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 , ANK@nlink.com.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 and interesting 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]. 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) [9], the discrete version of the symmetrical, Fourier-like, integral transform introduced by R. V. L. Hartley in 1942 [10]. 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 [11-13]. 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 [14] which has interesting applications in the field of digital multiplexing [15]. 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 introduced. Thus, in the next section a trigonometry for gaussian integers over a Galois field is introduced. In section 3 the cosine and sine (cas) function over a finite field is introduced and some orthogonality relations are derived. In section 4, the complex finite field Hartley transform (CFFHT) is defined using a Galois field gaussian integer argument for the transform kernel which removes the blocklength

restriction of the FFHT. Section 5 examines the condition for valid spectra which leads to results that are similar to the conjugacy constraints for the FFFT. An efficient algorithm for computing the CFFHT is presented in section 6. The paper closes with a few concluding remarks and suggestions of some possible areas of applications.

2. A TRIGONOMETRY FOR GAUSSIAN INTEGERS OVER A GALOIS FIELD

The set G(q) of gaussian integers over 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 $GF(q^2)$. ð

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 $p \equiv 3 \pmod 4$. Trigonometric functions over the elements of a Galois field can be defined as follows.

Definition 2: Let ζ be na element of multiplicative order N in GI(q), $q = p^r$, $p \neq 2$. The GI(q)-valued k-trigonometric functions of $\angle(\zeta^i)$ in GI(q) (by analogy, the trigonometric functions of k times the ″angle″ of the ″complex exponential″ ζ^i) are defined as

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

for i, k = 0, 1,...,N-1. For simplicity ζ is supposed to be fixed. We write $\cos_k(\angle\zeta^{\,i})$ as $\cos_k(i)$. The trigonometric functions above introduced satisfy properties P1-P10 below.

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

Proof:
$$\sin_k^2(i) + \cos_k^2(i) = \left[\frac{1}{2j}(\zeta^{ik} - \zeta^{-ik})\right]^2 + \left[\frac{1}{2}(\zeta^{ik} + \zeta^{-ik})\right]^2 =$$
$$= \frac{1}{-4}(\zeta^{2ik} - \zeta^{-2ik} - 2) + \frac{1}{4}(\zeta^{2ik} + \zeta^{-2ik} + 2) = 1. \qquad ð$$

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

$\sin_k(i) = -\sin_k(-i)$.

Proof. $\cos_k(-i) = \frac{1}{2}(\zeta^{-ik} + \zeta^{ik}) = \cos_k(i)$; $\sin_k(-i) = \frac{1}{2j}(\zeta^{-ik} - \zeta^{ik}) = -\sin_k(i)$. ð

P3. Euler Formula : $\zeta^{ik} = \cos_k(i) + j\sin_k(i)$.

Proof. $\cos_k(i) + j\sin_k(i) = \frac{1}{2}(\zeta^{-ik} + \zeta^{ik}) + \frac{1}{2}(\zeta^{ik} - \zeta^{-ik}) = \zeta^{ik}$. ð

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. Clearly $\cos_k(i + t) = \frac{1}{2}(\zeta^{(i+t)k} + \zeta^{-(i+t)k}) = \frac{1}{2}(\zeta^{ik}\zeta^{tk} + \zeta^{-ik}\zeta^{-tk}) =$

$= \frac{1}{2}\{[\cos_k(i)+j\sin_k(i)][\cos_k(t)+j\sin_k(t)]+[\cos_k(i)-j\sin_k(i)][\cos_k(t)-j\sin_k(t)]\}$

$= \cos_k(i)\cos_k(t)-\text{sen}_k(i)\text{sen}_k(t)$.

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

P5. Double arc:

$$\cos_k^2(i) = \frac{1 + \cos_k(2i)}{2}; \qquad \sin_k^2(i) = \frac{1 - \cos_k(2i)}{2}$$

Proof. According to P4,

$\cos_k(2i) = \cos^2_k(i) - \sin^2_k(i) = \cos^2_k(i) - [1 - \cos^2_k(i)] = 2\cos^2_k(i) - 1$.

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

P6. Symmetry:

$\cos_k(i) = \cos_i(k)$

$\sin_k(i) = \sin_i(k)$.

Proof. Follows directly from definition 2. ÿ

P7. Periodicity: $\cos_k(i + N) = \cos_k(i)$ e $\sin_k(i + N) = \sin_k(i)$.

Proof. $\cos_k(i + N) = \frac{1}{2}(\zeta^{i(k+N)} + \zeta^{-i(k+N)}) = \frac{1}{2}(\zeta^{ik}\zeta^{iN} + \zeta^{-ik}\zeta^{iN}) = \cos_k(i)$, since the order of ζ is N. ÿ

P8. Complement:

$\cos_k(i) = \cos_k(t)$ where $itk \neq 0$ and $i+t = N$

$\sin_k(i) = -\sin_k(t)$ where $itk \neq 0$ and $i+t = N$.

