Universidade Federal de Pernambuco

Centro de Tecnologia e Geociências

Departamento de Eletrônica e Sistemas

A Transformada de Hartley em um Corpo Finito e Aplicações

por André Neumann Kauffman

orientadores Prof. Dr. Ricardo Menezes Cainpello de Souza

Prof. Dr. Hélio Magalhães de Oliveira

Dissertação submetida à Coordenação do Mestrado em Engenharia Elétrica da Universidade Federal de Pernambuco, para preenchimento dos pré-requisitos parciais para obtenção do Título de Mestre em Engenharia Elétrica.

27 de Dezembro de 1999

Conteúdo

Notação

• Um ideal gerado por um elemento y será denotado por (y).

• Seja A um anel e J um ideal de A. Denotaremos o anel quociente por A / J.

• Seja A um anel, denotamos por x = {y e A tal que y = x mod (J)} a classe de equivalência do elemento x e A relativamente a relação • mod (J).

• Seja A um anel, denotamos por A[x] o conjunto de todos os polinómios, sobre A, em uma indeterminada x.

• O símbolo ® representa produto cartesiano.

• O símbolo := representa "igual por definição".

• O símbolo = relaciona corpos isomorfos.

• O símbolo *, por exemplo C*, representa o conjunto C sem o elemento zero.

• O símbolo * denota a convolução cíclica.

• O símbolo ^{A} representa o complexo conjugado.

• Seja G = {Gk} uma seqüência de comprimento N; G. denota a seqüência {GN-k}-

Capítulo 1

Introdução

1.1 Motivação

Transformadas discretas, definidas sobre corpos finitos ou infinitos, desempenham um importante papel em Engenharia. Um exemplo particularmente significativo é a bem conhecida Transformada Discreta de Fourier (DFT), que tem muitas aplicações em diversas áreas, especialmente em Engenharia Elétrica. Uma DFT para corpos finitos foi introduzida por Pollard em 1971 [20] e aplicada como uma ferramenta para efetuar convoluções discretas usando aritmética inteira (cálculo de convoluções de forma eficiente e sem a necessidade de truncagem ou arredondamentos [11], [17], [18]).

Desde então várias novas aplicações da Transformada de Fourier de Corpo Finito foram concebidas, não apenas nos campos de Processamento Digital de Sinais e Imagens, mas também em diferentes contextos tais como Codificação de Canal e Criptografia. Em ambos os casos, finito e infinito, a existência de algoritmos rápidos (FFT) para computar a DFT tem sido um fator decisivo para aplicações em tempo real.

Um outro relevante exemplo concerne a Transformada Discreta de Hartley (DHT) [1], a versão discreta da transformada integral simétrica introduzida por R. V. L. Hartley em 1942 [33]. Embora vista inicialmente como uma ferramenta com aplicações apenas no lado numérico e tendo conexões com o mundo físico apenas através da Transformada de Fourier, a DHT mostrou-se ser um instrumento útil com muitas aplicações interessantes [19]. Transformadas rápidas de Hartley também existem e desempenham um papel importante no uso da DHT.

Nesta dissertação uma nova transformada é proposta, a Transformada de Hartley em um Corpo Finito (THCF) e uma nova técnica de multiplexação digital utilizando transformadas sobre corpos finitos é apresentada como uma das possíveis aplicações da THCF. Na próxima seção tem-se uma descrição de como esta dissertação está organizada.

1.2 Organização da Dissertação

O capítulo 2 realiza uma breve revisão de Álgebra Abstrata, onde são descritos os teoremas sob os quais a definição da Transformada de Hartley em um Corpo Finito e suas propriedades estão fundamentadas. Todos os teoremas apresentados neste capítulo pertencem ao contexto da Álgebra Abstrata básica e como tal, suas demonstrações foram, em geral, suprimidas. Contudo, ao final de cada enunciado, tem-se uma referência no qual o respectivo teorema está demonstrado com o rigor necessário. Foi dada ênfase as estruturas algébricas que conduzem a construção de corpos finitos e principalmente as propriedades de tais corpos.

O capítulo 3 situa a Transformada de Hartley em um Corpo Finito dentre as diversas possíveis versões de transformadas, no que diz respeito aos domínios relacionados. Uma revisão geral da importância prática de se desenvolver transformadas discretas é apresentada e são detalhadas algumas transformadas freqüentemente utilizadas em Engenharia Elétrica. O aspecto prático é mais uma vez ressaltado na apresentação de algoritmos eficientes para o cálculo da Transformada Discreta de Fourier. As principais propriedades da Transformada Discreta de Hartley são enunciadas, com o objetivo de uma comparação com as propriedades satisfeitas pela Transformada de Hartley em um Corpo Finito (THCF), descritas no capítulo 4. Por fim, a Transformada de Fourier em um Corpo Finito foi definida, motivando assim o desenvolvimento de uma nova transformada no capítulo seguinte.

O capítulo 4 deste trabalho desenvolve uma nova transformada sobre corpos finitos. Os fundamentos para a definição da THCF são apresentados, tanto no que diz respeito a estrutura algébrica sobre a qual a transformada está definida (os Inteiros Gaussianos sobre corpos finitos), como no que se refere as funções trigonométricas sobre corpos finitos, que de fato são as bases para a definição desta nova transformada. Propriedades dos Inteiros Gaussianos são demonstradas, as semelhanças das funções trigonométricas sobre corpos finitos com relação as funções trigonométricas clássicas são apresentadas e como ponto chave deste capítulo tem-se o teorema 4.1 que torna possível a definição da Transformada de Hartley em um Corpo Finito. De uma forma impressionante, as propriedades desta nova transformada refletem, em quase a totalidade dos casos, as propriedades da Transformada Discreta de Hartley. O alto grau de simetria da transformada foi exposto, inclusive de forma visual. De fundamental importância foi o estabelecimento das relações entre a THCF e a Transformada de Fourier em um Corpo Finito, sendo esta última de uso já consagrado, além de possibilitar o desenvolvimento de um algoritmo rápido para a THCF. Ao final do capítulo obtém-se a lei de verificação dos possíveis espectros resultantes da THCF, o que, assim como para a Transformada de Fourier em um Corpo Finito, resulta na definição de classes ciclotômicas e estabelece o alto grau de redundância desta nova transformada, motivando a definição de um novo método de multiplexação digital, apresentado no capítulo seguinte.

No capítulo 5 uma breve revisão dos métodos de multiplexação digital é apresentada. Um novo sistema de multiplexação por divisão no código é desenvolvido com base na ortogonalidade das funções casi<(.) . Seu esquema de implementação é discutido e realiza-se uma comparação de seu requisito em banda passante com relação aos demais sistemas de multiplexação digital.

O capítulo 6 delimita os avanços realizados neste trabalho e apresenta sugestões de novos tópicos relacionados com a THCF a serem futuramente pesquisados. Por fim, descreve-se o momento histórico e a trágica vida do gênio Evariste Galois, além de uma pequena noção de sua influência na matemática e nos matemáticos e engenheiros que se seguiram.

Capítulo 2

Estruturas Algébricas

Este capítulo apresenta uma breve revisão sobre algumas estruturas algébricas básicas. São apresentados os axiomas de definição de anel, domínio e corpo, bem como a forma como estas estruturas estão relacionadas. Devido a sua intensa ligação com a Transformada de Hartley em um Corpo Finito (THCF), um maior aprofundamento é realizado na caracterização de corpos finitos no que diz respeito a sua estrutura, como também nas propriedades satisfeitas por seus elementos. São enunciados teoremas que serão utilizados no desenvolvimento da THCF e cuja demonstração está desenvolvida na respectiva referência indicada ao final de cada teorema. Por outro lado, alguns teoremas específicos sobre corpos finitos e que são essenciais na caracterização dos Inteiros Gaussianos sobre um corpo finito (estrutura sobre a qual a THCF está definida) são demonstrados. Além disto, alguns resultados clássicos de Álgebra Abstrata que fazem parte do contexto da THCF são apresentados, especialmente a noção de resíduo quadrático de um inteiro.

2.1 Anel

Seja A um conjunto não vazio onde estejam definidas duas operações denotadas por + e *. Assim,

+ : A ® A -> A e * : A ® A - » A
(a,b) -> a+b (a,b) -> a*b

A estrutura <A, +, *> é um Anel comutativo com unidade se os 8 seguintes axiomas são verificados quaisquer que sejam a,b,ce A.

Al (a+b)+c = a+(b+c).

A2 3 OeA tal que a+0 = 0+a = a.

A3 V XG A existe um único ye A, tal que x+y = y+x = 0.

A4 a+b = b+a.

A5 (a*b)*c = a*(b*c).

A6 a*(b+c) = a*b + a*c e (a+b)*c = a*c + b*c.

A7 3 l e A , 0***1** tal que x * l = l*x = x V XGA.

A8 V x,yeA, x*y = y*x.

Um subconjunto S dc um anel A que é um anel em relação às mesmas operações definidas em A, é dito ser um subanel de A. Um subconjunto J de um anel A é dito ser um ideal se J é um subanel de A e, para todo aeJ e re A, ambos ar e ra eJ.

Definição **2.1.** Seja **Z** o conjunto dos números inteiros e A um anel. Pode-se então definir o seguinte homomorfismo

$$f: z \xrightarrow{-+} A$$
$$n \xrightarrow{->} n.l$$

o núcleo de f, N(í), é um ideal de z que, por sua vez, é um domínio de ideais principais [8] e assim

$$N(f) = (c), \text{ com } c \in N.$$

Define-se c como a característica de A [8].

2.2 Domínio

Se <A, +, *> é um anel comutativo com unidade e verifica o axioma A9 abaixo, então tem-se que <A, +, *> é um Domínio de Integridade.

A9 x,yeA, x*y = 0 => x = 0 ou y = 0.

2.3 Corpos Finitos

Se um domínio de Integridade <A, +, *> verifica a propriedade AIO abaixo, então <A, +, *> é um corpo.

AIO V xeA, x*0, 3 yeA tal que x*y = y*x **=1.**

Denota-se por **F** um corpo genérico. No caso particular em que **F** tem um número finito de elementos, o mesmo é dito ser um Corpo Finito.

2.3.1 Estrutura

As propriedades básicas que os elementos de um corpo finito devem satisfazer foram listadas nas seções anteriores deste capítulo. Esta seção aborda outras características estruturais dos corpos finitos.

Teorema 2.1. z/(p), o anel de classes residuais de inteiros módulo o ideal gerado pelo primo p, é um corpo [3].

Definição 2.2. Para um primo p, seja F_p o conjunto { 0 , **1,** p-**1**} e seja (p : z/(p) -> F_p o mapeamento definido por <p(a) = a, para a = 0, **1,** ...»p-**1,** onde a denota a classe de resíduos modulo p do inteiro a. Então, F_p com a estrutura induzida por 9 é um corpo finito, chamado de Campo de Galois (*Galois Field*) de ordem p e denotado GF(p).

Definição 2.3. Seja **F** um corpo. Um subconjunto **K** de **F** que é um corpo sobre as operações de **F** será chamado de subcorpo de **F.** Nesse caso **F** é dito ser um corpo de extensão (ou simplesmente uma extensão) de **K.**

Definição 2.4. Corpo Primo de **F** é a interseção de todos os subcorpos de **F.**

Como decorrência de seus axiomas de definição, os corpos finitos não podem ter qualquer quantidade de elementos. Os dois teoremas seguintes estabelecem as possíveis ordens de um corpo finito, bem como sua estrutura vetorial com relação a seu corpo primo.

Teorema 2.2. O corpo primo de um corpo **F** é isomorfo a GF(p) ou **Q** (o corpo dos números racionais), respectivamente, se sua característica for p ou zero.

Teorema 2.3. Seja **F** um corpo finito. Então **F** tem p^r elementos, onde o primo p é a característica de **F** e r é o grau de **F** sobre seu corpo primo. Denota-se **F** por GF(q), onde q = $\mathbf{P}^r$ [3].

2.3.2 Polinómios Sobre Corpos Finitos

A definição de polinómios sobre corpos finitos é feita de forma similar a definição usual de polinómios. **F**[x] denota o conjunto de polinómios na variável x com coeficientes no corpo **F.**

Definição 2.5. Um polinómio p(x) e **F**[x] é dito ser irredutível sobre **F** se p(x) tem grau positivo e p(x) = a(x)b(x) com a(x),b(x) e **F**[x], implica que a(x) ou b(x) é uma constante.

A Transformada de Hartley em um Corpo Finito (THCF) é construída sobre um corpo finito com características específicas e que pode ser visto como um corpo de extensão de um corpo base. O teorema a seguir estabelece um critério para a construção de corpos de extensão de um dado corpo **F.**

Teorema 2.4. Seja f(x) e **F**[x]. Então o conjunto **F**[x] / (f(x)) de todos os polinómios e **F**[x], módulo f(x), juntamente com as operações de soma e multiplicação modulo f(x), é um corpo se e somente se f(x) é irredutível sobre **F** [3].

Corpos de extensão são construídos através de polinómios irredutíveis, contudo a comprovação da irredutibilidade de um polinómio, é, em geral, uma tarefa complexa. A exceção ocorre em polinómios de grau 2 ou 3, como estabelecido pelo seguinte teorema.

Teorema 2.5. O polinómio f(x) *e* **F**[x] de grau 2 ou 3 é irredutível em **F**[x] se e somente se f(x) não tem raízes em **F**[x] [3].

Particularmente, o teorema acima garante que o polinómio x^2+1 é irredutível em GF(q) se e somente se a equação $x^2 = -1$ não tem solução em GF(q). Este fato, bem como o teorema a seguir, serão utilizados na definição dos Inteiros Gaussianos sobre Corpos Finitos.

Teorema 2.6. Um polinómio de grau n e irredutível sobre GF(q) permanece irredutível sobre $GF(q^m)$ se e somente se m e n são relativamente primos [3].

2.3.3 Caracterização

O próximo teorema garante a existência e a unicidade dos corpos finitos.

Teorema 2.7. Para todo primo p e todo inteiro positivo r, existe um corpo finito com p^r elementos. Todo corpo finito com $q = p^r$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre GF(q) [3].

O critério a seguir caracteriza todos os subcorpos de um dado corpo.

Teorema 2.8. 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 [3].

Teorema 2.9. Para todo corpo finito GF(q), o grupo multiplicativo dos elementos não nulos, GF(q)* , é cíclico.

De acordo com o teorema anterior, sempre pode-se utilizar um elemento não nulo * 1 de GF(q) como base para uma representação exponencial dos q-1 elementos não nulos de GF(q).

2.3.4 Propriedades dos Elementos

Esta seção apresenta teoremas que caracterizam, de forma genérica, os elementos de um corpo finito.

Definição 2.6. Seja a um elemento não nulo de um corpo finito. Suponha que $a^t = 1$ e que $a^v \neq 1 \ \forall v, 0 < v < t$, com $t,v \in \mathbb{N}$. Nestas condições, diz-se que a ordem de a é t, o que será denotado por ord(a) = t.

Como já foi estabelecido pelo teorema 2.9, corpos finitos são estruturas cíclicas, onde não há noção de ordem. O teorema 2.10 esclarece este fato através de uma propriedade satisfeita por todo elemento de um corpo finito de ordem q. Esta propriedade será bastante utilizada no decorrer deste trabalho.

Teorema 2.10. Seja GF(q) um corpo , então todo $a \in GF(q)$ satisfaz $a^q = a$ [3].

O comprimento de transformadas sobre corpos finitos está relacionado com as ordens dos elementos que compõem seu núcleo. O teorema seguinte estabelece precisamente a distribuição de ordens dentre os elementos de um corpo finito. Este não é um teorema construtivo, mas sim de existência.

Teorema 2.11. Seja GF(q) um corpo com q elementos, e t um inteiro positivo:
i) Se t não divide (q-1), não há elementos de ordem t em GF(q).
ii) Se t divide (q-1), então existem exatamente $\phi(t)$ elementos de ordem t em GF(q) [2].

O teorema a seguir sugere uma forma de encontrar elementos de ordem desejada, a partir de elementos cuja ordem é conhecida.

Teorema 2.12. Sejam $c_i, a_i \in GF(q)$, tal que ord(a_i) = m e ord(a_2) = n, com mdc(m,n) = 1. Então ord($a_1 a_2$) = mn [2].

Definição 2.7. Um gerador do grupo cíclico GF(q) é chamado de elemento primitivo de GF(q). Sua ordem é q-1.

Definição 2.8. Seja $GF(q^m)$ uma extensão de GF(q) e considere $a \in GF(q^m)$. Então os elementos $a, a^q, a^{q^2}, \ldots, a^{q^{m-1}}$ são chamados de conjugados de a com respeito a GF(q).

Teorema 2.13. Os conjugados de $a \in GF(q)$ com respeito a algum subcorpo de GF(q) tem a mesma ordem em GF(q)*.

As relações entre corpos de extensão e seus subcorpos em geral não estão explícitas em seus elementos. O teorema abaixo estabelece uma condição necessária e suficiente para que um elemento de um corpo de extensão pertença a um de seus subcorpos.

Teorema 2.14. Seja $GF(q^m)$ um corpo finito com q^m elementos, e **K** um subcorpo de $GF(q^m)$ com q elementos. Um elemento $p \in GF(q^m)$ está em **K** se e somente se $p^q = p$ [2].

Tem-se a seguir uma propriedade da exponenciação sobre corpos finitos que será utilizada nas demonstrações de propriedades da THCF.

Teorema 2.15. Seja GF(q) um corpo de característica p. Então (cti + *aj* + ... + $ct_s)^{p^n}$ = cti^{p^n} + $ct_2^{p^n}$ + ...+ $a_s^{p^n}$, V ai,a_2, ct_s eGF(q) e neN [3].

2.4 Exponenciação

2.4.1 Teorema de Euler

Definição 2.9. Denomina-se Função de Euler a função aritmética (j) abaixo definida por

$$\begin{aligned} (() &: N \longrightarrow N \\ n &\longrightarrow \text{número de inteiros positivos menores} \\ &\quad \text{que n e relativamente primos com n.} \end{aligned}$$

Teorema 2.16. (Teorema de Euler) Sejam a e n dois inteiros positivos tais que o mdc(a,n)=l. Então **[9]:**

$$a^{*(n)} = 1 \bmod (n).$$

Definição 2.10. Sejam a um inteiro e p um primo ímpar tais que mdc(a,p) = 1. Nestas condições, se a congruência quadrática

$$x^2 = a \bmod (p)$$

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

2.4.2 Critério de Euler

Teorema 2.17. (Critério de Euler) Sejam a um inteiro e p um primo ímpar tais que mdc(a,p)=l. O inteiro a é um resíduo quadrático de p se e somente se

$$a^{(p-1)/2} = 1 \bmod (p).$$

Demonstração :
(=>) Como a é um resíduo quadrático de p, então existe um x tal que x^2 = a mod (p). Como mdc(a,p) = 1 então mdc(x,p) = 1. Assim, pelo Teorema de Fermat:

$$a^{(P-i)/2} = (x^2)^{\frac{p-i}{2}} = x^{P-I} = i \bmod (p).$$

(<=) Suponha que $a^{(p-1)/2} = 1 \bmod (p)$ e seja r um elemento primitivo de GF(p). Então $a = r^k \bmod (p)$, com $1< k <p-1$ e desta forma

$$r^{k(p-1)/2} = 1 \bmod (p),$$

implicando que $(p-1) \mid [k(p-1)/2]$, logo k é par: $k = 2t$. Portanto $x = r^t$ é uma solução da congruência $x^2 \equiv a \bmod (p)$. •

Proposição 2.1. Seja p um primo ímpar:

(i) Se $p = 1 \bmod (4)$ então -1 é um resíduo quadrático de p.
(ii) Se $p = 3 \bmod (4)$ então -1 é um resíduo não quadrático de p.

Demonstração :
(i) O primo p é da forma 4k+1, logo (p-1)/2 é par. Assim, $(-1)^{(p-1)/2} \equiv 1 \bmod (p)$ e pelo critério de Euler -1 é um resíduo quadrático de p.
(ii) Neste caso, p é da forma 4k+3, logo (p-1)/2 é ímpar. Novamente pelo critério de Euler a proposição está demonstrada. •

A seguir é demonstrado um teorema de grande importância no desenvolvimento da THCF, bem como na compreensão da estrutura algébrica sobre a qual esta é definida.

Teorema 2.18. Seja $q = p^r$, com $p = 3 \bmod (4)$ e r um inteiro ímpar, então não existe $j \in GF(q)$ tal que $j^2 = -1$ em GF(q).

Demonstração : De acordo com a proposição 2.1 não existe $j \in GF(p)$ tal que $j^2 = -1$, logo $s(x) = x^2 +1$ é irredutível sobre GF(p). Como r é ímpar, mdc(r,2) = 1, então pelo teorema 2.6 s(x) é irredutível sobre GF(q) e também não possui raízes neste corpo, já que possui grau 2. Desta forma $j^2 = -1$ não tem solução em GF(q). •

O próximo teorema generaliza a idéia do critério de Euler.

Teorema 2.19. Seja $k \in N$; então $a \in GF(q)^*$ é a k-ésima potência de algum elemento de GF(q) se e somente se $a^{(q-1)/d} = 1$, onde d = mdc(q-1,k) [3].

Capítulo 3

Transformadas Discretas

3.1 Contínuo Versus Discreto

Historicamente as transformadas contínuas são descobertas antes de suas versões discretas. A Transformada (Contínua) de Fourier, por exemplo, foi desenvolvida em 1810. Surgiram posteriormente a Transformada de Fourier de Tempo Discreto e a Transformada Discreta de Fourier. Em 1971 surgiu a Transformada de Fourier em um Corpo Finito. Estas quatro transformadas possuem propriedades semelhantes, possuem interpretações semelhantes, contudo seus pares transformados são completamente distintos. A Transformada de Fourier relaciona um sinal contínuo no tempo e definido em toda a reta real, $v(t)$, com seu espectro $V(f)$. Por outro lado, a Transformada de Fourier de Tempo Discreto relaciona um sinal discreto no tempo e definido em um número infinito (mas contável) de instantes e seu espectro (periódico). Já a Transformada Discreta de Fourier relaciona um vetor $[v]$, com um número finito de entradas (a menos de uma periodicidade) no tempo e seu espectro $[V]$, que é um vetor de mesmo comprimento (a menos de uma periodicidade). Por fim, a Transformada de Fourier em um Corpo Finito relaciona vetores sobre um espaço vetorial cujo corpo base é um corpo finito $GF(q)$, e cujo domínio transformado pertence a um espaço vetorial onde o corpo base é um corpo de extensão, $GF(q^m)$.

A idéia de que sempre é possível calcular a transformada de um sinal através de sua definição contínua utilizando a Transformada de Fourier, requer, ao menos, uma expressão exata durante um intervalo de tempo infinito (caso o sinal não seja periódico) do sinal a ser transformado. Na prática, a utilização da Transformada (Contínua) de Fourier é inviável, mas ainda assim, a necessidade de se analisar o espectro de um sinal é algo imprescindível na Engenharia Elétrica. Surge então a necessidade de uma transformação que não necessite de toda a informação de um sinal contínuo, mas descreva de forma satisfatória o seu espectro.

