Trabalho de Graduação

Processamento Digital de Sinais
Transformadas Digitais:
Implementação em MATLAB

Aluno: Marcos Müller Vasconcelos
Orientador: Prof. Dr. Hélio Magalhães de Oliveira
Grupo de Processamento Digital de Sinais
Departamento de Eletrônica e Sistemas
Centro de Tecnologia e Geociências - UFPE

15 de abril de 2004

Sumário

Capítulo 1

Introdução

1.1 Motivação

As muitas aplicações de transformadas discretas sobre corpos finitos e infinitos são bem conhecidas. A transformada discreta de Fourier (TDF) e a transformada discreta de Hartley (TDH) desempenham um papel importante em Engenharia Elétrica. Outras transformadas discretas importantes são as transformadas discretas do seno (TDS) e cosseno (TDC). Particularmente a TDC é uma ferramenta usada para compressão de imagens e vídeo nos padrões JPEG e MPEG. Essas transformadas, embora discretizadas no domínio da variável independente, possuem coeficientes que pertencem a um corpo infinito. Portanto, elas podem ser vistas como um tipo de "transformadas analógicas". Em contraste, as transformadas definidas sobre corpos finitos, além de discretizadas no domínio da variável independente, tem seus coeficientes definidos sobre um alfabeto finito e podem ser vistas como "transformadas digitais". Especificamente, transformadas discretas definidas sobre corpos finitos são atraentes por não introduzirem erros de truncagem ou arredondamento, e por permitirem aplicações com aritmética de baixa complexidade.

A primeira transformada discreta definida sobre corpos finitos, a transformada de Fourier em um corpo finito (TFCF), foi introduzida em 1971 [2] como uma ferramenta para efetuar convoluções discretas usando aritmética modular. Desde então várias aplicações da TFCF foram encontradas, em diversas áreas, tais como Processamento Digital de sinais e imagem, Codificação de Canal e Criptografia. Em 1998, a transformada de Hartley sobre

corpos finitos foi introduzida [6], a qual apresenta propriedades de simetria que a tornam mais atraente, para diversas aplicações, que a TFCF, e tem importantes aplicações no campo da multiplexação digital [7] e sistemas de acesso múltiplo. Além disso, são ferramentas em potencial para Processamentos de Sinais genéticos cuja natureza é intrinsecamente digital.

Recentemente, duas novas transformadas digitais, as transformadas dis cretas do seno e cosseno foram definidas. Estas transformadas apresentam propriedades de simetria muito interessantes que podem ser exploradas para a construção de algoritmos rápidos para seu cálculo eficiente.

O desenvolvimento de novas transformadas e ferramentas para processamento de sinais em corpos finitos é uma das linhas de pesquisa do Grupo de Pesquisa em Comunicações (CODEC). A implementação e simulação destas transformadas em *software* são de extrema utilidade e permitem uma maior rapidez no processo de pesquisa e desenvolvimento.

1.2 Objetivos

Este trabalho tem como objetivo o desenvolvimento de ferramentas para processamento digital de sinais em corpos finitos permitindo a simulação de diversas transformadas discretas definidas sobre corpos finitos.

O trabalho proposto se divide em três etapas:

A. A implementação de funções que lidem com os corpos de Inteiros Gaussianos $GI(p)$.

B. A implementação das funções k-trigonométricas.

C. A implementação das seguintes transformadas sobre corpos finitos:

   i. Transformada Numérica de Fourier

   ii. Transformada Discreta de Hartley

   iii. Transformada Discreta do Cosseno

   iv. Transformada Discreta do Seno

Capítulo 2

Corpos Finitos

Antes de definir e implementar as transformadas, é preciso compreender um pouco sobre a estrutura algébrica sobre a qual elas serão definidas. Primeiramente, será apresentada a definição, teoremas e propriedades dos corpos finitos.

Definição 1 *Um corpo F é um conjunto de elementos no qual duas operações estão definidas: adição $(+)$ e multiplicação $(\cdot)$, tal que os seguintes axiomas são válidos:*

i. A estrutura algébrica constituída pela operação adição juntamente com o conjunto F, $< F, + >$, é um grupo abeliano;

ii. A estrutura algébrica constituída pela operação multiplicação juntamente com o conjunto F, $< F^*, \cdot >$, é um grupo abeliano, onde $F^* = F - \{0\}$;

iii. $a \cdot (b + c) = a \cdot b + a \cdot c$, para todo a, b, $c \in F$;

iv. Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$, para todo a, $b \in F$.

Um corpo consiste de pelo menos dois elementos, a identidade aditiva e a identidade multiplicativa. O número de elementos de um corpo é chamado **ordem** do corpo. Um corpo com um número finito de elementos é chamado um **Corpo Finito**.

