A TRANSFORMADA NUMÉRICA DE HARTLEY E GRUPOS DE INTEIROS GAUSSIANOS

D. Silva, R. M. C. de Souza, , H. M. de Oliveira, L. B. E. Palma e M. M. C. de Souza

Resumo - Transformadas discretas desempenham um importante papel em Engenharia e suas aplicações devem-se principalmente à existência das chamadas transformadas rápidas. Especificamente, transformadas discretas definidas sobre corpos finitos são atraentes por não introduzirem erros de truncagem ou arredondamento, e por permitirem aplicações com aritmética de baixa complexidade. Neste artigo, a Transformada Numérica de Hartley (TNH) é introduzida e a partir da mesma a Transformada Numérica de Hartley-Mersenne é definida e algumas transformadas sem multiplicações são apresentadas. Algumas estruturas algébricas relacionadas com a Transformada de Hartley de Corpo Finito são estabelecidas e, em particular, os grupos dos módulos e das fases de um corpo finito são introduzidos, o que leva a uma representação polar dos elementos do corpo finito GF(p^2). Aplicações envolvendo a TNH são discutidas.

Palavras-Chave: Transformadas em corpos finitos, transformadas numéricas de Hartley, grupos de inteiros gaussianos.

Abstract - Finite field transforms are attractive since they do not introduce roundoff errors and, in many cases, can be implemented with a low computational complexity. In this paper, the Hartley Number-Theoretic Transform (HNTT) is introduced. In particular, the Mersenne HNTT is defined and some multiplication free transforms are given. Some algebraic structures that are related to the HNTT are introduced and, in particular, the group of modules and the group of phases of a finite field are defined, which allows the construction of a polar representation for the elements of the Galois field GF(p^2). A few applications involving the TNH are discussed.

Keywords: Finite field transforms, Hartley number theoretic transforms, groups of gaussian integers.

1. INTRODUÇÃO

Transformadas Discretas definidas sobre corpos finitos são ferramentas que, embora recentes, desempenham um papel importante em Engenharia. A transformada de Fourier em um corpo finito foi introduzida em [1] como uma ferramenta para efetuar convoluções discretas finitas usando aritmética inteira. Posteriormente, ela veio a ser utilizada em muitas outras aplicações, sobretudo nas áreas de Processamento Digital de Sinais, Teoria da Informação, Códigos Corretores de Erros e Criptografia [2-6]. Recentemente, a transformada de Hartley sobre corpos finitos foi introduzida em [7], [8], a qual apresenta propriedades de simetria que a tornam mais atraente, para diversas aplicações, que a transformada de Fourier de corpo finito, e tem importantes aplicações no campo da multiplexação digital [9], [10].

Transformadas em corpos finitos que mapeiam vetores de GF(p) em vetores de GF(p) e, portanto, empregam aritmética módulo p, são chamadas transformadas numéricas. Tais transformadas não provocam erros de arredondamento ou *overflow* e tem, em muitos casos de interesse prático, uma implementação em *hardware* simples. Um exemplo bem conhecido de tal transformada é a Transformada Numérica de Fourier [11].

Neste artigo, uma nova transformada numérica é introduzida, a Transformada Numérica de Hartley, e algumas estruturas algébricas finitas relacionadas com a mesma são discutidas. Em particular, os grupos dos módulos e das fases de um corpo finito são introduzidos e uma representação polar dos elementos do corpo finito GF(p^2) é proposta. Aplicações envolvendo a Transformada Numérica de Hartley são apresentadas. Na próxima seção são apresentados alguns fundamentos matemáticos que constituem ferramentas essenciais para os resultados contidos neste trabalho. Na Seção 3, as transformadas de Fourier e de Hartley de corpo finito são revistas e a TNH é definida usando-se os inteiros gaussianos sobre GF(p). Na Seção 4, as Transformadas Numéricas de Hartley-Fermat (TNHF) e Hartley-Mersenne (TNHM) são consideradas, onde são usados, respectivamente, os corpos finitos GF(2^s+1) e GF(2^s-1). Nesta seção algumas famílias de transformadas numéricas cuja implementação não requer multiplicações são construídas. Tais transformadas requerem apenas deslocamentos cíclicos, adições e subtrações para serem computadas, o que as torna atraentes para aplicações devido à sua baixa complexidade computacional. Na Seção 5 é introduzida a idéia de uma representação polar para corpos finitos. Isto requer uma nova definição de módulo que seja adequada para os elementos do corpo finito GF(p^2), a qual é obtida vinculando-se o módulo do elemento à condição de resíduo quadrático módulo p. Na Seção 6 o conceito de grupo unimodular é estendido e a estrutura algébrica denominada grupo supra-unimodular é definida e algumas de suas propriedades investigadas. Aplicações dos conceitos introduzidos são consideradas na Seção 7 no contexto das transformadas numéricas. A Seção 8 propõe um algoritmo

Os autores são do Grupo de Pesquisa em Comunicações - CODEC, Depto. de Eletrônica e Sistemas, UFPE, CP.7800, CEP 50711-970, Recife, PE. E-mails: lucianabeltrao@hotmail.com, {ricardo, hmo, marciam}@npd.ufpe.br, danilos@hotlink.com.br.
Editores responsáveis: Antonio Sérgio Bezerra Sombra e Max Gerken. Data de recebimento: 31/Dez/2001; data da revisão: 15/Mar/2002, data de aceitação: 8/Abr/2002.

para computar a TNH, após o que algumas conclusões são apresentadas na Seção 9.

2. FUNDAMENTOS MATEMÁTICOS

Esta seção apresenta uma breve introdução às principais ferramentas matemáticas usadas neste trabalho, os inteiros gaussianos e as funções *k*-trigonométricas, ambas definidas sobre corpos finitos.

2.1 INTEIROS GAUSSIANOS SOBRE CORPOS FINITOS

A estrutura algébrica GI(q) dos inteiros gaussianos sobre um corpo finito é construída a partir do processo de extensão de um corpo base, de forma análoga à extensão realizada pelos números complexos sobre o corpo dos números reais. As condições para a construção deste corpo de extensão impõem restrições importantes sobre a escolha da ordem do mesmo, como mostrado na definição a seguir.

Definição 1: G(q) := {$\zeta = a + jb$, $a, b \in$ GF(q)}, onde $q = p^r$, com $p \equiv 3$ (*mod* 4), r um inteiro ímpar e $j^2 = -1$, é o conjunto de Inteiros Gaussianos sobre GF(q).

Proposição 1: Sejam as operações $\oplus$ e *, definidas sobre os elementos de G(q), dadas por

$$\begin{aligned} \oplus : \mathrm{G}(q) \otimes \mathrm{G}(q) &\rightarrow \mathrm{G}(q) \\ (a_1 + jb_1 , a_2 + jb_2) &\rightarrow (a_1 + jb_1) \oplus (a_2 + jb_2) = \\ &\quad (a_1 + a_2) + j(b_1 + b_2) \end{aligned}$$

e

$$\begin{aligned} *: \mathrm{G}(q) \otimes \mathrm{G}(q) &\rightarrow \mathrm{G}(q) \\ (a_1 + jb_1 , a_2 + jb_2) &\rightarrow (a_1 + jb_1)*(a_2 + jb_2) = \\ &\quad (a_1a_2 - b_1b_2) + j(a_1b_2 + a_2b_1). \end{aligned}$$

A operação $\otimes$ denota o produto cartesiano. A estrutura GI(q) = <G(q) , $\oplus$, *> é um corpo isomorfo a GF(q^2) [11]. A aritmética descrita na Proposição 1 é análoga à aritmética dos números complexos.

