Hartley Transforms over Finite Fields

Jonathan Hong and Martin Vetterli[1]
Department of Electrical Engineering
and Center for Telecommunications Research
Columbia University, New York, NY 10027-6699
Phone # (212) 854-3109
e-mail: martin@ctr.columbia.edu

Abstract

We present a general framework for constructing transforms in the field of the input. The construction is carried out over finite fields, but is shown to be valid over the real and complex fields as well. It is shown that these basefield transforms can be viewed as projections of the DFT and that they exist for all length N for which the DFT is defined. The construction further shows that these transforms are not unique; that there are in fact $mn\phi(N)$ such transforms . Finally, the convolution property of the basefield transforms is derived and a condition given for such transforms to have the self-inverse property.

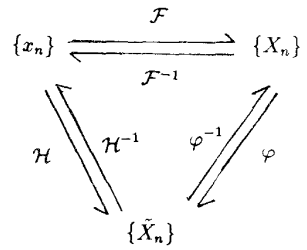
1. Introduction

The discrete Hartley transform (DHT) has been proposed as a real transform with convolution property [9] [12] [13] and is thus an alternative to the discrete Fourier transform (DFT) for the convolution of real sequences. Note that the DHT is self-inverse. Since the DFT can be defined over finite fields, it is natural to ask whether a Hartley or Hartley-like transform exists over finite fields. Aside from the theoretical interest for such a finite field DHT, its advantages are potentially more substantial than in the real case since computing finite field DFT's often involve going to much larger extension fields. The reason for this stems from the fact that we need an element of order N in order to compute a DFT of size N. Therefore, if the input belongs to GF(q), we have to go to GF(q^m) where m is such that $N|q^m - 1$ in order to compute the size N DFT. Because of the different extension fields involved and the fact that computation is invariably more complex in the extension fields (involving polynomial multiplications and reductions etc), it is desirable to have a transform in the basefield GF(q) when the input is in GF(q). In this paper we will construct such a basefield transform and show that it can be viewed as a "projection" of the DFT algorithm. We will also derive the convolution property of such a transform and give a condition for the transform to have the self-inverse property. Finally we will show that the theory, though developed in the context of finite fields, applies to the real and complex fields as well.

2. The Forward Transform

The most natural way to construct a Hartley transform over finite fields is to mimic its construction over the reals. Such a construction, however, leads to a non-invertible transform, indicating that the connection between the DFT and the DHT is deeper than what is suggested at a first glance by the real case. Our approach to this problem will therefore be indirect.

Consider figure 1 where we've denoted the input by $\{x_n\}$ and the DFT and the (yet undefined) DHT of $\{x_n\}$ by $\{X_n\}$ and $\{\tilde{X}_n\}$ respectively. Note that $\{x_n\}$ and $\{\tilde{X}_n\}$ will be elements of the same field B=GF(q) while $\{X_n\}$ depending on the length of the transform, will be in some extension field E=GF(q^m) of B. The function $\mathcal{F}$ between $\{x_n\}$and $\{X_n\}$is the usual DFT mapping. The function $\mathcal{H}$ is the Hartley transform that we seek. Shown also is an intermediate map, φ, between $\{X_n\}$ and $\{\tilde{X}_n\}$. Since $\mathcal{F}$ and $\mathcal{H}$ (if it exists) are bijections, clearly the Hartley transform exists iff the intermediate transform φ exists. Therefore if we can construct the mapping φ from $\{X_n\}$ to $\{\tilde{X}_n\}$ then the composition of $\mathcal{F}$ and φ will yield a Hartley transform, namely $\mathcal{H} = \varphi \circ \mathcal{F}$.



[1]Work supported in part by the National Science Foundation under grants CDR-84-21402,MIP-88-08277,MIP-90-14189 and Bellcore.