Definição 2 *Seja F um corpo. Um subconjunto de F é chamado um subcorpo se ele é também um corpo sob as operações de F. O corpo F é então chamado de corpo de extensão do subcorpo.*

Definição 3 *O número de elementos do menor subcorpo de F é chamado* ***característica*** *de F.*

Definição 4 *Para um primo p, seja o conjunto $F_p = \{0, 1, \ldots, p-1\}$ munido das operações adição e multiplicação módulo p, denotadas por $+_p$ e $\cdot_p$, respectivamente. A estrutura $< F_p, +_p, \cdot_p >$, é um corpo finito, chamado de* ***Campo de Galois***[1] *de ordem p. Esse corpo, também chamado de* ***corpo primo****, é denotado por GF(p).*

Teorema 1 *Para todo corpo finito GF(p) e todo inteiro positivo r, existe um corpo finito com $q = p^r$ elementos, denotado por GF(q), considerado um corpo de extensão de GF(p).*

Teorema 2 *Seja GF(q) um corpo com $q = p^r$ elementos. Então todo subcorpo de GF(q) tem ordem p^s, onde s é um divisor positivo de r. Por outro lado, se s é um divisor positivo de r, então existe exatamente um subcorpo de GF(q) com p^s elementos.*

Teorema 3 *O grupo multiplicativo dos elementos não nulos de $GF(q)$ é cíclico de ordem $q - 1$.*

Pelo teorema acima, a existência de um elemento cujas exponenciações geram todos os elementos não nulos do corpo é comprovada. Este elemento é denominado elemento **gerador** do corpo.

Definição 5 *Seja α um elemento não nulo de um corpo finito. O menor inteiro $t \geq 1$, tal que $\alpha^t = 1$, é chamado* ***ordem*** *de α, denotada por*

$$ord(\alpha) = t$$

Definição 6 *Um elemento gerador do grupo cíclico GF(q)* é chamado de* ***elemento primitivo*** *de GF(q) e a sua ordem é $q - 1$.*

Teorema 4 *Seja GF(q) um corpo de característica p. Então,*

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_s)^{p^n} = \alpha_1^{p^n} + \alpha_2^{p^n} + \ldots + \alpha_s^{p^n},$$

para todo α_1, α_2, ..., $\alpha_s \in GF(q)$ e $n \in \mathbb{N}$.

[1] *Galois Field*, em homenagem ao matemático francês Evariste Galois (1811-1832)

Definição 7 *$F_p[x]$ denota o conjunto dos polinômios em x com coeficientes em GF(p).*

Definição 8 *Um polinômio $p(x) \in F_p[x]$ é dito ser **irredutível** sobre GF(p) se $p(x)$ tem grau positivo e se $p(x) = a(x) \cdot b(x)$, com $a(x)$ e $b(x) \in F_p[x]$, implica que $a(x)$ ou $b(x)$ é uma constante.*

Definição 9 *Dado um corpo primo GF(p) e um polinômio de grau r irredutível, $p(x)$, com coeficientes em GF(p), pode-se contruir um corpo com p^r elementos.*

A maior dificuldade na construção de corpos é a comprovação da irredutibilidade dos polinômios. Para os polinômios de graus 2 e 3, esta tarefa é mais simples.

Teorema 5 *O polinômio $p(x) \in F_p[x]$, de grau 2 ou 3, é irredutível em GF(p) se e somente se não possui raízes nesse corpo.*

Pelo teorema acima, fica estabelecido que o polinômio $x^2 + 1$ é irredutível se a equação $x^2 + 1 = 0$ não tiver solução em $GF(\mathrm{p})$. Este fato, em conjunto com o teorema a seguir, será utilizado na definição dos Inteiros Gaussianos sobre Corpos Finitos na próxima seção.

Teorema 6 *Um polinômiode grau m irredutível sobre GF(p) permanece irredutível sobre GF(p^r) se e somente se $mdc(r, m) = 1$.*

Observa-se, do teorema acima, que mesmo para $q = p^r$, pode ser construído um corpo $GF(q^m)$ como uma extensão de $GF(q)$. Para isto, é suficiente mostrar que existem polinômios de grau m irredutíveis em $GF(\mathrm{q})$.

Teorema 7 *Para todo corpo finito GF(q) e um inteiro positivo m, existe pelo menos um polinômio de grau m irredutível sobre GF(q).*

No que segue, estão relacionadas definições e teoremas sobre teoria dos números, que serão necessários na caracterização das transformadas em corpos finitos.

Teorema 8 (Teorema de Euler) *Sejam a e n dois inteiros positivos tais que $mdc(a, n) = 1$. Então:*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

onde $\phi(\cdot)$ denota a função aritmética de Euler.

Definição 10 *Sejam a um inteiro e p um primo ímpar, tais que* $mdc(a, p) = 1$. *Nestas condições, se a congruência quadrática*

$$x^2 \equiv a \pmod{p}$$

tem solução, então a é um resíduo quadrático de p; caso contrário, a é um resíduo não quadrático de p.