2.2 AS FUNÇÕES *K*-TRIGONOMÉTRICAS

Esta seção apresenta uma definição de funções trigonométricas sobre corpos finitos, no sentido de que possuem propriedades semelhantes às das funções trigonométricas classicamente definidas. As famílias de funções $\cos_k(.)$ e $\mathrm{sen}_k(.)$ são inicialmente apresentadas e, a seguir, deriva-se destas funções básicas a família de funções $\mathrm{cas}_k(.)$ e o resultado principal desta seção, o Teorema 1. Este teorema fornece os elementos para a definição da transformada de Hartley em um corpo finito (Seção 3).

Definição 2: Seja ζ um elemento não nulo em GI(q), com $q = p^r$ e p é um primo ímpar da forma $4k + 3$. As funções *k*-trigonométricas de $\angle(\zeta^i)$ (arco do elemento ζ^i) em GI(q), são

$$\cos_k(\angle\zeta^i) := (\zeta^{ik} + \zeta^{-ik}) / 2 \text{ e}$$
$$\mathrm{sen}_k(\angle\zeta^i) := (\zeta^{ik} - \zeta^{-ik}) / 2j ,$$

onde $q = p^r$, ζ tem ordem N, $N \mid q^2-1$ e $i,k = 0, 1,..., N-1$.

Esta definição só faz sentido se GI(q) for um corpo, pois apenas nesta estrutura é garantida a existência de uma potência negativa do elemento ζ. Este é razão da exigência $p \equiv 3$ (*mod* 4).

Definição 3: Seja ζ um elemento não nulo em GI(q). A função $\mathrm{cas}_k(\angle\zeta^i)$ em GI(q), é

$$\mathrm{cas}_k(\angle\zeta^i) := \cos_k(\angle\zeta^i) + \mathrm{sen}_k(\angle\zeta^i)$$

A função $\mathrm{cas}_k(.)$, assim como no caso da trigonometria usual, é definida como a soma das funções seno e cosseno. As propriedades desta função *k*-trigonométrica, definida num corpo finito, são semelhantes às propriedades da função cas(q) definida sobre o corpo dos números reais. O teorema a seguir estabelece a ortogonalidade da função $\mathrm{cas}_k(.)$ [12].

Teorema 1:

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

onde $\zeta \in$ GI(q) tem ordem multiplicativa N.

3 A TRANSFORMADA NUMÉRICA DE HARTLEY

As chamadas transformadas numéricas de Fourier são ferramentas atraentes para diversas aplicações por apresentarem as mesmas propriedades básicas das transformadas discretas clássicas e permitirem, em muitos casos, implementações com complexidade computacional baixa. Nesta seção uma transformada numérica do tipo Hartley é introduzida.

Definição 4: Seja $f = (f_0 , f_1 , ... , f_{N-1})$ um vetor de comprimento N e componentes em GF(q), onde $q = p^r$. Então o vetor $F = (F_0 , F_1 , ... , F_{N-1})$, com componentes em GF($q^m$) dadas por

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

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

Quando $r = m = 1$, a transformação mapeia vetores com elementos em GF(p) e é chamada Transformada Numérica de Fourier (TNF). A TNF está restrita aos comprimentos N para os quais existe um elemento α de ordem N em GF(p), ou seja, N precisa ser um divisor de (p-1), o que nem sempre resulta em escolhas de interesse prático.

No que se segue, GI(q^m) denota o conjunto de inteiros gaussianos sobre GF(q^m), isto é, o conjunto dos inteiros da forma $a + jb$, onde $a, b \in$ GF(q^m) e $j \in$ GF(q^{2m}) é tal que $j^2 = -1$. Por analogia com os números complexos, os elementos de GI(q^m) são ditos complexos e os de GF(q^m), reais.

Definição 5: Seja $v = (v_0 , v_1 , ... , v_{N-1})$ um vetor de comprimento N com componentes em GF(q^m), onde $q=p^r$,

com r e m inteiros ímpares e $p \equiv 3$ (*mod* 4). Então o vetor $V = (V_0, V_1, \ldots, V_{N-1})$, com componentes em GI($q^m$), dadas por

$$V_k = \sum_{i=0}^{N-1} v_i cas_k(\mathbf{z}^i),$$

onde ζ é um elemento de ordem N em GI(q^m), é a Transformada de Hartley de Corpo Finito (THCF) de v. O núcleo da THCF é a função cas(.) em um corpo finito, definida na seção anterior.

A THCF é a versão de corpo finito da transformada discreta de Hartley (DHT) [13], a qual, por sua vez, corresponde à versão discreta da transformada integral simétrica introduzida por R. V. L. Hartley em 1942 [14]. 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 [15], [16], [17]. Transformadas rápidas de Hartley também existem e desempenham um papel importante no uso da DHT e da THCF [18].

Para se construir a TNH a partir da THCF, usa-se um procedimento diferente daquele empregado para a TNF. As Transformadas Numéricas de Hartley são obtidas a partir da Proposição 2 a seguir.

Proposição 2: Se $\zeta = a + jb$ é o argumento da função cas(.) empregada como núcleo na definição da THCF, então as componentes $V_k \in$ GF(p) (ou seja, são reais) se $a^2+b^2 \equiv 1$ (*mod p*).

Prova: Denotando ζ^{ik} por z, as funções seno e cosseno em um corpo finito podem ser reescritas, respectivamente, como

$$\cos_k(\zeta^i) = (z + z^{-1})/2 \text{ e } \mathrm{sen}_k(\zeta^i) = (z - z^{-1})/2j.$$

Se $a^2+b^2 \equiv 1 (mod\ p)$, então $z^{-1} = z^*$, onde $*$ denota o complexo conjugado. Isto resulta em $\cos_k(\zeta^i) = \Re\mathrm{e}(z)$ e $\mathrm{sen}_k(\zeta^i) = \Im\mathrm{m}(z)$, de modo que $cas_k(\zeta^i) = \mathrm{sen}_k(\zeta^i) + \cos_k(\zeta^i) = \Re\mathrm{e}(z) + \Im\mathrm{m}(z) \in$ GF(p) e a transformada tem apenas componentes reais.

