THE HARTLEY TRANSFORM IN A FINITE FIELD

R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman
CODEC - Grupo de Pesquisas em Comunicações
Departamento de Eletrônica e Sistemas - CTG - UFPE
C.Postal 7800, 50711 - 970, Recife - PE , Brasil
Phone: +55 xx 81 2718210 fax:+55 xx 81 2718215
{Ricardo, HMO}@npd.ufpe.br, kauffman@nortelnetworks.com

Resumo – Neste artigo definem-se funções k-trigonométricas sobre um corpo de Galois GF(q) e analisam-se suas principais propriedades. Isto leva a definição de função $cas_k(.)$ sobre GF(q) e consequentemente, a transformada de Hartley em campos finitos. As principais propriedades desta nova transformada finita são apresentadas e possíveis aplicações são mencionadas.

Abstract - In this paper, the k-trigonometric functions over the Galois Field GF(q) are introduced and their main properties derived. This leads to the definition of the $cas_k(.)$ function over GF(q), which in turn leads to a finite field Hartley Transform. The main properties of this new discrete transform are presented and areas for possible applications are mentioned.

Keywords - Finite field trigonometry, Galois fields, Hartley transform.

1. INTRODUCTION

Discrete transforms play a very important role in engineering. A significant example is the well known Discrete Fourier Transform (DFT), which has found many applications in several areas, specially in electrical engineering. A DFT for finite fields was introduced by Pollard in 1971 [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 [2-5], but also in different contexts such as error control coding and cryptography [6-8].

A second relevant example concerns the Discrete Hartley Transform (DHT) [9], the discrete version of the integral transform introduced by R. V. L. Hartley in [10]. Although seen initially 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 [11-13].

In this paper the DHT over a finite field is introduced. In order to obtain a transform that holds some resemblance with the DHT, it is firstly necessary to establish the equivalent of the cosine and sine functions over a finite structure. Thus, in the next section, the k-trigonometric functions cos_k and sin_k are defined from which the cas_k (cosine and sine) function is obtained and used, in section 3, to introduce a symmetrical discrete transform pair, the finite field Hartley transform, or FFHT for short. A number of properties of the FFHT is presented, including the cyclic convolution property and Parseval's relation. In section 4, the condition for valid spectra, similar to the conjugacy constraints for the Finite Field Fourier Transform, is given. Section 5 contains a few concluding remarks and some possible areas of applications for the ideas introduced in the paper. The FFHT presented here is different from an earlier proposed Hartley Transform in finite fields [14] and appears to be the more natural one.

2. K-TRIGONOMETRIC FUNCTIONS

The set G(q) of gaussian integers over the Galois field GF(q) defined below plays an important role in the ideas introduced in this paper (hereafter the symbol := denotes *equal by definition*).

Definition 1. *$G(q) := \{a + jb\ ,\ a, b \in GF(q)\}$, $q = p^r$, r being a positive integer, p being an odd prime for which $j^2 = -1$ is a quadratic non-residue in GF(q), is the set of gaussian integers over GF(q).*

Let $\otimes$ denote the cartesian product. It can be shown, as indicated below, that the set G(q) together with the operations $\oplus$ and $*$ defined below, is a field.

Proposition 1 : Let

$$\oplus : G(q) \otimes G(q) \rightarrow G(q)$$
$$(a_1 + jb_1\ ,\ a_2 + jb_2) \rightarrow (a_1 + jb_1) \oplus (a_2 + jb_2) = (a_1 + a_2) + j(b_1 + b_2)$$

and

$$* : G(q) \otimes G(q) \rightarrow G(q)$$
$$(a_1 + jb_1\ ,\ a_2 + jb_2) \rightarrow (a_1 + jb_1) * (a_2 + jb_2) = (a_1a_2 - b_1b_2) + j(a_1b_2 + a_2b_1).$$

The structure $GI(q) := < G(q)\ ,\ \oplus\ ,\ * >$ is a field. In fact, GI(q) is isomorphic to $GF(q^2)$. ■

Trigonometric functions over the elements of a Galois field can be defined as follows.

Definition 2. *Let α have multiplicative order N in GF(q), $q = p^r$, $p \neq 2$. The GI(q)-valued k-trigonometric functions of*

$\angle(\alpha^i)$ in GF(q) (by analogy, the trigonometric functions of k times the "angle" of the "complex exponential" α^i) are defined as

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

and

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

for i , k = 0, 1,..., N-1 .

For simplicity suppose α to be fixed. We write $\cos_k(\angle\alpha^i)$ as $\cos_k(i)$ and $\sin_k(\angle\alpha^i)$ as $\sin_k(i)$. The k-trigonometric functions satisfy properties P1-P11 below.