Teorema 9 (Critério de Euler) *Sejam a um inteiro e p um primo ímpar, tais que* $MDC(a, p) = 1$. *O inteiro a é um resíduo quadrático de p se e somente se*

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

Proposição 1 *Seja p um primo ímpar:*

i. Se $p \equiv 1 \pmod 4$, *então* -1 *é um resíduo quadrático de p;*

ii. Se $p \equiv 3 \pmod 4$, *então* -1 *é um resíduo não quadrático de p.*

Teorema 10 *Seja* $q = p^r$, *com* $p \equiv 3 \pmod 4$ *e r um inteiro ímpar. Então não existe* $j \in GF(q)$ *tal que* $j^2 = -1$ *em GF(q).*

2.1 Inteiros Gaussianos

Os Inteiros Gaussianos sobre Corpos Finitos se caracterizam como uma extensão de um corpo finito da mesma forma que os números complexos são uma extensão do corpo dos reais. Esta seção apresenta a sua definição e algumas de suas propriedades.

Definição 11 (Conjunto de Inteiros Gaussianos) $G(p) \triangleq \{\alpha + jb, \alpha, b \in GF(p)\}$, *p um primo ímpar tal que* $j^2 \equiv -1 \pmod p$ *não é um resíduo quadrático em* $GF(p)$ *(i.e.,* $p \equiv 3 \pmod 4$, *os chamados primos de Hartley), é o conjunto dos inteiros gaussianos sobre* $GF(p)$.

Seja

$$\begin{array}{lcl} \oplus : G(p) \otimes G(p) & \rightarrow & G(p) \\ (\alpha_1 + j\beta_1, \alpha_2 + j\beta_2) & \rightarrow & (\alpha_1 + j\beta_1) \oplus (\alpha_2 + j\beta_2) = \\ & & = (\alpha_1 + \alpha_2) + j(\beta_1 + \beta_2) \end{array}$$

e

$$\begin{array}{lcl} * : G(p) \otimes G(p) & \rightarrow & G(p) \\ (\alpha_1 + j\beta_1, \alpha_2 + j\beta_2) & \rightarrow & (\alpha_1 + j\beta_1) * (\alpha_2 + j\beta_2) = \\ & & = (\alpha_1\alpha_2 - \beta_1\beta_2) + j(\alpha_1\beta_2 + \alpha_2\beta_1) \end{array}$$

O corpo de extensão $GF(p^2)$ é isomórfico à estrutura "complexa" $GI(p)$, os inteiros gaussianos sobre $GF(p)$. Da definição acima, todo elemento de $GI(p)$ pode ser representado na forma $\alpha + j\beta$ e é denominado número complexo de corpo finito.

Definição 12 *O módulo de um elemento de $GF(p)$, $p = 4k + 3$, é dado por*

$$|a| = \begin{cases} \alpha & se\ \alpha^{(p-1)/2} \equiv 1 \pmod{p} \\ -\alpha & se\ \alpha^{(p-1)/2} \equiv -1 \pmod{p} \end{cases}$$

Proposição 2 *O módulo de um elemento de $GF(p)$ é sempre um resíduo quadrático módulo p.*

Definição 13 *O módulo de um elemento $\zeta = (\alpha + j\beta) \in GI(p)$, onde $p = 4k + 3$, é definido por*

$$|\alpha + j\beta| = \sqrt{|\alpha^2 + \beta^2|}$$

O módulo de ζ é sempre um resíduo quadrático módulo p.

Definição 14 (Conjunto Unimodular) *O conjunto unimodular de $GI(p)$ é o conjunto de elementos $\zeta = (\alpha + j\beta) \in GI(p)$, tais que $\alpha^2 + \beta^2 \equiv 1 \pmod{p}$. Os elementos ζ são denominados elementos unimodulares.*

Esse conjunto é um grupo cíclico de ordem $p+1$. É possível estender o grupo unimodular de $GI(p)$ anexando elementos complexos $(\alpha+j\beta)$ que satisfazem $\alpha^2 + \beta^2 \equiv -1 \pmod{p}$.

Definição 15 (Conjunto Nega-Unimodular) *O conjunto negaunimodular de $GI(p)$ é o conjunto de elementos $\zeta = (\alpha + j\beta) \in GI(p)$, tais que $\alpha^2 + \beta^2 \equiv -1 \pmod{p}$. Os elementos ζ são denominados elementos negaunimodulares.*

Definição 16 (Conjunto Supra-Unimodular) *O conjunto supraunimodular de $GI(p)$ é o conjunto de elementos $\zeta = (a + jb) \in GI(p)$, tais que $(\alpha^2 + \beta^2)^2 \equiv 1 \pmod{p}$.*

Esse conjunto é um grupo cíclico de ordem $2(p+1)$ e todos os seus elementos tem módulo igual a um.

