A Transformada Complexa de Hartley em um Corpo Finito

R. M. Campello de Souza, H. M. de Oliveira, A. N. Kauffman

CODEC - Grupo de Pesquisa em Comunicações
Departamento de Eletrônica e Sistemas - CTG - UFPE
C.P. 7800, 50711 - 970, Recife - PE , Brasil
E-mail: Ricardo@npd.ufpe.br , HMO@npd.ufpe.br, ANK@nlink.com.br

Abstract - ***Transformadas discretas, definidas sobre corpos finitos ou infinitos, desempenham um importante papel em Engenharia. Em qualquer caso, a aplicação de transformadas deve-se principalmente à existência das chamadas transformadas rápidas. Neste artigo, a transformada complexa de Hartley em um corpo finito é introduzida e um algoritmo rápido para computá-la é sugerido.***

1. INTRODUÇÃO

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 [1] e aplicada como uma ferramenta para efetuar convoluções discretas usando aritmética inteira. 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) [2], a versão discreta da transformada integral simétrica introduzida por R. V. L. Hartley em 1942 [3]. 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 [4]. Transformadas rápidas de Hartley também existem e desempenham um papel importante no uso da DHT.

Recentemente, uma nova transformada de Hartley sobre corpos finitos (a FFHT - *Finite Field Hartley Transform*) foi introduzida [5], a qual tem aplicações interessantes na área de multiplexação digital [6]. Entretanto, a FFHT tem a restrição de não permitir comprimentos que são uma potência de 2, um valor de grande interesse prático. Neste trabalho a transformada complexa de Hartley sobre um corpo finito (CFFHT) é definida. O uso de um inteiro gaussiano sobre um corpo finito como argumento para o núcleo da transformada remove a restrição em comprimento da FFHT. O novo núcleo da transformada é expresso em forma matricial e algumas simetrias são detetadas. A condição de espectros válidos semelhante às restrições das classes de elementos conjugados da Transformada de Fourier de corpo finito é estabelecida e um algoritmo eficiente para computar a CFFHT é apresentado.

No que se segue ζ denota um elemento de ordem multiplicativa N em GI(q), o conjunto de inteiros gaussianos sobre o campo de Galois GF(q), $q = p^r$, p um primo ímpar tal que $p \equiv 3 \pmod 4$. A função cas (*cosine and sine*) de $(\angle \zeta^i)$ é definida como (o símbolo := significa *igual por definiçao)*

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

onde

$$\cos_k(\angle\zeta^i) := \frac{1}{2}(\zeta^{ik} + \zeta^{-ik})$$

e

$$\sin_k(\angle\zeta^i) := \frac{1}{2j}(\zeta^{ik} - \zeta^{-ik}),$$

para i, k = 0, 1,..., N-1. Por simplicidade ζ é considerado como sendo um elemento fixo. Denota-se $\mathrm{cas}_k(\angle\zeta^i)$ por $\mathrm{cas}_k(i)$. O conjunto $\{\mathrm{cas}_k(.)\}_{k=0,\,1,\ldots,\,N-1}$ pode ser visto como um conjunto de sequências que satisfazem a seguinte condição de ortogonalidade:

Teorema 1 -

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

2. UMA NOVA TRANSFORMADA DE HARTLEY

Seja $v = (v_0\,,\ v_1\,,\ \ldots\,,\ v_{N-1})$ um vetor de comprimento N com componentes em GF(q). A

Transformada Complexa de Hartley de Corpo Finito de v é o vetor $V = (V_0, V_1, \ldots, V_{N-1})$ de componentes $V_k \in GI(q^m)$, dadas por

$$V_k := \sum_{i=0}^{N-1} v_i \, cas_k(\angle \zeta^i)$$

onde ζ um elemento especificado de ordem multiplicativa N em $GI(q^m)$.

Tal definição estende a definição da Transformada de Hartley de Corpo Finito. Existe uma analogia interessante entre o núcleo $cas_k(i)$ da CFFHT e o núcleo $e^{j\frac{2\pi}{N}ki}$ da DFT, no sentido de que para um valor fixo $k = k_0$, ambas tem espectro dado por $N\delta[k - k_0]$. A CFFHT inversa é dada pelo seguinte teorema:

Teorema 2 - O vetor N-dimensional v pode ser recuperado de seu espectro V de acordo com

$$v_i = \frac{1}{N(\mathrm{mod}\, p)} \sum_{k=0}^{N-1} V_k cas_k(\angle \zeta^i).$$

Um sinal v e seu espectro de Hartley V formam um par transformado complexo de Hartley de corpo finito, denotado por $v \leftrightarrow V$. A título de ilustração seja $\zeta = \alpha^{198}$, um elemento de ordem 11 em $GF(3^5)$, α sendo um elemento primitivo no mesmo corpo. Os vetores v e V dados abaixo formam um par CFFHT :

$$v = (0,1,0,2,0,0,0,0,1,0,2) \leftrightarrow V = (0, j\alpha^{171}, j\alpha^{208}, j\alpha^{29}, j\alpha^{57}, j\alpha^{19}, j\alpha^{140}, j\alpha^{178}, j\alpha^{150}, j\alpha^{87}, j\alpha^{50}).$$

Como exemplo simples de uma CFFHT de comprimento uma potência de 2 (N = 4), seja $\zeta = j$, um elemento de ordem 4 em GI(3). O sinal no domínio do tempo v = (1,0,2,1) tem espectro V = (1,1,2,0).