P1. *Unit Circle:* $sin_k^2(i) + cos_k^2(i) = 1.$

Proof: $\sin_k^2(i) + \cos_k^2(i) =$

$$= [\frac{1}{2j}(\alpha^{ik} - \alpha^{-ik})]^2 + [\frac{1}{2}(\alpha^{ik} + \alpha^{-ik})]^2 =$$

$$= \frac{1}{-4}(\alpha^{2ik} - \alpha^{-2ik} - 2) + \frac{1}{4}(\alpha^{2ik} + \alpha^{-2ik} + 2) = 1$$ ■

P2. *Even / Odd:* $cos_k(i) = cos_k(-i).$
$sin_k(i) = -sin_k(-i).$

Proof: $\cos_k(-i) = \frac{1}{2}(\alpha^{-ik} + \alpha^{ik}) = \cos_k(i);$

$$\sin_k(-i) = \frac{1}{2j}(\alpha^{-ik} - \alpha^{ik}) = -\sin_k(i).$$ ■

P3. *Euler Formula :* $\alpha^{ik} = cos_k(i) + jsin_k(i).$

Proof: $\cos_k(i) + j\sin_k(i) =$

$$= \frac{1}{2}(\alpha^{-ik} + \alpha^{ik}) + \frac{1}{2}(\alpha^{ik} - \alpha^{-ik}) = \alpha^{ik}.$$ ■

P4. *Addition of Arcs :*

$cos_k(i + t) = cos_k(i)cos_k(t) - sin_k(i)sin_k(t),$
$sin_k(i + t) = sin_k(i)cos_k(t) + sin_k(t)cos_k(i).$

Proof: $\cos_k(i + t) = \frac{1}{2}(\alpha^{(i+t)k} + \alpha^{-(i+t)k}) =$

$\frac{1}{2}(\alpha^{ik}\alpha^{tk} + \alpha^{-ik}\alpha^{-tk}) = \frac{1}{2}\{[\cos_k(i)+j\sin_k(i)][\cos_k(t)+ +j\sin_k(t)]+[\cos_k(i)-j\sin_k(i)][\cos_k(t)-j\sin_k(t)]\}$
$= \cos_k(i)\cos_k(t) - sen_k(i)sen_k(t).$

The proof for the sin(.) function is similar. ■

P5. *Double arc:*

$$\cos_k^2(i) = \frac{1 + \cos_k(2i)}{2}$$

$$\sin_k^2(i) = \frac{1 - \cos_k(2i)}{2}.$$

Proof: According to P4, $\cos_k(2i) = \cos^2_k(i) - \sin^2_k(i) = \cos^2_k(i) - [1 - \cos^2_k(i)] = 2\cos^2_k(i) - 1$, and the result follows.
The proof for the sin(.) function is similar. ■

P6. *Symmetry:* $cos_k(i) = cos_i(k)$
$sin_k(i) = sin_i(k).$

Proof: Follows directly from definition 2. ■

P7. Complementary Symmetry: With itkr≠0 and k+t = i+r = N,

$\cos_k(i) = \cos_r(t)$
$\sin_k(i) = \sin_r(t).$

Proof.

$$2[\cos_k(i) - \cos_r(t)] = (\alpha^{ik}+\alpha^{-ik}-\alpha^{rt}-\alpha^{-rt})\left(\frac{\alpha^{it}}{\alpha^{it}}\right) =$$

$$= \left(\frac{1}{\alpha^{it}}\right)(\alpha^{i(k+t)}+\alpha^{i(t-k)}-\alpha^{t(r+i)}-\alpha^{t(i-r)}) = (\alpha^{-ik} - \alpha^{-rt}) =$$

$$(\alpha^{-i(N-t)} - \alpha^{-(N-i)t}) = 0$$

since α has order N. ■

P8. *Periodicity:* $cos_k(i + N) = cos_k(i)$
$sin_k(i + N) = sin_k(i).$

Proof: $\cos_k(i + N) = \frac{1}{2}(\alpha^{i(k+N)} + \alpha^{-i(k+N)}) = \frac{1}{2}(\alpha^{ik}\alpha^{iN} + +\alpha^{-ik}\alpha^{iN}) = \cos_k(i)$, since the order of α is N.
The proof for the sin(.) function is similar. ■

P9. *Complement:*

$cos_k(i) = cos_k(t)$ *where itk ≠ 0 and i+t = N.*
$sin_k(i) = -sin_k(t)$ *where itk ≠ 0 and i+t = N.*

Proof:

$$2[\cos_k(i)-\cos_k(t)] = (\alpha^{ik}+\alpha^{-ik}-\alpha^{tk}-\alpha^{-tk})\left(\frac{\alpha^{kt}}{\alpha^{kt}}\right) =$$

$$\alpha^{-ik} - \alpha^{tk} = (\alpha^{-ik}-\alpha^{tk})\left(\frac{\alpha^{-kt}}{\alpha^{-kt}}\right) = 0.$$ ■

P10. $cos_k(i)$ *summation:*

$$\sum_{k=0}^{N-1} \cos_k(i) = \begin{cases} N, i = 0 \\ 0, i \neq 0. \end{cases}$$

