 1. Coeficientes de db2 sobre alguns corpos finitos.

Corpo	Coeficientes de db3 sobre GF(p)					
GF(p)	$h_0\equiv$	$h_1\equiv$	$h_2\equiv$	$h_3\equiv$	$h_4\equiv$	$h_5\equiv$
GF(31)	20	3	15	7	22	25
GF(41)	25	36	10	23	35	11
GF(79)	43	53	24	26	56	44
GF(281)	91	150	60	190	64	156
GF(359)	119	270	286	69	124	190
GF(431)	270	336	215	36	283	396
GF(449)	82	315	186	386	166	182

Tabela 2. Coeficientes de db3 sobre alguns corpos finitos.

6. UM ALGORITMO RÁPIDO PARA A TWCF BASEADO NA TFCF

A transformada de wavelet cíclica de comprimento N [27] pode ser calculada com auxílio dos operadores G e H definidos por[2]:

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

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

Sejam **c** e **d** as seqüências dadas por $c_k := (Hx)_k$ e $d_k := (Gx)_k$. Este somatório, que eqüivale a uma correlação seguida de uma subamostragem, pode ser calculado através da TFCF de comprimento N pelo teorema da convolução. 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. Entretanto, este cálculo pode ser efetuado de forma mais eficiente.

Calculando a TFCF do vetor **c** usando um elemento ζ do corpo finito, com ordem $N/2$ ($ord(\zeta) = N/2$), tem-se:

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

$$= \sum_{j=0}^{N-1} x(j) \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik}.$$

O somatório interno no segundo membro da equação acima pode ser calculado de forma separada nos casos em que j é par ou ímpar, introduzindo as seqüências $\tilde{h}^0$ e $\tilde{h}^1$ definidas por:

$$\tilde{h}^0 = \{h(0) \quad h(-2) \quad h(-4) \quad \cdots \quad h(2)\}$$

$$\tilde{h}^1 = \{h(1) \quad h(-1) \quad h(-3) \quad \cdots \quad h(3)\},$$

em que

$$\tilde{h}^0(k) := h(-2k \ (mod\ N))$$

e $\tilde{h}^1(k) := h(1-2k \ (mod\ N))$, k=0,1,...,N/2-1.

Logo para j par:

$$S_j := \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik} = \sum_{k=0}^{N/2-1} \tilde{h}^0(k)\zeta^{ik}\zeta^{\frac{ij}{2}} = \tilde{H}^0(i)\zeta^{\frac{ij}{2}}$$

em que $\tilde{H}^0(i) := TFCF(\tilde{h}^0(k))$, pois $ord(\zeta) = N/2$.

Para j ímpar,

$$S_j = \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik} = \sum_{k=0}^{N/2-1} \tilde{h}^1(k)\zeta^{ik}\zeta^{\frac{i(j-1)}{2}} = \tilde{H}^1(i)\zeta^{\frac{i(j-1)}{2}},$$

em que $\tilde{H}^1(i) := TFCF(\tilde{h}^1(k))$.

Mas,

$$\sum_{j=0}^{N-1} x(j) \sum_{k=0}^{N/2-1} h(j-2k)\zeta^{ik} = \sum_{j=0}^{N/2-1} x(2j)S_{2j} + \sum_{j=0}^{N/2-1} x(2j+1)S_{2j+1}$$

Substituindo esta relação na expressão de S_j, tem-se:

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

Definindo as expressões x^0 e x^1 dadas por:

$$x^0 := \{x(0) \quad x(-2) \quad x(-4) \quad \cdots \quad x(2)\},$$

$$x^1 := \{x(1) \quad x(-1) \quad x(-3) \quad \cdots \quad x(3)\}$$

tem-se:

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

Sejam X^0 e X^1 as TFCF de x^0 e x^1, respectivamente. Logo a expressão de $C(i)$ pode ser escrita da forma:

$$C(i) = X^0(i)\tilde{H}^0(i) + X^1(i)\tilde{H}^1(i)$$

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

O cálculo da seqüência $\{d_k\}$ é realizado de modo análogo. Sejam

$$\tilde{g}^0 := \{g(0) \quad g(-2) \quad g(-4) \quad \cdots \quad g(2)\},$$

$$\tilde{g}^1 := \{g(1) \quad g(-1) \quad g(-3) \quad \cdots \quad g(3)\}.$$

Definindo

$$\tilde{G}^0(i) := TFCF(\tilde{g}^0(k)),$$

$$\tilde{G}^1(i) := TFCF(\tilde{g}^1(k)),\ .$$

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

tem-se:

$$D(i) = X^0(i)\tilde{G}^0(i) + X^1(i)\tilde{G}^1(i)\,.$$

[2] Não confundir com os filtros G e H da AMR.

São necessárias agora duas TFCF diretas e duas TFCF inversas de comprimento $N/2$. O número de multiplicações no domínio da freqüência é $2N$.

Pode-se observar que:

$$\widetilde{H}^0(i) = \widetilde{H}^0(-i),\ \widetilde{H}^1(i) = \widetilde{H}^1(-i),$$
$$\widetilde{G}^0(i) = \widetilde{G}^0(-i) \text{ e } \widetilde{G}^1(i) = \widetilde{G}^1(-i).$$

Logo da relação entre as funções $\widetilde{H}^0(i)$, $\widetilde{H}^1(i)$, $\widetilde{G}^0(i)$, $\widetilde{G}^1(i)$ tem-se:

$$\widetilde{H}^0(i) = \widetilde{G}^1(i),$$
$$\widetilde{H}^1(i) = -\widetilde{G}^0(i).$$

Isto resulta em:

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

Observando que as expressões de $C(i)$ e $D(i)$ possuem a mesma estrutura de uma multiplicação complexa, elas podem ser calculadas por [26, p.73]

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

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

Uma alternativa para reduzir a complexidade do cálculo da transformada é o uso de filtros com poucos coeficientes não nulos. 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 $O(N\log_2(N))$ operações necessárias para um algoritmo usando a TFCF.

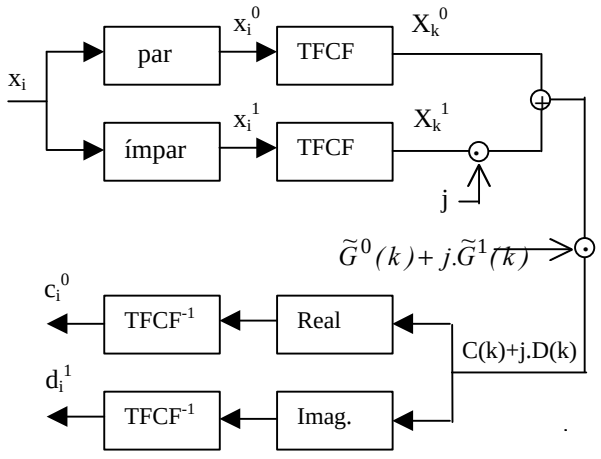

Figura 1. Esquema do cálculo da TWCF pela decomposição bifásica.

7. A TRANSFORMADA DE PACOTES WAVELET EM CORPOS FINITOS

Uma generalização da DWT foi proposta por Coifman [37], chamada de Transformada de Pacotes Wavelet (TPW). Nela, a decomposição é feita aplicando recursivamente os operadores H e G, sobre o resultado de cada filtragem. No caso particular da DWT, os filtros H e G são aplicados apenas sobre a seqüência resultante da filtragem passa-baixa. O número de combinações de bases possível para a TPW é proporcional a N^2, onde N é o comprimento da transformada. Esta flexibilidade de escolha da melhor base pode ser usada, por exemplo, na compressão de imagens.

No caso da transformada de wavelet sobre um corpo finito, são utilizadas recursivamente os operadores G^j e H^j, onde j é a escala, sobre o resultado da filtragem na escala j-1. A reconstrução é feita através dos operadores adjuntos $(G^j)^*$ e $(H^j)^*$. Desta forma, pode-se fazer a decomposição do espaço linear em subespaços:

$$W_j^n = W_{j+1}^{2n} \oplus W_{j+1}^{2n+1}$$

onde a notação $\oplus$ indica a soma direta e:

$$W_{j+1}^{2n} = H^j(W_j^n)$$
$$W_{j+1}^{2n+1} = G^j(W_j^n),$$

o que constitui uma generalização da decomposição em espaços V e W [25], em que V é um espaço vetorial.