A Proposição 2 mostra que é possível se obter uma THCF relacionando vetores com componentes em GF(p) apenas impondo uma condição sobre o núcleo $cas_k(\zeta^i)$ da transformada. Essa condição não é excessivamente restritiva em relação à escolha do núcleo, uma vez que se $\zeta = a+jb$ satisfaz a condição mencionada, então a mesma também é satisfeita para qualquer elemento do conjunto $\Gamma := \{b+ja, (p-a)+jb, b+j(p-a), a+j(p-b), (p-b)+ja, (p-a)+j(p-b), (p-b)+j(p-a)\}$, de modo que muitas escolhas são possíveis para ζ. A Tabela 1 a seguir lista algumas dessas escolhas para alguns valores de p.

Definição 6: Seja $v = (v_0, v_1, \ldots, v_{N-1})$ um vetor de comprimento N com componentes em GF(p), $p \equiv 3$ (*mod* 4). Então a Transformada Numérica de Hartley de v é o vetor $V = (V_0, V_1, \ldots, V_{N-1})$, com componentes em GF($p$) dadas por

$$V_k = \sum_{i=0}^{N-1} v_i cas_k(\mathbf{z}^i), \qquad (1)$$

onde $\zeta = a + jb$ é um elemento de ordem N em GI(p) satisfazendo $a^2+b^2 \equiv 1$ (*mod p*).

Teorema 2: A Transformada Numérica de Hartley inversa do vetor V é o vetor v de componentes em GF(p) dadas por

$$v_i = N^{-1} \sum_{k=0}^{N-1} V_k cas_k(\mathbf{z}^i) \ (mod\ p). \qquad (2)$$

p	$\zeta = a + jb$
3	2, j, 2j
7	j, 2+j2, 5+j2, 2+j5, 5+j5
11	3+j5, 5+j3, 8+j5, 5+j8, 3+j6, 6+j3, 8+j6, 6+j8
19	2+j4, 4+j2, 17+j4, 4+j17, 2+j15, 15+j2, 17+j15, 15+j17
19	3+j7, 7+j3, 16+j7, 7+j16, 3+j12, 12+j3, 16+j12, 12+j17
23	4+j10, 10+j4, 19+j10, 10+j19, 4+j13, 13+j4, 19+j13,
23	13+j19, 8+j12, 12+j8, 15+j12, 12+j15, 8+j11, 11+j8
23	15+j11, 11+j15, 9+j9, 14+j9, 9+j14, 14+j14
31	2+j20, 20+j2, 29+j20, 20+j29, 2+j11, 11+j2, 29+j11,
31	11+j29, 4+j4, 27+j4, 4+j27, 27+j27, 5+j21, 21+j5,
31	26+j21, 21+j26, 5+j10, 10+j5, 26+j10, 10+j21, 7+j13,
31	13+j7, 24+j13, 13+j24, 7+j18, 18+j7, 24+j18, 18+j24

Tabela 1. Alguns valores de $\zeta = a+jb$ satisfazendo a Proposição 2.

Prova: Substituindo V_k (expressão (1)) na expressão para v_i acima e denotando por v_i' o lado direito da expressão (2), tem-se

$$v_i' = N^{-1} \sum_{k=0}^{N-1} \sum_{t=0}^{N-1} v_t cas_k(\mathbf{z}^t) cas_k(\mathbf{z}^i) \ (mod\ p)$$

Invertendo a ordem dos somatórios,

$$v_i' = N^{-1} \sum_{t=0}^{N-1} v_t \sum_{k=0}^{N-1} cas_k(\mathbf{z}^t) cas_k(\mathbf{z}^i) \ (mod\ p)$$

Aplicando então a propriedade de ortogonalidade da função $cas_k(.)$ (Teorema 1), chega-se a (apenas o termo $t = i$ é selecionado do somatório) $v_i' = v_i$.

Um sinal v e seu espectro de Hartley V formam um par TNH denotado por $v \leftrightarrow V$. Por simplicidade, ζ é visto como um elemento fixo, de modo que, no que se segue, é usada a notação cas(ki) em substituição a $cas_k(\zeta^i)$.

Exemplo 1: Considerando $p = 3$, seja $\zeta = j$, um elemento de ordem 4 em GI(3). A matriz de transformação $cas_k(ki)$, i, k= 0, 1, 2, 3, é

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

que é a matriz de Hadamard permutada de ordem 4×4. Nesse caso, a transformada não requer multiplicações.

A TNF não permite enquadrar a transformada de Hadamard como uma transformada numérica, o que seria um resultado esperado. Entretanto, com a TNH isto é possível.

Exemplo 2: Uma TNH mapeando vetores com componentes em GF(7) pode ser construída escolhendo-se $\zeta = 5+j2$, um

elemento de ordem 8 em GI(7). A matriz de transformação $\mathrm{cas}_k(\zeta^i)$, $i, k = 0, 1, ...7$, é

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 4 & -1 & 0 & 1 & -4 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 4 & 1 & 0 & -1 & -4 & -1 & 0 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 0 & -1 & 4 & -1 & 0 & 1 & 4 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -4 & 1 & 0 & -1 & 4 & -1 & 0 \end{bmatrix}$$

Essa transformada tem comprimento N=8 e, portanto, pode ser computada através de um algoritmo rápido tipo Cooley-Tukey.

Das Proposições 3 e 4 abaixo, é possível determinar que valores para o comprimento N são possíveis para a TNH.

Definição 7: O conjunto unimodular de GI(p), denotado por G_1, é o conjunto dos elementos $\zeta = (a+jb) \in$ GI(p), tais que $a^2+b^2 \equiv 1 \ (mod\ p)$.

Proposição 3: Para ζ como na Proposição 2, tem-se :

$$z^{p+1} \equiv |z|^2 \equiv a^2 + b^2 (mod\ \mathrm{p}).$$

Prova: Pode-se escrever

$$z^p = (a + jb)^p \equiv a^p + j^p b^p (mod\ \mathrm{p}),$$

pois GI(p) é isomorfo a GF(p^2), um corpo de característica p. Como $p = 4k+3$, $j^p = -j$, de modo que

$$z^p \equiv a - jb\ (mod\ p) = z^*\ (mod\ p)$$

e portanto,

$$z^{p+1} \equiv zz^* = |z|^2 \equiv a^2 + b^2\ (mod\ p).$$

Proposição 4: A estrutura <G_1, *> é um grupo cíclico de ordem (p+1).

Prova: G_1 é fechado em relação a multiplicação, pois se ($a+jb$) e ($c+jd$) estão em G_1, isto é, se $a^2 + b^2 \equiv c^2 + d^2 \equiv 1$ ($mod\ p$), então

$$e + jf = (a + jb)(c + jd) = (ac - bd) + j(ad + bc),$$

de modo que

$$e^2 + f^2 = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2$$

$$= a^2(c^2 + d^2) + b^2(c^2 + d^2) \equiv a^2 + b^2 \equiv 1 (mod\ p),$$

e portanto $e+jf \in G_1$. Por outro lado, é um fato conhecido que o conjunto dos elementos não nulos de GF(q), juntamente com a operação de multiplicação do corpo, é um grupo cíclico de ordem (q-1) (denotado aqui por G) [19]. Portanto, sendo G_1 um subconjunto fechado de G, o mesmo é um subgrupo cíclico de G. Além disso, da proposição 2, $\zeta \in G_1$ satisfaz $\zeta^{p+1} \equiv 1$ ($mod\ p$) e ζ é uma das (p+1) raízes da unidade em GF(p^2). Existem (p+1) tais raízes e portanto G_1 tem ordem (p+1).