Proof: Let $\sigma_c := \sum_{k=0}^{N-1} \cos_k(i) = \frac{1}{2}\sum_{k=0}^{N-1} (\alpha^{ik} + \alpha^{-ik})$. If i = 0 then $\sigma_c = N$. Otherwise $\sigma_c = \frac{1}{2}[\frac{1(\alpha^i)^N - 1}{\alpha^i - 1} + +\frac{1(\alpha^i)^N - 1}{\alpha^i - 1}] =$

$\frac{1}{2}[0 + 0] = 0.$ ■

P11. $sin_k(i)$ *summation:* $\sum_{k=0}^{N-1} sin_k(i) = 0.$

Proof: Let $\sigma_s := \sum_{k=0}^{N-1} \sin_k(i) = \frac{1}{2j}\sum_{k=0}^{N-1} (\alpha^{ik} - \alpha^{-ik})$. If i = 0 then $\sigma_s = 0$. Otherwise $\sigma_s = \frac{1}{2j}[\frac{1(\alpha^i)^N - 1}{\alpha^i - 1} - \frac{1(\alpha^i)^N - 1}{\alpha^i - 1}] =$.

$\frac{1}{2j}[0 - 0] = 0$ ■

A simple example is given to illustrate the behaviour of such functions.

Example 1. *Let $\alpha = 3$, a primitive element of GF(7). The $cos_k(i)$ and $sin_k(i)$ functions take the following values in GI(7):*

Table 1. Discrete cosine and sine functions over GI(7).

$cos_k(i)$

(k) \ (i)	0	1	2	3	4	5
0	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

$sin_k(i)$

(k) \ (i)	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	j	j	0	6j	6j
2	0	j	6j	0	j	6j
3	0	0	0	0	0	0
4	0	6j	j	0	6j	j
5	0	6j	6j	0	j	j

The k-trigonometric functions have interesting orthogonality properties, such as the one shown in lemma 1.

Lemma 1. *The k-trigonometric functions $cos_k(.)$ and $sin_k(.)$ are orthogonal in the sense that*

$$A := \sum_{k=0}^{N-1} [cos_k(\angle\alpha^i)\, sin_k(\angle\alpha^i)] = 0,$$

where α is an element of multiplicative order N in GF(q).

Proof: By definition 2,

$$A = \sum_{k=0}^{N-1} [\frac{1}{2}(\alpha^{ik} + \alpha^{-ik})\frac{1}{2j}(\alpha^{tk} - \alpha^{-tk})] = \frac{1}{4j}$$

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

Now, If i = t, then A = (0 + 0 + N - N) / 4j = 0. If i = -t, then A = (N - N + 0 - 0) / 4j = 0. Otherwise, A= (0 + 0 + 0. + 0)/4j = 0 ■

A general orthogonality condition, which leads to a new Hartley Transform, is now presented via the $cas_k(\angle\alpha^i)$ function. The notation used here follows closely the original one introduced in [10].

We now introduce the $cas_k(\angle\alpha^i)$ function which plays an important role in the definition of a finite field Hartley Transform

Definition 3. *Let $\alpha \in GF(q)$, $\alpha \neq 0$. Then*

$$cas_k(\angle\alpha^i) := cos_k(\angle\alpha^i) + sin_k(\angle\alpha^i).$$

We use $cas_k(i)$ to denote $cas_k(\angle\alpha^i)$. The $cas_k(i)$ function satisfies properties C1-C7 bellow:

C1 - k-trigonometric Relations

i) $cas_k(i + t) = cos_k(i)\, cas_k(t) + sin_k(i)\, cas_k(-t)$.

ii) $cas_k(i - t) = cos_k(i)\, cas_k(-t) + sin_k(i)\, cas_k(t)$.

iii) $cas_k(i)\, cas_k(t) = cos_k(i - t) + sin_k(i + t)$.

Proof:

i) By definition $cas_k(i + t) = cos_k(i + t) + sin_k(i + t)$ and from P1 and P2 we may write

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

ii) The proof is similar to i) above.

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

and the result follows from P2 and P4. ■

C2. *Symmetry: $cas_k(i) = cas_i(k)$*

Proof: Follows directly from P6. ■

C3. *Quadratic Norm*

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

Proof: With $cas_k(i) = a+jb$, then

$$(cas_k(i))^q = a^q + j^q b^q = a - jb.$$

Therefore

$$[cas_k(i)]^{q+1} = |cas_k(i)|^2 = [cos_k(i)]^2 - [sin_k(i)]^2$$

$$= cos_k(2i)\ (P1 \text{ and } P5).$$ ■

C4. *Primitivity: If $cas_k(i)$ is primitive in GI(q) then $|cas_k(i)|^2$ is primitive in GF(q).*

Proof: If $cas_k(i)$ is primitive in GI(q) then the least integer n such that $(cas_k(i))^n = 1$ is $n = (q+1)(q-1)$. From C4

$$[cas_k(i)^{q+1}]^{q-1} = (|cas_k(i)|^2)^{q-1} = 1$$

and the least integer r such that $(|cas_k(i)|^2)^m = 1$ is $m = q-1$. Since $|cas_k(i)|^2$ is in GF(q), that implies it is

primitive. ■

C5. *Periodicity:* $cas_k(i+N) = cas_k(i)$.