Para cada j=1,2,...,n, define-se o subespaço W_j como o complemento ortogonal de V_j tal que

$$V_{j-1} = W_j \oplus V_j.$$

Logo $V_0 = W_0^0$, $V_1 = W_1^0$, $W_1 = W_1^1$ e assim por diante.

O resultado é uma árvore binária em que cada nó representa um subespaço, cujas funções são divididas por um banco de filtros de dois canais, como pode ser visto na figura 2. As funções resultantes geram subespaços filhos ortogonalmente complementares ao subespaço pai.

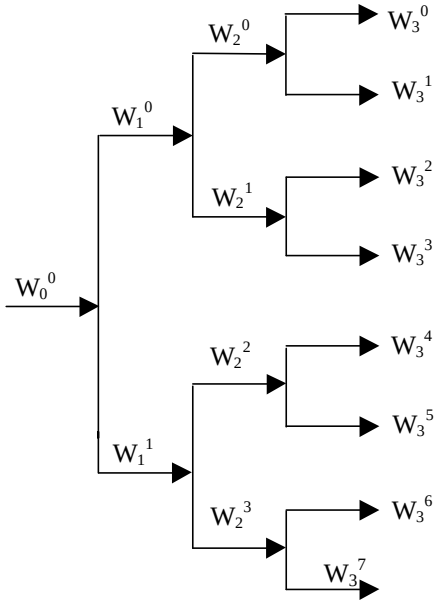

Figura 2. Decomposição em subespaços usando a Transformada de Pacotes Wavelet.

8. APLICAÇÃO: PROJETO DE SEQÜÊNCIAS DE ESPALHAMENTO ESPECTRAL

Multiplexação digital costuma se referir a TDM (do inglês, *Time Division Multiplex*), podendo também ser obtida por CDM (do inglês, *Coding Division Multiplex*), que tem sido largamente utilizado após a padronização IS-95 do sistema CDMA (do inglês, *Code Division Multiple Access*) para telefones celulares [38]. CDMA tem se tornado um esquema de acesso múltiplo para comunicações móveis bastante popular na atualidade. Nesta seção introduziremos uma nova classe de esquemas CDM/CDMA baseado em transformadas de wavelet sobre corpos finitos.

As portadoras wavelet digitais têm a mesma duração T de um símbolo de entrada a ser modulado, tendo então N *chips* por símbolo de dados. O intervalo de cada wavelet-símbolo é de T/N. Tem-se, em conseqüência disto, um fator expansão da largura de banda, N, quando são multiplexados N canais. Este é o mesmo resultado de multiplexações FDM (do inglês, *Frequency Division Multiplex*) e TDM.

Dois exemplos simples e ilustrativos serão apresentados a seguir, considerando um projeto de seqüências ortogonais de espalhamento espectral de comprimento N=8. A Wavelets *FF*-Haar sobre GF(p) pode ser usada para derivar as seqüências. Outras *FF*-wavelets podem também ser usadas, definidas sobre outros corpos (e.g. vide Exemplo 6).

Exemplo 5. Seqüências de espalhamento espectral utilizando wavelets *FF*-Haar sobre GF(7).

Wavelets Ortogonais (e.g. Exemplo 2) podem ser usadas como as seqüências de espalhamento espectral. Cada usuário tem uma seqüência que corresponderá a uma versão escalonada/transladada de uma mesma wavelet-mãe. Um esquema deste sistema pode ser visto na figura 3.