Um outro aspecto, também de natureza prática, que impõe a definição de transformadas discretas recai sobre o fato de que o tratamento computacional de um sinal só pode ser realizado através de um número finito de amostras deste sinal, e mais, estas amostras devem variar sua amplitude dentre um número finito de valores. Há então, a necessidade de se operar com estas transformadas de maneira discreta.

E claro que o resultado do cálculo de uma transformada discreta de um sinal é, teoricamente, totalmente diferente do cálculo da transformada contínua deste mesmo sinal (com raras exceções, como por exemplo sinais que são discretos e periódicos). A fim de tratar-se um sinal de forma discreta, deve-se truncá-lo, amostrá-lo e quantizar estas amostras, o que causa efeitos em seu espectro que podem distorcê-lo a tal ponto de ficar impossível retornar ao domínio temporal e recuperar ao menos uma versão semelhante do sinal original. Desta forma, as etapas de amostragem e truncamento são vitais para o processo de avaliação de um espectro através dc transformadas discretas.

Transformadas discretas são freqüentemente utilizadas em:

- Compressão de dados de voz e vídeo para permitir sua transmissão com banda reduzida.
- Cálculo rápido de convoluções (filtragem digital) e correlações.
- Processamento de imagem, especialmente em reconhecimento de padrões.
- Análise espectral de sinais.
- Modulação digital.

3.2 Transformadas Discretas

Seja E um corpo e F um corpo de extensão de E. Sejam $v = (v_0, vi, \ldots VN-I)$ e $V = (Vo, Vi, \ldots VN-I)$ vetores de comprimento N em E e F, respectivamente. Assim, define-se genericamente uma Transformada Discreta como uma transformação T descrita por

$$T : E^N \rightarrow F^N$$
$$T(v) = V$$

3.2.1 Classificação

As componentes do par transformado descrito anteriormente podem pertencer a um corpo finito (característica p), ou infinito (característica zero), como mostrado pelo teorema 2.2. Pode-se então agrupar as transformadas discretas em duas classes distintas de acordo com a característica do corpo sobre a qual estão definidas.

As transformadas discretas de característica zero foram desenvolvidas espelhando-se em suas versões contínuas. Como tal, o par transformado discreto é bastante semelhante ao par transformado contínuo.

Por outro lado, as transformadas discretas de característica p são bem mais recentes e menos numerosas. São poucas as transformadas discretas sobre corpos infinitos que possuem uma versão num corpo de característica p. Vale ressaltar que mesmo possuindo propriedades semelhantes as propriedades das transformadas discretas de característica zero, os pares

transformados sobre corpos finitos em geral são completamente diferentes dos pares transformados discretos sobre corpos infinitos .

	Característica Zero	Característica p
Transformadas Discretas	**Transformada Discreta de Fourier**	**Transformada de Fourier em um Corpo Finito**
	Transformada Discreta do Cosseno	
	Transformada Discreta do Seno	
	Transformada Discreta de Hartley	**Transformada de Hartley em um Corpo Finito**
	Outras	**Outras**

[Transformada de Fourier de Corpo Finito (TFCF) - *Galois Field Transform* (GFT)

Transformada Numérica de Fourier - *Number Theoretic Transform* (NTT) [Fermat [Mersenne

3.2.2 A Transformada Discreta de Fourier

Sendo de fundamental importância no Processamento de Sinais, bem como na análise de Sistemas de Comunicações, a Transformada de Fourier é uma ferramenta constantemente utilizada em Engenharia Elétrica. Suas aplicações se destacam, por exemplo, no cálculo eficiente de convoluções, na obtenção da resposta em freqüência de sistemas, na análise espectral de sinais, entre diversas outras.

A Transformada Discreta de Fourier tem a seguinte lei de transformação

$$v_k = \sum_{i=0} v_i w^{ik}$$

$$v_i = \frac{1}{N} \sum_{k=0}^{N-1} v_k w^{-ik}$$

onde i,k = 0, 1 , N - l e W é uma raiz N-ésima da unidade em F .

A seguir tem-se uma representação da Transformada de Fourier na forma matricial

$$[V] \quad [T]_{N \times N} [v]_{N \times 1} \quad , \text{ onde}$$

$$T = \begin{matrix} W & W^2 & \cdots & W^{N-1} \\ \vdots & & & \\ W^{N-1} & W^{N-2} & \cdots & W \end{matrix}$$

Se E é o corpo dos reais **R** (ou dos complexos C) e F = C, então $W = e^{\frac{2\pi}{N}}$ e assim tem-se a chamada Transformada Discreta de Fourier (TDF) ou DFT *(Discreíe Fourier Transform).*

Se E = F = GF(p), então W e GF(p) é um elemento de ordem N. Neste caso, tem-se uma NTT. Se p for um primo de Mersenne, obtém-se uma NTT de Mersenne, ou MNT *(Mersenne Number Transform).* Se p for um primo de Fermat, obtém-se uma NTT de Fermat, ou FNT *{Fermat Number Transform).*

Se E = GF(p) e F = GF(p^m), com m > 1, então W = a é um elemento de ordem N de GF(p^m). Neste caso, tem-se uma GFT.

Ao contrário da TDF, cuja imagem é complexa, as transformadas discretas mostradas a seguir são mapeamentos cuja imagem está contida em **R,** ou seja, E = F = **R.**

3.2.3 A Transformada Discreta do Cosseno

Esta transformada foi proposta em 1974 [10], e tem seu uso consagrado em processamento digital de imagem. Sua definição é baseada nos polinómios de Chebyshev, de onde decorrem algumas excelentes propriedades, como por exemplo seu erro médio quadrático, que é similar ao erro cometido pela transformada de Karhunen-Loève, ótima neste requisito. Uma propriedade relevante da transformada discreta do cosseno (TDC) é seu desempenho no que diz respeito a taxa de distorção. Esta transformada é utilizada também no contexto de reconhecimento de padrões.

Especificamente, um par transformado da TDC é definido por

$$V_k = M(k)\sqrt{\frac{2}{N}} \sum_{i=0}^{N-1} v_i \cos\left(\frac{(2i+1)k\pi}{2N}\right)$$

c

$$v_i = \sqrt{\frac{2}{N}} \sum_{k=0}^{N-1} M(k) V_k \cos\left(\frac{(2i+1)k\pi}{2N}\right),$$

ondei,k = 0, 1,...,N-1 e $M(k) = \begin{cases} -7 =, \text{ se } k = 0 \\ 1, \text{ se } k * 0 \end{cases}$

3.2.4 A Transformada Discreta do Seno

A Transformada Discreta do Seno (TDS) e a TDC foram definidas simultaneamente. Suas definições são similares, como descrito abaixo, onde tem-se o par da TDS

$$Vk = \boldsymbol{h} \quad M(k)£ \quad v.\ \text{sen}^{f}\ (2i - \backslash)kK$$
$$V \qquad 2N$$

$$\mathbf{V\ i} = J \wedge Z \quad M(k)V_{k}\text{sen}\ \frac{(2i - l)fcr}{2N}$$

ondei,k = 0, 1, ...,N-1.

3.2.5 A Transformada Discreta de Hartley

A Transformada Contínua de Hartley foi originalmente publicada em 1942 por R. V. L. Hartley, no *Proceedings of the Institute of Radio Engineers* [33]. Em sua publicação, Hartley deu ênfase ao caráter simétrico de seu par transformado assim definido:

$$H(v) = J\ v(t)\text{cas}(27\text{ivt})dt$$

$$v(t) = J\ H(f)\text{cas}(27\text{ivt})dv,$$

onde v é real e a função cas(.) é definida como a soma de cos(.) e sen(.), isto é

$$\text{cas}(6) = \cos(9) + \text{sen}(8).$$

A Transformada Discreta de Hartley (TDH) foi proposta por Bracewell em 1982. Similarmente a Transformada Contínua de Hartley, a TDH possui a função cas(.) como núcleo e novamente possui um caráter simétrico. Tem-se abaixo a definição do par transformado da TDH

$$V_{k} = \ > \quad \mathbf{v_j}\ \text{cas} \frac{\quad}{\quad}$$

1 » *(2km)*

onde i,k = 0, 1 , N - l .

Na próxima seção algumas propriedades da TDH são citadas, cujas demonstrações podem ser encontradas em [1]. Como será apresentado no capítulo 4, estas propriedades são similares as encontradas para a Transformada de Hartley em um Corpo Finito.

3.2.5.1 Propriedades

Sejam g <-» G e h <-> H pares tranformados TDH de comprimento N.

TD1 Linearidade

Sejam a,b e **R;** então ah + bg <-» aH + bG .

TD2 Deslocamento no Tempo

$$\overline{\cos}\ V\ N\ j\ Ok - sen\ \overline{|}\ 1\ N\ )$$

TD3 Soma da Seqüência

$$H_o = \sum_{j=0}^{N-1} h_j .$$

TD4 Valor Inicial

$$h_n = -\sum_{k=0}^{N-1} H_k .$$

TD5 Reversão Temporal

$h_n \leftrightarrow H_{-k}$.

TD6 Simetria

$H \leftrightarrow N h$.

TD7 Convolução Cíclica

$g * h \leftrightarrow Vi\ (GH + GH. + G.H - G.H.)$,

onde G. e H. denotam, respectivamente, $G_{n,-k}$ e $H_{n,-k}$.

TD8 Relação de Parseval

$$N \sum_{j=0}^{N-1} h_j^2 = \sum_{k=0}^{N-1} H_k^2 .$$

3.2.6 Relações entre as Transformadas de Fourier e de Hartley

Nesta seção são apresentadas relações entre F_k, a k-ésima componente da Transformada Discreta de Fourier do vetor v = (v_0 ,V| , VN-I), e H_k, a k-ésima componente da Transformada Discreta de Hartley do mesmo vetor. Re e Im denotam, respectivamente, a parte real e a parte imaginária.

i) H_k = Re{(l+j)F_k}.

Demonstração : De acordo com a definição da TDF

$$F_k = Z\ v_i e^{j2k71,/N} = 2.\ viços\ \frac{(2km)}{} .« - J2.\ Visen| V\ N\ *$$

logo

$$Re\{F_k\} = \sum_{1n}^{N-1} 2u \cdot i \cdots 2\ km \quad e \quad Im\{F_k\} = -\sum_{iD}^{N-1} Vjsen\ 2km$$

Pela definição da TDH tem-se

$$H_k = (Re\{F_k\} - Im\{F_k\}) = Re\{(l + j)F_k\}$$

ii) F_k = ^{H_{N-k} + H_k} + j{H_{N-k} - H_k}.

Demonstração :

$$H_{k-k} = 2 - \sum_{i} \cdot i \cdots \frac{(2(N-k)m^{\wedge}}{N}$$

$$\sum_{i=0}^{N-1} \cdot i [\cdots \left| \frac{(2km)}{2m - \frac{}{N)}} \right| + sen \left| 2m - \frac{2km\backslash}{N\ J} \right|$$

contudo,

$$cosi\ 2m - \frac{2km\backslash}{N} I = cos\ (\frac{2km}{N\ *} \quad e \quad sen\ 2m - \frac{2\ km}{\sim N \sim} = -sen\ \frac{2km}{N >}$$

Desta forma

$$H_{N-k} = \sum_{i-0}^{N-1} X \cdot i [COS \left| \frac{}{s\ N)} \right| - sen \left| \frac{(2km\backslash}{l\ N\ J} \right|$$

Tem-se então que

$$Re\{F_k\} = -\{ H_{N-k} + H_k \}$$

e

$$Im\{F_k\} = \frac{1}{2}\{ H_{N-k} - H_k \}.$$

Todas estas transformadas discretas descritas acima possuem algoritmos rápidos semelhantes às Transformadas Rápidas de Fourier *(Fast Fourier Transform* - FFT). A próxima seção apresenta as FFTs clássicas.

3.3 Transformadas Rápidas

A Transformada Discreta de Fourier detém um papel fundamental na análise, projeto e implementação de algoritmos para processamento digital de sinais. A descoberta das Transformadas Rápidas de Fourier (FFT) possibilitou um aumento substancial na eficiência do cálculo computacional da DFT. O cálculo direto da DFT a partir da definição requer N^2 multiplicações e N(N-l) adições. Este número pode ou não ser aceitável, dependendo da aplicação. Assim, entende-se por FFT, um algoritmo que reduz a complexidade computacional em relação ao cálculo direto. E um fato bem estabelecido que existem vantagens computacionais em se formular a DFT unidimensional como um problema bidimensional [6]. Isto é, o vetor unidimensional de entrada é mapeado num arranjo bidimensional, o qual após ser processado é mapeado num vetor unidimensional de saída. Assim funcionam, por exemplo, os algoritmos de Cooley-Tukey e Good-Thomas [6].

3.3.1 Cooley-Tukey

A TDF que desejamos calcular tem como comprimento o número composto N = njn2, onde ni e n2 são inteiros positivos. As novas coordenadas, \\ e Í2, do mapeamento bidimensional do vetor de entrada Vj são definidas por

$$i = ii + mÍ2, \quad com \quad i] = 0,l,...,ni-1 \quad e \quad Í2 = 0,l,...,ri2-1.$$

O vetor de entrada, agora bidimensional, será transformado em um vetor de saída V_k, cujas novas coordenadas ki e k2 são dadas por

$$k = n2ki + k2, \quad com \quad ki = 0,l,...,ni-1 \quad e \quad k_2 = 0,l,...,n.2-1.$$

Aplicando-se o mapeamento bidimensional à definição da TDF, manipulando-se os índices convenientemente e utilizando o fato de que $W^N = 1$, pode-se reescrever a TDF como

$$\mathbf{n \quad +1<2 = Z \; x^{i_1 k_1}\left(W^{i_1 k_2} \sum_{i_2=0}^{n_2-l} \gamma^{i_2 k_2} v_{i_l + n i' 2} \right.}$$

onde $y = W^{n_1 r}$ e $r = W^{n_2}$.

O algoritmo consiste em se calcular ni TDFs de comprimento n2, seguido por N multiplicações complexas devido ao fator $W^{r \cdot k_2}$ e por fim, efetua-se n2 TDFs de comprimento ni . Este algoritmo requer a seguinte complexidade computacional:

Número de multiplicações complexas: N(ni + n2 + 1).
Número de adições complexas: N(ni + n2 - 2).

Em muitas aplicações o algoritmo de Cooley-Tukey utiliza comprimentos N da forma potência de 2. Neste caso, o comprimento $N = 2^a$ é fatorado da seguinte forma

$$n_1 = 2 \quad e \quad n_2 = 2^{a-1}$$

Como conseqüência, o algoritmo calcula uma Transformada de Fourier de comprimento N através de duas Transformadas de Fourier de comprimento N/2, mais alguns cálculos extras. Deste modo, o algoritmo é utilizado recursivamente e, em cada nível, uma transformada de comprimento N é substituída por duas de comprimento N/2, que são processadas da mesma forma. Assim, a complexidade computacional para esta FFT é dada por [6]:

Número de multiplicações complexas: (N/2)log2 N.
Número de adições complexas: Nlog2 N.

3.3.2 Good-Thomas

Este algoritmo é bastante semelhante ao anterior, com a restrição de que ni e n2 devem ser primos entre si. O mapeamento bidimensional é baseado no Teorema Chinês dos Restos [9] e é apresentado a seguir.

As novas coordenadas, i| e Í2, do mapeamento bidimensional do vetor de entrada Vj são definidas por

$$ii = i \bmod (ni) \quad e \quad Í2 \bullet i \bmod (n2).$$

Pelo Teorema Chinês dos Restos, existem inteiros Ni e N2 tais que o índice de entrada pode ser recuperado por

$$i = iiN_2n_2 + Í2Njni \mod (n),$$

onde N| e N2 são inteiros que satisfazem

$$N_1n_1 + N_2n_2 = 1.$$

O vetor de entrada, agora bidimensional, será transformado em um vetor de saída Vk, cujas novas coordenadas ki e k2 são dadas por

$$ki = Nik \bmod (ni) \quad e \quad k2 = Njk \bmod (n2),$$

e desta forma recupera-se o índice k através da relação

$$k = r\backslash 2k\backslash + r\backslash\backslash k2 \mod (n).$$

A vantagem deste mapeamento, com relação ao algoritmo de Cooley-Tukey, é a eliminação do termo $W^{\cdot\cdot k2}$ durante a computação. Desta forma, a TDF pode ser calculada como

$$V_{n_2 k|+n|k_2} = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} r^{i_1 k_1} y^{i_1 k_2} v_{'i^{\wedge}2^{\wedge}2 *'2^{\wedge}i"i\ '}$$

onde $y = W^{N \cdot V}$ e $r = W^{N\ '^{nj}\backslash}$

Portanto, este algoritmo requer N multiplicações a menos que o algoritmo de Cooley-Tukey. Sua complexidade computacional é descrita abaixo:

Número de multiplicações complexas: N(ni + n2).
Número de adições complexas: N(ni + n2 - 2).

3.4 A Transformada de Fourier em um Corpo Finito

A Transformada de Fourier em um Corpo Finito foi originalmente introduzida em 1971 [20] 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 [6], [11], [15], [16], [17].

O cálculo de transformadas em corpos finitos tem a vantagem de não introduzir erros de truncagem ou arredondamento e apresentar uma aritmética de baixa complexidade (especialmente nos casos em que a característica do corpo é um primo de Mersenne ou um primo de Fermat).

Definição 3.1. Seja v = (vo , vi , ... , $v_{N_}$i) um vetor de comprimento N e componentes em GF(q), onde $q = p^{r}$, então o vetor V = (V_0 , Vi ,... , V_{N}.|) com componentes em GF(q^{m}) dadas por

$$V_k = \sum_{i=0}^{N-1} v^{\wedge 1},$$

onde a é um elemento de ordem N em GF(q^{m}), é a Transformada de Fourier em um Corpo Finito (TFCF) de v.

3.4.1 Propriedades

Sejam g <-> G e f <-> F pares tranformados TFCF de comprimento N, como definidos anteriormente.

Fl Linearidade
Sejam a,beGF(q) então af + bg <-» aF + bG.

F2 Deslocamento no Tempo
Suponha que fj = gj.i; então $F_k = et^{n_i} Gk$.

F3 Convolução Cíclica
g*f^>GF={$G_k F_k$}.

F4 Espectros Válidos

'k 'kq(modN)'

A relação F4 induz uma partição dos inteiros módulo N em classes de equivalência chamadas ciclotômicas ou de conjugação. As componentes Fk cujos índices pertencem a uma dada classe estão relacionadas por F4, de modo que é neccessário especificar apenas uma delas para se determinar todas as outras.

3.4.2 As Transformadas Numéricas de Fourier

No nível do *hardware,* a implementação de NTTs é de extrema facilidade e simplicidade, se comparado ao *hardware* necessário para se efetuar uma DFT, por exemplo. Além de resultar em custos menores, o cálculo de NTTs pode se dar de maneira bastante rápida. A atração pelas NTT's surge, dentre outros, pelo fato delas não causarem erros por arredondamento, *overflow,* ou quantização. Já no cálculo de uma DFT, todos esses problemas ocorrem e, de maneira geral, seus efeitos estão intimamente relacionados com N, a ordem da transformação.

Como escolher a NTT apropriada para uma transformação de comprimento longo ? Pode-se destacar três considerações práticas importantes (no que diz respeito a eficiência computacional) na definição de uma NTT.

(i) Escolha do módulo p 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 de N - comprimento 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 de W - núcleo da transformada:
A multiplicação por potências de W deve ser de baixa complexidade computacional (deve resultar, se possível, apenas em deslocamentos).

A escolha óbvia para p, seria algum valor baseado em uma potência de 2, já que os sistemas eletrônicos digitais são baseados em operações binárias onde, por exemplo, o contador é um sistema inerentemente modular. Dessa forma, existem as seguintes escolhas possíveis para p:

$$p = 2^q - 1 \qquad \text{ou} \qquad p = 2^q + 1 .$$

Como $p = 2^q - 1$ é um número de Mersenne, as NTTs baseadas neste módulo são denominadas Transformadas Numéricas de Mersenne (MNT) e, equivalentemente, para $p = 2^q + 1$, geram-se as Transformadas Numéricas de Fermat (FNT).

3.4.2.1 A Transformada Numérica de Mersenne

Se p é um primo de Mersenne, pode-se escolher $W = 2$ e $N = p$ ou ainda $W = -2$ e $N = 2p$. Neste último caso, é possível usar uma FFT para calcular a NTT desejada. Uma grande vantagem da MNT é que a aritmética em GF(p) é bastante coveniente se os inteiros forem representados como binários de q bits, pois neste corpo $2^q - 1 = 0$, ou seja, o *overflow* $2^q = 1$.

3.4.2.2 A Transformada Numérica de Fermat

A vantagem de se implementar uma NTT sobre GF(p) com p um primo de Fermat é que W é uma potência de 2 ou uma soma (ou subtração) de potências de 2. Com isto as multiplicações em binário são convertidas em deslocamentos. Outra vantagem decorre do fato que N é uma potência de 2, e a FFT de Cooley-Tukey pode ser aplicada para calcular tal NTT.

E importante observar que as NTTs possuem a propriedade da convolução cíclica e portanto podem ser utilizadas para calcular convoluções em corpos finitos. Além disso as FFTs descritas anteriormente podem ser aplicadas no cálculo da GFT bem como no cálculo das NTTs.

Capítulo 4

A Transformada de Hartley em um Corpo Finito

Este capítulo apresenta a definição do conjunto de Inteiros Gaussianos sobre um Corpo Finito, determina as propriedades de seus elementos, bem como suas características estruturais. Em seguida é introduzida, pela primeira vez na literatura, uma trigonometria sobre corpos finitos. Especificamente, as funções k-trigonométricas sobre corpos finitos são definidas e suas propriedades exploradas. Dentre as funções k-trigonométricas, a família de funções cask(.) apresenta uma forma de ortogonalidade que possibilita a definição da Transformada de Hartley em um Corpo Finito (THCF), uma nova transformada sobre corpos finitos que apresenta um mesmo núcleo tanto para a transformada direta, como para a transformada inversa. São desenvolvidas as propriedades desta nova transformada, que assemelham-se às propriedades da Transformada Discreta de Hartley (TDH), bem como novas propriedades que não possuem equivalentes na TDH. As relações entre as Transformadas de Fourier em um Corpo Finito (TFCF) e a THCF também são estabelecidas.

4.1 Inteiros Gaussianos sobre Corpos Finitos

Nesta seção é construído, a partir de um corpo finito, um corpo de extensão similar a extensão realizada pelos números Complexos sobre o corpo dos números Reais. As condições para a construção deste corpo de extensão impõem restrições sobre a escolha da ordem do corpo, como mostrado na definição abaixo. No que se segue o símbolo := denota igual por definição.

4.1.1 Definição

Definição 4.1. G(q) := {Ç = a + jp , a,p e GF(q)}, onde $q = p^r$, com p = 3 mod (4) e r um inteiro ímpar, é o conjunto de Inteiros Gaussianos sobre GF(q).