A CFFHT pode ser expressa em forma matricial V = Tv, onde

$$T := \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & cas_1(1) & cas_1(2) & \ldots & cas_1(N-1) \\ 1 & cas_2(1) & cas_2(2) & \ldots & cas_2(N-1) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & cas_{N-1}(1) & cas_{N-1}(2) & \ldots & cas_{N-1}(N-1) \end{bmatrix}$$

A fim de explorar as simetrias existentes na CFFHT, seja T' a matriz obtida a partir de T pela remoção da primeira linha e da primeira coluna, i.e.,

$$T' := \begin{bmatrix} cas_1(1) & cas_1(2) & \ldots & cas_1(N-1) \\ cas_2(1) & cas_2(2) & \ldots & cas_2(N-1) \\ \ldots & \ldots & \ldots & \ldots \\ cas_{N-1}(1) & cas_{N-1}(2) & \ldots & cas_{N-1}(N-1) \end{bmatrix}$$

Considerando que (i) T' é uma matriz simétrica, (ii) T' é também simétrica com respeito à diagonal secundária e em função das propriedades de simetria complementares da função cas(.) [5], resulta que toda a informação contida em T' está representada pela área mostrada na fig.1(iii), onde a forma quadrada representa T'.

(i) (ii) (iii)

Fig.1 - Simetrias da matriz de transformação

3. ESPECTROS VÁLIDOS

A proposição 1 a seguir estabelece uma relação que precisa ser satisfeita pelas componentes do spectrum V

$$V_k^q = V_{N-kq}$$

para o mesmo ser um espectro CFFHT valido, isto é, um espectro de um sinal v com componentes em GF(q).

Proposição 1: O vetor $V = \{V_k\}$, $V_k \in GI(q^m)$, é o espectro de um sinal $v = \{v_i\}$, $v_i \in GF(q)$, se e só se

onde os índices são considerados módulo N, i, k = 0, 1, ..., N-1 e $N \mid (q^m - 1)$. A partição em classes laterais ciclotômicas induzidas por esta relação é tal que um elemento e seu recíproco módulo N pertencem à mesma classe. Isto implica que o número de componentes da CFFHT que precisa ser computado de modo a especificar inteiramente o espectro V é aproximadamente metade do número necessário para a transformada de Fourier de corpo finito.

4. COMPUTANDO A CFFHT

Uma transformada bem conhecida definida sobre corpos finitos é a transformada de Fourier de corpo finito (FFFT) [1]. Seja $v = (v_0, v_1, \ldots, v_{N-1})$ um vetor de comprimento N com componentes em $GF(q) \subset GI(q)$, $q = p^r$. A FFFT de v é o vetor $F = (F_0, F_1, \ldots, F_{N-1})$ de componentes $F_k \in GF(q^m) \subset GI(q^m)$, dadas por

$$F_k := \sum_{i=0}^{N-1} v_i \alpha^{ki}.$$

onde α é um elemento especificado de ordem multiplicativa N em $GF(q^m)$. Existe uma relação entre a FFFT e a CFFHT, como mostrado na proposição 2.

Proposição 2 - Sejam $v = \{v_i\} \leftrightarrow V = \{V_k\}$ e $v = \{v_i\} \leftrightarrow F = \{F_k\}$ pares CFFHT e FFFT, respectivamente. Então

$$V_k = \frac{1}{2}[(F_k + F_{N-k}) + j(F_{N-k} - F_k)] =$$
$$= F_e + jF_o$$

onde F_e e F_o denotam as partes par e ímpar de F, respectivamente. Alguns casos especiais são de interesse. Um espectro $F = \{F_k\}$ é dito ter simetria par se $F_k = F_{N-k}$ e simetria ímpar se $F_k = -F_{N-k}$, k = 0. 1, ..., N-1. Com esta terminologia, a proposição 2 implica que

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

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

Um esquema eficiente pode ser concebido para computar V como mostrado abaixo. É necessário apenas computar a FFFT de v o que pode ser feito via um algoritmo FFT.

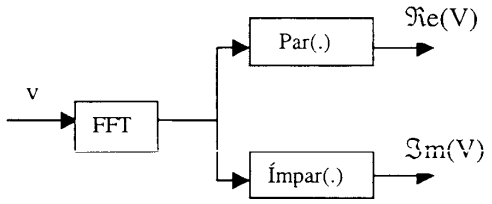

Fig. 2 - Computando a CFFHT

A existência de algoritmos rápidos (FFT) para computar a CFFHT é um fator decisivo para que a mesma possa ser considerada para aplicações em tempo real tal como multiplexação digital.

5. CONCLUSÕES

Neste artigo, uma nova transformada de Hartley, a Transformada Complexa de Hartley em um Corpo Finito (CFFHT), foi introduzida. As condições de simetria verificadas pelas componentes de um espectro CFFHT válido foram estabelecidas. Um algoritmo rápido para computação da CFFHT foi sugerido, o qual se baseia no cálculo da transformada de Fourier de corpo finito através de um algoritmo FFT. A CFFHT parece ter aplicações interessantes em diversas áreas. Especificamente, seu uso em Processamento Digital de Sinais no contexto de transformadas numéricas (e.g. transformadas de Mersenne e Fermat) deve ser investigado. Na área de codificação de canal, a CFFHT pode ser usada para descrever códigos para controle de erros no domínio da freqüência. Outras aplicações podem incluir multiplexação digital e espalhamento espectral baseado em transformadas discretas.

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

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

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

[5] 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.

[6] 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.