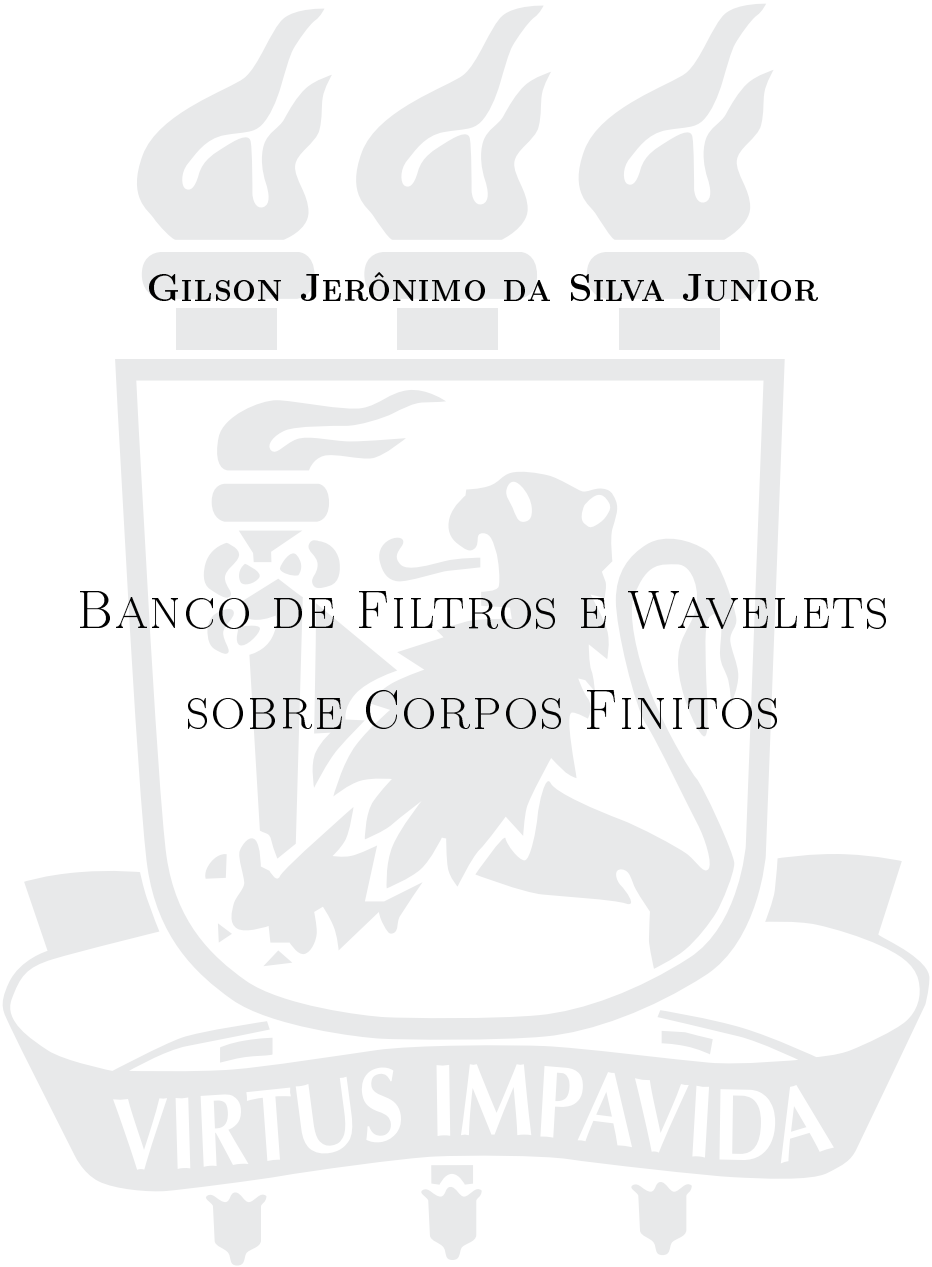
Universidade Federal de Pernambuco
Centro de Tecnologia e Geociências
Programa de Pós-graduação em Engenharia Elétrica



Gilson Jerônimo da Silva Junior

Banco de Filtros e Wavelets sobre Corpos Finitos

Recife, Abril de 2008.

Gilson Jerônimo da Silva Junior

Banco de Filtros e Wavelets sobre Corpos Finitos

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do grau de **Mestre em Engenharia Elétrica**

Orientador: Prof. Ricardo Menezes Campello de Souza, Ph.D.

Recife, Abril de 2008.

S586b **Silva Junior, Gilson Jerônimo da**

Banco de filtros e wavelets sobre corpos finitos / Gilson Jerônimo da Silva Junior. -Recife: O Autor, 2008.

134 f.; il., gráfs., tabs.

Dissertação (Mestrado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2008.

Inclui apêndice e bibliografia

1. Engenharia Elétrica. 2. Banco de filtros. 3. Wavelets . 4. Corpos finitos. 5. Sistemas cíclicos I. Título.

621.3CDD (22.ed.) **UFPE/BCTG/2008-114**

Universidade Federal de Pernambuco

Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE DISSERTAÇÃO DO MESTRADO ACADÊMICO DE

GILSON JERÔNIMO DA SILVA JÚNIOR

TÍTULO

"BANCO DE FILTROS E WAVELETS SOBRE CORPOS FINITOS"

A comissão examinadora composta pelos professores: RICARDO MENEZES CAMPELLO DE SOUZA, DES/UFPE, HÉLIO MAGALHÃES DE OLIVEIRA, DES/UFPE, e MYLÈNE CHRISTINE QUEIROZ DE FARIAS, DCC/UNIFESP sob a presidência do primeiro, consideram o candidato **GILSON JERÔNIMO DA SILVA JÚNIOR** **APROVADO**.

Recife, 18 de abril de 2008.

EDUARDO FONTANA
Coordenador do PPGEE

RICARDO MENEZES CAMPELLO DE SOUZA
Orientador e Membro Titular Interno

MYLÈNE CHRISTINE QUEIROZ DE FARIAS
Membro Titular Externo

HÉLIO MAGALHÃES DE OLIVEIRA
Membro Titular Interno

Universidade Federal de Pernambuco

Centro de Tecnologia e Geociências

Programa de Pós-graduação em Engenharia Elétrica

Gilson Jerônimo da Silva Junior

Banco de Filtros e Wavelets sobre Corpos Finitos

'Esta Dissertação foi julgada adequada para obtenção do Título de Mestre em Engenharia Elétrica, Área de Concentração em Comunicações, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco'.

Prof. Eduardo Fontana, Ph.D.
Coordenador do Programa de
Pós-graduação em Engenharia Elétrica

Banca Examinadora:

Prof. Ricardo Menezes Campello de Souza, Ph.D.
Orientador
Universidade Federal de Pernambuco

Profa. Mylène Christine Queiroz de Farias, Ph.D.
Universidade Federal de São Paulo

Prof. Hélio Magalhães de Oliveira, Docteur
Universidade Federal de Pernambuco

18 de Abril de 2008

Agradecimentos

Aqui expresso meus sinceros agradecimentos às pessoas que contribuíram direta e indiretamente para o desenvolvimento dessa dissertação. Em especial agradeço:

À minha família, todos os Batités e Florêncios, em especial, aos meus pais e meu irmão, pelos apoios e incentivos constantes.

Ao meu orientador, professor Ricardo Campello, por me aceitar e confiar em mim como orientado no mestrado; pelas contribuições, motivações e correções; por sua disponibilidade e vibração e por ser um excelente professor, na minha opinião, o melhor professor do curso de engenharia eletrônica. Além disso, uma ótima pessoa.

Ao professor Hélio Magalhães, pelas valorosas contribuições e incentivos. Além disso, por ser um excelente professor, segundo Eric Bouton [1]: "Seu entusiasmo, criatividade e amor à Ciência e à Engenharia serão sempre uma fonte de inspiração.", não achei frase que o descreve-se melhor.

Aos professores do grupo de Telemática, em especial, à professora Márcia Mahon e ao professor Valdemar Cardoso, que também me ensinaram muito no decorrer do mestrado.

Aos amigos da pós-graduação, que me ajudaram no desenvolvimento dessa dissertação. Em especial ao Eng. Daniel Simões, orientado do professor Valdemar Cardoso, por suas valorosas sugestões, contribuições e incentivos em nossas interessantes discussões. A Giovanna Araújo, André Ricardson e Andrei Formiga por me ajudarem com os modelos da dissertação e com outras ferramentas utilizadas nesse trabalho.

Gilson Jerônimo da Silva Junior

Universidade Federal de Pernambuco

18 de Abril de 2008

Resumo da Dissertação apresentada à UFPE como parte dos requisitos necessários para a obtenção do grau de Mestre em Engenharia Elétrica

Banco de Filtros e Wavelets sobre Corpos Finitos

Gilson Jerônimo da Silva Junior

Abril/2008

Orientador: Prof. Ricardo Menezes Campello de Souza, Ph.D.
Área de Concentração: Comunicações
Palavras-chaves: Banco de filtros, wavelets, corpos finitos, sistemas cíclicos, característica dois
Número de páginas: 134

Banco de filtros e wavelets são ferramentas da Engenharia, definidas sobre o corpo dos complexos, com diversas aplicações. Esta dissertação introduz a teoria de banco de filtros e wavelets, definidas sobre corpos finitos, em estruturas cíclicas e não cíclicas. O problema de se definir banco de filtros de dois canais e decomposição em wavelets para corpos de característica dois foi resolvido, propiciando uma nova condição de reconstrução perfeita para esse tipo de estrutura. São apresentadas e sugeridas aplicações nas áreas de segurança de dados, códigos corretores de erros, multiplexação e espalhamento espectral para essas novas ferramentas.

Abstract of Dissertation presented to UFPE as a partial fulfillment of the requirements for the degree of Master in Electrical Engineering

Filter Banks and Wavelets on Finite Fields

Gilson Jerônimo da Silva Junior

April/2008

Supervisor: Prof. Ricardo Menezes Campello de Souza, Ph.D.
Area of Concentration: Communications
Keywords: Filter banks, wavelets, finite fields, cyclic systems, characteristic two
Number of pages: 134

Filter banks and wavelets are tools of Engineering, defined over complex fields, with many applications. This dissertation introduces the theory of filter banks and wavelets defined over finite fields, over cyclical and noncyclical structures. The problem of defining two-channel filter banks and wavelet decompositions over fields of characteristic two was solved, thereby providing a new perfect reconstruction condition for these structures. Applications, in the areas of data security, error correcting codes, multiplex and spread spectrum, of these new tools are suggested.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

QMF	Filtros de quadratura espelhada (*quadrature mirror filters*)
TFCF	Transformada de Fourier de corpo finito
THCF	Transformada de Hartley de corpo finito
TFTD	Transformada de Fourier de tempo discreto
RP	Reconstrução perfeita
TFCD	Transformada de Fourier de curta duração
FIR	Resposta ao impulso finita (*finite impulse response*)
SWTD	Série wavelet de tempo discreto
LIT	Linear e invariante no tempo
TWCF	Transformada wavelet de corpo finito
CLIT	Cíclico, linear e invariante aos deslocamentos cíclicos no tempo
DFT	Transformada discreta de Fourier (*discrete Fourier transform*)
FFT	Transformada rápida de Fourier (*fast Fourier transform*)
BFC	Banco de filtros cíclicos
DWT	Transformada wavelet discreta (*discrete wavelet transform*)
EBFC	Estrutura com bancos de filtros cíclicos
TFCDC	Transformada de Fourier de curta duração cíclica
ACJ	Árvore completa de J estágios
bps	Bits por segundo
IIR	Resposta ao impulso infinita (*infinite impulse response*)

Sumário

capítulo 1

Introdução

Banco de filtros e *wavelets* são ferramentas de uma área da Engenharia Elétrica conhecida como processamento de sinais e têm aplicações em processamento de voz e imagem, visão computacional, geologia sísmica e outras [2]. Existe uma conexão entre essas ferramentas, embora tenham sido descobertas separadamente.

As primeiras wavelets surgiram em 1909, no apêndice da tese de doutorado de Alfred Haar [2, 3], onde se menciona a análise escalonada. Naturalmente, não foram chamadas de wavelets, pois não existia formalismo ainda para esse tipo de análise. A primeira vez que o termo "wavelets" apareceu foi em 1984, com os trabalhos de J. Goupillaud, J. Morlet and A. Grossman, na área de processamento de sinais geofísicos [2, 3]. Esse termo deriva do francês "ondelettes" e pode ser traduzido como "ondinha". A idéia proposta pelos autores era uma alternativa a análise local de Fourier, baseada na decomposição em funções, as quais eram geradas a partir de escalonamentos e deslocamentos de uma mesma função protótipo (wavelet).

Historicamente, os bancos de filtros surgiram primeiro. Em 1976, uma ferramenta de processamento de sinais com aplicações em compressão de voz e imagem, denominada de Codificação de Sub-bandas ("subband coding"), foi proposta por Croiser, Esteban e Galand [3, 4]. Essa proposta utilizava uma classe de filtros chamados "quadrature mirror filters" (QMF). Esses estudos levaram a condição de reconstrução perfeita para banco de filtros, problema resolvido por volta de 1980 por várias pessoas, incluindo Smith, Barnwell, Mintzer, Vetterli e Vaidyanathan [3].

Na área de visão computacional, uma técnica de multirresolução, chamada de Codificação

Piramidal ("pyramid coding"), foi proposta por Burt e Adelson para codificação de imagem em 1983 [3]. Esse método era similar à codificação de Sub-bandas e suas sucessivas aproximações eram também similares a técnicas de multirresolução usadas em esquemas de análise via wavelets.

A descrição matemática para a teoria de wavelets foi construída no final da década de 80 com contribuições de vários autores, como Daubechies, Mallat e Meyer [2]. A formalização dessas construções levou à criação de uma ferramenta para expansões em wavelets chamada de análise multirresolução, estabelecendo ligações com métodos usados em outros campos, como os filtros QMF, codificação piramidal e banco de filtros. Em particular, a construção de wavelets proposta por Daubechies é intimamente ligada a estruturas de banco de filtros, usadas em processamento digital de sinais, e formam o mais usado conjunto de wavelets ortogonais de suporte compacto [2].

Em matemática, um corpo finito é um corpo em que o conjunto dos elementos é finito. Corpos finitos, também chamados de campos de Galois, em honra ao matemático francês Évariste Galois, vêm se tornando uma alternativa ao corpo dos complexos no sentido de que os mesmos podem ser armazenados em máquinas e processadores digitais evitando erros de quantização e arredondamento causados por operações com ponto flutuante. Além disso, estruturas em corpos finitos têm aplicações nas áreas de comunicação digital, criptografia, codificação de canal, espalhamento espectral e outras.

A utilização de ferramentas de processamento de sinais sobre corpos finitos teve um grande impulso quando Pollard propôs a transformada de Fourier de corpo finito (TFCF) em 1971 [5]. A partir de então, muitas ferramentas de Engenharia vêm emergindo para estruturas definidas sobre corpos finitos. Em 1998, Campello de Souza, de Oliveira e Kauffman apresentaram a transformada de Hartley sobre um corpo finito (THCF) [6]. Além disso, construíram uma trigonometria sobre corpos finitos que originou também as transformadas trigonométricas sobre corpos finitos [7].

1.1 Objetivos

Técnicas para processamento digital de sinais, derivadas de corpos finitos, têm sido aplicadas com sucesso na concepção de novas transformadas digitais e no projeto de sistemas de acesso múltiplo e de seqüências multiníveis para espalhamento espectral [8]. Nesta dissertação é proposta a investigação de uma análise de sinais/multirresolução baseada em wavelets

e banco de filtros definidos sobre corpos finitos.

Uma novidade são os banco de filtros e wavelets em corpos de característica igual a 2 e wavelets e banco de filtros cíclicos. Aplicações são propostas para essas novas ferramentas.

1.2 Contribuições

Existem poucos trabalhos sobre wavelets e banco de filtros definidos sobre corpos finitos. Entre eles, destacam-se: [9], no qual os autores propõem as wavelets cíclicas sobre os reais e sobre corpos finitos, excluindo os corpos de característica dois; [10], banco de filtros sobre corpos finitos para seqüências de comprimento finito (corpos de característica dois não são estudados); [11], na qual propõem-se estudos sobre a classe de banco de filtros e wavelets ortogonais não cíclicos (paraunitários) sobre corpos de característica dois.

A principal contribuição desta dissertação é unificar a teoria de banco de filtros e wavelets sobre corpos finitos, de qualquer característica, ortogonais e biortogonais, em estruturas cíclicas e não cíclicas. O estudo foi realizado com abordagem diferente dos trabalhos já existentes.

1.3 Organização da Dissertação

A dissertação esta organizada em quatro partes principais. A primeira parte envolve a introdução e uma breve revisão sobre banco de filtros e wavelets sobre o corpo dos complexos, referente aos capítulos 1 e 2. As contribuições do trabalho começam a partir do capítulo 3, o qual trata, essencialmente, sobre banco de filtros e wavelets em corpos finitos com característica ímpar; novas definições e teoremas são apresentados. O capítulo 4, trata de sistemas de bloco, definidos aqui como sistemas cíclicos, em analogia ao tipo de convolução utilizada; neste capítulo são apresentados banco de filtros e wavelets cíclicos. Finalmente, o capítulo 5, apresenta banco de filtros, transformadas multirresolução e wavelets para corpos de característica dois. As razões da inclusão de um capítulo específico para tratar de corpos de característica dois são a diferença acentuada dos resultados obtidos, em relação aos demais corpos, e o caráter inovador do assunto. Aplicações em códigos convolucionais e códigos de bloco lineares são apresentadas em exemplos. O capítulo 6 mostra as conclusões, sugestões para aplicações e indica trabalhos futuros. Uma breve revisão de alguns resultados da teoria de corpos finitos é apresentada no apêndice A.

capítulo 2

Banco de Filtros e Wavelets sobre o Corpo dos Reais

Este capítulo apresenta de forma bastante resumida a teoria de banco de filtros e wavelets discretas sobre o corpo dos reais. A parte principal é o estudo de bancos de filtros e suas condições para reconstrução perfeita. A partir dos bancos de filtros é possível gerar bases e wavelets biortogonais e ortogonais. Existem muitas aplicações para banco de filtros e wavelets no corpo dos reais, entre elas destacam-se análise multirresolução, compactação de imagens, espalhamento espectral em comunicações, e outras [2–4].

Para o estudo de banco de filtros e wavelets, duas transformadas são de grande importância: a transformada de Fourier de tempo discreto (TFTD) e a transformada Z, as quais são apresentadas nas próximas seções.

2.1 A Transformada de Fourier de Tempo Discreto

Dada uma seqüência $x[n]$, $n \in \mathbb{Z}$, existe uma função, $X(e^{j\omega})$, $\omega \in \mathbb{R}$, chamada de transformada de Fourier de tempo discreto (TFTD) de $x[n]$. O par TFTD é denotado por

$$x[n] \overset{\mathcal{F}}{\longleftrightarrow} X(e^{j\omega})$$

As equações de análise e síntese, (4.2) e (4.3) respectivamente, são

$$X(e^{j\omega}) \triangleq \sum_{n=-\infty}^{\infty} x[n]e^{-j\omega n} \tag{2.1}$$

$$x[n] = \frac{1}{2\pi} \int_{-\pi}^{\pi} X(e^{j\omega}) e^{j\omega n} d\omega. \tag{2.2}$$

Algumas propriedades da TFTD podem ser encontradas na Tabela 2.1.

Tabela 2.1: Propriedades da transformada de Fourier de tempo discreto

Tempo	Freqüência	Propriedade
$x[n]$	$X(e^{j\omega})$	
$y[n]$	$Y(e^{j\omega})$	
$ax[n] + by[n]$	$aX(e^{j\omega}) + bY(e^{j\omega})$	Linearidade
$x[n-d]$	$e^{-j\omega d}X(e^{j\omega})$	Deslocamento no tempo
$e^{j\omega_0 n}x[n]$	$X(e^{j(\omega-\omega_0)})$	Deslocamento na freqüência
$x[n] * y[n]$	$X(e^{j\omega})Y(e^{j\omega})$	Convolução
$x[n]y[n]$	$\frac{1}{2\pi}\int_{2\pi} X(e^{j\theta})Y(e^{j(\omega-\theta)})d\theta$	Multiplicação

2.2 A Transformada Z

Para uma seqüência $x[n]$, $n \in \mathbb{Z}$, existe uma função $X(z)$, $z \in \mathbb{C}$, chamada de transformada Z de $x[n]$ e denotada por

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

onde

$$X(z) = \sum_{n=-\infty}^{\infty} x[n] z^{-n}, \tag{2.3}$$

definida na sua região de convergência [12].

Algumas propriedades da transformada Z estão mostradas na Tabela 2.2.

Tabela 2.2: Propriedades da Transformada Z

Tempo	Z	Propriedade
$x[n]$	$X(z)$	
$y[n]$	$Y(z)$	
$ax[n] + by[n]$	$aX(z) + bY(z)$	Linearidade
$x[n-d]$	$z^{-d}X(z)$	Deslocamento no tempo
$nx[n]$	$-z\frac{d}{dz}X(z)$	Derivada em Z
$x[n] * y[n]$	$X(z)Y(z)$	Convolução

A TFTD pode ser obtida pela transformada Z, através da relação

$$X(e^{j\omega}) = X(z)|_{z=e^{j\omega}}, \tag{2.4}$$

desde que a região de convergência contenha o ciclo unitário [12].

2.3 Sistemas Subamostrador e Sobreamostrador

Antes de iniciar a seção dos bancos de filtros é necessário apresentar dois sistemas fundamentais dessas estruturas. São os sistemas *subamostrador* e *sobreamostrador*. Ambos são lineares e variantes no tempo e não possuem complexidade computacional aritmética.

Sistema Subamostrador

O sistema da Figura 2.1 é um sistema *subamostrador* ou *compressor* de parâmetro M. Sua saída é definida por

$$x_d[n] \triangleq x[Mn], \tag{2.5}$$

onde $M \in \mathbb{N}^*$.

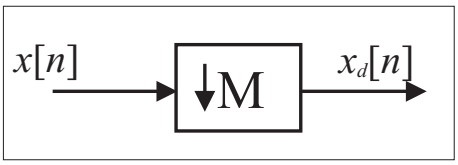


Figura 2.1: Diagrama de um sistema subamostrador.

Pode-se mostrar que a transformada Z da saída do subamostrador, $X_d(z)$, se relaciona com a transformada Z da entrada, $X(z)$, pela equação [3]

$$X_d(z) = \frac{1}{M} \sum_{m=0}^{M-1} X(e^{-j\frac{2\pi}{M}m} z^{\frac{1}{M}}). \tag{2.6}$$

Sistema Sobreamostrador

O sistema *sobreamostrador* ou *expansor* de parâmetro L está mostrado na Figura 2.2 [13]. Dado um sinal de entrada $x[n]$, a saída do sobreamostrador, $x_e[n]$, é definida por

$$x_e[n] \triangleq \sum_{m=-\infty}^{\infty} x[m]\delta[n - mL], \tag{2.7}$$

ou, de forma equivalente, por

$$x_e[n] \triangleq \begin{cases} x[n/L], & \text{se } n \equiv 0 \ (mod\ L) \\ 0, & \text{caso contrário.} \end{cases} \tag{2.8}$$

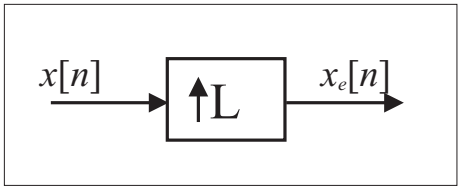


Figura 2.2: Diagrama de um sistema sobreamostrador L no tempo.

Pode-se mostrar que a transformada Z da saída do sobreamostrador, $X_e(z)$, se relaciona com a transformada Z da entrada, $X(z)$, pela equação [3]

$$X_e(z) = X(z^L). \tag{2.9}$$

2.4 Processamento de Sinais Multitaxa

São apresentadas duas identidades, conhecidas como identidades nobres [4]. Elas são válidas para sistemas definidos em qualquer corpo.

2.4.1 Identidades Nobres

A primeira identidade nobre está representada na Figura 2.3.

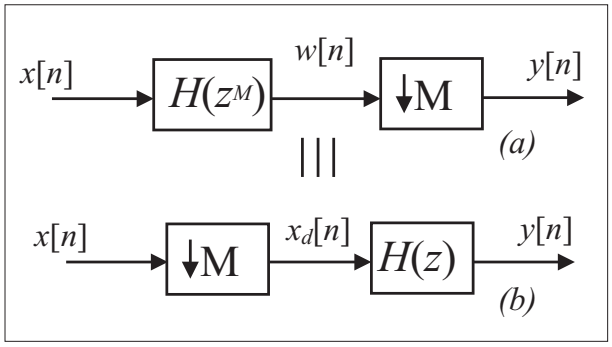


Figura 2.3: Ilustração da primeira identidade nobre, os sistemas (a) e (b) são equivalentes.

Teorema 2.1 *Os sistemas (a) e (b) da Figura 2.3 são equivalentes.*

Demonstração: Para verificar a primeira identidade, expressa-se a saída do sistema (a) da Figura 2.3. Observando que

$$h[n] \overset{\mathbf{Z}}{\longleftrightarrow} H(z) \Rightarrow \sum_{m=-\infty}^{\infty} h[m]\delta[n - mM] \overset{\mathbf{Z}}{\longleftrightarrow} H(z^M), \tag{2.10}$$

então

$$w[n] = x[n] * \sum_{m=-\infty}^{\infty} h[m]\delta[n - mM] = \sum_{m=-\infty}^{\infty} h[m]x[n - mM]. \tag{2.11}$$

Aplicando $w[n]$ no subamostrador, por definição

$$y[n] = w[Mn] = \sum_{m=-\infty}^{\infty} h[m]x[M(n - m)] = h[n] * x[Mn], \tag{2.12}$$

exatamente como o sistema (b) da Figura 2.3. ■

A segunda identidade nobre está representada na Figura 2.4.

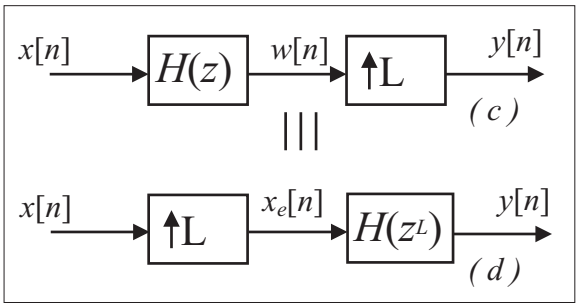


Figura 2.4: Ilustração da segunda identidade nobre, os sistemas (c) e (d) são equivalentes.

Teorema 2.2 *Os sistemas (c) e (d) da Figura 2.4 são equivalentes.*

Demonstração: Para verificar a segunda identidade, expressa-se a transformada Z da saída do sistema (c) da Figura 2.4.

$$W(z) = X(z)H(z), \tag{2.13}$$

$$Y(z) = W(z^L), \tag{2.14}$$

$$Y(z) = X(z^L)H(z^L) \tag{2.15}$$

e

$$Y(z) = X_e(z)H(z^L), \tag{2.16}$$

exatamente como no sistema (d) da Figura 2.4. ■

2.4.2 Decomposição Polifásica

A decomposição polifásica é uma forma eficiente de processamento de sinais multitaxa, bastante utilizada na implementação de filtros dizimadores e interpoladores [13] utilizados em banco de filtros. A seguir, são apresentadas as decomposições polifásica tipo I e tipo II.

Decomposição Polifásica Tipo I

A decomposição polifásica tipo I de uma seqüência $h[n]$ é mostrada na Figura 2.5.

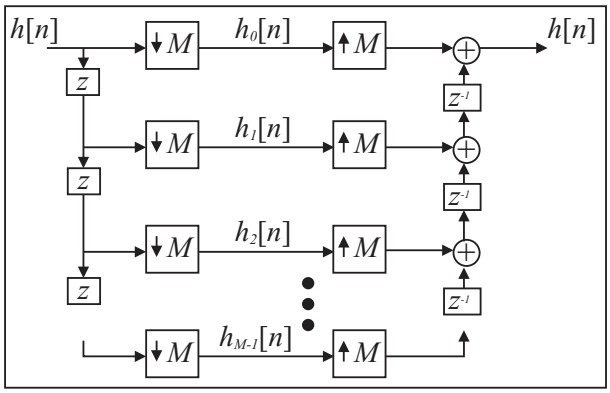


Figura 2.5: Decomposição polifásica tipo I.

Matematicamente, essa decomposição representa uma seqüência $h[n]$, por meio de M seqüências $h_i[n]$ chamadas de componentes polifásica tipo I de $h[n]$, onde

$$h_i[n] = h[Mn + i], \tag{2.17}$$

e

$$h[n] = \sum_{i=0}^{M-1} h_i[(n-i)/M], \tag{2.18}$$

com $h_i[r/M] = 0$, se $r \neq 0(mod\ M)$. Assim, cada componente polifásica corresponde à uma classe de equivalência dos inteiros módulo M.

Um filtro $H(z)$ pode ser implementado utilizando-se a decomposição polifásica tipo I por

$$H(z) = \sum_{n=-\infty}^{\infty} \sum_{i=0}^{M-1} h[Mn + i] z^{-(Mn+i)}, \tag{2.19}$$

$$H(z) = \sum_{i=0}^{M-1} z^{-i} \sum_{n=-\infty}^{\infty} h[Mn + i] z^{-Mn} \tag{2.20}$$

ou

$$H(z) = \sum_{i=0}^{M-1} z^{-i} H_i(z^M). \tag{2.21}$$

A implementação polifásica desse filtro está mostrada na Figura 2.6.

Decomposição Polifásica Tipo II

A decomposição polifásica tipo II de uma seqüência $h[n]$, mostrada na Figura 2.7, representa

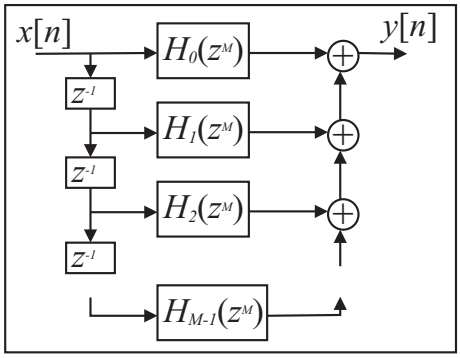


Figura 2.6: Implementação polifásica tipo I do filtro $H(z)$.

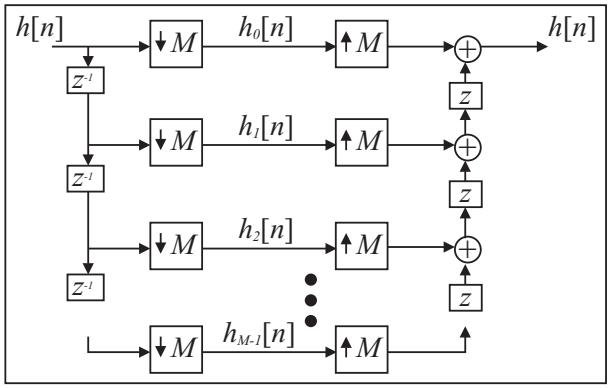


Figura 2.7: Decomposição polifásica tipo II.

uma seqüência $h[n]$, por meio de M seqüências $h_i[n]$ chamadas de componentes polifásica tipo II de $h[n]$, onde

$$h_i[n] = h[Mn - i], \tag{2.22}$$

e

$$h[n] = \sum_{i=0}^{M-1} h_i[(n+i)/M]. \tag{2.23}$$

Um filtro $H(z)$ pode ser implementado utilizando-se a decomposição polifásica tipo II, por

$$H(z) = \sum_{n=-\infty}^{\infty} \sum_{i=0}^{M-1} h[Mn - i] z^{-(Mn-i)}, \tag{2.24}$$

$$H(z) = \sum_{i=0}^{M-1} z^i \sum_{n=-\infty}^{\infty} h[Mn - i] z^{-Mn} \tag{2.25}$$

ou

$$H(z) = \sum_{i=0}^{M-1} z^i H_i(z^M). \tag{2.26}$$

Implementação de Filtros Dizimadores

Filtros dizimadores são componentes fundamentais de banco de filtros de análise, assim como filtros interpoladores são fundamentais nos bancos de síntese. A implementação polifásica do sistema mostrado na Figura 2.8 pode ser feita utilizando-se a decomposição polifásica tipo I de $H(z)$, ilustrada na Figura 2.6, e aplicando-se a primeira identidade nobre. O resultado é a implementação da Figura 2.9 [13]. Observa-se que a transformada Z da saída $y[n]$

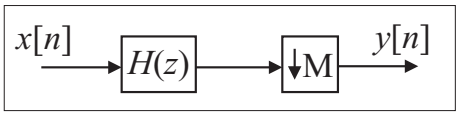


Figura 2.8: Diagrama de um filtro dizimador.

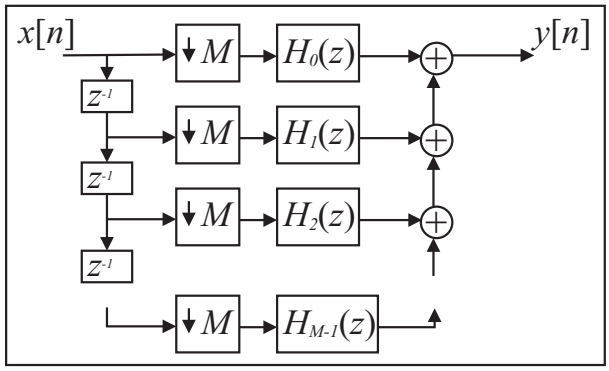


Figura 2.9: Diagrama de um filtro dizimador implementado utilizando-se a decomposição polifásica tipo I para $h[n]$.

é dada por

$$Y(z) = \sum_{i=0}^{M-1} X_i(z) H_i(z), \tag{2.27}$$

onde as componentes $x_i[n]$ e $h_i[n]$, respectivamentes, correspondem às componentes polifásica tipo II de $x[n]$ e tipo I de $h[n]$.

Existe uma outra implementação por meio da decomposição polifásica tipo II para $h[n]$, essa implementação não é causal. Pode-se trabalhar da mesma forma para encontrar duas decomposições polifásica para filtros interpoladores.

Supondo que $x[n]$ tem comprimento N e que $h[n]$ tem comprimento L, a implementação polifásica substituiu uma convolução linear NxL por M convoluções lineares (N/M)x(L/M), o que implica em redução da complexidade por um fator de M [13].