Proposição 4.1. Sejam © e * operações definidas sobre os elementos de GF(q) e dadas por

$$\begin{aligned} &\copyright : G(q) \times G(q) \rightarrow G(q) \\ &(a_1 + jp_1) \copyright (a_2 + jp_2) \rightarrow (a_1 + jp_1) \copyright (a_2 + jp_2) = (a_1 + a_2) + j(p_1 + p_2) \end{aligned}$$

e

$$\begin{aligned} &* : G(q) \times G(q) \rightarrow G(q) \\ &(a_1 + jp_1) * (a_2 + jp_2) = (a_1 a_2 - p_1 p_2) + j(a_1 p_2 + a_2 p_1). \end{aligned}$$

A estrutura definida por GI(q) = < G(q) , © , * > é um Corpo isomorfo a $GF(q^2)$ (denota-se $GI(q)=GF(q^2)$).

Demonstração : Observando-se os teoremas 2.4, 2.5 e 2.18, conclui-se que GI(q) é um corpo. Com as operações definidas acima, há um isomorfismo entre GI(q) e GF(q)[x] / (x^2+1), dado por

$$M : GI(q) \rightarrow GF(q)[x] / (x^2+1)$$

$$a + JP \rightarrow a + \sim p\, x$$

$$j \rightarrow x$$

$$a \rightarrow a$$

Pelo teorema 2.7 tem-se que GI(q) é isomorfo a $GF(q^2)$. •

4.1.2 Propriedades

Esta seção apresenta, sob a forma de proposições, algumas propriedades básicas satisfeitas pelos Inteiros Gaussianos sobre Corpos Finitos. Antes porém, definem-se a Norma Quadrática e a Ordem Complexa de um elemento em GI(q).

Definição 4.2. Seja Ç = a + jp eGI(q). A Norma Quadrática deste elemento é definida como $|Ç|^2 = |(a + jp)|^2 = (a^2 + p^2)$ eGF(q).

Definição 4.3. Seja Ç = a + jp eGI(q). Define-se a Ordem Complexa deste elemento, ocx(Q, como sendo o menor natural n tal que $(a + jp)^n$ eGF(q).

Proposição 4.2. Seja Ç = a + jp eGI(q), onde $q = p^r$. Nestas condições tem-se

i) ord(Ç) | (q+l)(q-l).

ii) $Ç^{q} = C,\wedge$, onde ^{A} denota complexo conjugado.

iii $K^{q+1} = |ç|^{2}$.

Demonstração :
i) Pela proposição 4.1 tem-se que GI(q) = $GF(q^{2})$ e o resultado segue pelo teorema 2.11.

ii) Ç - a + j(3 eGI(q) e, por definição, a, j, peGI(q) = $GF(q^{2})$ = $GF(p^{2t})$. Pelo teorema 2.15 tem-se que

$$Ç^{q} = cc^{q}+j^{q}p^{q},$$

O fato de que j = -1 gGF(q) resulta, pelo teorema 2.18, que q é uma potência de um primo da forma 4k+3, implicando que $j^{q} = -j$. Pelo teorema 2.10 concluí-se que

$$Ç^{q} = ct-JP = Ç - .$$

iii) Pelo item anterior: $Ç^{q+1} = (a - JP)(a + JP) = a^{2} + p^{2}$. •

Proposição 4.3. Se Ç é primitivo em GI(q) => $|Ç|^{2}$ é primitivo em GF(q).

Demonstração: Como Ç é primitivo, então o menor n tal que $Ç^{n} = 1$ é n = (q+l)(q-l). Logo, pela proposição 4.2,

Conclui-se então, que o menor m tal que $(|Ç|^{2})^{m} = 1$ é m = q-1. Como $|Ç1^{2}$eGF(q), isto implica que |Ç| é primitivo.

•

Proposição 4.4. Seja GI(q). A ocx(Q é um divisor de (q+1).

Demonstração: Se Ç é real a demonstração segue, pois 1 | (q+1). Se Ç é complexo, denote ocx(Q = n. Por definição da Ordem Complexa n < (q+1), pois $Ç^{q+1}$ é real. Suponha, por absurdo, que n não divide (q+1); logo (q+l) = dn+r, com 0 < r < n e d um inteiro positivo. Considere ct|, a_{2} GGF(q), $Ç^{n} = ai$ e $Ç^{q+1} = a_{2}$. Desta forma,

$$Çq+l_{=}Çdn_{+}r = çdnçr = (ai y > çr = (X25$$

logo

$$Ç = a_{2}(a_{l})^{-0} \quad eG¥(q),$$

o que é uma contradição pois r < n. Conclui-se então, que n divide (q+1). •

4.2 Funções k-Trigonométricas

Esta seção apresenta uma definição de funções trigonométricas sobre corpos finitos, no sentido de que possuem propriedades semelhantes as das funções trigonométricas classicamente definidas. As famílias de funções coSk(.) e senk(.) são inicialmente apresentadas, bem como suas propriedades. A seguir, deriva-se destas funções básicas a família de funções cask(.), suas propriedades e o resultado principal desta seção, que é o teorema 4.1. Este teorema fornece os elementos para a definição da Transformada de Hartley em um Corpo Finito, que é definida na próxima seção.

4.2.1 As Funções $\cos_k$ e sen_k

Definição 4.4. Seja Ç um elemento não nulo em GI(q), com q = p^r, p um primo ímpar da forma 4k + 3. Definem-se as funções k-trigonométricas de Z(Ç') := i (arco do elemento Ç') em GI(q) da seguinte forma

$$\cos_k(UÇ)_{:} = I(C^k + C^k)$$

e

$$\mathrm{sen}_k(ZÇ)_{:} = \pm(Ç^{ik} - Ç^{ik})$$

onde q = p^r, Ç tem ordem multiplicativa N , N | q^2-l e i,k = 0, 1 , N - l .

Esta definição e as propriedades seguintes só fazem sentido se GI(q) é um corpo (pois apenas nesta estrutura é garantida a existência de uma potência negativa do elemento Ç). Este é o porque da exigência de p = 3 mod (4) como definido acima.

4.2.1.1 Propriedades

Por simplicidade considera-se Ç fixo na definição da função k-trigonométrica, denotando-se então $\cos_k(ZÇ^i) := \cos_k(i)$ e $\mathrm{sen}_k(ZÇ^i) := \mathrm{sen}_k(i)$ com i,k = 0, 1, 2, ...,N-1.

PI Círculo Unitário

$\mathrm{senk}^2(i) + \mathrm{cosk}^2(i) = 1$.

Demonstração :

$\mathrm{sen}_k'(i) + \cos_k'(i) = [\wedge(Ç^{ik} - Ç'')T + (Ç^{ik} + Ç'')Y =$

$= —(Ç^{2,k} + Ç^{-2ik} - 2) + -(Ç^{2,k} + Ç'^{2,k} + 2) = 1.$ •

P2 Par/Impar

$cos_k(i) = cos_k(-i)$ e $sen_k(i) = -sen_k(-i)$.

Demonstração :

$cosk(-i) = \frac{1}{2}(C^{ik} + C^{-ik}) = cosk(i)$ e $sen_k(-i) = \frac{1}{2j}(C^{ik} - C^{-ik}) = -sen_k(i)$. •

P3 Fórmula de Euler

$C^{ik} = cos_k(i) + j\,sen_k(i)$.

Demonstração :

$cos_k(i) + j\,sen_k(i) = \frac{1}{2}(C^{ik} + C^{-ik}) + \frac{j}{2}(C^{ik} - C^{-ik}) = C^{ik}$ •

P4 Adição de Arcos

$cos_k(i + t) = cos_k(i)cos_k(t) - sen_k(i)sen_k(t)$.

$sen_k(i + t) = sen_k(i)cos_k(t) + sen_k(t)cos_k(i)$.

Demonstração :

$cos_k(i + t) = \frac{1}{2}(C^{(i+t)k} + C^{-(i+t)k}) = \frac{1}{2}(C^{ik}C^{tk} + C^{-ik}C^{-tk})$

$= -\frac{1}{2}\{[cos_k(i) + j\,sen_k(i)][cos_k(t) + j\,sen_k(t)] + [cos_k(i) - j\,sen_k(i)][cos_k(t) - j\,sen_k(t)]\}$

$= cosk(i)cos_k(t) - sen_k(i)sen_k(t)$.

A demonstração do seno é similar. •

P5 Arco Duplo

$cosk(i) = \frac{1 + cos_k(2i)}{2}$ e $sen_k^2(i) = \frac{1 - cos_k(2i)}{2}$

Demonstração :

De acordo com a propriedade P4,

$\cos_k(2i) = \cos^2_k(i) - \mathrm{sen}^2_k(i) -$

$$= \cos^2_k(i) - [1 - \cos^2_k(i)] = 2\cos^2_k(i) - 1 \bullet$$

A demonstração do seno é similar.

P6 Simetria Principal

$\cos_k(i) = \cos_J(k)$ e $\mathrm{sen}_k(i) = \mathrm{sen}^*(k)$.

Demonstração : Segue imediatamente da definição das funções k-trigonométricas.

P7 Simetria Secundária

$\cos_k(i) = \cos_i(t)$ com $itkl * 0$ e $k+t = i+l = N$.

$\mathrm{sen}_k(i) = \mathrm{sen}_](t)$ com $itkl * 0$ e $k+t = i+l = N$.

Demonstração :

$$2[\cos_k(i) - \cos_,(t)] = (\zeta^{ik} + C^{ik} - \zeta^{h} - C^{U}) \left| \quad \right| = \left| f \quad i \right| \wedge \zeta i(k+t)\, \zeta i(t-k) \_ \zeta t(i+i) \_ \zeta t($$

$$\_ \wedge\text{--}ik \quad \pounds\text{--}lt \_ \wedge"'k \qquad /\text{--}it = 0.$$

A demonstração do seno é similar.

P8 Complemento

$\cos_k(i) = \cos_k(t)$ com $itk * 0$ e $i+t = N$.

$\mathrm{senk}(i) = -\mathrm{sen}_k(t)$ com $itk * 0$ e $i+t = N$.

Demonstração :

$$2[\cos_k(i) - \cos_k(t)] = \{C + \quad -C - \zeta'^{k}) \quad — \ \zeta^{jk} - \zeta^{ik} =$$

$$= (C^{k} - Ç^{*}) \qquad = 0.$$

A demonstração do seno é similar . •

P9 Somatório da seqüência cos_k (i)

$$\sum_{k\ i)}^{N-1} Yj\ \cos_k(i) = \begin{matrix} N, i = 0 \\ 0, i \# 0 \end{matrix}$$

Demonstração :

$$a = \sum_{k\ 1)}^{N-1} \cos_k(i) = -\sum_{k-o}^{N-!} \mathbf{2}\ K^{ik} + C^{ik}).$$

Se i = 0 tem-se imediatamente a = N.

Se i * 0 então $a = -[\ \frac{1}{\_\ j}\ 1(4"')"-1 + \frac{\{Ç)^{N}-\}}{y\ \_\ j}\ ] = -[0 + 0] = 0.$ •

PIO Somatório da seqüência sen_k (i)

$$\sum_{k=0}^{N-1} sen_k(i) = 0.$$

Demonstração :

$$\sum_{k=0}^{N-1} \qquad \sum_{k=o}^{N-1} \mathbf{2j}$$

Se i = 0 tem-se imediatamente o* = 0.

Se i * 0 então $a = \frac{1}{2)}[\ \frac{1(0"-1}{Ç\sim\backslash};\ -\ \frac{\{Ç)^{N}-\}}{Ç-\backslash}\ ] = \frac{1}{2j}[0-0] = 0.$ •

P11 Periodicidade

$cos_k(i + N) = cos_k(i)$ e $sen_k(i + N) = sen_k(i)$.

Demonstração :

$\cos_k(i + N) = |(Ç^{l(k+N)} + C'^{i(k+N)}) - -(Ç^{ik}Ç^{iN} + Ç * C^{iN}) = \cos_k(i)$, pois a ordem de Ç é N.

A demonstração do seno é similar. •

Proposição **4.5.** As funções k-trigonométricas $\cos_k(.)$ e $\text{sen}_k(.)$ são ortogonais no seguinte sentido:

$$\sum_{k=0} [\cos_k(ZÇ)\ \text{sen}_k(ZÍ)] = 0,$$

onde a ordem multiplicativa de Ç é N em GI(q).

Demonstração: Pela propriedade P4, tem-se que

$\cos_k(ZÇ')\ \text{sen}\wedge ZÇ^{1}) = \wedge[\text{sen}_k(t + i) + \text{sen}_k(t - i)]$, logo

$$£_{k=o}^{N-1} [\cos_k(ZÕ\ \text{sen}_k(ZÇ^{1})] = \frac{j^{N-1}}{2_{k-0}} [\text{sen}_k(t + i) + \text{sen}_k(t - i)]$$

e, pela propriedade PIO, o resultado segue. •

4.2.2 A Função cas_k

Definição **4.5.** Seja Ç um elemento não nulo em GI(q). Define-se a função cas_k de $ZÇ^{1}$ em GI(q) da seguinte forma:

$$\text{cas}_k(ZC) := \cos_k(ZÇ^{j}) + \text{sen}_k(ZCj).$$

4.2.2.1 Propriedades

A função k-trigonométrica $\text{cas}_k(.)$, assim como no caso contínuo, é definida como a soma das funções seno e cosseno. As propriedades desta função k-trigonométrica definida num corpo finito são semelhantes as propriedades da função cas(9) definida sobre o corpo dos números reais. Estas propriedades são listadas a seguir.

Cl Relações k-trigonométricas

i) $\text{cas}_k(i + t) = \cos_k(i)\ \text{cas}_k(t) + \text{sen}_k(i)\ \text{cas}_k(-t)$.

ii) $\text{cas}_k(i - 1) = \cos_k(i)\ \text{cas}_k(-t) + \text{sen}_k(i)\ \text{cas}_k(t)$.

iii) $\text{cas}_k(i)\ \text{cas}_k(t) = \cos_k(i - 1) + \text{sen}_k(i + t)$.

Demonstração :

i) Pela definição 4.5 tem-se

$cask(i+1) = coSk(i+t) + sen_k(i+t)$, e pelas propriedades P2 e P4 conclui-se que

$$cas_k(i+t) = cos_k(i)cos_k(t) - sen_k(i)sen_k(t) + sen_k(i)cos_k(t) + sen_k(t)cos_k(i)$$

$$= cos_k(i)[cos_k(t) + sen_k(t)] + sen_k(i)[cos_k(-t) + sen_k(-t)] =$$

$$= cos_k(i)cas_k(t) + sen_k(i)cas_k(-t).$$

ii) Similar a demonstração do item anterior.

iii) $cas_k(i)\, cas_k(t) = [cos_k(i) + sen_k(i)][cos_k(t) + sen_k(t)] =$

$$= cos_k(i)cos_k(t) + sen_k(i)sen_k(t) +$$

$$+ sen_k(i)cos_k(t) + sen_k(t)cos_k(i).$$

Observando-se as propriedades P4 e P2, tem-se o resultado.

C2 Simetria

$$cas_k(i) = casj(k)$$

Demonstração: Segue imediatamente da propriedade P6.

C3 Norma Quadrática

Seja a função $cas_k(ZÇ')$, cujo argumento $Ç = \alpha$ eGF(q). Nestas condições,

$[cas_k(i)]^{q+1} = I\ cas_k(i)\ 1^2 = cos_k(2i)$.

Demonstração: Pela proposição 4.2 tem-se

$[cas_k(i)]^{q+1} = I\ cas_k(i)\ 1^2 = [cos_k(i)]^2 - [sen_k(i)]^2$, aplica-se então P5 e PI.

C4 Ordem

Se $cas_k(i)$ é primitivo em $GF(q^2) \Rightarrow |\ cas_k(i)\ 1^2$ é primitivo em GF(q).

Demonstração : Segue diretamente da proposição 4.3. •

C5 **Periodicidade**

cask(i) é periódico, de período N.

Demonstração : Segue diretamente da propriedade PI 1. •

C6 **Nulidade**

i) Seja a função caSk(ZÇ'), cujo argumento Ç = a eGF(q). Nestas condições, $cas_k(ZÇ') * 0$ para todo i,k = 0 , 1 , N - l .

ii) Seja a função caSk(ZÇ'), cujo argumento Ç eGI(q) e Ç íGF(q). Nestas condições, se ord(Ç) não divide 8ik, então caSk(ZÇ') * 0.

Demonstração :

De acordo com as definições 4.4 e 4.5, pode-se expressar a função cask(.) na seguinte forma:

$$cas_k(zC) = \frac{I(C^k + ç^{ik})}{2} + \frac{\wedge(C - C^k) = k;^{ik} + ç\ V\ X\ Ç * - C^k)l -}{2j\qquad 2}$$

$$= |[(C^k + JC^{ik}) - j(C^k + JC^k)],$$

tem-se então

Supondo, por contradição, que caSk(ZÇ') = 0, tem-se que $Ç^{,k} + jÇ''^{lk} = 0$, ou seja, $Ç^{2,k} = -j$. Desssa forma,

i) Por hipótese, tem-se que Ç = a eGF(q), logo $a^{2,k} = -j$, o que é um absurdo, pois j gGF(q).

ii) Por hipótese, tem-se que ord(Ç) não divide 8ik, em particular Ç*l. Seja b = ord(Q, assim 8ik = db + r, com 0<r<b , logo

$$\wedge 8ik\_ pàbçr\_\_$$

mas

$$Ç^{2ik} = -j, ou\ seja,\ Ç^{8ik} = l,$$

tem-se então

o que é um absurdo, pois 0<r<ord(Q. •

C7 Relações Proibitivas

i) Seja Ç = a eGF(q). Nestas condições,

coSk(i) *• 0, para todo i,k = 0, **1 ,** N - l .

ii) Suponha que Ç eGI(q) e Ç gGF(q) e ainda que ord(Ç) não divide 8ik. Nestas condições,

$sen_k(2i) * -1$ e coSk(2 i) * 0.

Demonstração :

i) Pela definição 4.4 tem-se que

$$cosk(Za^{i}) = a^{-k} + a^{*ik}).$$

Suponha, por contradição, que cosk (Za^{i}) = 0, com a eGF(q). Desta forma, $a^{ik} + a^{*ik} = 0$, ou seja, $a^{2ik} = -1$, ou ainda, $(a^{ik})^2 = -1$, o que é um absurdo, pois oc^{ik} eGF(q), que é um corpo no qual a equação $x^2 + 1 = 0$ não tem solução.

ii) Pelo item (iii) da propriedade C1, fazendo-se i = j tem-se $[cask(i)]^2 = 1 + senk(2i)$. Contudo, pelo item (ii) da propriedade C6, tem-se que $cas_k(i) * 0$ e, como GI(q) é um corpo, então [caSk(i)]^2 * 0 e assim senk(2i

Por outro lado, como foi mostrado na propriedade C3, $[cask(i)]^{q+1} = coSk(2i)$. Observando-se o item (i) da propriedade C6 e o fato de que GI(q) é um corpo, então $[cask(i)]^{q+1} * 0$ e assim coSk(2 i) * 0. •

C8 Relações de Conjugação

Seja a função caSk(ZÇ'), cujo argumento Ç = a eGF(q). Nestas condições,

i) $cas_k(i) = [sec_k(2i) + tg_k(2i)][cas_k(i)]^{A}$.

ii) $[caSk(i)]^2 + [cas_k(i)]^{2A} = 2$.

Demonstração :

i) Pela propriedade C3, tem-se que $[cask(i)]^{q+1} = coSk(2i)$ e, como foi mostrado em C7, $[cask(i)]^2 = 1 + senk(2i)$. Logo $[cask(i)]^{q} = \frac{COS(A1)}{1 + sen_k(2i)}$, donde pode-se concluir que

$$cas_k(i) = \left(\frac{1 + sen_k(2i)}{cos_k(2i)}\right) [cas_k(i)]^q.$$

Observando-se a proposição 4.2, item (ii), o resultado segue.

ii) Como foi visto no item anterior, $[cas_k(i)]^2 = 1 + sen_k(2i)$. Desde que Ç = a eGF(q) tem-se $[cas_k(i)]^{2A} = 1 - sen_k(2i)$, o que demonstra o resultado. •

O teorema a seguir é o resultado mais importante desta seção. Com efeito, o próximo teorema estabelece a ortogonalidade da função $cas_k(.)$ e torna possível a definição da Transformada de Hartley em um Corpo Finito.

Teorema **4.1.** $\sum_{k=0}^{JIzJ} cas^ZÇ^cas^ZÇ') = \begin{cases} \N, & [= l \\ [0, & i * t \end{cases}$, onde a ordem de Ç é N.

Demonstração : Pela propriedade C1, item (iii), segue-se que

$$\sum_{k=0}^{N-1} [cas_k(ZOcas_k(ZÇ^1)] = \sum_{k=0}^{N-1} [cos_k(i-1) + sen_k(i+t)].$$

Então, pela propriedade PIO, tem-se que

$$X_{k=0} [caSk(ZC)caSk(ZC)] = £_{k-0} [cos_k(i-1)],$$

e da propriedade P9 o resultado segue. •

4.3 A Transformada de Hartley em um Corpo Finito

Esta seção introduz uma nova transformada em corpos finitos, que possui propriedades semelhantes as da Transformada Discreta de Hartley, descrita na seção 3.2. 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 $GI(q^m)$.

4.3.1 Definição da Transformada

Definição **4.6.** Seja v = (vo , V| , ... , VN-I) um vetor de comprimento N e componentes em GF(q), onde $q = p^r$, com p = 3 mod **(4)** e r um inteiro ímpar. Então o vetor V = (Vo , Vj , ... , VN-I) com componentes em $GI(q^m)$, onde m é um inteiro ímpar, dadas por

$$V_k :=]T \quad Vjcas_k(ZÇ),$$

onde Ç é um elemento de ordem N em GI(q^m), é a Transformada de Hartley de Corpo Finito de v.

Utilizando-se a propriedade de ortogonalidade da função $cas_k(.)$, a THCF pode ser invertida, como é mostrado pelo teorema a seguir.

Teorema 4.2. $\mathbf{Vj} = \frac{1}{N(modp)_k} \overset{N-l}{X} \quad V_k cas_k(ZO.$

Demonstração :

$$\mathbf{Vi} = \frac{1}{N(modp)} \overset{N-l}{X}_{k=0} \overset{N-l}{X}_{r=0} v_r cas_k(ZC) cas_k(ZC),$$

invertendo a ordem dos somatórios, tem-se

$$\mathbf{Vi} = \frac{1}{N(modp)} \overset{N-l}{X}_{r=0} v_r \pounds_{k=0}^{N-l} cas_k(ZC) cas_k(ZÓ,$$

que, pelo teorema 4.1, é o mesmo que

$$\mathbf{Vj} = \frac{1}{N(modp)} \begin{cases} N-l & N, \quad i = r' \\ f^{\wedge} & 0, \quad i * r \end{cases} = \mathbf{Vi} \qquad \bullet$$

Nota-se então que a THCF é simétrica, isto é, possui o mesmo núcleo tanto na transformação direta quanto na transformação inversa, assim como ocorre com as transformadas de Hartley contínua e discreta. O par transformado definido acima é denotado por v <-» V ou THCF(v)=V.