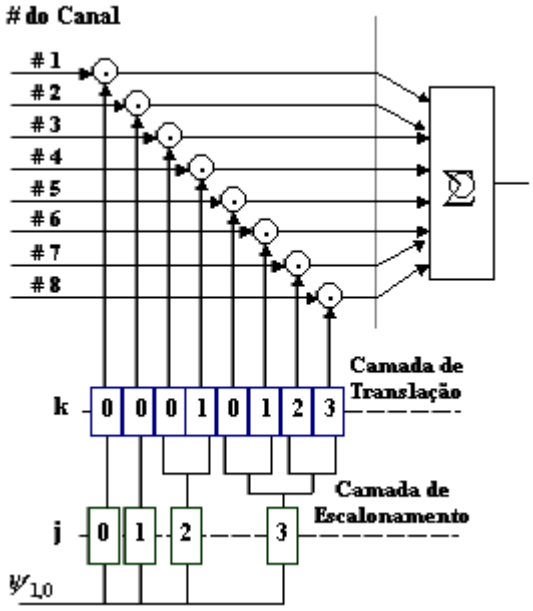

Figura 3. Sistema Multiplex utilizando wavelets *FF*- Haar.

O operador $\sum$ denota a adição vetorial convencional com componentes tomados modulo p. A multiplicação indicada por $\odot$ denota uma multiplicação "*componente a componente*", reduzida módulo p. A duração do símbolo de informação na entrada é N vezes maior que a de um símbolo GF(p) da seqüência de espalhamento. Suponha que, por exemplo, num determinado intervalo de tempo, o dado a ser transmitido pelo usuário do canal #3 seja 2, sendo $2 \in$ GF(7). A seqüência de espalhamento espectral deste canal é

$$\underline{\psi}_{2,0} = (4\,4\,3\,3\,0\,0\,0\,0),$$

o sinal espalhado será então:

$$(2\,2\,2\,2\,2\,2\,2\,2) \otimes (4\,4\,3\,3\,0\,0\,0\,0) \equiv (1\,1\,6\,6\,0\,0\,0\,0) \ (mod\ 7)$$

Por simplicidade isto é denotado por:

$$2^{(8)} \otimes 4^{(2)}\,3^{(2)}\,0^{(4)} \equiv 1^{(2)}\,6^{(2)}\,0^{(4)} \ (mod\ 7).$$

Suponha, num certo intervalo de tempo, que os usuários dos canais 1 ao 8 estejam transmitindo os seguintes dados: $(3\,0\,2\,1\,6\,5\,5\,4)^T$. As seqüências de espalhamento correspondentes (assinatura codificada do usuário) são, respectivamente

$$(\underline{\psi}_{0,0}\ \underline{\psi}_{1,0}\ \underline{\psi}_{2,0}\ \underline{\psi}_{2,1}\ \underline{\psi}_{4,0}\ \underline{\psi}_{4,1}\ \underline{\psi}_{4,2}\ \underline{\psi}_{4,3}).$$

A seqüência CDM será então:

$$CDMed \equiv 3^{(8)} \oplus 0^{(8)} \oplus 1^{(2)}6^{(2)}0^{(4)} \oplus 0^{(4)}4^{(2)}3^{(2)}$$
$$\oplus\, 2^{(1)}5^{(1)}0^{(6)} \oplus 0^{(2)}4^{(1)}3^{(1)}0^{(4)} \oplus 0^{(4)}4^{(1)}3^{(1)}0^{(2)} \oplus 0^{(6)}6^{(1)}1^{(1)},$$

ou seja, $CDM_{ed} \equiv (6\,2\,6\,5\,4\,3\,5\,0)$ $(mod\ 7) := \underline{r}$. Fica claro que este sinal nem é TDM nem FDM.

Os sistemas de multiplexação e de acesso múltiplo derivados de Wavelets sobre Corpos Finitos podem ser enquadradas no escopo da técnica denominada de GDMA (do inglês, *Galois Field Multiple Access*), recentemente introduzida [39].

