The Complex Finite Field Hartley Transform

R. M. Campello de Souza, H. M. de Oliveira, A. N. Kauffman
CODEC - Communications Research Group
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

Abstract - Discrete transforms, defined over finite or infinite fields, play a very important role in Engineering. In either case, the successful application of transform techniques is mainly due to the existence of the so-called fast transform algorithms. In this paper, the complex finite field Hartley transform is introduced and a fast algorithm for computing it is suggested.

1. Introduction

Discrete transforms are a very important tool and play a significant role in Engineering. A particularly striking example is the well known Discrete Fourier Transform (DFT), which has found many applications in several areas, specially in the field of Electrical Engineering. A DFT over Galois fields was also defined [1] and applied as a tool to perform discrete convolutions using integer arithmetic. Since then several new applications of the Finite Field Fourier Transform (FFFT) have been found, not only in the fields of digital signal and image processing, but also in different contexts such as error control coding and cryptography. In both cases, infinite and finite, the existence of fast algorithms (FFT) for computing the DFT has been a decisive factor for its real-time applications. Another interesting example is the Discrete Hartley Transform (DHT) [2], the discrete version of the symmetrical, Fourier-like, integral transform introduced by R. V. L. Hartley in 1942 [3]. Although seen initially mainly as a tool with applications only on the numerical side and having connections to the physical world only via the Fourier transform, the DHT has proven over the years to be a very useful instrument with many interesting applications [4]. Fast Hartley transforms also do exist and play an important role in the use of the DHT.

Recently, a new Hartley transform over finite fields (FFHT) was introduced [5] which has interesting applications in the field of digital multiplexing [6]. However, the FFHT has the restriction that it does not allow blocklengths that are a power of two. In this paper, the complex finite field Hartley transform (CFFHT) is defined. The use of a Galois field gaussian integer argument for the transform kernel removes the blocklength restriction of the FFHT. The new transform kernel is expressed in matrix form and some symmetries are detected. The condition for valid spectra, similar to the conjugacy constraints for the FFFT is given and an efficient algorithm for computing the CFFHT is presented.

In what follows ζ denotes an element of multiplicative order N in GI(q), the set of gaussian integers over GF(q), $q = p^r$, p an odd prime such that $p \equiv 3 \pmod 4$. The cas (cosine and sine) function of $\angle(\zeta^i)$ (by analogy, the cas functions of k times the ″angle″ of the ″complex exponential″ ζ^i) is defined as (the symbol := denotes *equal by definition*)

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

where

$$\cos_k(\angle\zeta^{\,i}) := \frac{1}{2}\left(\zeta^{\,ik} + \zeta^{\,-ik}\right) \quad \text{and} \quad \sin_k(\angle\zeta^{\,i}) := \frac{1}{2j}\left(\zeta^{\,ik} - \zeta^{\,-ik}\right),$$

for i , k = 0, 1,..., N-1. For simplicity ζ is supposed to be fixed.We write $\mathrm{cas}_k(\angle\zeta^{\,i})$ as $\mathrm{cas}_k(i)$. The set $\{\mathrm{cas}_k(.)\}_{k=0,\,1,\ldots,\,N-1}$ may be viewed as a set of sequences that satisfy the following orthogonality property:

Theorem 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. The Complex Finite Field Hartley Transform

Let $v = (v_0 , v_1 , ... , v_{N-1})$ be a vector of length N with components over GF(q). The Complex Finite Field Hartley Transform (CFFHT) of v is the vector $V = (V_0 , V_1 , ... , V_{N-1})$ of components $V_k \in GI(q^m)$, given by

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

where ζ is a specified element of multiplicative order N in $GI(q^m)$.

Such a definition extends the definition of the Finite Field Hartley Transform . The inverse CFFHT is given by the following theorem.

Theorem 2: The N-dimensional vector v can be recovered from its spectrum V according to

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

A signal v and its discrete Hartley spectrum V are said to form a complex finite field Hartley transform pair, denoted by $V = \mathcal{H} v$ or $v \leftrightarrow V$. As an illustration let $\zeta = \alpha^{198}$, an element of order 11 in $GF(3^5)$, α being a primitive element in the same field. The vectors v and V given below form a CFFHT pair:

$$V=(01020000102) \leftrightarrow V=(0\ j\alpha^{171}\ j\alpha^{208}\ j\alpha^{29}\ j\alpha^{57}\ j\alpha^{19}\ j\alpha^{140}\ j\alpha^{178}\ j\alpha^{150}\ j\alpha^{87}\ j\alpha^{50})$$

As a naive example of a CFFHT of blocklength a power of two (N = 4), let $\zeta = j$, an element of order 4 in GI(3). The time domain v=(1021) has spectru V=(1120).

3. Conjugacy Constraints

Proposition 1 states a relation that must be satisfied by the components of the spectrum V for it to be a valid finite field Hartley spectrum, that is, a spectrum of a signal v with GF(q)-valued components.

Proposition 1: The vector $V = \{V_k\}$, $V_k \in GI(q^m)$, is the spectrum of a signal $v = \{v_i\}$, $v_i \in GF(q)$, if and only if

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

where indexes are considered modulo N, i, k = 0, 1, ..., N-1 and $N \mid (q^m - 1)$. The cyclotomic coset partition induced by this relation is such that an element and its reciprocal modulo N belongs to the same class, which implies that the number of CFFHT components that need to be computed to completely spcify the spectrum V is approximately half of the number needed for the FFHT.

4. Computing the CFFHT

A well known transform defined over finite fields is the Finite Field Fourier Transform (FFFT) [1]. Let $v = (v_0 , v_1 , ... , v_{N-1})$ be a vector of length N with components over $GF(q) \subset GI(q)$, $q = p^r$. The FFFT of v is the vector $F = (F_0 , F_1 , ..., F_{N-1})$ of components $F_k \in GF(q^m) \subset GI(q^m)$, given by

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

where α is a specified element of multiplicative order N in $GF(q^m)$. There is a close relation between the FFFT and the FFHT, as it is shown in proposition 2.

Proposition 2 - Let $v = \{v_i\} \leftrightarrow V = \{V_k\}$ and $v = \{v_i\} \leftrightarrow F = \{F_k\}$ denote, respectively, a CFFHT and an FFFT pair. Then

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

where F_e and F_o denote the even and odd parts of F respectively. Based on this result an efficient scheme can be devised to compute V as shown below. It is necessary only to compute the FFFT of v which can be done via a Fast Fourier Tranasform algorithm.

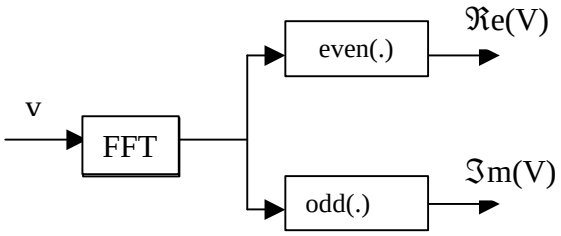

Fig. 2 - Computing the CFFHT

The existence of fast algorithms (FFT) for computing the CFFHT is a decisive factor for its real-time applications such as digital multiplexing, which makes it atractive for DSP implementations.

5. References

[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, August 1999.

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