Hartley Transforms Over Finite Fields

Jonathan Hong and Martin Vetterli, *Senior Member, IEEE*

***Abstract*—A general framework is presented for constructing transforms in the field of the input which have a convolution-like property. 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 discrete Fourier transform (DFT) and that they exist for all lengths N for which the DFT is defined. The convolution property of the basefield transforms is derived and a condition for such transforms to have the self-inverse property is given. Also, fast algorithms for these basefield transforms are developed, showing gains when compared to computations using the FFT. Application of the methodology to Hartley transforms over R leads to a simple derivation of fast algorithms for computing real Hartley transforms.**

***Index Terms*— Finite fields, Hartley transforms, discrete Fourier transform, fast algorithms, complexity.**

I. Introduction

THE DISCRETE Hartley transform (DHT) has been proposed as a real transform with a convolution property [11], [14], [15], [16], and thus, is an alternative to the discrete Fourier transform (DFT) for the convolution of real sequences. 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 greater than in the real case since computing finite field DFT's often involves going to large extensions of the basefield. The reason for this stems from the fact that an element of order N is required to compute a DFT of size N. Therefore, if the input belongs to $\mathrm{GF}(q)$ it is necessary to go to $\mathrm{GF}(q^m)$ where m is such that $N \mid q^m - 1$ in order to compute a 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 $\mathrm{GF}(q)$ when the input is in $\mathrm{GF}(q)$.

In this paper, we show that finite field Hartley transforms do in fact exist and give a general technique for their construction. We derive the convolution property of such transforms and state a condition for the transforms to have the self-inverse property. (This property is satisfied, for example, by DHT's over the reals). Next we develop fast algorithms for the finite field DHT which will be seen as finite field "projections" of well-known FFT algorithms. Finally, we will show that the theory, though developed in the context of finite fields, applies to the real and complex fields as well.

Manuscript received March 5, 1991; revised December 12, 1992. This work was supported in part by the National Science Foundation under Grants CDR-84-21402 and MIP-90-14189. This work was presented in part at the 24th Asilomar Conference on Signals, Systems and Computers, November 1989.

The authors are with the Department of Electrical Engineering, Columbia University, New York, NY 10027.

IEEE Log Number 9210710.

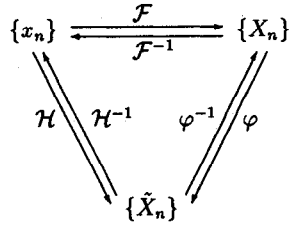

Fig. 1. Relations between $\{x_n\}$, $\mathrm{DFT}\{x_n\}$, and $\mathrm{DHT}\{x_n\}$.

II. 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 noninvertible transform, indicating that the connection between the DFT and the DHT is more intricate than what is initially suggested by the real case. Our approach to this problem will therefore be indirect.

Consider Fig. 1, where we have denoted the input by $\{x_n\}$, the DFT of $\{x_n\}$ by $\{X_n\}$ and the (yet undefined) DHT of $\{x_n\}$ by $\{\tilde{X}_n\}$. Note that $\{x_n\}$ and $\{\tilde{X}_n\}$ reside in the same field $\boldsymbol{B} = \mathrm{GF}(q)$ while $\{X_n\}$ is in an extension field $\boldsymbol{E} = \mathrm{GF}(q^m)$ of $\boldsymbol{B}$. 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, it follows that the Hartley transform exists iff the intermediate transform φ exists. Thus, if we can construct the map φ from $\{X_n\}$ to $\{\tilde{X}_n\}$ then the composition of $\mathcal{F}$ and φ will yield a Hartley transform, namely $\mathcal{H} = \varphi \circ \mathcal{F}$.