24ACSSC-12/90/0103 $1.00

To construct φ, consider $\{X_n\}$, the DFT of $\{x_n\}$. Since the x_n's are in the basefield B, X_n's satisfy the conjugacy constraint [7]

$$X_{kq^l} = X_k^{q^l} \qquad \forall k, l. \tag{1}$$

The conjugacy class of X_k with respect to B therefore consist of

$$\{X_k, X_{kq}, X_{kq^2}, \cdots, X_{kq^{m-1}}\} = \{X_k, X_k^q, X_k^{q^2}, \cdots, X_k^{q^{m-1}}\}.$$

Let M be a matrix with elements in E such that

$$M \begin{pmatrix} X_k \\ X_{kq} \\ X_{kq^2} \\ \cdots \\ X_{kq^{m-1}} \end{pmatrix} = M \begin{pmatrix} X_k \\ X_k^q \\ X_k^{q^2} \\ \cdots \\ X_k^{q^{m-1}} \end{pmatrix} \in B^m = GF(q)^m.$$

Clearly M must be circulant, invertible and it must send the conjugacy class of X_k into B. Can we always find such an M? Yes. Let $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\} \triangleq \langle\alpha\rangle$ be a normal basis of E viewed as a vector space over B (notation : E_B). Define

$$M = \begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{m-2}} \\ \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & \alpha & \cdots & \alpha^{q^{m-3}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{pmatrix}$$

then M is circulant, invertible and we have

$$\begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{m-2}} \\ \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & \alpha & \cdots & \alpha^{q^{m-3}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{pmatrix} \begin{pmatrix} X_k \\ X_k^q \\ X_k^{q^2} \\ \cdots \\ X_k^{q^{m-1}} \end{pmatrix} = \begin{pmatrix} Tr(\alpha X_k) \\ Tr(\alpha X_k^q) \\ Tr(\alpha X_k^{q^2}) \\ \cdots \\ Tr(\alpha X_k^{q^{m-1}}) \end{pmatrix}$$

where Tr is the trace function [1] [2] [6] . Since the trace function is a linear functional on E_B, defining $\tilde{X}_{kq^i}$ by $Tr(\alpha X_k^{q^i})$ we have $\tilde{X}_{kq^i} \in$ B as desired. The map

$$\varphi : X_k \longmapsto \tilde{X}_k = Tr(\alpha X_k) \tag{2}$$

thus defines a one-to-one correspondence between $\{X_n\}$and $\{\tilde{X}_n\}$.

To obtain a Hartley transform $\mathcal{H}$, consider

$$X_k = \sum_{n=0}^{N-1} x_n W_N^{nk}$$

where $x_n \in B$ and W_N is an element of order N in E. Let $\{\beta_0, \beta_1, \beta_2, \cdots, \beta_{m-1}\}$ be a basis of E_B, then W_N^{nk} has a unique representation with respect to this basis

$$W_N^{nk} = w_{nk}^{(0)}\beta_0 + w_{nk}^{(1)}\beta_1 + w_{nk}^{(2)}\beta_2 + \cdots + w_{nk}^{(m-1)}\beta_{m-1}.$$

Therefore

$$\begin{aligned} X_k &= \beta_0 \sum_{n=0}^{N-1} x_n w_{nk}^{(0)} + \beta_1 \sum_{n=0}^{N-1} x_n w_{nk}^{(1)} + \cdots + \beta_{m-1} \sum_{n=0}^{N-1} x_n w_{nk}^{(m-1)} \\ &= \beta_0 X_k^{(0)} + \beta_1 X_k^{(1)} + \beta_2 X_k^{(2)} + \cdots\cdots + \beta_{m-1} X_k^{(m-1)} \end{aligned}$$

where $X_k^{(i)} \triangleq \sum_{n=0}^{N-1} x_n w_{nk}^{(i)} \in B$. Since $\mathcal{H} = \varphi \circ \mathcal{F}$, we have

$$\tilde{X}_k = Tr(\alpha\beta_0)X_k^{(0)} + Tr(\alpha\beta_1)X_k^{(1)} + \cdots + Tr(\alpha\beta_{m-1})X_k^{(m-1)} \tag{3}$$

which is indeed a basefield transform. While this proves the existence of a basefield transform, expression (3)is not optimal. We can reduce the amount of computation significantly by choosing our basis cleverly. Instead of an arbitrary basis, choose $\{\beta_i\}$ to be the (unique) dual basis of $\langle\alpha\rangle$. With this choice of bases, α_i and β_j are trace-orthogonal, i.e.

$$Tr(\alpha_i\beta_j) = \delta_{ij}$$

thus (3)reduces to

$$\tilde{X}_k = X_k^{(0)} = \sum_{n=0}^{N-1} x_n w_{nk}^{(0)} = \sum_{n=0}^{N-1} x_n Tr(\alpha W_N^{nk}). \tag{4}$$

This is the final form of our basefield transform which we will henceforth call a Hartley transform.