Os elementos ζ pertencentes a $GI(p)$, assim como os números complexos, possuem uma representação polar além da forma retangular da definição 11. Portanto, todo ζ pode ser escrito como $r\varepsilon^{\theta}$, onde r pertence ao grupo dos módulos e ε^{θ} pertence ao grupo das fases de $GI(p)$, permitindo até mesmo uma representação gráfica do plano complexo Z sobre $GF(p)$.

2.2 Funções K-Trigonométricas

A trigonometria em corpos finitos, introduzida em [6], define as funções k-trigonométricas e apresenta propriedades muito semelhantes às das funções trigonométricas definidas sobre os números reais.

Definição 17 (Seno e Cosseno em um Corpo Finito) *Seja ζ um elemento de ordem multiplicativa N em $GI(p)$. As funções k-trigonométricas $\sin_k(.)$ e $\cos_k(.)$, em $GI(p)$, de $\angle\zeta^i$, são definidas como*

$$\sin_k(\angle\zeta^i) \triangleq \frac{\zeta^{ik} - \zeta^{-ik}}{j2}$$

e

$$\cos_k(\angle\zeta^i) \triangleq \frac{\zeta^{ik} + \zeta^{-ik}}{2}$$

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

2.2.1 Propriedades

Por simplicidade, cosidera-se ζ fixo na definição da função k-trigonométrica, denotando-se então

$$\cos_k(\angle\zeta^i) \triangleq \cos_k(i)$$

e

$$\sin_k(\angle\zeta^i) \triangleq \sin_k(i)$$

com $i, k = 0, 1, \ldots, N-1$.

P1 **Círculo Unitário**

$$\sin_k^2(i) + \cos_k^2(i) = 1$$

P2 **Par/Ímpar**

$$\cos_k(i) = \cos_k(-i)$$

e

$$\sin_k(i) = -\sin_k(-i)$$

P3 **Fórmula de Euler**

$$\zeta^{ik} = \cos_k(i) + j\sin_k(i)$$

P4 **Adição de Arcos**

$$\cos_k(i+t) = \cos_k(i)\cos_k(t) - \sin_k(i)\sin_k(t)$$

e

$$\sin_k(i+t) = \sin_k(i)\cos_k(t) + \cos_k(i)\sin_k(t)$$

P5 **Arco Duplo**

$$\cos_k^2(i) = \frac{1+\cos_k(2i)}{2}$$

e

$$\sin_k^2(i) = \frac{1-\cos_k(2i)}{2}$$

P6 **Simetria Principal**

$$\cos_k(i) = \cos_i(k)$$

e

$$\sin_k(i) = \sin_i(k)$$

É posssível ainda definir uma outra função k-trigonométrica, a função $\mathrm{cas}_k(.)$, núcleo da transformada discreta de Hartley de corpo finito.

$$\mathrm{cas}_k(\angle\zeta^i) \triangleq \cos_k(\angle\zeta^i) + \sin_k(\angle\zeta^i)$$

Esta função apresenta apresenta diversas propriedades, dentre as quais se destaca a importante propriedade de ortogonalidade. Onde

$$\sum_{k=0}^{N-1} \mathrm{cas}_k(\angle\zeta^i)\mathrm{cas}_k(\angle\zeta^t) = \begin{cases} N, & i = t \\ 0, & i \neq t \end{cases} .$$

Capítulo 3

Transformadas em Corpos Finitos

3.1 A Transformada Discreta de Fourier

A Transformada de Fourier em um Corpo Finito foi originalmente introduzida em 1971 como uma ferramenta para efetuar convoluções discretas finitas usando aritmética inteira e, desde então, várias outras aplicações tem surgido, especialmente nas áreas de Processamento Digital de Sinais e Teoria da Informação.

Definição 18 *Seja $f = (f_0, f_1, ..., f_{N-1})$ um vetor de comprimento N e componentes em $GF(q)$, onde $q = p^r$, então o vetor $F = (F_0, F_1, ..., F_{N-1})$ com componentes em $GF(q^m)$ dadas por*

$$F_k = \sum_{i=0}^{N-1} f_i \alpha^{ki},$$

onde α é um elemento de ordem N em $GF(q^m)$, é a Transformada de Fourier em um Corpo Finito (TFCF) de f.

Pode-se demonstrar que a transformada inversa do vetor F é dada por

$$f_i = \frac{1}{N \pmod p} \sum_{k=0}^{N-1} F_k \alpha^{-ki}.$$

3.1.1 Propriedades

Sejam $g \leftrightarrow G$ e $f \leftrightarrow F$ pares tranformados TFCF de comprimento N, como definidos anteriormente.

F1. **Linearidade:** Sejam $a, b \in GF(q)$ então $af + bg \leftrightarrow aF + bG$.