Exemplo 3: Os grupos unimodulares de GF(7^2) e GF(11^2). Em cada caso, a Tabela 2 lista os elementos dos subgrupos G_1 de ordem 8 e 12 dos grupos multiplicativos cíclicos dos elementos não nulos de GF(7^2) e GF(11^2), respectivamente, e suas ordens.

(a)

ζ	ordem
1	1
-1	2
j, $-j$	4
$2+j2$, $2+j5$, $5+j2$, $5+j5$	8

(b)

ζ	ordem
1	1
-1	2
$5+j3$, $5+j8$	3
j, $-j$	4
$6+j8$, $6+j3$	6
$8+j6$, $8+j5$, $3+j6$, $3+j5$	12

Tabela 2. Elementos dos grupos unimodulares de (a) GF(49) e (b) GF(121).

A Figura 1 ilustra as 12 raízes da unidade em GF(11^2). Observa-se que o subgrupo cíclico G_1 é isomórfico a C_{12}, o grupo das rotações próprias (no plano) de um polígono regular de 12 lados. Um elemento gerador é $\zeta=8+j6$, correspondente a uma rotação de $2\pi/12 = 30^o$ no sentido anti-horário. Os símbolos de mesma cor indicam elementos de mesma ordem, os quais ocorrem em pares complexos conjugados.

Da Proposição 4, conclui-se que os comprimentos possíveis para a TNH, dados pelos divisores da ordem de ζ, são os valores N que dividem (p+1).

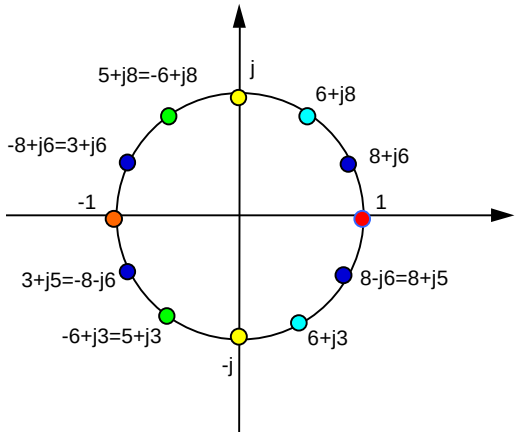

Figura 1. Raízes da unidade em GF(11^2) expressas como elementos de GI(11).

4. A TRANSFORMADA NUMÉRICA DE HARTLEY-MERSENNE (TNHM)

Alguns valores especiais de p originam classes específicas de transformadas numéricas. Assim, quando p é um primo de Fermat ou de Mersenne, as transformadas correspondentes são denominadas, respectivamente, Transformadas Numéricas de Hartley-Fermat (TNHF) ou Transformadas Numéricas de Hartley-Mersenne (TNHM).

No primeiro caso, p é um primo da forma 2^s+1, ou seja, $p\equiv 1$ (*mod* 4). Isso implica que -1 é um resíduo quadrático de p, o que significa que as estruturas GI(p) e GF(p) são as mesmas. Portanto, as TNHF são mapeamentos de GF(p) para GF(p), e seus comprimentos são os divisores de $p-1=2^s$. Assim, essas transformadas apresentam as mesmas características das Transformadas Numéricas de Fourier-Fermat, incluindo os comprimentos do tipo potência de 2.

Quando p é um primo de Mersenne, isto é, um primo da forma 2^s-1, tem-se $p\equiv 3$ (*mod* 4), de modo que as condições da Definição 2 são atendidas. As TNHM são de interesse especial porque os corpos finitos onde a operação de multiplicação é mais simples são aqueles da forma GF(2^s-1). Especificamente, se os inteiros nesse corpo são representados como s-uplas binárias, então como $2^s \equiv 1$ (*mod* 2^s-1), a aritmética em corpos finitos cuja ordem é um primo de Mersenne é a aritmética complemento a 1. Os comprimentos das TNH que podem ser usados em GF(p), quando p é um primo de Mersenne, são os divisores de $p+1=2^s$, ou seja, são as potências de 2: 2^s, 2^{s-1}, ...8, 4, 2. Assim, qualquer TNH em GF(2^s-1) pode ser computada através do algoritmo Cooley-Tukey de base 2. É interessante observar nesse ponto, que as Transformadas Numéricas de Fourier-Mersenne não podem ser calculadas por um algoritmo rápido tipo Cooley-Tukey, uma vez que $(2^s-1)-1$ não é uma potência de 2.

As Transformadas Numéricas de Hartley-Mersenne permitem, em alguns casos particulares, uma implementação com complexidade multiplicativa nula, o que é atraente do ponto de vista prático. Nesses casos, o núcleo da transformação inclui apenas os valores 0, 1 e -1, ou potências não triviais de 2. Nesse último caso, as multiplicações correspondem a deslocamentos cíclicos.

Proposição 5: Em GF(2^s-1), TNHMs de comprimento N=8, sem multiplicações, podem ser construídas com $z = a + jb = 2^{\frac{s-1}{2}} + j\,2^{\frac{s-1}{2}}$.

Prova*:* ζ é um núcleo válido pois

$$|z|^2 = a^2 + b^2 = 2^{s-1} + 2^{s-1} = 2^s \equiv 1 (mod\ p).$$

Além disso,

$$z^2 = 2^s\, j \equiv j\ (mod\ p),$$

de modo que, como j tem ordem 4, ζ tem ordem 8.

Exemplo 4: Em GF(31), o elemento $4+j4$ tem ordem 8. Usado como argumento da função cas(.), o mesmo gera uma TNHM de comprimento N=8. A Tab. 3 abaixo lista as potências de ζ e os valores correspondentes das funções cos(.), sen(.) e cas(.), onde se tem $\text{cas}(\zeta^i)=\Re\text{e}(\zeta^i)+\Im\text{m}(\zeta^i)$.

i	ζ^i	cos(.)=$\Re$e(ζ^i)	sen(.)=$\Im$m(ζ^i)	cas(.)
1	$4+j4$	4	4	8
2	j	0	1	1
3	$-4+j4$	-4	4	0
4	-1	-1	0	-1
5	$-4-j4$	-4	-4	-8
6	$-j$	0	-1	-1
7	$4-j4$	4	-4	0
8	1	1	0	1

Tabela 3. Elementos de uma TNHM em GF(31).

Na matriz de transformação, mostrada a seguir, os elementos não nulos são potências de 2, de modo que a TNHM pode ser computada apenas com deslocamentos cíclicos e adições/subtrações.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 8 & 1 & 0 & -1 & -8 & -1 & 0 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 0 & -1 & 8 & -1 & 0 & 1 & -8 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 0 & -1 & 4 & -1 & 0 & 1 & 4 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -4 & 1 & 0 & -1 & 4 & -1 & 0 \end{bmatrix}$$

Transformadas sem multiplicações podem ser construídas com outros tipos de primos, como mostra a proposição a seguir.