Rmk :

1. There is nothing special about $X_k^{(0)}$. By permuting the elements of $\{\alpha_i\}$ and $\{\beta_i\}$ we could just as easily obtain
$$\tilde{X}_k = X_k^{(i)} = \sum_{n=0}^{N-1} x_n w_{nk}^{(i)}.$$
for any i.

2. Equation (4) actually defines a whole class of transforms thereby showing that basefield transforms are not unique. In fact by taking all possible combinations of W_N and α it is easy to see that we can construct $mn\phi(N)$ transforms of the type defined by (4), where m is the dimension of E_B, n is the number of normal basis in E_B and ϕ is the Euler function . Note, however, not all of these transforms will be 'distinct'. It can be shown that many of these will be permutations of each other.

3. The Inverse Transform

To find the inverse Hartley transform (as defined by (4)) we need to first invert the intermediate map φ. Equivalently, we need to find the inverse of the matrix M of section 2. Recall that the elements of M are members of a normal basis $\{\alpha_i\} = \langle\alpha\rangle = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\}$. If $\{\beta_i\}$ is the dual basis of $\{\alpha_i\}$ then it can be shown that $\{\beta_i\}$ is also normal, i.e. $\{\beta i\} = \langle\beta\rangle = \{\beta, \beta^q, \beta^{q^2}, \cdots, \beta^{q^{m-1}}\}$ for some

$\beta \in E$, and that M^{-1} is given by

$$M^{-1} = \begin{pmatrix} \beta & \beta^{q^{m-1}} & \beta^{q^{m-2}} & \cdots & \beta^{q} \\ \beta^{q} & \beta & \beta^{q^{m-1}} & \cdots & \beta^{q^2} \\ \beta^{q^2} & \beta^{q} & \beta & \cdots & \beta^{q^3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \beta^{q^{m-1}} & \beta^{q^{m-2}} & \beta^{q^{m-3}} & \cdots & \beta \end{pmatrix}.$$

Therefore

$$\begin{pmatrix} X_k \\ X_{kq} \\ X_{kq^2} \\ \cdots \\ X_{kq^{m-1}} \end{pmatrix} = \begin{pmatrix} \beta & \beta^{q^{m-1}} & \beta^{q^{m-2}} & \cdots & \beta^{q} \\ \beta^{q} & \beta & \beta^{q^{m-1}} & \cdots & \beta^{q^2} \\ \beta^{q^2} & \beta^{q} & \beta & \cdots & \beta^{q^3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \beta^{q^{m-1}} & \beta^{q^{m-2}} & \beta^{q^{m-3}} & \cdots & \beta \end{pmatrix} \begin{pmatrix} \tilde{X}_k \\ \tilde{X}_{kq} \\ \tilde{X}_{kq^2} \\ \cdots \\ \tilde{X}_{kq^{m-1}} \end{pmatrix}$$

implying that

$$\varphi^{-1} : \tilde{X}_k \longmapsto X_k = \beta\tilde{X}_k + \beta^{q}\tilde{X}_{kq^{m-1}} + \cdots + \beta^{q^{m-1}}\tilde{X}_{kq}. \quad (5)$$

Refering back to fig. 1 we see that $\mathcal{H}^{-1} = \mathcal{F}^{-1} \circ \varphi^{-1}$. Composing the two functions yields the following inverse transform

$$x_k = N^{-1} \sum_{n=0}^{N-1} (\beta\tilde{X}_n + \beta^{q}\tilde{X}_{nq^{m-1}} + \cdots + \beta^{q^{m-1}}\tilde{X}_{nq}) W_N^{-nk}. \quad (6)$$

While expression (6) will compute the correct inverse, note however, this computation is performed in the extension field E. Since we seek a transform in the basefield B, we need an alternative to (6) . To that end consider the first summand of (6)

$$\begin{aligned} \sum_{n=0}^{N-1} \beta\tilde{X}_n W_N^{-nk} &= \beta\alpha \sum_{n=0}^{N-1} X_n W_N^{-nk} + \beta\alpha^{q} \sum_{n=0}^{N-1} X_n^{q} W_N^{-nk} + \\ &\quad \cdots + \beta\alpha^{q^{m-1}} \sum_{n=0}^{N-1} X_n^{q^{m-1}} W_N^{-nk}. \end{aligned}$$

It can be shown that the terms $\sum_{n=0}^{N-1} X_n^{q^i} W_N^{-nk}$ are elements of B. Using this fact and the fact that α_i and β_j are trace-orthogonal, we have that

$$Tr(\sum_{n=0}^{N-1} \beta\tilde{X}_n W_N^{-nk}) = \sum_{n=0}^{N-1} X_n W_N^{-nk} = N x_k.$$