2.5 Banco de Filtros e Codificação em Sub-bandas

Um banco de filtros é um conjunto de filtros lineares e invariantes no tempo (LIT), interligados por subamostradores e sobreamostradores. Um diagrama para um banco de filtro de M canais é mostrado na Figura 2.10. Essas estruturas têm aplicações em processamento e compressão de imagens, multiplexação e espalhamento espectral [3, 4]. Nela, o sinal de entrada $x[n]$ é decomposto nas chamadas *componentes de sub-bandas* $x_i^{(1)}[n]$.

Notação utilizada:

$x_i^{(j)}[n] \rightarrow$ Componente de sub-bandas ($j = 1$) ou coeficiente wavelet;
$i \rightarrow$ Canal ou sub-banda da componente;
$j \rightarrow$ Estágio ou escala da wavelet de tempo discreto.

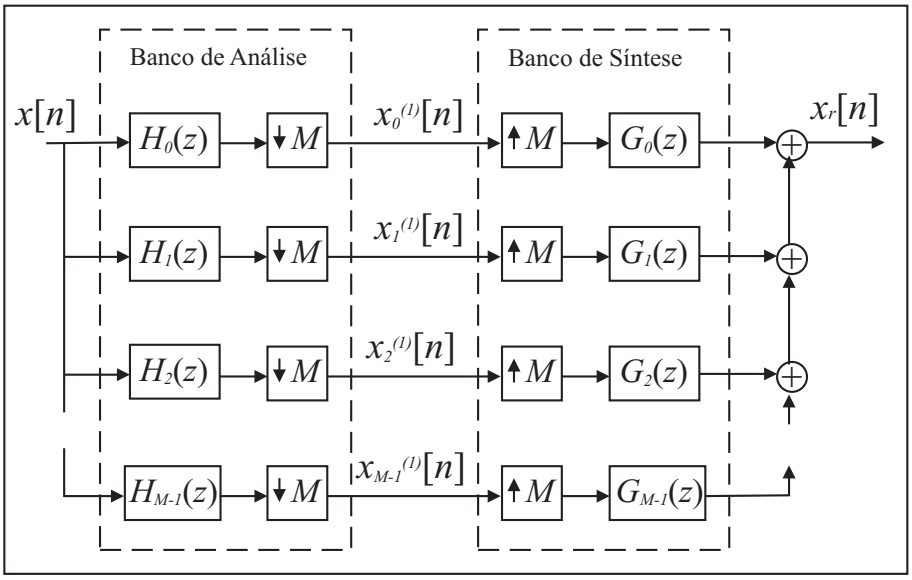


Figura 2.10: Diagrama ilustração de um banco de filtros de M canais.

A saída do banco de síntese é o sinal $x_r[n]$. Uma reconstrução perfeita (RP) ocorre quando $x_r[n] = x[n]$, independente de $x[n]$. O objetivo dessa seção é estudar as condições para RP.

Teorema 2.3 *Para um banco de filtros de M canais, como mostrado na Figura 2.10, se a chamada condição de reconstrução perfeita (2.28) é satisfeita, ou seja, se*

$$\sum_{i=0}^{M-1} H_i(e^{-j\frac{2\pi}{M}m}z)G_i(z) = M\delta[m], \tag{2.28}$$

para $m = 0, 1, \ldots, M-1$*, então,* $x_r[n] = x[n]$*, para qualquer* $x[n]$*.*

A prova pode ser encontrada em [3, 4].

A relação RP pode ser escrita no domínio de Fourier, resultando em

$$\sum_{i=0}^{M-1} H_i(e^{j(\omega - \frac{2\pi}{M}m)})G_i(e^{j\omega}) = M\delta[m]. \tag{2.29}$$

As equações de análise do banco de filtros da Figura 2.10 são dadas por

$$x_i^{(1)}[n] = \sum_{l=-\infty}^{\infty} x[l]h_i[Mn - l], \tag{2.30}$$

para $i = 0, 1, \ldots, M-1$, e a equação de síntese é dada por

$$x[n] = \sum_{i=0}^{M-1} \sum_{l=-\infty}^{\infty} x_i^{(1)}[l]g_i[n - Ml], \tag{2.31}$$

desde que a condição RP seja satisfeita.

2.6 Banco de Filtros de Dois Canais

Banco de filtros de dois canais são as estruturas mais simples e mais utilizadas na teoria de banco de filtros. A grande vantagem é a simplificação computacional para o projeto dos bancos. A estrutura de dois canais está apresentada na Figura 2.11. Nessa estrutura, o sinal é dividido em duas componentes, a componente de baixa freqüência, $x_0^{(1)}[n]$, e a componente de alta freqüência, $x_1^{(1)}[n]$, o que significa que os filtros $H_0(z)$ e $H_1(z)$ são, respectivamente, passa baixas e passa altas.

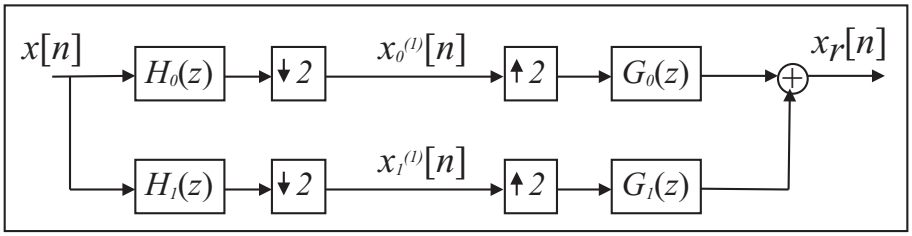


Figura 2.11: Diagrama ilustração de um banco de filtros de dois canais.

A condição RP (2.28) fica reduzida a

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 2 \tag{2.32}$$

e

$$H_0(-z)G_0(z) + H_1(-z)G_1(z) = 0. \tag{2.33}$$

Escrevendo em forma matricial, tem-se

$$\begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix} \begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix}. \tag{2.34}$$

Definindo a *matriz de modulação*, $H_m(z)$, por

$$H_m(z) \triangleq \begin{bmatrix} H_0(z) & H_0(-z) \\ H_1(z) & H_1(-z) \end{bmatrix}, \tag{2.35}$$

os filtros de síntese podem ser obtidos através dos filtros de análise por

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \frac{2}{\Delta(z)} \begin{bmatrix} H_1(-z) \\ -H_0(-z) \end{bmatrix}, \tag{2.36}$$

onde $\Delta(z) \triangleq det(H_m(z)) = H_0(z)H_1(-z) - H_0(-z)H_1(z)$. Como $\Delta(z)$ é uma função ímpar, isto é, $\Delta(-z) = -\Delta(z)$, isso significa que o mesmo contém apenas potências ímpares de z^{-1}.

Outra condição importante é descrita pelo teorema a seguir.

Teorema 2.4 (Relação de Biortogonalidade) *Se $H_i(z)$ e $G_i(z)$, $i = 0, 1$, são filtros de análise e síntese, respectivamente, de um banco de filtros com reconstrução perfeita, então*

$$\langle h_i[-n], g_j[n-2m] \rangle \triangleq \sum_{n=-\infty}^{\infty} h_i[-n]g_j[n-2m] = \delta[i-j]\delta[m], \tag{2.37}$$

para $i, j \in \{0, 1\}$ e $m \in \mathbb{Z}$. Além disso, se $g_i[n] = \sigma h_i[-n]$, então é dito que o banco de filtros é ortogonal, isto é

$$\langle g_i[n], g_j[n-2m] \rangle = \sigma\delta[i-j]\delta[m]. \tag{2.38}$$

Quando $\sigma = 1$, o banco de filtro é dito ortonormal. A prova desse teorema pode ser encontrada em [3].

2.7 Implementação Polifásica

Bancos de filtros podem ser implementados utilizando-se a decomposição polifásica.

2.7.1 Implementação Polifásica do Banco de Análise

A implementação polifásica tipo I do banco de análise é mostrada na Figura 2.12. Os filtros $H_{ij}(z)$ são componentes polifásicas tipo I de $H_i(z)$, dados no domínio do tempo por

$$h_{ij}[n] = h_i[2n + j]. \tag{2.39}$$

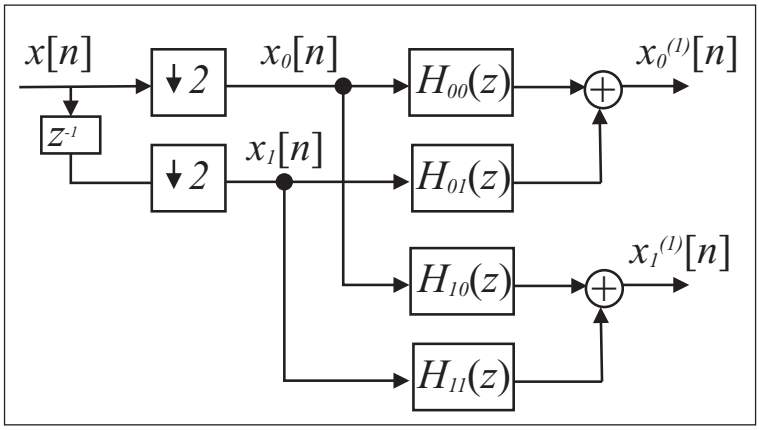


Figura 2.12: Diagrama da implementação polifásica do banco de análise.

As seqüências $x_0[n]$ e $x_1[n]$ são formadas, respectivamente, pelos termos pares e ímpares de $x[n]$ e correspondem às componentes polifásica de $x[n]$ tipo II. A equação de análise pode ser escrita de forma matricial por

$$\begin{bmatrix} H_{00}(z) & H_{01}(z) \\ H_{10}(z) & H_{11}(z) \end{bmatrix} \begin{bmatrix} X_0(z) \\ X_1(z) \end{bmatrix} = \begin{bmatrix} X_0^{(1)}(z) \\ X_1^{(1)}(z) \end{bmatrix}. \tag{2.40}$$

A matriz de polinômios $[H_{ij}(z)]$ é denominada *matriz polifásica de análise*, sendo denotada por $H_p(z)$.

2.7.2 Implementação Polifásica do Banco de Síntese

A implementação polifásica tipo II do banco de síntese é mostrada na Figura 2.13. Os filtros $G_{ij}(z)$ são componentes polifásicas tipo II de $G_i(z)$, dados no domínio do tempo por

$$g_{ij}[n] = g_i[2n - j]. \tag{2.41}$$

As seqüências $x_{r0}[n]$ e $x_{r1}[n]$ são formadas, respectivamente, pelos termos pares e ímpares de $x_r[n]$, correspondendo à representação polifásica tipo II de $x_r[n]$. A equação de síntese polifásica pode ser escrita de forma matricial por

$$\begin{bmatrix} G_{00}(z) & G_{10}(z) \\ G_{01}(z) & G_{11}(z) \end{bmatrix} \begin{bmatrix} X_0^{(1)}(z) \\ X_1^{(1)}(z) \end{bmatrix} = \begin{bmatrix} X_{r0}(z) \\ X_{r1}(z) \end{bmatrix}. \tag{2.42}$$

A matriz $[G_{ij}(z)]$ é definida como *matriz polifásica de síntese*, sendo denotada por $G_p(z)$. Utilizando (2.40), tem-se que

$$\begin{bmatrix} X_{r0}(z) \\ X_{r1}(z) \end{bmatrix} = G_p(z)H_p(z) \begin{bmatrix} X_0(z) \\ X_1(z) \end{bmatrix}. \tag{2.43}$$

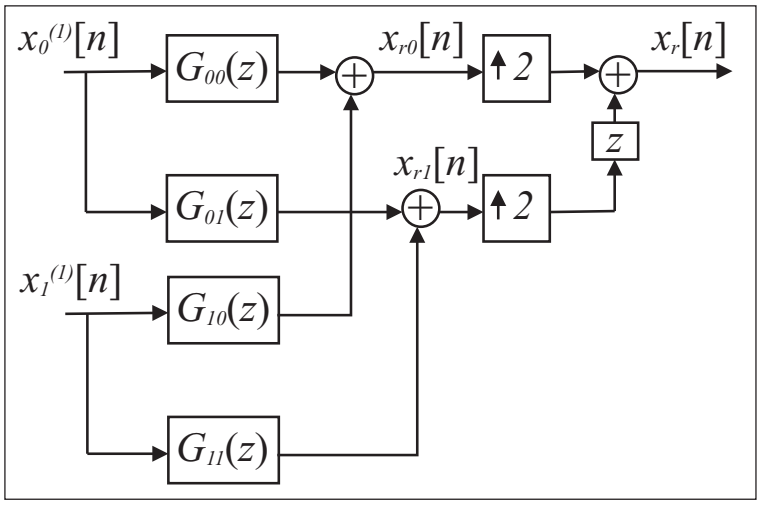


Figura 2.13: Diagrama da implementação polifásica do banco de síntese.

Assim, a condição RP na forma polifásica é dada por

$$G_p(z)H_p(z) = I. \tag{2.44}$$

2.8 Banco de Filtros Estruturados em Árvore

Na saída de um banco de filtros de análise de dois canais, é possível colocar outro banco do mesmo tipo, formando uma estrutura diferente. Novas estruturas formadas por cascateamento de banco de filtros são chamadas de *pacotes de wavelets* ("wavelet packets"), as quais produzem bases biortogonais organizadas de forma adequada e são utilizadas para criação de transformadas, análise multirresolução e compactação de dados [3, 4].

Nesta seção são apresentadas duas transformadas de tempo discreto que derivam de pacotes de wavelets, a transformada de Fourier de curta duração e a *série wavelets* (ou *transformada wavelets de tempo discreto*), ambas de tempo discreto. Para simplificar a representação, os bancos de filtros de dois canais de análise e síntese são representados por árvores, como mostram as Figuras 2.14 e 2.15.

Dependendo de como essas estruturas são organizadas, é possível fazer análise e síntese no domínio tempo e freqüência.

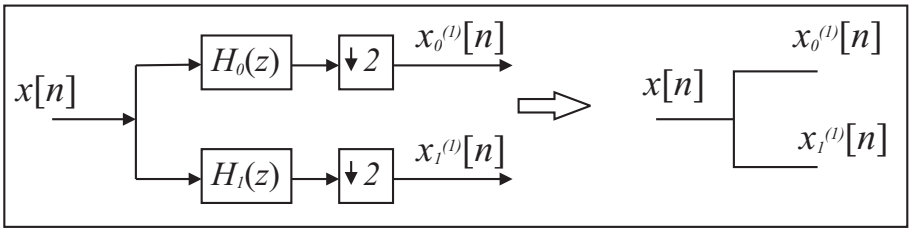


Figura 2.14: Representação simplificada do banco de filtros de análise.

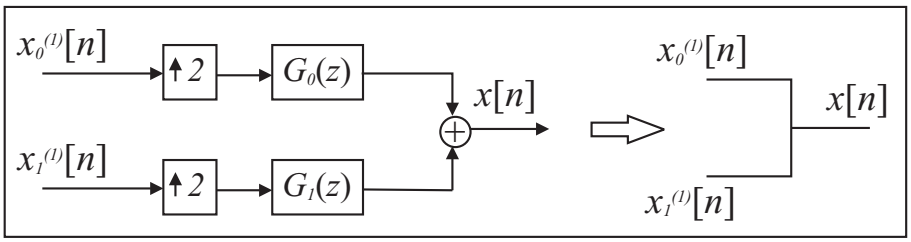


Figura 2.15: Representação simplificada do banco de filtros de síntese.

2.8.1 Transformada de Fourier de Curta Duração

A figura 2.16 mostra uma estrutura em árvore para a transformada de Fourier de curta duração (TFCD) de tempo discreto [3, 4].

Nessa estrutura, escolhe-se o banco de filtro de M canais e forma-se uma árvore completa até J estágios. A transformada associada é análoga a transformada de Fourier de curta duração de tempo contínuo. A TFCD de tempo discreto, para um banco de filtros de M canais e com J estágios, é dada por

$$X[k,l] \triangleq \sum_{n=-\infty}^{\infty} x[n]h^{(k)}[M^J l - n], \tag{2.45}$$

para $l \in \mathbb{Z}$ e $k = \{0, 1, \ldots, M^J - 1\}$. A TFCD inversa é dada por

$$x[n] = \sum_{k=0}^{M^J-1} \sum_{l=-\infty}^{\infty} X[k,l]g^{(k)}[n - M^J l]. \tag{2.46}$$

As seqüências $h^{(k)}[n]$ e $g^{(k)}[n]$ são obtidas no domínio Z por

$$H^{(\sum_{j=0}^{J-1} a_j M^j)}(z) = \prod_{j=0}^{J-1} H_{a_j}(z^{M^{J-1-j}}) \tag{2.47}$$

e

$$G^{(\sum_{j=0}^{J-1} a_j M^j)}(z) = \prod_{j=0}^{J-1} G_{a_j}(z^{M^{J-1-j}}), \tag{2.48}$$

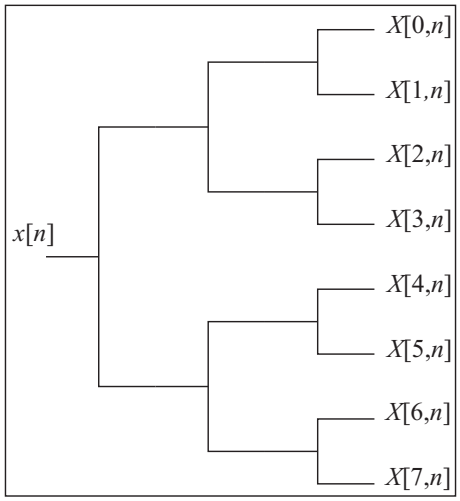


Figura 2.16: Estrutura de banco de filtros para a transformada de Fourier de curta duração de tempo discreto com $M = 2$ e $J = 3$.

onde os a_j podem assumir valores entre 0 e $M - 1$. A partir desses valores, obtém-se todos os filtros $G^{(k)}(z)$ e $H^{(k)}(z)$. A TFCD é denotada por

$$x[n] \overset{TFCD}{\longleftrightarrow} X[k, l]. \tag{2.49}$$

O termo *curta duração* decorre quando $H^{(k)}(z)$ e $G^{(k)}(z)$ são filtros com resposta ao impulso finita (filtros FIR, do inglês *Finite Impulse Response*). Os índices (k) indicam a ordem da componente de freqüência, por exemplo, na Figura 2.16 a seqüência $X[0, l]$ representa a componente do sinal de menor freqüência, enquanto a seqüência $X[7, l]$, representa a de maior freqüência. Existe ainda uma dependência temporal, representada pela variável l, isso caracteriza a análise no domínio tempo e freqüência.

A estrutura de síntese é mostrada na Figura 2.17.

2.8.2 Série Wavelet de Tempo Discreto

A série wavelet de tempo discreto (SWTD) pode ser obtida pela estrutura em árvore mostrada na Figura 2.18.

Esta estrutura também é chamada de *árvore logarítmica*. A análise tempo freqüência ocorre porque as saídas dos estágios são as componentes de maior freqüência (componentes de detalhe). O sinal de menor freqüência é $x_0^{(J)}[n]$, esse constitui um espaço de resolução menor e as demais componentes, ao serem adicionadas, formam os espaços com maior resolução (multirresolução). Assim, pode-se definir a expressão de análise da SWTD. Os coeficientes

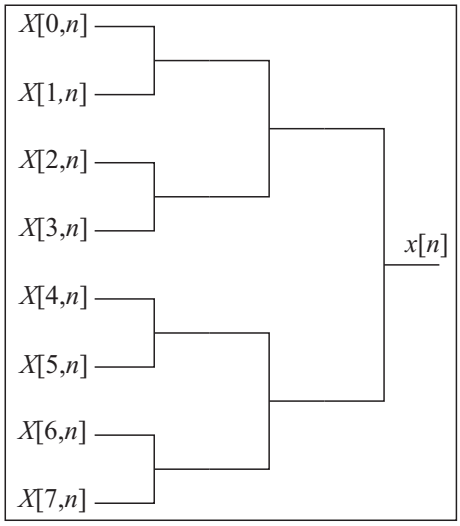


Figura 2.17: Estrutura de banco de filtros para a transformada de Fourier de curta duração inversa, $M = 2$ e $J = 3$.

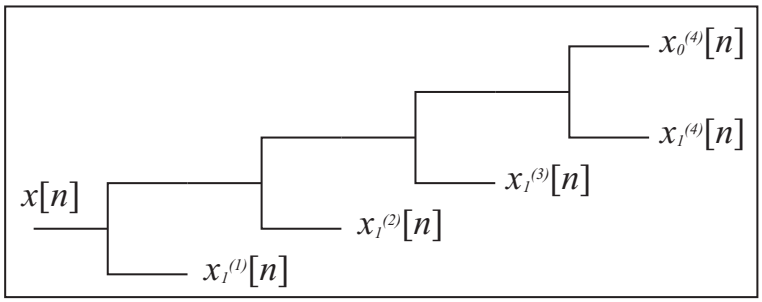


Figura 2.18: Estrutura de banco de filtros para a série wavelet de tempo discreto.

wavelet na escala j, para J estágios, são dados por

$$x_1^{(j)}[l] \triangleq \sum_{n=-\infty}^{\infty} x[n] h_1^{(j)}[2^j l - n], \tag{2.50}$$

para $j = 1, 2, \ldots, J$ e

$$x_0^{(J)}[l] \triangleq \sum_{n=-\infty}^{\infty} x[n] h_0^{(j)}[2^J l - n], \tag{2.51}$$

onde $h_i^{(j)}[n]$ pode ser encontrado no domínio Z por

$$H_0^{(j)}(z) = \prod_{i=0}^{j-1} H_0(z^{2^i}) = H_0^{(j-1)}(z) H_0(z^{2^{j-1}}) \tag{2.52}$$

e

$$H_1^{(j)}(z) = H_1(z^{2^{j-1}}) \prod_{i=0}^{j-2} H_0(z^{2^i}) = H_0^{(j-1)}(z) H_1(z^{2^{j-1}}). \tag{2.53}$$

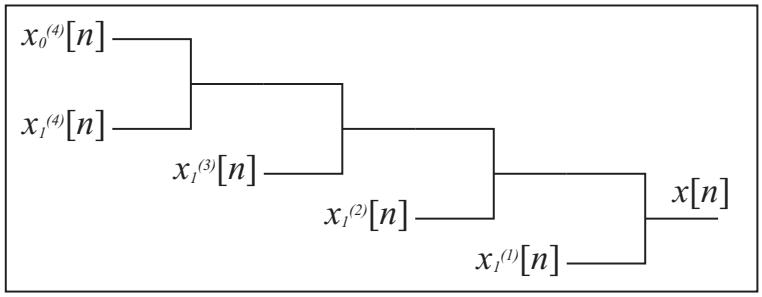


Figura 2.19: Estrutura de banco de filtros para a série wavelet de tempo discreto.

A SWTD para J estágios é representada por

$$x[n] \overset{SW}{\longleftrightarrow} x_1^{(j)}[l], x_0^{(J)}[l].$$

A síntese da SWTD é obtida pela estrutura da Figura 2.19. A equação de síntese fica

$$x[n] = \sum_{j=1}^{J} \sum_{l=-\infty}^{\infty} x_1^{(j)}[l] g_1^{(j)}[n - 2^j l] + \sum_{l=-\infty}^{\infty} x_0^{(J)}[l] g_0^{(J)}[n - 2^J l], \tag{2.54}$$

onde $g_i^{(j)}[n]$ pode ser encontrado no domínio Z por

$$G_0^{(j)}(z) = \prod_{i=0}^{j-1} G_0(z^{2^i}) = G_0^{(j-1)}(z) G_0(z^{2^{j-1}}) \tag{2.55}$$

e

$$G_1^{(j)}(z) = G_1(z^{2^{j-1}}) \prod_{i=0}^{j-2} G_0(z^{2^i}) = G_0^{(j-1)}(z) G_1(z^{2^{j-1}}). \tag{2.56}$$

Wavelets de tempo discreto são seqüências discretas com médias nulas. O sinal analisado é decomposto nas *wavelets de tempo discreto*, $g_1^{(j)}[n]$, e na *função escala de tempo discreto*, $g_0^{(J)}[n]$. As wavelets de análise são $h_1^{(j)}[-n]$. Para $J = 1$, o resultado é a decomposição em sub-bandas dos bancos de filtros.

capítulo 3

Banco de Filtros sobre Corpos Finitos

A proposta deste capítulo é a análise de sinais e sistemas discretos definidos sobre corpos finitos, baseada na transformada Z. O objetivo é definir e encontrar bancos de filtros com reconstrução perfeita e transformadas baseadas nessas estruturas sobre campos de Galois. A primeira ferramenta de análise introduzida é a transformada Z definida sobre corpos finitos. Em seguida são apresentadas condições de reconstrução perfeita para banco de filtros definidos sobre corpos finitos. Outra novidade é a dependência da característica do corpo, p (Apêndice A), com o número de canais, M, na condição de reconstrução perfeita (RP).

3.1 Transformada Z sobre Corpos Finitos

A transformada Z para análise de sinais e sistemas discretos é de grande importância [13]. Banco de filtros e wavelets, definidos sobre os complexos, são analisados no domínio da transformada Z e da transformada de Fourier de tempo discreto [3, 4]. Daí surge a importância de se definir uma transformada Z para seqüências de comprimento arbitrário sobre campos de Galois.

Definição 3.1 (Convergência Indutiva) *Uma série infinita sobre $GF(q)$ converge, no sentido de convergência indutiva, se existe um único elemento em $GF(q)$ que pode satisfazer a igualdade da série.*

Esta é uma definição de convergência introduzida neste trabalho a fim de resolver séries infinitas sobre corpos finitos, sem utilizar uma definição de limite para as mesmas.

Teorema 3.1 *A série geométrica infinita com razão $\alpha \in GF(q)$, $\alpha \neq 0$ e $\alpha \neq 1$, converge indutivamente, e resulta em*

$$\sum_{n=0}^{\infty} \alpha^n = (1-\alpha)^{-1}. \tag{3.1}$$

Demonstração: Supondo que a série converge indutivamente para S, têm-se que

$$\sum_{n=0}^{\infty} \alpha^n = S. \tag{3.2}$$

Multiplicando ambos os membros por α e adicionando a unidade, têm-se

$$1 + \sum_{n=1}^{\infty} \alpha^n = 1 + \alpha S. \tag{3.3}$$

Observa-se que o lado esquerdo da expressão acima é igual a série. assim

$$S = 1 + \alpha S \tag{3.4}$$

e portanto

$$S = (1-\alpha)^{-1} \tag{3.5}$$

é o único valor que a série pode assumir. ■

Definição 3.2 *Dado uma seqüência $x[n] \in GF(q)$, $n \in D \subset \mathbb{Z}$, com comprimento N, a transformada Z dessa seqüência, denotada por $X(z)$, $z \in GF(q^m)$, onde m é um inteiro positivo tal que $q^m - 1 \geq N$, é dada por*

$$X(z) \triangleq \sum_{n \in D} x[n] z^{-n}. \tag{3.6}$$

Teorema 3.2 *A transformada Z inversa é dada por*

$$x[n] = -\sum_{z \in GF(q^m)} X(z) z^n, \tag{3.7}$$

para $n \in D$ e $q^m - 1 \geq N$.

Demonstração: Considere a seqüência $s[n]$, $n \in D$, obtida por

$$s[n] = \sum_{z \in GF(q^m)} X(z) z^n. \tag{3.8}$$

Substituindo $X(z)$ pela definição em 3.6, tem-se

$$s[n] = \sum_{z \in GF(q^m)} \sum_{r \in D} x[r] z^{n-r}. \tag{3.9}$$

Trocando a ordem das somas, pode-se escrever que

$$s[n] = \sum_{r \in D} x[r] \sum_{z \in GF(q^m)} z^{n-r}. \tag{3.10}$$

A última soma pode ser considerada como

$$\sum_{z \in GF(q^m)} z^{n-r} = \sum_{i=0}^{q^m-2} \alpha^{(n-r)i}, \tag{3.11}$$

onde α é um elemento primitivo de $GF(q^m)$, em outras palavras, α tem ordem $q^m - 1$. O somatório é necessariamente zero se $\alpha^{n-r} \neq 1$, isso pode ser mostrado utilizando-se a série geométrica. Quando $\alpha^{n-r} = 1$, então $n \equiv r \ (mod\ q^m - 1)$ e o somatório resulta em $q^m - 1 \equiv -1 (mod\ p)$. Assim, pode-se escrever que

$$\sum_{z \in GF(q^m)} z^{n-r} = - \sum_{l=-\infty}^{\infty} \delta[n - r - l(q^m - 1)]. \tag{3.12}$$

Agora, supondo que $n, r \in D$, então $\max|n - r| = N - 1$ que é menor que $(q^m - 1)$ por hipótese. Com isso a expressão (3.12), para $n, r \in D$, fica

$$\sum_{z \in GF(q^m)} z^{n-r} = \delta[n - r]. \tag{3.13}$$

Utilizando (3.1) em (3.10) chega-se a

$$s[n] = - \sum_{r \in D} x[r] \delta[n - r] = -x[n]. \tag{3.14}$$

Isto significa que

$$x[n] = - \sum_{z \in GF(q^m)} X(z) z^n. \tag{3.15}$$

■

O par ($x[n], X(z)$) é representado por

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

Algumas propriedades dessa transformada linear estão listadas na Tabela 3.1.

Tabela 3.1: Propriedades da Transformada Z sobre Corpos Finitos

Tempo	Domínio Z	Propriedade
$x[n]$	$X(z)$	
$y[n]$	$Y(z)$	
$ax[n] + by[n]$	$aX(z) + bY(z)$	Linearidade
$x[n-d]$	$z^{-d}X(z)$	Deslocamento no tempo
$nx[n]$	$-z\frac{d}{dz}X(z)$	Derivada em Z
$x[n] * y[n]$	$X(z)Y(z)$	Convolução

3.1.1 Transformada Z de Seqüências Semi-Infinitas

A transformada Z de seqüências finitas é simplesmente uma notação polinomial. No caso de seqüências infinitas à direita, isto é, seqüências com início determinado, o comprimento da seqüência N é infinito e $D = \{n_0 \leq n < \infty\}$. A definição continua a mesma, mas a forma de calcular a transformada Z direta e inversa muda. Utiliza-se, nesse caso, o resultado da série geométrica infinita. A seguir, são mostrados cálculo de algumas transformadas Z.

Exemplo 3.1

Considere a seqüência $x[n] = \alpha^n u[n]$, $\alpha \in GF(q)$. Por definição

$$X(z) = \sum_{n=0}^{\infty} \alpha^n z^{-n} = \sum_{n=0}^{\infty} (\alpha z^{-1})^n$$

usando o Teorema 3.1, o resultado é

$$X(z) = (1 - \alpha z^{-1})^{-1} = z(z - \alpha)^{-1}.$$

Observa-se que $X(z)$ contém um zero em $z = 0$ e um pólo em $z = \alpha$. De forma geral, $x[n]$, no regime permanente, contém uma componente com período igual à ordem do pólo α, de sua transformada Z, quando α é um pólo de primeira ordem.

•

Exemplo 3.2

Considere agora a seqüência $x[n] = -\alpha^n u[-n-1]$, $\alpha \in GF(q)$. Esta seqüências é infinita à esquerda. Por definição

$$X(z) = -\sum_{n=-1}^{-\infty} \alpha^n z^{-n},$$

fazendo a mudança de variável $m = -n$,

$$X(z) = -\sum_{m=1}^{\infty}(\alpha^{-1}z)^m = -(1-\alpha^{-1}z)^{-1} + 1 = (1-\alpha z^{-1})^{-1}.$$

Esse resultado é o mesmo do Exemplo 3.1, semelhante ao corpo dos complexos. No caso complexo a diferença das transformadas está na região de convergência. Isso pode ser substituído pela informação do conjunto domínio D, $n \in D$. Para evitar a verificação de soluções com seqüências infinitas à esquerda (não causais) são consideradas apenas seqüências infinitas à direita.

•

Exemplo 3.3

Considere a seqüência $x[n] = n\alpha^n u[n]$, $\alpha \in GF(q)$. Utilizando a propriedade da derivada em Z, em conjunto com o resultado do Exemplo 3.1, têm-se

$$X(z) = -z\frac{d}{dz}\left(\frac{1}{1-\alpha z^{-1}}\right)$$

$$X(z) = \frac{\alpha z^{-1}}{(1-\alpha z^{-1})^2}$$

A seqüência possui um pólo de segunda ordem em $z = \alpha$. O período da seqüência é dado por $N = mmc(M, p)$, onde M é a ordem de α e p é a característica do corpo.

•

Trabalhando unicamente com seqüências à direita, a Tabela 3.2 mostra alguns pares de transformadas Z.

Tabela 3.2: Par Transformada Z de algumas seqüências sobre Corpos Finitos

Seqüência no domínio do "tempo"	Transformada Z
$\delta[n-d]$	z^{-d}
$u[n]$	$\frac{1}{1-z^{-1}}$
$\alpha^n u[n]$	$\frac{1}{1-\alpha z^{-1}}$
$n\alpha^n u[n]$	$\frac{\alpha z^{-1}}{(1-\alpha z^{-1})^2}$

3.1.2 Sinais e Sistemas sobre Corpos Finitos

Sinais e sistemas sobre corpos finitos podem ser analisados através da transformada Z sobre corpos finitos. A representação para um sistema linear e invariante no tempo (LIT) está mostrada na Figura 3.1. Nessa figura, $x[n]$, $y[n]$ e $h[n]$ são seqüências finitas ou infinitas à direita definidas sobre um corpo finito $GF(q)$.

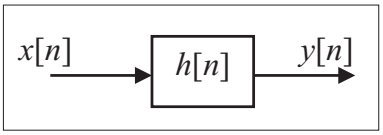


Figura 3.1: Diagrama de um sistema linear e invariante no tempo, caracterizado por sua resposta ao impulso $h[n]$, sobre corpos finitos.

A saída $y[n]$ pode ser calculada através da entrada $x[n]$ por

$$y[n] = \sum_{m=-\infty}^{\infty} x[m]h[n-m] = x[n] * h[n]. \tag{3.16}$$

O operador "$*$" representa a convolução linear e é bem conhecido nos estudos de sinais e sistemas. Aplicando a propriedade da convolução da transformada Z, o resultado, também conhecido, é

$$Y(z) = X(z)H(z), \tag{3.17}$$

onde $Y(z)$, $X(z)$ e $H(z)$ são, respectivamente, as transformadas Z de $y[n]$, $x[n]$ e $h[n]$.

Exemplo 3.4

Considere o sistema da Figura 3.2 sobre $GF(2)$.

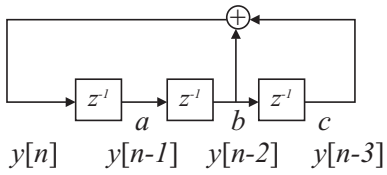


Figura 3.2: Diagrama do sistema linear do exemplo 3.4.