Proof: It follows directly from the fact that both $\cos_k(i)$ and $\sin_k(i)$ functions are periodic with period N. ■

C6. *Nulity:* $cas_k(\angle\alpha^i) \neq 0, \ \forall i,k = 0, 1, ..., N-1$.

Proof: The $cas_k(.)$ function can be written as

$$cas_k(i) = \frac{1}{2}(\alpha^{ik} + \alpha^{-ik}) + \frac{1}{2j}(\alpha^{ik} - \alpha^{-ik}) =$$

$$\frac{1}{2}[(\alpha^{ik} + \alpha^{-ik}) + j(\alpha^{-ik} - \alpha^{ik})] =$$

$$= \frac{1}{2}[(\alpha^{ik} + j\alpha^{-ik}) - j(\alpha^{ik} + j\alpha^{-ik})],$$

so that

$$cas_k(i) = \frac{1-j}{2}(\alpha^{ik} + j\alpha^{-ik}).$$

Supposing now that $cas_k(\alpha^i) = 0$, we have $\alpha^{ik} + j\alpha^{-ik} = 0$, i.e., $\alpha^{2ik} = -j$, which is an absurd since $j \notin GF(q)$. ■

C7. *Conjugacy Relations*

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

ii) $[cas_k(i)]^2 + \{[cas_k(i)]^2\}^{\blacktriangle} = 2$, where $\blacktriangle$ denotes complex conjugate.

Proof:

i) From C3 and C7 we have, respectively,

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

and

$$[cas_k(i)]^2 = 1 + sen_k(2i).$$

Therefore

$$[cas_k(i)]^{q-1} = \frac{\cos_k(2i)}{1 + sen_k(2i)},$$

so that we may write

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

and, from C3, the result follows.

ii) As seen above

$$[cas_k(i)]^2 = 1 + sen_k(2i).$$

Since $\alpha \in GF(q)$, we may write

$$[cas_k(i)]^{2\blacktriangle} = 1 - sen_k(2i),$$

and the result follows. ■

The set $\{cas_k(.)\}_{k=0, 1, ..., N-1}$, can be viewed as a set of sequences that satisfy the following orthogonality property:

Theorem 1.

$$H := \sum_{k=0}^{N-1} cas_k(\angle\alpha^i)\, cas_k(\angle\alpha^t) = \begin{cases} N, & i = t \\ 0, & i \neq t \end{cases},$$

where α has multiplicative order N.

Proof: From definition 3 it follows that

$$H = \sum_{k=0}^{N-1} [\cos_k(i)\cos_k(t) + \sin_k(i)\sin_k(t) + +\sin_k(i)\cos_k(t) + \sin_k(t)\cos_k(i)],$$

which, by lemma 1, is the same as

$$H = \sum_{k=0}^{N-1} \cos_k(i)\cos_k(t) + \sin_k(i)\sin_k(t).$$

It follows then, from property P4, that

$$H = \sum_{k=0}^{N-1} \cos_k(i - t),$$

and, from P9, the result follows. ■

3. THE FINITE FIELD HARTLEY TRANSFORM

Definition 4. *Let $v = (v_0, v_1, ..., v_{N-1})$ be a vector of length N with components over GF(q), $q = p^r$, $p \neq 2$. The Finite Field Hartley Transform (FFHT) of v is the vector $V = (V_0, V_1, ..., V_{N-1})$ of components $V_k \in GF(q^r)$, given by*

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

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

Such a definition clearly mimics the classical definition of the Discrete Hartley Transform [9]. The inverse FFHT is given by the following theorem.

Theorem 2. *The N-dimensional vector v can be recovered from its Hartley discrete spectrum V according to*

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

Proof: Let $\hat{v}_i := \frac{1}{N(\mathrm{mod}\, p)} \sum_{k=0}^{N-1} V_k cas_k(\angle\alpha^i)$.

After substituting the V_k given by definition 4 in the above expression, it follows that

$$\hat{v}_i = \frac{1}{N(\mathrm{mod}\, p)} \sum_{k=0}^{N-1} \sum_{r=0}^{N-1} v_r \mathrm{cas}_k(\angle\alpha^r)\mathrm{cas}_k(\angle\alpha^i) .$$

Changing the order of summation,

$$\frac{1}{N(\mathrm{mod}\, p)} \sum_{r=0}^{N-1} v_r \sum_{k=0}^{N-1} \mathrm{cas}_k(\angle\alpha^r)\mathrm{cas}_k(\angle\alpha^i)$$

$$= \frac{1}{N(\mathrm{mod}\, p)} \sum_{r=0}^{N-1} v_r \begin{Bmatrix} N, & r = i \\ 0, & r \neq i \end{Bmatrix} = v_i$$

■

A signal v and its discrete Hartley spectrum V are said to form a finite field Hartley Transform pair, denoted by $v \leftrightarrow V$ or $V = H(v)$. It is worthwhile to mention that the FFHT belongs to a class of discrete transforms for which the kernel of the direct and the inverse transform is exactly the same.