If we expand W_N^{-nk} with respect to the normal basis $\langle\alpha\rangle$

$$W_N^{-nk} = w_{-nk}^{(0)}\alpha + w_{-nk}^{(1)}\alpha^{q} + w_{-nk}^{(2)}\alpha^{q^2} + \cdots + w_{-nk}^{(m-1)}\alpha^{q^{m-1}}$$

then $Tr(\beta W_N^{-nk}) = w_{-nk}^{(0)}$ and we have

$$x_k = N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n w_{-nk}^{(0)} = N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n Tr(\beta W_N^{-nk}). \quad (7)$$

This then is the basefield inverse of the DHT.

4. The Self-Inverse Problem

Let us restate the Hartley transform and its inverse

$$\begin{aligned} \tilde{X}_k &= \sum_{n=0}^{N-1} x_n w_{nk}^{(0)} = \sum_{n=0}^{N-1} x_n Tr(\alpha W_N^{nk}) \quad (8) \\ x_k &= N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n w_{-nk}^{(0)} = N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n Tr(\beta W_N^{-nk}). \quad (9) \end{aligned}$$

From the definitions it is clear that the forward and inverse transform will be the same iff $w_i^{(0)} = w_{-i}^{(0)} \quad \forall i$ (note that these components are with respect to different bases). The following proposition therefore characterizes the self-inverse transforms.

Proposition 1 *Let E be an extension field of B. There exist a self-inverse B-transform (of the form (8)(9)) iff there is a normal basis $\langle\alpha\rangle$ of E_B such that*

$$Tr(\alpha W_N^{k}) = Tr(\beta W_N^{-k}) \quad \forall k \quad (10)$$

where W_N is any element of order N in E and $\langle\beta\rangle$ is the dual basis of $\langle\alpha\rangle$.

5. The Convolution Property

The convolution property of the Hartley transforms can be deduced readily with the aid of the intermediate map φ. Since convolution corresponds to pointwise product in the Fourier domain , to obtain the convolution property in the Hartley domain, simply map the sequences which we are convolving to the Fourier domain (via φ^{-1}), perform the convolution there (pointwise product), and map the result back to the Hartley domain (via φ).

Let $\{y_n\}$ be the convolution of $\{x_n\}$ and $\{h_n\}$. Using the notations of the previous sections, we have

$$X_k = \varphi^{-1}(\tilde{X}_k) = \beta\tilde{X}_k + \beta^{q}\tilde{X}_{kq^{m-1}} + \beta^{q^2}\tilde{X}_{kq^{m-2}} + \cdots + \beta^{q^{m-1}}\tilde{X}_{kq}$$

$$H_k = \varphi^{-1}(\tilde{H}_k) = \beta\tilde{H}_k + \beta^{q}\tilde{H}_{kq^{m-1}} + \beta^{q^2}\tilde{H}_{kq^{m-2}} + \cdots + \beta^{q^{m-1}}\tilde{H}_{kq}$$

implying that

$$\begin{aligned} Y_k &= H_k X_k = (\sum_{i=0}^{m-1} \beta^{q^i}\tilde{X}_{kq^{m-i}})(\sum_{j=0}^{m-1} \beta^{q^j}\tilde{H}_{kq^{m-j}}) \\ &= \sum_{i,j=0}^{m-1} \beta^{q^i+q^j}\tilde{X}_{kq^{m-i}}\tilde{H}_{kq^{m-j}}. \end{aligned}$$

To express $\tilde{Y}_k$ in terms of $\tilde{X}_k$ and $\tilde{H}_k$, we 'project' Y_k to the basefield by taking its trace with α. This results in the following convolution formula for Hartley transforms

$$\begin{aligned} \tilde{Y}_k &= \varphi(Y_k) = Tr(\alpha Y_k) \\ &= \sum_{i,j=0}^{m-1} Tr(\alpha\beta^{q^i+q^j})\tilde{X}_{kq^{m-i}}\tilde{H}_{kq^{m-j}}. \quad (11) \end{aligned}$$

6. Hartley Transform over R Revisited

It is easy to see that the results of the previous sections hold, mutatis mutandis, for R and C. In fact if we replace 'conjugate' by 'complex conjugate' and the definition of trace by

$$Tr(\alpha) = \alpha + \alpha^*$$

then the derivation of the preceeding results for the real and complex fields would be exactly the same as that for finite fields.