As constantes binárias a, b e c são os valores iniciais da estrutura, quando $n = 0$. A equação que descreve o comportamento do sistema é

$$y[n] = y[n-2] + y[n-3] + (b+c)\delta[n] + (a+b)\delta[n-1] + a\delta[n-2].$$

A transformada Z pode ser utilizada, resultando em

$$Y(z) = z^{-2}Y(z) + z^{-3}Y(z) + (b+c) + (a+b)z^{-1} + az^{-2}.$$

Logo

$$Y(z) = \frac{(b+c) + (a+b)z^{-1} + az^{-2}}{1 + z^{-2} + z^{-3}}.$$

Os pólos de $Y(z)$ pertencem a $GF(8)$, pois o polinômio $\pi(x) = 1 + x + x^3$ é um polinômio primitivo sobre $GF(2)$. Supondo que α é raiz do polinômio $\pi(x)$, pode-se representar $Y(z)$ por

$$Y(z) = \frac{(b+c) + (a+b)z^{-1} + az^{-2}}{(1+\alpha z^{-1})(1+\alpha^2 z^{-1})(1+\alpha^4 z^{-1})}.$$

O sistema pode ser resolvido utilizando-se frações parciais; é possível encontrar A, B e C tais que

$$Y(z) = \frac{A}{(1+\alpha z^{-1})} + \frac{B}{(1+\alpha^2 z^{-1})} + \frac{C}{(1+\alpha^4 z^{-1})}.$$

No domínio do tempo ou da seqüência, tem-se que

$$y[n] = A\alpha^n u[n] + B\alpha^{2n} u[n] + C\alpha^{4n} u[n].$$

Supondo $a = b = 0$ e $c = 1$, $Y(z)$ se reduz a

$$Y(z) = \frac{1}{(1+\alpha z^{-1})(1+\alpha^2 z^{-1})(1+\alpha^4 z^{-1})}.$$

Tabela 3.3: Corpo $GF(8)$, $1 + \alpha + \alpha^3 = 0$

α^∞	0
α^0	1
α^1	α
α^2	α^2
α^3	$1 + \alpha$
α^4	$\alpha + \alpha^2$
α^5	$1 + \alpha + \alpha^2$
α^6	$1 + \alpha^2$

Resolvendo as frações parciais, considerando a Tabela 3.3 de $GF(8)$,

$$A = \frac{1}{(1+\alpha)(1+\alpha^3)} = \alpha^3,$$

$$B = \frac{1}{(1+\alpha^6)(1+\alpha^2)} = \alpha^6$$

e

$$C = \frac{1}{(1+\alpha^4)(1+\alpha^5)} = \alpha^5.$$

Assim

$$y[n] = (\alpha^{n+3} + \alpha^{2n+6} + \alpha^{4n+5})u[n].$$

Verifica-se que $y[n]$ pertence a $GF(2)$ e o período da seqüência é igual a ordem dos pólos, nesse caso igual a 7.

Este esquema é geralmente utilizado para geração de seqüências binárias pseudo aleatórias (Sequências-m [14]) bastante utilizadas em comunicações e criptografia [15, 16].

•

Exemplo 3.5

Considere o calculo da transformada inversa de $X(z)$ dado por

$$X(z) = \frac{1}{1+z^{-2}+z^{-3}}.$$

Os pólos de $X(z)$ estão em $GF(8)$ (exemplo anterior). Isso significa que a seqüência $x[n]$ têm período 7 e pode ser escrita por

$$X(z) = \hat{X}(z)\sum_{n=0}^{\infty} z^{-7n} = \frac{\hat{X}(z)}{1-z^{-7}},$$

onde $\hat{X}(z)$ é a transformada Z de uma seqüência finita. Assim pode-se encontrar $\hat{x}[n]$ obtendo-se $\hat{X}(z)$ e completando os polinômios para formar o denominador desejado, ou seja,

$$X(z) = \frac{1}{(1+z^{-1}+z^{-3})}\frac{(1+z^{-1}+z^{-3})}{(1+z^{-1}+z^{-3})}\frac{(1+z^{-1})}{(1+z^{-1})} = \frac{(1+z^{-1})(1+z^{-2}+z^{-3})}{1+z^{-7}}.$$

Então

$$\hat{X}(z) = (1+z^{-1})(1+z^{-1}+z^{-3}) = 1+z^{-2}+z^{-3}+z^{-4}$$

e

$$\hat{x}[n] = [1\ 0\ 1\ 1\ 1\ 0\ 0],$$

para $n = 0, 1, \ldots, 6$. A seqüência $x[n]$ é dada por

$$x[n] = \sum_{l=0}^{\infty} \hat{x}[n-7l] = [1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ \ldots],$$

para $0 \leq n < \infty$. Esse resultado corresponde à saída do sistema do Exemplo 3.4.

•

Exemplo 3.6

Considere uma seqüência $x[n] \in GF(5)$, com $D = \{0, 1, 2, 3\}$, e transformada Z dada por

$$X(z) = 1 + 2z^{-1} + 4z^{-3}.$$

Obviamente, $x[n] = [1\ 2\ 0\ 4]$, mas será calculado pelo Teorema 3.7. Tem-se

$$x[n] = -\sum_{z \in GF(5)} X(z)z^n = -\sum_{z=1}^{4} X(z)z^n = -X(1) - X(2)2^n - X(3)3^n - X(4)4^n,$$

$$x[n] = 3 + 3^{n+1} (\text{mod } 5),$$

e, para $n \in D$, o resultado segue.

•

3.2 Banco de Filtros de M Canais sobre $GF(p^m)$, p e M Relativamente Primos

A estrutura conhecida como banco de filtros é mostrada na Figura 3.3. Comparando as equações existentes no corpo dos complexos, basta substituir o elemento $e^{-j2\pi/M}$ por um elemento α, de ordem M, de uma extensão do corpo $GF(q)$, na equação do subamostrador. Entretanto, algumas ordens são proibidas para algumas características de corpo.

Teorema 3.3 *Um corpo finito de característica p contém elementos de ordem M se, e somente se, $mdc(M, p) = 1$.*

Demonstração: Suponha que $GF(q)$ tem característica p, então $q = p^m$. Se $mdc(M, p) = 1$, considere o corpo $GF(q^{\phi(M)})$, onde $\phi(.)$ denota a função de Euler; então, $q^{\phi(M)} - 1 \equiv 0(mod\ M)$, pelo teorema de Euler. Isso significa que $M|(q^{\phi(M)} - 1)$ e portanto existe um elemento de ordem M que pertence a $GF(q^{\phi(M)})$ [14]. Por outro lado, se existe um elemento de ordem M, então, existe n tal que $M|(q^n - 1)$, ou seja, $p^{mn-1}p - rM = 1$, e portanto $mdc(M, p) = 1$. ■

Em outras palavras, as estensões de $GF(q)$ contém elementos de qualquer ordem, desde que esta seja relativamente primo com a característica do corpo.

Corolário 3.1 *Em um corpo finito $GF(q)$ de característica p, onde $mdc(p, M) = 1$, as transformadas Z da saída de um subamostrador de M, $X_d(z)$, e do conjunto subamostrador-sobreamostrador de M, $X_s(z)$, podem ser expressas em termos da transformada Z da entrada*

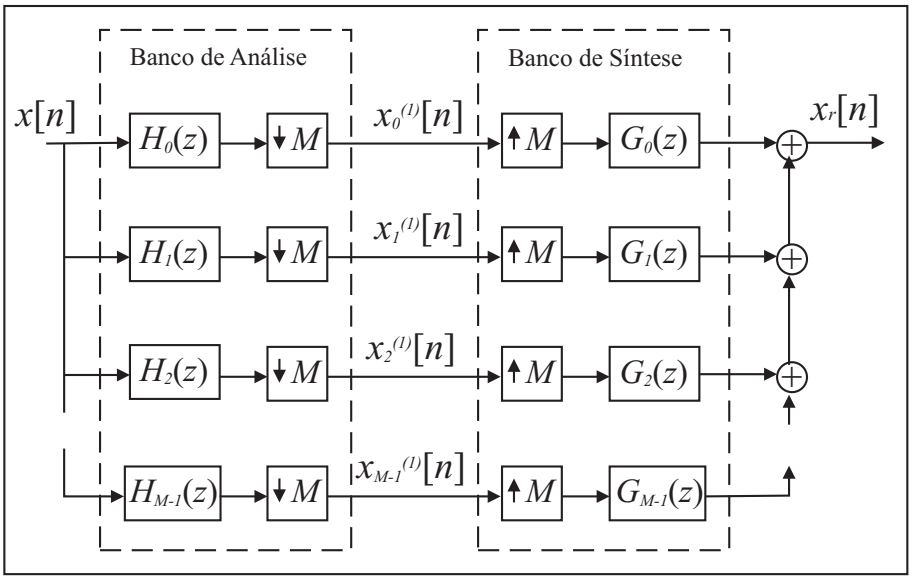


Figura 3.3: Diagrama ilustração de um banco de filtros de M canais sobre corpos finitos. A representação é a mesma do corpo dos reais.

$X(z)$ (Figura 3.4), respectivamente, por

$$X_d(z) = M^{-1}(mod\ p) \sum_{m=0}^{M-1} X(\alpha^m z^{\frac{1}{M}}) \tag{3.18}$$

e

$$X_s(z) = M^{-1}(mod\ p) \sum_{m=0}^{M-1} X(\alpha^m z), \tag{3.19}$$

onde α é um elemento de ordem M de uma extensão de $GF(q)$.

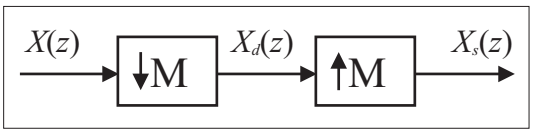


Figura 3.4: Diagrama demonstrando o esquema do subamostrador e o conjunto subamostrador-sobreamostrador.

Demonstração: O Teorema 3.3 garante a existência de um elemento α de ordem M; assim, considere a seqüência

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

Essa seqüência pode ser expressa por

$$s_M[n] = M^{-1}(mod\ p) \sum_{m=0}^{M-1} \alpha^{-mn}. \tag{3.20}$$

Sabe-se que $x_s[n] = s_M[n]x[n]$; usando-se a definição da transformada Z,

$$X_s(z) = M^{-1}(mod\ p) \sum_{n=-\infty}^{\infty} x[n] \sum_{m=0}^{M-1} \alpha^{-mn} z^{-n}, \tag{3.21}$$

$$X_s(z) = M^{-1}(mod\ p) \sum_{m=0}^{M-1} \sum_{n=-\infty}^{\infty} x[n](\alpha^m z)^{-n} \tag{3.22}$$

e

$$X_s(z) = M^{-1}(mod\ p) \sum_{m=0}^{M-1} X(\alpha^m z). \tag{3.23}$$

Observa-se que $x_d[n] = x[Mn] = x_s[Mn]$, assim

$$X_d(z) = \sum_{n=-\infty}^{\infty} x_s[Mn] z^{-n}. \tag{3.24}$$

Fazendo a mudança de variável $Mn = k$,

$$X_d(z) = \sum_{M|k} x_s[k] z^{\frac{-k}{M}}. \tag{3.25}$$

Como $x_s[k] = 0$ se M não divide k, então

$$X_d(z) = \sum_{k=-\infty}^{\infty} x_s[k] z^{\frac{-k}{M}} = X_s(z^{\frac{1}{M}}) \tag{3.26}$$

e está completa a prova. ■

Este resultado é análogo à expressão encontrada na saída do subamostrador e no conjunto subamostrador-sobreamostrador sobre o corpo dos complexos. Vale observar que a saída do sobreamostrador é expressa da mesma forma em qualquer corpo por $X_e(z) = X(z^M)$.

3.2.1 Reconstrução Perfeita

A condição de reconstrução perfeita é importante para o projeto de banco de filtros. Contudo, a mesma depende do corpo e do número de canais. Sobre um corpo $GF(q)$, filtros são simplesmente seqüências ou polinômios, por meio dos quais seqüências sobre $GF(q)$ podem ser analisadas e sintetizadas.

Teorema 3.4 *Para um banco de filtros de M canais sobre um corpo $GF(q)$ de característica p, $mdc(p, M) = 1$, como mostrado na Figura 3.3, $x_r[n] = x[n]$ se a condição de reconstrução perfeita,*

$$\sum_{i=0}^{M-1} H_i(\alpha^m z)G_i(z) = M\delta[m], \tag{3.27}$$

para $m = 0, 1, \ldots, M-1$, é satisfeita.

Demonstração: A prova segue a mesma idéia do corpo dos complexos, para a i-ésima linha da estrutura, chamando a saída do filtro $G_i(z)$ de $y_i[n]$, temos a seguinte equação de saída da linha i:

$$Y_i(z) = G_i(z)(H_i(z)X(z))_s, \tag{3.28}$$

onde $(H_i(z)X(z))_s$ representa a transformada Z da seqüência $h_i[n] * x[n]$ amostrada a cada M valores (resultado da subamostragem seguida por sobreamostragem). Considerando a expressão (3.19),

$$Y_i(z) = G_i(z)M^{-1}(mod\ p) \sum_{m=0}^{M-1} H_i(\alpha^m z)X(\alpha^m z). \tag{3.29}$$

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

$$X_r(z) = \sum_{i=0}^{M-1} Y_i(z) = \tag{3.30}$$

$$M^{-1}(mod\ p) \sum_{i=0}^{M-1} G_i(z) \sum_{m=0}^{M-1} H_i(\alpha^m z)X(\alpha^m z) = \tag{3.31}$$

$$M^{-1}(mod\ p) \sum_{m=0}^{M-1} X(\alpha^m z) \sum_{i=0}^{M-1} H_i(\alpha^m z)G_i(z). \tag{3.32}$$

Substituindo o último somatório pela relação de reconstrução perfeita (3.27), a expressão de $X_r(z)$ se reduz a

$$X_r(z) = M^{-1}(mod\ p) \sum_{m=0}^{M-1} X(\alpha^m z)M\delta[m] = \tag{3.33}$$

$$\sum_{m=0}^{M-1} X(\alpha^m z)\delta[m] = X(z). \tag{3.34}$$

Trazendo para o domínio do tempo, tem-se que $x_r[n] = x[n]$. ■

Existem duas observações importantes sobre essas M equações, a primeira é que $x_r[n] = x[n-d]$ é considerada reconstrução perfeita com retardo d. No caso de $d = 0$, é dito que ocorre reconstrução perfeita ou reconstrução perfeita sem retardo. A segunda observação é que o teorema não fala de existência de banco de filtros.

Para qualquer corpo existem bancos de filtros de M canais, um exemplo é a decomposição polifásica que existe para qualquer corpo. Além disso, é possível obter a condição de reconstrução perfeita para banco de filtros com p canais sobre $GF(p^m)$, p primo. Para isso basta deduzir a equação utilizando $s_p[n] = 1 - n^{p-1}$, a qual é válida pelo pequeno teorema de Fermat [14, 17].

Assumindo que ocorre a condição RP, as equações de análise e de síntese do banco de filtros podem ser obtidas.

Teorema 3.5 *Para um banco de filtros de M canais satisfazendo a condição de reconstrução perfeita, as equações de análise e síntese do banco são, respectivamente,*

$$x_i^{(1)}[l] = \sum_{n=-\infty}^{\infty} x[n] h_i[Ml - n], \tag{3.35}$$

para $i = 0, \ldots, M-1$, e

$$x[n] = \sum_{i=0}^{M-1} \sum_{l=-\infty}^{\infty} x_i^{(1)}[l] g_i[n - Ml], \tag{3.36}$$

onde $h_i[n]$ e $g_i[n]$ são as transformadas Z inversas dos filtros $H_i(z)$ e $G_i(z)$.

Demonstração: A análise é simplesmente uma convolução, seguida por uma subamostragem de M. A síntese é obtida por expansão e convolução, para cada linha do banco de filtros tem-se

$$x_{ie}^{(1)}[n] * g_i[n] = \sum_{l=-\infty}^{\infty} x_i^{(1)}[l] \delta[n - Ml] * g_i[n] = \sum_{l=-\infty}^{\infty} x_i^{(1)}[l] g_i[n - Ml]. \tag{3.37}$$

Somando-se todas as linhas chega-se ao resultado. ■

As equações de análise e síntese do banco de filtros com RP definem uma transformada, de forma que $x[n] \leftrightarrow x_i^{(1)}[l]$. Além disso, os filtros formam bases biortogonais.

Definição 3.3 *O produto interno sobre $GF(q)$ entre duas seqüências, $x[n], y[n] \in GF(q)$, é dado por*

$$\langle x[n], y[n] \rangle \triangleq \sum_{n=-\infty}^{\infty} x[n] y[n] \tag{3.38}$$

Teorema 3.6 (Relação de biortogonalidade) *Num banco de filtros de M canais com reconstrução perfeita, os filtros geram bases biortogonais, isto é*

$$\langle h_i[-n], g_j[n - Ml] \rangle = \delta[i - j]\delta[l], \tag{3.39}$$

para $i, j = 0, \ldots, M - 1$ e $l \in \mathbb{Z}$.

Demonstração: Observando o banco de filtros como transformada, pode-se escolher o valor de $x_i^{(1)}[l]$ e obter $x[n]$ e vice-versa. Considere então a entrada do banco de síntese na linha j igual a $\delta[n - k]$ e zero nas outras linhas. Assim, utilizando a equação de síntese (3.36) com $x_i^{(1)}[l] = \delta[l - k]\delta[i - j]$, o resultado é $x[n] = g_j[n - Mk]$. Utilizando agora a equação de análise (3.35), chega-se a

$$x_i^{(1)}[l] = \sum_{n=-\infty}^{\infty} g_j[n - Mk]h_i[Ml - n] = \langle g_j[n - Mk], h_i[Ml - n] \rangle, \tag{3.40}$$

que deve ser igual ao valor inicial, isto é

$$\langle g_j[n - Mk], h_i[Ml - n] \rangle = \delta[l - k]\delta[i - j], \tag{3.41}$$

fazendo $l = 0$ e mudanças de variáveis chega-se ao resultado. ■

Isso significa que RP implica em biortogonalidade. Isso acontece também em banco de filtros sobre o corpo dos reais.

Uma situação particular ocorre quando $g_i[n] = \sigma h_i[-n]$. Nessas condições a equação (3.39) fica

$$\langle g_i[n], g_j[n - Ml] \rangle = \sigma\delta[i - j]\delta[l], \tag{3.42}$$

e é dito que os filtros $g_i[n]$ ou $h_i[n]$ formam bases *ortogonais*.

Quando $\sigma = 1$, é dito que as bases são *ortonormais* e a equação (3.42) fica

$$\langle g_i[n], g_j[n - Ml] \rangle = \delta[i - j]\delta[l]. \tag{3.43}$$

3.3 Banco de Filtros de Dois Canais sobre $GF(p^m)$ com p Ímpar

O banco de filtro mais utilizado é o de dois canais ($M = 2$), mostrado na Figura 3.5, por sua facilidade de projeto e por sua interpretação sobre o corpo dos reais, onde o sinal é divido em partes de baixa e alta freqüência. Em corpos finitos, a interpretação de baixa ou alta freqüência é perdida. Em compensação, a implementação pode ser realizada livre do ruído computacional, que ocorre quando o corpo dos reais é "implementado" em máquinas digitais através da aritmética de ponto flutuante [13].

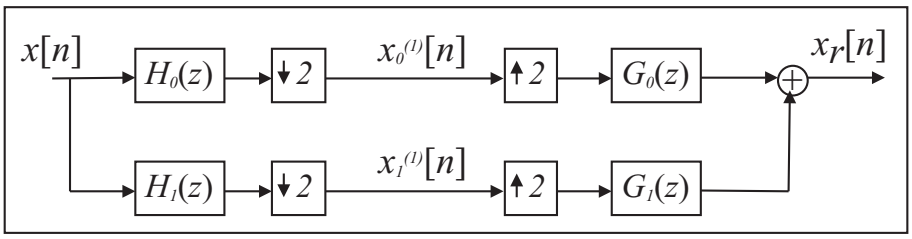


Figura 3.5: Diagrama ilustração de um banco de filtros de dois canais.

Um corolário que decorre do Teorema 3.4 é que quando o corpo tem característica p ímpar, a condição RP do teorema para $M = 2$ pode ser utilizada.

Corolário 3.2 *Em um corpo $GF(q)$ de característica ímpar, a relação de reconstrução perfeita para dois canais é*

$$\begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix} \begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \begin{bmatrix} 2z^{-d} \\ 0 \end{bmatrix}. \tag{3.44}$$

Demonstração: Decorre diretamente do Teorema 3.4, fazendo $M = 2$, $\alpha = -1$, e colocando as duas equações na forma matricial. ■

A equação é a mesma para banco de filtros sobre os complexos, dessa forma, todas as técnicas utilizadas para projeto, tais como o *filtro produto* $P(z)$ e a definição da *matriz modulação* $H_m(z)$, podem ser utilizadas também para essa situação.

3.3.1 Projeto do Banco de Filtros com p Ímpar

Utilizando o Corolário 3.2, é possível obter os filtros de síntese, $G_0(z)$ e $G_1(z)$, através dos filtros de análise, $H_0(z)$ e $H_1(z)$, invertendo a matriz. Definindo

$$H_m^T(z) \triangleq \begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix} \tag{3.45}$$

e

$$\Delta(z) \triangleq det[H_m(z)] = det[H_m^T(z)], \tag{3.46}$$

pode-se escrever

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \frac{1}{\Delta(z)} \begin{bmatrix} H_1(-z) & -H_1(z) \\ -H_0(-z) & H_0(z) \end{bmatrix} \begin{bmatrix} 2z^{-d} \\ 0 \end{bmatrix} \tag{3.47}$$

e

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \frac{2z^{-d}}{\Delta(z)} \begin{bmatrix} H_1(-z) \\ -H_0(-z) \end{bmatrix}. \tag{3.48}$$

O polinômio $\Delta(z)$ satisfaz $\Delta(z) = -\Delta(-z)$, o que significa que ele têm apenas potências ímpares de z^{-1}. Uma situação simples para encontrar filtros FIR é forçar $\Delta(z) = 2z^{-l}$ com l ímpar. Escolhendo $d = 0$, têm-se que

$$G_0(z) = z^l H_1(-z) \tag{3.49}$$

e

$$G_1(z) = -z^l H_0(-z) \tag{3.50}$$

Substituindo no Corolário 3.2, a segunda equação é automaticamente satisfeita. Entretanto, a primeira equação fica

$$H_0(z)G_0(z) + H_0(-z)G_0(-z) = 2. \tag{3.51}$$

Definindo o filtro produto $P(z)$ como

$$P(z) \triangleq H_0(z)G_0(z), \tag{3.52}$$

e substituindo em (3.51), vem

$$P(z) + P(-z) = 2. \tag{3.53}$$

Pela equação (3.53), observa-se que $P(z)$ só têm potências ímpares de z^{-1} e o termo independente é igual a unidade.

Proposição 3.1 *Método de projeto de banco de filtros FIR de dois canais sobre $GF(p^m)$ com p ímpar:*

- *Escolher um filtro $P(z)$ satisfazendo (3.53);*
- *Fatorar $P(z)$ em $H_0(z)G_0(z)$;*
- *Utilizar as equações*

$$H_1(z) = -z^{-l} G_0(-z) \tag{3.54}$$

e

$$G_1(z) = -z^l H_0(-z), \tag{3.55}$$

com l ímpar, para encontrar $H_1(z)$ e $G_1(z)$.

Observa-se que estes filtros, diferentemente dos projetados sobre o corpo dos complexos, não apresentam uma classificação em passa baixa ou passa alta. Além disso, este em método bem conhecido em banco de filtros sobre o corpo dos reais [4]. Pode-se utilizar também outros métodos de projeto, derivados do corpo dos reais, como é mostrado no próximo exemplo.

Exemplo 3.7

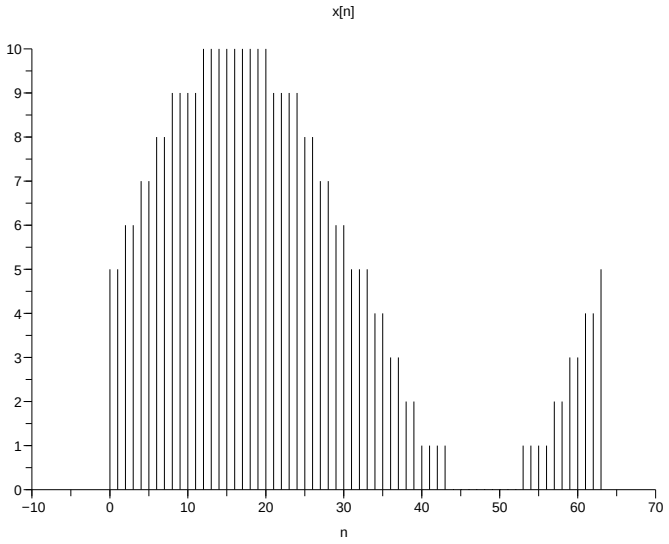


Figura 3.6: A seqüência de entrada $x[n]$ do Exemplo 3.7.

Considere o corpo $GF(11)$; escolhendo-se o filtro produto $P(z)$ da forma

$$P(z) = (1 + z^{-1})^2(1 + z)^2(az + b + az^{-1}),$$

o resultado é

$$P(z) = az^3 + (4a + b)z^2 + (7a + 4b)z + (8a + 6b) + (7a + 4b)z^{-1} + (b + 4a)z^{-2} + az^{-3}.$$

Para que $P(z)$ satisfaça (3.53), os coeficientes de z^2 e z^{-2} devem ser zero e o termo independente igual a 1. Assim

$$(4a + b) \equiv 0(mod\ 11)$$

e

$$(8a + 6b) \equiv 1(mod\ 11).$$

A solução é

$$a = 2,\ b = 3.$$

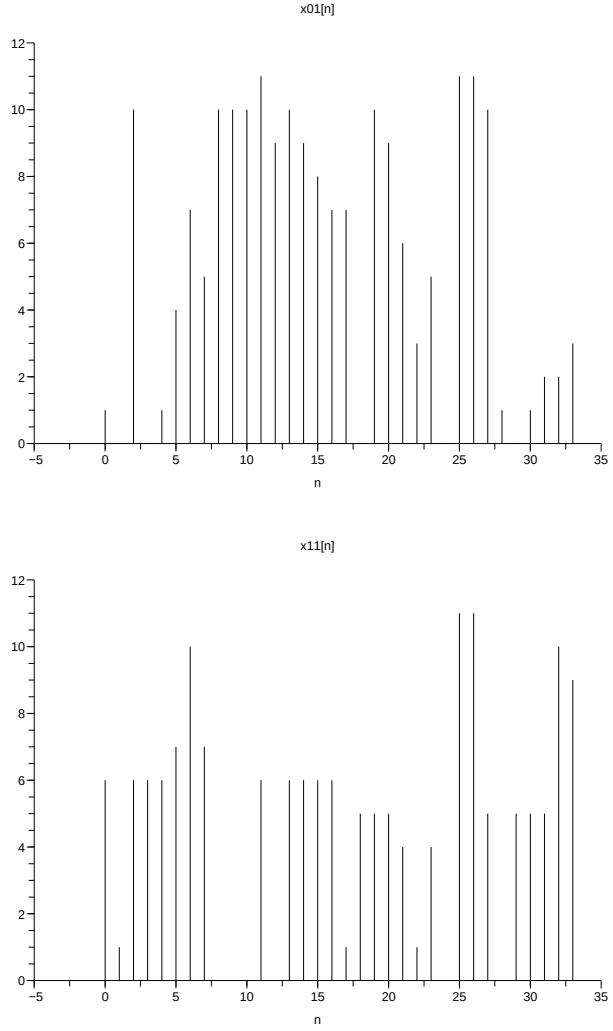


Figura 3.7: As seqüências de saída, $x_0^{(1)}[n]$ e $x_1^{(1)}[n]$, do Exemplo 3.7.

Dessa forma

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

O último polinômio pode ser fatorado em $GF(11)$, resultando em

$$P(z) = (1 + z^{-1})^2(1 + z)^2 8(1 + 3z)(1 + 3z^{-1}).$$

Escolhendo a fatoração

$$H_0(z) = 9(1 + z^{-1})^2(1 + 3z^{-1}) = 9 + z^{-1} + 8z^{-2} + 5z^{-3}$$

e

$$G_0(z) = 7(1 + z)^2(1 + 3z) = 7 + 2z + 5z^2 + 10z^3,$$

e escolhendo $l = 3$, têm-se que

$$H_1(z) = -z^{-3}G_0(-z) = 10 + 6z^{-1} + 2z^{-2} + 4z^{-3}$$

e

$$G_1(z) = -z^3 H_0(-z) = 5 + 3z + z^2 + 2z^3.$$

Esse banco de filtros é similar ao banco encontrado utilizando-se a construção de Daubechies D_2 para wavelets ortogonais [3].

Na estrutura da Figura 3.5, considere a sequência de entrada

$$x[n] = ROUND\{5[1 + sen(2\pi n/64)]\},$$

para $n = 0, \ldots, 63$. A função $ROUND(.)$ representa um arredondamento para um valor inteiro e a função $sen(.)$ representa a função seno, definida sobre os reais. Contudo, $x[n] \in GF(11)$ (Figura 3.6) e assim, pode ser analisado pelo banco de filtros.

As saídas, $x_0^{(1)}[n]$ e $x_1^{(1)}[n]$, estão mostradas na Figura 3.7. Duas observações podem ser feitas. A primeira é que a taxa de transmissão dos sinais de saída é duas vezes menor que a do sinal de entrada, equivalente a operação inversa do espalhamento espectral. A segunda é que os sinais de saída não têm semelhança com o sinal de entrada, o que sugere aplicações com segurança de dados.

Por fim, o sinal de entrada pode ser recuperado utilizando-se os filtros causais

$$\tilde{G}_0(z) = z^{-3}G_0(z) = 10 + 5z^{-1} + 2z^{-1} + 7z^{-3}$$

e

$$\tilde{G}_1(z) = z^{-3}G_1(z) = 2 + z^{-1} + 3z^{-2} + 5z^{-3}.$$

Isto provoca um atraso na saída recuperada, mas é uma boa sugestão para implementação em ferramentas tipo SCILAB e MATLAB. A saída recuperada por estes filtros está mostrada na Figura 3.8.

•

3.4 Implementação Polifásica

A implementação polifásica pode ser utilizada em corpos finitos. Considere a implementação polifásica do banco de análise mostrada na Figura 3.9. A decomposição transforma as

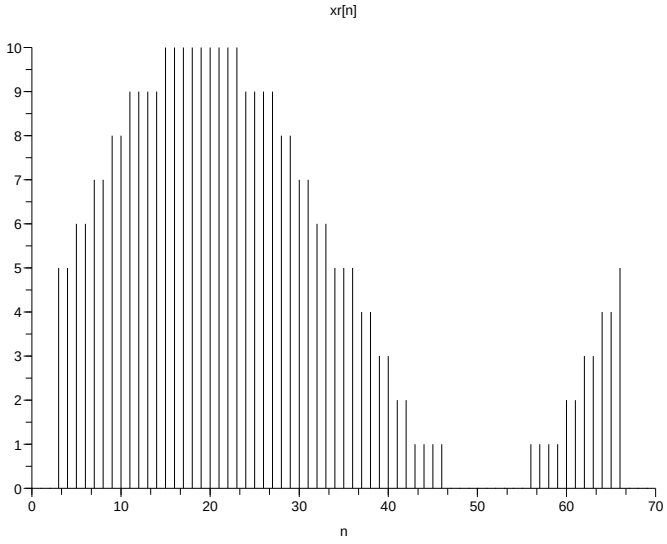


Figura 3.8: A seqüência recuperada a partir de $x_0^{(1)}[n]$ e $x_1^{(1)}[n]$ utilizando versões causais dos filtros de síntese do Exemplo 3.7.

duas seqüências de entrada, $x_0[n]$ e $x_1[n]$ que são componentes polifásica tipo II da entrada $x[n]$, nas seqüências de saída do banco, $x_0^{(1)}[n]$ e $x_1^{(1)}[n]$. No domínio da variável z, tem-se

$$\begin{bmatrix} H_{00}(z) & H_{01}(z) \\ H_{10}(z) & H_{11}(z) \end{bmatrix} \begin{bmatrix} X_0(z) \\ X_1(z) \end{bmatrix} = \begin{bmatrix} X_0^{(1)}(z) \\ X_1^{(1)}(z) \end{bmatrix}, \tag{3.56}$$

onde $H_{00}(z)$ e $H_{01}(z)$ são decomposições polifásica tipo I de $H_0(z)$ e os filtros $H_{10}(z)$ e $H_{11}(z)$ são decomposições polifásica tipo I de $H_1(z)$.

Definindo a matriz polifásica de análise $H_p(z)$ por

$$H_p(z) \triangleq \begin{bmatrix} H_{00}(z) & H_{01}(z) \\ H_{10}(z) & H_{11}(z) \end{bmatrix} \tag{3.57}$$

e os vetores $X_p(z)$ e $X^{(1)}(z)$, respectivamente, por

$$X_p(z) \triangleq \begin{bmatrix} X_0(z) \\ X_1(z) \end{bmatrix} \tag{3.58}$$

e

$$X^{(1)}(z) \triangleq \begin{bmatrix} X_0^{(1)}(z) \\ X_1^{(1)}(z) \end{bmatrix}, \tag{3.59}$$

a equação (3.56) pode ser reescrita simplesmente por

$$X^{(1)}(z) = H_p(z)X_p(z). \tag{3.60}$$

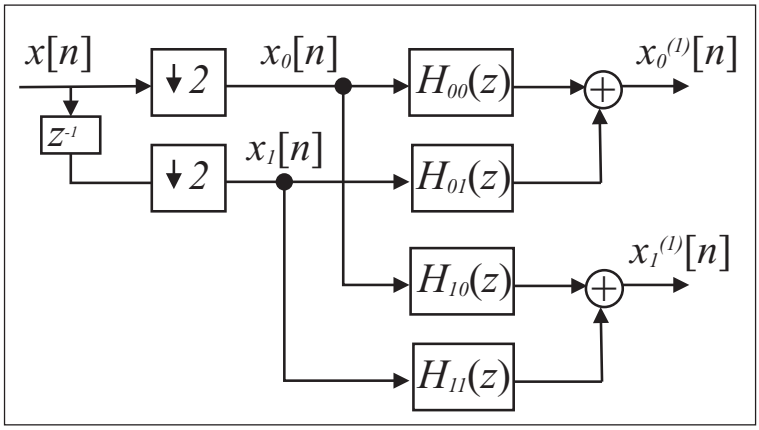


Figura 3.9: Diagrama da implementação polifásica do banco de análise.