Letting now $g = \{g_i\} \leftrightarrow G = \{G_k\}$ and $v = \{v_i\} \leftrightarrow V = \{V_k\}$ denote FFHT pairs of length N, the following set of useful properties can be derived.

H1. *Linearity*

$$ag + bv \leftrightarrow aG + bV, \quad \forall\, a,b \in GF(q).$$

H2. *Time Shift*

If $v_i = g_{i-d}$, then $V_k = \cos_k(d)G_k + \sin_k(d)G_{n-k}$.

Proof:

$$V_k = \sum_{i=0}^{N-1} g_{i-d}\mathrm{cas}_k(i).$$

Making $i - d = r$ leads to

$$V_k = \sum_{r=-d}^{N-1-d} g_r \mathrm{cas}_k(d + r),$$

which, from C1 and C5, is the same as

$$V_k = \sum_{r=0}^{N-1} g_r(\cos_k(d)\mathrm{cas}_k(r) + \sin_k(d)\mathrm{cas}_k(-r))$$

and

$$V_k = \cos_k(d)G_k + \sin_k(d)G_{n-k}.$$

H3. *Sum of Sequence (dc term):* $V_0 = \sum_{i=0}^{N-1} v_i$.

H4. Initial Value: $v_0 = \frac{1}{N(\mathrm{mod}\, p)} \sum_{k=0}^{N-1} V_k$.

H5. *Symmetry:* $G \leftrightarrow Ng$.

Proof: Denoting the FFHT of $G = \{G_r\}$ by $F = \{F_k\}$, we have

$$F_k = \sum_{r=0}^{N-1} G_r \mathrm{cas}_k(r).$$

By the definition of the FFHT this can be written as

$$F_k = \sum_{r=0}^{N-1} \sum_{i=0}^{N-1} g_i \mathrm{cas}_r(i)\mathrm{cas}_k(r).$$

Changing the order of summation,

$$F_k = \sum_{i=0}^{N-1} g_i \sum_{r=0}^{N-1} \mathrm{cas}_r(i)\mathrm{cas}_k(r).$$

Considering the symmetry property of the cas(.) function, we may use theorem 1 which implies that the innermost summation is nonzero only when i=k. Therefore we obtain $F_k = Ng_k$ and the proof is complete. ■

H6. Time Reversal: $g_{-i} \leftrightarrow G_{-k}$.

Proof: Denoting $g_{-i} \leftrightarrow F_k$ we have

$$F_k = \sum_{i=0}^{N-1} g_{-i}\mathrm{cas}_k(i).$$

Changing $-i = r$

$$F_k = \sum_{r=0}^{N-1} g_r \mathrm{cas}_k(-r),$$

which, from C2, is the same as G_{N-k}. ■

H7. Cyclic Convolution: If ★ denotes cyclic convolution, then

$$g \star v \leftrightarrow \tfrac{1}{2}(GV + G_-V_- + G_-V - GV_-).$$

where G_- and V_- denotes, respectively, the sequences $\{G_{N-k}\}$ and $\{V_{N-k}\}$.

Proof: The cyclic convolution of g and v is given by

$$g \star v = \sum_{r=0}^{N-1} g_r v_{i-r},$$

so that its FFHT is

$$H(g \star v) = \sum_{i=0}^{N-1} [\sum_{r=0}^{N-1} g_r v_{i-r}](\mathrm{cas}_k(i)).$$

Changing the order of summation and using property H2, we obtain

$$H(g \star v) = \sum_{r=0}^{N-1} g_r(\cos_k(r)V_k + \sin_k(r)V_{N-k})$$

From definition 3 it is possible to express $\cos_k(i)$ and $\sin_k(i)$ in termos of the $cas_k(i)$ function. Specifically,

$$\cos_k(i) = \tfrac{1}{2}[cas_k(i) + cas_k(-i)]$$

and

$$\sin_k(i) = \tfrac{1}{2}[cas_k(i) - cas_k(-i)].$$

Therefore

$$H(g\star v) = \frac{V_k}{2}\sum_{r=0}^{N-1} g_r[cas_k(i)+cas_k(-i)]+$$

$$+\frac{V_{N-k}}{2}\sum_{r=0}^{N-1} g_r[cas_k(i)-cas_k(-i)],$$

or

$$H(g\star v) = \frac{V_k}{2}(G_k + G_{-k}) + \frac{V_{N-k}}{2}(G_k - G_{-k})$$

and the result follows. ■

H8. Parseval's Relation $\sum_{i=0}^{N-1} g_i^2 = \frac{1}{N(\text{modp})}\sum_{k=0}^{N-1} G_k^2$.

