TRANSFORMADAS NUMÉRICAS DE HARTLEY

R. M. CAMPELLO DE SOUZA, H. M. DE OLIVEIRA,
L. B. ESPINOLA PALMA E M. M. CAMPELLO DE SOUZA

CODEC - Grupo de Pesquisas em Comunicações,
Departamento de Eletrônica e Sistemas - UFPE,
Caixa Postal 7800, 50711 - 970, Recife - PE , Brasil,
E-mail: Ricardo@npd.ufpe.br, HMO@npd.ufpe.br, Palma@elogica.com.br, marciam@npd.ufpe.br

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 apresentarem uma aritmética de baixa complexidade. Neste artigo, a Transformada Numérica de Hartley (TNH) é introduzida. Em particular, a Transformada Numérica de Hartley-Mersenne é definida e algumas transformadas sem multiplicações são apresentadas. Um algoritmo rápido para computar a TNH é sugerido.

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 [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].

Transformadas em corpos finitos que mapeiam vetores de GF(p) em vetores de GF(p) e, portanto, empregam aritmética modulo p, são chamadas transformadas numéricas (TN). Tais transformadas não provocam erros de arredondamento ou *overflow* e tem, em muitos casos de interesse, uma implementação em *hardware* consideravelmente simples. Neste artigo, uma nova transformada numérica é introduzida, a Transformada Numérica de Hartley (TNH). Na próxima seção, a Transformada de Fourier de corpo finito é revista e a TNH é definida usando-se os inteiros gaussianos sobre um corpo finito. Na seção 3, 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 a sua baixa complexidade computacional. A seção 4 propõe um algoritmo eficiente para computar a TNH, após o que algumas conclusões são apresentadas na seção 5.

2. A TRANSFORMADA NUMÉRICA DE HARTLEY

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

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

onde α é um elemento de ordem N em GF(q^m), é a Transformada de Fourier em um Corpo Finito (TFCF) de f. Quando r = m = 1, a transformação mapeia vetores com elementos em GF(p) e é chamada Transformada Numérica de Fourier (TNF). Essa transformada apresenta aspectos atraentes em alguns casos, tais como baixa complexidade computacional e simplicidade de implementação. Entretanto, a TNF está restrita àqueles 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 2: Seja v = (v_0 , v_1 , ... , v_{N-1}) um vetor de comprimento N com componentes em GF(q), onde $q=p^r$, com r um inteiro ímpar e $p \equiv 3 \pmod 4$. Então o vetor V = (V_0, V_1 , ... , V_{N-1}), com componentes em GI(q^m) dadas por

$$V_k = \sum_{i=0}^{N-1} v_i \mathrm{cas}_k(\zeta^i),$$

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(.) (*cosine and sine*) em um corpo finito, definida por

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

onde

$$\cos_k(\zeta^i) = (\zeta^{ik} + \zeta^{-ik})/2$$

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

são as funções seno e cosseno definidas em um corpo finito [8]. ■

Para 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 1 a seguir.

Proposição 1: Se ζ=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 $a^2+b^2 \equiv 1 \pmod p$.

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

$$\cos_k(\zeta^i) = (z + z^{-1})/2$$

e

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

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

■

A proposição 1 mostra que é possível obter uma THCF relacionando vetores com componentes em GF(p) apenas impondo uma condição sobre o núcleo $\text{cas}_k(\zeta^i)$ da transformada. Essa condição não é excessivamente restritiva em relação à escolha do núcleo, uma vez que se ζ = a+jb satisfaz à condição mencionada, então a mesma também é satisfeita para qualquer elemento do conjunto Γ = {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.

TABELA I – Alguns valores de ζ = a+jb satisfazendo a proposição 1.

p	ζ = 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

A proposição 1 estabelece os elementos necessários para a definição da Transformada Numérica de Hartley.