O banco de síntese também pode ser implementado de forma polifásica, como mostra a Figura 3.10.

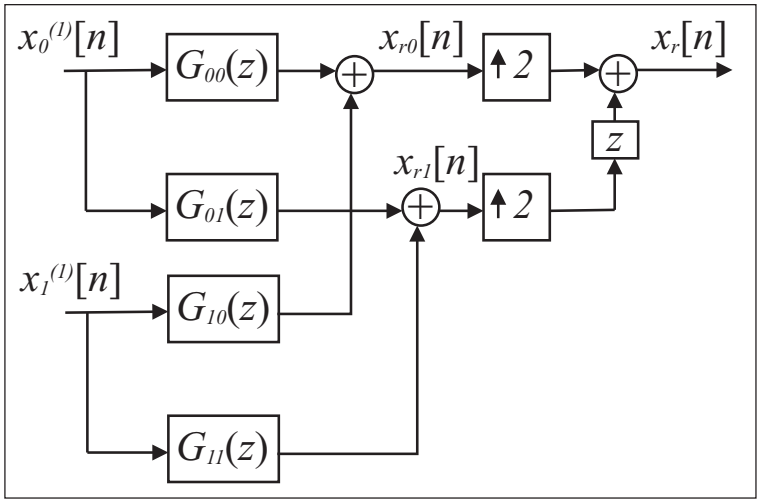


Figura 3.10: Diagrama da implementação polifásica do banco de síntese.

A equação de síntese é dada por

$$\begin{bmatrix} X_{r0}(z) \\ X_{r1}(z) \end{bmatrix} = \begin{bmatrix} G_{00}(z) & G_{10}(z) \\ G_{01}(z) & G_{11}(z) \end{bmatrix} X^{(1)}(z). \tag{3.61}$$

onde $G_{00}(z)$ e $G_{01}(z)$ são decomposições polifásica tipo II de $G_0(z)$ e os filtros $G_{10}(z)$ e $G_{11}(z)$ são decomposições polifásica tipo II de $G_1(z)$.

Definindo a matriz polifásica de análise $G_p(z)$ por

$$G_p(z) \triangleq \begin{bmatrix} G_{00}(z) & G_{10}(z) \\ G_{01}(z) & G_{11}(z) \end{bmatrix}, \tag{3.62}$$

e observando a reconstrução perfeita, isto é

$$\begin{bmatrix} X_{r0}(z) \\ X_{r1}(z) \end{bmatrix} = X_p(z), \tag{3.63}$$

pode-se então escrever que

$$X_p(z) = G_p(z)X^{(1)}(z). \tag{3.64}$$

A equação de síntese é, portanto,

$$X(z) = [1 \quad z^{-1}]X_p(z^2) = [1 \quad z^{-1}]G_p(z^2)X^{(1)}(z^2). \tag{3.65}$$

Utilizando (3.60) para expressar $X^{(1)}(z)$, a equação (3.64) fica

$$X_p(z) = G_p(z)H_p(z)X_p(z). \tag{3.66}$$

Isto ocorre quando

$$G_p(z)H_p(z) = I_2. \tag{3.67}$$

É possível encontrar $H_0(z)$ e $H_1(z)$ a partir de $H_p(z)$ e vice versa. O mesmo vale para os filtros de síntese e a matriz polifásica de síntese. A equação (3.67) é conhecida como *a condição de reconstrução perfeita na forma polifásica*, a qual implica também na relação de biortogonalidade. Estruturas na forma polifásica são mais eficientes em termos de complexidade multiplicativa [13].

Teorema 3.7 *Se as matrizes polifásicas de análise e síntese de um banco de filtros, $H_p(z)$ e $G_p(z)$ respectivamente, satisfazem a*

$$G_p(z) = H_p^{-1}(z) = \sigma H_p^T(z^{-1}), \tag{3.68}$$

então o banco de filtros satisfaz a condição de reconstrução perfeita com filtros ortogonais. Particularmente para $\sigma = 1$, os filtros são ortonormais.

Demonstração: A primeira igualdade garante a reconstrução perfeita como mostrado anteriormente. Sabe-se que o filtro de análise $H_i(z)$ pode ser obtido através de $H_p(z)$ por

$$H_i(z) = H_{i0}(z^2) + z^{-1}H_{i1}(z^2), \tag{3.69}$$

assim como o filtro $G_i(z)$ pode ser obtido através de $G_p(z)$ por

$$G_i(z) = G_{i0}(z^2) + zG_{i1}(z^2). \tag{3.70}$$

Entretanto, a segunda igualdade implica que

$$\begin{bmatrix} G_{00}(z) & G_{01}(z) \\ G_{10}(z) & G_{11}(z) \end{bmatrix} = \sigma \begin{bmatrix} H_{00}(z^{-1}) & H_{01}(z^{-1}) \\ H_{10}(z^{-1}) & H_{11}(z^{-1}) \end{bmatrix}. \tag{3.71}$$

Com isso, pode-se escrever que

$$G_i(z) = \sigma[H_{i0}(z^{-2}) + zH_{i1}(z^{-2})] = \sigma H_i(z^{-1}), \tag{3.72}$$

o que significa que

$$g_i[n] = \sigma h_i[-n], \tag{3.73}$$

e a equação (3.39) se torna a equação (3.42) como mostrado anteriormente. Fazendo $\sigma = 1$, o resultado é (3.43) e a demonstração está completa. ■

A equação (3.68) pode ser utilizada para a construção de banco de filtros ortogonais, utilizando estruturas reticuladas concatenadas. A equação (3.68), com $\sigma = 1$, pode ser reescrita como

$$H_p(z)H_p^T(z^{-1}) = I_2. \tag{3.74}$$

As matrizes que satisfazem a equação (3.74) são chamadas de *Paraunitárias* [4].

3.4.1 Estruturas Reticuladas

Estruturas reticuladas podem ser utilizadas para construir bancos de filtros com reconstrução perfeita [3],[4]. Uma estrutura reticulada é a implementação de uma matriz transformação 2x2 com coeficientes constantes. Na Figura 3.11 está mostrado uma estrutura reticulada que implementa a matriz A com coeficientes a_{ij}.

Considere a *matriz retardo*, $\Lambda(z)$, definida por

$$\Lambda(z) \triangleq \begin{bmatrix} 1 & 0 \\ 0 & z^{-1} \end{bmatrix}. \tag{3.75}$$

Então, pode-se construir a matriz polifásica de análise $H_p(z)$ por

$$H_p(z) = A_L\Lambda(z)A_{L-1}\Lambda(z)\ldots A_1\Lambda(z)A_0, \tag{3.76}$$

onde as matrizes A_k, $k = 0, \ldots, L$, são matrizes inversíveis. A implementação desta estrutura está mostrada na Figura 3.12.

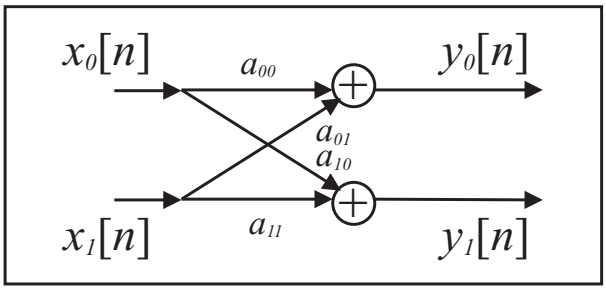


Figura 3.11: Diagrama da estrutura reticulada de uma matriz A com coeficientes a_{ij}.

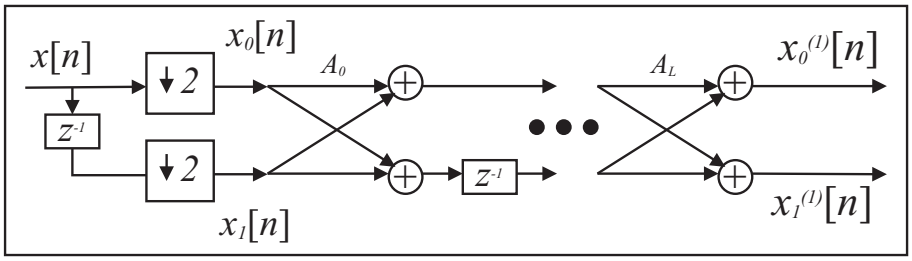


Figura 3.12: Diagrama da implementação do banco de filtros de análise com estruturas reticuladas.

Com isso, a matriz polifásica de síntese $G_p(z)$ pode ser obtida por

$$G_p(z) = H_p^{-1}(z) = A_0^{-1}\Lambda(z^{-1})A_1^{-1}\Lambda(z^{-1})\ldots A_{L-1}^{-1}\Lambda(z^{-1})A_L^{-1}. \tag{3.77}$$

A implementação do banco de síntese utilizando estruturas reticuladas está mostrada na Figura 3.13. Isso constitui outra possibilidade para construção de banco de filtros com reconstrução perfeita. Além disso, se $A_k^{-1} = A_k^T$, $k = 0, \ldots, L$, então a relação $H_p(z) = G_p^T(z^{-1})$ é satisfeita e os filtros são ortonormais.

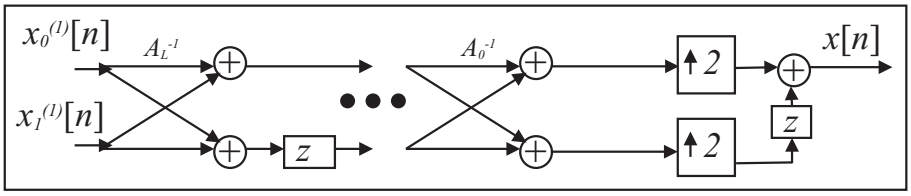


Figura 3.13: Diagrama da implementação do banco de filtros de síntese com estruturas reticuladas.

Exemplo 3.8

Considere o corpo $GF(7)$. As matrizes U_m da forma

$$U_m \triangleq \begin{bmatrix} \cos_k(m) & -\text{sen}_k(m) \\ \text{sen}_k(m) & \cos_k(m) \end{bmatrix}, \tag{3.78}$$

onde $\cos_k(.)$ e $\text{sen}_k(.)$ representam funções k-trigonométricas sobre $GF(7)$ com $\zeta = 2 + j2$ [6], são unitárias. Isto é $U_m^{-1} = U_m^T$, análogo a matrizes unitárias no corpo dos reais.

Dessa forma, essas matrizes podem ser utilizadas para projeto de banco de filtros sobre corpos de característica ímpar com filtros ortonormais.

Considerando

$$H_p(z) = U_{m1}\Lambda(z)U_{m2},$$

e escolhendo $k = 1$, $m1 = 1$ e $m2 = 3$ a matriz polifásica de análise fica

$$H_p(z) = \begin{bmatrix} 2 & -2 \\ 2 & 2 \end{bmatrix} \Lambda(z) \begin{bmatrix} 5 & -2 \\ 2 & 5 \end{bmatrix},$$

que resulta em

$$H_p(z) = \begin{bmatrix} 3 + 3z^{-1} & 3 + 4z^{-1} \\ 3 + 4z^{-1} & 3 + 3z^{-1} \end{bmatrix}.$$

Os filtros são

$$H_0(z) = 3 + 3z^{-1} + 3z^{-2} + 4z^{-3}$$

e

$$H_1(z) = 3 + 3z^{-1} + 4z^{-2} + 3z^{-3}.$$

Os filtros de síntese podem ser obtidos por $G_i(z) = H_i(z^{-1})$ e a matriz polifásica de síntese por $G_p(z) = H_p^T(z^{-1})$. Os filtros constituem bases ortonormais das seqüências de $GF(7)$, e a matriz polifásica é paraunitária.

•

3.5 Bancos de Filtros Estruturados em Árvores

É possível construir novas estruturas cascateando adequadamente banco de filtros com reconstrução perfeita. Nesse contexto será utilizada a representação em árvores para banco de filtros. A Figura 3.14 mostra a representação em árvore de um banco de análise e a Figura 3.15 mostra a representação de um banco de síntese, ambos de dois canais.

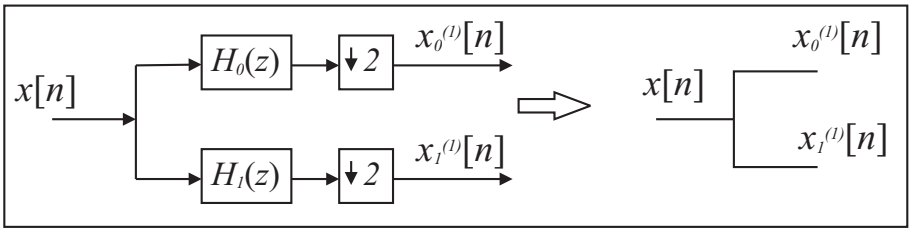


Figura 3.14: Representação em árvore do banco de filtros de análise.

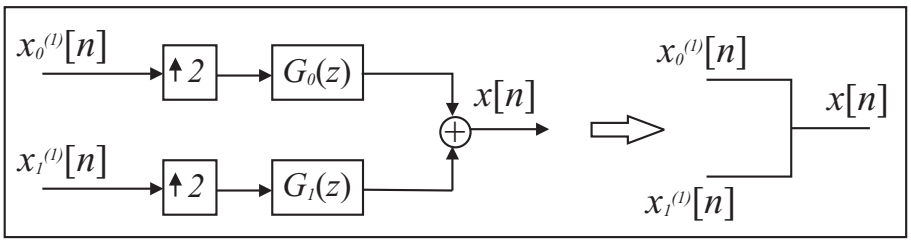


Figura 3.15: Representação em árvore do banco de filtros de síntese.

Essas estruturas em árvore podem ser utilizadas para gerar banco de filtros com multicanais, para criação de novas transformadas e para análise multirresolução, além de várias aplicações derivadas dessas como codificação de canal e criptografia. Dependendo da aplicação, algumas estruturas podem ser valiosas.

Em particular, a transformada wavelet e a transformada de Fourier de curta duração, ambas sobre corpos finitos, são derivadas a partir de estruturas em árvore para banco de filtros. A diferença entre elas é a forma de estruturação das árvores.

3.5.1 Transformada Wavelet sobre Corpos Finitos

A *transformada wavelet sobre corpos finitos* (TWCF) é análoga a série wavelet de tempo discreto e também pode ser chamada de *série wavelet sobre corpos finitos*. Essa transformada é implementada a partir da estrutura em árvore logarítmica com banco de filtros de dois canais. Um exemplo com quatro estágios é mostrado na Figura 3.16.

As saídas do banco de filtros são os coeficientes da TWCF. Cada banco de filtro constitui um estágio j. O sinal é analisado até o estágio J. Existe uma componente $x_1^{(j)}[l]$ para cada estágio j e no estágio J existe uma componente adicional, $x_0^{(J)}[l]$, que representa o restante das componentes dos estágios subsequentes. A componente adicional serve para limitar o número de estágios e componentes na análise.

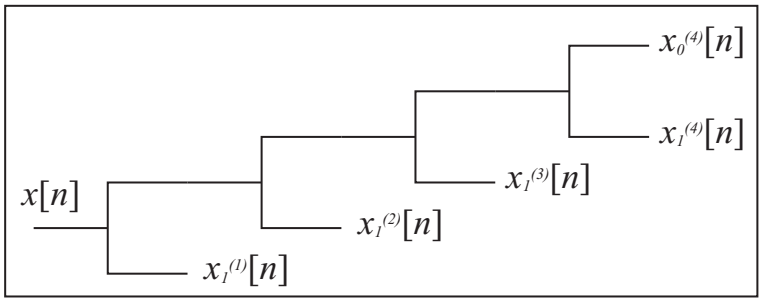


Figura 3.16: Exemplo de uma estrutura em árvore para transformada wavelet sobre corpos finitos com quatro estágios.

O sinal analisado pode ser recuperado utilizando a estrutura em árvore inversa à da análise. Um exemplo é mostrado na Figura 3.17.

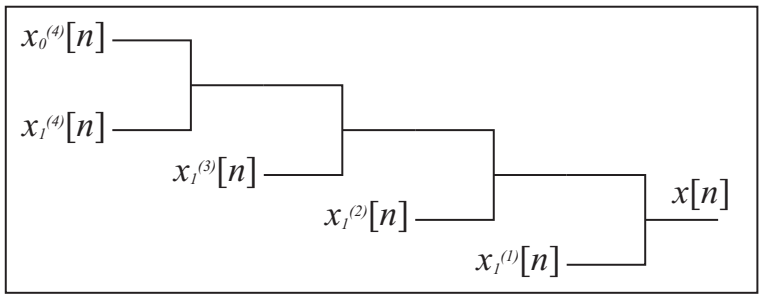


Figura 3.17: Estrutura em árvore para a transformada wavelet inversa sobre corpos finitos com quatro estágios.

Seja uma seqüência $x[n] \in GF(q)$, $n \in \mathbb{Z}$. A transformada wavelet de corpos finito de $x[n]$ é dada por

$$x_1^{(j)}[l] \triangleq \sum_{n=-\infty}^{\infty} x[n] h_1^{(j)}[2^j l - n], \tag{3.79}$$

para $j = \{1, \ldots, J\}$, e

$$x_0^{(J)}[l] \triangleq \sum_{n=-\infty}^{\infty} x[n] h_0^{(J)}[2^J l - n], \tag{3.80}$$

com $l \in \mathbb{Z}$.

A transformada wavelet inversa é dada por

$$x[n] = \sum_{j=1}^{J} \sum_{l=-\infty}^{\infty} x_1^{(j)}[l] g_1^{(j)}[n - 2^j l] + \sum_{l=-\infty}^{\infty} x_0^{(J)}[l] g_0^{(J)}[n - 2^J l]. \tag{3.81}$$

A transformada wavelet com J estágios é representada por

$$x[n] \overset{W}{\longleftrightarrow} x_1^{(j)}[l], x_0^{(J)}[l]. \tag{3.82}$$

As seqüências $h_i^{(j)}[n], g_i^{(j)}[n] \in GF(q)$ são obtidas em suas transformadas Z, $H_i^{(j)}(z)$ e $G_i^{(j)}(z)$, através da iteração entre os filtros $H_i(z)$ e $G_i(z)$ do banco de filtros da estrutura em árvore. O sinal analisado é decomposto em ondas deslocadas sobre $GF(q)$, $g_1^{(j)}[n]$ e $g_0^{(J)}[n]$, $j = \{1, \ldots, J\}$, que representam *wavelets* sobre corpos finitos.

Para demonstrar a equação de análise da transformada, utiliza-se a primeira identidade nobre na estrutura em árvore da Figura 3.16 para colocar todos os subamostradores à direita. A estrutura em árvore logarítmica fica equivalente ao esquema da Figura 3.18.

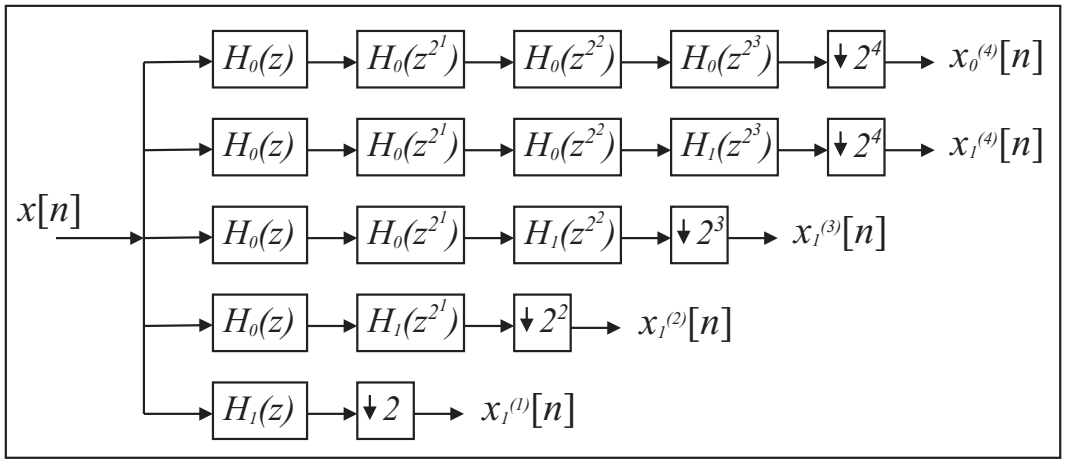


Figura 3.18: Banco de filtros para a transformada wavelet, após a utilização da primeira identidade nobre. Um exemplo com quatro estágios.

A saída de cada estágio j é equivalente à aplicação de um filtro, definido como $H_1^{(j)}(z)$, seguido de uma compressão de 2^j. Observa-se que

$$H_1^{(j)}(z) = H_0(z)H_0(z^2)H_0(z^{2^2}) \ldots H_0(z^{2^{j-2}})H_1(z^{2^{j-1}}). \tag{3.83}$$

O último filtro, definido como $H_0^{(J)}(z)$, é dado por

$$H_0^{(J)}(z) = H_0(z)H_0(z^2)H_0(z^{2^2}) \ldots H_0(z^{2^{J-2}})H_0(z^{2^{J-1}}). \tag{3.84}$$

Essas equações podem ser expressas simplesmente pela definição da equação recursiva

$$H_i^{(j)}(z) \triangleq H_0^{(j-1)}(z)H_i(z^{2^{j-1}}), \tag{3.85}$$

com

$$H_0^{(0)}(z) \triangleq 1. \tag{3.86}$$

As seqüências $h_i^{(j)}[n]$ da transformada wavelet são obtidas por

$$h_i^{(j)}[n] \overset{\mathbf{Z}}{\longleftrightarrow} H_i^{(j)}(z). \tag{3.87}$$

Essa é a relação entre as wavelets de análise e os filtros de análise de bancos de filtros com reconstrução perfeita. Assim, os coeficientes da transformada wavelet, $x_i^{(j)}[l]$, são obtidos através da convolução, $x[n] * h_i^{(j)}[n]$, seguido de uma compressão de 2^j.

Para demonstrar a equação de síntese, ou transformada wavelet inversa, é necessário arrumar a estrutura em árvores da Figura 3.17, utilizando a segunda identidade nobre para colocar os sobreamostradores à esquerda. O resultado está mostrado na Figura 3.19.

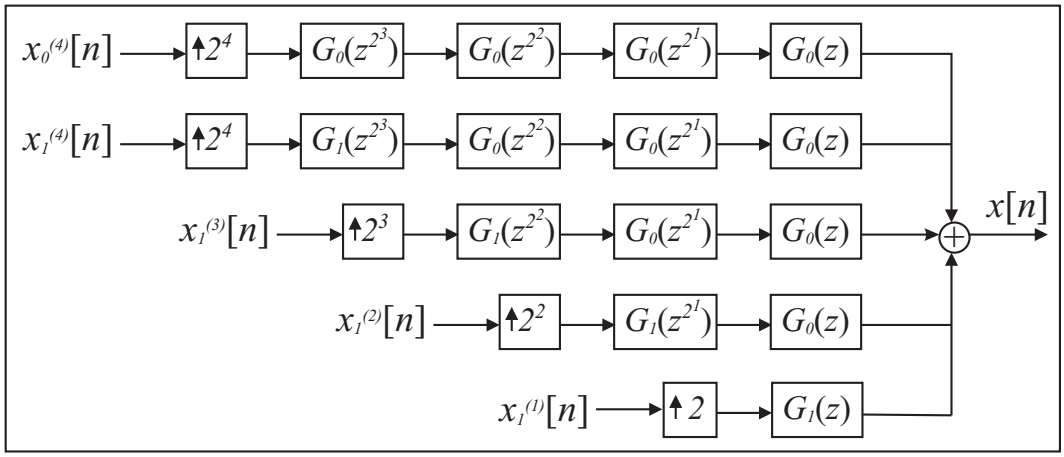


Figura 3.19: Banco de filtros para a transformada wavelet inversa, após a utilização da segunda identidade nobre. Um exemplo com quatro estágios.

Os filtros, após a expansão de 2^j do estágio j, são definidos como $G_1^{(j)}(z)$. O ultimo é definido como $G_0^{(J)}(z)$. Os filtros podem ser obtidos através da equação recursiva

$$G_i^{(j)}(z) \triangleq G_0^{(j-1)}(z) G_i(z^{2^{j-1}}), \tag{3.88}$$

com

$$G_0^{(0)}(z) \triangleq 1. \tag{3.89}$$

Assim, os filtros wavelets de síntese $g_i^{(j)}[n]$ (ou simplesmente *wavelets de síntese*) são obtidas por

$$g_i^{(j)}[n] \overset{\mathbf{Z}}{\longleftrightarrow} G_i^{(j)}(z). \tag{3.90}$$

A saída de cada estágio, $y_j[n]$, é dada por

$$y_j[n] = (\sum_{l=-\infty}^{\infty} x_1^{(j)}[l]\delta[n-2^j l]) * g_1^{(j)}[n] = \sum_{l=-\infty}^{\infty} x_1^{(j)}[l] g_1^{(j)}[n-2^j l], \tag{3.91}$$

e a saída da linha adicional do último estágio $\bar{y}[n]$ é dada por

$$\bar{y}[n] = (\sum_{l=-\infty}^{\infty} x_0^{(J)}[l]\delta[n-2^J l]) * g_0^{(J)}[n] = \sum_{l=-\infty}^{\infty} x_1^{(j)}[l] g_0^{(J)}[n-2^J l]. \tag{3.92}$$

Somando-as, o resultado é a equação de síntese (3.81).

Teorema 3.8 (Biortogonalidade) *As wavelets de análise $h_1^{(j)}[n]$ e a seqüência de escala de análise $h_0^{(J)}[n]$ formam bases biortogonais em relação às wavelets de síntese $g_1^{(j)}[n]$ e a seqüência de escala de síntese $g_1^{(j)}[n]$, isto é*

$$\langle h_1^{(j)}[2^j l - n], g_1^{(i)}[n - 2^i k]\rangle = \delta[j-i]\delta[l-k], \tag{3.93}$$

$$\langle h_0^{(J)}[2^J l - n], g_1^{(i)}[n - 2^i k]\rangle = \langle h_1^{(j)}[2^j l - n], g_0^{(J)}[n - 2^J k]\rangle = 0 \tag{3.94}$$

e

$$\langle h_0^{(J)}[2^J l - n], g_0^{(J)}[n - 2^J k]\rangle = \delta[l-k]. \tag{3.95}$$

Demonstração: A prova segue a mesma ideia da biortogonalidade entre os filtros de síntese e análise de bancos de filtros com reconstrução perfeita. ■

Simplificando, banco de filtros com reconstrução perfeita estruturados em árvores logarítmicas produzem transformadas wavelets. A biortogonalidade está diretamente relacionada à condição de reconstrução perfeita do banco de filtros. As wavelets de análise e síntese dependem diretamente dos filtros utilizados e se os filtros são FIR, então as wavelets têm suporte compacto (duração finita). Além disso, filtros ortogonais geram wavelets ortogonais. Assim, se existe banco de filtros de dois canais sobre $GF(q)$ com reconstrução perfeita, então, também existe transformada wavelet sobre $GF(q)$ associada a esse banco de filtros.

Dessa forma, existe transformada wavelet, via banco de filtros, para qualquer corpo finito $GF(q)$ (a situação em que q é potência de dois é tratada no capítulo 5).

Wavelets sobre corpos finitos podem ser utilizadas para análise multirresolução em corpos finitos, de forma análoga ao corpo dos complexos. Essa ferramenta pode apresentar aplicações em codificação de canal, compactação de dados e comunicações digitais.

3.5.2 Transformada de Fourier de Curta Duração sobre Corpos Finitos

Considere a estrutura com árvore completa e J estágios, como mostrado na Figura 3.20. Esta estrutura define uma transformada conhecida como *Transformada de Fourier de curta duração* quando aplicada sobre o corpo dos reais. Assim, define-se também a *transformada de Fourier de curta duração sobre corpos finitos*, utilizando a mesma estrutura em árvore para corpos finitos. Bem como a transformada wavelet, esta transformada têm caracter local.

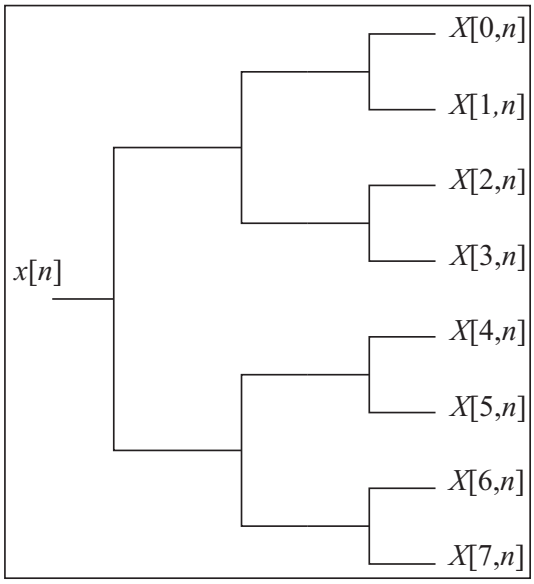


Figura 3.20: Estrutura em árvore para a transformada de Fourier de curta duração sobre corpos finitos.

Seja uma seqüência $x[n] \in GF(q)$, $n \in \mathbb{Z}$. A transformada de Fourier de curta duração (TFCD) de $x[n]$ é dada por

$$X[k,l] \triangleq \sum_{n=-\infty}^{\infty} x[n]h[k, 2^J l - n], \tag{3.96}$$

para $k = \{0, 1, \ldots, 2^J - 1\}$ e $l \in \mathbb{Z}$.

A transformada inversa, ou síntese da TFCD, é dada por

$$x[n] = \sum_{k=0}^{2^J-1} \sum_{l=-\infty}^{\infty} X[k,l]g[k, n - 2^J l]. \tag{3.97}$$

A condição para validade da transformada é a biortogonalidade dada por

$$\langle h[k_1, 2^J l_1 - n], g[k_2, n - 2^J l_2] \rangle = \delta[k_2 - k_1]\delta[l_2 - l_1], \tag{3.98}$$

para $k_1, k_2 = \{0, 1, \ldots, 2^J - 1\}$ e $l_1, l_2 \in \mathbb{Z}$.

Assim como na TWCF, as seqüências $h[k,n]$ e $g[k,n]$ podem ser obtidas por iterações de banco de filtros. Além disso, a transformada também é implementada com os banco de filtros. As relações de $h[k,n]$ e $g[k,n]$ com os filtros do banco de filtros utilizado são dadas por

$$H_{i_0}(z^{2^{J-1}})H_{i_1}(z^{2^{J-2}}) \ldots H_{i_{J-2}}(z^2)H_{i_{J-1}}(z) = H[\sum_{j=0}^{J-1} i_j 2^j](z) \tag{3.99}$$

e

$$G_{i_0}(z^{2^{J-1}})G_{i_1}(z^{2^{J-2}})\ldots G_{i_{J-2}}(z^2)G_{i_{J-1}}(z) = G[\sum_{j=0}^{J-1} i_j 2^j](z) \tag{3.100}$$

onde

$$h[k,n] \overset{\mathbf{Z}}{\longleftrightarrow} H[k](z) \tag{3.101}$$

e

$$g[k,n] \overset{\mathbf{Z}}{\longleftrightarrow} G[k](z). \tag{3.102}$$

Essa transformada pode ser aplicada para espalhamento espectral e multiplexação, utilizados em comunicações móveis [18]. Além disso, o caracter de transformadas sobre corpos finitos pode ser explorado em segurança de dados.

capítulo 4

Banco de Filtros e Wavelets para Sistemas Cíclicos

4.1 Introdução

Sistemas baseados nas chamadas estruturas cíclicas são de especial interesse em engenharia, uma vez que apresentam comprimento finito, como por exemplo os códigos cíclicos [19] e sistemas baseados na DFT[5, 13].

Formalmente, um sistema é dito *Sistema de Bloco* se suas entradas e saídas são blocos de comprimento fixo.

Definição 4.1 *Um sistema cíclico linear e invariante no tempo (CLIT) é um sistema de bloco linear onde qualquer deslocamento cíclico na entrada produz o mesmo deslocamento cíclico na saída.*

Nesse cenário, a operação usual de deslocamento é substituída pelo deslocamento circular ou cíclico. De forma análoga aos sistemas lineares e invariantes no tempo, um sistema CLIT também pode ser caracterizado por sua resposta ao impulso, $h[n]$ (Figura 4.1).

Dessa forma, um sinal cíclico $x[n]$ é um vetor com N elementos. 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

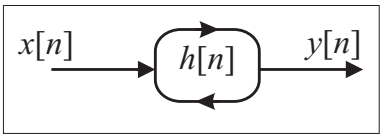


Figura 4.1: Diagrama ilustração de um sistema CLIT.

$$y[n] = \sum_{j=0}^{N-1} x[j]h[((n-j))_N] = x[n] \textcircled{N} h[n], \tag{4.1}$$

onde $((.))_N$ representa $(mod\ N)$ e $\textcircled{N}$ denota convolução cíclica de comprimento N.

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

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

se

$$X[k] \triangleq \sum_{n=0}^{N-1} x[n]\alpha^{kn}, \tag{4.2}$$

e

$$x[n] = N^{-1}(mod\ p) \sum_{k=0}^{N-1} X[k]\alpha^{-kn}, \tag{4.3}$$

onde α é um elemento de ordem N de $GF(q^m)$. A mesma abordagem pode ser feita nos complexos, utilizando a transformada discreta de Fourier (DFT)

A TFCF possui propriedades análogas às da DFT [12], [5].

Outra transformada de interesse é a transformada Z cíclica, que pode ser vista como uma notação polinomial do sinal ou do sistema, notação bastante utilizada em códigos cíclicos [19]. Para a seqüência $x[n]$, $n = 0, 1, \ldots, N-1$, onde $x[n] \in GF(q)$, existe um polinômio $X(z)$, com coeficientes em $GF(q)$, na variável z^{-1}, o qual representa a transformada Z cíclica de $x[n]$, denotada por

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

se

$$X(z) \triangleq \sum_{n=0}^{N-1} x[n]z^{-n}. \tag{4.4}$$

Então, mostra-se que

$$x[n] = (p-1) \sum_{z \in GF(q^m)} X(z)z^n, \tag{4.5}$$

onde $q^m - 1 \geq N$. Como o sistema é cíclico, a transformada Z está associada a aritmética polinomial módulo $(z^{-N} - 1)$.

Algumas propriedades dessa transformada estão listadas na Tabela 4.1.