F2. **Deslocamento no Tempo:** Suponha que $f_i = g_{i-I}$; então $F_k = a^{jI} G_k$.

F3. **Convolução Cíclica:** $g \circledast f \leftrightarrow GF = G_k F_k$.

F4. **Espectros Válidos:** $F_k^q = F_{kq \pmod N}$.

3.1.2 Transformadas Numéricas de Fourier

As transformadas numéricas compõem um subconjunto de transformadas onde são relacionados vetores com componentes em um mesmo corpo finito $GF(p)$. A implementação em *hardware* das transformadas numéricas é de extrema facilidade e simplicidade, o que implica em um baixo custo de implementação. Além disto o seu cálculo pode ser realizado de maneira rápida e eficiente. Para obter uma transformada numérica de Fourier é preciso fazer com que $q = p$ e $m = 1$. O núcleo da transformada α passa a ser um elemento de ordem N em $GF(p)$.

Pode-se destacar três considerações práticas importantes, no que diz respeito a eficiência computacional, na definição de uma transformada numérica.

i. **Escolha de $GF(p)$:**
O módulo p deve ser grande o suficiente para evitar *overflow* e também deve permitir uma fácil implementação da operação modular requerida.

ii. **Escolha do comprimento N da transformada:**
O comprimento N deve ser composto para podermos utilizar algoritmos rápidos e deve ser grande o suficiente para aplicações em longas seqüências.

iii. **Escolha do núcleo α da transformada:**
A multiplicação por potências de α deve ser de baixa complexidade computacional. Uma possível escolha para α, seria a de uma potência de 2, já que os sistemas eletrônicos digitais são baseados em operações binárias onde as multiplicações por potências de 2 são deslocamentos das seqüências binárias sendo multiplicadas.

Dessa forma, duas escolhas para p podem ser consideradas:

- **Primos de Fermat:** $p = 2^q + 1$
- **Primos de Mersenne:** $p = 2^q - 1$

3.2 A Transformada Discreta de Hartley

A Transformada de Hartley em um Corpo Finito foi originalmente introduzida em 1998 e possui propriedades semelhantes as da Transformada Discreta de Hartley definida no contínuo. A Transformada de Hartley em um Corpo Finito é um mapeamento de $GF(q)$ para $GI(q^m)$, cujo núcleo é um elemento pertencente a $GI(q^m)$ de ordem N.

Definição 19 *Seja $h = (h_0, h_1, ..., h_{N-1})$ um vetor de comprimento N e componentes em $GF(p)$, então o vetor $H = (H_0, H_1, ..., H_{N-1})$ com componentes em $GI(q^m)$ dadas por*

$$H_k = \sum_{i=0}^{N-1} h_i cas_k(\angle\zeta^i),$$

onde ζ é um elemento de ordem N em $GI(q^m)$, é a Transformada de Hartley em um Corpo Finito (THCF) de h.

Pode-se demonstrar que a transformada inversa do vetor H é dada por

$$h_i = \frac{1}{N \pmod p} \sum_{k=0}^{N-1} H_k \mathrm{cas}_k(\angle\zeta^i).$$

3.2.1 Propriedades

Sejam $g \leftrightarrow G$ e $h \leftrightarrow H$ pares tranformados THCF de comprimento N, como definidos anteriormente.

H1. **Linearidade:** Sejam $a, b \in GF(q)$ então $ah + bg \leftrightarrow aH + bG$.

H2. **Deslocamento no Tempo:** Suponha que $h_i = g_{i-I}$; então $H_k = \cos_k(I)G_k + \sin_k(I)G_{-k}$.

H3. **Convolução Cíclica:** $g \circledast h \leftrightarrow \frac{1}{2}(GH + G_{-}H + GH_{-} - G_{-}H_{-})$.

H4. **Espectros Válidos:** Suponha uma THCF, cujo núcleo $\text{cas}_k(\angle\zeta^i)$ utiliza como argumento da função $\text{cas}_k(\cdot)$ o elemento $\zeta = \alpha \in GF(q)$. O vetor $H = H_k$, $H_k \in GI(q)$, é o espectro de um sinal $h = h_i$, $h_i \in GF(q)$, $q = p^r$, se e somente se $H_k^q = H_{-kq \pmod N}$.

3.2.2 A Transformada Numérica de Hartley

Fazendo com que $q = p$ e $m = 1$, torna que o mapeamento dos vetores seja entre $GF(p)$ e $GI(p)$. Para que o vetor transformado H possua componentes em $GF(p)$ é necessário escolher um valor apropriado para ζ. Se ζ pertencer ao conjunto unimodular de $GI(p)$, é mostrado em [14] que a função $\text{cas}_k(\cdot)$ assume valores sobre $GF(p)$, tornando a THCF uma transformada numérica.