Proposição 6: Seja p um número primo da forma $p = 2^{2k}+3$, $k \geq 1$. Então $\zeta = 2^k + j2$ é uma raiz da unidade em GF(p).

Prova: Da proposição 2, $\zeta^{p+1} = |\zeta|^2 = 2^{2k} + 4 \equiv 1$ (*mod* $(2^{2k}+3)$).

Como os termos da forma ζ^{ik} envolvem apenas potências de 2, esse argumento do núcleo cas(.) pode ser usado para construir TNHs em GF(p) que envolvem apenas deslocamentos cíclicos e adições ou subtrações. A Tabela 4 a seguir lista alguns valores de k, p e ζ. Todos os elementos listados tem ordem $N=p+1$ em GI(p).

k	p	ζ
1	7	$2+j2$
2	19	$4+j2$
3	67	$8+j2$
6	4099	$64+j2$
8	65539	$256+j2$

Tabela 4. Alguns valores referentes a Proposição 6.

As transformadas indicadas nas Proposições 5 e 6 acima, representam famílias de soluções especiais do problema geral de se encontrar $\zeta = 2^u+j2^v$ em GI(p) satisfazendo a congruência $4^u+4^v\equiv 1$ (*mod* p). Outras soluções particulares que resultam em transformadas numéricas livres de multiplicações podem ser obtidas, e.g., para $\zeta = 2^4+j2^6$ em GI(19); $\zeta = 2^2+j2^7$ ou $\zeta = 2^5+j2^5$ em GI(23) [20].

5. FORMA POLAR PARA INTEIROS GAUSSIANOS EM CORPOS FINITOS

É um fato bem conhecido, na aritmética usual dos números complexos, que a chamada representação polar apresenta aspectos que a tornam atraente em muitas aplicações, principalmente quando as operações usuais de multiplicação e exponenciação estão presentes. Mantendo-se este mesmo ponto de vista, e objetivando-se a implementação de uma aritmética módulo p mais eficiente para a computação da TNH, uma representação polar para

os elementos do corpo finito GF(p^2) é proposta nesta seção. Inicialmente, a Definição 1 é reescrita considerando r =1, isto é, $p = q$.

Definição 8: O conjunto dos inteiros gaussianos sobre GF(p) é o conjunto G(p) = {$a + jb$, a, $b \in$ GF(p)}, onde p é um primo para o qual j^2 = -1 é um resíduo não-quadrático em GF(p). (Apenas os primos da forma $p \equiv 3$ (*mod* 4) satisfazem esse requisito [21]).

Na definição de GI(p) acima, os elementos são representados na forma $a + jb$, que é chamada de forma retangular. No que se segue, é proposta uma nova representação que permite escrever os elementos do grupo multiplicativo de GI(p) na forma $r\varepsilon^{\theta}$. Por analogia com o contínuo, esta representação será chamada de polar.

Proposição 7: Sejam G_A e G_B subgrupos do grupo multiplicativo G_C dos elementos não nulos de GI(p), de ordens N_A=(p-1)/2 e N_B=2(p+1), respectivamente. Todos os elementos de GI(p), com exceção do zero, podem ser escritos na forma ζ = AB, onde A $\in$ G_A e B $\in$ G_B.

Prova: Sendo G_C um grupo cíclico, então os subgrupos G_A e G_B de GI(p) existem, pois N_A e N_B são divisores de p^2-1, a ordem do grupo multiplicativo de GI(p). Além disso, o grupo G_C formado pelo produto direto entre os grupos G_A e G_B, tem ordem p^2-1, uma vez que, como p é da forma 4k+3, então o máximo divisor comum (MDC) entre N_A e N_B satisfaz

$$\mathrm{MDC}(N_A, N_B) = \mathrm{MDC}(2k+1, 4(2k+2)) = 1;$$

ou seja, o número de elementos de G_C, que é dado pelo mínimo múltiplo comum das ordens de G_A e G_B, é $|G_C|$ = mmc($|G_A|$, $|G_B|$) = $N_A N_B$ = p^2-1. Assim, G_C é o próprio grupo multiplicativo de GI(p), ou seja, todos os elementos deste último grupo podem ser escritos na forma ζ = AB, onde A $\in$ G_A e B $\in$ G_B.

Tendo em vista que qualquer elemento de um grupo cíclico pode ser escrito como potência de um elemento gerador desse grupo, podemos fazer r = A e ε^{θ} = B, onde ε é um gerador de G_B. Assim, a representação polar adquire a forma procurada, $\zeta = r\varepsilon^{\theta}$.

Antes de prosseguir com as propriedades da representação polar, é preciso introduzir o conceito de módulo de um elemento em um corpo finito. Considerando-se os elementos não nulos de GF(p), metade deles possui raiz quadrada e são chamados de resíduos quadráticos (RQ) de p [21]. Os que não possuem raiz quadrada são chamados de resíduos não-quadráticos (RNQ). Da mesma forma, no corpo infinito dos reais, os números são divididos em positivos e negativos, que são, respectivamente, os que possuem e os que não possuem raiz quadrada. A operação convencional de módulo, nos reais, produz sempre um resultado positivo. Por analogia, a operação de módulo em GF(p) é definida para que produza sempre um resíduo quadrático.

Definição 9: O módulo de um elemento de GF(p), onde p=4k+3, é dado por

$$|a| = \begin{cases} a, & se\ a^{\frac{p-1}{2}} \equiv 1 \pmod p \\ -a, & se\ a^{\frac{p-1}{2}} \equiv -1 \pmod p. \end{cases}$$

Proposição 8: O módulo de qualquer elemento de GF(p) é sempre um resíduo quadrático.

Prova: Como p=4k+3, tem-se que (p-1)/2=2k+1, e portanto $(-1)^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$. Pelo critério de Euler [21], se $a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$, então a é um RQ de p; se $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$, então a é um RNQ. Assim $(-a)^{\frac{p-1}{2}} \equiv (-1)(-1) \equiv 1 \ (mod\ p)$ e segue-se portanto que a é um RQ de p.

Definição 10: O módulo de um elemento de GI(p), onde p=4k+3, é dado por:

$$|a + jb| = \left|\sqrt{\left|a^2 + b^2\right|}\right|.$$

O módulo interior na expressão acima é necessário para que sempre se possa extrair a raiz quadrada da norma a^2+b^2 e o módulo exterior garante que essa operação fornece um único resultado apenas. No contínuo, essas expressões se reduzem às conhecidas, pois tanto a^2+b^2 quanto a operação de raiz quadrada fornecem apenas resíduos quadráticos.

Nesse ponto, podemos substituir G_A e G_B por denominações mais adequadas à representação polar.

Definição 11: O grupo dos módulos de GI(p), denotado por G_r, é definido como sendo o subgrupo de ordem (p-1)/2 de GI(p).

Definição 12: O grupo das fases de GI(p), denotado por G_θ, é definido como sendo o subgrupo de ordem 2(p+1) de GI(p).