Proof: Considering the inverse FFHT of the pair established in H7 we may write

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

$$= \frac{1}{2N}\sum_{k=0}^{N-1}(G_k V_k + G_k V_{-k} + G_{-k} V_k - G_{-k} V_{-k})cas_k(i).$$

Choosing v and g such that $v_j = g_{-j}$ implies that $v_{i-r} = g_{r-i}$ and $V_k = G_{-k}$. Therefore

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

$$= \frac{1}{2N}\sum_{k=0}^{N-1}(G_k G_k + G_k G_{-k} + G_{-k} G_k - G_{-k} G_{-k})cas_k(i).$$

Now observing that the summations $\Sigma G_k G_k$ and $\Sigma G_{-k} G_{-k}$ are the same, and simplifying terms, we get

$$\sum_{r=0}^{N-1} g_r g_{i-r} = \frac{1}{N}\sum_{k=0}^{N-1} G_k G_k cas_k(i).$$

Making i=0 the result follows. ■

4. VALID SPECTRA

The following theorem states a relation that must be satisfied by the components of a 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. In what follows GCD(r, s) denotes the greatest common divisor of r and s.

Theorem 3. *The vector $V = \{V_k\}$, $V_k \in GI(q^m)$, is the spectrum of a signal $v = \{v_i\}$, $v_i \in GF(q)$, $q = p^r$, if and only if*

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

where indexes are considered modulo N, i, k = 0, 1, ..., N-1 and $N \mid (q^m - 1)$.

Proof: ($\Rightarrow$) From the FFHT definition and considering that $GF(p^r)$ has characteristic p, it follows that

$$V_k^q = (\sum_{i=0}^{N-1} v_i cas_k(i))^q = (\sum_{i=0}^{N-1} v_i^q cas_k^q(i)).$$

If $v_i \in GF(q)$ $\forall$ i, then $v_i^q = v_i$. The fact that $j^2 = -1 \notin GF(q)$ if and only if q is a prime power of the form 4s + 3, implies that $j^q = -j$. Hence,

$$V_k^q = \sum_{i=0}^{N-1} v_i cas_{N-qk}(i) = V_{N-qk}.$$

($\Leftarrow$) On the other hand, suppose $V_k^q = V_{N-qk}$. Then

$$\sum_{i=0}^{N-1} v_i^q cas_{N-qk}(i) = \sum_{i=0}^{N-1} v_i cas_{N-qk}(i).$$

Now, let N-qk = r. Since $GCD(q^m - 1, q) = 1$, both k and r ranges over the same values, which implies

$$\sum_{i=0}^{N-1} v_i^q cas_r(i) = \sum_{i=0}^{N-1} v_i cas_r(i),$$

r = 0, 1, ..., N-1. By the uniqueness of the FFHT, $v_i^q = v_i$ so that $v_i \in GF(q)$ and the proof is complete. ■

Example 2. *With q = p = 3, r = 1, m = 5 and $GF(3^5)$ generated by the primitive polynomial $f(x) = x^5 + x^4 + x^2 + 1$, a FFHT of length N = 11 may be defined by taking an element of order 11 (α^{22} is such an element, where $f(\alpha)=0$). The vectors v and V given below are an FFHT pair.*

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

The relation for valid spectra shown above implies that only two components V_k are necessary to completely specify the vector V, namely V_0 and V_1. This can be verified simply by calculating the cyclotomic classes Cs induced by theorem 3 which, in this case, are $C_0 = (0)$ and $C_1 = (1, 8, 9, 6, 4, 10, 3, 2, 5, 7)$.

5. MODULAR ENERGY

Definition 5. *A signal* $v = (v_0, v_1, ..., v_{N-1})$ *with components* $v_i \in GF(p)$ *has a modular energy E given by* $E := \sum_{i=0}^{N-1} v_i^2 \pmod p$.

The energy of a signal vector v assumes values over GF(p). Supposing that v over GF(p) has a finite field transform V over an extension field $GF(p^m)$, there exists a Parseval relationship

$$\sum_{i=0}^{N-1} v_i^2 = \frac{1}{N(\text{mod } p)} \sum_{k=0}^{N-1} V_k^2 .$$

And, althought the symbols V_k are on the extension field, the righ-side sum lies always on the ground field. Aiming to define an energy density, the summation cannot be carried out over arbitrary index sets, because it may not yield a value over GF(p).

Proposition 2. *If V is the finite field transform (either Fourier or Hartley) of a signal v, then the sum* $\sum_{k\in C_s} V_k^2 \in GF(p)$, *where* C_s *is the cyclotomic coset whose leader is s. Therefore,*

$$E = \sum_{i=0}^{N-1} v_i^2 = \sum_s \left(\sum_{k\in C_s} V_k^2 \right).$$

Proof: a) FFFT - The conjugacy class constraint for the Finite Field Fourier Transform states that the inverse transform components are in GF(p) if and only if $V_k^p = V_{kp}$, with indexes taken modulo N [6]. Considering the cyclotomic coset whose leader is s, i.e., $C_s \equiv F_s := (s, ps, p^2 s, ..., p^{m_s-1} s)$, *where* m_s *is such that* $p^{m_s} s \equiv s \pmod{p^m - 1}$, it is possible to write