Exemplo 4.1. Seja Ç = a = 3 , um elemento primitivo de GF(7) c GI(7). As funções $cos_k(.)$ e $sen_k(.)$ assumem os seguintes valores em GI(7)

$cos_k(i)$

	0	**1**	**2**	**3**	**4**	**5**	**(i)**
o	**1**	**1**	**1**	**1**	**1**	**1**	
1	**1**	**4**	**3**	**6**	**3**	**4**	
2	**1**	**3**	**3**	**1**	**3**	**3**	
3	**1**	**6**	**1**	**6**	**1**	**6**	
4	**1**	**3**	**3**	**1**	**3**	**3**	
5	**1**	**4**	**3**	**6**	**3**	**4**	
(k)							

$sen_k(i)$

	0	**1**	**2**	**3**	**4**	**5**	**(i)**
0	**0**	**0**	**0**	**0**	**0**	**0**	
1	**0**	*j*	1	**0**			
2	**0**	*i*		**0**	j		
3	**0**	**0**	**0**	**0**	**0**	**0**	
4	**0**			**0**		*j*	
5	**0**	<?	4	**0**	1		
(k)							

Tabela 4.1 - funções k-trigonométricas sobre GI(7).

A seguir tem-se um exemplo de um par transformado:

v = (1, 6, 0, 2, **4,** 3) <-> V = (2, 5+6j, 0, 1, 0, 5+j).

Exemplo **4.2.** Seja Ç = a^{198} um elemento de ordem 11 de GF(3^5), gerado por 7i(x) = x^5 + x^4 + x^2 + 1 como descrito no apêndice 2 (tabela **A4),** onde a é um elemento primitivo de GF(3^5). **A** função $cos_k(l)$ assume os seguintes valores em GI(3^5):

k	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Cos_k(**1**)	**1**	a^{32}	a^{46}	a^{96}	a^{172}	a^{138}	a^{138}	a^{172}	a^{96}	$a^{4"}$	a^{32}

Tabela 4.2 - cos_k(ZQ sobre GI(3^5), onde ord(Ç) = 11

Com apenas estes cossenos listados acima pode-se determinar cos_k(i), com i,k = 0, 1 , 1 0 .

A seguir tem-se um exemplo de um par transformado:

v = (0, 1, 0, 2, 0, 0, 0, 0, 1, 0, 2) <-> V = (0, ja^{171}, ja^{208}, ja^{29}, ja^{57}, ja^{19}, ja^{140}, ja^{178}, ja^{150}, ja^{87}, ja^{50}).

Exemplo **4.3.** Seja Ç = j , um elemento de ordem **4** de GI(3). As funções cos_k(.) e sen_k(.) assumem os seguintes valores em GI(3)

cos_k (i)

(k) \ (i)	**0**	**1**	**2**	**3**
0	**1**	**1**	**1**	**1**
1	**1**	**0**	**2**	**0**
2	**1**	**2**	**1**	**2**
3	**1**	**0**	**2**	**0**

sen_k (i)

(k) \ (i)	**0**	**1**	**2**	**3**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**0**	**2**
2	**0**	**0**	**0**	**0**
3	**0**	**2**	**0**	**1**

Tabela **4.3** - funções k-trigonométricas sobre **GI(3).**

A seguir tem-se um exemplo de um par transformado:

v = (l,0, 2, 1)**V-(1, 1,2, 0).

4.3.2 Representação Matricial

Transformadas discretas são comumente representadas de uma forma mais compacta na notação matricial. Sendo T a matriz que representa a THCF tem-se então, na forma vetorial,

V = Tv,

onde a matriz T é dada por

$$T = \begin{matrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \text{casi}(1) & \text{caS}\vert(2) & \text{cas,}(N\text{-}1) \\ \mathbf{1} & \text{cas}_2(1) & \text{cas}_2(2) & \text{cas}_2(N\text{-}1) \\ \mathbf{1} & \text{cas}_N.\vert(1) & \text{cas}_N.\vert(2) & \text{cas}_N.\vert(N\text{-}1) \end{matrix}$$

- NxN

Com a finalidade de ressaltar as simetrias da THCF, é mais natural trabalhar-se com a matriz T' definida a seguir:

$$\begin{matrix} \text{casi}(1) & \text{casi}(2) & \text{casj}(N\text{-}1) \\ \text{cas2}(1) & \text{cas2}(2) & \text{cas}_2(N\text{-}1) \\ \\ \text{cas}_N.\text{i}(1) & \text{cas}_N.\text{i}(2) & \mathbf{casN\text{-}i}(N\text{-}1) \end{matrix}$$

-(N-l)x(N-l)

ou seja, define-se a matriz T' retirando-se a primeira linha e a primeira coluna da matriz T. Utilizando-se as propriedades de simetria das funções senk(.) e coSk(.) pode-se concluir que:

- De acordo com a propriedade P6, T é uma matriz simétrica; em particular, T' também é uma matriz simétrica.

- Pela propriedade P7, T' também é simétrica com relação a diagonal secundária.

Devido às simetrias descritas acima e à propriedade P8, conclui-se que toda a informação necessária para determinar T' está contida numa pequena quantidade de elementos desta matriz. Admitindo-se que a matriz T' é ilustrada por um quadrado, então os únicos elementos necessários para determinar T' estão contidos no triângulo sombreado abaixo:

V =

Figura 4.1 - Simetria da THCF.

Em seguida são demonstradas algumas propriedades da THCF.

4.3.3 Propriedades

Sejam g <-» G e h <-> H pares transformados de comprimento N.

Hl Linearidade

Sejam a,beGF(q); então ah + bg <-> aH + bG.

Demonstração :

$$THCF\{ahi + b_{gi}\} = \sum_{i=0}^{N-1}(ah, + b_{gi}\}cas_k(ZÇ') =$$

$$= a]T\ h_{ic}as_k(ZÇ') + bX_{gi}\ cas_k(ZO = aH_k + bG_k$$

H2 Deslocamento no Tempo

Suponha que hj = gj.i; então $H_k = cos_k(I)G_k + sen_k(I)G._k$.

Demonstração :

$H_k = THCF\{gj.|\} = \sum_{i=0}^{N-i} g,.icas_k(i)$ fazendo i-I = r tem-se $H_k = \sum_{r=0}^{N-1} g_r cas_k(r+I)$.

Contudo, pela propriedade C l, item (i), tem-se

$$Hk = \sum_{r=0}^{N-1} \&\bullet\{^{cos}k(^{1})^{cas}k(^{'}) + ^{sen}k(I)cas_k(-r)\} = cos_k(I)G_k + sen_k(I)G._k.$$

H3 Soma da Seqüência

$$H_0 = \sum_{i=0}^{N-1} h,.$$

Demonstração : Diretamente da definição **4.6.**

•

H4 Valor Inicial

$$h_0 = \frac{j}{N(mod\,p)S} \sum^{N-1} H_k.$$

Demonstração : Diretamente do teorema **4.2.**

H5 Simetria

H <-> Nh.

Demonstração : Denotando a THCF{H} por *H,* tem-se

$$H_k = \sum_{tí}^{N-1} Hj\,cas_k(i); \quad \text{contudo} \quad hj = \frac{I}{N(mod\,p)S} \sum^{N-1} H_k\,cas_k(i),$$

conclui-se então que *Hy,* = Nh_k.

H6 Reversão Temporal

h.j <-> H.$_k$.

Demonstração: THCF {h.j} = V ÍLjcas$_k$(ZÔ = $\underset{Z\sim\backslash}{X}$ ^{h}*cas^ZÇ^1),

mas {hj} e cas$_k$(i) tem período N, logo THCF {h.j} = $\underset{i\ o}{\overset{N-l}{X}}$ hjcas.$_k$(ZÇ') = H.$_k$.

H7 Convolução Cíclica

g*h <-> *Vz* (GH + GH. + G.H - G.H.).

Demonstração : A i-ésima componente da convolução cíclica é

$(g*h)i = \overset{N-\backslash}{X}$ grhj.$_r$, assim

THCF{(g*h)j} = $\overset{N-l}{\underset{=0}{\hat{}}}$ $\overset{N-l}{\underset{r»0}{^Z}}$[g$_r$ hj.$_r$]cas$_k$(i), trocando as ordens dos somatórios tem-se

$= \underset{r»0}{\overset{A\ M}{X}}$ g r $\underset{i\ d}{\overset{N-l_i}{X}}$ h,.$_r$cas$_k$(i), que pela propriedade H2 é o mesmo que

$= \overset{/V-l}{X}$ gr [cos$_k$ (r) H$_k$ + sen$_k$ (r) H.$_k$], ou ainda,

$= \underset{r-0}{X}$ gr {'/2[cas$_k$(r) + cas$_k$(-r)] H$_k$ + !/$_2$[cas$_k$(r) - cas$_k$(-r)] H.$_k$} =

= »/$_2$(G$_k$H$_k$ + G.$_k$H$_k$ + G$_k$H.$_k$ - G-kH-k). •

H8 Relação de Parseval

$N\underset{i-0}{\overset{N-l}{£}} h,^2 = \underset{k-0}{\overset{N-l}{X}} H_k^{\ 2}$.

Demonstração : $V\ Hk = \underset{k-0}{\overset{N-l}{X}}\ \underset{j=0}{\overset{J\wedge J}{X}}$ $^{caSk\wedge'}$)1 ' invertendo-se os somatórios tem-se

$\underset{k\ 1)}{\overset{N-l}{\ }}$ $\underset{k-0}{\overset{N-l}{\ }}$ $\underset{j=0}{\overset{N\wedge J}{\ }}$

$H_k = \underset{k-0}{\overset{N-l}{X}}\ h'\ \underset{k-0}{\overset{N-l}{X}}$ ^{caSk}(') ^{caSk}(') ^{e} P$^{e'}$$^{o\ teorema}$ 4.1,

$\underset{k-0}{\overset{N-l}{\ }}$ $\underset{j=o}{\overset{,}{\ }}$ $\underset{k-0}{\overset{N-l}{\ }}$

$\overset{N-l}{X}$ H$_k^{\ 2}$ = NX hj^2. •

Exemplo 4.4. Os seguintes pares transformados foram calculados utilizando-se o Programa 4, descrito no apêndice 2. Neste exemplo algumas das propriedades listadas acima foram exemplificadas. Seja Ç = 3, um elemento primitivo de GF(7), assim como descrito no exemplo 4.1. Tem-se então,

Propriedade H2:

g = (1, 1, 2, 4, 0, 3) <-> G = (4, 5, 2+3j, 2, 2+4j, 5),

fazendo-se I = 3 obtém-se

h = (4, 0, 3, 1, 1, 2) <-> H = (4, 2, 2+3j, 5, 2+4j, 2).

Propriedade H6:

g = (1, 2, 3, 4, 5, 6) G = (0, 4+j, 4+5j, 4, 4+2j, 4+6j),

efetuando-se a reversão temporal, tem-se

h = (1, 6, 5, 4, 3, 2) <-> H = (0, 4+6j, 4+2j, 4, 4+5j, 4+j).

4.3.4 Relações entre a TFCF e a THCF

Seja v = (v_0, vi , ... , VN-I) um vetor de comprimento N e componentes em GF(q), onde q = p^r . Sua TFCF será denotada pelo vetor F = (F_0, Fi , ..., F_{N-i}), de comprimento N e componentes em GF(q^2) = GI(q) como na definição 3.1, com m=2.

$$\sum_{i=0}^{N-1}$$

onde Ç é um elemento de ordem N em GF(q^2).

Seja H a THCF do vetor v, com núcleo cas(ZÇ'), ^ e v como acima definidos. Então

i) $H_k = i[(F_k + F_{i\,v\,k}) + j(F_{N-k} - F_k)]$.

Demonstração :

$F_{N-k} = \sum_{i=0} v\,\hat{}\,-"* = \sum_{i=0} v, Ç^{ki}$ assim,

$\frac{1}{2}(F_k + FN-]C) = \cos_k(Z\,Ç)$ e $\frac{1}{2}j(F_{N-k} - F_k) = \frac{\hat{}}{2j}(F_k - F_{N-k}) = \text{sen}_k(Z\,Ç)$. LI

ii) $F_k = |[(H_k + H_{N-k}) - r - j(H_k - H_{N-k})]$.

—

Demonstração :

De (i) tem-se que HN-I< $= \frac{1}{2}[(F_k + F_{N-k}) + j(F_k - F_{N-k})]$. Assim,

$H_k + H_{N-k} = F_k + F_{N-k}$ e $H_k - H_{N-k} = j(F_{N-k} - F_k)$. •

Definição 4.7. A seqüência G = {G_k}, de comprimento N, é dita ser ímpar se G_k = **-GN-$_k$.** Por outro lado, se G_k = GN-I< então G é dita ser par.

Definição 4.8. Um Inteiro Gaussiano ÇeGI(q) é real se Ç = cteGF(q). Do mesmo modo, se Ç = jp com PeGF(q) então Ç é dito ser imaginário puro.

Observando-se as relações (i) e (ii) entre a TFCF e a THCF e supondo que Ç (núcleo da transformada) é um elemento real, pode-se concluir que

iii) F é par o H é real e par.

Demonstração : Se F é par, tem-se F_k = FN-I<; então H = F (em particular, H possui apenas componentes reais). Por outro lado, se H é real e par, então H = F. •

iv) F é impar < : 11 é imaginário puro.

Demonstração : Se F é impar tem-se F_k = -FN-I< então H = jF. Por outro lado, se H é imaginário puro, então (F_k + FN-IC) = 0. Logo H = jF. •

Em geral, tem-se VjeGF(q), F_keGF(q^2) e H_keGI(q)=GF(q^2). No exemplo abaixo, tem-se $q=3^3$, contudo **V**JGGF(3), F_keGF(3^3) e H_keGI(3^3)=GF(3^6), pois o núcleo da transformada é dado porÇ = PeGF(3^3).

Exemplo 4.5. Seja GF(27) o corpo gerado pelo polinómio 7i(x) = $x^3 + 2x + 1$, descrito no apêndice 2 (tabela A3). Seja a um elemento primitivo de GF(27) e p = $2x^2 + 2x = a^6$ um elemento de ordem 13 deste corpo. Desta forma, dado o vetor

v = (1,0, 1, 1,0, 1,0, 0, 0, 0, 0, 0,0),

tem-se sua Transformada de Fourier em um Corpo Finito

F = ($1, a^{21}, a^9, a^{11}, a^{23}, a^3, a, a^3, a^9, a^7, a^{25}, a, a^{17}$),

e sua Transformada de Hartley em um Corpo Finito

H = ($1, a^{16} + ja, a^7 + ja^{23}, a^{22} + ja^3, a^{14} + ja^{22}, a^{11} + ja^{25}, a^{21} + ja^{11}, a^{21} + ja^4, a^{11} + ja^{12},$

$a^{14} + ja^{17}, a^{22} + ja^{16}, a^7 + ja^{10}, a^{16} + ja^{14}$).

Exemplo 4.6. Seja Ç = a^{198}, um elemento de ordem 11 de GF(3^5), assim como descrito no exemplo 4.2. Seja v = (0, 1,0, 2, 0, 0, 0, 0, 1, 0, 2), sua THCF foi determinada no exemplo 4.2 como sendo um vetor imaginário puro. Calculando-se a TFCF do vetor v, tem-se

r - (u, a , a , a ,ot , a , et , et , a , a , ct).

Como em GF(3^5) a^{121} = - 1, comprova-se que F é ímpar.

Exemplo 4.7 Neste exemplo serão calculados as transformadas das palavras de um código BCH ternário, gerado pelo polinómio p(x) = x^2 + x + 2. Seja Ç = 1+j, um elemento primitivo de GI(3), as transformadas dos vetores v = (v_0, V j , $v_{(}$, V7) do código são representadas pelos vetores H = (Ho, Hj , H_6, H7), descritos a seguir.

$\mathbf{v}_0$	**vi**	$\mathbf{v}_2$	$\mathbf{v}_3$	$\mathbf{v}_4$	$\mathbf{v}_5$	$\mathbf{v}_6$	$\mathbf{v}_7$
0	0	0	0	0	0	0	0
2	1	0	1	1	2	0	2
2	2	1	0	1	1	2	0
0	2	2	1	0	1	1	2
2	0	2	2	1	0	1	1
1	2	0	2	2	1	0	1
1	1	2	0	2	2	1	0
0	1	1	2	0	2	2	1
1	0	1	1	2	0	2	2

Tabela 4.4 - **Vetores do código BCH**

Hp	**H,**	**H_2**	**H_3**	**H_4**	**H_5**	**H_6**	**H_7**
0	0	0	0	0	0	0	0
0	1 + j2	0	1 + j2	0	1 + j	0	1 + j
0	2	0	j	0	2	0	j2
0	2 + j2	0	1 + j	0	2 + j	0	1 + j2
0	j	0	2	0	j2	0	2
0	2 + j	0	2 + j	0	2 + j2	0	2 + j2
0	1	0	j2	0	1	0	j
0	1 + j	0	2 + j2	0	1 + j2	0	2 + j
0	j2	0	1	0	j	0	1

Tabela 4.5 - **Transformada de Hartley dos vetores v**

De fato, GI(3) é gerado pelo polinómio $q(x) = x^2 + 1$, que não é primitivo sobre GF(3), pois j tem ordem 4. Contudo, (1 + j) é um elemento primitivo de GI(3) e desta forma pode-se construir um isomorfismo entre GI(3) e GF(9). Tal isomorfismo entre GI(3) e GF(9) é descrito pelo mapeamento a seguir.

1 + j	->	a
J2	—>	a^2
1 + J2	->	a^3
2	->	4 (/.
2 + J2	- >	a^5
j	->	a"
2 + j	—>	a'
1	>	a*

Tabela 4.6 - **GI(3) = GF(9)**

Ainda neste exemplo, é interessante calcular a Transformada de Fourier em um Corpo Finito dos mesmos vetores que compõem o código BCH descrito acima, já que esta transformada é utilizada em alguns algoritmos de decodificação de tais códigos. Utilizando-se a, um elemento primitivo de GF(9) gerado pelo polinómio $TC(X) = x^2 + x + 2$, tem-se os seguintes vetores transformados:

Fo	Fi	F_2	Fi	F_4	F_5	F_6	F_7
0	0	**0**	0	**0**	0	**0**	0
0	2		2	**0**	0	**0**	0
0	a^5		o 7		0	**0**	0
0	a^6		a^2		0	**0**	0
0	a^7		a^5		0	**0**	0
0	1		1	**0**	0	**0**	0
0	a		a)		0	**0**	0
0	a^2		a^6		0	**0**	0
0	a^3		a	**0**	0	**0**	0

Tabela 4.7 - **Transformada de Fourier dos vetores v**

Desta forma, pode-se inclusive verificar as relações entre a THCF e a TFCF utilizando-se o mapeamento descrito pela tabela 4.6. Tome como exemplo a THCF do vetor v = (0, 2, 2, 1, 0, 1, 1,2), tem-se então

$$H = (0,2+j2, 0, 1 +j,0,2+j,0, 1 +J2).$$

De acordo com a seção 4.3.4 pode-se calcular as componentes da TFCF do mesmo vetor v como se segue:

Fo = 0

F, = i[(2 +J2) + (1 +J2)] +jl[(2 +J2) - (1 +j2)] =j2 +j2 =j = a^6

$F_2 = I_{[0+}$ o] +ji[0-0] = 0

F3 - +j) + (2+j)] +j|[(l +j) - (2 +j)] =j +j =j2 = a^2

F_4 = i[0 + 0] +ji[0-0] = 0

F_5 = |[(2 +j) + (1 +j)] +j|[(2 +j) - (1 +j)] -j +j2 = 0

F_6 = $I_{[0+}$ 0] +ji[0-0] = 0

F_7 = +j2) + (2 +J2)] +j2) - (2 +J2)] =j2 +j = 0 .

4.3.5 Algoritmo Rápido

De acordo com o item (i) da seção 4.3.4 tem-se que

$$V_k = \wedge[(F_k + F_{N-k})+j(F_{N-k}-F_k)],$$

o que possibilita o cálculo da k-ésima componente do vetor v transformado pela THCF a partir da combinação de duas componentes da TFCF do mesmo vetor v . Pode-se utilizar então as FFTs descritas no capítulo 3 para compor um algoritmo eficiente destinado ao cálculo da THCF, conforme indicado no diagrama a seguir.

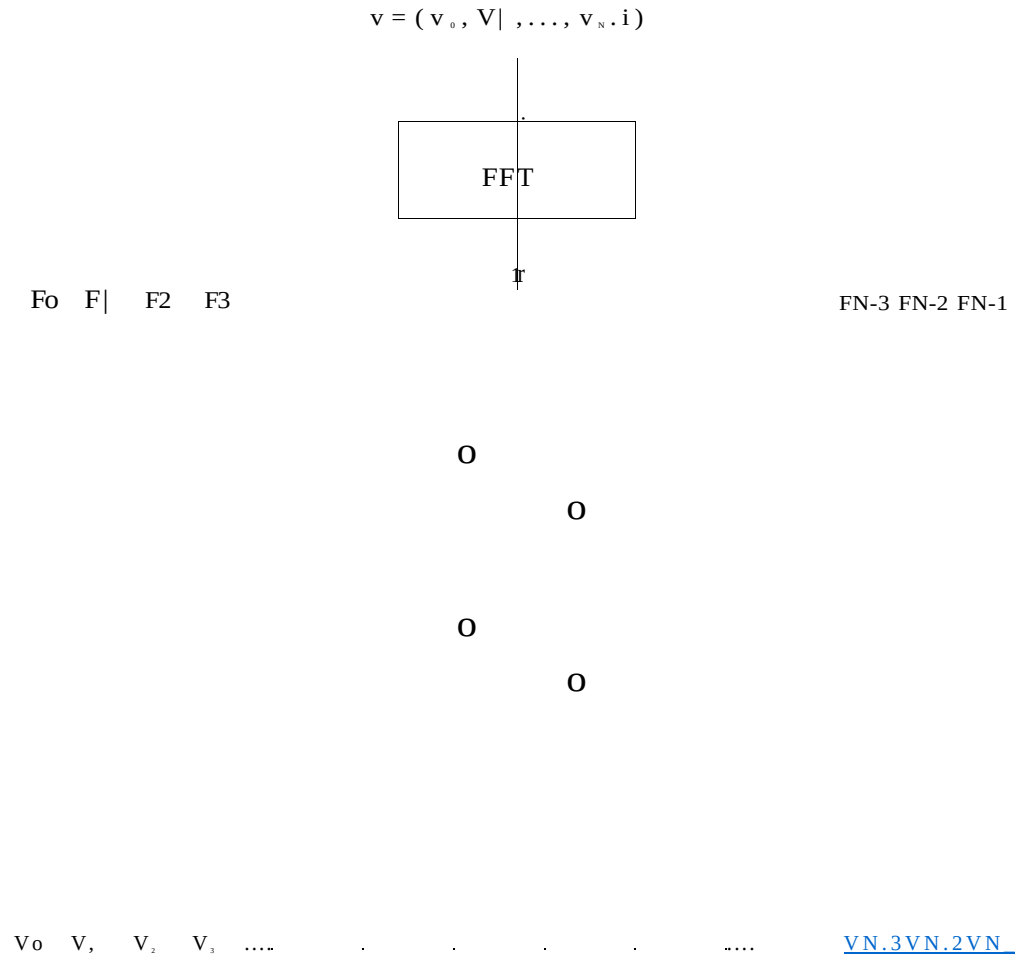


Figura 4.2 - Implementação do Algoritmo Rápido para a THCF

No esquema acima, o símbolo Q efetua a adição em GF(q) e o símbolo realiza a multiplicação por (-1) em GF(q).