Tabela 4.1: Propriedades da Transformada Z cíclica

Tempo	Z	Propriedade
$x[n]$	$X(z)$	
$y[n]$	$Y(z)$	
$ax[n] + by[n]$	$aX(z) + bY(z)$	Linearidade
$x[((n-d))_N]$	$z^{-d}X(z)(mod\ z^{-N} - 1)$	Deslocamento cíclico 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

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

$$X[k] = X(z)|_{z=\alpha^{-k}} = X(\alpha^{-k}), \tag{4.6}$$

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

Para que exista tais transformadas em corpos finitos, é necessário que $mdc(N, p) = 1$, pois α tem ordem N.

4.2 Sistema Subamostrador ou Compressor Cíclico

O sistema da Figura 4.2 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.

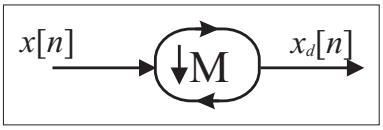


Figura 4.2: Diagrama de um sistema subamostrador cíclico de parâmetro M.

Definição 4.2 *Um sistema subamostrador M cíclico, com entrada $x[n]$ e saída $x_d[n] = x[((Mn))_N]$, existirá se M divide N.*

Teorema 4.1 *A saída de um subamostrador M, $x_d[n]$, apresenta período igual a N/M, ou seja,*

$$x_d[((n + N/M))_N] = x_d[n]. \tag{4.7}$$

Demonstração: Por definição, $x_d[n + N/M] = x[((M(n + N/M)))_N] = x[((Mn + N))_N] = x[((Mn))_N] = x_d[n]$. ■

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

Exemplo 4.1

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.

•

4.2.1 Análise do Subamostrador Cíclico

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

$$s_M[n] = \begin{cases} 1, & \text{se } n \equiv 0 \ (mod \ M) \\ 0, & \text{caso contrário,} \end{cases} \tag{4.8}$$

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

$$s_M[n] = \sum_{j=0}^{N/M-1} \delta[n - jM] \tag{4.9}$$

ou

$$s_M[n] = M^{-1} \sum_{j=0}^{M-1} \alpha^{-\frac{N}{M}jn}. \tag{4.10}$$

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

$$x_s[n] = x[n]s_M[n], \tag{4.11}$$

cuja transformada Z cíclica pode ser obtida por meio de (4.9) como sendo

$$X_s(z) = \sum_{j=0}^{N/M-1} x[((Mj))_N]z^{-jM} = \sum_{j=0}^{N/M-1} x_d[j]z^{-jM}. \tag{4.12}$$

Alternativamente, partindo-se de (4.10), chega-se a

$$X_s(z) = M^{-1} \sum_{j=0}^{M-1} X(\alpha^{\frac{N}{M}j} z). \tag{4.13}$$

Utilizando as equações (4.4) e (4.7), chega-se à expressão da transformada Z do sinal $x_d[n]$,

$$X_d(z) = \sum_{j=0}^{M-1} z^{-\frac{N}{M}j} \sum_{n=0}^{N/M-1} x[((Mn))_N] z^{-n}. \tag{4.14}$$

De (4.9) e (4.12), pode-se escrever

$$X_d(z) = S_{\frac{N}{M}}(z) X_s(z^{\frac{1}{M}}), \tag{4.15}$$

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 (4.13) chega-se a uma expressão que só depende de $X(z)$,

$$X_d(z) = M^{-1} S_{\frac{N}{M}}(z) \sum_{j=0}^{M-1} X(\alpha^{\frac{N}{M}j} z^{\frac{1}{M}}). \tag{4.16}$$

Utilizando (4.6) para obter resultados no domínio da freqüência, chega-se a

$$X_s[k] = M^{-1} \sum_{j=0}^{M-1} X[((k - \frac{N}{M}j))_N] \tag{4.17}$$

e

$$X_d[k] = \begin{cases} \sum_{j=0}^{M-1} X[((\frac{k}{M} - \frac{N}{M}j))_N], & \text{se } M \text{ divide } k \\ 0, & \text{caso contrário.} \end{cases} \tag{4.18}$$

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

4.3 Sistema Sobreamostrador ou Expansor Cíclico

O sistema sobreamostrador cíclico, Figura 4.3, é definido de acordo com a Figura 4.4, ou seja, a saída do sistema em cascata subamostrador-sobreamostrador por L resulta em $x_s[n]$ para uma entrada $x[n]$. Essa relação vale também para sistemas não cíclicos.

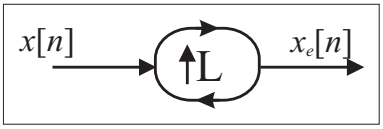


Figura 4.3: Representação de um sistema sobreamostrador L cíclico no tempo.

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

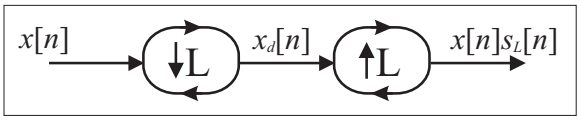


Figura 4.4: O sistema sobreamostrador é definido de forma que o sistema em cascata subamostrador sobreamostrador, para uma entrada $x[n]$, resulta em $x[n]s_L[n]$, assim como em sistemas não cíclicos.

Definição 4.3 *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*

$$x_e[n] = \sum_{j=0}^{N/L-1} x[j]\delta[((n - jL))_N]. \tag{4.19}$$

Pode-se fazer algumas observações sobre essa definição:

- Os sinais sobreamostrados 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 subamostragem de L), então o sinal expandido é dado simplesmente por

$$x_e[n] = \begin{cases} x[n/L], & \text{se } L \text{ divide } n \\ 0, & \text{caso contrário.} \end{cases} \tag{4.20}$$

- 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.

Em outras palavras, a saída do sobreamostrador, equação (4.19), apresenta a perda da informação das componentes $x[n]$ para $n \geq N/L$. Essa perda não acontece se houver redundância dos termos subsequentes, como ocorre na subamostragem. Assim, para $x[n]$ um sinal sobreamostrados, se $MDC(L, p) = 1$, então

$$x_e[n] = L^{-1}(mod\ p) \sum_{j=0}^{N-1} x[j]\delta[((n - jL))_N]. \tag{4.21}$$

4.3.1 Análise do Sobreamostrador Cíclico

O sinal $x_e[n]$ pode ser analisado a partir da definição da transformada Z cíclica, Equação (4.4), e da relação (4.21). Tem-se

$$X_e(z) = L^{-1}(mod\ p)X(z^L)(mod\ z^{-N} - 1). \tag{4.22}$$

Passando para o domínio de Fourier,

$$X_e[k] = L^{-1}(mod\ p)X[((Lk))_N]. \tag{4.23}$$

Essas relações são válidas para $MDC(L,p) = 1$. Conclui-se que uma compressão cíclica no tempo gera uma expansão cíclica na freqüência e uma expansão cíclica no tempo gera uma compressão cíclica na freqüência, semelhante ao caso de sistemas não cíclicos.

4.4 Processamento de Sinais Cíclicos Multitaxa

4.4.1 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

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

ou

$$x[n] \textcircled{N} y[n] = \sum_{j=0}^{R-1} x[j] \sum_{m=0}^{M-1} y[((n-j-m\frac{N}{M}))_N]. \tag{4.24}$$

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

$$y_R[n] = \sum_{m=0}^{M-1} y[((n-mR))_N], \tag{4.25}$$

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

$$x[n] \textcircled{N} y[n] = \sum_{j=0}^{R-1} x[j]y_R[((n-j))_R] = x[n] \textcircled{R} y_R[n]. \tag{4.26}$$

A computação da representação reduzida (4.25) 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 (4.25) para calcular a representação reduzida de $y[n]$ e sabendo que,

$$y[n] = y[((n+mR))_N], \tag{4.27}$$

chega-se a

$$y_R[n] = \sum_{m=0}^{M-1} y[((n - mR))_N] = My[((n))_R]. \tag{4.28}$$

A expressão da convolução para sinais reduzidos pode ser encontrada substituindo (4.28) em (4.26), resultando em

$$x[n] \textcircled{N} y[n] = Mx[n] \textcircled{R} y[n]. \tag{4.29}$$

4.4.2 Identidades Nobres Cíclicas

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. Elas são as identidades nobres.

Primeira Identidade Nobre

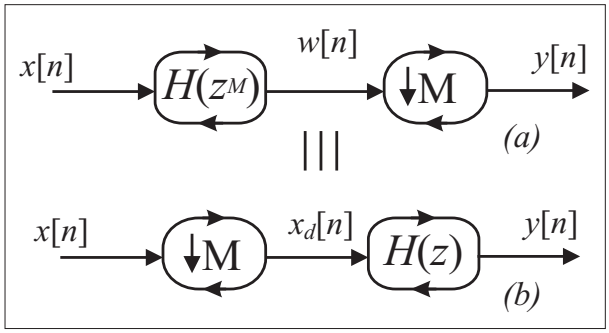


Figura 4.5: Primeira identidade nobre - Os sistemas (a) e (b) são equivalentes.

Teorema 4.2 *Os sistemas (a) e (b) da Figura 4.5 são equivalentes.*

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

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

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). ■

Segunda Identidade Nobre

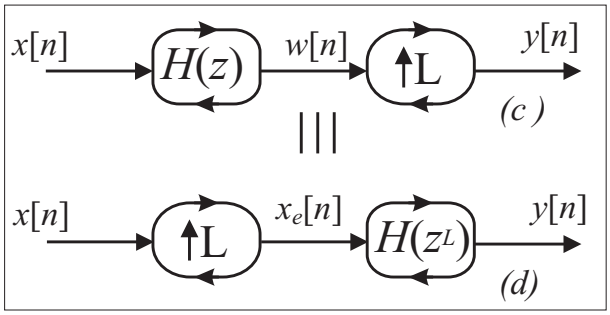


Figura 4.6: Segunda identidade nobre - Os sistemas (c) e (d) são equivalentes.

Teorema 4.3 *Os sistemas (c) e (d) da Figura 4.6 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). ■

4.4.3 Decomposição Polifásica Cíclica

A decomposição polifásica cíclica é também bastante eficiente para o projeto de banco de filtros cíclicos. Assim como em sistemas não cíclicos [13]. A seguir, são apresentadas as decomposições polifásicas cíclicas tipo I e tipo II.

Decomposição Polifásica Cíclica Tipo I

A decomposição polifásica cíclica representa uma seqüência $h[n]$, por meio de M seqüências $h_i[n]$ chamadas de componentes polifásica de $h[n]$. A equação para a decomposição polifásica tipo I seguem o mesmo princípio para sistemas não cíclicos, elas são

$$h_i[n] = h[((Mn + i))_N], \tag{4.30}$$

para $i = 0, \ldots, M-1$, e

$$h[n] = \sum_{i=0}^{M-1} h_i[((n-i))_{N/M}/M], \tag{4.31}$$

onde $h_i[r/M] = 0$, se $r \neq 0(mod\ M)$. As seqüências $h_i[n]$ são subamostradas, isto é, tem período cíclico de N/M. Um exemplo para $N = 15$ e $M = 3$ é mostrado na Figura 4.7, os valores na figura são preenchidos de baixo para cima, da esquerda para a direita.

$h[0]$	$h[3]$	$h[6]$	$h[9]$	$h[12]$	$\rightarrow h_0[n]$
$h[1]$	$h[4]$	$h[7]$	$h[10]$	$h[13]$	$\rightarrow h_1[n]$
$h[2]$	$h[5]$	$h[8]$	$h[11]$	$h[14]$	$\rightarrow h_2[n]$

Figura 4.7: Exemplo de decomposição polifásica cíclica tipo I de $h[n]$, $N = 15$ e $M = 3$.

Um filtro cíclico $H(z)$ pode ser implementado utilizando-se a decomposição polifásica tipo I por

$$H(z) = \sum_{i=0}^{M-1} \sum_{n=0}^{N/M-1} h[Mn+i] z^{-(Mn+i)}, \tag{4.32}$$

$$H(z) = \sum_{i=0}^{M-1} z^{-i} \sum_{n=0}^{N/M-1} h[Mn+i] z^{-Mn} \tag{4.33}$$

mas

$$\sum_{n=0}^{N/M-1} h[Mn+i] z^{-Mn} = M^{-1} H_i(z^M)(mod\ z^{-N} - 1), \tag{4.34}$$

onde

$$H_i(z) = \sum_{n=0}^{N-1} h_i[n] z^{-n}. \tag{4.35}$$

Assim,

$$H(z) = M^{-1} \sum_{i=0}^{M-1} z^{-i} H_i(z^M)(mod\ z^{-N} - 1). \tag{4.36}$$

A implementação polifásica desse filtro está mostrada na Figura 4.8. Para a implementação do filtro $H(z)$, esta estrutura apresenta desvantagens computacionais, entretanto, para a implementação de filtros dizimadores cíclicos, componente fundamental em banco de filtros cíclicos, a estrutura é eficiente.

Decomposição Polifásica Cíclica Tipo II

A decomposição polifásica tipo II de uma seqüência $h[n]$ representa uma seqüência $h[n]$, por meio de M seqüências $h_i[n]$ chamadas de componentes polifásica tipo II de $h[n]$, onde

$$h_i[n] = h[((Mn-i))_N], \tag{4.37}$$

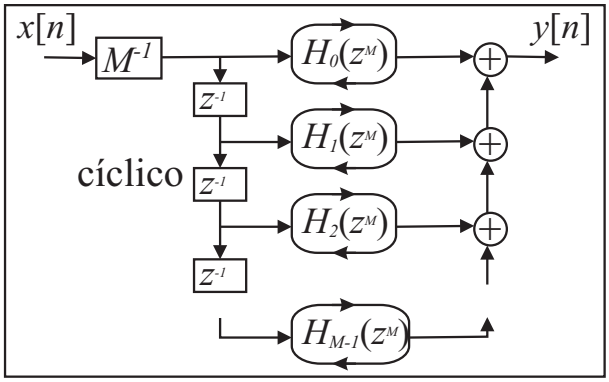


Figura 4.8: Implementação polifásica tipo I do filtro $H(z)$.

e

$$h[n] = \sum_{i=0}^{M-1} h_i[((n+i))_N/M]. \tag{4.38}$$

Um exemplo está mostrado na Figura 4.9 com $N = 15$ e $M = 3$, nesse caso, os valores são preenchidos de baixo para cima e da esquerda para a direita.

$h[0]$	$h[3]$	$h[6]$	$h[9]$	$h[12]$	$\rightarrow h_0[n]$
$h[14]$	$h[2]$	$h[5]$	$h[8]$	$h[11]$	$\rightarrow h_1[n]$
$h[13]$	$h[1]$	$h[4]$	$h[7]$	$h[10]$	$\rightarrow h_2[n]$

Figura 4.9: Exemplo de decomposição polifásica cíclica tipo II de $h[n]$, $N = 15$ e $M = 3$.

Um filtro $H(z)$ pode ser implementado utilizando-se a decomposição polifásica tipo II, por

$$H(z) = \sum_{i=0}^{M-1} \sum_{n=0}^{N/M-1} h[Mn - i]z^{-(Mn-i)}, \tag{4.39}$$

$$H(z) = \sum_{i=0}^{M-1} z^i \sum_{n=0}^{N/M-1} h[Mn - i]z^{-Mn} \tag{4.40}$$

ou

$$H(z) = M^{-1} \sum_{i=0}^{M-1} z^i H_i(z^M)(mod\ z^{-N} - 1). \tag{4.41}$$

Implementação Polifásica de Filtros Dizimadores Cíclicos

A implementação polifásica do sistema cíclico mostrado na Figura 4.10 (filtro dizimador cíclico) pode ser feita utilizando-se a decomposição polifásica cíclica tipo I de $H(z)$, ilustrada na Figura 4.8, e aplicando-se a primeira identidade nobre. O resultado é a implementação da Figura 4.11. Observa-se que a transformada Z da saída $y[n]$ é dada por

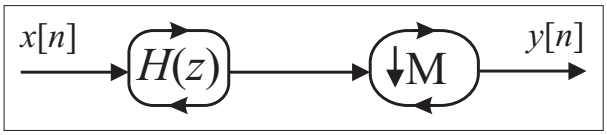


Figura 4.10: Diagrama de um filtro dizimador cíclico.

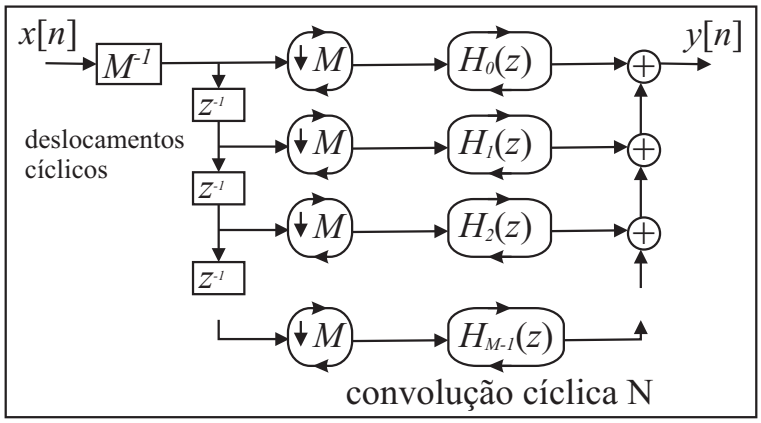


Figura 4.11: Diagrama de um filtro dizimador cíclico implementado utilizando-se a decomposição polifásica cíclica tipo I para $h[n]$.

$$Y(z) = M^{-1} \sum_{i=0}^{M-1} X_i(z) H_i(z) (mod\ z^{-N} - 1). \tag{4.42}$$

Voltando para o domínio do tempo,

$$y[n] = M^{-1} \sum_{i=0}^{M-1} x_i[n] \textcircled{N} h_i[n], \tag{4.43}$$

onde as componentes $x_i[n] \overset{\mathbf{Z}}{\longleftrightarrow} X_i(z)$ e $h_i[n] \overset{\mathbf{Z}}{\longleftrightarrow} H_i(z)$, respectivamente, correspondem às componentes polifásica tipo II de $x[n]$ e tipo I de $h[n]$, ambas com período $R = N/M$, valendo então a Equação (4.29). Portanto

$$y[n] = \sum_{i=0}^{M-1} x_i[n] \textcircled{R} h_i[n]. \tag{4.44}$$

A implementação com convoluções cíclicas de comprimento R está mostrada na Figura 4.12. A Figura 4.13 ilustra um procedimento para a implementação do filtro dizimador cíclico com $N = 15$ e $M = 3$.

Esta implementação necessita de M convoluções cíclicas de comprimento N/M. Tem complexidade M vezes menor que a implementação usual, além de pode ser implementada

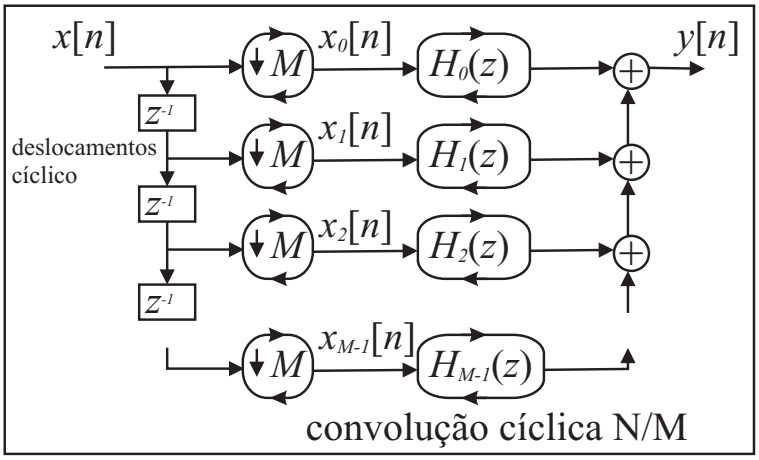


Figura 4.12: Diagrama de um filtro dizimador cíclico implementado utilizando-se a decomposição polifásica cíclica tipo I para $h[n]$.

$x[0]$	$x[3]$	$x[6]$	$x[9]$	$x[12]$	⑤	$h[0]$	$h[3]$	$h[6]$	$h[9]$	$h[12]$	$\longrightarrow \oplus\ y[n]$
$x[14]$	$x[2]$	$x[5]$	$x[8]$	$x[11]$	⑤	$h[1]$	$h[4]$	$h[7]$	$h[10]$	$h[13]$	$\rightarrow \oplus \uparrow$
$x[13]$	$x[1]$	$x[4]$	$x[7]$	$x[10]$	⑤	$h[2]$	$h[5]$	$h[8]$	$h[11]$	$h[14]$	$\rightarrow \uparrow$

Figura 4.13: Implementação do filtro dizimador cíclico, $N = 15$ e $M = 3$.

utilizando-se a transformada rápida de Fourier sobre corpos finitos [5], ou no caso dos complexos, utilizando-se uma FFT [13, 20].

4.5 Banco de Filtros para Sistemas Cíclicos

Considere a estrutura da Figura 4.14, um banco de filtros cíclicos (BFC) de M canais com reconstrução perfeita.

Teorema 4.4 *Para um banco de filtros cíclicos de M canais, como mostrado na Figura 4.14, se a chamada condição de reconstrução perfeita (2.28) é satisfeita, ou seja, se*

$$\sum_{j=0}^{M-1} H_j(\alpha^{\frac{N}{M}m}z)G_j(z)(mod\ z^{-N}-1) = M\delta[m], \tag{4.45}$$

$m = 0, \ldots, M-1$ e α é um elemento de corpo de ordem N, então ocorre recuperação perfeita, isto é, $x_r[n] = x[n]$ para qualquer $x[n]$.

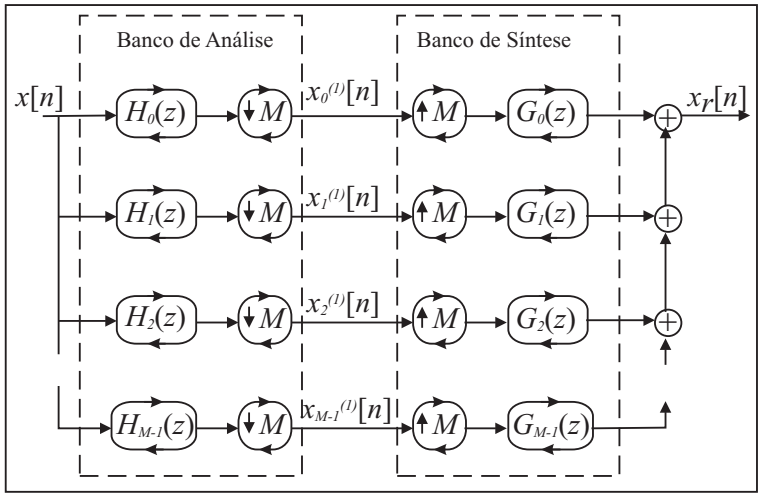


Figura 4.14: Estrutura de um banco de filtros cíclicos de M canais, ilustrando o banco de análise e de síntese.

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

$$Y_j(z) = G_j(z)(H_j(z)X(z))_s(mod\ z^{-N} - 1). \tag{4.46}$$

Considerando as expressões (4.16) e (4.22),

$$Y_j(z) = G_j(z)M^{-1}\sum_{m=0}^{M-1} H_j(\alpha^{\frac{N}{M}m}z)X(\alpha^{\frac{N}{M}m}z)(mod\ z^{-N} - 1). \tag{4.47}$$

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

$$X_r(z) = \sum_{j=0}^{M-1} Y_j(z) = \tag{4.48}$$

$$M^{-1}\sum_{j=0}^{M-1} G_j(z)\sum_{m=0}^{M-1} H_j(\alpha^{\frac{N}{M}m}z)X(\alpha^{\frac{N}{M}m}z)(mod\ z^{-N} - 1) = \tag{4.49}$$

$$M^{-1}\sum_{m=0}^{M-1} X(\alpha^{\frac{N}{M}m}z)\sum_{j=0}^{M-1} H_j(\alpha^{\frac{N}{M}m}z)G_j(z)(mod\ z^{-N} - 1). \tag{4.50}$$

Substituindo o último somatório pela relação de reconstrução perfeita (2.28), a expressão de $X_r(z)$ se reduz a

$$X_r(z) = M^{-1}\sum_{m=0}^{M-1} X(\alpha^{\frac{N}{M}m}z)M\delta[m] = \tag{4.51}$$

$$\sum_{m=0}^{M-1} X(\alpha^{\frac{N}{M}m}z)\delta[m] = X(z). \tag{4.52}$$

■

A reconstrução perfeita pode também ser analisada no domínio da freqüência por (4.6). A Equação (2.28) torna-se

$$\sum_{j=0}^{M-1} H_j[((k - \frac{N}{M}m))_N]G_j[k] = M\delta[m]. \tag{4.53}$$

Uma observação importante para corpos finitos é que a relação de reconstrução perfeita (4.45) é valida se $MDC(p, M) = 1$, onde p é a característica do corpo.

Teorema 4.5 *Para banco de filtros cíclicos de M canais satisfazendo a condição de reconstrução perfeita, as equações de análise e síntese do banco são, respectivamente,*

$$x_i^{(1)}[l] = \sum_{n=0}^{N-1} x[n]h_i[((Ml - n))_N], \tag{4.54}$$

para $i = 0, \ldots, M-1$, e

$$x[n] = \sum_{i=0}^{M-1}\sum_{l=0}^{N/M-1} x_i^{(1)}[l]g_i[((n - Ml))_N], \tag{4.55}$$

onde $h_i[n]$ e $g_i[n]$ são, respectivamente, as transformadas Z cíclicas inversas dos filtros $H_i(z)$ e $G_i(z)$ de comprimento N.

Demonstração: A análise é simplesmente uma convolução cíclica de comprimento N, seguida por uma subamostragem por M. A síntese é obtida por expansão e convolução cíclica de mesmo comprimento, para cada linha do banco de filtros tem-se

$$x_{ie}^{(1)}[n] \circledN g_i[n] = \sum_{l=0}^{N/M-1} x_i^{(1)}[l]\delta[((n - Ml))_N] \circledN g_i[n] = \sum_{l=0}^{N/M-1} x_i^{(1)}[l]g_i[((n - Ml))_N]. \tag{4.56}$$

Somando-se todas as linhas chega-se ao resultado. ■

Definição 4.4 *O produto interno entre duas seqüências de comprimento N, $x[n], y[n]$, definidas sobre um corpo qualquer, é dado por*

$$\langle x[n], y[n]\rangle \stackrel{\Delta}{=} \sum_{n=0}^{N-1} x[n]y[n] \tag{4.57}$$

Teorema 4.6 (Relação de biortogonalidade cíclica) *Num banco de filtros cíclicos de M canais com reconstrução perfeita, os filtros geram bases biortogonais cíclicas, isto é*

$$\langle h_i[((-n))_N], g_j[((n-Ml))_N]\rangle = \delta[i-j]\delta[l], \tag{4.58}$$

para $i, j = 0, \ldots, M-1$ *e* $l = 0, \ldots, N/M-1$.

A prova segue como no caso de sistemas não cíclicos.

Exemplo 4.2

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 (4.53), escolhe-se os filtros sem sobreposição:
$H_0[k] = (1,1,1,0,1,0,0,0,1,0,0,0,0,0,0) = G_0[k]$,
$H_1[k] = (0,0,0,0,0,1,0,1,0,0,0,1,0,1,1) = G_1[k]$,
$H_2[k] = (0,0,0,1,0,0,1,0,0,1,1,0,1,0,0) = G_2[k]$.
A Equação (4.53) é facilmente verificada, pois, $H_i[k]G_i[k] = H_i[k]$ e $H_i[((k-5m))_15]G_i[k] = 0$, para $m \neq 0(mod\ 3)$. Além disso, $H_0[k] + H_1[k] + H_2[k] = 1$, para $k = 0, 1, \ldots, 14$. Logo, essa estrutura é um banco de filtros com reconstrução perfeita (Figura 4.14, 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
$x_0^{(1)}[n] = (0,0,0,0,0)$,
$x_1^{(1)}[n] = (0,0,1,1,0)$,
$x_2^{(1)}[n] = (1,1,1,0,1)$.
Aplicando esses valores nas entradas do banco de síntese, verifica-se que ocorre a reconstrução perfeita de $x[n]$ na saída.

•

4.5.1 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 4.15.

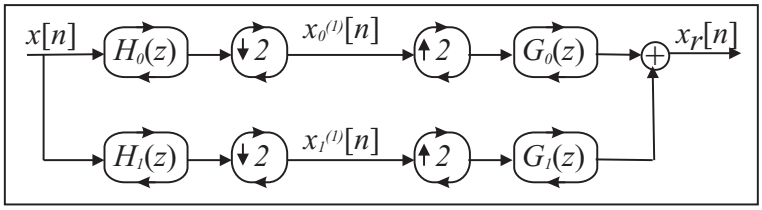


Figura 4.15: Estrutura de um banco de filtros de dois canais.

Escrevendo a Equação (4.45) em forma matricial com $M = 2$, tem-se

$$\begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix} \begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} (mod\ z^{-N} - 1) = \begin{bmatrix} 2 \\ 0 \end{bmatrix}. \tag{4.59}$$

Definindo a matriz modulação $H_m(z)$ como

$$H_m^T(z) = \begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix}, \tag{4.60}$$

resulta em

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = 2\Delta^{-1}(z)(mod\ z^{-N} - 1) \begin{bmatrix} H_1(-z) \\ -H_0(-z) \end{bmatrix}, \tag{4.61}$$

onde $\Delta(z) = det(H_m(z))(mod\ z^{-N} - 1)$.

O método apresentado para o projeto consiste em restringir $\Delta(z)$, que é um polinômio ímpar, de tal forma que $MDC(\Delta(z), z^{-N} - 1) = 1$. Isto faz com que sempre se encontre solução para $\Delta^{-1}(z)(mod\ z^{-N} - 1)$. A equação matricial (4.61) resulta em

$$G_0(z) = 2\Delta^{-1}(z)H_1(-z)(mod\ z^{-N} - 1) \tag{4.62}$$

e

$$G_1(z) = -2\Delta^{-1}(z)H_0(-z)(mod\ z^{-N} - 1). \tag{4.63}$$

Com esses dois resultados, a equação matricial (4.59) reduz-se a

$$[H_0(z)G_0(z) + H_0(-z)G_0(-z)](mod\ z^{-N} - 1) = 2. \tag{4.64}$$

Definindo o filtro produto cíclico por

$$P(z) \triangleq H_0(z)G_0(z)(mod\ z^{-N} - 1) \tag{4.65}$$

e substituindo em (4.64), tem-se

$$P(z) + P(-z) = 2. \tag{4.66}$$

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 4.1 *Método 1 para projeto de banco de filtros cíclicos sobre corpos com característica p ímpar:*

- *Escolher um filtro $P(z)$ satisfazendo (4.66);*
- *Fatorar $P(z)$ em $H_0(z)G_0(z)(mod\ z^{-N}-1)$;*
- *Utilizar as equações*

$$H_1(z) = -2^{-1}(mod\ p)\Delta(z)G_0(-z)(mod\ z^{-N}-1) \tag{4.67}$$

e

$$G_1(z) = -2\Delta^{-1}(z)H_0(-z)(mod\ z^{-N}-1), \tag{4.68}$$

onde $\Delta(z)$ é um polinômio ímpar satisfazendo a $MDC(\Delta(z), z^{-N}-1) = 1$, para encontrar $H_1(z)$ e $G_1(z)$.

No método de projeto usual utilizado no corpo dos reais, $\Delta(z)$ deve ser um retardo puro para que os filtros sejam FIR. Nesta situação ocorre uma liberdade maior devido a aritmética polinomial, associada a equação RP. Este método de projeto constitui uma novidade tanto para corpos finitos quanto para o corpo dos reais.

4.5.2 Implementação Polifásica para Banco de Filtros Cíclicos de Dois Canais

A estrutura da Figura 4.15 pode ser implementada de forma polifásica, utilizando a decomposição tipo I para o banco de síntese com convoluções cíclicas de comprimento $N/2$, como mostra a Figura 4.16.

A equação de análise é dada por

$$x_0^{(1)}[n] = x_0[n] \circledR h_{00}[n] + x_1[n] \circledR h_{01}[n] \tag{4.69}$$

$$x_1^{(1)}[n] = x_0[n] \circledR h_{10}[n] + x_1[n] \circledR h_{11}[n], \tag{4.70}$$

onde $R = N/2$, $h_{ij}[n]$ são decomposições polifásicas tipo I de $h_i[n]$ e $x_i[n]$ são decomposições polifásicas tipo II. Utilizando a transformada Z cíclica de comprimento $N/2$ e colocando em forma matricial, a equação de análise resulta em

$$\begin{bmatrix} X_0^{(1)}(z) \\ X_1^{(1)}(z) \end{bmatrix} = \begin{bmatrix} H_{00}(z) & H_{01}(z) \\ H_{10}(z) & H_{11}(z) \end{bmatrix} \begin{bmatrix} X_0(z) \\ X_1(z) \end{bmatrix} (mod\ z^{-N/2}-1), \tag{4.71}$$

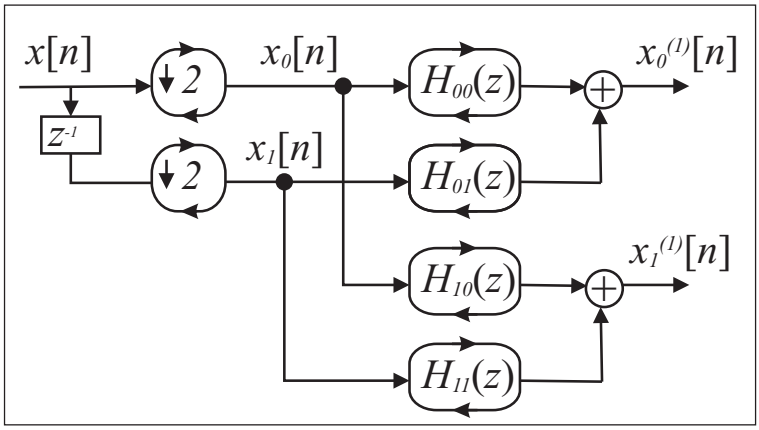


Figura 4.16: Implementação polifásica de um banco de filtros cíclicos de análise com dois canais.

O sinal cíclico é recuperado com a estrutura da Figura 4.17, que é a estrutura de síntese implementada utilizando a decomposição polifásica tipo II.