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

$$V_k = \sum_{i=0}^{N-1} v_i \,\text{cas}_k(\zeta^i)\,,$$

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

Teorema 1: A Transformada Numérica de Hartley inversa do vetor V é o vetor v de componentes em GF(p) dadas por [8], [10]

$$v_i = \frac{1}{N \pmod p} \sum_{k=0}^{N-1} V_k \,\text{cas}_k(\zeta^i)\,.$$

Um sinal v e seu espectro de Hartley V formam um par TNH denotado por $v \leftrightarrow V$.

Exemplo 1: Considerando p = 3, seja $\zeta = j$, um elemento de ordem 4 em GI(3). A matriz de transformação $\text{cas}_k(\zeta^i)$, 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 $\text{cas}_k(\zeta^i)$, 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 2 e 3 abaixo, é possível determinar que valores para o comprimento N são possíveis para a TNH.

Definição 4: O conjunto unimodular de GI(p), denotado por G_1, é o conjunto dos elementos ζ = (a+jb) ∈ GI(p), satisfazendo $a^2+b^2 \equiv 1 \pmod p$.

Proposição 2: $\zeta^{p+1} \equiv |\zeta|^2 \equiv a^2 + b^2 \pmod p$.

Prova: $\zeta^p = (a + jb)^p \equiv a^p + j^p b^p \pmod p$, pois GI(p) é isomorfo a GF(p^2), um corpo de característica p. Como p = 4k+3,

$j^p = -j$, de modo que $\zeta^p \equiv a - jb \,(\text{mod}\, p) = \zeta^*(\text{mod}\, p)$. Portanto, $\zeta^{p+1} \equiv \zeta\zeta^* = |\zeta|^2 \equiv a^2 + b^2 \,(\text{mod}\, p)$. ■

Proposição 3: 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

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

$$= a^2(c^2 + d^2) + b^2(c^2 + d^2) \equiv$$

$$\equiv a^2 + b^2 \equiv 1 \,(\text{mod}\, p),$$

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) [11]. 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 $\zeta^{p+1} \equiv 1 \,(\text{mod}\, p)$ 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 II 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.

TABELA II - Elementos dos grupos unimodulares de (a) GF(49) e (b) GF(121).

(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

A Figura 1 ilustra as 12 raízes da unidade em $GF(11^2)$. Claramente, 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 ζ=8+j6, correspondente a uma rotação de $2\pi/12 = 30^0$ no sentido anti-horário. Os símbolos de mesma cor indicam elementos de mesma ordem, os quais ocorrem em pares complexos conjugados.

Da proposição 3, conclui-se que os comprimentos possíveis para a TNH, dados pelos divisores da ordem de ζ, são os valores N que dividem (p+1).

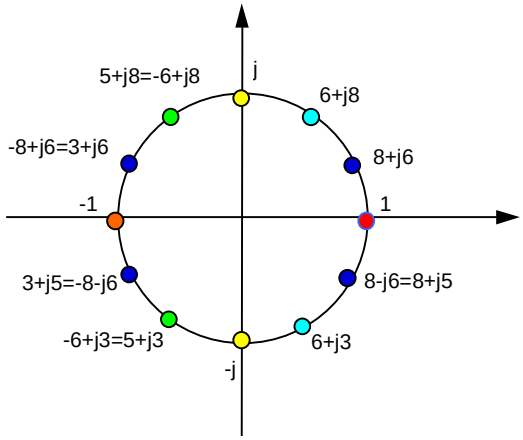

Fig. 1 - Raízes da unidade em $GF(11^2)$ expressas como elementos de GI(11).

3. 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≡1 (mod 4). Isso implica que $j^2 = -1$ 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 dois.

Quando p é um primo de Mersenne, isto é, um primo da forma 2^s-1, tem-se p≡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 $\zeta = a + jb = 2^{\frac{s-1}{2}} + j\,2^{\frac{s-1}{2}}$.