De fato, a complexidade computacional deste algoritmo será determinada pela complexidade da FFT utilizada, adicionando-se o cálculo necessário para a combinar as componentes da TFCF. Observando-se que Vo = Fo, tem-se então que o fator de acréscimo para a complexidade é dada por 2(N-1), onde N é o comprimento da transformada. Desta forma a eficiência do algoritmo permanece praticamente inalterada.

Como foi visto no capítulo 3, obtém-se uma maior eficiência computacional utilizando-se transformadas de comprimento potência de 2. Contudo, a THCF possui restrições com relação ao seu comprimento, já que este deve dividir a ordem de GI(q). A seguir são utilizados primos de Mersenne para a construção de corpos nos quais podem ser obtidas transformadas com comprimentos da forma 2^a. Os primos de Mersenne (como exemplificados no apêndice 2) são da forma $p = 2^s - 1$, portanto, para $s > 2$ temos $p \bullet 4(2^{s*2}) - 1 = 3 \bmod (4)$. Assim, podemos utilizar os primos de Mersenne como característica de GF(q), onde $q = p^r$ e r é um inteiro ímpar.

Sabe-se que N, o comprimento da THCF deve dividir ord(Q, que por sua vez divide $(q^2 - 1)$, a ordem de GI(q). Contudo,

$$q^2 = [(2^s - 1)^r]^2 = (2^s - 1)^{2r} = \sum_{n=0}^{2r} (-1)^n \binom{2r}{n} "(2^*)^{2r-n} =$$

$$= 2^{2rs} \binom{2r}{is(2r-1)} + \ldots + \binom{2r}{2r-2} 2^{2s} - (2r)2^s + 1.$$

Com r>1 e s>1, pode-se fatorar q - 1 na forma

$$ot\ -1 \equiv 2^{s+1+(2r-1)s-1} \left[\binom{2r}{s(2r-2) - 1} + \ldots + \binom{2r}{2r-2} 2^{s"'1} - r \right]$$

ou seja, N pode ser uma potência de 2, $N = 2^d$, onde $d < s+1$.

Uma observação importante é que para a transformada ter um comprimento da forma 2^d com d>1, o elemento Ç, que é o núcleo da TFCF e que compõe o núcleo da THCF (cas(ZÇ')), pertence a GI(q) e obrigatoriamente ÇéGF(q). Isto ocorre pois o expoente e do binômio $(2^s - 1)^e$ deve ser par e assim o termo independente de s no desenvolvimento do binômio é (+1), o que possibilita a fatoração desejada.

4.3.6 Espectros Válidos

O espaço vetorial $\{GI(q)\}^N$ possui q^{2N} elementos, mas nem todos são a imagem de algum vetor de $\{GF(q)\}^N$. Desde que o núcleo da THCF tenha, no argumento da função cask(.), um elemento de GF(q), tem-se uma condição necessária e suficiente para que um vetor de $\{GI(q)\}^N$ seja a imagem de algum vetor de $\{GF(q)\}^N$.

Proposição **4.6.** Suponha uma THCF, cujo núcleo cas(ZÇ') utiliza como argumento da função cas(.) o elemento Ç = a eGF(q). O vetor $V = \{V_k\}$, V_k eGI(q), é o espectro de um sinal $v = \{VJ\}$, **Vj** GGF(q), $q = p^r$, se e somente se

$$V^q_{\text{`}k} = V_{\text{`}N-kq>}$$

onde os índices são considerados módulo N, i, k = 0, 1 , N - l e N | (q - 1).

Demonstração : Da definição da THCF e considerando que a e j são elementos de GI(q), ou seja, otj eGF($p^{2'}$) que tem característica p, segue-se pelo teorema 2.15 que

$$\text{`}XviCasJZa^{i}) = £v'casj(Za^{j})],$$

contudo,

$$\mathbf{casj} = \frac{1}{2}[(a^{ik} + a^{iik}) + -i(a^{ik} - a^{ik})]^q,$$

O fato de que $j^2 = -1$ g GF(q) se e somente se q é uma potência de um primo da forma 4k+3, implica que $j^q = -j$. Dessa forma, novamente pelo teorema 2.15, tem-se

$$cas^q_k = \frac{-(ot^{ikq} + a^{ikq})}{2} - \frac{(a^{ikq} - a'^{ikq})}{2j} = cos._{kq}(i) + sen._{kq}(i) - cas._{kq}(i).$$

Se **Vj** G GF(q) V i, então $\mathbf{Vj^q = Vj}$ e pode-se escrever,

$$\mathbf{V_k^q = X v_j cas_{N\cdot qk}(Z a^i) = V_{N\cdot qk}}$$

Por outro lado, suponha $V^q = V_{N-qk}$. Então

$$\mathbf{Z\ v^i\ cas_{N-qk}(Z a^i) = Z\ v^i Cas_{N\cdot qk}(Z a^i)}$$

Agora, seja N-qk = r. Desde que mdc(q-l, q) = 1, k e r variam sobre os mesmos valores, o que implica

$$\mathbf{Z\ v^q cas_r(Z a^i) = Z\ Vj Cas_j(Z a^i),}$$

r = 0, 1, N-l. Pela unicidade da THCF, $v^q = \mathbf{Vj}$, logo VjeGF(q) e a demonstração está completa. •

Definição 4.9. De acordo com a proposição 4.6, definem-se classes ciclotômicas para a THCF do vetor v, com VjeGF(q), $q = p^r$, obtidas pela partição do conjunto de inteiros k, através pela relação

$$-kq \bmod (N)$$

onde k e {0,1,..., N-l} e N divide q-1.

Uma extensa lista de classes ciclotômicas para a THCF é apresentada no apêndice 2.

Exemplo 4.8. Seja $GF(3^5)$ o corpo gerado pelo polinómio $7i(x) = x^5 + x^4 + x^2 + 1$, como descrito no apêndice 2. Seja a um elemento primitivo de $GF(3^5)$ e $p = x^2 + x + 1 = a'^{88}$ um elemento de ordem 11 deste corpo. Desta forma, o vetor descrito abaixo

$$v = (0,\ 1,2,\ 1,\ 1,0,\ 0,\ 0,\ 2,1,1)$$

tem como transformada o vetor

$$V = (\ 0,\ a^{215} + ja^{46},\ a^{24'} + ja^{5'},\ a^{161} + ja'^{38},\ a^{2''} + ja''^{6},\ a^{23''} + ja^{32},\ a^{239} + ja'^{53},\ a^{233} + ja^{2''},$$

$$a^{161} + ja^{17},\ a^{24\cdot} + ja^{\cdot 72},\ a^{215} + ja^{1<'17}).$$

Como descrito no apêndice 2, este exemplo possui apenas duas classes ciclotômicas

Co = (0).
C, = (1,8,9,6,4, 10,3,2,5,7),
ou seja, toda a informação do vetor V está contida em Vo e Vj. De fato, observando-se a tabela de GF(3") descrita no apêndice 2, tem-se que

$$(V,)^3 = (a^{215} + ja^{46})^3 = a^{645} - ja^{138} = a^{161} + 2ja^{138} = a'''' + j(a^4 + 2a^3 + 2a^2 + 2a + 1) =$$

$$= a'''' + ja^{17} = V_8.$$

$$(V_8)^3 = (a'^{6'} + ja^{17})^3 = a^{241} + 2ja^{51} = a^{241} + j(a^4 + 2a^3 + a^2) = a^{241} + ja^{172} = V_9.$$

Capítulo 5

Um Novo Sistema de Multiplexação Digital

Neste capítulo um novo sistema de multiplexação por divisão em códigos é apresentado. Este sistema é baseado em transformadas sobre corpos finitos, o que resulta em um ganho de eficiência espectral com relação aos sistemas convencionais de multiplexação TDM, FDM e até mesmo com relação ao CDM. Será mostrado que, dentre as transformadas de corpos finitos, a que apresenta o melhor fator de compactação de banda passante é a Transformada de Hartley em um Corpo Finito, já que esta possui maior redundância. Neste sistema, usuários com mensagens sobre um corpo finito GF(p) são multiplexados, considerando como domínio o espectro do sinal sobre um corpo de extensão $GF(p^m)$, resultante de uma transformação pela THCF. Devido a redundância presente no vetor transformado, não é necessário a transmissão de todo o sinal multiplexado, mas apenas dos líderes das classes ciclotômicas. Como conseqüência, a multiplexação de N sinais de largura B resulta num sinal com requisitos de banda substancialmente inferior a NB, o que não ocorre nos sistemas TDM e FDM.

5.1 Multiplexação Analógica (FDM)

Suponha que haja a necessidade de se enviar simultaneamente em um dado meio de transmissão, r sinais, $v'(t)$, $v^2(t)$, $v^r(t)$, cada um deles limitado em faixa em f_m Hz. A multiplexação por divisão em freqüência é realizada através da modulação linear (tipicamente SSB) destes r sinais com subportadoras senoidais em f|, **f2,** f_r , de tal forma que cada subportadora seja separada da subportadora adjacente de, pelo menos, f_m Hz. Desta forma, os r sinais são transmitidos num mesmo intervalo temporal, mas ocupam faixas distintas do espectro de Fourier.

O diagrama de um sistema simplificado de multiplexação FDM é ilustrado a seguir.

v'(t)

Z

v²(t)

0 Transmissão

vʳ(t)

Z_{fr}

Claramente, a banda passante requisitada para a transmissão dos r sinais multiplexados é dada por rB , onde B é a banda passante necessária para a transmissão de um único sinal v'(t).

5.2 Multiplexação Digital

Nesta seção será descrita, de forma bastante breve, a filosofia dos dois sistemas de multiplexação digital utilizados em sistemas comerciais: o TDM *(Time Division Multiplex)* e o CDM *(Code Division Multiplex).* De fato, a multiplexação digital consiste na transmissão de diversos sinais digitais em um mesmo canal, de forma que estes sinais embora misturados em um domínio, estejam separados em outro. Esquematicamente, tem-se

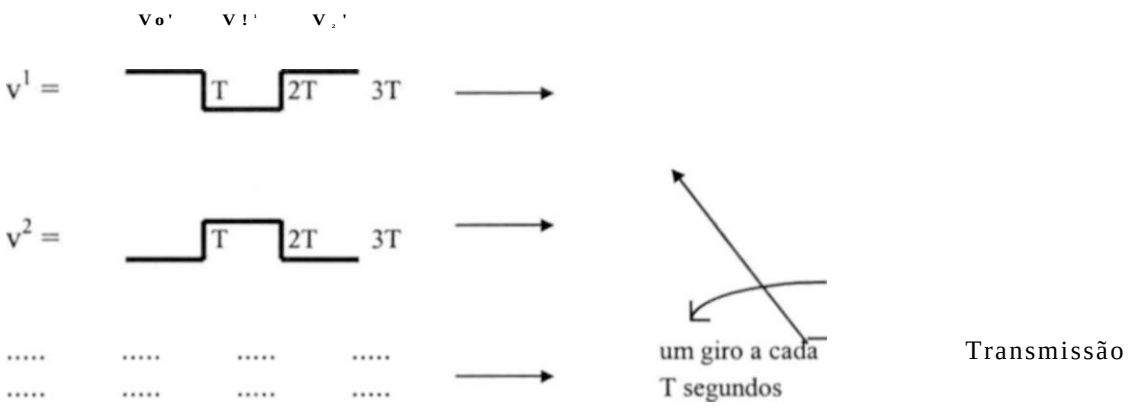
Sinal 1
Sinal 2 MUX DIGITAL Transmissão
Sinal r

Pode-se também multiplexar sinais de natureza analógica (como voz, em telefonia) através de sistemas de multiplexação digital. Neste caso, multiplexação digital é realizada a luz do teorema da amostragem [12], que demonstra ser possível a transmissão de toda a informação de um sinal limitado em faixa, desde que a taxa de amostragem seja superior a $2f_m$ amostras por segundo, onde f_m é a mais alta componente de freqüência do sinal limitado em faixa.

No decorrer desta seção, suponha que dispõe-se de r sinais digitais a serem multiplexados v¹, v², vʳ, onde v' = (v_0', vj', $v_{N'}$-i'), em que cada componente tem duração de T segundos. Caso os sinais sejam analógicos v'(t), v²(t), vʳ(t), então os mesmos serão digitalizados (amostrados de acordo com o teorema da amostragem e então quantizados) e cada amostra do sinal v'(t) será então representada pelo vetor v¹ = (vo\ *V*\\ VN-I'), onde cada componente terá a duração de T segundos.

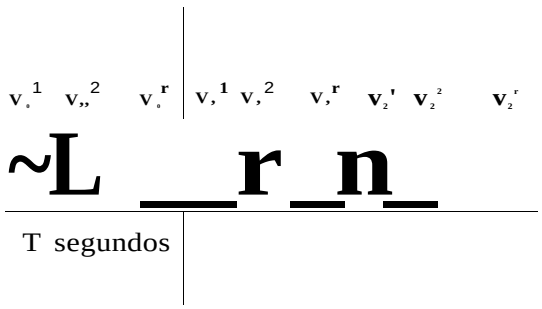
5.2.1 TDM

Na multiplexação por divisão no tempo (MUX de dados síncronos), o transmissor é encarregado do intervalamento dentre os r sinais digitais a serem transmitidos a cada T segundos, como ilustra a figura a seguir.



T 2T 3T

Desta forma, o sinal binário multiplexado (em banda básica) a ser transmitido, correspondente ao exemplo ilustrado acima, é apresentado a seguir.

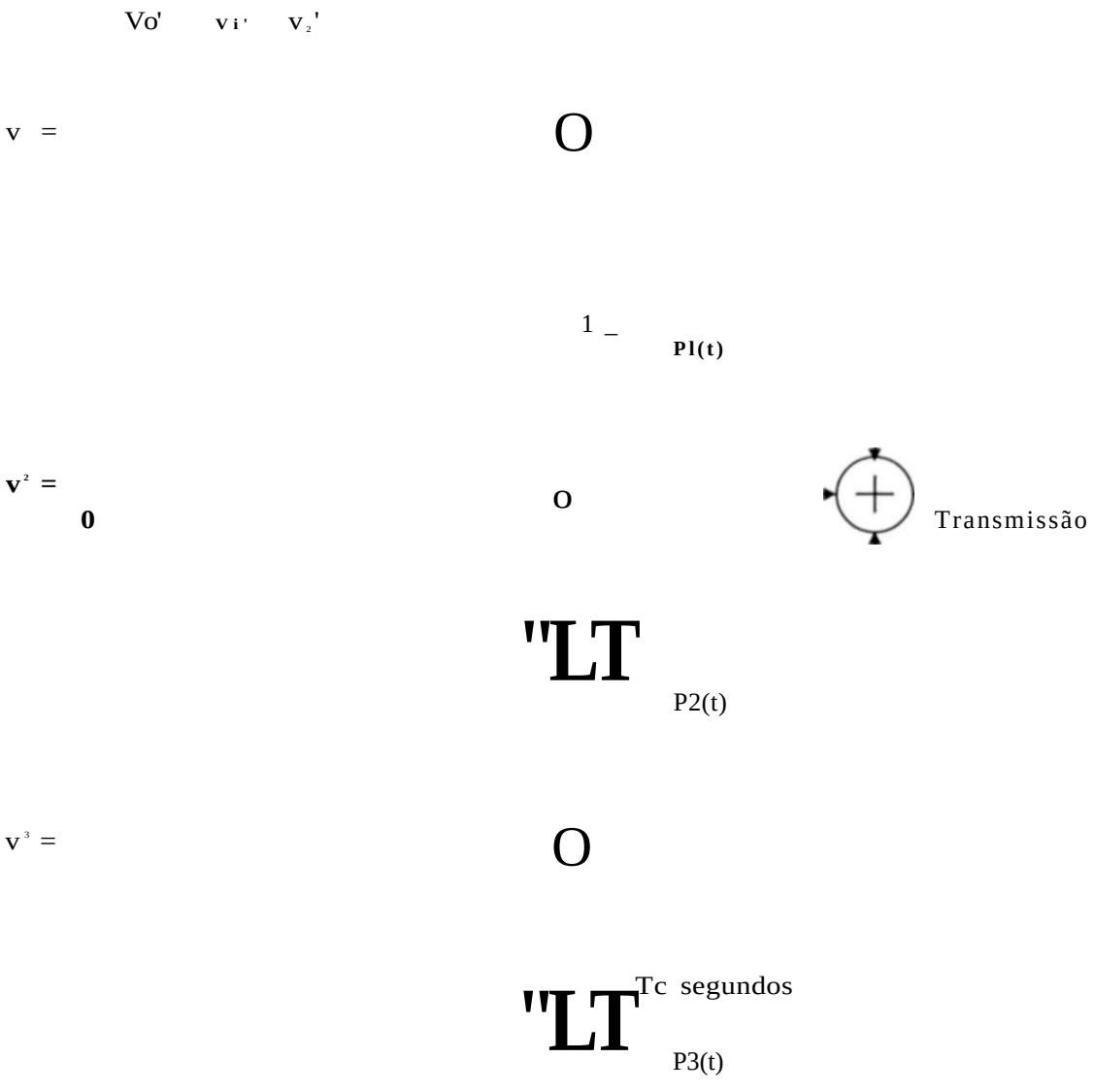


Fica claro então, que o sinal multiplexado adota pulsos de largura T/r segundos. Desta forma, a banda passante necessária para a transmissão dos r sinais síncronos multiplexados por divisão no tempo (TDM) é de rB, onde B é a banda passante necessária para a transmissão de uma única componente de um vetor v'. Este resultado proporciona requisitos de banda idênticos com relação a FDM.

5.2.2 CDM

O sistema CDM é uma técnica baseada no espalhamento espectral, sendo utilizada na transmissão de dados que possuem uma banda passante muito menor que a largura de faixa do canal disponível para a transmissão. O espalhamento é então realizado através de seqüências pseudo aleatórias. Existem várias técnicas diferentes de espalhamento espectral. Contudo, matematicamente, todas as técnicas são baseadas em um mesmo princípio. Do ponto de vista

da implementação, as principais técnicas de espalhamento espectral são: por seqüência direta (DS - *Direct Sequence),* por *Frequency Hopping* (FH), por *Time Hopping* e o híbrido FH/DS. Os sistemas TDM e FDM descritos anteriormente possuem a característica de que cada sinal é alocado em um subcanal individual, isto é, não há sobreposição das amostras temporais ou dos espectros, respectivamente, nestes métodos de multiplexacão. No CDM, cada usuário possui uma assinatura distinta, que é implementada sob a forma de uma seqüência pseudo aleatória, p(t), que o usuário utiliza para realizar o espalhamento espectral [34]. Desta forma, no CDM todos os usuários transmitem ao mesmo tempo e utilizam a mesma faixa de freqüência. O usuário extrai sua mensagem realizando uma correlação do sinal recebido com sua seqüência p(t). Assim, os sinais dos outros usuários serão tratados como um ruído durante a recepção, pois as demais seqüências p,(t) são não correlacionadas ou possuem apenas uma correlação residual com a seqüência p(t) deste usuário. A figura a seguir ilustra este método na multiplexacão de três sinais, onde cada sinal é composto por 3 bits (cada bit ocupa T segundos). Neste exemplo, o espalhamento espectral é realizado através do método de seqüência direta e o símbolo © combina os sinais a serem multiplexados utilizando a lógica de maioria.



No esquema acima, a operação descrita por Q realiza o espalhamento espectral (via seqüência direta) da seguinte forma: cada bit (T_c segundos) da seqüência p,(t) é invertido se no mesmo instante o sinal v^1 vale **1** e nada ocorre com o bit de pj(t) quando o sinal v^1 tem valor 0. A seguir tem-se uma descrição desta operação.

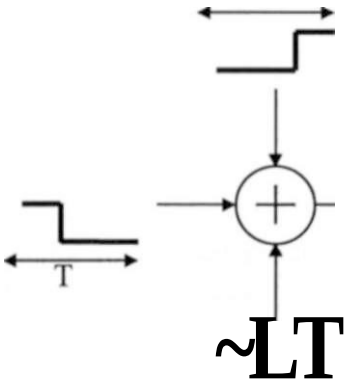
Tomando-se como exemplo o sinal v^3 e sua correspondente seqüência de espalhamento pi(t), obtém-se:

O sinal v"

A seqüência p3(t)

O sinal espalhado, em banda básica ~Lr~L_n_rL

Ainda no esquema anterior, tem-se vo' = **1,** vo^2 = **1,** vo^3 = 0 . Desta forma, durante os primeiros T segundos observa-se o seguinte sinal transmitido:



Tc

Sinal Transmitido

~LT

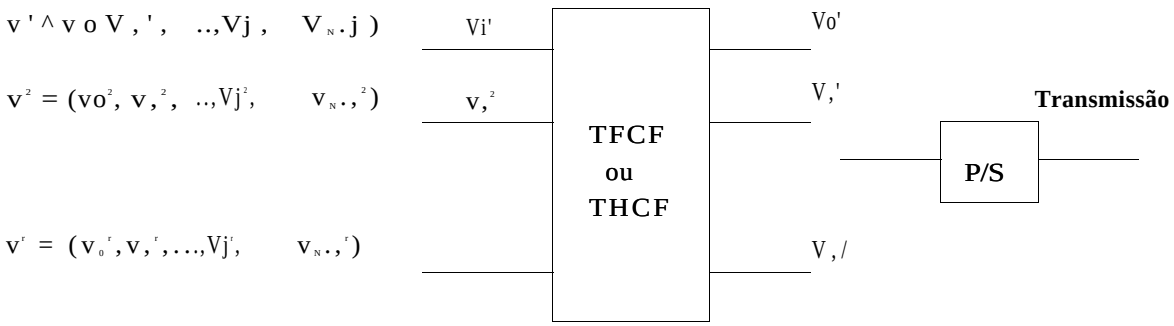
Define-se N = T / T_c. Numa situação em que as seqüências p,(t) fossem descorrelacionadas duas a duas, o número máximo de sinais que poderiam ser multiplexados por este método seria r < N e desta forma a banda passante necessária para a transmissão dos r sinais multiplexados por divisão no código (CDM) seria de rB, onde B é a banda passante necessária para a transmissão de uma única componente de um vetor v^1.

Contudo, visando melhorar a eficiência espectral, normalmente as seqüências pj(t) são projetadas de tal forma que possuem apenas uma correlação residual e desta forma tem-se N > r, o que acarreta um (pequeno) ganho no número de usuários com relação aos sistemas TDM e FDM. Nenhum comentário é feito aqui com relação ao processo de deteção, considerado fora do escopo desta dissertação.