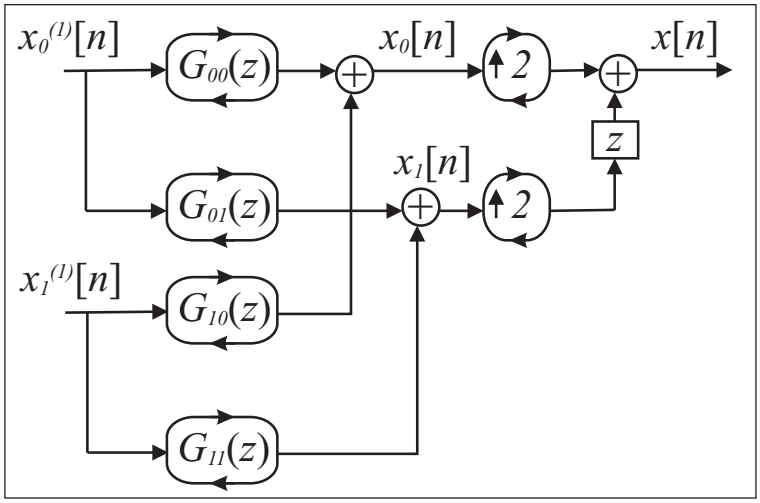


Figura 4.17: Implementação polifásica de um banco de filtros cíclicos de síntese com dois canais.

As equações de síntese são

$$x_0[n] = x_0^{(1)}[n] \circledR g_{00}[n] + x_1^{(1)}[n] \circledR g_{10}[n] \tag{4.72}$$

$$x_1[n] = x_0^{(1)}[n] \circledR g_{01}[n] + x_1^{(1)}[n] \circledR g_{11}[n], \tag{4.73}$$

onde $g_{ij}[n]$ são componentes polifásicas tipo II de $g_i[n]$. Aplicando a transformada Z de

comprimento $N/2$, o resultado é

$$\begin{bmatrix} X_0(z) \\ X_1(z) \end{bmatrix} = \begin{bmatrix} G_{00}(z) & G_{10}(z) \\ G_{01}(z) & G_{11}(z) \end{bmatrix} \begin{bmatrix} X_0^{(1)}(z) \\ X_1^{(1)}(z) \end{bmatrix} (mod\ z^{-N/2} - 1), \tag{4.74}$$

As matrizes polifásicas cíclicas de análise e síntese, $H_p(z)$ e $G_p(z)$, respectivamente, são definidas por

$$H_p(z) \triangleq \begin{bmatrix} H_{00}(z) & H_{01}(z) \\ H_{10}(z) & H_{11}(z) \end{bmatrix} \tag{4.75}$$

e

$$G_p(z) \triangleq \begin{bmatrix} G_{00}(z) & G_{10}(z) \\ G_{01}(z) & G_{11}(z) \end{bmatrix}. \tag{4.76}$$

Teorema 4.7 (Condição RP polifásica cíclica) *Para um banco de filtros cíclicos com matrizes polifásicas cíclicas de análise e síntese, $H_p(z)$ e $G_p(z)$ respectivamente, se*

$$G_p(z)H_p(z)(mod\ z^{-N/2} - 1) = I_2, \tag{4.77}$$

então ocorre a reconstrução perfeita.

Demonstração: As componentes polifásicas tipo II do sinal recuperado são dadas, no domínio da transformada Z cíclica de comprimento $N/2$, por

$$\begin{bmatrix} X_{0r}(z) \\ X_{1r}(z) \end{bmatrix} = G_p(z) \begin{bmatrix} X_0^{(1)}(z) \\ X_1^{(1)}(z) \end{bmatrix} (mod\ z^{-N/2} - 1), \tag{4.78}$$

utilizando (4.71),

$$\begin{bmatrix} X_{0r}(z) \\ X_{1r}(z) \end{bmatrix} = G_p(z)H_p(z)(mod\ z^{-N/2} - 1) \begin{bmatrix} X_0(z) \\ X_1(z) \end{bmatrix}, \tag{4.79}$$

então, se (4.77) é satisfeita, a decomposição polifásica do sinal recuperado é igual a do sinal original e, portanto, ocorre a reconstrução perfeita. ■

Proposição 4.2 *Método 2 para projeto de banco de filtros cíclicos:*

- *Escolhe-se uma matriz $H_p(z)$ MxM inversível $(mod\ z^{-N/2} - 1)$, onde M é o número de canais;*
- *Encontra-se $G_p(z) = H_p^{-1}(z)(mod\ z^{-N/2} - 1)$;*
- *Encontram-se os filtros de análise e síntese através de $H_p(z)$ e $G_p(z)$, respectivamente.*

Este método pode ser utilizado independentemente da característica do corpo e do número de canais, o que não acontece com o método 1 de projeto.

4.6 Wavelets Cíclicas

As expressões da série wavelet cíclica podem ser obtidas por iterações de banco de filtros cíclicos de dois canais, estruturas conhecidas como árvore logarítmica (em algumas referências essas estruturas são denominadas *Octave-Band*, divide o sinal em oitavas, no caso de sistemas sobre os reais e não cíclicos), como mostra a Figura 4.18.

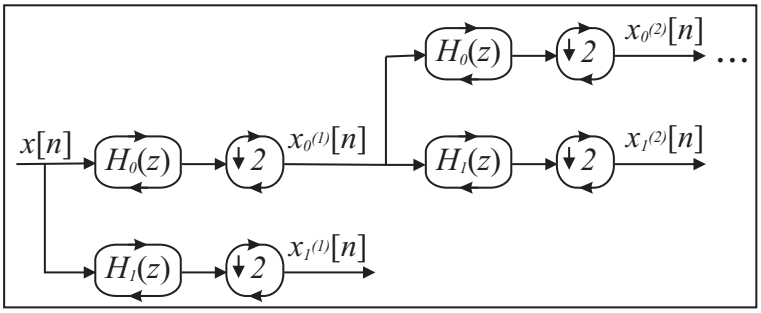


Figura 4.18: BFC de análise estruturados em árvore logarítmica (resulta nas séries wavelet cíclicas).

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 4.19.

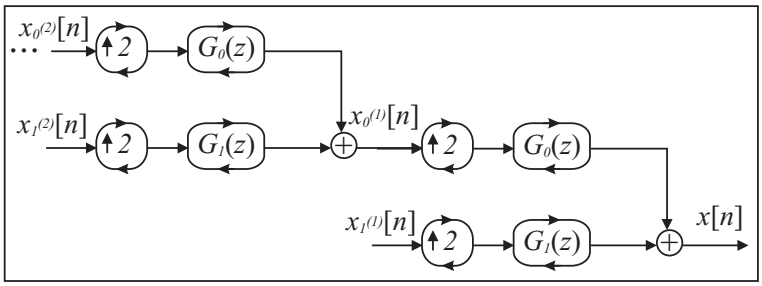


Figura 4.19: BFC de síntese estruturados em árvore logarítmica.

A partir da Figura 4.18, pode-se utilizar a primeira identidade nobre para colocar todos os subamostradores nas extremidades da direita. Assim, define-se

$$H_0^{(0)}(z) \triangleq 1 \tag{4.80}$$

e

$$H_i^{(j)}(z) \triangleq H_0^{(j-1)}(z) H_i(z^{2^{j-1}}) (mod\ z^{-N} - 1), \tag{4.81}$$

onde

$$h_i^{(j)}[n] \stackrel{\mathbf{Z}}{\longleftrightarrow} H_i^{(j)}(z), \tag{4.82}$$

para $i = 0, 1$ e $j = 1, 2, \ldots, J$, em que J é o maior número tal que $2^J | N$. As equações de análise são

$$x_1^{(j)}[l] = \sum_{n=0}^{N-1} x[n] h_1^{(j)}[((2^j l - n))_N] \tag{4.83}$$

e

$$x_0^{(J)}[l] = \sum_{n=0}^{N-1} x[n] h_0^{(J)}[((2^j l - n))_N]. \tag{4.84}$$

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

$$G_0^{(0)}(z) = 1 \tag{4.85}$$

e

$$G_i^{(j)}(z) = G_0^{(j-1)}(z) G_i(z^{2^{j-1}}) (mod\ z^{-N} - 1), \tag{4.86}$$

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

$$X(z) = \sum_{j=1}^{J} 2^{-j} X_1^{(j)}(z^{2^j}) G_1^{(j)}(z) + 2^{-J} X_0^{(J)}(z^{2^j}) G_0^{(J)}(z)\ (mod\ z^{-N} - 1). \tag{4.87}$$

Considerando a transformada Z inversa de (4.87), encontra-se a expressão de síntese para J estágios,

$$x[n] = \sum_{j=1}^{J} \sum_{l=0}^{N/2^j - 1} x_1^{(j)}[l] g_1^{(j)}[((n - 2^j l))_N] + \sum_{l=0}^{N/2^J - 1} x_0^{(J)}[l] g_0^{(J)}[((n - 2^J l))_N]. \tag{4.88}$$

As wavelets cíclicas são as seqüências $g_1^{(j)}[n]$ de comprimento N. Qualquer seqüência de comprimento N, $x[n]$, pode ser decomposta nas wavelets cíclicas e por deslocamentos cíclicos das mesmas. A série wavelet cíclica pode ser representada como transformada, definida como transformada wavelets discreta (DWT), análoga a transformada discreta de Fourier (DFT), a qual também é cíclica [13].

Exemplo 4.3

Considere o corpo $GF(7)$, $N = 48$. Utilizando-se o método 1 de projeto, considere $P(z) = (1 + z^{-1})^4 R(z) (mod\ z^{-48} - 1)$.

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 (4.66). A solução em GF(49) é $a = 3$ e $b = 2$, ou seja,

$P(z) = (1 + z^{-1})^4(3 + 2z^{-1} + 3z^{-2})z^3(mod\ z^{-48} - 1)$.

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 (4.67) e (4.68), com $\Delta(z) = 2z$, 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:

$x_1^{(1)}[l] = (5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6)$,

$x_1^{(2)}[l] = (4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5)$,

$x_1^{(3)}[l] = (0, 0, 0, 0, 0, 1)$,

$x_1^{(4)}[l] = (5, 0, 6)$,

$x_0^{(4)}[l] = (5, 2, 4)$.

Utilizando o banco de síntese para D_2 em $GF(7)$, recupera-se exatamente o sinal original de comprimento $N = 48$.

•

4.7 Aplicações de Banco de Filtros e Wavelets Cíclicos sobre Corpos Finitos em Códigos de Bloco Lineares

Banco de filtros cíclicos (BFC) e wavelets cíclicas podem ser utilizados para análise, geração, codificação e decodificação de códigos de bloco. Cada filtro cíclico constitui per si um codificador cíclico, em função da utilização da convolução cíclica. Para o contexto de códigos, pode ser introduzida a denominação *banco de códigos*.

A notação indicada a seguir é utilizada para o contexto de códigos:

$N \rightarrow$ Comprimento do código;

$K \rightarrow$ Dimensão do código (Comprimento da mensagem);

$d \rightarrow$ distância de Hamming mínima do código;

$C(N, K, d) \rightarrow$ Representação dos parâmetros do código C;

$c[n] \rightarrow$ Palavra código;

$u_i^{(j)}[n] \rightarrow$ Mensagem no canal i, estágio j;

$\tilde{c}[n] \rightarrow$ Palavra recebida do canal;

$\tilde{u}_i^{(j)}[n] \rightarrow$ Mensagem decodificada no canal i, estágio j;

Transformadas sobre corpos finitos (a TFCF e a transformada Z cíclica) são utilizadas para a análise dos códigos e as estruturas BFC implementam sua codificação e decodificação.

Em um artigo recente [21], outra abordagem para a construção de códigos de bloco lineares por meio de banco de filtros foi apresentada, porém utilizando BFC diferentes daqueles apresentados nessa dissertação.

4.7.1 Estruturas BFC para Códigos de Bloco Lineares

A idéia básica para a construção de códigos lineares é mostrada na figura 4.20. O código é gerado colocando mensagens $u_i^{(1)}[n]$ nas entradas dos filtros de síntese escolhidos e adicionando o sinal nulo para os outros filtros, gerando o sinal palavra código $c[n]$. Para decodificar $c[n]$, basta aplicá-lo ao banco de análise. As posições escolhidas como nulas estão associadas às equações de paridade do código ($s_i^{(1)}[n] = 0$) e, na recepção, são denominadas de *síndrome*.

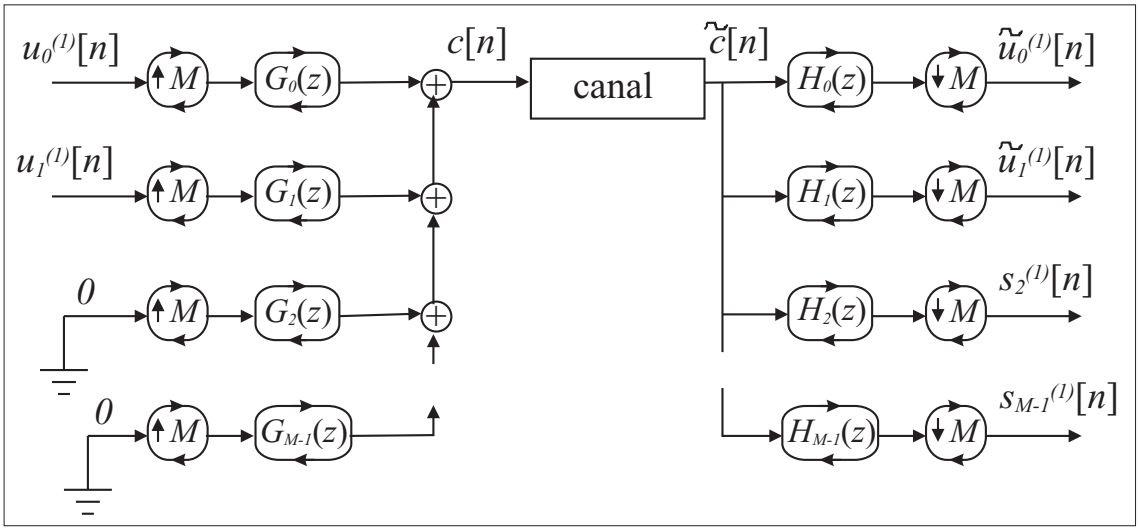


Figura 4.20: Construção de códigos de bloco lineares por meio da estrutura básica BFC com M canais.

Para simplificar a representação da estrutura básica, é utilizada a representação reduzida (em forma de árvores) de síntese e análise, mostradas nas figuras 4.21 e 4.22 respectivamente.

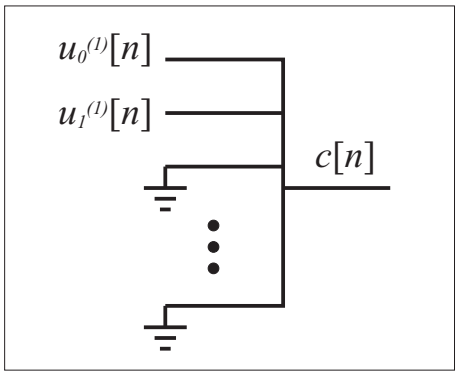


Figura 4.21: Representação reduzida do banco de síntese

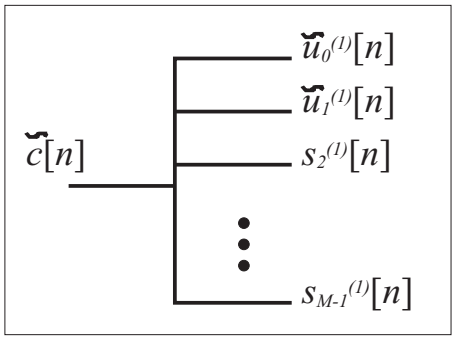


Figura 4.22: Representação reduzida do banco de análise

Para a codificação, escolhe-se de forma geral um espaço código denotado por $\mathbf{C}$, que contém os índices i das mensagens $u_i^{(1)}[n]$ permitidas no código. Assim, uma palavra código $c[n] \in \mathbf{C}$ será expressa por

$$c[n] = \sum_{i \in \mathbf{C}} \sum_{l=0}^{N/M-1} u_i^{(1)}[l] g_i[((n - Ml))_N]. \tag{4.89}$$

Após $c[n]$ passar por um canal, recebe-se $\tilde{c}[n]$. Aplicando-se $\tilde{c}[n]$ ao banco de análise, obtém-se as equações de decodificação (4.90) e síndrome (4.91),

$$\tilde{u}_i^{(1)}[l] = \sum_{n=0}^{N-1} \tilde{c}[n] h_i[((Ml - n))_N], \tag{4.90}$$

para $i \in \mathbf{C}$, e

$$s_i[l] = \sum_{n=0}^{N-1} \tilde{c}[n] h_i[((Ml - n))_N], \tag{4.91}$$

para $i \notin \mathbf{C}$. Se $\tilde{c}[n]$ pertence ao código, então $s_i[n] = 0$ para $n = 0, 1, \ldots, N/M - 1$.

Partindo da estrutura básica, é possível montar outros tipos de estruturas.

Estrutura BFC com Árvore Wavelet

A estrutura BFC (EBFC) para wavelets é mostrada na Figura 4.23. Para este caso, o código pode ser formado retirando os níveis de detalhes dos primeiros estágios $u_1^{(j)}[n]$. Na verdade não há uma regra específica na escolha dos detalhes a serem retirados; essa escolha influencia diretamente nos parâmetros K e d do código. Retirando-se os $J_0 - 1$ primeiros

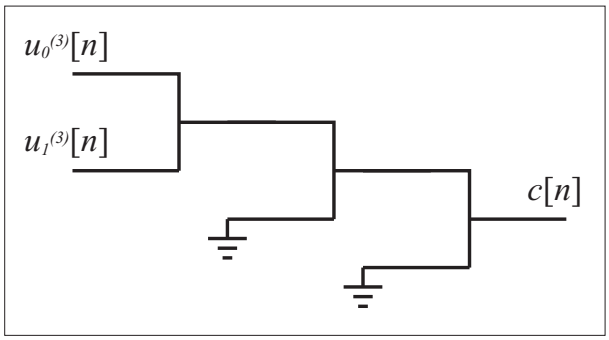


Figura 4.23: Estrutura BFC com árvore wavelets

detalhes para geração de $c[n]$, tem-se

$$c[n] = \sum_{j=J_0}^{J} \sum_{l=0}^{N/2^j-1} u_1^{(j)}[l] g_1^j[((n - 2^j l))_N] + \sum_{l=0}^{N/2^J-1} u_0^{(J)}[l] g_0^J[((n - 2^J l))_N]. \tag{4.92}$$

Para este caso, a decodificação fica

$$\tilde{u}_i^{(j)}[l] = \sum_{n=0}^{N-1} \tilde{c}[n] h_i^{(j)}[((2^j l - n))_N], \tag{4.93}$$

para $l = 0, 1, \ldots, N/2^j - 1$ e $j = J_0, J_0 + 1, \ldots, J$. As síndromes são dadas por

$$s_1^{(j)}[l] = \sum_{n=0}^{N-1} \tilde{c}[n] h_1^{(j)}[((2^j l - n))_N], \tag{4.94}$$

para $l = 0, 1, \ldots, N/2^j - 1$ e $j = 1, 2, \ldots, J_0 - 1$.

Exemplo 4.4

Considere a EBFC projetada para $GF(9)$ com $N = 8$. É possível projetar os filtros no corpo $GF(3) \subset GF(9)$, $J = 3$. A estrutura está mostrada na Figura 4.23 e forma o código

$C_1(8,2,d)$. Os filtros escolhidos, satisfazendo a condição RP, são:

$G_0(z) = 2 + 2z^{-1} + 2z^{-5} + 2z^{-6}$,

$G_1(z) = 2z^{-1} + 2z^{-2} + 2z^{-3}$,

$H_0(z) = 1 + 2z^{-1} + z^{-2}$,

$H_1(z) = 2 + 2z^{-4} + z^{-5} + z^{-7}$. Analisando a distância mínima do código para essa estrutura com esses filtros, tem-se $d = 4$. A equação do código se reduz a

$$c[n] = u_1^{(3)}[0]g_1^j[n] + u_0^{(3)}[0]g_0^J[n].$$

Gerando a palavra código a partir de

$u_1^{(3)}[0] = 1$;

$u_0^{(3)}[0] = 2$;

tem-se:

$c[n] = [0\ 2\ 0\ 2\ 1\ 2\ 1\ 2]$. Como $d = 4$, esse código detecta até três erros. A EBFC de análise é mostrada na Figura 4.24. Considerando

$\tilde{c}[n] = [0\ 2\ 0\ 2\ 1\ 2\ 1\ 2] + [1\ 0\ 0\ 2\ 0\ 1\ 0\ 0]$, o decodificador apresenta

$s_1^{(1)}[n] = [0\ 0\ 0\ 0]$,

$s_1^{(2)}[n] = [1\ 1] \neq 0$, (Erro detectado)

$u_1^{(3)}[0] = 0$,

$u_0^{(3)}[0] = 1$. Modificando a estrutura de entrada da EBFC para anular a posição $u_1^{(3)}[0]$, o código resultante é o de repetição $C(8,1,8)$.

•

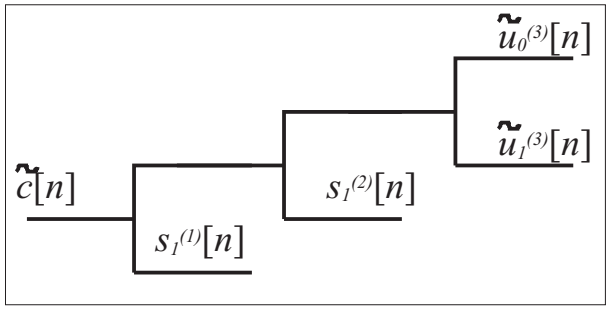


Figura 4.24: Estrutura BFC de análise do Exemplo 4.4.

O código produzido varia com os filtros projetados e com a estrutura de entrada escolhida, possibilitando uma grande variação de códigos a serem produzidos.

Estrutura BFC com Árvore Completa

A EBFC com árvore completa é uma estrutura mais ampla, no sentido de que engloba as estruturas BFC com árvore wavelet. Um exemplo dessa estrutura é apresentada na Figura 4.25. Nessa estrutura, escolhe-se a EBFC básica e forma-se uma árvore completa até o maior

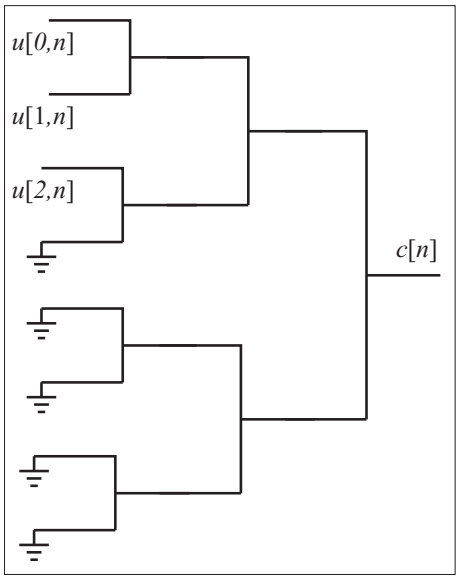


Figura 4.25: Estrutura BFC com árvore completa.

número possível de estágios. Escolhe-se a estrutura de entrada e o código é produzido por interações BFC, assim como na estrutura anterior. Para essa situação, a transformada associada é análoga à TFCD. A TFCD cíclica (TFCDC) sobre corpos finitos, para um BFC básico de M canais e com J estágios, é dada por

$$X[k,l] \triangleq \sum_{n=0}^{N-1} x[n] h^{(k)}[((M^J l - n))_N], \tag{4.95}$$

para $l = 0, 1, \ldots, N/M^J - 1$ e $k = 0, 1, \ldots, M^J - 1$. A TFCDC inversa é dada por

$$x[n] = \sum_{k=0}^{M^J-1} \sum_{l=0}^{N/M^J-1} X[k,l] g^{(k)}[((n - M^J l))_N], \tag{4.96}$$

para $n = 0, 1, \ldots, N-1$. As seqüências $h^{(k)}[n]$ e $g^{(k)}[n]$ são obtidas no domínio Z por

$$H^{(\sum_{j=0}^{J-1} a_j M^j)}(z) = \prod_{j=0}^{J-1} H_{a_j}(z^{M^{J-1-j}})(mod\ z^{-N} - 1) \tag{4.97}$$

e

$$G^{(\sum_{j=0}^{J-1} a_j M^j)}(z) = \prod_{j=0}^{J-1} G_{a_j}(z^{M^{J-1-j}})(mod\ z^{-N} - 1), \tag{4.98}$$

onde os a_j podem assumir valores entre 0 e $M-1$. A partir desses valores, obtém-se todos os filtros $G^{(k)}(z)$ e $H^{(k)}(z)$. Análogo ao caso não cíclico apresentado no capítulo 3.

Supondo o caso particular em que $M = 2$ e $N = 2^J$, usando a notação para códigos e escolhendo a estrutura de entrada, tem-se

$$c[n] = \sum_{k \in \mathbf{C}} u[k,0] g^{(k)}[n], \tag{4.99}$$

sendo as equações de decodificação e de síndrome dadas por

$$\tilde{u}[k,0] = \sum_{n=0}^{N-1} \tilde{c}[n] h^{(k)}[((-n))_N], \tag{4.100}$$

para $k \in \mathbf{C}$, e

$$s[k,0] = \sum_{n=0}^{N-1} \tilde{c}[n] h^{(k)}[((-n))_N], \tag{4.101}$$

para $k \notin \mathbf{C}$.

Exemplo 4.5

Considera-se a mesma EBFC básica do exemplo 4.4 em $GF(9)$, com a estrutura de entrada mostrada na Figura 4.26. Nessa situação o código gerado é $C_2(8,3,4)$ para $GF(3)$. O código pode ser obtido por

$$c[n] = \sum_{k=0}^{2} u[k,0] g^{(k)}[n],$$

onde

$$G^{(0)}(z) = G_0(z) G_0(z^2) G_0(z^4),$$
$$G^{(1)}(z) = G_0(z) G_0(z^2) G_1(z^4),$$
$$G^{(2)}(z) = G_0(z) G_1(z^2) G_0(z^4).$$

Para decodificação e cálculo da síndrome, pode-se utilizar a estrutura da Figura 4.27.

•

Estrutura BFC Mista

Estruturas BFC mistas são formadas por mais de uma EBFC básica com número de canais diferentes. Dessa forma é possível fatorar o comprimento do código N. Um exemplo para $N = 15$ está mostrado na Figura 4.28.

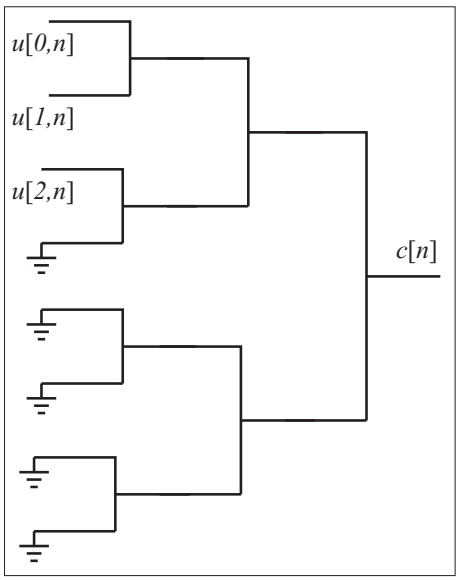


Figura 4.26: Estrutura BFC de síntese com árvore completa do exemplo 4.5.

Exemplo 4.6

Considere o corpo $GF(2^4)$, com $N = 15$ e α raiz do polinômio primitivo $\pi(x) = 1+x+x^4$. Os filtros da estrutura básica de 3 canais são dados no domínio da TFCF:

$H_0[k] = G_0[k] = [1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$,

$H_1[k] = G_1[k] = [0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0]$,

$H_2[k] = G_2[k] = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1]$,

e os da estrutura básica de 5 canais, por

$H_0^*[k] = G_0^*[k] = [1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$,

$H_1^*[k] = G_1^*[k] = [0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$,

$H_2^*[k] = G_2^*[k] = [0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0]$,

$H_3^*[k] = G_3^*[k] = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0]$,

$H_4^*[k] = G_4^*[k] = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1]$.

Filtros construídos por essa regra sempre satisfazem a condição RP. A estrutura de entrada da Figura 4.28 gera o código Reed-Solomon $C_3(15, 2, 14)$ com polinômio gerador dado por $g(x) = (x - \alpha^0)(x - \alpha^1)\ldots(x - \alpha^{12})$.

•

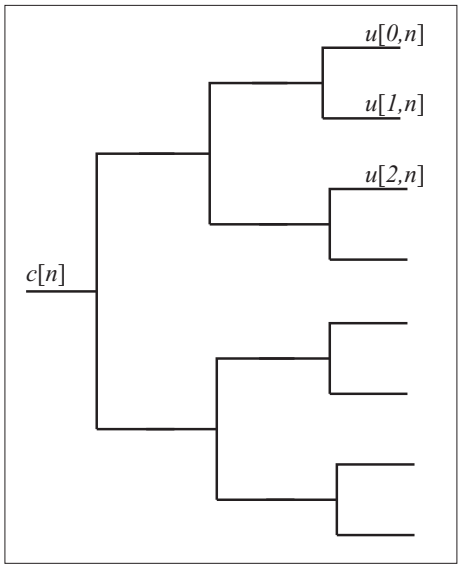


Figura 4.27: Estrutura BFC de análise com árvore completa do exemplo 4.5.

4.7.2 Projeto de Códigos com árvore completa de J-estágios

Um método para o projeto de bons códigos lineares (no sentido de maximizar d) é apresentado com estruturas BFC para um dado corpo $GF(q)$. O procedimento consiste nos seguintes passos:

1. Escolher um valor apropriado para $N = M^J$ com $MDC(M, p) = 1$, onde p é a característica do corpo;
2. Projetar os filtros da estrutura básica BFC. O código muda de acordo com o filtro produto, $P(z) = H_0(z)G_0(z)$, e para cada fatoração escolhida;
3. Calcular a matriz de transformação da TFCDC encontrando os $g^{(i)}[n]$ através de (4.98). Cada coluna dessa matriz constitui as linhas da EBFC com árvore completa. Escolher as componentes de entrada ($i \in \mathbf{C}$) significa escolher as linhas da matriz G geradora do código. A quantidade de colunas escolhidas constitui o parâmetro K do código;
4. Escolher as colunas cuja combinação linear resulte no código de maior distância mínima, definindo a estrutura de entrada. A sugestão é aplicar a TFCF na matriz de transformação da TFCDC e escolher o grupo que apresentar maior número de zeros consecutivos em suas combinações lineares. Dessa forma, se existe $\delta - 1$ zeros consecutivos, o código terá $d \geq \delta$ (cota BCH [22]).

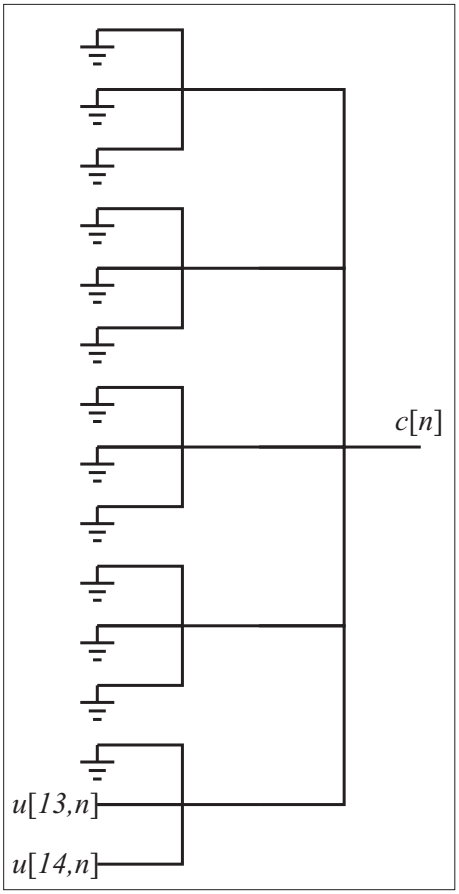


Figura 4.28: Estrutura BFC mista para $N = 15$, mesma configuração do exemplo 4.6.

Exemplo 4.7

Código de Hamming $C_4(4, 2, 3)$ em $GF(3)$, pelo método ACJ.

1. $N = 4 = 2^2 \Rightarrow 4|(3^2 - 1)$.
2. Escolhe-se o filtro produto $P(z) = 1$ que satisfaz a condição RP. Isto significa que $H_0(z) = G_0(z)^{-1}(mod\ z^{-4} - 1)$.

   Escolhendo

   $H_0(z) = z^{-1} + z^{-2} + 2z^{-3}$,

   $G_0(z) = 1 + z^{-1} + 2z^{-3}$,

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

   $G_1(z) = 1 + 2z^{-1} + 2z^{-2}$.

3. Calculando todos os $g^{(i)}[n]$, tem-se que

$$\begin{bmatrix} c[0] \\ c[1] \\ c[2] \\ c[3] \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 2 \\ 2 & 2 & 0 & 1 \end{bmatrix} \begin{bmatrix} u[0,0] \\ u[1,0] \\ u[2,0] \\ u[3,0] \end{bmatrix}.$$

Escolhe-se a segunda e a terceira coluna da matriz de transformação da TFCD para definir a estrutura de entrada. A EBFC mostrada na Figura 4.29 gera o código de Hamming ternário $C_4(4,2,3)$. A estrutura de análise está na Figura 4.30 e a matriz geradora do código, G, pode ser obtida pela matriz da TFCD, resultando em

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

A matriz de paridade H pode ser encontrada através de (4.101), sendo dada por

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

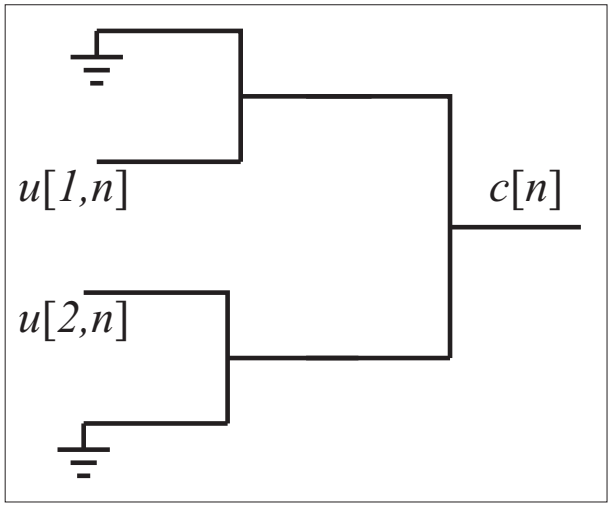


Figura 4.29: Estrutura BFC geradora do código de Hamming $C_4(4,2,3)$, em $GF(3)$, do exemplo 4.7.