Proposição 9: Se $\zeta = a + jb = r\varepsilon^{\theta}$, onde $r \in G_r$ e $\varepsilon^{\theta} \in G_\theta$, então $r = |\zeta|$.

Prova: Todos os elementos do grupo dos módulos (G_r) possuem ordem que divide (p-1)/2. Assim, se $r \in G_r$, então $r^{(p-1)/2} \equiv 1 \ (mod\ p)$, e portanto $|r| = r$. Além disso, como mostrado na seção seguinte, o grupo G_θ é formado pelos elementos $a + jb$ tais que $a^2 + b^2 \equiv \pm 1$ (*mod* p). Logo, de acordo com a Definição 10, o módulo desses elementos é igual a 1. Temos então que $|\zeta| = |r\varepsilon^{\theta}| = |r||\varepsilon^{\theta}| = r \cdot 1 = r$.

Uma expressão para a fase θ em função de a e b pode ser encontrada normalizando-se o elemento ζ (ou $\zeta/r = \varepsilon^{\theta}$), e em seguida resolvendo-se o problema do logaritmo discreto de ζ/r na base ε, que é viável para valores não muito elevados de p (valores com menos de 100 dígitos decimais, o que cobre a faixa de interesse prático). Assim, é possível a conversão da representação retangular para a polar. A

conversão inversa é feita simplesmente efetuando-se as potenciações.

Como se pode observar, a representação proposta é consistente com a representação polar no contínuo: o módulo r pertence a GF(p) (o módulo é um número real) e é um resíduo quadrático (número positivo), e a componente exponencial ε^{θ} ($e^{j\theta}$) tem módulo 1 e pertence a GI(p) ($e^{j\theta}$ pertence ao corpo dos complexos).

6. GRUPOS SUPRA-UNIMODULARES

É possível estender o grupo unimodular de GI(p), permitindo a inclusão de elementos satisfazendo $a^2 + b^2 \equiv -1$ ($mod\ p$).

Definição 13: O conjunto supra-unimodular de GI(p), denotado por G_S, é o conjunto dos elementos $\zeta = a + jb \in$ GI(p) tais que $(a^2 + b^2)^2 \equiv 1$ ($mod\ p$).

Proposição 10: Se $\zeta=a + jb$, então $\zeta^{2(p+1)} \equiv (a^2 + b^2)^2$ ($mod\ p$).

Prova: $\zeta^p = (a + jb)^p \equiv a^p + j^p b^p$ ($mod\ p$), pois GI(p) é isomorfo a GF(p^2), um corpo de característica p. Como p = $4k+3$, $j^p=-j$, de modo que $\zeta^p \equiv a - jb$ ($mod\ p$). Portanto, $\zeta^{p+1} \equiv (a + jb)(a - jb) \equiv a^2 + b^2$ ($mod\ p$). Assim, $\zeta^{2(p+1)} \equiv (a^2 + b^2)^2$ ($mod\ p$).

Proposição 11: A estrutura $<G_S,*>$, denominada supra-unimodular, é um grupo cíclico de ordem $2(p+1)$.

Prova: G_S é fechado em relação à multiplicação, pois se $(a+jb)$ e $(c+jd)$ estão em G_S, isto é, se

$$(a^2 + b^2)^2 \equiv (c^2 + d^2)^2 \equiv 1\ (mod\ p),$$

então como

$$e + jf = (a + jb)(c + jd) = (ac - bd) + j(ad + bc),$$

obtém-se

$$(e^2 + f^2)^2 = (a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2)^2 =$$

$$= ((a^2 + b^2)(c^2 + d^2))^2 = (a^2 + b^2)^2(c^2 + d^2)^2 \equiv 1\ (mod\ p),$$

e portanto $(e + jf) \in G_S$. Como G_S é um subconjunto fechado de um grupo cíclico (o grupo multiplicativo de GI(p)), G_S é um subgrupo cíclico. Além disso, da Proposição 10, $\zeta \in G_S$ satisfaz $\zeta^{2(p+1)} \equiv 1$ ($mod\ p$). Assim, ζ é uma das raízes $2(p+1)$-ésimas da unidade em GI(p). Existem $2(p+1)$ tais raízes e portanto G_S tem ordem $2(p+1)$.

Reconhece-se que, no grupo supra-unimodular, os elementos $\zeta = a + jb$ são tais que $(a^2 + b^2)^2 \equiv 1$ ($mod\ p$), ou seja, $a^2 + b^2 \equiv \pm 1$ ($mod\ p$), e portanto todos têm módulo, em GF(p), igual a 1, assim como no grupo unimodular. Porém, para preservar a definição já estabelecida e ressaltar que o mesmo possui ordem maior, o grupo de ordem $2(p+1)$ recebeu o nome de supra-unimodular. É importante observar que, devido ao fato de que um grupo cíclico não possui mais de um subgrupo distinto de mesma ordem [22], o grupo supra-unimodular é exatamente o grupo das fases definido na seção anterior.

O problema de se encontrar um elemento gerador do grupo supra-unimodular é tratado a seguir.

Proposição 12: Se p é um primo de Mersenne, isto é, um primo da forma $p = 2^n - 1$, então os elementos $\zeta=a + jb$ tais que $a^2 + b^2 \equiv -1$ ($mod\ p$) são geradores do grupo supra-unimodular de GI(p).

Prova: Seja N a ordem do elemento ζ. Como $a^2+b^2 \equiv -1$ ($mod\ p$), ζ é um elemento supra-unimodular, ou seja, N divide $2(p+1)=2^{n+1}$. Entretanto, pelo mesmo motivo, ζ não é unimodular, isto é, N não divide $p+1=2^n$. Dessa forma, $N = 2^{n+1} = 2(p+1)$, e portanto ζ é um gerador do grupo supra-unimodular.

Assim, se p for um primo de Mersenne, um elemento de ordem $2(p+1)$ em GI(p) pode ser encontrado da seguinte forma: escolhe-se um elemento aleatório de GI(p), divide-se este elemento por seu módulo, e por fim calcula-se sua norma (a^2+b^2). Se o resultado for -1, tem-se o elemento desejado; caso contrário, repete-se o processo.

7. APLICAÇÕES

Desde a introdução da transformada de Fourier em corpo finito, concebida inicialmente para auxiliar o cálculo de convoluções discretas, muitas outras aplicações da mesma foram propostas, não apenas nas áreas de processamento digital de sinais e imagem, mas também em diferentes contextos tais como codificação de canal e criptografia. Um outro exemplo relevante é a transformada de Hartley de corpo finito, a qual tem importantes aplicações no campo da multiplexação digital. Uma THCF de especial interesse é a chamada Transformada Numérica de Hartley, a qual é construída a partir de uma escolha apropriada do núcleo da THCF, escolha esta que resulta em uma transformada com componentes em GF(p). Dessa forma, não é necessário restringir o corpo de extensão a GF(p) para se obter uma transformada numérica, o que é feito para a Transformada Numérica de Fourier (TNF). Neste caso, isto significa que N, o comprimento da transformada, é um divisor de $(p^2-1) = (p-1)(p+1)$ e não apenas de $(p-1)$ como no caso da TNF. Assim, para um dado p, a TNH apresenta uma maior flexibilidade de aplicação em relação à TNF, uma vez que um número maior de escolhas para o valor de N, o comprimento da transformada, é possível.