We derive, in the appendix, the classes of real transforms and self-inverse real transforms permissible under this theory. It is seen that the real transforms are essentially Ansari's Discrete Combinational Fourier Transforms for real input [10] and the self-inverse real transforms are essentially the Hartley transforms.

7. Conclusion and Direction

We have presented a general framework for constructing basefield transforms having a convolution property. The construction is valid in finite fields as well as the real and complex fields and results in transforms which can be viewed as projections of the DFT. A problem of interest is to derive fast algorithms for these DHT's. It is shown in a future paper that this can be done.

Appendix

In this appendix we apply the theory developed for finite fields to the real and complex fields. We will start by determining the normal bases of C_R. Since C is a two dimensional vector space over R, a normal basis of C_R is of the form

$$A = \{\alpha, \alpha^*\} = \{a + ib, a - ib\}.$$

The dual basis of A is also normal, hence it too is of the form

$$B = \{\beta, \beta^*\} = \{c + id, c - id\}.$$

The parameters a, b, c, d are not completely independent since the bases must satisfy the trace-orthogonality relation

$$Tr(\alpha_i \beta_j) = \alpha_i \beta_j + \alpha_i^* \beta_j^* = \delta_{ij}.$$

The constraint forces $c = \frac{1}{4a}$ and $d = -\frac{1}{4b}$, consequently the normal bases of C_R and their corresponding dual bases are exactly

$$\begin{aligned} A &= \{\alpha, \alpha^*\} = \{a + ib, a - ib\} \\ B &= \{\beta, \beta^*\} = \{\frac{1}{4a} - i\frac{1}{4b}, \frac{1}{4a} + i\frac{1}{4b}\} \end{aligned}$$

where $a, b \in R$ are arbitrary.

Over the complex field, the elements of order N are

$$\{e^{-i\frac{2\pi}{N}m} \mid 1 \leq m < N, \ (m, N) = 1\}.$$

It follows that

$$Tr(\alpha W_N^k) = 2a cos\frac{2\pi}{N}nk + 2b sin\frac{2\pi}{N}nk$$

$$Tr(\beta W_N^{-k}) = \frac{1}{2a} cos\frac{2\pi}{N}nk + \frac{1}{2b} sin\frac{2\pi}{N}nk$$

which yield the following real transforms

$$\begin{aligned} \tilde{X}_k &= \sum_{n=0}^{N-1} x_n Tr(\alpha W_N^{nk}) \\ &= \sum_{n=0}^{N-1} x_n [2a cos\frac{2\pi}{N}nnk + 2b sin\frac{2\pi}{N}nnk] \quad (12) \end{aligned}$$

$$\begin{aligned} x_k &= N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n Tr(\beta W_N^{-nk}) \\ &= N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n [\frac{1}{2a} cos\frac{2\pi}{N}nnk + \frac{1}{2b} sin\frac{2\pi}{N}nnk] (13) \end{aligned}$$

For m=1, the above reduces to Ansari's Discrete Combinational Fourier Transforms for real input [10]

$$\begin{aligned} \tilde{X}_k &= \sum_{n=0}^{N-1} x_n [2a cos\frac{2\pi}{N}nk + 2b sin\frac{2\pi}{N}nk] \\ x_k &= N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n [\frac{1}{2a} cos\frac{2\pi}{N}nk + \frac{1}{2b} sin\frac{2\pi}{N}nk]. \end{aligned}$$

Let us now impose the self-inverse condition (10) on equations (12) and (13) . By Proposition 1, the transforms defined by (12) and (13) will have the self-inverse property iff

$$Tr(\alpha W_N^k) = Tr(\beta W_N^{-k}) \qquad \forall k.$$

This means that we must have, for all k

$$2a cos\frac{2\pi}{N}nk + 2b sin\frac{2\pi}{N}nk = \frac{1}{2a} cos\frac{2\pi}{N}nk + \frac{1}{2b} sin\frac{2\pi}{N}nk$$

which is satisfied only if

$$a = \pm\frac{1}{2} \qquad and \qquad b = \pm\frac{1}{2}.$$

Substituting these values into (12) and (13) yields the following self-inverse real transforms

$$\begin{aligned} \tilde{X}_k &= \sum_{n=0}^{N-1} x_n [(\pm) cos\frac{2\pi}{N}nnk + (\pm) sin\frac{2\pi}{N}nnk] \quad (14) \\ x_k &= N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n [(\pm) cos\frac{2\pi}{N}nnk + (\pm) sin\frac{2\pi}{N}nnk] (15) \end{aligned}$$

Our theory thus permits $4\phi(N)$ self-inverse real transforms of which the Hartley transform is but one case (corresponding to the case where m=1 and a=b=$\frac{1}{2}$). It should be noted however that different choices of m, a, and b do not lead to radically new transforms. In fact it is easy to see that other permissible values of m, a and b lead to only permutations

and/or sign changes of the basic Hartley transform.