•

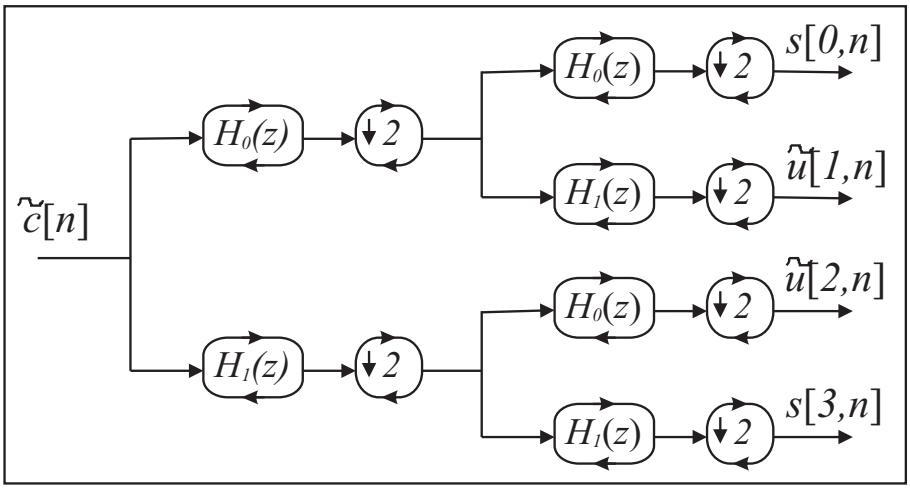


Figura 4.30: Estrutura de análise do exemplo 4.7.

Exemplo 4.8

Em $GF(3)$, procura-se um código linear $C_5(8,2,d)$ com máximo d, utilizando a mesma estrutura básica BFC do exemplo 4.4. Pode-se escrever a matriz da TFCDC como sendo

$$c[n] = \begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 2 & 2 & 0 \\ 1 & 0 & 2 & 0 & 1 & 2 & 0 & 1 \\ 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 2 & 0 & 2 & 2 & 1 & 2 & 0 \\ 1 & 0 & 2 & 0 & 1 & 1 & 0 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 0 & 1 & 0 & 1 & 2 & 0 & 2 \end{bmatrix} u[k,0].$$

Escolhendo as colunas 6 e 8, obtem-se a matriz G do código $C_5(8,2,6)$

$$G = \begin{bmatrix} 2 & 2 & 0 & 1 & 1 & 1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 \end{bmatrix}$$

e a EBFC mostrada na Figura 4.31.

•

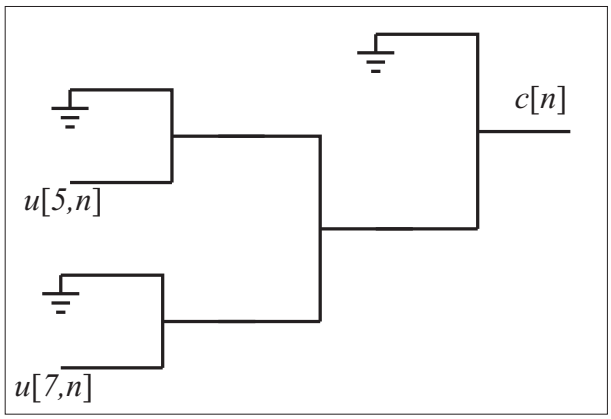


Figura 4.31: Estrutura BFC do exemplo 4.8, $C_5(8,2,6)$.

capítulo 5

A Teoria de Wavelets e Wavelets Cíclicas sobre Corpos de Característica Dois

Existem alguns artigos publicados sobre wavelets e banco de filtros sobre corpos finitos [9, 10]. Em geral, corpos finitos de característica $p = 2$ não são estudados. Não pela falta de interesse mas sim porque os corpos $GF(2^m)$ apresentam situações diferentes para serem tratadas. O primeiro avanço no estudo de banco de filtros sobre corpos de característica dois foi um artigo de Fekri, Mersereau e Schafer [11], no qual apresenta-se uma análise de matrizes paraunitárias sobre $GF(2^m)$, com o objetivo de estabelecer um método capaz de gerar todas as matrizes paraunitárias (MxM) de um determinado grau.

Neste capítulo é introduzida a teoria de banco de filtros de dois canais e wavelets, não cíclicos e cíclicos, sobre corpos de característica dois. Este estudo apresenta novas equações de reconstrução perfeita, estuda filtros ortogonais e biortogonais, além de mostrar exemplos da condição ortonormal (matrizes polifásica paraunitárias).

Para banco de filtros com M canais (não cíclicos), M ímpar, pode-se utilizar as equações mostradas no capítulo 3, pois, $MDC(M, 2) = 1$. Quando $M = 2$ para $GF(2^m)$, as equações do capítulo 3 não funcionam. Dessa forma, é necessário uma nova relação RP para banco de filtros de dois canais para esses corpos.

5.1 Banco de Filtros de Dois Canais e Wavelets sobre $GF(2^m)$

A condição RP para dois canais sobre $GF(2^m)$ é relevante para o projeto de banco de filtros. Além disso, banco de filtros de dois canais podem ser combinados com banco de filtros de número ímpar de canais para obter banco de filtros com M, onde M pode ser qualquer valor inteiro.

5.1.1 Banco de Filtros de Dois Canais sobre $GF(2^m)$

Como foi mencionado no capítulo 3, para se obter a condição RP para M canais é necessário representar a seqüência $s_M[n]$ nesse corpo. Para $GF(2^m)$, $s_2[n] = (n+1)$, levando ao teorema a seguir.

Teorema 5.1 *Num corpo finito $GF(2^m)$, a transformada Z da saída de um subamostrador por 2, $X_d(z)$, e do conjunto subamostrador-sobreamostrador por 2, $X_s(z)$, podem ser expressas em termos da transformada Z da entrada $X(z)$ (Figura 5.1), respectivamente, por*

$$X_d(z) = z^{\frac{1}{2}} X'(z^{\frac{1}{2}}) + X(z^{\frac{1}{2}}) \tag{5.1}$$

e

$$X_s(z) = zX'(z) + X(z) \tag{5.2}$$

onde $X'(z) = \frac{d}{dz}X(z)$ é a derivada em z de $X(z)$.

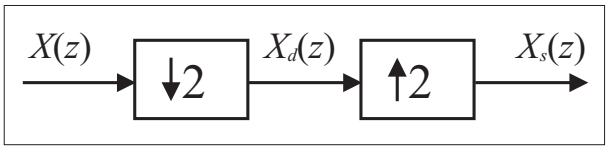


Figura 5.1: Diagrama demonstrando o esquema do subamostrador e o conjunto subamostrador-sobreamostrador de parâmetro $M = 2$.

Demonstração: Observa-se que $x_s[n]$ em $GF(2^m)$ pode ser expresso como

$$x_s[n] = (n+1)x[n] = nx[n] + x[n]. \tag{5.3}$$

Aplicando a transformada Z e utilizando a propriedade da derivada na Tabela 3.1, tem-se que

$$X_s(z) = zX'(z) + X(z). \tag{5.4}$$

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

Com essas expressões, é possível deduzir uma nova condição de reconstrução perfeita para corpos finitos de característica $p = 2$ com dois canais, inédita na literatura. A dificuldade em encontrar a condição RP para corpos de característica dois surge na representação da seqüência $s_2[n]$ na forma usual (o inverso multiplicativo de dois não existe nesses corpos).

Teorema 5.2 *Num corpo finito $GF(2^m)$, a condição de reconstrução perfeita com retardo de d, num banco de filtros de dois canais, é*

$$\begin{bmatrix} H_0(z) & H_1(z) \\ H_0'(z) & H_1'(z) \end{bmatrix} \begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \begin{bmatrix} 0 \\ z^{-1-d} \end{bmatrix}. \tag{5.5}$$

Demonstração: Pelo diagrama da Figura 3.5 e utilizando o Teorema 5.1, pode-se escrever

$$[z(H_0(z)X(z))' + H_0(z)X(z)]G_0(z) + [z(H_1(z)X(z))' + H_1(z)X(z)]G_1(z) = z^{-d}X(z). \tag{5.6}$$

ou seja,

$$\begin{aligned} X(z)[z(G_0(z)H_0'(z) + G_1(z)H_1'(z)) + H_0(z)G_0(z) + H_1(z)G_1(z)] + \\ zX'(z)[H_0(z)G_0(z) + H_1(z)G_1(z)] = z^{-d}X(z). \end{aligned} \tag{5.7}$$

Para que ocorra reconstrução perfeita, a componente $X'(z)$ deve ser anulada. Então

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 0 \tag{5.8}$$

e

$$z[G_0(z)H_0'(z) + G_1(z)H_1'(z)] + H_0(z)G_0(z) + H_1(z)G_1(z) = z^{-d}. \tag{5.9}$$

Substituindo (5.8) em (5.9), tem-se as duas condições de reconstrução perfeita

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 0 \tag{5.10}$$

e

$$G_0(z)H_0'(z) + G_1(z)H_1'(z) = z^{-1-d}. \tag{5.11}$$

■

Teorema 5.3 (Reciprocidade para 2 canais) *Se $H_0(z)$ e $H_1(z)$ são filtros de análise e $G_0(z)$ e $G_1(z)$ são filtros de síntese de um banco de filtros com reconstrução perfeita de dois canais, então o banco de filtros que possui $G_0(z)$ e $G_1(z)$ como filtros de análise e $H_0(z)$ e $H_1(z)$ como filtros de síntese satisfaz a condição de reconstrução perfeita.*

Demonstração: Considere que o corpo é da forma $GF(p^m)$, com p ímpar. Então a condição de reconstrução perfeita, pelo Corolário (3.2), é

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 2 \tag{5.12}$$

e

$$H_0(-z)G_0(z) + H_1(-z)G_1(z) \triangleq \theta(z) = 0. \tag{5.13}$$

Trocando $H_0(z)$ por $G_0(z)$ e $H_1(z)$ por $G_1(z)$, as equações ficam

$$G_0(z)H_0(z) + G_1(z)H_1(z) = H_0(z)G_0(z) + H_1(z)G_1(z) = 2 \tag{5.14}$$

e

$$G_0(-z)H_0(z) + G_1(-z)H_1(z) = \theta(-z) = 0, \tag{5.15}$$

e portanto, a condição de reconstrução perfeita é satisfeita.

Na situação em que o corpo é da forma $GF(2^m)$ a condição de reconstrução perfeita é

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 0 \tag{5.16}$$

e

$$H_0'(z)G_0(z) + H_1'(z)G_1(z) = z^{-1}. \tag{5.17}$$

Trocando $H_0(z)$ por $G_0(z)$ e $H_1(z)$ por $G_1(z)$, a primeira equação não se altera. Para a segunda equação é necessário avaliar

$$\theta(z) = G_0'(z)H_0(z) + G_1'(z)H_1(z). \tag{5.18}$$

Derivando ambos os membros da relação

$$G_0(z)H_0(z) = G_1(z)H_1(z), \tag{5.19}$$

o resultado é

$$G_0'(z)H_0(z) + G_0(z)H_0'(z) = G_1'(z)H_1(z) + G_1(z)H_1'(z), \tag{5.20}$$

o que implica que

$$G_0'(z)H_0(z) + G_1'(z)H_1(z) = G_0(z)H_0'(z) + G_1(z)H_1'(z). \tag{5.21}$$

Portanto,

$$\theta(z) = G_0'(z)H_0(z) + G_1'(z)H_1(z) = H_0'(z)G_0(z) + H_1'(z)G_1(z) = z^{-1} \tag{5.22}$$

e logo ocorre reconstrução perfeita. ■

Isto significa que, em banco de filtros de dois canais sobre corpos finitos, é possível trocar os filtros de análise com os de síntese e ainda assim a condição de reconstrução perfeita é satisfeita. Embora não mencionado, isto ocorre também no corpo dos reais.

5.1.2 Projeto do Banco de Filtros sobre $GF(2^m)$

Utilizando o Teorema 5.2, é possível obter uma expressão para os filtros de síntese, $G_0(z)$ e $G_1(z)$, a partir dos filtros de análise, $H_0(z)$ e $H_1(z)$. Pode-se escrever que

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \frac{1}{H_0(z)H_1'(z) + H_1(z)H_0'(z)} \begin{bmatrix} H_1'(z) & H_1(z) \\ H_0'(z) & H_0(z) \end{bmatrix} \begin{bmatrix} 0 \\ z^{-1-d} \end{bmatrix}. \tag{5.23}$$

Definindo o filtro produto binário $P_b(z)$ como

$$P_b(z) \triangleq H_0(z)H_1(z), \tag{5.24}$$

os filtros de síntese podem ser encontrados através de

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = \frac{z^{-1-d}}{P_b'(z)} \begin{bmatrix} H_1(z) \\ H_0(z) \end{bmatrix}. \tag{5.25}$$

Desde que a derivada do filtro produto binário seja não nula, é possível recuperar a entrada a partir dos dados de análise. Uma situação que resulta em filtros FIR é quando $P_b'(z)$ é um retardo puro. Escolhendo $d = 0$ e $P_b(z)$ da forma

$$P_b(z) = z^{-l} + \sum_{k=-\infty}^{\infty} a_{2k} z^{-2k}, \tag{5.26}$$

onde l é ímpar e a_{2k} são constantes de $GF(2^m)$, os filtros podem ser encontrados por

$$G_0(z) = z^l H_1(z) \tag{5.27}$$

e

$$G_1(z) = z^l H_0(z). \tag{5.28}$$

Proposição 5.1 *Método de projeto de banco de filtros FIR de dois canais sobre $GF(2^m)$:*

- *Escolher um filtro $P_b(z)$ satisfazendo (5.26);*
- *Fatorar $P_b(z)$ em $H_0(z)H_1(z)$;*

- *Utilizar as equações*

$$G_0(z) = z^l H_1(z) \tag{5.29}$$

e

$$G_1(z) = z^l H_0(z), \tag{5.30}$$

com l ímpar e idêntico ao da Equação (5.26), para encontrar $G_0(z)$ e $G_1(z)$.

Exemplo 5.1

Projetar um banco de filtro sobre $GF(2)$ com $H_0(z) = 1 + z^{-1}$. Escolhendo $l = 1$ e $H_1(z) = a + bz^{-1} + cz^{-2} + dz^{-3}$, então

$$P_b(z) = a + (a+b)z^{-1} + (b+c)z^{-2} + (c+d)z^{-3} + dz^{-4}.$$

Para satisfazer (5.26)

$$a + b = 1,\ c + d = 0.$$

Uma solução é

$$a = c = d = 1,\ b = 0.$$

Assim os filtros de análise são

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

e

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

Os filtros de síntese são

$$G_0(z) = zH_1(z) = z + z^{-1} + z^{-2}$$

e

$$G_1(z) = zH_0(z) = z + 1.$$

•

5.1.3 Aplicações em Códigos Convolucionais

Banco de filtros de análise sobre $GF(2^m)$ podem ser vistos como codificadores de códigos convolucionais.

Considere o esquema da Figura 5.2 sobre $GF(2)$. Esta estrutura é utilizada para gerar códigos convolucionais [23]. As estruturas de codificação e decodificação são semelhantes às apresentadas no capítulo anterior para códigos de bloco.

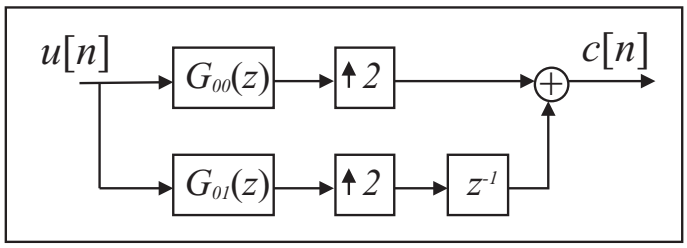


Figura 5.2: Estrutura utilizada para gerar códigos convolucionais, Exemplo 5.2.

Exemplo 5.2

Na Figura 5.2, os filtros são

$$G_{00}(z) = 1 + z^{-2}$$

e

$$G_{01}(z) = 1 + z^{-1} + z^{-2}.$$

A estrutura pode ser vista como um "interpolador" implementado de forma polifásica. Utilizando a segunda identidade nobre, a estrutura pode ser implementada da forma mostrada na Figura 5.3, onde

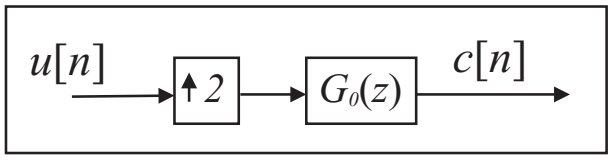


Figura 5.3: Implementação equivalente à estrutura da Figura 5.2 do Exemplo 5.2.

$$G_0(z) = G_{00}(z^2) + z^{-1}G_{01}(z^2) = 1 + z^{-1} + z^{-3} + z^{-4} + z^{-5}.$$

Essa estrutura é parte de um banco de filtro de síntese. Pode-se então utilizar a equação do filtro produto binário para encontrar um possível $G_1(z)$. Como neste problema é mais fácil encontrar os filtros de síntese, utiliza-se a reciprocidade dos bancos. Então

$$P_b(z) = G_0(z)G_1(z)$$

e, escolhendo $l = 1$,

$$H_0(z) = zG_1(z),$$
$$H_1(z) = zG_0(z).$$

Supondo que

$$G_1(z) = a + bz^{-1} + cz^{-2} + dz^{-3}$$

então

$$P_b(z) = a + (a+b)z^{-1} + (b+c)z^{-2} + (a+c+d)z^{-3} + (a+b+d)z^{-4} + (a+b+c)z^{-5} + (b+c+d)z^{-6} + (c+d)z^{-7} + cz^{-8}.$$

Para satisfazer (5.26) com $l = 1$ é necessário que

$$a + b = 1,\ a + b + d = 0,\ a + b + c = 0,\ c + d = 0.$$

Uma solução é

$$a = 0,\ b = c = d = 1.$$

Assim, o conjunto é

$$H_0(z) = 1 + z^{-1} + z^{-2},$$

$$H_1(z) = z + 1 + z^{-2} + z^{-3} + z^{-4},$$

$$G_0(z) = 1 + z^{-1} + z^{-3} + z^{-4} + z^{-5}$$

e

$$G_1(z) = z^{-1} + z^{-2} + z^{-3}.$$

Isso significa que é possível obter $u[n]$ a partir de $c[n]$ com a estrutura mostrada na Figura 5.4. Além disso, é possível construir uma estrutura para detectar erros (Figura 5.5), se $s[n] \neq 0$ então $c[n]$ não pertence ao código. Ambas podem ser simplificadas ainda mais utilizando a decomposição polifásica. O exemplo sugere uma síndrome $s[n]$ para códigos convolucionais, o que é uma novidade.

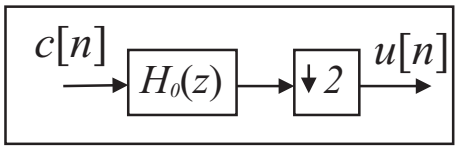


Figura 5.4: Estrutura de recuperação de $u[n]$ a partir de $c[n]$ do Exemplo 5.2.

•

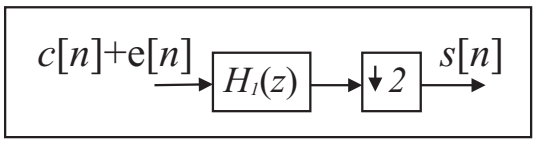


Figura 5.5: Implementação da estrutura para detecção de erros do Exemplo 5.2.

5.1.4 Implementação Polifásica

Pode-se utilizar a abordagem polifásica para se implementar estruturas reticuladas sobre corpos de característica dois. A relação RP na forma polifásica é válida independente do corpo e do número de canais.

Exemplo 5.3

Considere o corpo $GF(16)$ e α um elemento primitivo desse corpo, raiz do polinômio primitivo $\pi(x) = x^4 + x + 1$. A composição desse corpo está mostrada na Tabela 5.1.

Tabela 5.1: Corpo $GF(16)$, com $1 + \alpha + \alpha^4 = 0$.

$\alpha^{-\infty}$	0
α^0	1
α^1	α
α^2	α^2
α^3	α^3
α^4	$1+\alpha$
α^5	$\alpha+\alpha^2$
α^6	$\alpha^2+\alpha^3$
α^7	$1+\alpha+\alpha^3$
α^8	$1+\alpha^2$
α^9	$\alpha+\alpha^3$
α^{10}	$1+\alpha+\alpha^2$
α^{11}	$\alpha+\alpha^2+\alpha^3$
α^{12}	$1+\alpha+\alpha^2+\alpha^3$
α^{13}	$1+\alpha^2+\alpha^3$
α^{14}	$1+\alpha^3$

Considere as matrizes A e B dadas por

$$A = \begin{bmatrix} \alpha & \alpha^4 \\ \alpha^4 & \alpha \end{bmatrix}$$

e

$$B = \begin{bmatrix} \alpha^3 & \alpha^{14} \\ \alpha^{14} & \alpha^3 \end{bmatrix}.$$

Essas matrizes satisfazem $A^{-1} = A^T = A$ e $B^{-1} = B^T = B$, ou seja, são unitárias. Assim sendo, o banco de filtros sobre $GF(16)$ formado pela matriz polifásica de análise dada por

$$H_p(z) = A\Lambda(z)B$$

e matriz polifásica de síntese dada por

$$G_p(z) = B\Lambda(z^{-1})A$$

satisfaz a condição de reconstrução perfeita com filtros ortonormais, isto é, as matrizes são paraunitárias.

A matriz $H_p(z)$ fica

$$H_p(z) = \begin{bmatrix} \alpha^4 + \alpha^3 z^{-1} & 1 + \alpha^7 z^{-1} \\ \alpha^7 + z^{-1} & \alpha^3 + \alpha^4 z^{-1} \end{bmatrix}$$

e a matriz $G_p(z)$ pode ser encontrada pela relação $G_p(z) = H_p^T(z^{-1})$. Os filtros são

$$H_0(z) = \alpha^4 + z^{-1} + \alpha^3 z^{-2} + \alpha^7 z^{-3}$$

e

$$H_1(z) = \alpha^7 + \alpha^3 z^{-1} + z^{-2} + \alpha^4 z^{-3}.$$

Esses filtros formam bases ortonormais, de forma que

$$\langle h_i[n] h_j[n - 2m] \rangle = \delta[i - j]\delta[m],$$

para $i = \{0, 1\}$ e $m \in \mathbb{Z}$.

Outra observação é que esses filtros são ortogonais e simétricos. No corpo dos reais, os únicos filtros que possuem esta característica são os filtros de Haar [3, 4]. O corpo $GF(16)$ é utilizado no código *Reed-Solomon* [19], bastante utilizado em CDs.

•

5.1.5 Wavelets sobre $GF(2^m)$

Também é possível fazer decomposição em wavelets para corpos de característica dois para análise multirresolução. Interessante observar que, particularmente para $GF(2)$, as wavelets são ondas binárias de curta duração (para filtros FIR). Nesse contexto, pode-se utilizar a denominação de *wavelets binárias*. Um exemplo é mostrado a seguir.

Exemplo 5.4

Considerando o corpo $GF(2)$, sendo os filtros de síntese dados por

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

e

$$G_1(z) = 1 + z^{-2} + z^{-3},$$

e os filtros de análise dados por

$$H_0(z) = z + z^{-1} + z^{-2}$$

e

$$H_1(z) = z + 1,$$

verifica-se que estes filtros satisfazem a condição de reconstrução perfeita (Exemplo 5.1). É possível obter as wavelets binárias, $g_1^{(j)}[n]$ e $g_0^{(J)}[n]$, $j = 1, \ldots, J$, utilizando as equações (3.88) e (3.89). As wavelets para $J = 4$ estão mostradas nas figuras 5.6 à 5.8.

Uma observação importante, no contexto da multirresolução, é que as componentes de menor resolução, $g_1^{(4)}[n]$ e $g_0^{(4)}[n]$, estão nas saídas dos últimos estágios enquanto que a componente de maior resolução, $g_1^{(1)}[n]$, esta na saída do primeiro estágio.

A transformada pode ser utilizada para análise multirresolução; considere a seqüência $x[n]$, mostrada na Figura 5.9. Esta seqüência está representada em forma de degraus, e o impulso, $\delta[n]$, é representado logo em seguida na mesma figura.

Utilizando a TWCF,

$$x[n] \overset{W}{\longleftrightarrow} x_1^{(j)}[l], x_0^{(4)}[l].$$

A seqüência pode ser descrita por

$$x[n] = \sum_{j=1}^{4} \sum_{l=-\infty}^{\infty} x_1^{(j)}[l] g_1^{(j)}[n - 2^j l] + \sum_{l=-\infty}^{\infty} x_0^{(4)}[l] g_0^{(4)}[n - 2^4 l].$$

É possível analisar esta seqüência no contexto de multirresolução [3, 4], utilizando wavelets binárias. Considere o primeiro nível de resolução dado por

$$x_{(-1)}[n] = \sum_{l=-\infty}^{\infty} x_0^{(4)}[l] g_0^{(4)}[n - 2^4 l].$$

Os níveis de resolução r maiores são dados por

$$x_{(r)}[n] = x_{(-1)}[n] + \sum_{j=4-r}^{4} \sum_{l=-\infty}^{\infty} x_1^{(j)}[l] g_1^{(j)}[n - 2^j l],$$

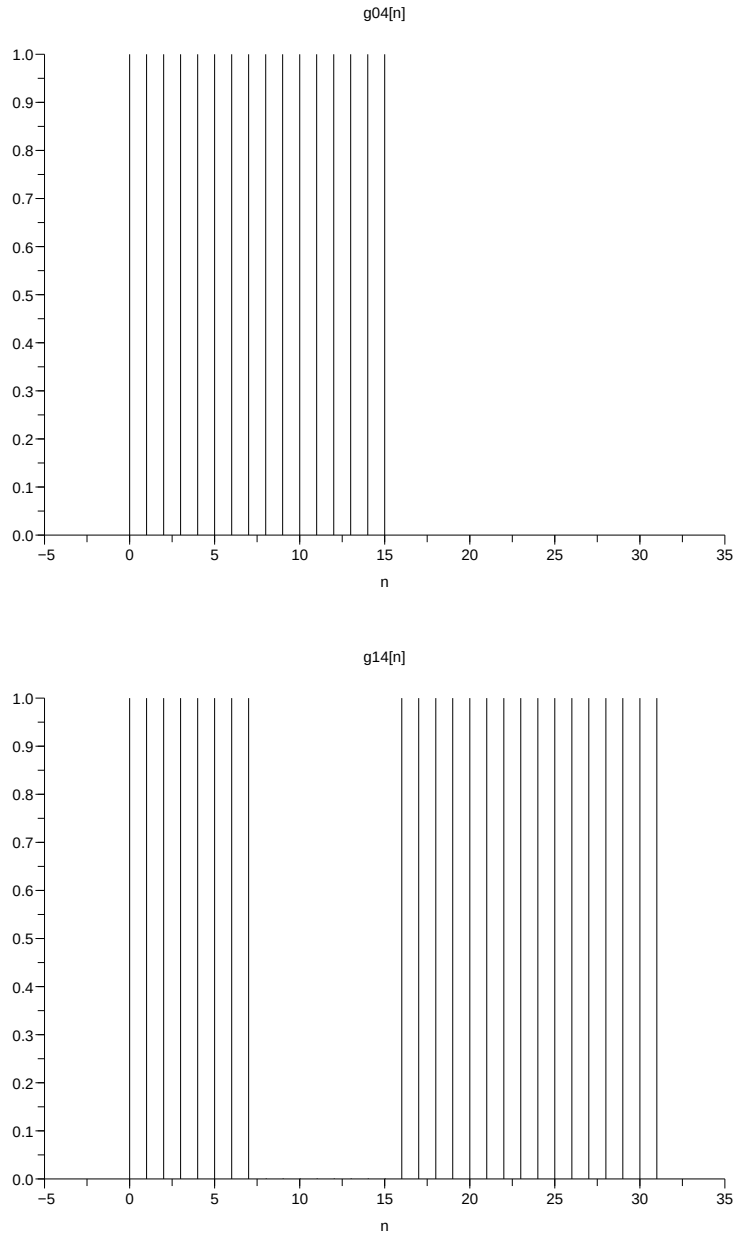


Figura 5.6: Wavelets binárias $g_0^{(4)}[n]$ e $g_1^{(4)}[n]$ do Exemplo 5.4.

para $r = 0, 1, 2, 3$. Observa-se que $x_{(3)}[n] = x[n]$.

Nas Figuras 5.10 e 5.11 são mostrados os resultados das várias resoluções de $x[n]$. Esta análise multirresolução é utilizada também com a série wavelets de tempo discreto, definida sobre o corpo dos reais [3].

•

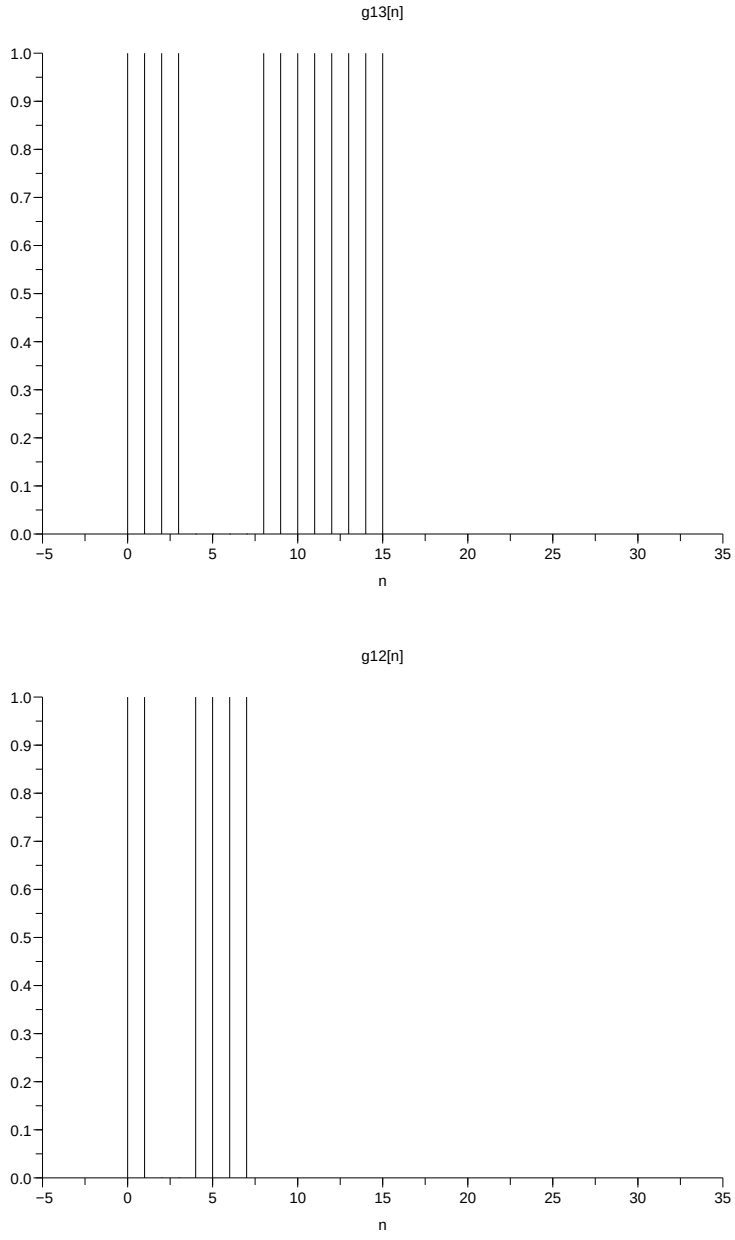


Figura 5.7: Wavelets binárias $g_1^{(3)}[n]$ e $g_1^{(2)}[n]$ do Exemplo 5.4.

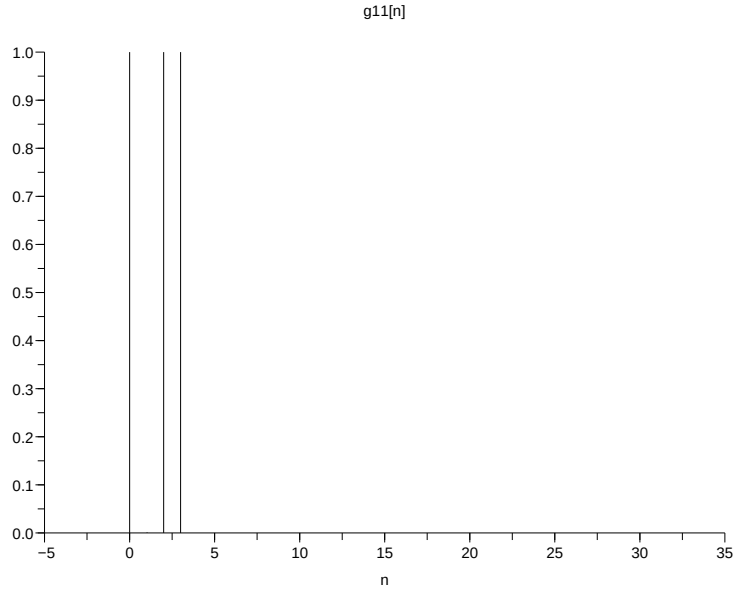


Figura 5.8: Wavelet binária $g_1^{(1)}[n]$ do Exemplo 5.4.