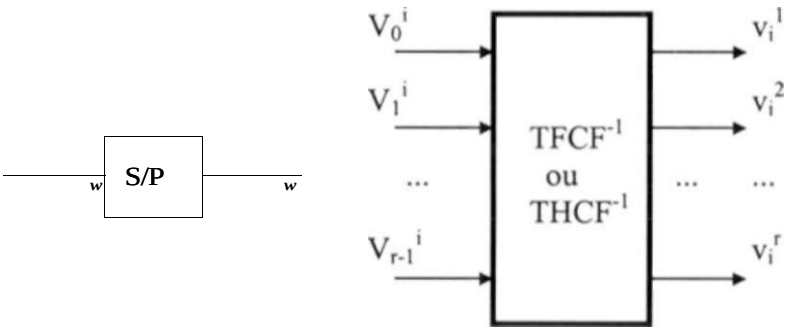
5.3 GDM

Os sistemas de multiplexação anteriormente discutidos incrementam a taxa de transmissão no canal, mas simultaneamente aumentam a banda passante do sinal multiplexado pelo mesmo fator, o que implica na manutenção da eficiência espectral com relação ao sistema de comunicação com um único usuário. No sistema de Multiplexação por Divisão em Campos de Galois (GDM - *Galois Division Multiplexing)* há uma expansão do alfabeto utilizado, o que pode trazer como conseqüência uma diminuição na banda passante do sinal multiplexado. De fato, desde que a relação sinal ruído (SNR) do canal utilizado permita ao receptor discriminar estes níveis acrescentados ao alfabeto, é possível realizar uma "negociação entre banda passante e amplitude" sem que haja uma extrapolação da capacidade do canal.

Sejam v^1, v^2, v^r os r sinais a serem multiplexados, com $v^i = (v_0^i, v_1^i, \ldots, v_{N-1}^i)$, onde cada símbolo $v_j^i \in GF(p)$ tem duração T segundos. Os r sinais podem ser multiplexados utilizando-se transformadas sobre corpos finitos, tais como a Transformada de Fourier em um Corpo Finito e a Transformada de Hartley em um Corpo Finito. Um esquema simplificado deste novo sistema de multiplexação é apresentado a seguir.



Como está indicado acima, a cada T segundos as i-ésimas componentes dos r sinais a serem multiplexados V_j^1, V_j^2, V_j^r, são transformadas. Desta forma, o i-ésimo vetor transformado V contém informação de cada um dos r sinais multiplexados. A demultiplexação é realizada simplesmente aplicando-se a inversa da transformada utilizada, como ilustrado abaixo.



5.3.1 GDM Utilizando a THCF

Nesta seção é desenvolvido um sistema de multiplexação GDM com base na THCF. Uma interpretação deste sistema de multiplexação em termos da técnica de espalhamento espectral é realizada e é calculado seu ganho em eficiência espectral com relação aos sistemas FDM e TDM.

Com o objetivo de simplificar a notação, considere, no que se segue, a multiplexação apenas da i-ésima componente de cada um dos r sinais a serem multiplexados. Desta forma, o vetor

$$(Vi^1, Vj^2, \ldots, v,^r)$$

será denotado por

$$(Vfc\,Vi, V,w|)$$

e seu espectro de Galois-Hartley representado por

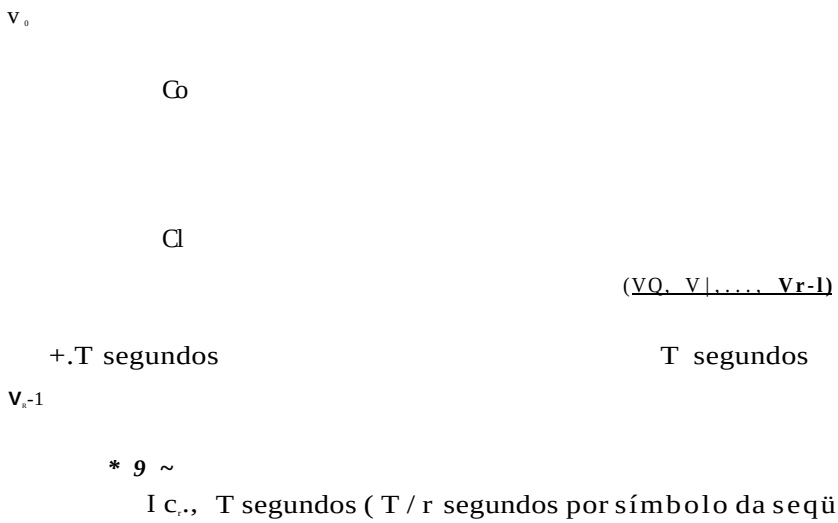
$$(Vo, V|, .., Vr\text{-}l),$$

onde

$$V_k = Yj\ ^{v}i^{\cdot\cdot\cdot}ki \quad .$$

assim como na definição 4.6.

Seja c_k a seqüência definida por $c_k = (cas_k0, cas_kl, \quad cas_kr\text{-}l)$, com k = 0, 1, r - l. Desta forma, o sistema de multiplexação GDM utilizando a THCF pode ser ilustrado como se segue:



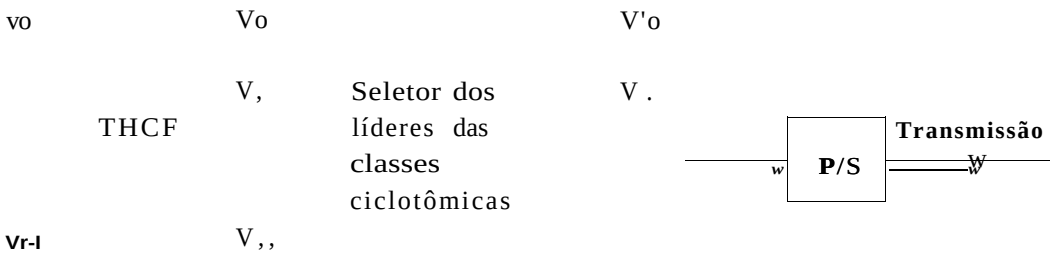
Na ilustração acima o símbolo Q realiza a modulação do sinal **Vj** pela respectiva seqüência $c_,$. Por outro lado, o símbolo + efetua a adição em GI(q).

A duração de cada seqüência c_k é T segundos (a mesma duração do símbolo de entrada **Vj),** ou seja, cada elemento da seqüência c_k tem a duração de T/r segundos, o que resulta em uma banda passante para o sinal multiplexado dada por r vezes a banda passante de um único símbolo **Vj** . As seqüências c_k podem ser interpretadas como as seqüências p(t) que realizam o

espalhamento espectral no sistema de multiplexação CDM descrito anteriormente, observando-se, contudo, que tais seqüências c_k são ortogonais (teorema 4.1).

De fato, o resultado obtido para o acréscimo da banda passante do sinal multiplexado é o mesmo resultado encontrado para os sistemas FDM e TDM. Nota-se, contudo, que o sinal multiplexado (V) tem seus símbolos definidos sobre GI(q), isto é, sobre um alfabeto maior que o alfabeto dos sinais de entrada e, como foi mostrado na seção 4.3.6, há uma redundância presente nos vetores transformados pela THCF. Dessa forma, apenas os líderes das classes ciclotômicas (definição 4.9) são necessários para se recompor todo o espectro de Hartley.

A compressão espectral no domínio Galois-Hartley é então obtida "em troca" de uma expansão do alfabeto, e é realizada transmitindo-se apenas os líderes das classes ciclotômicas formadas pela THCF. Um esquema de implementação do sistema GDM com compressão espectral é descrito abaixo.



Na ilustração acima, os símbolos V'_k, com k = 0, 1, c-1, representam os líderes das c classes ciclotômicas associadas a THCF utilizada.

Capítulo 6

Conclusões

6.1 A Transformada de Hartley em um Corpo Finito

Esta dissertação apresenta novas idéias e ferramentas a serem utilizadas em sistemas de Comunicação. Nesse contexto, uma nova transformada foi proposta, a Transformada de Hartley em um Corpo Finito (THCF) e uma nova técnica de multiplexação digital (GDM) utilizando transformadas sobre corpos finitos foi apresentada como uma das possíveis aplicações da THCF.

Inicialmente, a construção de uma Transformada Discreta de Hartley em um corpo finito foi investigada. Para tal foi necessário estabelecer primeiro uma estrutura equivalente às funções senoidais cos(.) e sen(.), sobre um corpo finito, de modo a obter uma transformada que apresentasse alguma semelhança com a Transformada Discreta de Hartley introduzida por Bracewell, Essa tarefa foi realizada e uma Trigonometria sobre corpos finitos foi introduzida. Assim, as funções k-trigonométricas $\cos_k$ e $\sin_k$ foram definidas, das quais a função cas_k (cosine and sine) foi obtida e usada para introduzir a THCF. Diversas propriedades da THCF foram apresentadas, incluindo a propriedade de convolução cíclica e uma relação do tipo Parseval. A relação entre a THCF e a TFCF foi estabelecida e a condição de espectros válidos, semelhante as relações de conjugação da TFCF, foi determinada. Baseado nesta relação, um algoritmo rápido para computação da THCF foi sugerido. A THCF apresentada aqui é diferente de uma outra versão proposta anteriormente porém apresenta-se como a mais natural.

A Transformada de Hartley em um Corpo Finito surge como uma nova ferramenta matemática no contexto da Comunicação Digital. Foi proposto um novo sistema de multiplexação digital de concepção diferente dos sistemas de multiplexação até então conhecidos na literatura. Tal singularidade está evidenciada pelo ganho em eficiência espectral alcançado por este novo sistema com relação aos sistemas tradicionais.

6.2 Possíveis Aplicações da THCF

A transformada de Hartley em um corpo finito estudada nesta dissertação pode conduzir a relevantes aplicações no contexto de Telecomunicações. Particularmente, ela aparenta ter potencial uso em Processamento de Imagens e em Sistemas de Comunicação (multiplex, acesso múltiplo, espalhamento espectral, etc). O capítulo 5 propõe um novo sistema de multiplexação digital. Esta nova estratégia de multicanalização (multiplex) é especialmente atrativa para canais que apresentam uma alta relação sinal-ruído. Embora fibras ópticas ainda não possam ser consideradas como canais com limitação em banda passante, este novo tipo de multiplex pode ser adotado em canais de satélites ou até mesmo em canais de comunicação móvel celular. Nessa técnica, os tributários são *"empilhados"* ao invés de intercalados no tempo ou na freqüência. Estes esquemas digitais, baseados em transformadas discretas, são do tipo Multiplex por Divisão em Códigos *Multiniveis* (CDM multinível). A principal vantagem deste esquema com relação a outros esquemas digitais clássicos (os quais requerem uma expansão de banda passante diretamente proporcional ao número de canais multiplexados) diz respeito a sua melhor eficiência espectral.

Os esquemas GDM introduzidos na seção 5.3 são baseados em transformadas para as quais existem algoritmos rápidos, tornando-os bastante atrativos. Eles também são convenientes do ponto de vista prático desde que sua implementação pode ser feita utilizando um processador digital de sinais *(chip* DSP). O compromisso entre extensão do alfabeto e a largura de banda deve ser explorado. O fator de ganho por compactação de banda passante com relação a TDM/TDMA depende fortemente da expansão do alfabeto utilizada na transformada, i.e., do corpo de extensão usado.

6.3 Sugestões para Investigações Futuras

Nesta dissertação, novas técnicas para Comunicação Digital foram desenvolvidas e consequentemente novas linhas de investigações foram abertas. A THCF certamente tem aplicações interessantes em diversas áreas. Resta portanto muito a ser explorado e para iniciar este trabalho, algumas sugestões para futuras pesquisas são apresentadas a seguir.

• Uma nova abordagem para se obter um algoritmo rápido para a THCF que não utilize diretamente algoritmos FFTs poderia ser derivada de um algoritmo rápido desenvolvido por Bracewell para a Transformada Discreta de Hartley. De fato, este algoritmo é baseado em propriedades da TDH que possuem uma equivalência com as propriedades da THCF. Uma motivação extra nesta pesquisa seria a utilização da forte simetria presente na THCF no momento de se agrupar os cálculos efetuados. Desta forma, uma complexidade computacional inferior a complexidade das FHTs poderia ser alcançada e assim, uma FFT mais eficiente poderia ser desenvolvida com base nas relações entre a THCF e a TFCF (seção 4.3.4).

• No capítulo 5 foi apresentado um novo sistema de multiplexação digital denominado GDM. Como foi visto, este sistema realiza uma compressão espectral através da seleção dos líderes das classes ciclotômicas da THCF. Pode-se, contudo, realizar a multiplexação sem necessariamente se obter compressão espectral. Neste caso, os símbolos redundantes presentes na THCF podem ser utilizados para codificação de canal. Desta forma, um futuro tema de pesquisa seria a determinação dos possíveis Códigos Corretores de Erros obtidos via Transformada de Hartley em um Corpo Finito.

• O uso da THCF em Processamento Digital de Sinais, especialmente no contexto das chamadas Transformadas Numéricas (e.g., Transformada de Mersenne), deve ser investigado. Especificamente, sugere-se a definição das Transformadas Numéricas de Hartley-Mersenne (HMNT) e Hartley-Fermat (HFNT).

• Na área de Codificação de Canal, a THCF pode ser usada para fornecer uma descrição no domínio da freqüência (espectro de Galois) de códigos corretores de erros (especialmente para a família de códigos BCH), proporcionando portanto uma abordagem alternativa para o método introduzido por R.E. Blahut.

• Possíveis aplicações da FFHT no contexto de processamento de imagens deveriam ser examinadas. Algumas variantes desta transformada (FFHT), incluindo a introdução de uma versão negacíclica, poderiam também ser estudadas.

• Sugere-se investigar o uso das transformadas em corpos finitos como ferramenta para o projeto de seqüências de espalhamento espectral. A idéia é explorar as propriedades de ortogonalidade das seqüências síncronas multiníveis definidas sobre o conjunto de inteiros gaussianos. O espalhamento com formas de onda síncronas com base em seqüências {cas(.)} provê uma interferência nula entre usuários. Obviamente, um certo número de aspectos tais como sincronização imperfeita, desempenho em probabilidade de erro, ou ainda potências de usuários desiguais, são deixados para investigações futuras.

• A THCF pode ser usada, no contexto de Criptografia, como uma ferramenta de auxílio na determinação da complexidade linear de seqüências digitais a ser empregadas nos dispositivos geradores de chave para cripto-sistemas de chave privada.

Apêndice 1

Evariste Galois

A1.1 Período Histórico

O ponto de partida dos eventos históricos que influenciaram definitivamente a vida de Galois foi a tomada da Bastilha em 14 de julho de 1789. Nesta época a monarquia de Louis XVI atravessava grandes dificuldades ao enfrentar a união do povo francês em prol da eliminação dos privilégios estabelecidos pela igreja e pelo estado.

Para a compreensão do movimento revolucionário é fundamental descrever a situação da França pouco antes de 1789, quando a Revolução Francesa representou um golpe definitivo no Absolutismo, no poder da Igreja e da nobreza, que caracterizaram o Antigo Regime. A França possuía uma sociedade estratificada: 1.Clero, 2.Nobreza, 3. Todo o resto (a maioria ligada a terra, servos, camponeses) encabeçado pela burguesia.

Em 1774 Luís XVI sobe ao trono, tendo que se defrontar com graves problemas, dos quais o mais premente era o déficit crônico das finanças públicas.

A economia na Europa continental tinha na agricultura sua principal atividade. Pelo menos 20 milhões de franceses viviam nos campos. Em 1784, chuvas intensas destruíram várias regiões, no ano seguinte uma forte seca abalou o país. O governo francês participou de guerras na Europa, sendo derrotado, o que aumentou as dificuldades da monarquia absolutista na França, que já era fortemente criticada no plano da política interna. O absolutismo do direito divino, mantendo-se nos fins do século XVIII tal como na época de Luís XIV (século XVII - nesta época a corte estabelecida em Versalhes chegou a abrigar 10 mil pessoas, na sua maioria nobres que viviam as custas do Estado), apresentava-se como um anacronismo na sociedade francesa.

Em 5 de maio de 1789 em Versalhes deu-se a sessão de abertura da Assembléia dos Estados Gerais. Esta assembléia, convocada pelo rei, visava discutir a questão do déficit. Clero e Nobreza boicotaram as assembléias. A partir daí, a burguesia passou a liderar os acontecimentos, exigindo e realizando reformas por meio de leis. Tentando reagir, Luís XVI mandou reprimir manifestações em Paris. As medidas repressivas aumentaram a agitação, que culminou no dia 14 de julho com a "Tomada de Bastilha".

Em 1791 a Constituição ficou pronta e foi jurada por Luís XVI. Por ela a Doutrina dos Três Poderes de Montesquieu era implantada na França. Os restos de Feudalismo, e os privilégios foram abolidos e foi proclamada a igualdade de todos perante a lei. Contudo amplas camadas de camponeses e trabalhadores urbanos continuavam agitando-se. Em 1792 decretou-se o fim da monarquia e a prisão da família real. A república proclamada passaria a ser governada por uma Convenção Nacional.

Em 1793 Luís XVI foi executado. Os anos seguintes foram altamente conturbados, ocorrendo vários golpes que colocavam e retiravam grupos do poder. Em 1795 promulgou-se uma nova constituição, criando-se um novo regime, chamado de Diretório, que era dominado pela alta burguesia. Ainda em 1795 a nobreza tentou um golpe e o governo foi salvo graças à intervenção das tropas comandadas por Napoleão Bonaparte.

Em 1799 o Diretório já estava desgastado, setores da burguesia clamavam por um governo forte. No dia 18 de Brumário, contando com o apoio do exército e da alta burguesia Napoleão realiza um golpe e estabelece um novo governo.

Napoleão governou a França de 1799 a 1814, quando foi deposto e obrigado a exilar-se. Retomou ao governo durante os "Cem Dias", em 1815, sendo então definitivamente deposto. Sob vários aspectos o governo de Napoleão afastou-se dos ideais de liberdade e igualdade apregoados pela revolução. Apoiado pela alta burguesia e pelo exército, estabeleceu um regime fortemente autoritário.

Com a derrota de Napoleão, começou a Restauração na França. A dinastia dos Bourbons voltou a reinar com Luís XVIII e com o novo governo retornaram os elementos do clero e da nobreza ansiosos para restaurar sua antiga condição de privilegiados. Luís XVIII, no entanto, sentindo a impopularidade de seu governo, procurou manter boas relações com a burguesia. Essa política moderada foi abandonada por Carlos X, que sucedeu Luís XVIII em 1824. Contra o novo rei desencadeou-se, em julho de 1830, uma revolução liderada pela burguesia que, vitoriosa, levou ao trono Luís Felipe, o chamado "rei dos banqueiros", que iniciou a dinastia Orléans e um regime liberal.

A 1.2 A Vida de Évariste Galois

Em Paris, na obscura manhã do dia 30 de maio de 1832, perto de um pequeno lago e não tão longe da pensão Sieur Faultrier, Evariste Galois confrontou-se, num duelo com pistolas e foi atingido no estômago. Horas depois, estirado no chão, ferido e sozinho, Galois foi encontrado por um camponês que passava pelo local. Ele foi levado para o Hospital Cochin, onde morreu no dia seguinte nos braços de seu irmão Alfred, após recusar os serviços de um padre. Tivesse Galois vivido outros cinco meses, teria então completado 21 anos.

Mapa de Paris no Século XIX, destacando Bourg-la-Reine

Evariste Galois nasceu na pequena aldeia francesa de Bourg-la-Reine, no dia 25 de outubro de 1811. Quando Evariste tinha apenas quatro anos de idade, seu pai foi eleito prefeito de Bourg-la-Reine. Nicolas-Gabriel Galois era um homem culto e cortês e durante seu mandato como prefeito conquistou o respeito da comunidade. Fora da política, seu maior interesse parece ter sido a composição de versos satíricos. Galois herdou de seu pai a veia poética e de sua mãe a melhor instrução possível até os 12 anos, quando o mandou para o Liceu de Louis-le-Grand, em Paris. Aquela casa de ensino mais parecia uma relíquia da idade média, dominada por um carrasco que fazia as vezes de diretor. Normalizada a vida no Liceu, Evariste continuou a ouvir suas aulas e dar conta das obrigações razoavelmente, graças principalmente à magnífica base primária que sua mãe lhe havia dado. Apesar de ter brilhado como aluno, no primeiro ano, Galois jamais foi um estudante atencioso aos ensinamentos. Sua mente estava quase sempre fora da classe de aula. Para ele aquelas preleções nada representavam, pois dentro de seu organismo já havia o gérmen da criação.

No ano seguinte, quando Galois tinha 13 anos, a Matemática invade todo o seu corpo e, ele se desinteressa pelo estudo da Retórica. A esta altura cai-lhe às mãos a Geometria de Legendre que Galois lê rápida e sofregamente a interpreta tão bem quanto seu autor. Os compêndios relativos à matemática que circulavam no Liceu, nunca mereceram atenção de Galois pois eram demais triviais.

Foi somente com a idade de dezesseis anos que Galois pôde fazer seu primeiro curso de matemática. A ânsia de Galois pela matemática logo superou a capacidade do seu professor, e assim ele passou a estudar diretamente dos livros escritos pelos gênios da época.

Indubitavelmente Galois recebeu de Lagrange suas idéias iniciais em Teoria das Equações. Isto ocorreu em fevereiro de 1827, quando descobriu textos de Legendre sobre geometria e logo após, um exemplar original de Lagrange : *Resolução de Equações Numéricas* (Equações Algébricas) *Teoria das Funções Analíticas* e *Lições sobre o Cálculo de Funções.* Havia um caminho claro para o jovem prodígio, todavia seu brilho seria o maior obstáculo ao seu progresso. Embora soubesse mais matemática do que seria necessário para passar nas provas do Liceu, as soluções de Galois eram freqüentemente tão sofisticadas e inovadoras que seus professores não conseguiam julgá-las corretamente. E o jovem gênio não melhorava a situação

com seu temperamento explosivo e uma precipitação que só conquistava a inimizade de seus tutores e de todos os que cruzavam seu caminho.

Galois tentou o exame da Ecole Polytechnique, sem a ajuda usual de um curso preparatório em matemática e então foi reprovado. Galois não desistiu. No mesmo ano, 1828, ele entrou no curso de Louis Paul Emile Richard, um distinto professor de matemática. Richard o encorajou e até defendeu a idéia de que Galois deveria ser admitido sem a necessidade de um exame. Os resultados deste encorajamento foram espetaculares e Galois publicou seu primeiro trabalho ("Prova de um Teorema sobre Frações Periódicas Contínuas") em abril de 1829 no *"Annales de Gergonne*\ Um ano após a primeira tentativa, Galois novamente realiza o exame de admissão para a Polytechnique e mais uma vez seus saltos lógicos na prova oral só confundiram seu examinador, *Monsieur* Dinet. Conta-se que, sentindo que estava a ponto de ser reprovado pela segunda vez, e frustrado por sua inteligência não estar sendo reconhecida, Galois perdeu a calma e jogou um apagador em Dinet, acertando em cheio. Nunca mais ele voltaria a entrar na Polytechnique.