$$\sum_{k\in F_s} V_k^2 = V_s^2 + V_{ps}^2 + ... + V_{p^{m_s-1}s}^2$$

$$= V_s^2 + V_s^{2p} + ... + V_s^{2p^{m_s-1}}$$

$$= V_s^2 + (V_s^2)^p + ... + (V_s^2)^{p^{m_s-1}} = Tr(V_s^2),$$

where Tr(x) is the trace function [6]. Since $Tr(\alpha) \in GF(p)$ for every $\alpha \in GF(p^m)$, the case for the FFFT is settled.
b) FFHT - From theorem 3, the corresponding expression for the Hartley case is

$$\sum_{k\in H_s} V_k^2 = V_s^2 + V_{-ps}^2 + V_{p^2 s}^2 + V_{-p^3 s}^2 + ... = \sum_i V_{(-p)^i s}^2 .$$

where Hs denotes the Hartley cyclotomic coset whose leader is s. Since p and m are both odd, it will happen that $p^{m_s} s \equiv -s \pmod{p^m - 1}$ and a repetition will occur only at p^{2m_s}, which means that the Hartley cosets are given by the union of the Fourier cosets of s and -s, i.e.,

$$H_s = F_s \cup F_{-s} ,$$

where -s is the reciprocal modulo N of s. Therefore

$$\sum_{k\in H_s} V_k^2 = Tr(V_s^2) + Tr(V_{-s}^2) ,$$

which belongs to GF(p). ■

Definition 6. *The cyclotomic density of modular energy (spectral density over a finite field) is defined by*

$$G_s := \sum_{k\in C_s} V_k^2 .$$

Indeed, $\sum_s G_s = E$, which is similar to $\int_{-\infty}^{+\infty} G(f)df = E$ in the continuos case. Since the sum is carried out over all the frequencies, we can interpret the cyclotomic sets as some sort of "cyclotomic frequencies". It is interesting to consider the particular case in which we have no extension on the alphabet, that is, when the transform is defined from GF(p) to GF(p), or even from GF(p) to GI(p). In such a case, each cyclotomic class has two elements: k and -k. Thus, $G_k = V_k^2 + V_{-k}^2$ which corresponds to the frequency f and -f. We propose then a spectral representation (finite field spectrum) by plotting the cyclotomic energy density versus cyclotomic frequencies. Each spectral line furnishes its contribution to the total modular energy in the corresponding "cyclotomic frequency".

c-Spectrograms. We can also define a finite field spectrogram for such a modular energy spectral density, where each element of GF(p) corresponds to a color of a p^m-color "rainbow". This representation is termed a cyclotomic-spectrogram or a c-spectrogram for short. The (infinite) signal sequence over GF(p) is partitioned into N-symbol-blocks and the FFHT is evaluated for each block yielding a spectral representation which is plotted in a 2-dimensional grid (block x cyclotomic frequencies).

Example 3. *We consider FFHT pairs from GF(7) to GI(7), with N=6 and* α*=3 an element of order N in the multiplicative group of* $GF^*(7) := GF(7)-\{0\}$:

100120 ↔ 4 6+5j 1+2j 2 1+5j 6+2j
023065 ↔ 2 6+2j 6 2 6 6+6j
300212 ↔ 1 5+4j 6j 0 j 5+3j
110235 ↔ 5 4 2+6j 3 2+j 4
601024 ↔ 6 3+2j 6+4j 5 6+3j 3+5j

$$234011 \leftrightarrow 4\ \ 5+5j\ \ 1+6j\ \ 3\ \ 1+j\ \ 5+2j$$

Applying theorem 3 to this case leads to $V_k^7 = V_{6-7k}$, so that $V_0^7 = V_0$ (k=0), $V_2^7 = V_4$ (k=1), $V_3^7 = V_3$ (k=2) and $V_k^7 = V_{6-7k}$ (k=3). Observe that the components V_0 and V_3 are not complex, i.e., thy are in the ground field. Therefore the cyclotomic classes C_s induced by theorem 3 are

$$C_0 = (0), C_1 = (1, 5), C_2 = (2,4), C_3 = (3).$$

Table 2 below shows, for each transform pair, the energy contained in each cyclotomic class

Table 2. Modular energy in the cyclotomic classes of example 3.

s				
0	1	2	3	E
2	1	1	4	1
4	0	2	4	3
1	4	5	0	3
4	4	6	2	2
1	3	5	4	6
2	0	0	2	4

Figure 1 below shows the c-spectrogram for the block (N=6) data sequence over GF(7) (with α=3) given in example 3.

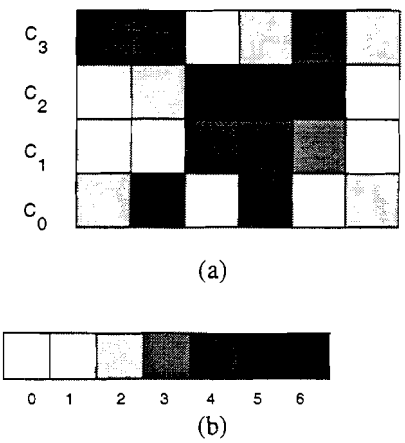

Figure 1. (a) c-spectrogram of the data sequence in example 3. (b) Energy levels.