3.3 A Transformada Discreta do Cosseno

Embora apresentem muitas propriedades semelhantes da trigonometria usual, funções $\sin_k(\cdot)$ e $\cos_k(\cdot)$, não são ortogonais e portanto, as funções k-cos não podem ser usadas diretamente para definir uma transformada discreta do cosseno (TDC) sobre um corpo finito. De fato, a TDC usual (sobre os reais) na sua forma mais comumente utilizada, é construída por um processo que envolve a duplicação da seqüência $x[n]$ de comprimento N, cuja TDC se quer definir, seguida pela computação da transformada discreta de Fourier (TDF) dessa seqüência de comprimento $2N$, o que requer que se use um núcleo de ordem $2N$. A TDC é então obtida a partir dessa TDF. A transformada discreta do cosseno em um corpo finito (TDCCF) pode ser obtida por um processo semelhante e foi definida em [15].

Definição 20 *Seja $c = (c_0, c_1, ..., c_{N-1})$ um vetor de comprimento N e componentes em $GF(p)$, então o vetor $C = (C_0, C_1, ..., C_{N-1})$ com componentes em $GI(p)$ dadas por*

$$C_k \triangleq \sum_{i=0}^{N-1} 2c_i \cos_k\Big(\frac{2i+1}{2}\Big),$$

onde ζ é um elemento de ordem $2N$ em $GI(p)$, é a Transformada Discreta do Cosseno em um Corpo Finito (TDCCF) de c.

Pode-se demonstrar que a transformada inversa do vetor C é dada por

$$c_i = \frac{1}{N \,(\mathrm{mod}\ p)} \sum_{k=0}^{N-1} \beta_k C_k \cos_k\Big(\frac{2i+1}{2}\Big),$$

onde

$$\beta_k = \begin{cases} 1/2, & \text{se } k = 0 \\ 1, & \text{se } k \neq 0 \end{cases}$$

A TDCCF é uma transformada linear, no entanto suas outras propriedades ainda estão em aberto pelo fato de ser muito recente e pouco explorada. Também é possível construir um transformada numérica do cosseno, bastando que o elemento ζ seja escolhido de modo que sua raiz quadrada λ sobre $GI(p)$ seja um elemento unimodular.

3.4 A Transformada Discreta do Seno

Assim como a TDCCF, podemos definir a transformada discreta do seno (TDS) em um corpo finito através de um procedimento semelhante ao descrito na seção anterior.

Definição 21 *Seja $s = (s_0, s_1, ..., s_{N-1})$ um vetor de comprimento N e componentes em $GF(p)$, então o vetor $S = (S_1, S_2, ..., S_N)$ com componentes em $GI(p)$ dadas por*

$$S_k \triangleq \sum_{i=0}^{N-1} 2 s_i \mathit{sin}_k\Big(\frac{2i+1}{2}\Big),$$

onde ζ é um elemento de ordem $2N$ em $GI(p)$, é a Transformada Discreta do Seno em um Corpo Finito (TDSCF) de s.

Pode-se demonstrar que a transformada inversa do vetor S é dada por

$$s_i = \frac{1}{N \,(\mathrm{mod}\ p)} \sum_{k=1}^{N} \beta_k S_k \sin_k\Big(\frac{2i+1}{2}\Big),$$

onde

$$\beta_k = \begin{cases} 1/2, & \text{se } k = N \\ 1, & \text{se } k \neq N \end{cases}$$

A TDSCF é uma transformada linear, no entanto suas outras propriedades, assim como a TDSCF ainda estão em aberto pelo fato de ser muito recente e pouco explorada. Também é possível construir um transformada numérica do seno, bastando que o elemento ζ seja escolhido de modo que sua raiz quadrada λ sobre $GI(p)$ seja um elemento unimodular.

3.5 Representação Matricial

Transformadas discretas lineares são comumente representadas de uma forma mais compacta na notaão matricial. Sendo T a matriz $N \times N$ de transformação direta, tem-se então, na forma vetorial,

$$V = Tv$$

onde v é o vetor no domínio do tempo e V é o vetor no domínio da freqüência ou espectro de v.

Capítulo 4

Implementação em MATLAB®

Para a implementação das transformadas digitais foi escolhido o MATLAB®. Este *software* tem a dificuldade de não apresentar funções ou bibliotecas que permitam o cálculo diretamente em corpos finitos como o MAPLE®. No entanto, a linguagem de programação do MATLAB® é bastante versátil e de fácil aprendizado o que facilitou a elaboração das linhas de código.

Primeiramente, foram implementadas diversas funções para manipulação dos Inteiros Gaussianos sobre comrpos finitos. Estes programas trabalham isoladamente e como subrotinas das funções que implementam as transformadas. A seguir será apresentado o primeiro grupo de funções.