Um caso particular de interesse prático da TNH é obtido quando p é um primo de Mersenne, isto é, um primo da forma $p=2^s-1$. As transformadas correspondentes, denominadas Transformadas Numéricas de Hartley-Mersenne, permitem implementações com complexidade multiplicativa nula, bem como comprimentos que permitem a utilização da FFT de Cooley-Tukey, algo que não é possível para a Transformada Numérica de Fourier.

Na definição da TNH (Definição 6), o elemento ζ, implícito na definição de cas(.), é um elemento unimodular de ordem N de GI(p). O valor de N é o comprimento da transformada. Assim, para implementar uma TNH de comprimento N, é necessário primeiramente encontrar um elemento unimodular de ordem N de GI(p). Se p é um primo de Mersenne, isto pode ser feito através do método descrito na seção anterior.

Exemplo 5: p = 11. Como p não é da forma 2^n-1, o método descrito não resulta necessariamente em geradores de G_S. Temos que $2(p+1) = 24$ e $(p+1) = 12$; assim, os elementos tais que $a^2+b^2 \equiv -1$ (*mod p*) possuem ordem 8 ou 24, pois ambos valores dividem 24 mas não dividem 12. Por exemplo, $3 + j$ tem ordem 24, enquanto $4 + 4j$ tem ordem 8, apesar de ambos possuírem norma igual a -1.

Exemplo 6: p = 31 (primo de Mersenne). Como $p = 2^5$-1, pode-se usar o método descrito. Escolhe-se aleatoriamente um elemento de GI(p), por exemplo, $\zeta = 9 + 11j$, após o que seu módulo é calculado através da Definição 3:

$$r = \left|\sqrt{\left|9^2 + 11^2\right|}\right| \equiv \left|\sqrt{|16|}\right| \equiv |4| \equiv 4 \ \ (mod\ p)\,.$$

Em seguida o elemento ζ é normalizado: $\varepsilon = \zeta/r = 10 + 26j$. Finalmente, sua norma é calculada: $a^2+b^2 = 10^2 + 26^2 \equiv 1$ (*mod* 31). Escolhendo-se um novo elemento, por exemplo, $\zeta = 6 + 16j$, tem-se que

$$r = \left|\sqrt{\left|6^2 + 16^2\right|}\right| \equiv \left|\sqrt{|13|}\right| \equiv \left|\sqrt{18}\right| \equiv |7| \equiv 7 \ \ (mod\ p)\,,$$

$\varepsilon = \zeta/r = 23 + 20j$ e $a^2+b^2 = 6^2 + 16^2 \equiv -1$ (*mod p*). Portanto, ε tem ordem $2(p+1) = 64$. Um elemento unimodular β de ordem N, tal que $N \mid 2^5$, pode ser encontrado fazendo-se $\beta = \varepsilon^{\frac{2(p+1)}{N}} = \varepsilon^{\frac{64}{N}}$. Por exemplo, $\beta = \varepsilon^2 = 5 + 21j$ é unimodular de ordem 32; e assim, pode ser usado como núcleo de uma TNH de comprimento 32.

8. A TNH RÁPIDA

Existe uma relação simples entre a TNF e a TNH, como mostrado na Proposição 13.

Proposição 13: Sejam $v = \{v_i\} \leftrightarrow H = \{H_k\}$ e $v = \{v_i\} \leftrightarrow F = \{F_k\}$ pares da transformada numérica de Hartley e de Fourier, respectivamente. Então

(i) $H_k = [(F_k + F_{N-k}) + j(F_{N-k} - F_k)]/2 = F_e - jF_o$.

(ii) $F_k = [(H_k + H_{N-k}) + j(H_k - H_{N-k})]/2 = H_e + jH_o$

onde F_e e F_o denotam as partes par e ímpar de F, respectivamente, e H_e e H_o denotam as partes par e ímpar de H, respectivamente.

Prova: (i) Da Definição 1

$$F_k = \sum_{i=0}^{N-1} v_i z^{\,ki}$$

e

$$F_{N-k} = \sum_{i=0}^{N-1} v_i z^{\,(N-k)i} = \sum_{i=0}^{N-1} v_i z^{\,-ki}\,,$$

de modo que,

$$(F_k + F_{N-k})/2 = \sum_{i=0}^{N-1} v_i (z^{\,ki} + z^{\,-ki})/2 = \sum_{i=0}^{N-1} v_i \cos(ki)$$

e

$$(F_{N-k} - F_k)/2j = \sum_{i=0}^{N-1} v_i (z^{\,ki} - z^{\,-ki})/2j = \sum_{i=0}^{N-1} v_i \,\mathrm{sen}(ki)$$

e assim, das Definições 3 e 5, o resultado segue.

(ii) De (i) tem-se que

$$H_{N-k} = [(F_k + F_{N-k}) + j(F_k - F_{N-k})]/2\,.$$

Assim,

$$H_k + H_{N-k} = F_k + F_{N-k}$$

e

$$H_k - H_{N-k} = j(F_{N-k} - F_k)\,.$$

Multiplicando-se por j a última expressão e adicionando-se o resultado à expressão para $H_k + H_{N-k}$, (ii) segue.

A Proposição 13 implica que qualquer algoritmo rápido para computar a TNH é também um algoritmo rápido para computar a TNF e vice-versa. Dessa forma, um esquema eficiente pode ser concebido para computar H através da Proposição 13. É necessário apenas computar F, a TNF de v, o que pode ser feito através de algum algoritmo FFT. Selecionadas as partes par (F_e) e ímpar (F_o) de F, o espectro TNH é dado diretamente por $H_k = F_e - jF_o$.

A TNH também pode ser computada diretamente adaptando-se, para corpos finitos [23], os algoritmos rápidos clássicos de Cooley-Tukey, Rader-Brenner, Good-Thomas e Winograd usados para computar a DHT [24], [25], [26]. Em particular, um algoritmo do tipo Cooley-Tukey base 2 com dizimação no tempo para computar uma TNH de comprimento N, requer uma complexidade computacional de ($N\log_2 N$-$3N$+4) multiplicações reais e ($3N\log_2 N$-$3N$+4) adições reais, ao invés das N^2 multiplicações reais e $N(N$-1) adições reais necessárias para o cálculo direto [26]. Além desses, um outro algoritmo baseado em uma decomposição em blocos de Hadamard foi proposto recentemente para o cálculo da THN, o qual atinge a complexidade multiplicativa mínima para vários comprimentos [27].