Prova: ζ é um núcleo válido pois

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

Além disso,

$$\zeta^2 = 2^s j \equiv j (\mathrm{mod}\, p),$$

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 tabela III abaixo lista as potências de ζ e os valores correspondentes das funções cos(.), sen(.) e cas(.), onde cas(ζ) = $\Re e(\zeta^i) + \Im m(\zeta^i)$.

TABELA III - Elementos de uma TNHM em GF(31).

i	ζ^i	cos(.)=$\Re e(\zeta^i)$	sen(.)=$\Im m(\zeta^i)$	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

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 raíz 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 IV a seguir lista alguns valores de k, p e ζ. Os elementos listados tem todos ordem N=p+1 em GI(p).

TABELA IV - Alguns valores referentes a proposição 6.

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

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 GF(19); $\zeta = 2^2 + j2^7$ ou $\zeta = 2^5 + j2^5$ em GF(23), etc.

4. COMPUTANDO A TNH

Existe uma relação simples entre as transformadas de corpo finito de Fourier e de Hartley, como mostrado na proposição 7.

Proposição 7: Sejam $v = \{v_i\} \leftrightarrow V = \{V_k\}$ e $v = \{v_i\} \leftrightarrow F = \{F_k\}$ pares da Transformada de Corpo Finito de Hartley e de Fourier, respectivamente. Então

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

(ii) $F_k = [(V_k + V_{N-k}) + j(V_k - V_{N-k})]/2 = V_e + jV_o$

onde F_e e F_o denotam as partes par e ímpar de F, respectivamente, e V_e e V_o denotam as partes par e ímpar de V, respectivamente.

Prova: (i) Da definição 1

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

e

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

de modo que,

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

e

$$(F_{N-k} - F_k)/2j = \sum_{i=0}^{N-1} v_i (\zeta^{ki} - \zeta^{-ki})/2j = \sum_{i=0}^{N-1} v_i sen_k(\zeta^i)$$

e, da definição 3, o resultado segue. ■

(ii) De (i) tem-se que $V_{N-k} = [(F_k + F_{N-k}) + j(F_k - F_{N-k})]/2$. Assim, $V_k + V_{N-k} = F_k + F_{N-k}$ e $V_k - V_{N-k} = j(F_{N-k} - F_k)$. Multiplicando por j a última expressão e adicionando o resultado à expressão para $V_k + V_{N-k}$, (ii) segue. ■

Alguns casos especiais são de interesse. Um espectro $V = \{V_k\}$ é dito ter simetria par se $V_k = V_{N-k}$, e simetria ímpar se

$V_k = V_{N-k}$, k = 0. 1, ..., N-1. Com esta terminologia, a proposição 7 implica que ($\Leftrightarrow$ significa *se e só se*)

$$F \text{ é par } \Leftrightarrow V \text{ é real e par,}$$

$$F \text{ é ímpar } \Leftrightarrow V \text{ é imaginário e ímpar.}$$

A proposição 7 implica que qualquer algoritmo rápido para computar $V = \{V_k\}$ é também um algoritmo rápido para computar $F = \{F_k\}$ e vice-versa. Dessa forma um esquema eficiente pode ser concebido para computar V, através da proposição 7 (i). É necessário apenas computar F, a TFCF de v, o que pode ser feito através de algum algoritmo FFT (Transformada Rápida de Fourier). Selecionadas as partes par (F_e) e ímpar (F_o) de F, o espectro TNH é dado diretamente por $V_k = F_e - jF_o$.

5. 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 $cas_k(\zeta^i)$, 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.

AGRADECIMENTOS

Os autores agradecem a A. N. Kauffman da Nortel Networks por valiosas sugestões e comentários.

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 Mathematics, 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] 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.

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

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

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

[14] R. N. Bracewell, *The Hartley Transform*, Oxford University Press, 1986.

[15] 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.

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

[17] H. M. de Oliveira, R. M. Campello de Souza and A. N. Kauffman, *A Transformada Complexa de Hartley em um Corpo Finito*, Simpósio Brasileiro de Telecomunicações, Vitória-ES, set. 1999.