Como as Wavelets *FF*-Haar são ortogonais, dados de cada usuário podem ser facilmente recuperados com um simples produto interno sobre GF(p). Como exemplo, considere a recepção dos sinais enviados pelos usuários dos canais # 3 e # 8.

$$Canal\ \#3 < \underline{r}, \underline{\psi}_{2,0} > \equiv 2 \ (mod\ 7),$$

$$Canal\ \#8 < \underline{r}, \underline{\psi}_{4,3} > \equiv 4 \ (mod\ 7).$$

O sistema GDM baseado na transformada de Hartley de corpo finito tem que garantir um sincronismo perfeito entre as portadoras casoidais usadas nos multiplexadores e nos demultiplexadores [40, 41]. TWCF ortogonais podem ser usadas como seqüências de espalhamento espectral, sendo implementadas em novos sistemas GDM, resultando em um controle de sincronismo mais eficiente. Isto ocorre devido ao fato de que as seqüências de cada usuário são versões de uma mesma wavelet-mãe. Estas seqüências podem ser geradas com uma mesma freqüência de "relógio", realizando sucessivos escalonamentos e translações. Uma outra idéia atrativa é a aplicação da multiresolução para implementar a (de)multiplexação.

Exemplo 6. Denote a seqüência de entrada do multiplex por $s = \{s_o, s_1, s_2, s_3, s_4, s_5, s_6, s_7\}$, em que cada símbolo proveniente de um usuário distinto é um elemento do corpo finito. A saída do multiplexador é dada pela soma

$$M = s_0\phi_{0,0} + s_1\psi_{0,0} + s_2\psi_{1,0} + s_3\psi_{1,1} + s_4\psi_{2,0} + s_5\psi_{2,1} + s_6\psi_{2,2} + s_7\psi_{2,3}.$$

Este esquema eqüivale ao cálculo da TWCF inversa as seqüências, portanto a demultiplexação eqüivale ao cálculo da TWCF direta.

Seja N=8 sobre o corpo GI(11), com os filtros gerados a partir de $\{\widetilde{G}^0\}=\{3\ \ 0\ \ 0\ \ 0\}$ e $\{\widetilde{G}^1\}=\{5\ \ 10\ \ 10\ \ 10\}$, utilizando $\zeta = j$ (i.e., $\zeta^2 \equiv -1$) no cálculo da TFCF.

A TWCF pode ser representada por

$$\{c_{0,0},\ d_{0,0},\ d_{1,0},\ d_{1,1},\ d_{2,0},\ d_{2,1},\ d_{2,2},\ d_{2,3}\}.$$

As portadoras wavelet são calculadas a seguir:

$$\phi_{0,0} = TWCF^1(\{1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\}) = \{5\ 8\ 9\ 8\ 8\ 8\ 9\ 8\}$$

$$\psi_{0,0} = TWCF^1(\{0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\}) = \{3\ 10\ 3\ 10\ 5\ 10\ 3\ 10\}$$

$$\psi_{1,0} = TWCF^1(\{0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\}) = \{5\ 5\ 10\ 5\ 5\ 5\ 9\ 5\}$$

$$\psi_{1,1} = TWCF^1(\{0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\}) = \{5\ 5\ 9\ 5\ 5\ 5\ 10\ 5\}$$

$$\psi_{2,0} = TWCF^1(\{0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\}) = \{9\ 6\ 9\ 7\ 9\ 7\ 9\ 7\}$$

$$\psi_{2,1} = TWCF^1(\{0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\}) = \{9\ 7\ 9\ 6\ 9\ 7\ 9\ 7\}$$

$$\psi_{2,2} = TWCF^1(\{0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\}) = \{9\ 7\ 9\ 7\ 9\ 6\ 9\ 7\}$$

$$\psi_{2,3} = TWCF^1(\{0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\}) = \{9\ 7\ 9\ 7\ 9\ 7\ 9\ 6\}.$$

Considerando uma seqüência de entrada particular, por exemplo, $s = \{1, 2, 3, 4, 5, 6, 7, 8\}$, a saída do multiplexador será então

$$\begin{aligned} M &= s_0\phi_{0,0} + s_1\psi_{0,0} + s_2\psi_{1,0} + s_3\psi_{1,1} + s_4\psi_{2,0} + \\ &\quad s_5\psi_{2,1} + s_6\psi_{2,2} + s_7\psi_{2,3} \\ &= \{5\ \ 9\ \ 7\ \ 8\ \ 1\ \ 7\ \ 8\ \ 6\}. \end{aligned}$$

Como as seqüências das portadoras wavelet são ortogonais, os símbolos de entrada podem ser recuperados através do produto interno sobre GI(11).