9. CONCLUSÕES

As Transformadas Numéricas de Fourier relacionam vetores com componentes em GF(p) e empregam aritmética módulo p. Embora com características interessantes sob o ponto de vista de sua implementação, seu comprimento é um divisor de (p-1), o que limita a escolha dos comprimentos possíveis. Neste trabalho, uma nova transformada, a Transformada Numérica de Hartley, foi introduzida. A TNH é obtida a partir da Transformada de Hartley de Corpo Finito, pela escolha judiciosa de seu núcleo $\mathrm{cas}_k(\zeta^i)$, escolha esta que resulta em uma transformada com componentes em GF(p). Dessa forma, não é necessário restringir o corpo de extensão a GF(p) para se obter uma transformada numérica, o que significa que N, o comprimento da transformada, é um divisor de (p-1)(p+1), de modo que, para um dado p, um número maior de escolhas para o valor de N é possível. Um caso particular de interesse prático é obtido quando p é um primo de Mersenne. As transformadas correspondentes, denominadas Transformadas Numéricas de Hartley-Mersenne, permitem implementações com complexidade multiplicativa nula, bem como comprimentos que permitem a utilização da FFT de Cooley-Tukey, algo que não é possível para a Transformada Numérica de Fourier, uma vez que 2^s-2 não admite potências não triviais de 2 como divisores. Um algoritmo rápido para a computação da Transformada Numérica de Hartley foi proposto.

Neste artigo, algumas estruturas algébricas finitas, relacionadas com a Transformada Numérica de Hartley e relevantes para sua concepção, são introduzidas. Em particular, os grupos dos módulos e das fases de um corpo finito são definidos e, através de uma nova definição de módulo, conveniente para os elementos de um corpo finito GI(*p*), uma representação polar dos elementos do corpo finito GI(*p*) é proposta pela primeira vez na literatura. Aplicações dos conceitos introduzidos são consideradas na construção de Transformadas Numérica de Hartley.

REFERÊNCIAS

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

[2] I. S. Reed and T. K. Truong, The Use of Finite Fields to Compute Convolutions, *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 208-213, Mar. 1975.

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

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

[5] R. M. Campello de Souza and P. G. Farrell, Finite Field Transforms and Symmetry Groups, *Discrete Math*, vol. 56, pp. 111-116, 1985.

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

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

[8] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, The Hartley Transform in a Finite Field, *Revista da Sociedade Brasileira de Telecomunicações*, vol. 14, No. 1, pp. 46-54, junho 1999.

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

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

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

[12] A. N. Kauffman, A Transformada de Hartley em um Corpo Finito*, Dissertação de Mestrado*, Programa de Pós-graduação em Engenharia Elétrica, Departamento de Eletrônica e Sistemas, UFPE, 1999.

[13] R. N. Bracewell, The Discrete Hartley Transform*, J. Opt. Soc. Amer*., vol. 73, pp. 1832-1835, Dec. 1983.

[14] R. V. L. Hartley, A More Symmetrical Fourier Analysis Applied to Transmission Problems, *Proc. IRE*, vol. 30, pp. 144-150, Mar. 1942.

[15] R. N. Bracewell, Aspects of the Hartley Transform, *IEEE Proc*., vol. 82, pp. 381-387, Mar. 1994.

[16] J.-L. Wu and J. Shiu, Discrete Hartley Transform in Error Control Coding, *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-39, pp. 2356-2359, Oct. 1991.

[17] I. Duleba, Hartley Transform in Compression of Medical Ultrasonic Images, *Proceedings of the 10th International Conference on Image Analysis and Processing*, 1998.

[18] C. L. Wang, and C. H. Chang, A Novel DHT-based FFT/IFFT Processor for ADSL Transceivers, *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 51-54, vol. 1, 1999.

[19] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1986.

[20] L. B. E. Palma, A Transformada Numérica de Hartley, *Dissertação de Mestrado*, Programa de Pós-graduação em Engenharia Elétrica, Departamento de Eletrônica e Sistemas, UFPE, 2000.

[21] D. M. Burton., Elementary Number Theory, Allyn and Bacon, 1976.

[22] J. R. Durbin, Modern Algebra: An Introduction, John Wiley, 1992.

[23] R. G. F. Távora, D. Silva, H. M. de Oliveira e R. M. Campello de Souza, On Fast Finite Field Hartley Transform Algorithms, *International Conference on Systems Engineering, Communication and Information Technology*, Punta-Arenas, Apr. 2001..

[24] H. V. Sorensen, D. L. Jones, C. S. Burrus e M. T. Heideman, On Computing the Hartley Transform, *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-33, pp. 1231-21238, Oct. 1985.

[25] M. N. Yatsimirskiy, A Radder-Brenner Fast Hartley Transformation, *Telecom. Radio Eng.*, vol. 47, pp. 106-110, 1992 (publicado originalmente em *Radiotekhnika*, vol. 1-2, pp. 66-70, 1992)

[26] D. P.-K. Lun, W. -C. Siu, On Prime Factor Mapping for the Discrete Hartley Transform, *IEEE Trans. on Signal Processing*, vol. 40, pp. 1399-1411, Jun. 1992.

[27] H. M. de Oliveira, R.G.F. Távora e R. M. Campello de Souza, Fast Finite Field Hartley Transform based on Hadamard Decomposition, *Sixth International Symposium on Communication Theory and Applications*, Ambleside, UK, Jul. 2001.

D. Silva é concluinte do Curso de Graduação em Engenharia Elétrica, modalidade Eletrônica, da Universidade Federal de Pernambuco. Seus interesses de pesquisa incluem processamento digital de sinais, processamento de voz e comunicação digital.

R. M. Campello de Souza formou-se em Engenharia Elétrica pela Universidade Federal de Pernambuco em 1974, obteve o título de Mestre em Ciências pela mesma Universidade em 1979 e o titulo de Ph.D. pela University of Manchester, Inglaterra, em 1983, ambos em Engenharia Elétrica. Desde 1979 é Professor do Departamento de Eletrônica e Sistemas da UFPE, onde foi coordenador do Programa de Pós-graduação em Engenharia Elétrica no período 1984-1987, Chefe do Departamento no período 1987-1992 e atualmente ocupa a posição de Professor Adjunto. Seus interesses de pesquisa incluem matemática discreta, criptografia, teoria algébrica da codificação e processamento digital de sinais.

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

L. B. E. Palma formou-se em Engenharia Elétrica, modalidade Eletrônica, pela Universidade Federal de Pernambuco em 1995, onde atuou como Professora Substituta no período 1996-1998 e obteve o título de Mestre em Ciências em Engenharia Elétrica em 2000. Atualmente cursa o Programa de Mestrado em Ciência Atuarial na City University, em Londres. Seus interesses de pesquisa incluem. processamento digital de sinais, estatística, probabilidade, atuária e administração pública.

M. M. Campello de Souza formou-se em Engenharia Elétrica pela Universidade Federal de Pernambuco em 1976 e obteve o título de Ph.D. pela University of Manchester, Inglaterra, em 1983, em Engenharia Elétrica. Desde 1988 é Professora do Departamento de Eletrônica e Sistemas da UFPE, onde foi Coordenadora do Curso de Graduação em Engenharia Elétrica/Eletrônica no período 1990-1992, Subchefe do Departamento no período 1992-1994 e atualmente ocupa a posição de Professora Adjunto. Seus interesses de pesquisa incluem matemática discreta, sistemas lineares e processamento digital de sinais.