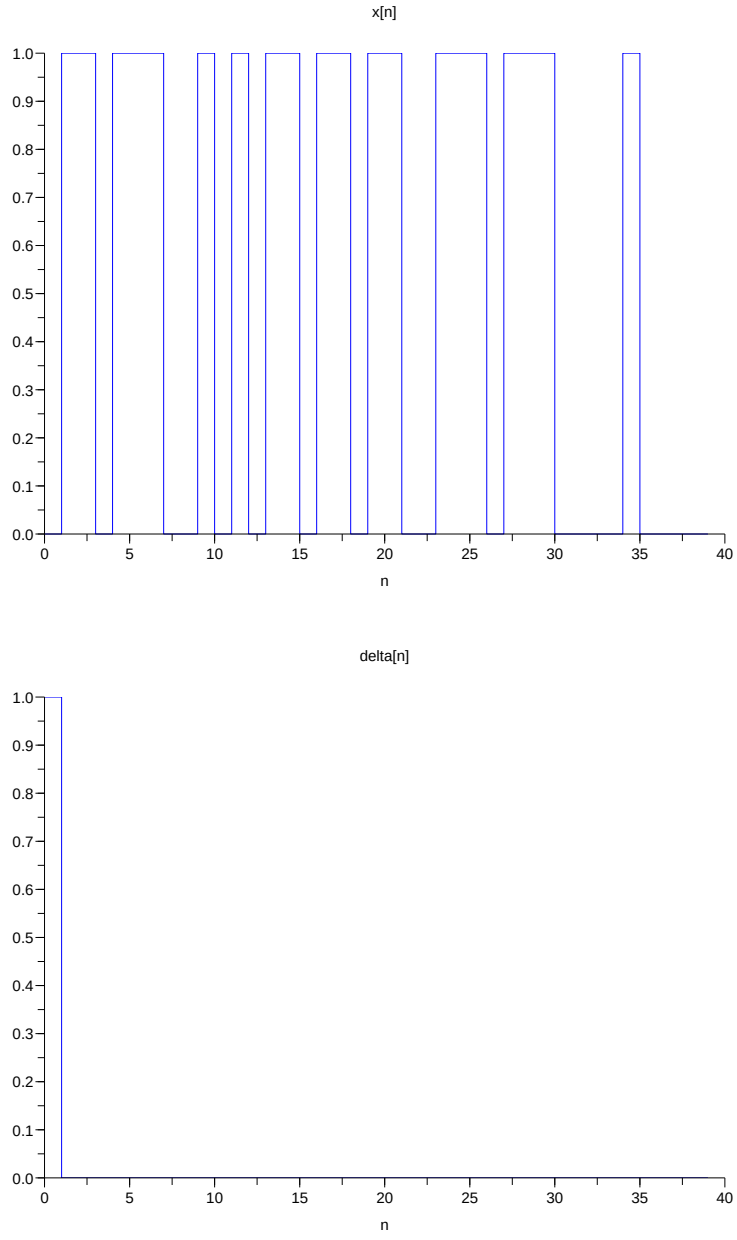


Figura 5.9: Seqüência $x[n]$ e o impulso $\delta[n]$ representados em forma de degrau, Exemplo 5.4.

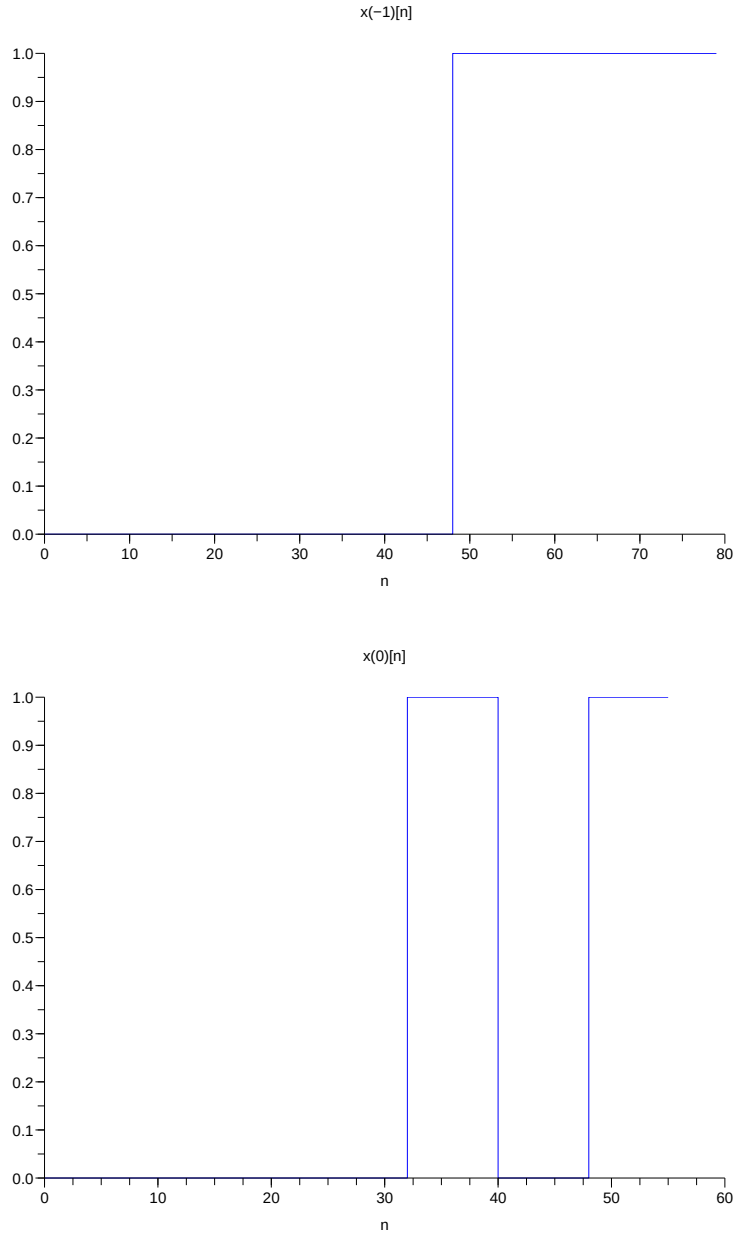


Figura 5.10: Seqüências $x_{(-1)}[n]$ e $x_{(0)}[n]$ representadas em forma de degrau, na análise multirresolução de $x[n]$ do Exemplo 5.4.

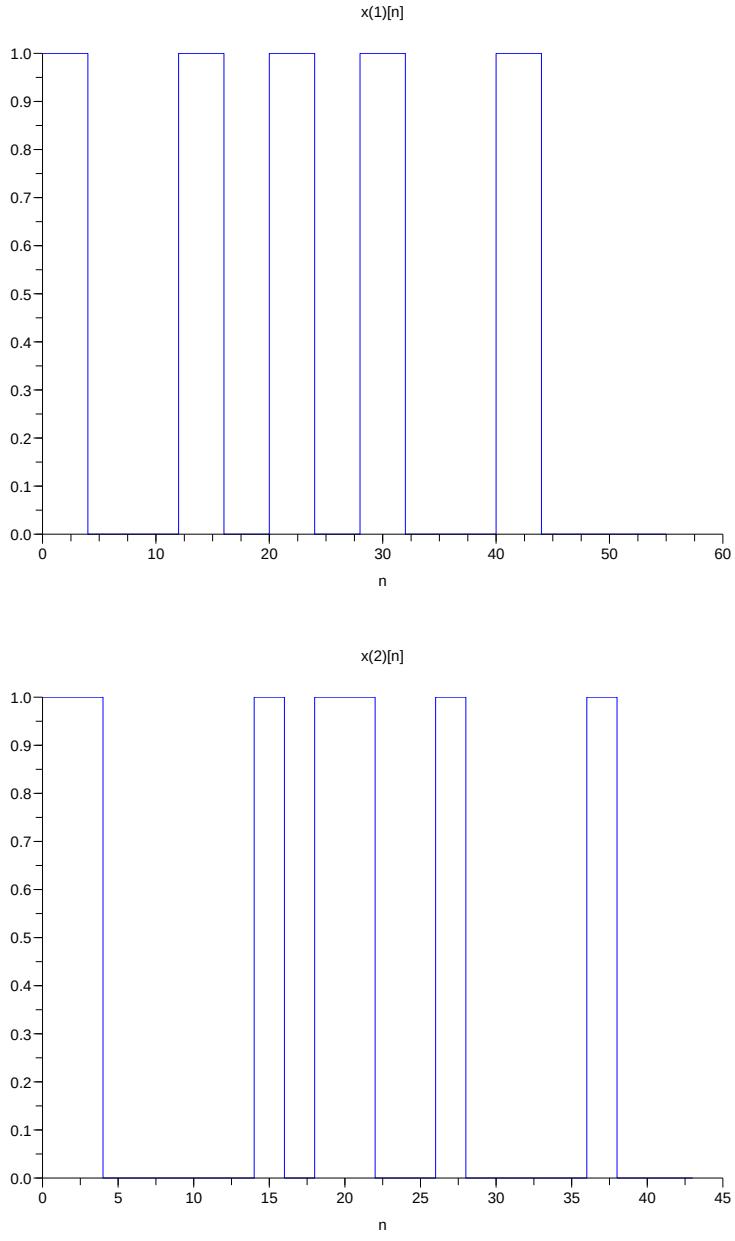


Figura 5.11: Seqüências $x_{(1)}[n]$ e $x_{(2)}[n]$ representadas em forma de degrau, na análise multirresolução de $x[n]$ do Exemplo 5.4.

5.2 Banco de Filtros e Wavelets Cíclicos sobre $GF(2^m)$

Para banco de filtros e wavelets cíclicos sobre $GF(2^m)$, é apresentada uma análise semelhante ao caso não cíclico. Para esse estudo, o comprimento N é obrigatoriamente par. Assim é possível analisar os sinais cíclicos em banco de filtros cíclicos de dois canais. Um fato interessante é que nessas condições não existe TFCF pois $MDC(N,p) \geq 2$, contudo, as equações da transformada Z cíclica são válidas para qualquer situação.

5.2.1 Banco de Filtros de Dois Canais Sobre $GF(2^m)$

Para banco de filtros cíclicos, as expressões encontradas no capítulo anterior se basearam no fato de que $MDC(N,p) = 1$ e portanto $MDC(M,p) = 1$, onde N e M são o comprimento do bloco e o número de canais, respectivamente. Para a situação particular $M = 2$ e N par sobre corpos de característica dois, as equações de saída do subamostrador e sobreamostrador no domínio da transformada Z cíclica são diferentes, embora no domínio do tempo permaneçam iguais as anteriores.

Teorema 5.4 *Num corpo $GF(2^m)$, a transformada Z cíclica da saída de um sobreamostrador por 2 (Figura 5.12), $X_e(z)$, é expressas em termos da transformada Z da entrada $X(z)$, supondo que a entrada tem período $N/2$, por*

$$X_e(z) = \frac{X(z^2)}{1 + z^{-N}}, \tag{5.31}$$

onde a fração significa divisão polinomial.

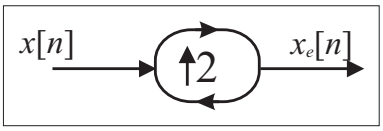


Figura 5.12: Representação de um sistema sobreamostrador por 2 cíclico.

Demonstração: Se a entrada tem período cíclico de $N/2$, a sua transformada Z cíclica é dada por

$$X(z) = \sum_{n=0}^{N-1} x[n]z^{-n} = (1 + z^{-N/2}) \sum_{n=0}^{N/2-1} x[n]z^{-n}, \tag{5.32}$$

portanto,

$$\frac{X(z)}{1 + z^{-N/2}} = \sum_{n=0}^{N/2-1} x[n]z^{-n}. \tag{5.33}$$

Pela definição (4.19), então

$$X_e(z) = \sum_{n=0}^{N/2-1} x[n]z^{-2n}, \tag{5.34}$$

o que, por (5.33), resulta no teorema. ■

Observa-se que $(1 + z^{-N/2})$ sempre divide $X(z)$ quando o mesmo vêm de uma seqüência de período cíclicos $N/2$.

Teorema 5.5 *Num corpo $GF(2^m)$, a transformada Z cíclica da saída de um subamostrador por 2, $X_d(z)$, e do conjunto subamostrador-sobreamostrador por 2, $X_s(z)$, podem ser expressas em termos da transformada Z da entrada $X(z)$ (Figura 5.13), respectivamente, por*

$$X_d(z) = (1 + z^{-N/2}) \left(z^{\frac{1}{2}} X'(z^{\frac{1}{2}}) + X(z^{\frac{1}{2}}) \right) \tag{5.35}$$

e

$$X_s(z) = zX'(z) + X(z) \tag{5.36}$$

onde $X'(z) = \frac{d}{dz}X(z)$ é a derivada formal de $X(z)$ [19].

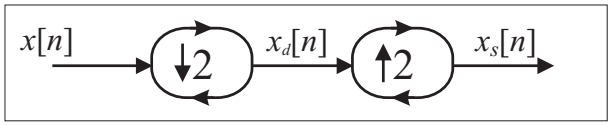


Figura 5.13: Diagrama demonstrando o esquema do subamostrador e o conjunto subamostrador-sobreamostrador, cíclicos, de parâmetro $M = 2$.

Demonstração: Observa-se que $x_s[n]$ em $GF(2^m)$ pode ser expresso como

$$x_s[n] = (n + 1)x[n] = nx[n] + x[n]. \tag{5.37}$$

Aplicando a transformada Z e utilizando a propriedade da derivada na Tabela 3.1, tem-se que

$$X_s(z) = zX'(z) + X(z). \tag{5.38}$$

Como $X_d(z) = (1 + z^{-N/2})X_s(z^{\frac{1}{2}})$, por (4.15), a prova está completa. ■

Com essas relações, é possível obter a condição RP para banco de filtros cíclicos de dois canais sobre $GF(2^m)$.

Teorema 5.6 *Num corpo finito $GF(2^m)$, a condição de reconstrução perfeita num banco de filtros cíclicos de dois canais, é*

$$\begin{bmatrix} H_0(z) & H_1(z) \\ H_0'(z) & H_1'(z) \end{bmatrix} \begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} (mod\ z^{-N}+1) = \begin{bmatrix} 0 \\ z^{-1} \end{bmatrix}. \tag{5.39}$$

Demonstração: A prova segue como no caso não cíclico, levando em consideração a aritmética polinomial módulo $(z^{-N}+1)$. ■

A parte de projeto de banco de filtros cíclicos segue a parte não cíclica, levando em conta a aritmética polinomial.

5.2.2 Projeto do Banco de Filtros Cíclicos sobre $GF(2^m)$

Utilizando o Teorema 5.6, pode-se escrever que

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = (H_0(z)H_1'(z) + H_1(z)H_0'(z))^{-1} (mod\ z^{-N}-1) \begin{bmatrix} H_1'(z) & H_1(z) \\ H_0'(z) & H_0(z) \end{bmatrix} \begin{bmatrix} 0 \\ z^{-1} \end{bmatrix}. \tag{5.40}$$

Definindo o filtro produto binário $P_b(z)$ como

$$P_b(z) \triangleq H_0(z)H_1(z)(mod\ z^{-N}+1), \tag{5.41}$$

os filtros de síntese podem ser encontrados através de

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = z^{-1}P_b'(z)^{-1} (mod\ z^{-N}+1) \begin{bmatrix} H_1(z) \\ H_0(z) \end{bmatrix}. \tag{5.42}$$

Desde que a derivada do filtro produto binário seja não nula e que

$$MDC(P_b'(z), z^{-N}+1) = 1, \tag{5.43}$$

é possível recuperar a entrada a partir dos dados de análise. Nesse caso, $P_b'(z)$ não precisar ser necessariamente um retardo puro.

Proposição 5.2 *Método de projeto de banco de filtros cíclicos de dois canais sobre $GF(2^m)$:*

- *Escolher um filtro $P_b(z)$ satisfazendo (5.43);*
- *Fatorar $P_b(z)$ em $H_0(z)H_1(z)$;*

- *Utilizar as equações*

$$G_0(z) = z^{-1}P_b'(z)^{-1}(mod\ z^{-N} - 1)H_1(z) \tag{5.44}$$

e

$$G_1(z) = z^{-1}P_b'(z)^{-1}(mod\ z^{-N} - 1)H_0(z), \tag{5.45}$$

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

Observa-se que banco de filtros não cíclicos podem ser utilizados como banco de filtros cíclicos, operando os filtros $(mod\ z^{-N} + 1)$. Entretanto, existe uma liberdade maior para banco de filtros cíclicos no projeto de $P_b(z)$.

Exemplo 5.5

Considere os filtros projetados no exemplo 5.1, $H_i(z)$ e $G_i(z)$, os quais são filtros não cíclicos. Para se projetar filtros cíclicos com $N = 8$ utilizando-se filtros não cíclicos, basta fazer simplesmente

$$H_i^c(z) = H_i(z)(mod\ z^{-8} + 1)$$

e

$$G_i^c(z) = G_i(z)(mod\ z^{-8} + 1),$$

$i = 0, 1$. É como aplicar a aritmética modular polinomial na relação RP, o resultado é a relação RP para banco de filtros cíclicos. Os filtros cíclicos são

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

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

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

e

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

Assim

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

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

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

e

$$g_1^c[n] = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 1]$$

Para uma entrada $x[n] \in GF(16)$ dada por

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

as saídas do banco são

$$x_0^{(1)}[n] = [\alpha\ \alpha^2\ 0\ 0]$$

e

$$x_0^{(1)}[n] = [\alpha\ \alpha\ \alpha^2\ 0].$$

A seqüência é recuperada no banco de síntese.

•

Exemplo 5.6

Agora, um caso diferente, que em sistemas não cíclicos resulta em filtros IIR (resposta ao impulso infinita, do inglês *Infinite Impulse Response*). Considere $N = 8$, e o filtro produto binário dado por

$$P_b(z) = 1 + z^{-1} + z^{-3} + z^{-4} + z^{-5} + z^{-6} = (1 + z^{-1})(1 + z^{-3} + z^{-5}).$$

A derivada formal desse filtro é dada por

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

satisfazendo $MDC(P_b'(z), z^{-8} + 1) = 1$. Observe também que

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

o que significa que $P_b'(z)^{-1}(mod\ z^{-8} - 1) = P_b'(z)$.

Assim, pode-se projetar os filtros pela Proposição 5.2, onde a fatoração de $P_b(z)$ escolhida é

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

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

e com isso, os filtros de síntese cíclicos são

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

e

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

Esses filtros satisfazem a condição RP, entretanto $P_b'(z)$ não é um retardo puro, situação exclusiva para banco de filtros cíclicos.

•

5.2.3 Identidades Nobres Cíclicas para $GF(2^m)$

As identidades nobres demonstradas no capítulo anterior devem ser modificadas para esta situação ($M = L = 2$, sobre $GF(2^m)$), pois as expressões do subamostrador e sobreamostrador no domínio da transformada Z cíclica se modificaram. Mesmo assim, as identidades são válidas.

Primeira Identidade Nobre

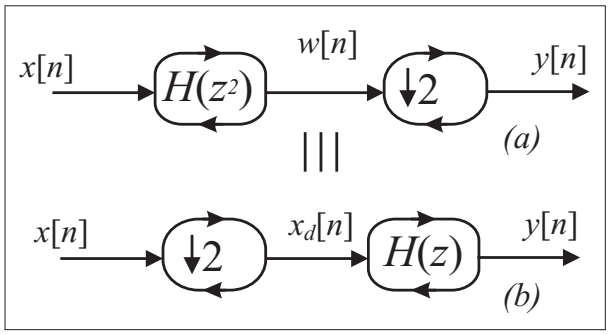


Figura 5.14: Primeira identidade nobre - Os sistemas (a) e (b) são equivalentes.

Teorema 5.7 *Os sistemas (a) e (b) da Figura 5.14 são equivalentes.*

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

$$W(z) = X(z)H(z^2)(mod\ z^{-N}+1)$$

e

$$Y(z) = W_d(z) = (1 + z^{-N/2})\left(z^{\frac{1}{2}}W'(z^{\frac{1}{2}}) + W(z^{\frac{1}{2}})\right),$$

mas

$$W'(z) = X'(z)H(z^2) + 2H'(z^2)X(z)(mod\ z^{-N}-1) = X'(z)H(z^2)(mod\ z^{-N}+1),$$

assim,

$$Y(z) = (1 + z^{-N/2}) \left(z^{\frac{1}{2}} X'(z^{\frac{1}{2}}) H(z) + X(z^{\frac{1}{2}}) H(z) \right) (mod\ z^{-N} + 1),$$

ou

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

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

Segunda Identidade Nobre

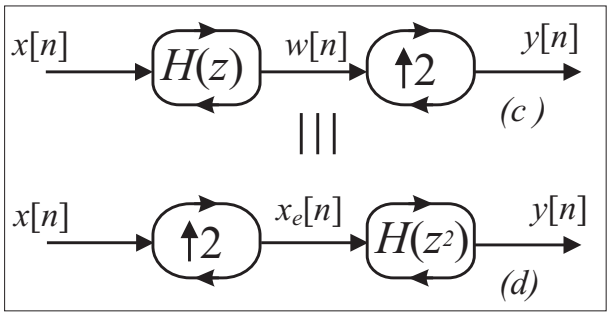


Figura 5.15: Segunda identidade nobre - Os sistemas (c) e (d) são equivalentes.

Teorema 5.8 *Os sistemas (c) e (d) da Figura 4.6 são equivalentes.*

Demonstração: Partindo do sistema (c),

$$W(z) = X(z) H(z) (mod\ z^{-N} + 1)$$

e

$$Y(z) = W_e(z) = \frac{W(z^2)}{1 + z^{-N}}$$

Se $X(z)$ tem período cíclicos $N/2$, então $(1 + z^{-N})$ divide $X(z^2)$, e então,

$$\left(\frac{X(z^2)}{1 + z^{-N}} \right) H(z^2) (mod\ z^{-N} + 1) = \left(\frac{X(z^2)}{1 + z^{-N}} H(z^2) \right) (mod\ z^{-N} + 1) = W_e(z),$$

o que significa que

$$Y(z) = X_e(z) H(z^2) (mod\ z^{-N} + 1),$$

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

5.2.4 Implementação Polifásica Cíclica para $GF(2^m)$

Outra forma para se obter banco de filtros cíclicos com RP é utilizar a condição polifásica cíclica para o projeto. As equações encontradas no capítulo anterior são válidas.

A condição RP é dada por

$$G_p(z)H_p(z)(mod\ z^{-N/2}-1) = I_2, \tag{5.46}$$

onde $G_p(z)$ e $H_p(z)$ são matrizes polifásica cíclicas de síntese e análise, respectivamente, definidas no capítulo anterior.

Exemplo 5.7

Considere $N = 8$ e uma matriz polifásica de análise, $H_p(z)$, dada por

$$H_p(z) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1+z^{-1}+z^{-3} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

ou

$$H_p(z) = \begin{bmatrix} z^{-1}+z^{-3} & 1+z^{-1}+z^{-3} \\ 1+z^{-1}+z^{-3} & 1+z^{-1}+z^{-3} \end{bmatrix}.$$

Para essa matriz $H_p(z)$, encontra-se a matriz $G_p(z)$ por

$$G_p(z) = H_p^{-1}(z)(mod\ z^{-4}+1) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1+z^{-1}+z^{-3} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

ou

$$G_p(z) = \begin{bmatrix} 1 & 1 \\ 1 & z^{-1}+z^{-3} \end{bmatrix}.$$

Os filtros de análise são obtidos pela equação da decomposição polifásica tipo I cíclica,

$$H_i(z) = \left(H_{i0}(z^2) + z^{-1}H_{i1}(z^2)\right)(mod\ z^{-8}+1), \tag{5.47}$$

e os filtros de síntese pela equação da decomposição polifásica cíclica tipo II,

$$G_i(z) = \left(G_{i0}(z^2) + zG_{i1}(z^2)\right)(mod\ z^{-8}+1). \tag{5.48}$$

Os resultados são

$$H_0(z) = z^{-1}+z^{-2}+z^{-3}+z^{-6}+z^{-7},$$

$$H_1(z) = 1+z^{-1}+z^{-2}+z^{-3}+z^{-6}+z^{-7},$$

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

e

$$G_1(z) = 1 + z^{-1} + z^{-5},$$

Os quais satisfazem a condição RP para qualquer entrada com $N = 8$.

•

5.2.5 Wavelets Cíclicas e Estruturas para Códigos de Bloco

As expressões da transformada wavelet seguem aquelas obtidas através de estruturas em árvore logarítmica, as identidades nobres apresentadas nesta seção garantem a validade das equações. Estruturas em árvore podem ser utilizadas para gerar códigos de bloco sobre $GF(2)$. O modelo da codificação e decodificação foi apresentado no capítulo anterior. Para gerar códigos em $GF(2)$ basta projetar os bancos de filtros cíclicos como mostrado no decorrer desta seção.

Exemplo 5.8

Considere os filtros cíclicos projetados no exemplo 5.5, sobre $GF(2)$ e com $N = 8$. Considere a estrutura wavelet da Figura 5.16. A matriz do geradora do código é

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

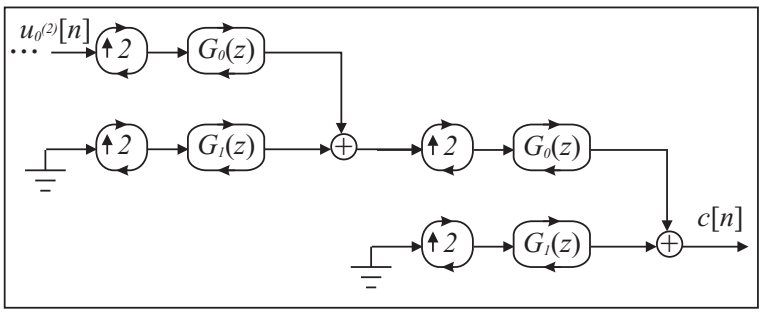


Figura 5.16: Estrutura geradora do código de bloco linear do exemplo 5.8.

Os parâmetros do códigos são: $C_1(8, 2, 5)$. Existe um código de Goppa (código de bloco) com esses mesmos parâmetros [19].

•

capítulo 6

Conclusões

6.1 Descrição Resumida do Conteúdo

Essa dissertação apresentou a teoria de banco de filtros e wavelets sobre corpos finitos. Essa dissertação foi dividida em cinco capítulos. O capítulo 1 apresenta introdução, objetivos e a organização da dissertação. O Capítulo 2 apresenta uma revisão resumida da teoria de banco de filtros e wavelets existente no corpo dos reais. No capítulo 3 é introduzida a teoria de banco de filtros com M canais sobre corpos finitos de característica p, quando $MDC(M,p) = 1$, e wavelets sobre corpos finitos de característica ímpar (caso não cíclico). No capítulo 4 é introduzida a teoria de banco de filtros e wavelets cíclicos sobre corpos finitos, bem como são apresentadas aplicações em códigos de bloco lineares. No Capítulo 5 é mostrado o caso particular para banco de filtros de dois canais sobre corpos de característica dois, e conseqüentemente, wavelets, para os casos cíclico e não cíclico. Também são apresentadas aplicações em códigos de canal (códigos convolucionais e códigos de bloco) sobre $GF(2)$.

6.2 Contribuições do Trabalho

Embora existam artigos que tratam de wavelets sobre corpos finitos [9–11, 21], essa dissertação apresenta resultados e equações inéditas na literatura. Foi mostrado que é possível obter wavelets e banco de filtros, cíclicos ou não cíclicos, para qualquer corpo finito, contrariando algumas referências conhecidas [10] e complementando outras [9]. Além disso, a teoria de banco de filtros cíclicos constitui, per si, uma novidade, tanto para corpos finitos quanto para o corpo dos reais.

Dentre as principais contribuições do trabalho, se destacam as seguintes:

- A condição de reconstrução perfeita (RP) para banco de filtros de M canais sobre corpos finitos no capítulo 3 (depende de M e da característica do corpo p);
- Uma nova expressão para a transformada Z inversa para seqüências de comprimento finito no capítulo 4 (A expressão apresentada no capítulo 4 difere da usual [10] e é válida mesmo que $MDC(N, p) \neq 1$);
- A definição dos sistemas sobreamostrador e subamostrador cíclico, o que possibilitou uma nova teoria sobre processamento multitaxa e banco de filtros, ambos cíclicos, no capítulo 4;
- A introdução da condição RP para banco de filtro de dois canais sobre corpos de característica dois, no capítulo 5 (também é mostrado como obter condições RP quando $MDC(M, p) \neq 1$). Isso possibilita novas formas de projetos de banco de filtros e wavelets biortogonais.

6.3 Sugestões e Trabalhos Futuros

Banco de filtros e wavelets, cíclicos ou não cíclicos, foram definidos para corpos finitos. Entretanto, o estudo das wavelets e dos filtros ainda não esta aprofundado. Em geral, os melhores filtros e as melhores wavelets dependem da aplicação no caso real. É de se esperar que o mesmo ocorra para corpos finitos.

Essas ferramentas têm um grande potencial em aplicações. Banco de filtros e wavelets não cíclicos podem ser utilizados em aplicações com códigos convolucionais, análise multirresolução sobre corpos finitos e espalhamento espectral, como foi mostrado em exemplos. Banco de filtros e wavelets cíclicos têm aplicações em códigos de bloco lineares e podem ser utilizados em segurança de dados [24]. No corpo dos reais, wavelets e banco de filtros cíclicos podem ser utilizados em processamento de Imagens. Trabalhos em andamento implementam análise multirresolução em imagens sem alterar suas dimensões originais, utilizando-se a FFT2D ("Fast Fourier Transform" bidimensional) e com aplicações em esteganografia e marca d'água.

Como sugestões para trabalhos futuros relativos aos temas apresentados nessa dissertação, podemos indicar:

- Um método para correção de códigos convolucionais e de bloco lineares a partir de banco de filtros definidos sobre corpos finitos. É possível demonstrar que todo código de bloco linear pode ser implementado utilizando banco de filtros cíclicos sobre corpos finitos, assim

como todo código convolucional pode ser implementado utilizando banco de filtros sobre corpos finitos;

- Um estudo relativo as matrizes paraunitárias sobre corpos finitos utilizando a k-trigonometria [6], como mostrado em exemplo nessa dissertação (Capítulo 3). A idéia é fazer algo semelhante ao artigo de Fekri et al. [11] para corpos de característica maior que dois, porém, seria bem mais simples;
- Implementar a análise multirresolução em corpos finitos para aplicações em marca d'água e esteganografia. Para isso é necessário um estudo sobre o comportamento de filtros sobre corpos finitos, bem como da amostragem ou aquisição de dados sobre corpos finitos;
- Utilizar banco de filtros sobre corpos finitos para multiplexação em multirresolução, como em [1].

Bibliografia

[1] E. A. Bouton, "Multiplexação por divisão em multirresolução: um novo sistema baseado em wavelets," Master's thesis, UFPE, Agosto 2006.

[2] H. M. de Oliveira, *Análise de Sinais para Engenheiros: uma abordagem via Wavelets*. Brasport, 2007.

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

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

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

[14] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers.* Kluwer Academic Publishers, 1987.

[15] S. W. Golomb, *Shift Register Sequences.* Holden-Day, 1967.

[16] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1996.

[17] D. M. Burton, *Elementary Number Theory*, 4th ed. McGraw-Hill, 1998.

[18] T. S. Rappaport, *Wireless Communications principles and practice*, 2nd ed. Prentice Hall PTR, 2002.

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

[20] R. E. Blahut, *Fast Algorithms for Digital Signal Processing.* Addison-Wesley Publishing Company, 1984.

[21] 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.

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

[23] R. J. McEliece, *The Theory of Information and Coding*, 2nd ed. Cambridge University Press, 2002.

[24] K. S. Chan and F. Fekri, "A block cipher cryptosystem using wavelet transforms over finite fields," *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2975–2991, October 2004.

[25] H. S. Stone, *Discrete Mathematical Structures and Their Applications*. Science Research Associates, 1973.

APÊNDICE A

Sobre Corpos Finitos

O objetivo deste apêndice é apresentar, de forma muito resumida, as principais definições e teoremas que envolvem a teoria de corpos finitos. Contudo, para um primeiro estudo, é recomendado a consulta às referências [14, 19, 25].

Definição A.1 *Um grupo $\langle G, \circ \rangle$ é uma estrutura algébrica, onde G é um conjunto e $\circ$ é uma operação sobre esse conjunto, satisfazendo os seguintes axiomas:*

(a) *(Fechamento) $g \circ h \in G$ para todo $g, h \in G$;*

(b) *(Associatividade) $g \circ (h \circ k) = (g \circ h) \circ k$ para todo $g, h, k \in G$;*

(c) *(Identidade) existe um elemento $e \in G$ tal que $e \circ g = g \circ e = g$ para todo $g \in G$;*

(d) *(Inversos) para todo $g \in G$ existe $g^{-1} \in G$ tal que $g \circ g^{-1} = g^{-1} \circ g = e$.*

Definição A.2 *Um grupo $\langle G, \circ \rangle$ é dito ser* abeliano *ou* comutativo*, quando nele vale o axioma da comutatividade, isto é, $g \circ h = h \circ g$ para todo $g, h \in G$.*

Definição A.3 *Um corpo $\langle F, +, \cdot \rangle$ é uma estrutura algébrica onde F é um conjunto, $+$ (adição) e $\cdot$ (multiplicação) são operações sobre F, satisfazendo os seguintes axiomas:*

(i) *$\langle F, + \rangle$ é um grupo abeliano com identidade chamada de* zero *e denotada por 0;*

(ii) *$\langle F - 0, \cdot \rangle$ é um grupo abeliano com identidade chamada de* um *e denotada por 1;*

(iii) *(Distributivideda da multiplicação sobre a adição) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ para todo $x, y, z \in F$.*

Um corpo é dito *finito* quando o número de elementos do corpo é finito.

Definição A.4 *O número de elementos de um corpo finito, q, é chamado de* ordem do corpo.

Corpos finitos são chamados também de *campos de Galois*.

Definição A.5 *A característica de um corpo, p, é o menor valor de N, tal que*

$$\sum_{n=1}^{N} 1 = 0. \tag{A.1}$$

A característica, p, de um corpo finito é sempre um número primo.

Teorema A.1 *A ordem de um corpo finito q deve ser potência de um número primo, mais precisamente, da característica do corpo, p, isto é, $q = p^m$, para $m \in \mathbb{N}^*$.*

Definição A.6 *Um corpo finito de ordem q é representado por $GF(q)$.*

Teorema A.2 *O grupo multiplicativo formado por $GF(q)^*$ é cíclico de ordem $q-1$.*

Esse teorema indica que existe um elemento primitivo, α, que gera todos os elementos do corpo por α^n, $n = 1, \ldots, q-1$, excluindo o zero.

Corolário A.1 (Pequeno Teorema de Fermat) *Todo elemento $\beta \in GF(q)$ satisfaz a identidade*

$$\beta^q = \beta. \tag{A.2}$$

Teorema A.3 *Para qualquer primo p e $m \in \mathbb{N}^*$, existe um corpo $GF(p^m)$, este corpo é essencialmente único.*

De modo menos formal, todos os corpos finitos de mesma ordem são isomorfos entre si. O corpo $GF(p)$, com p primo, é simplesmente a aritmética residual módulo p [17], isto é, o conjunto $\{0, 1, \ldots, p-1\}$ com operações de adição e multiplicação $(mod\ p)$.

Teorema A.4 *Suponha que $\pi(x)$ é um polinômio irredutível sobre $GF(p)$ de grau m. Então o conjunto de todos os polinômios na variável x de grau menor que m e coeficientes em $GF(p)$, com adição e multiplicação sobre a aritmética polinomial $(mod\ \pi(x))$, forma o corpo $GF(p^m)$.*

Esse é um método simples para a geração de um corpo finito, o método mais comum é a utilização de *polinômios primitivos*, cujas raízes são elementos primitivos do corpo.