Trigonometry in Finite Fields and a New Hartley Transform

R. M. Campello de Souza, H. M. de Oliveira, A. N. Kauffman, A. J. A. Paschoal
CODEC - Grupo de Pesquisas 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

Abstract-**A trigonometry for finite fields is introduced. In particular, the k-trigonometric functions over the Galois Field GF(q) are defined 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 (FFHT). The FFHT presented here is different from an earlier version and seems to be the more natural one.**

I. INTRODUCTION

Discrete transforms play an important role in Electrical Engineering, particularly the well known Discrete Fourier Transform (DFT). A DFT for finite fields (FFFT) was introduced by Pollard [1] and applied as a tool to perform discrete convolutions. A second and relevant example concerns the Discrete Hartley Transform (DHT) [2], the discrete version of the integral transform introduced by R.V.L. Hartley. In this paper the construction of a DHT over a finite field is approached. In order to obtain a transform that holds some resemblance with the DHT, sinusoidal functions over a finite structure are defined and, to the best of our knowledge, trigonometry in finite fields is formally introduced for the first time in the literature.

II. k-TRIGONOMETRIC FUNCTIONS

The set G(q) of gaussian integers over GF(q) plays an important role in the ideas introduced in this paper.

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.

Proposition 1: Let $\oplus : G(q)\otimes G(q)\rightarrow G(q)$ and $* : G(q)\otimes G(q)\rightarrow G(q)$

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

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

The structure $GI(q)=\langle G(q), \oplus, * \rangle$ is a field isomorphic to $GF(q^2)$.

Trigonometric functions over GF(q) 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 $\cos_k(\angle\alpha^i)=1/2\ (\alpha^{ik}+\alpha^{-ik})$ and $\sin_k(\angle\alpha^i)=1/(2j)\ (\alpha^{ik}-\alpha^{-ik})$, for i,k=0,1,...,N-1. 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 the following properties: P1. Unit Circle: $\sin_k^2(i)+\cos_k^2(i)=1$. P2. Even/Odd: $\cos_k(i)=\cos_k(-i)$ and $\sin_k(i)=-\sin_k(-i)$. P3. Euler Formula: $\alpha^{ik}=\cos_k(i)+j\sin_k(i)$. P4. Addition of Arcs: $\cos_k(i+t)=\cos_k(i)\cos_k(t)-\sin_k(i)\sin_k(t)$, $\sin_k(i+t)=\sin_k(i)\cos_k(t)+\sin_k(t)\cos_k(i)$. P5. Double Arc: $2\cos_k^2(i)=1+\cos_k(2i)$ and $2\sin_k^2(i)=1-\cos_k(2i)$. P6. Summation:

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

P7. Orthogonality: $\sum_{k=0}^{N-1}[\cos_k(\angle\alpha^i)\sin_k(\angle\alpha^j)]=0$.

A general orthogonality condition, which leads to a new Hartley Transform, is now presented via the $cas_k(\angle\alpha^i)$ function, $\alpha\neq 0$.

Definition 3: Let $\alpha\in GF(q)$. Then $cas_k(\angle\alpha^i)=\cos_k(\angle\alpha^i)+\sin_k(\angle\alpha^i)$.

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

III. THE FINITE FIELD HARTLEY TRANSFORM

Definition 4: Let $v=(v_0,v_1,\ldots,v_{N-1})$ be a vector of length N with components over GF(q), $q=p^r$. The Finite Field Hartley Transform (FFHT) of v is the vector $V=(V_0,V_1,\ldots,V_{N-1})$ of components $V_k\in GI(q^m)$, given by $V_k=\sum_{k=0}^{N-1}v_i\,cas_k(\angle\alpha^i)$ where α is a specified element of multiplicative order N in $GF(q^m)$. Such a definition clearly mimics the classical definition [2]. 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

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

A signal v and its discrete Hartley spectrum V are said to form a transform pair, denoted by $v\leftrightarrow V$. Letting $g=\{g_i\}\leftrightarrow G=\{G_k\}$ and $v=\{v_i\}\leftrightarrow V=\{V_k\}$ denote FFHT pairs, the following properties can be derived: H1-Linearity: $ag+bv\leftrightarrow aG+bV, \forall a,b\in GF(q)$. H2-Time Shift: If $v_i=g_{i-d}$, then $V_k=\cos_k(d)G_k+\sin_k(d)G_{-k}$. H3-Symmetry: $G\leftrightarrow Ng$. H4-Time Reversal: $g_{-i}\leftrightarrow G_{-k}$. H5-Cyclic Convolution: If H denotes cyclic convolution, then $g\mathrm{H}\,v\leftrightarrow\frac{1}{2}(GV+GV_-+G_-V-G_-V_-)$ where G_- and V_- denotes the sequences $\{G_{N-k}\}$ and $\{V_{N-k}\}$. H6-Parseval's Relation: $N\sum_{k=0}^{N-1}g_i^2=\sum_{k=0}^{N-1}G_k^2$. H7-Let $v=\{v_i\}\leftrightarrow V=\{V_k\}$ and $v=\{v_i\}\leftrightarrow F=\{F_k\}$ denote an FFHT and an FFFT pair [1], then $V_k=1/2[(F_k+F_{N-k})+j(F_{N-k}-F_k)]$ and $F_k=1/2\,[(V_k+V_{N-k})+j(V_k-V_{N-k})]$.

Lemma 2 states a relation that must be satisfied by the components of the spectrum V for it to be a valid finite field Hartley spectrum.

Lemma 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 $N|(q^m-1)$.

IV. 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. The $cas_k(\angle\alpha^i)$ function was defined and used to introduce a new Hartley Transform, different and more natural than an earlier proposed version [3]. The FFHT have interesting applications in a number of areas. New schemes of efficient-bandwidth code-division-multiple-access for band-limited channels based on the FFHT are currently under development.

ACKNOWLEDGEMENTS The authors wish to thank Prof. James Massey for his suggestions and insightful comments.

REFERENCES

[1] J.M. Pollard, *The Fast Fourier Transform in a Finite Field*, Math. Comput., v. 25, N. 114, pp. 365-374, Apr. 1971.

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

[3] J. Hong and M. Vetterli, *Hartley Transform Over Finite Fields*, IEEE Trans, vol. IT-39, pp.1628-1638, Sept. 1993.

0-7803-5000-6/98/$10.00 © 1998 IEEE.