Outra vantagem deste esquema para aplicações CDM/CDMA é a facilidade de implementação em moduladores multinível. No entanto este esquema apresenta baixa imunidade a erros e eficiência depende da aplicação de códigos corretores de erro, que por sua vez, também utilizam a teoria de corpos finitos [26,30].

9. CONCLUSÕES

O processamento de sinais em corpos finitos vem se revelando uma ferramenta cada vez mais atrativa na manipulação da informação. Este trabalho apresenta técnicas que utilizam estruturas em corpos finitos, mostrando potenciais aplicações. A Transformada de wavelet de corpo finito (TWCF) é apresentada, explicitando as funções wavelets em corpo finito. Apresentam-se condições matriciais sobre os coeficientes do filtro suavizador de uma AMR para garantir a nulidade de momentos de uma wavelet. Estes resultados são facilmente adaptados para a TWCF. Um novo algoritmo rápido para o cálculo da TWCF, baseado em uma decomposição bifásica, é introduzido. As Transformadas de Pacotes Wavelets (TPWs) sobre corpos finitos são também consideradas. *FF*-Wavelets podem ser usadas como uma poderosa ferramenta em projetos de seqüência de espalhamento espectral multinível. Os usuários têm diferentes categorias de espalhamento, dependendo do fator de escalonamento. Novos esquemas de multiplexação digital baseados em tais seqüências também foram introduzidos, se encaixando em esquemas de multiplex por divisão em códigos CDM Multinível. Essa abordagem explora as propriedades da ortogonalidade das seqüências não-binárias síncronas, definidas sobre corpos finitos. Tais seqüências (esquemas) podem ser promissoras para canais com alta relação sinal-ruído.

AGRADECIMENTOS

Os autores agradecem ao Prof. R.M. Campello de Souza por valiosas sugestões para melhorar a apresentação deste trabalho. A Renato J.S. Cintra, pelo apoio na geração das tabelas 1 e 2.

REFERÊNCIAS

[1] A. Grossmann e J. Morlet, Decomposition of Hardy Functions into Square Integrable Wavelets of Constant Shape, *SIAM J. Math. Anal.*, Vol. 15, pp.723-736, 1984.

[2] P. Goupillaud, A. Grossman and J. Morlet, Cycle-octave and related transforms in seismic Signal Analysis, *Geoexploration*, vol.23,pp.85-102, 1984/85.

[3] Y. Meyer, S. Jafar e O. Rioul, L´Analyse par Ondelettes, *Pour la Science*, n.119, pp.28-37, Sept., 1987.

[4] L-M. Reissel, Multiresolution and Wavelets, in: Wavelets and their Applications in Computer Graphics, *SIGGRAPH*, A. Fournier Ed., 1994.

[5] A. Bruce, D. Donoho, M-Y. Gao, Wavelet Analysis, *IEEE Spectrum*, October, 1996, pp. 26-35.

[6] R. Polikar, *The Engineer's Ultimate Guide to Wavelet Analysis*,http://www.public.iaste.edu/~rpolikar/WAVELETS/WTtutorial.html

[7] *Wavelets and their Applications in Computer Graphics,* Alain Fournier Ed., Siggraph´94, Course Notes, 1995. Disponível em ftp.cs.ucb.ca/pub/local/bobl/wvlt

[8] E.J. Stollnitz, T.D. DeRose, D.H. Salesin, Wavelets for Computer Graphics: A Primer, Part 1. *IEEE Computer Graphics and Applications*, May, 1995.

[9] A. Manduca, Compressing Images with Wavelets/Subband Coding, *IEEE Engineering in Medicine and Biology*, vol.14, n.5, Sept./Oct., pp.639-646.

[10] D.L. Donoho, Wavelet Shrinkage and WVD: A 10-minute Tours, *Progress in Wavelet Applications*, Y. Meyer, S. Roques eds., Editions Frontieres, 1993.