4.1 Inteiros Gaussianos

F1 `ord.m`

- **Descrição:** Calcula a ordem multiplicativa de um elemento não nulo de $GI(p)$.
- **Argumentos:** p e ζ
- **Chamada da função:** `ord(p,`ζ`)`
- **Exemplo:**

F2 `euler.m`

- **Descrição:** Utiliza o critério de Euler para determinar se um elemento de $GF(p)$ é ou não resíduo quadrático módulo p. A função retorna `1` se o elemento for resíduo quadrático e `0` caso contrário.

- **Argumentos:** p e α
- **Chamada da função:** `euler(p,`α`)`
- **Exemplo:**

F3 `modulus.m`

- **Descrição:** Calcula o módulo de um elemento de $GF(p)$.
- **Argumentos:** p e α
- **Chamada da função:** `modulus(p,`α`)`
- **Exemplo:**

F4 `GImodulus.m`
Calcula o módulo de um elemento de $GI(p)$. Argumentos: `modulus(p,`ζ`)`

F5 `FFinv.m`
Calcula o inverso multiplicativo de um elemento não nulo de $GF(p)$. Argumentos: `FFinv(p,`α`)`

F6 `GIinv.m`
Calcula o inverso multiplicativo de um elemento não nulo de $GI(p)$. Argumentos: `GIinv(p,`ζ`)`

F7 `FFsqrt.m`
Calcula a raiz quadrada de um elemento de $GF(p)$. Argumentos: `FFsqrt(p,`α`)`

F8 `GIsqrt.m`
Calcula a raiz quadrada de um elemento de $GI(p)$. Argumentos: `FFinv(p,`ζ`)`

F9 `chooseroot.m`
Utiliza o critério de Euler para escolher apenas a raiz quadrada que é um resíduo quadrático módulo p.

F10 `isprime.m`
Verifica se p é um primo de Hartley ($p \equiv 3 \pmod 4$). Argumentos: `isprime(p)`

F11 `powerofz.m`
Calcula a n-ésima potência de um elemento de $GI(p)$. `powerofz(p,`ζ`,n)`

F12 `unimod.m`
Gera o grupo dos elementos unimodulares de $GI(p)$. Argumentos: `unimod(p)`

F13 `negaunimod.m`
Gera o conjunto dos elementos nega-unimodulares de $GI(p)$. Argumentos: `negaunimod(p)`

F14 `phase.m`
Gera o grupo das fases de $GI(p)$. Argumentos: `phase(p)`

F15 `moduli.m`
Gera o grupo dos módulos de $GI(p)$. Argumentos: `moduli(p)`

F16 `unigen.m`
Encontra um gerador do grupo dos elementos unimodulares de $GI(p)$. Argumentos: `unigen(p)`

F17 `phasegen.m`
Encontra um gerador do grupo das fases de $GI(p)$. Argumentos: `phasegen(p)`

F18 `sgn.m`
Função *sinal* em um corpo finito. Argumentos: `sgn(p,k)`

4.2 Funções K-Trigonométricas

F19 `ksin.m`
Calcula a função k-trigonométrica $\sin_k(\angle\zeta^i)$ sobre $GI(p)$. Argumentos: `ksin(p,`ζ`)`

F20 `kcos.m`
Calcula a função k-trigonométrica $\cos_k(\angle\zeta^i)$ sobre $GI(p)$. Argumentos: `kcos(p,`ζ`)`

F21 `kcas.m`
Calcula a função k-trigonométrica $\mathrm{cas}_k(\angle\zeta^i)$ sobre $GI(p)$. Argumentos: `kcas(p,`ζ`)`

4.3 Transformadas sobre Corpos Finitos

F22 `NTFT.m`
Calcula a transformada numérica de Fourier de um vetor de comprimento N, f, com componentes em $GF(p)$. N =ord(α), onde α é o núcleo utilizado na definição da transformada. Argumentos: `NTFT(p,`ζ`,f)`

F23 `INTFT.m`
Calcula a transformada numérica de Fourier inversa de um vetor de comprimento N, F, com componentes em $GF(p)$. N =ord(α), onde α é o núcleo utilizado na definição da transformada. Argumentos: `INTFT(p,`α`,F)`

F24 `FFHT.m`
Calcula a transformada discreta de Hartley de um vetor de comprimento N, h, com componentes em $GF(p)$. N =ord(ζ), onde ζ é o argumento de cas_k utilizado na definição da transformada. Argumentos: `FFHT(p,`ζ`,h)`

F25 `IFFHT.m`
Calcula a transformada discreta de Hartley inversa de um vetor de comprimento N, H, com componentes em $GI(p)$. N =ord(ζ), onde ζ é o argumento de cas_k utilizado na definição da transformada. Argumentos: `IFFHT(p,`ζ`,H)`

F26 `FFDCT.m`
Calcula a transformada discreta do cosseno de um vetor de comprimento N, c, com componentes em $GF(p)$. N =ord(ζ)/4, onde ζ é o argumento de $\cos_k$ utilizado na definição da transformada. Argumentos: `FFDCT(p,`ζ`,c)`