We will conclude the appendix by deriving the convolution property of the Hartley transform. By equation (11) the convolution property (adapted for the real field) is given by

$$\begin{aligned}\tilde{Y}_k &= Tr(\alpha\beta\beta)\tilde{H}_k\tilde{X}_k + Tr(\alpha\beta\beta^*)\tilde{H}_k\tilde{X}_{-k} \\ &+ Tr(\alpha\beta^*\beta)\tilde{H}_{-k}\tilde{X}_k + Tr(\alpha\beta^*\beta^*)\tilde{H}_{-k}\tilde{X}_{-k}.\end{aligned}$$

As indicated above the Hartley transform corresponds to the choice m=1 and a=b=$\frac{1}{2}$, which means that the associated normal and dual bases are

$$A = \{\alpha, \alpha^*\} = \{\frac{1}{2}(1+i), \frac{1}{2}(1-i)\}$$

$$B = \{\beta, \beta^*\} = \{\frac{1}{2}(1-i), \frac{1}{2}(1+i)\}.$$

It is readily verified that $Tr(\alpha\beta\beta) = Tr(\alpha\beta\beta^*) = \frac{1}{2}$ and $Tr(\alpha\beta^*\beta^*) = -\frac{1}{2}$, therefore

$$\begin{aligned}\tilde{Y}_k &= \frac{1}{2}\tilde{H}_k\tilde{X}_k + \frac{1}{2}\tilde{H}_k\tilde{X}_{-k} + \frac{1}{2}\tilde{H}_{-k}\tilde{X}_k - \frac{1}{2}\tilde{H}_{-k}\tilde{X}_{-k} \\ &= \tilde{H}_k(\frac{\tilde{X}_k + \tilde{X}_{-k}}{2}) + \tilde{H}_{-k}(\frac{\tilde{X}_k - \tilde{X}_{-k}}{2}) \\ &= \tilde{H}_k\tilde{X}_k^{(even)} + \tilde{H}_{-k}\tilde{X}_k^{(odd)}\end{aligned}$$

which is as expected [9].

References

[1] R. Lidl and H. Niederreiter, *Finite Fields,* Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison-Wesley, 1983.

[2] L.C. Grove, *Algebra,* Academic Press, 1983.

[3] T.W. Hungerford, *Algebra,* Springer-Verlag, 1974.

[4] I.N. Herstein, *Abstract Algebra,* Macmillan, 1986.

[5] I.N. Herstein, *Topics in Algebra,* Xerox Publishing, 1975.

[6] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes,* North-Holland, 1977.

[7] R.E. Blahut, *Theory and Practice of Error Control Codes,* Addison-Wesley, 1983.

[8] R.E. Blahut, *Fast Algorithms for Digital Signal Processing,* Addison-Wesley, 1986.

[9] R.N. Bracewell, *The Fourier Transform and Its Applications,* McGraw-Hill, 1986.

[10] R. Ansari, "An Extension of the Discrete Fourier Transform," IEEE Trans. on Circuits and Systems, Vol. 32, No. 6, June 1985, pp. 618-619.

[11] P. Duhamel and M. Vetterli, "Fast Fourier transforms : a tutorial review and a state of the art," invited paper, Signal Processing, Vol. 19, No. 4, April 1990, pp.259-299.

[12] P. Duhamel and M. Vetterli, "Improved Fourier and Hartley Transform Algorithms. Application to Cyclic Convolution of Real Data," IEEE Trans. on Acoust., Speech, Signal Processing, Vol. 35, No. 6, June 1987, pp. 818-824.

[13] H.V. Sorensen, D.L. Jones, C.S. Burrus and M.T. Heideman, "On Computing The Discrete Hartley Transform," IEEE Trans. on Acoust., Speech, Signal Processing, Vol. 33, No. 5, October 1985, pp. 1231-1238.