[11] C. Taswell, The What, How, and Why of Wavelet Shrinkage Denoising, *Computing in Science & Engineering*, May/June, pp.12-19, 2000.

[12] B. Reddy, P. Elko, D. Christenson e G. Rowlandson, Detection of p-waves in resting ECG: A Preliminary Study, *Proc. of Computers in Cardiology Conf.*, IEEE Computer Soc., CA, pp.87-90, 1992.

[13] A. Laine, J. Fan e W. Yang, Wavelets for Contrast Enhancement of Digital Mammography, *IEEE Engineering in Medicine and Biology*, vol.14, n.5, Sept./Oct., pp.536-550.

[14] M. Unser, A. Aldroubi, A Review of Wavelets in Biomedical Applications, *Proc. of the IEEE*, April, pp. 626-638, 1996.

[15] A. Akay, Wavelet Applications in Medicine, *IEEE Spectrum*, May, 1977, pp. 50-56.

[16] P.A. Morettin, Ondaletas e seus Usos em Estatística. Short Course delivered at the *Seventh Time Series and Econometrics School*, Canela, RS, Brazil, 6-8 August 1997.

[17] D.B. Percival e A.T. Walden, *Wavelet Methods for Time Series Analysis*, Cambridge Press, (594p.), 2000.

[18] M.M.S. Lira, H.M. de Oliveira, R.M. Campello de Souza, Elliptic-Cylinder Wavelets: A Family of Mathieu Wavelets, in preparation.

[19] C.K. Chui, *An Introduction to Wavelets*, San Diego: Academic Press, 1992.

[20] J.M. Gomes, L. Velho e S. Goldenstein, *Wavelets: Teoria, Software e Aplicações*, IMPA, Inst. Mat. Pura e Aplicada, 1997.

[21] S. Mallat, A Theory for Multiresolution Signal Decomposition: The Wavelet Representation, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.11, n.7, July, 1989, pp.674-693.

[22] P.J. Burt e E.H. Adelson, The Laplacian Pyramid as a Compact Image Code, *IEEE Trans. On Comm.,* Vol. 31, April, pp.532-540, 1983.

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

[24] R.M. Campello de Souza, H.M. de Oliveira, A.N. Kauffman e A.J.A. Paschoal, "Trigonometry in Finite Fields and a new Hartley Transform", *IEEE Int. Symp. on Info. Theory*, ISIT, MIT Cambridge, MA, THB4: Finite Fields and Appl., p. 293, 1998.

[25] D. Silva, R. M. Campello de Souza, H. M. de Oliveira, L.B.E. Palma, M.M.C. de Souza, A Transformada Numérica de Hartley e Grupos de Inteiros Gaussianos, *Rev. Da Soc. Bras. de Telecomunicações*, neste número.

[26] R.E. Blahut, Fast Algorithm for Digital Signal Processing. Addisson-Wesley, 1985.

[27] G. Caire, R. Grossman, H.V. Poor, Wavelet Transforms Associated with Finite Cyclic Groups, *IEEE Trans. Info. Theory*, vol.39,pp.1157-1166, July, 1993.

[28] A. Klappenecker, T. Beth, Galois Theory and Wavelet Transforms, *Proc. IEEE Int. Symp. Info. Theory*, pp.429, 17-22 Sept., 1995.

[29] S. Sarkar, H.V. Poor, Finite Wavelet Transforms and Multilevel error Protection, *Proc. IEEE Int. Symp. Info. Theory*, pp.428, 17-22 Sept., 1995.

[30] F. Fekri, Finite Field Wavelets and Their Application to Error Control Coding, Seminar- MIT Department of Electrical Engineering And Computer Science, April, 2000. http:www-eecs.mit.edu/AY00-00/events/69.html

[31] R.M. Mersereau, Finite-Field Wavelets and Some of their Applications: Many Questions and a Few Answers, *The Frontiers of High Technology Colloquium Series*, Rice University, February, 2000. http://www.ece.rice.edu/ece/colloq/99-00/Feb8.html

[32] T. Cooklev, A. Nishihara, M. Sablatash, Theory of Filter Banks over Finite Fields, *IEEE Asia-Pacific Conference on Circuits and Systems*, APCCAS '94, pp.260-265,1994.