F27 `IFFDCT.m`
Calcula a transformada discreta do cosseno inversa de um vetor de comprimento N, C, com componentes em $GI(p)$. N =ord(ζ)/4, onde ζ é o argumento de $\cos_k$ utilizado na definição da transformada. Argumentos: `IFFDCT(p,`ζ`,C)`

F28 `FFDFT.m`
Calcula a transformada discreta de Fourier de um vetor de comprimento N, f, com componentes em $GF(p)$. N =ord(ζ), onde ζ é o núcleo utilizado na definição da transformada. Argumentos: `FFDFT(p,`ζ`,f)`

F29 `IFFDFT.m`
Calcula a transformada discreta de Fourier inversa de um vetor de comprimento N, F, com componentes em $GI(p)$. N =ord(ζ), onde ζ é o núcleo utilizado na definição da transformada. Argumentos: `IFFDFT(p,ζ,F)`

F30 `FFDST.m`
Calcula a transformada discreta do seno de um vetor de comprimento N, f, com componentes em $GF(p)$. N =ord(ζ), onde ζ é o núcleo utilizado na definição da transformada. Argumentos: `FFDST(p,ζ,s)`

F31 `IFFDST.m`
Calcula a transformada discreta do seno inversa de um vetor de comprimento N, F, com componentes em $GI(p)$. N =ord(ζ), onde ζ é o núcleo utilizado na definição da transformada. Argumentos: `IFFDST(p,ζ,S)`

Capítulo 5

Conclusão

Apêndice A

Código Fonte

A.1 Programas

Referências Bibliográficas

[1] Transform Coding: Past, Present and Future, IEEE Signal Processing Magazine Special Issue, vol. 18, No. 5, Sep. 2001.

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

[3] I. S. Reed, T. K. Truong, V. S. Kwoh and E. L. Hall, Image Processing by Transforms over a Finite Field, IEEE Trans. Comput., vol.C-26, pp. 874-881, Sep. 1977.

[4] R. E. Blahut, Transform Techniques for Error-Control Codes, IBM J. Res. Dev., vol. 23, pp. 299-315, May 1979.

[5] J. L. Massey, *The Discrete Fourier Transform in Coding and Cryptography*, 1998 IEEE Information Theory Workshop, ITW 98, San Diego, CA, Feb 9-11.

[6] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, *Trigonometry in Finite Fields and a New Hartley Transform*, Proceedings of the 1998 IEEE International Symposium on Information Theory, p. 293, Cambridge, MA, Aug. 1998.

[7] H. M. de Oliveira, R. M. Campello de Souza and A. N. Kauffman, *Efficient Multiplex for Band-Limited Channels*, Proceedings of the Workshop on Coding and Cryptography - WCC '99, pp. 235 - 241, Paris, Jan. 1999.

[8] J. P. C. L. Miranda, H. M. de Oliveira, *On Galois-Division Multiple Access Systems: Figures of Merit and Performance Evaluation*, Anais do 19 Simpósio Brasileiro de Telecomunicações, Fortaleza CE, 2001.

[9] H. M. de Oliveira, R. M. Campello de Souza, *Orthogonal Multilevel Spreading Sequence Design, in Coding, Communications and Broadcasting*, pp. 291-303, Eds. P. Farrell, M. Darnell and B. Honary, Research Studies Press / John Wiley, 2000.

[10] R. E. Blahut, *Fast Algorithms for Digital Signal Processing*, Addison Wesley, 1985.

[11] D. Silva, R. M. Campello de Souza, H. M. de Oliveira, L. B. E. Palma and M. M. Campello de Souza, *A Transformada Numérica de Hartley e Grupos de Inteiros Gaussianos*, Revista da Sociedade Brasileira de Telecomunicações, Campinas, SP, v.17, No.1, pp. 48-57, 2002.

[12] A. N. Kauffman, *A Transformada de Hartley em um Corpo Finito e Aplicações*, Dissertação de Mestrado, Departamento de Eletrônica e Sistemas, UFPE, 1999.

[13] J. S. Lim, Two-Dimensional Signal and Image Processing, Prentice-Hall, 1990.

[14] R. M. Campello de Souza, H. M. de Oliveira, L.B Espínola e M. M. Campello de Souza, *Transformadas Numéricas de Hartley*, Anais do XVIII Simpósio Brasileiro de Telecomunicações, pp. 357-366, Gramado, RS, setembro 2000.

[15] R. M. Campello de Souza, H. M. de Oliveira, M. M. Campello de Souza e M. M. Vasconcelos *A Transformada Discreta do Cosseno em um Corpo Finito*, Anais do XX Simpósio Brasileiro de Telecomunicações, pp. 357-366, Rio de Janeiro, RJ, outubro 2003.