5. CONCLUSIONS

In this paper, trigonometry for finite fields was introduced. In particular, the k-trigonometric functions of the *angle* of the *complex exponential* α^i were defined and their basic properties derived. From the $\cos_k(\angle\alpha^i)$ and $\sin_k(\angle\alpha^i)$ functions, the $\text{cas}_k(\angle\alpha^i)$ function was defined and used to introduce a new Hartley Transform, the Finite Field Hartley Transform (FFHT). It has been shown that the cyclotomic coset partition induced by the FFHT is such that an element and its reciprocal modulo N belongs to the same class, which implies that the number of FFHT components that need to be computed to completely specify the spectrum V is approximately half of the number needed for the Finite Field Fourier Transform.

The concepts of modular energy and c-spectrograms were also introduced and the notion of a modular energy spectral density assuming values on a finite field was defined.

The FFHT seems to have interesting applications in a number of areas. Specifically, its use in digital signal processing, along the lines of the so-called number theoretic transforms (e.g. Mersenne and Fermat number transforms) should be investigated. In the field of error control codes, the FFHT might be used to produce a transform domain description of the field, therefore providing, possibly, an alternative to the approach introduced in [6]. Digital multiplexing and spread spectrum are areas that might also benefit from the new Hartley transform introduced in this paper. In particular, new schemes of efficient-bandwidth code-division-multiple-access for band-limited channels based on the FFHT are currently under development.

ACKNOWLEDGEMENT

The authors wish to thank Prof. James Massey for his suggestions and insightful comments which improved the final version of this paper.

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] C. M. Rader, *Discrete Convolution via Mersenne Transforms*, IEEE Trans. Comput., vol. C-21, pp. 1269-1273, Dec. 1972.

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

[4] R. C. Agarwal and C. S. Burrus, *Number Theoretic Transforms to Implement Fast Digital Convolution*, IEEE Proc., vol. 63, pp. 550-560, Apr. 1975.

[5] 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.

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

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

[8] J. L. Massey, *The Discrete Fourier Transform in Coding and Cryptography*, 1998 IEEE Inform. Th. Workshop, ITW 98, San Diego, CA, Feb 9-11.

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

[10] R. V. L. Hartley, *A More Symmetrical Fourier Analysis Applied to Transmission Problems*, Proc. IRE, vol. 30, pp. 144-150, Mar. 1942.
[11] R. N. Bracewell, *The Hartley Transform*, Oxford University Press, 1986.
[12] 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.
[13] R. N. Bracewell, *Aspects of the Hartley Transform*, IEEE Proc., vol. 82, pp. 381-387, Mar.
1994
[14] J. Hong and M. Vetterli, *Hartley Transforms Over Finite Fields*, IEEE Trans. Inform. Theory, vol. IT-39, pp. 1628-1638, Sep. 1993.

Ricardo Menezes Campello de Souza was born in Recife-PE. He received both the B.Eng. and M.Sc. degrees in Electrical Engineering from the Federal University of Pernambuco (UFPE) Brazil, in 1974 and 1979, respectively, and the PhD degree from the University of Manchester, UK, in 1983. Since 1979 he is a member of staff at the Electronics and Systems Department at UFPE where he is now an Associate Professor. He was the head of the graduate program in electrical engineering at UFPE from 1984 to 1987, and head of Department from 1987 to 1992. From 1992 to 1997 he was a member of the scientific comittee of Facepe, the Pernambuco agency for scientific and technological development. His current research interests include discrete mathematics, cryptography, digital signal processing and algebraic coding theory. Dr. Campello de Souza is a member of the Brazilian Telecommunications Society (SBrT) and the Institute of Electrical and Electronics Engineers (IEEE).

Hélio Magalhães de Oliveira was born in Arcoverde-PE. He received both the B.Eng. and the M.Sc. degrees in Electrical Engineering from the Federal University of Pernambuco (UFPE) Brazil, in 1980 and 1983, respectively. then he joined the staff of the Electronics and Systems Department at the same University as a lecturer. In 1992, he earned the "Docteur de l'École Supérieure des Télécommunications" degree, in Paris, France, in current research interests include data communication, digital signal processing, applied information theory and error-control coding with emphasis on coded-modulation. Dr. de Oliveira is a member of the Brazilian Telecommunication Society (SBrT) and the Institute of Electrical and Electronics Engineers (IEEE).

André Neumman Kauffman was born in Recife, PE. He graduated *cum laude* in Electrical Engineering at the Federal University of Pernambuco (UFPE) Brazil, in 1997, where he is currently working towards his M.Sc. degree. His research interests are in discrete mathematics, digital signal processing, digital communications and cryptography.