Proof.

$$2[\cos_k(i)-\cos_k(t)] = (\zeta^{ik}+\zeta^{-ik}-\zeta^{tk}-\zeta^{-tk})\left(\frac{z^{kt}}{z^{kt}}\right) = \zeta^{-ik}-\zeta^{tk} = (\zeta^{-ik}-\zeta^{tk})\left(\frac{z^{-kt}}{z^{-kt}}\right) = 0.$$ ÿ

P9. $\cos_k(i)$ summation:

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

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

$\sigma = \frac{1}{2}[\frac{1(z^i)^N - 1}{z^i - 1} + \frac{1(z^i)^N - 1}{z^i - 1}] = \frac{1}{2}[0 + 0] = 0.$ ÿ

P10. $\sin_k(i)$ summation:

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

Proof. Let $\sigma := \sum_{k=0}^{N-1} \sin_k(i) = \frac{1}{2j}\sum_{k=0}^{N-1} (\zeta^{ik} - \zeta^{-ik})$. If i = 0 then $\sigma = 0$. Otherwise σ

$= \frac{1}{2j}[\frac{1(z^i)^N - 1}{z^i - 1} - \frac{1(z^i)^N - 1}{z^i - 1}] = \frac{1}{2j}[0 - 0] = 0.$ ÿ

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

Example 1: Let $\zeta = j$, an element of order 4 in GI(3). The $\cos_k(i)$ and $\sin_k(i)$ functions take the following values in GI(3):

Table 1 – Discrete cosine and sine functions over GI(3).

$\cos_k(i)$

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

$\sin_k(i)$

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

3. ORTHOGONALITY RELATIONS

The trigonometric functions (definition 2) 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

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

where ζ is an element of multiplicative order N in GI(q).

Proof. From P4, we have $\cos_k(\angle\zeta^i) \sin_k(\angle\zeta^t) = \frac{1}{2}[\sin_k(t + i) + \sin_k(t - i)]$, and therefore

$$\sum_{k=0}^{N-1} [\cos_k(\angle\zeta^i) \sin_k(\angle\zeta^t)] = \frac{1}{2}\sum_{k=0}^{N-1} [\sin_k(t + i) + \sin_k(t - i)].$$

Then, from P10, the result follows. ÿ

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

Definition 3: Let $\zeta \in GI(q)$, $\zeta \neq 0$. Then $cas_k(\angle\zeta^i) := \cos_k(\angle\zeta^i) + \sin_k(\angle\zeta^i)$. ð

The $cas_k(.)$ function satisfies properties C1-C5 below:

C1. Addition of Arcs:

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

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

Proof: i) By definition $cas_k(i + t) = \cos_k(i + t) + \sin_k(i + t)$, so that from P2 and P4,
$cas_k(i + t) = \cos_k(i)\cos_k(t) - \sin_k(i)\sin_k(t) + \sin_k(i)\cos_k(t) + \sin_k(t)\cos_k(i) =$
$= \cos_k(i)[\cos_k(t) + \sin_k(t)] + \sin_k(i)[\cos_k(-t) + \sin_k(-t)] = \cos_k(i)cas_k(t) + \sin_k(i)cas_k(-t)$. □

The proof for (ii) is similar.

C2. Product: $cas_k(i)\, cas_k(t) = \cos_k(i - t) + \sin_k(i + t)$

Proof: $cas_k(i)\, cas_k(t) = [\cos_k(i)+\sin_k(i)][\cos_k(t)+\sin_k(t)] = \cos_k(i)\cos_k(t)+$
$+\sin_k(i)\sin_k(t) + \sin_k(i)\cos_k(t) + \sin_k(t)\cos_k(i)$, and, from P2 and P4, the result follows.

C3. Symmetry: $cas_k(i) = cas_i(k)$

Proof: Direct from P6. □

C4. Quadratic Norm: Let $cas(\angle\zeta^i)$, with argument $\zeta = \alpha \in GF(q)$. Then

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

Proof: With $cas_k(i) = a+jb$, then $(cas_k(i))^q = a^q + j^q b^q = a - jb$. Therefore
$[cas_k(i)]^{q+1} = |\, cas_k(i)\,|^2 = [\cos_k(i)]^2 - [\mathrm{sen}_k(i)]^2 = \cos_k(2i)$ (P1 and P5). ÿ

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

Proof: Direct from P11. ÿ

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

Theorem 1. $\sum_{k=0}^{N-1} cas_k(\angle\zeta^i)cas_k(\angle\zeta^t) = \begin{cases} N, & i = t \\ 0, & i \neq t \end{cases}$, where ζ has multiplicative order N.