[33] D.M. Burton, *An Introduction to Number Theory*, Allyn and Bacon, 1998.

[34] C. Mulcahy, Image Compression Using the Haar Wavelet Transform (Review), *Spelman Science and Math. Journal*, pp.22-31, 1996. http://www.ime.usp.br/~pam/papers.html

[35] A. Cohen, Ondelettes, Analyses Multirésolutions et Filters Mirroirs en Quadrature, *Ann. Inst. H. Poincaré*, Anal. Non linéaire 7, 5 (1990) pp.439-459.

[36] I. Daubechies, Orthonormal Bases of Compactly Supported Wavelets, *Comm. Pure and Applied Math*., 41 (1988) pp.909-996.

[37] R.R. Coifman, M.V. Wickerhauser, Entropy-based Algorithms for Best Basis Selection*, IEEE Trans. Info. Theory*, v.38, p. 713-718, março 1992.

[38] Qualcomm, *The CDMA Network Engineering Handbook*, Qualcomm Inc., San Diego, CA, 1992.

[39] H.M. de Oliveira, R.M. Campello de Souza e A.N. Kauffman, Efficient Multiplex for Band-limited Channels: Galois Division Multiple Access, *Proceedings of the 1999 Workshop on Coding and Cryptography*, WCC-99, pp.235-241, Paris, Jan., 1999.

[40] H. M. de Oliveira e R. M. Campello de Souza, Orthogonal Multilevel Spreading Sequence Design, *Coding, Communications and Broadcasting*, Research Studies Press, Baldock, UK, pp. 291 – 301, 2000.

[41] H. M. de Oliveira, J. P. C. L. Miranda e R. M. Campello de Souza, Spread Spectrum Based on Finite Field Fourier Transforms, ICSECIT 2001 – *International Conference on Systems Engineering, Communications and Information Technologies*, Punta Arenas, Chile, ISBN 956-7189-11-0, April 2001.

H.M. de Oliveira nasceu em Arcoverde, Pernambuco, em Maio 1959. Ele recebeu os graus de B.Eng e Mestre em Engenharia Elétrica (MEE) da Universidade Federal de Pernambuco (UFPE), em 1980 e 1983. Ingressou no Departamento de Eletrônica e Sistemas DES-UFPE como Docente em 1983, e em 1992 recebeu o grau de *Docteur de l'École Nationale Supérieure des Télécommunications*, Paris, especialidade em Eletrônica e Telecomunicações. Foi professor homenageado de mais de 15 turmas de Engenharia de Engenharia Elétrica. Foi Coordenador do Mestrado de Eng. Elétrica da UFPE de 1992 a 1996. Interesses: Teoria das Comunicações, Teoria da Informação, Processamento de Sinais. Dr. De Oliveira é sócio do IEEE *Institute of Electrical and Electronic Engineering* e da Sociedade Brasileira de Telecomunicações.

T.H. Falk nasceu em Recife, Pernambuco, em Setembro de 1979. Atualmente é aluno de Graduação do Curso de Engenharia Eletrônica da Universidade Federal de Pernambuco. É bolsista de Iniciação Científica (IC) do CNPq. Recebeu o prêmio Jovem Cientista Prof. Newton Maia de IC (UFPE-CNPq) em 2001. Suas áreas de interesse são: Teoria da Comunicações e Processamento de Sinais. Tiago Falk é sócio estudante do IEEE *Institute of Electrical and Electronic Engineering* e da Sociedade Brasileira de Telecomunicações.

R.G.F. Távora nasceu na cidade de Fortaleza, Ceará, em 22/05/1973. É Bacharel em Engenharia de Comunicações, graduado pelo Instituto Militar de Engenharia (IME) e recebeu em 2001 o título de Mestre em Engenharia Elétrica pela Universidade Federal de Pernambuco (UFPE). Suas áreas de interesse são algoritmos rápidos, processamento de sinais, Teoria da Informação e Criptografia.