Sem deixar se abalar pelas reprovações, Galois continuou confiante em seu talento matemático. Ele prosseguiu com suas pesquisas e seu principal interesse era em teoria das equações ("Teoria de Galois"). Em 1 de junho de 1829, ainda com 17 anos, ele submeteu a Academia suas primeiras pesquisas sobre a solubilidade de equações de grau primo. Augustin Louis Cauchy foi designado juiz.

Este ponto da história é bastante polêmico e tem sido um ponto comum de discórdia dentre os escritores que tem escrito sobre Galois. Alguns afirmam que Cauchy perdeu ou esqueceu os papéis e nunca deu uma resposta (Dupuy [29], Bell [27]), "ocasionando um dos maiores desastres na história da matemática" (Bell [27]). Outros (Infeld [26]) afirmam que Cauchy intencionalmente os jogou fora. Recentemente, surgiram fatos levantados por pesquisadores, sugerindo que Cauchy tinha planejado apresentar o trabalho de Galois na Academia em janeiro de 1830 e que ainda o tinha incentivado.

Infelizmente, nos três anos seguintes uma série de tragédias pessoais e profissionais iria destruir as ambições de Galois. Seu pai, Nicolas-Gabriel Galois se suicidou após uma campanha de difamação realizada por um sacerdote jesuíta. Galois então tenta novamente o reconhecimento de seu talento, enviando para o secretário da Academia, Joseph Fourier, uma nova versão de seus trabalhos. Fourier por sua vez deveria entregá-lo para o comitê avaliador. Outra tragédia ocorre e Fourier morre algumas semanas antes da data da decisão dos juizes, e embora um maço de trabalhos tivesse sido entregue ao comitê, o de Galois não estava dentre eles. Galois achou que seu trabalho fora propositadamente perdido devido às orientações políticas da Academia. Uma crença que foi reforçada no ano seguinte, quando a Academia rejeitou seu manuscrito seguinte, alegando que "seus argumentos não eram suficientemente claros nem suficientemente desenvolvidos para que possamos julgá-lo com rigor". Galois concluiu que havia uma conspiração para excluí-lo da comunidade matemática. Em conseqüência disto ele passou a negligenciar suas pesquisas em favor da luta pela causa republicana.

No dia 4 de dezembro de 1830 Galois tentou se tornar um rebelde profissional alistando-se na Artilharia da Guarda Nacional. Tratava-se de um ramo da milícia conhecido também como "Amigos do Povo". Antes do fim do mês o rei extinguiu a Artilharia da Guarda Nacional e Galois se viu desamparado e sem lar. Enquanto a paixão de Galois pela política continuava, era inevitável que sua sorte deteriorasse ainda mais. Galois ficou detido por um mês na prisão de Sainte-Pélagie após ser apanhado segurando um punhal e realizando um brinde ameaçador ao rei em um banquete republicano. No Dia da Bastilha Galois marchou através de Paris vestido com o uniforme da proscrita Guarda da Artilharia. Galois foi então sentenciado a seis meses de prisão e então voltou para Sainte-Pélagie. Em março de 1832, um mês antes do final

da sentença, irrompeu uma epidemia de cólera em Paris e os prisioneiros foram libertados. O que aconteceu com Galois nas semanas seguintes tem motivado muita especulação, mas o que se sabe com certeza é que a tragédia foi o resultado de um romance com uma mulher misteriosa, chamada Stéphanie-Félicie Poterine du Motel. Stéphanie estava comprometida com um cidadão chamado Pescheux D'Herbinville, que descobriu a infidelidade de sua noiva e desafiou Galois para um duelo ao raiar do dia. Galois conhecia muito bem a perícia de seu desafiante com a pistola. Na noite anterior ao confronto, que ele acreditava ser a última oportunidade que teria para registrar suas idéias no papel, ele escreveu cartas para os amigos explicando as circunstâncias.

Em uma tentativa desesperada de conseguir um reconhecimento, ele trabalhou a noite toda, escrevendo o teorema que acreditava explicaria o enigma da equação de quinto grau. As páginas eram, na maior parte, uma transcrição das idéias que ele já enviara a Cauchy e Fourier. No final da noite, quando seus cálculos estavam completos, ele escreveu uma carta explicativa ao seu amigo Auguste Chevalier, pedindo que, caso morresse, aquelas páginas fossem enviadas aos grandes matemáticos da Europa.

Na manhã seguinte, quarta-feira, 30 de maio de 1832, num campo isolado, Galois e D'Herbinville se enfrentaram a uma distância de vinte e cindo passos, armados com pistolas. D'Herbinville viera acompanhado de dois assistentes. Galois estava sozinho. Ele não contara a ninguém sobre seu drama. Um mensageiro que enviara ao seu irmão, Alfred, só entregaria a notícia depois do duelo terminado. E as cartas que escrevera na noite anterior só chegariam aos seus amigos vários dias depois.

As pistolas foram erguidas e disparadas. D'Herbinville continuou de pé. Galois foi atingido no estômago. Ficou agonizando no chão. Não havia nenhum cirurgião por perto e o vencedor foi embora calmamente, deixando seu oponente ferido para morrer. Algumas horas depois Galois foi levado para o Hospital Cochin. Era muito tarde, já ocorrera uma peritonite e no dia seguinte Evariste Galois faleceu.

A 1.3 Citações

• Em toda a história da ciência não existe um exemplo maior do triunfo da estupidez sobre um gênio, do que o proporcionado pela curta vida de Evariste Galois .
(E. T. Bell, [27])

• Na França, em torno de 1830, uma nova estrela de brilho inimaginável surgiu nos campos da Matemática Pura ... Evariste Galois.
(Felix Klein)

• O fato é que Galois era capaz, com pouca idade e sem o benefício de uma educação superior formal, de fazer descobertas que mais tarde o dariam tanta fama. Hoje, acontece de jovens matemáticos serem desencorajados pela história de Galois, dizendo a si mesmo: "Aqui eu estou, com X anos, X-20 anos mais velho do que Galois tinha quando morreu e apesar de gostar de matemática e ser bem sucedido no seu estudo, eu não seria capaz de fazer uma grande descoberta. Como Galois foi capaz de fazê-lo ? Ele foi abençoado com algum dom sobre humano que o colocou numa classe a parte ?" Eu acho que não. E claro que talento é essencial, e poucos são tão talentosos quanto Galois. Contudo, apenas o talento não é suficiente. Galois teve que pesquisar até o ponto onde ele sabia o suficiente e tinha técnicas o

suficiente ao seu alcance para assim poder ser capaz de se distanciar do que já se tinha feito antes.
(Harold M. Edwards, [28])

• Hoje fala-se muito nas escolas secundárias em "Matemática Moderna", mas ela só é moderna no sentido que as idéias de Galois finalmente estão chegando a todos, mais de um século depois que o destino o tratou tão mal.
(Carl B. Boyer, [24])

• Este é o único estudante que tem me respondido pobremente, ele não sabe absolutamente nada. Eu fui informado que este estudante tem uma extraordinária capacidade para matemática. Isto me deixa fortemente assombrado, pois após seu exame, eu acredito que ele tenha uma pequena inteligência.
(Relatório do seu examinador de literatura do "Ecole Normale ")

• Este homem tem uma superioridade de pensamento sobre todos nós e se preocupa unicamente com as partes mais difíceis e profundas da matemática.
(Louis Paul Emil Richard - professor de matemática comentando o insucesso de Galois na ' 'Polytechn ique")

• Eu experimentei um intenso prazer no instante em que, tendo preenchido alguns pequenos detalhes, eu vi a versão completamente correta do método pelo qual Galois provou, em particular, este belo teorema : Para que uma equação irredutível de grau primo seja solúvel por radicais é necessário e suficiente que todas as suas raízes sejam funções racionais de quaisquer duas delas.
(Joseph Liouville, 24 anos após a morte de Galois, publicou alguns manuscritos de Galois com o comentário acima)

• Sua argumentação não é suficientemente clara nem suficientemente desenvolvida para nos permitirjulga-lacomrigor.
(Carta enviada por Poisson quando Galois estava na prisão de Sainte-Pélagie)

• "Eu espero que seja do interesse desta Academia o fato de que entre os trabalhos de Evariste Galois eu encontrei uma solução tão precisa quanto profunda deste belo problema: Sobre que condições uma equação é solúvel por meio de radicais..."
(Joseph Liouville - O discurso de entrada na Academia de Ciências em 4 de Julho de 1843)

• "Para entendermos as demonstrações de Galois é suficiente dedicar-se exclusivamente a elas durante um ou dois meses, sem pensar em nada mais."
(Palavras de Liouville)

• Com 16-17 anos, Galois, um estudante do Louis-le-Grand, formulou um dos mais difíceis problemas em matemática. Contudo, dificilmente ele poderia saber da importância deste problema; ele dificilmente poderia saber que seus métodos revolucionários e poderosos através dos quais ele pode resolver o problema, iriam influenciar o desenvolvimento da matemática um século depois.
(Leopold Infeld, [26])

• Grandes matemáticos usualmente tem vida comum, ou seja, o drama de suas vidas é decorrente da matemática e não pode ser apreciado por não matemáticos. A grande exceção é Evariste Galois, sua história de vida (ou o que sabemos dela) é como um romance.
(Harold M. Edwards, [28])

• Se a verdade é tão difícil de ser estabelecida em casos de homens ricos e famosos que morreram idosos a um século atrás, muito mais difícil é o caso de Galois, que morreu jovem e desconhecido. Usualmente biografias realmente começam quando o herói atinge a idade em que a vida de Galois terminou.
(Leopold Infeld, [26])

• Quando Galois morreu, ele era conhecido apenas como um ardente Republicano que amava a França, que amava a liberdade, que odiava e lutava contra a tirania. Para os matemáticos de hoje, familiares com as expressões "Grupos de Galois", *"Galois Field* (GF)" , "Teoria de Galois" ele é conhecido como um dos grandes matemáticos de todos os tempos, que morreu na juventude em um duelo. Mas enquanto ele viveu ele era ambos. Sua história merece ser conhecida e relembrada não apenas pelos matemáticos, mas por todos os homens livres.
(Leopold Infeld, [26])

• Questione Jacobi ou Gauss publicamente para que dêem suas opiniões, não sobre a verdade, mas sobre a importância destes teoremas. Mais tarde surgirá, eu espero, alguém que irá encontrá-los e terá interesse em decifrar toda esta confusão ...
(O fim de sua carta escrita para Chevalier na véspera do duelo)

• ... Não tenho tempo ...
(Evariste Galois)

• *A* seu funeral compareceram milhares de republicanos. Tinha apenas vinte anos então, o mais jovem matemático que jamais fez descobertas tão significativas.
(Carl B. Boyer, [24])

Apêndice 2

Classes Ciclotômicas para a Transformada de Hartley em um Corpo Finito

De acordo com a definição 4.9, dados $q = p^r$ a ordem do corpo e N o comprimento da transformada, as classes ciclotômicas são então definidas pela relação

$$-kq \bmod (N)$$

onde k = 0,1,..., N - l e N divide q - 1.

$q = 27 = 3^3$

N = 13

Co = (0)
C_1 = (1,10,9,12,3,4)
C_2 = (2,7,5,11,6,8)

N = 26

Co = (0)
C_1 = (1,23,9,25,3, 17)
C_2 = (2,20, 18,24,6,8)
C_4 = (4, 14, 10,22, 12, 16)
C_5 = (5,11,19,21,15,7)
C,3= (13)

q = 243 = 3^5

N - 11

Co = (O)

C, = (1, 8, 9, 6, 4, 10, 3, 2, 5, 7)

N = 22

Co = (O)

C, = (1, 19, 9, 17, 15, 21, 3, 13, 5, 7)

C_2 = (2, 16, 18, 12,8,20,6,4, 10, 14)

Cu - (11)

N = 121

Co = (O)

C, = (1, 118,9,94,81, 120,3, 112,27,40)

C_2 = (2, 115, 18, 67, 41, 119, 6, 103, 54, 80)

C_4 = (4, 109,36, 13,82, 117, 12,85, 108,39)

C_5 = (5, 106,45, 107,42, 116, 15,76, 14,79)

C_7 = (7, 100, 63, 53, 83, 114, 21, 58, 68, 38)

C_8 = (8, 97, 72, 26, 43, 113, 24, 49, 95, 78)

C,o= (10,91,90,93,84, 111,30,31,28,37)

C n = (11,88,99,66,44, 110,33,22,55,77)

$C_{,6}$ = (16, 73, 23, 52, 86, 105, 48, 98, 69, 35)

C,7= (17,70,32,25,46, 104,51,89,96, 75)

Ci9 = (19, 64, 50, 92, 87, 102, 57, 71, 29, 34)

C_{20}= (20,61,59,65,47, 101,60,62,56,74)

q = 125 = 5^3

N == 31

Co = (0)

c, = (1,26,25,30,5,6)

c_2 = (2,21, 19,29, 10, 12)

c_3 = (3, 16, 13,28, 15, 18)

c_4 = (4, 11,7,27,20,24)

C_8 = (8,22,14,23,9,17)

N == 62

Co - (0)

c, = (1,57,25,61,5,37)

c_2 = (2,52,50,60, 10, 12)

c_3 = (3,47,13,59,15,49)

c_4 = (4, 42, 38, 58, 20, 24)

c_6 = (6, 32, 26, 56, 30, 36)

c_7 = (7,27,51,55,35, 11)

c_8 = (8,22, 14,54,40,48)

c_9 = (9, 17,39,53,45,23)

Cl6 = (16,44,28,46, 18,34)

C|9 = (19,29,41,43,33,21)

c_3, = (31)

Apêndice **1**

q = 343 = 7^3

N = 9

Co - (O)
C_1 = (1,2,4,8,7,5)
C_3 = (3, 6)

N = 18

Co = (O)
C_1 = (1, 11, 13, 17,7,5)
C_2 = (2,4,8, 16, 14, 10)
C_3 = (3, 15)
C_6 = (6,12)
Co = (9)

N = 19

Co = (O)
C_1 = (1,12,11,18,7,8)
C_2 = (2,5,3, 17, 14, 16)
C_4 = (4, 10,6, 15,9, 13)

Primos de Mersenne

s	p = 2^s - l
2	3
3	7
5	31
7	127
13	8191
17	131071
19	524287
31	2147483647
61	2305843009213693951

Tabela Al - Primos de Mersenne.

Apêndice **1**

Polinómios Primitivos

P"	*(X)
3[J]	$x^3 + 2x^2 + 1$
3"	$x^3 + x^4 + x^2 + 1$
3>	$x^7 + x^6 + x^4 + 1$
3°	$x^y + x^7 + x^5 + 1$
7[J]	$x^3 + x^2 + x + 2$
7[S]	$x^5 + x^4 + 4$
7>	$x^7 + x^5 + 4$
11[J]	$x^3 + x^2 + 5$
11[S]	$x^5 + x^3 + x^2 + 9$
19[J]	$x^3 + x^2 + 16$
23[3]	$x^3 + x^2 + 16$
31[J]	$x^3 + x + 28$

Tabela A2 - Polinómios Primitivos.

Tabela de GF**(3[3]).**

a °	1	a [13]	2
a [1]	X	a [14]	2x
a [2]	x^2	a [15]	$2x^2$
a [3]	$x^2 + 2$	a [16]	$2x^2 + 1$
a[4]	$x^2 + 2x + 2$	**a»**[7]	$2x^2 + x + 1$
a [5]	$2x + 2$	a [18]	$x + 1$
a [6]	$2x^2 + 2x$	a [19]	$x^2 + X$
a [7]	x^2 - M	a [20]	$2x^2 + 2$
a [8]	$x^2 + x + 2$	a [21]	$2x^2 + 2x + 1$
a'	$2x^2 + 2x + 2$	**a**[22]	$x^2 + x + 1$
a[10]	$x^2 + 2x + 1$	**a**[23]	$2x^2 + x + 2$
a"	$x + 2$	**a**[24]	$2x + 1$
a'[2]	$x^2 + 2x$	**a**[25]	$2x^2 + x$

Tabela A3 - Tabela de GF(3[3]) gerado por ;r(x)=x^3 + 2x^2 + 1.

Tabela de GF(3^5).

a°	1	**a^{41}**	**$2x^3 + x^2 + x + 2$**	**a"**	**$2x^4 + 2x^2 + 1$**
a'	X	**a^{42}**	**$2x^4 + x^3 + x^2 + 2x$**	**a^{w}**	**$x^4 + 2x^3 + x^2 + x + 1$**
a^{2}	X"	a^{43}	**$2x^4 + x^3 + 1$**	a^{84}	**$x^4 + x^3 + x + 2$**
a^3	X$^{!}$	**a^{44}**	**$2x^4 + x^2 + x + 1$**	**a^{85}**	**$2x + 2$**
a^4	**x^4**	**a^{45}**	**$x^4 + x^3 + 2x^2 + x + 1$**	**a'»"**	**$2x^2 + 2x$**
a^5	**$2x^4 + 2x^2 + 2$**	**a^{46}**	**$2x^3 + x + 2$**	**a^{87}**	**$2x^3 + 2x^2$**
a^6	**$x^4 + 2x^3 + x^2 + 2x + 1$**	**a^{47}**	**$2x^4 + x^2 + 2x$**	**a^{88}**	**$2x^4 + 2x^3$**
a^7	**$x^4 + x^3 + x^2 + x + 2$**	a^{48}	**$x^4 + x^3 + 1$**	a^{89}	**$x^2 + 1$**
a^8	**$x^3 + 2x + 2$**	**a^{49}**	**$2x^2 + x + 2$**	**a^{90}**	**$x^3 + x$**
a^9	**$x^4 + 2x^2 + 2x$**	**a^{50}**	**$2x^3 + x^2 + 2x$**	**a$^{9'}$**	**$x^4 + x^2$**
a^{10}	**$2x^4 + 2x^3 + x^2 + 2$**	a$^{5'}$	**$2x^4 + x^3 + 2x^2$**	a^{92}	**$2x^4 + x^3 + 2x^2 + 2$**
a"	**$x^3 + x^2 + 2x + 1$**	**a^{52}**	**$2x^4 + 2x^3 + x^2 + 1$**	**a^{93}**	**$2x^4 + 2x^3 + x^2 + 2x + 1$**
a^{12}	**$x^4 + x^3 + 2x^2 + x$**	**a^{53}**	**$x^3 + x^2 + x + 1$**	**a^{94}**	**$x^3 + x + 1$**
a$^{'3}$	**$2x^3 + 2$**	a^{54}	**$x^4 + x^3 + x^2 + X$**	a^{95}	**$x^4 + x^2 + X$**
a'^{4}	**$2x^4 + 2x$**	**a^{55}**	**$x^3 + 2$**	**a^{96}**	**$2x^4 + x^3 + 2$**
a^{15}	**$x^4 + 1$**	a^{56}	**$x^4 + 2x$**	a^{97}	**$2x^4 + x^2 + 2x + 1$**
a^{16}	**$2x^4 + 2x^2 + x + 2$**	**a^{57}**	**$2x^4 + x^2 + 2$**	**a^{98}**	**$x^4 + x^3 + x + 1$**
a^{17}	**$x^4 + 2x^3 + 2x^2 + 2x + 1$**	**a^{58}**	**$x^4 + x^3 + x^2 + 2x + 1$**	**a""**	**$x + 2$**
a^{18}	**$x^4 + 2x^3 + x^2 + x + 2$**	**a^{59}**	**$x^3 + x^2 + x + 2$**	**a^{100}**	**$x^2 + 2x$**
a'^{9}	**$x^4 + x^3 + 2x + 2$**	a^{60}	**$x^4 + x^3 + x^2 + 2x$**	a^{101}	**$x^3 + 2x^2$**
a^{20}	**$x^2 + 2x + 2$**	**a$^{6'}$**	**$x^3 + x^2 + 2$**	**a'^{102}**	**$x^4 + 2x^3$**
a$^{2'}$	**$x^3 + 2x^2 + 2x$**	**a^{62}**	**$x^4 + x^3 + 2x$**	**a'^{103}**	**$x^4 + 2x^2 + 2$**
a^{22}	**$x^4 + 2x^3 + 2x^2$**	**a^{63}**	**$x^2 + 2$**	**a^{104}**	**$-X^4 - X^3 - X^2 - X - 1^{i}$**
a^{23}	**$x^4 + 2x^3 + 2x^2 + 2$**	**a^{64}**	**$x^3 + 2x$**	**a'^{105}**	**$2x^3 + 2x + 1$**
a^{24}	**$x^4 + 2x^3 + 2x^2 + 2x + 2$**	a^{65}	**$x^4 + 2x^2$**	a'^{06}	**$2x^4 + 2x^2 + x$**
a^{25}	**$x^4 + 2x^3 + x^2 + 2x + 2$**	**a^{66}**	**$2x^4 + 2x^3 + 2x^2 + 2$**	**a^{107}**	**$x^4 + 2x^3 + 2x^2 + 1$**
a^{26}	**$x^4 + x^3 + x^2 + 2x + 2$**	**a^{67}**	**$2x^3 + x^2 + 2x + 1$**	**a'^{08}**	**$x^4 + 2x^3 + 2x^2 + x + 2$**
a^{27}	**$x^3 + x^2 + 2x + 2$**	**a^{68}**	**$2x^4 + x^3 + 2x^2 + x$**	**a'"'"**	**$x^4 + 2x^3 + 2x + 2$**
a^{28}	**$x^4 + x^3 + 2x^2 + 2x$**	a^{69}	**$2x^4 + 2x^3 + 2x^2 + 1$**	a"^{0}	**$x^4 + x^2 + 2x + 2$**
a^{29}	**$2x^3 + x^2 + 2$**	**a^{70}**	**$2x^3 + x^2 + x + 1$**	**a$^{'n}$**	**$2x^4 + x^3 + x^2 + 2x + 2$**
a^{30}	**$2x^4 + x^3 + 2x$**	**a^{71}**	**$2x^4 + x^3 + x^2 + x$**	**a"^{2}**	**$2x^4 + x^3 + 2x + 1$**
a$^{3'}$	**$2x^4 + 1$**	**a^{72}**	**$2x^4 + x^3 + 2x^2 + 1$**	**a"^{3}**	**$2x^4 + x + 1$**
a^{32}	**$x^4 + x^2 + X + 1$**	a^{73}	**$2x^4 + 2x^3 + x^2 + x + 1$**	a$^{'u}$	**$x^4 + 2x^2 + x + 1$**
a^{33}	**$2x^4 + x^3 + x + 2$**	**a^{74}**	**$x^3 + 2x^2 + x + 1$**	**a"^{5}**	**$2x^4 + 2x^3 + x + 2$**
a^{34}	**$2x^4 + 2x^2 + 2x + 1$**	**a^{75}**	**$x^4 + 2x^3 + x^2 + x$**	**a"^{6}**	**$2x^2 + 2x + 1$**
a^{35}	**$x^4 + 2x^3 + x + 1$**	a^{76}	**$x^4 + x^3 + 2$**	a"^{7}	**$2x^3 + 2x^2 + x$**
a^{36}	**$x^4 + x + 2$**	a^{77}	**$2x^2 + 2x + 2$**	a"^{8}	**$2x^4 + 2x^3 + x^2$**
a^{37}	**$2x^4 + 2x + 2$**	**a^{78}**	**$2x^3 + 2x^2 + 2x$**	**a"^{9}**	**$x^3 + x^2 + 1$**
a^{38}	**$x^4 + 2x + 1$**	**a^{79}**	**$2x^4 + 2x^3 + 2x^2$**	**a'^{20}**	**$x^4 + x^3 + X$**
a^{39}	**$2x^4 + x^2 + x + 2$**	**a^{80}**	**$2x^3 + x^2 + 1$**	**a'$^{2'}$**	**2**
a^{40}	**$x^4 + x^3 + 2x^2 + 2x + 1$**	a$^{8'}$	**$2x^4 + x^3 + x$**		

Tabela A4 - Tabela de GF(3^5) gerada por $7i(x)=x^5 + x^4 + x^2 + 1$.