Proof. From C2 it follows that

$$\sum_{k=0}^{N-1} [cas_k(\angle\zeta^i)cas_k(\angle\zeta^t)] = \sum_{k=0}^{N-1} [\cos_k(i - t) + \sin_k(i + t)] .$$

Now, using P10, we obtain

$$\sum_{k=0}^{N-1} [cas_k(\angle\zeta^i)cas_k(\angle\zeta^t)] = \sum_{k=0}^{N-1} [\cos_k(i - t)],$$ and, from P9, the result follows. ÿ

4. THE COMPLEX FINITE FIELD HARTLEY TRANSFORM

Let $v = (v_0 , v_1 , \ldots , v_{N-1})$ be a vector of length N with components over GF(q). The Complex Finite Field Hartley Transform (CFFHT) of v is the vector $V = (V_0, V_1 , \ldots , V_{N-1})$ 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. A signal v and its discrete Hartley spectrum V are said to form a complex finite field Hartley transform pair, denoted by $V = H(v)$ or $v \leftrightarrow V$.

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

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

Proof.

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

interchanging the summations

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

which, by theorem 1, is the same as

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

Therefore, as it happens in the continuous Hartley Transform, the CFFHT is symmetrical in the sense that it uses the same kernel for the direct and inverse transforms.

5. CONJUGACY CONSTRAINTS

Theorem 3 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.

Theorem 3: The vector $V = \{V_k\}$, $V_k \in GI(q^m)$, is the spectrum of a signal $v = \{v_i\}$, $v_i \in GF(q)$, if and only if $V_k^q = V_{N-kq}$, where indexes are considered modulo N, i, k = 0, 1, ..., N-1 and $N \mid (q^m - 1)$.

Proof: From the CFFHT definition and considering that GF(q), $q = p^r$, has characteristic p, it follows that

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

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,

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

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, 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 CFFHT, $v_i^q = v_i$ so that $v_i \in GF(q)$ and the proof is complete. ð

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 specify the spectrum V is approximately half of the number needed for the Finite Field Fourier Transform.

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 or order 11 (α^{198} is such an element). The vectors v and V given below are an FFHT pair.

$$v = (0, 1, 2, 1, 1, 0, 0, 0, 2, 1, 1)$$

$$V = (0, \alpha^{215} + j\alpha^{46}, \alpha^{241} + j\alpha^{51}, \alpha^{161} + j\alpha^{138}, \alpha^{233} + j\alpha^{96}, \alpha^{239} + j\alpha^{32}, \alpha^{239} + j\alpha^{153},$$
$$\alpha^{233} + j\alpha^{217}, \alpha^{161} + j\alpha^{17}, \alpha^{241} + j\alpha^{172}, \alpha^{215} + j\alpha^{167}).$$

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 induced by lemma 1 which, in this case, are $C_0 = (0)$ and $C_1 = (1, 8, 9, 6, 4, 10, 3, 2, 5, 7)$.

6. 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.
Proof:

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

so that

$$\frac{1}{2}[(F_k + F_{N-k}) + j(F_{N-k} - F_k)] = \sum_{i=0}^{N-1} v_i \cos_k(\angle\alpha^i) + \sum_{i=0}^{N-1} v_i \sin_k(\angle\alpha^i) =$$

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

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 Transform algorithm.

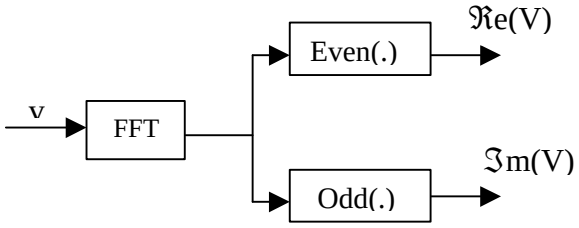

Fig. 1- Computing the CFFHT

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 attractive for DSP implementations.

7. CONCLUSIONS

In this paper, a trigonometry for gaussian integers over a Galois field was introduced. In particular, the k-trigonometric functions of the *angle* of the *complex exponential* ζ^i were defined and some of their basic properties derived. From the $\cos_k(\angle\zeta^i)$ and $\sin_k(\angle\zeta^i)$ functions, the $cas_k(\angle\zeta^i)$ (cosine and sine) function was defined. It was then shown that the set $\{cas_k(.)\}_{k=0,\,1,\ldots,\,N-1}$, can be viewed as a set of sequences that satisfy an orthogonality relation, which in turn was used to introduce a new Hartley Transform, the Complex Finite Field Hartley Transform (CFFHT).

Two important relations that have implications as far as the computation of the CFFHT were established. Firstly it was shown that the CFFHT components satisfy

the so-called conjugacy constraints, which implies that only the leaders of the conjugacy classes need to be computed. Secondly, a simple relation between the CFFHT and the Finite Field Fourier Transform was established, which meant that FFT type algorithms can be used to compute the CFFHT.

The CFFHT 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 transforms) should be investigated. In the field of error control codes, the CFFHT 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 is another area that might 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.

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*, accepted for presentation at the 1998 IEEE Inform. Theory 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] 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.
[15] 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.