Utilizando-se a tabela acima e a identidade $a^{121} = -1$, pode-se facilmente calcular qualquer elemento de GF(3^5).

Tabelas de Funções $sen_x(i)$ e $cos_x(i)$.

Funções geradas por $1 + j$, sobre GI(3).

$\cos_k(i)$

	0	**1**	2	3	4	5	6	7
0	1	1	1	1	1	1	1	1
1	1	,	0	j2	2	j2	0	J
2	1	0	2	0	1	0	2	0
3	1	j2	0	j	2	j	0	j2
4	1	2	1	2	1	2	1	2
5	1	j2	0	j	2	J	0	j2
6	1	0	2	0	1	0	2	0
7	1	J	0	j2	2	j2	0	j

k)

	0	**1**	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	,)2	2	j2	0	j	1	j
2	0	2	0	1	0	2	0	1
3	0	J2	1	j2	0	j	2	j
4	0	0	0	0	0	0	0	0
5	0	j	2	j	0	j2	1	j2
6	0	1	0	2	0	1	0	2
7	0	j	1	j	0	J2	2	Í2

(k)

Funções geradas por Ç = 4 , sobre GI(19)

$cos_k(i)$

k \ i	0	1	2	3	4	5	6	7	8
0	1	1	1	1	1	1	1	1	1
1	1	14	11	9	13	13	')	11	14
2	1	11	13	9	14	14	9	13	11
3	1	9	9	1	9	9	1	9	9
4	1	13	14	9	11	11	9	14	13
5	1	13	14	9	11	11	9	14	13
6	1	9	9	1	9	9	1	9	9
7	1	11	13	9	14	14	9	13	11
8	1	14	11	9	13	13	9	11	14

(k)

$sen_k(i)$

k \ i	0	**1**	2	3	4	5		7	8
0	0	0	0	0	0	0	0	0	0
1	**0**	**jio**	j ' 4	**j2**	J 4			**j5**	J 9
2	0		**J4**		**j9**	jlO	**j2**	J15	
3	**0**	**j2**	**J17**	**0**	**j2**		**0**	**j2**	**i ' 7**
4	**0**	**J4**	**J9**	**j2**	J5	J I 4	J I 7	**jio**	
5	**0**	**J15**	**jio**	**J17**	j ' 4	**j5**	**j2**		J 4
6	0	**J17**	**j2**	0	**J17**	**j2**	**0**	J 1 7	**j2**
7	**0**		**jl5**	**j2**	**no**	**j9**	J I 7	J 4	j ' 4
8	0		**J5**	**,i'** 7	**,i** 15	J 4	**J2**	**j 14**	**ilO**

(k)

Funções geradas por Ç = 2 , sobre GI(11).

$cos_k(i)$

	0	**1**	2	3	4	5	6	7	8	9
0	1	1	1	1	1	1	1	1	1	1
1	1	4	9	2	7	10	7	2	9	4
2	1	9	7	7	9	1	9	7	7	9
3	1	2	7	4	9	10	9	4	7	2
4	1	7	9	9	7	1	7	9	9	7
5	1	10	1	10	1	10	1	10	1	10
6	1	7	9	9	7	1	7	9	9	7
7	1	2	7	4	9	10	9	4	7	2
8	1	9	7	7	9	1	9	7	7	9
9	1	4	9	2	7	10	7	2	9	4

(k)

$sen_k(i)$

	0	**1**	2	3	4	5	6	7	X	9
0	0	0	0	0	0	0	0	0	0	0
1	**0**	**j2**	**J5**	**j5**	**j2**	**0**	**}9**	**j«**	**J6**	**J'**
2	**0**	**J5**	**j2**	**,)'**	**j«**	**0**	**,Í5**	**j2**	**J'**	**j6**
3	**0**	**J5**	**J9**	**j'**	**j5**	**0**	**J6**	**J2**	**j2**	**j«**
4	**0**	**j2**	**J6**	**j5**	**Í'**	**0**	**j2**	**J6**	**j5**	**J'**
5	0	0	0	0	0	0	0	0	0	0
6	**0**	**j9**	**J5**	**j<5**	**j2**	**0**	**J'**	**j5**	**J6**	**j2**
7	**0**		**j2**	**j2**	**J6**	**0**	**,Í5**	**i'**	**J'**	**|5**
8	**0**	**i«**	**j'**	**j2**	**j5**	**0**	**Í«**	**J'**	**j2**	**J5**
9	**0**	**J9**	**j<5**	**j«**	**.i'**	**0**	**J2**	**J5**		**Í2**

(k)

Apêndice 3

Neste apêndice estão listados os programas mais utilizados durante as simulações realizadas para este trabalho.

Programa **1**

Este programa foi desenvolvido utilizando-se o Maple V Realease 4. Sua função é calcular a Transformada de Fourier em um Corpo Finito sobre corpos GF(p^m) onde m > 1.

Neste caso particular o programa foi desenvolvido para o corpo base GF(3^5), uma transformada de comprimento 11, o polinómio gerador do corpo TT(X) = $x^5 + x^4 + + x^2 + 1$ e o elemento de ordem 11 dado por x + x+1.

```
readlib(GF):
G      :=      GF(3,5,p^5+p^4+p^2+l):
a      :=      G[ConvertIn](p^2+p+l):
q:=3^5-l:
n:=ll-l:

u[0]:=0:u[l]:=l:u[2]:=0:u[3]:=2:u[4]:=0:u[5]:=0:u[6]:=0:u[7]:=0:u^
10]:=2:
for ifrom 0 to n do:
u[i]          :=G[ConvertIn](u[ij);
od:
Vr:array(0..n):
for kfrom 0 to n do
Vr[k]:=0:
for ifrom 0 to n do
```

```
 Vr[k]:=Gr+\](Vr[k],G["*'](u[i],G[^](a,i*k))):
 od:
 od:
for k from 0 to n do
 print(G[ConvertOut](Vr[k]));
 od;
 b:=G[ Convertln]    (p):
for jfrom 0 to q do
 B[j]:=G[ConvertOut](Gr^](b,j));
 od:
for j from 0 to n do
for I from 0 to q do
 ifG[ConvertOut](Vr[j])=0        then
 er/jj:     =Indefinido:
 else
 ifG[ConvertOut](Vr[j])=B[l]          then
 er/jj:=l:
fi:
fi:
 od:
 od:
for k from 0 to n do
 if erfkj =Indefinido then
 print('u'=          G[ConvertOut](u[k]),0);
 else
 print('u'=       G[ConvertOut](u[k])      ,alpha^er[kJ):
fi;
 od;
```

Programa 2

Este programa foi desenvolvido utilizando-se o Maple V Realease 4. Sua função é construir a tabela de corpos finitos $GF(p^m)$ com $m>1$.

Neste caso particular o corpo gerado é $GF(3^5)$ e o polinómio gerador é dado por $7T(X) = X^5 + X^4 + X^2 + 1$.

```
 readlib(GF):G:=          GF(3,5,p^5+p^4+p^2+J):
 a:=G[ Con    vert In](p):
for ifrom 0 to 242 do
 v[iJ:=Gr^l(a,i):
 od:
for ifrom I to 242 do
print(G[ConvertOut] (v[i])    =    alpha^i):
 od;
```

Programa **3**

Este programa foi desenvolvido utilizando-se o Maple V Realease 4. Sua função é calcular a Transformada de Hartley em um Corpo Finito sobre corpos $GF(p^m)$ onde $m > 1$.

```
readlib(GF):
G:=GF(3,2,p^2+p+2):
a   :=    G[ConvertIn](p):
coss:=i              ->G[T](Gr+            l((G[^](a,i)),(Gn(a,-i))),2):
sen:=i           ->G[T](Gr-         l((G[^](a,-i)),(Gri(a,i))).2):
ufOJ:=p:u[I]:=0:u[2]:=2*p+1     :u[3]:     =     /     :u[4]:=0:u[5]:=0:u[6]:=0:u[7]:=0:
for ifrom 0 to 7 do:
u[ij:=   G[ Con  vert  In](u[i]);
od:
Vr: array (0.. 7):
for k from 0 to 7 do
Vr[k]:=0:
for ifrom 0 to 7 do
Vr[k]:=G['+'](Vr[k],G[***](u[i],coss(i*k))):
od:
od:
Vi:array(0..7):
for kfrom 0 to 7 do
Vi[k]:=0:
for ifrom 0 to 7 do
Vi[k]:=Gr+*](Vi[k],Gr*](u[i],sen(i*k))):
od:
od:
for k from 0 to 7 do
print(G[ConvertOut](Vr[k])       ,       GfConvertOutJ(VifkJ));
od;
for j from 0 to 7 do
B[/J:=G[ConvertOutJ(Gr^%](aJ));
od:
for jfrom 0 to 7 do
for I from 0 to 7 do
ifG[ConvertOut](Vr[j])=0      then
er/JJ:    = Indefinido:
else
ifG[ConvertOut](Vr[j])=B[l]       then
erO]:=l:
fi:
fi:
od:
od:
for j from 0 to 7 do
for I from 0 to 7 do
ifG[ConvertOut](Vi[j])=0      then
ei/JJ:     =Indefinido:
```

```
 else
 ifG[ConvertOut](Vi[j])=B[l]        then
 ei/j]:=l:
fi:
fi:
 od:
 od:
for k from  0 to  7 do
 if erfkj  =Indefinido  and  erfkj  =Indefinido  then
printf'u  '=     G[ConvertOut](u[k]),  0);
 else
 if  erfkj  =Indefmido  then
print('u'=              G[ConvertOut](u[k]),'j'*(alpha^ei[k])):
 else
 ifei[k]=Indefinido      then
printfu  '=       GfConvertOutJ(ufkJ),   alpha^er[k]):
 else
print('u'=     G[Con\>ertOut](u[k])     ,alpha^er[k]      +     'j'*(alpha^ei[k])):
fi:
fi:
fi:
 od;
```

Programa **4**

Este programa foi desenvolvido utilizando-se o Turbo Pascal 7.0. O programa calcula a Transformada de Hartley em um Corpo Finito em GI(p), m=T.

Dados a ordem de um corpo GF(p), onde p é um primo, e o comprimento da transformada, o programa calcula e expõe na tela as tabelas das funções senk e cosk e depois, a partir de um vetor de entrada dado, calcula o vetor transformado.

```
uses  crt;
var
n,i,k,p,a,al J.aik,a 1 ik,i2,band  :     integer;
v,vj,w,wj  :  array  [0.. 70]  of integer;
cos,sen   .array  [0..70,0..70]  of integer;
begin
clrscr;
writelnf'Digitep     de      GF(p)');
readln(p);
writelnf'Digite  o  tamanho  da  transformada  N/(P-l)');
readln(n);
writelnÇDigite  um  elemento  de  ordem  ',n,'de  GF(',p,')');
readln(a);
writelnÇDigite  o  inverso  deste  elemento  em  GFÇp,')');
readln(al);
writelnÇDigite  o  inverso  do  2  em  GFÇp,')');
```

```
readln(i2);
{calculo da matriz cos e da matriz sen}
for i:=l ton-l do
  fork:=l to n-1 do
   begin
   aik:=a;
   alik:=al;
        forj:=l to (i*k-l) do
         begin
         aik:=aik*a modp;
         a 1 ik: =a 1 ik *a 1 mod p;
         end;
   cosfi,k]: =i2*(aik+a 1 ik) modp;
   senfi.k] :=i2*(alik+(p-l)*aik) modp;
   end;
for i:=0 to n-1 do
 begin
 cos[i,0]:=l; cos[0,i]:=l; sen[i,0]:=0; sen[0,i]:=0;
 end;
 {escrevendo estas matrizes}
for i:=0 to n-1 do
   begin
  for k:=0 to n-1 do
   begin
   if cos[i,k]<10 then
   write(cos[i,k],' ')
   eise
   write(cos[i,kJ,");
   end;
   writeln;
   end;
 writeln;
 writeln;
for i:=0 to n-1 do
   begin
  for k:=0 to n-1 do
   write(sen[i,k]',' ');
   writeln;
   end;
 {calculo da transformada}
 band: =0;
 {vetor de entrada}
 while band=0 do
 begin
 writeln('Digite as componentes do vetor de entrada'),
for i—O to n-1 do
 begin
 write('v[',i,']= ');
 readln(vfij);
```

```
end;
writeln;
{vetor de saída (tem duas componentes)}
for k:=0 to n-l do
begin
w[k]:=0;
wj[k]:=0;
end;
for k:=0 to n-l do
   for i:=0 to n-l do
    begin
    wfkj :=(w[k]+ v[i] *cos[i, k] )mod p;
    w/fkj: =(wj[k]+v[i] *sen[i,k])mod p;
end;
writelnÇO vetor de saida , ');
for i:=0 to n-l do
writelnÇV[',i,'] = ',w[i],' + \wj[i] ,'j');
writelnÇDeseja calcular outro vetor ? Sim=0 Nao=l');
readln(band);
clrscr;
end;
readkey;
end.
```

Programa 5

Este programa foi desenvolvido utilizando-se o Turbo Pascal 7.0. O programa calcula a Transformada de Hartley em um Corpo Finito em GI(p), m=l. Com efeito, este programa é mais geral que o programa anterior, pois ele adimite a utilização de núcleos complexos para o cálculo da Transformada de Hartley em um Corpo Finito.

Dados a ordem de um corpo GF(p), onde p é um primo, e o comprimento da transformada, o programa calcula e expõe na tela as tabelas das funções senk e cosk e depois, a partir de um vetor de entrada dado (que pode ser complexo), calcula o vetor transformado.

```
uses crt;
var
n,i,k,p,a,b,alJ,aik,alik,i2,band: integer;
salva,salvai,bl,blik.bik : integer;
v,vj,w,wj : array [0.. 70] of integer;
cos.sen.cosj.senj -.array [0..70,0..70] of integer;
begin
clrscr;
writelnÇDigitep de GF(p)');
readln(p);
writelnÇ Digite o tamanho da transformada N / (P^2-1)');
readln(n);
```

```
writeln('Digite um elemento de ordem \n,' de GF(',p*p,') . Digite a parte real e a imaginaria');
readln(a);      readlnfb);
writelnÇDigite o inverso deste elemento em GFÇp,')');
readln(al);readln(bl);
writelnÇ Digite o inverso do 2 em GFÇp, ')');
readln(i2);
{calculo da matriz cos e da matriz sen}
for i:=l to n-l do
   for k:=l to n-l do
    begin
    aik: =a;
    bik:=b;
    alik:=al;
    blik:=bl;
          forj:=l          to(i*k-l)do
           begin
           salva: —aik;
           salvai :=al ik;
           aik:=(aik*a-b*bik+100*p)          modp;
           bik:=(b*salva+a*bik+100*p)          modp;
           alik:=(alik*al-bl*blik+100*p)               modp;
           blik:=(bl*salval+al*blik+100*p)               modp;
           end;
    cos[i,k]:=(i2*(aik+alik)+100*p)            modp;
    cosjfi, k]:= (i2 *(bik+bl ik)+100 *p)   mod p;
    senj[i,kj:=(i2*(alik+(p-l)*aik)+100*p)              modp;
    senfi, k]: =(i2 *((p- l)*bl ik+bik)+100 *p)   mod p;
    end;
for i:=0 to n-l do
 begin
 cos[i,0]:=l;
 cos[0,i]:=l;
 sen[i,0]:=0;
 sen[0,i]:=0;
 cosj[i,0]:=0;
 cosj[0,i]:=0;
 senj[i,0]:=0;
 senj[0,i]:=0;
 end;
 {escrevendo estas matrizes)
for i:=0 to n-l do
    begin
   for k:=0 to n-l do
    begin
    if cos[i,k]<10     then
    write(cosfi,k],'          cosjfi,k],'    ')
    else
    write(cos[i,k],'          +j',cosj[i,k],'');
```

```
    end;
    writeln;
    end;
writeln;
writeln;
for i:=0 ton-1 do
    begin
   for k:=0 to n-1 do
    write(sen[i,k], '+j',senj[i,kj,' ');
    writeln;
    end;
{calculo da transformada}
band:=0;
{vetor de entrada}
while band=0 do
begin
writelnÇDigite as componentes do vetor de entrada. Parte real e imaginaria');
for i:=0 to n-1 do
begin
write('v[',i,']= ');
readlnfvfi]);readln(vj[ij);
end;
writeln;
for k:=0 to n-1 do
begin
w[k]:=0;
wj[k]:=0;
end;
for k:=0 to n-1 do
   for i:=0 to n-1 do
    begin
    w[k]:=(w[kj+v[ij *(cos[i,kJ +sen[i,k])-vj[i] *(cosj[i,k] +senj [i,k]))mod p;
    wjfkj :=(wj[kj+vj[ij *(cos[i,kJ+sen[i,kj)+v[ij *(cosj[i,kJ +senj[i,kJ))mod p;
end;
writelnÇO vetor de saida , ');
for i:=0 to n-1 do
writeln('V[',i,']= \w[ij,'+ \wj[i] ,'f);
writelnÇDeseja calcular outro vetor ? Sim=0 Nao=l');
readln(band);
clrscr;
end;
readkey;
end.
```

Bibliografia

I. R. N. Bracewell, *The Hartley Transform,* Oxford University Press, 1986.

2. R. J. McEliece, *Finite Fields for Computer Scientists and Engineers,* Kluwer Academic Publishers, 1987.

3. R. Lidl e H. Niederreiter, *Introduction to Finite Fields and their Applications,* Cambridge University Press, 1986.

4. D. G. Myers, *Digital Signal Processing - Efficient Convolution and Fourier Transform Techniques,* Prentice-Hall, 1990.

5. A. J. A. Paschoal, *A Transformada Aritmética de Fourier,* Dissertação de Mestrado, Departamento de Eletrônica e Sistemas, UFPE, 1993.

6. R. E. Blahut, *Fast Algorithms for Digital Signal Processing,* Addison-Wesley, 1985.

7. A. Gonçalves, *Introdução à Algebra,* IMPA, 1979.

8. A. Hefez, *Curso de Álgebra,* IMPA, 1993.

9. E. de Alencar Filho, *Teoria das Congruências,* Nobel, 1986.

10. N. Ahmed, T. Natarajan, e K. R. Rao, *Discrete Cosine Transform,* IEEE Transactions on Computers, pg. 90-93, Janeiro 1974.

I I . I. S. Reed e T. K. Truong, *The Use of Finite Fields to Compute Convolutions,* IEEE Transactions on Information Theory, vol. 21, N° 2, pg. 203-207, Março 1975.

12. B. P. Lathi, *Sistemas de Comunicação,* Guanabara Dois, 1979.

13. A. V. Oppenheim e R. W. Schafer, *Discrete-Time Signal Processing,* Prentice Hall, 1989.

14. J. G. Proakis, *Digital Communications,* McGraw-Hill, 1995.

15.1. S. Reed, T. K. Truong, V. S. Kwoh e E. L. Hall, *Image Processing by Transforms over a Finite Field,* IEEE Trans. Comput., vol. C-26, pg. 874-881, setembro 1977.

16. R. E. Blahut, *Transform Techniques for Error-Control Codes,* IBM J. Res. Dev., vol. 23, pg. 299-315, maio 1979.

17. R. C. Agarwal e C. S. Burrus, *Number Theoretic Transforms to Implement Fast Digital Convolution,* IEEE Proc., vol. 63, pg. 550-560, abril 1975.

18. C. M. Rader, *Discrete Convolution via Mersenne Transforms,* IEEE Trans. Comput., vol. C-21,pg. 1269-1273, dezembro 1972.

19. R. N. Bracewell, *Aspects of the Hartley Transform,* IEEE Proc., vol. 82, pg. 381-387, março 1994.

20. J. M. Pollard, *The Fast Fourier Transform in a Finite Field,* Math. Comput. , vol. 25, N° 114, pg. 365-374, abril 1971.

21. R. M. Campello de Souza e P. G. Farrell, *Finite Fields Transforms and Symmetry Groups,* Discrete Mathematics, vol. 56, pg. 111-116, 1985.

22. R. N. Bracewell, *The Fast Hartley Transform,* IEEE Proc, vol. 72, N° 8, pg. 1010-1018, agosto 1984.

23. D. Yang, *Prime Factor Fast Hartley Transform,* Electronics Letters, vol. 26, N° 2, pg. 119-121, Janeiro 1990.

24. C. B. Boyer, *História da Matemática,* Editora da Universidade de São Paulo, 1976.

25. I. Stewart, *Galois Theory,* Chapman & Hall Mathematics, 1989.

26. L. Infeld, *Whom the Gods Love,* Whittlesey House, 1978.

27. E. T. Bell, *Men of Mathematics,* 1937.

28. H. M. Edwards, *Galois Theory,* Springer, 1984.

29. P. Dupuy, *La Vie d'Evariste Galois: Annates de I'Ecole Normal,* vol. 13, 1896.

30. A. Dumas, *Mes Memories,* vol. 10, 1865.

31. R. Campos, *Estudos de História Moderna e Contemporânea,* Atual, 1988.

32. S. Singh, *O Último Teorema de Fermat,* Record, 1998.

33. R. V. L. Hartley, *A More Symmetrical Fourier Analysis Applied to Transmission Problems,* proc. IRE, vol. 30, pg. 144-150, 1942.

34. M. Y. Rhee, CDMA & Network Security, Prentice Hall, 1998.

Publicações resultantes desta dissertação

Trigonometry in Finite Fields and a new Hartley Transform , IEEE International Symposium on Information Theory, ISIT, **MIT,** Cambridge, EUA, agosto 1998.

The Hartley Transform in a Finite Field, SBT/IEEE International Telecommunications Symposium, **ITS,** São Paulo, agosto 1998.

Efficient Multiplex for Band-Limited Channels: Galois-Field Division Multiple Access , Workshop on Coding and Cryptography, **WCC,** Paris, França, janeiro 1999.

The Complex Finite Field Hartley Transform , 5th International Symposium on Communication Theory and Application, **ISCTA,** Ambleside, Inglaterra, julho 1999.

Ortogonal Multilevel Spreading Sequence Design , 5th International Symposium on Communication Theory and Application, ISCTA, Ambleside, Inglaterra, julho 1999.

A Transformada Complexa de Hartley , Simpósio Brasileiro de Telecomunicações, Vila Velha, setembro 1999.

Revista

The Hartley Transform in a Finite Field
Número Especial da Revista da Sociedade Brasileira de Telecomunicações