The key to constructing φ is to consider the vector space structure of the fields $\boldsymbol{E}$ and $\boldsymbol{B}$. It is well known that if $\boldsymbol{E} = \mathrm{GF}(q^m)$ and $\boldsymbol{B} = \mathrm{GF}(q)$ then in addition to being an extension field of $\boldsymbol{B}$, $\boldsymbol{E}$ is also an m-dimensional vector space over $\boldsymbol{B}$ (notation: $\boldsymbol{E}_{\boldsymbol{B}}$) [1]–[5]. The function φ we seek can thus be viewed as a linear functional on $\boldsymbol{E}_{\boldsymbol{B}}$. All linear functionals on $\boldsymbol{E}_{\boldsymbol{B}}$ arise from the trace functions [1], that is, if φ is a linear functional on $\boldsymbol{E}_{\boldsymbol{B}}$ then there exists a unique α in $\boldsymbol{E}$ such that

$$\varphi(\zeta) = \mathrm{tr}(\alpha\zeta), \qquad \forall \zeta \in \boldsymbol{E},$$

where $\mathrm{tr}(\zeta) = \zeta + \zeta^q + \zeta^{q^2} + \cdots + \zeta^{q^{m-1}}$. Thus, φ must be of the form

$$\begin{aligned}\varphi(X_k) &= \mathrm{tr}(\alpha X_k) \\ &= \alpha X_k + \alpha^q X_k^q + \alpha^{q^2} X_k^{q^2} + \cdots + \alpha^{q^{m-1}} X_k^{q^{m-1}}, \quad (1)\end{aligned}$$

where the element α remains to be determined.

To find the element α and to facilitate the derivation of φ^{-1} later on, it is instructive to look at the matrix representation of φ. To that end we note that since $\{X_n\}$ is the Fourier transform of a basefield sequence $\{x_n\}$, it must satisfy the conjugacy constraint [6], [7]:

$$X_{kq^l} = X_k^{q^l}, \qquad \forall k, l. \tag{2}$$

The conjugacy class of X_k with respect to $\boldsymbol{B}$ therefore, consists of

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

It follows that (1) can be rewritten as

$$\varphi(X_k) = \operatorname{tr}(\alpha X_k) = \alpha X_k + \alpha^q X_{kq} + \alpha^{q^2} X_{kq^2} + \cdots + \alpha^{q^{m-1}} X_{kq^{m-1}} \tag{3}$$

and we can identify the restriction of φ to the conjugacy class of X_k with the matrix operator

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

so that

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

Note that M is circulant which is as we would expect. From this and the fact that the conjugacy relation is an equivalence relation on $\{X_n\}$ (hence the conjugacy classes are disjoint) it follows that the action of φ on $\{X_n\}$ can be represented by the block diagonal matrix

$$\varphi_M = \begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix} \tag{4}$$

with appropriate permutation and/or repetition of the input.

Equation (4) implies that φ is invertible iff M is invertible, hence the restriction on the choice of α is simply that it must render the matrix M nonsingular. The following theorems give a precise characterization of α.

Theorem 1 [1]: M is invertible iff

$$\langle \alpha \rangle = \left\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\right\}$$

is a basis of $\boldsymbol{E_B}$, i.e., iff $\langle \alpha \rangle$ is a normal basis of $\boldsymbol{E_B}$.

Theorem 2 [1]: A normal basis always exists.

Thus by taking α to be a generator of a normal basis of $\boldsymbol{E_B}$ the map

$$\varphi: X_k \mapsto \tilde{X}_k = \operatorname{tr}(\alpha X_k) \tag{5}$$

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

To obtain a Hartley transform $\mathcal{H}$, consider the DFT of $\{x_n\}$

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

where $x_n \in \boldsymbol{B}$ and W_N is an element of order N in $\boldsymbol{E}$. Let $\{\beta_0, \beta_1, \beta_2, \cdots, \beta_{m-1}\}$ be a basis of $\boldsymbol{E_B}$, 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,

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

where $X_k^{(i)} \stackrel{\text{def}}{=} \sum_{n=0}^{N-1} x_n w_{nk}^{(i)} \in \boldsymbol{B}$ is the ith component of X_k with respect to $\{\beta_0, \beta_1, \beta_2, \cdots, \beta_{m-1}\}$. Since $\mathcal{H} = \varphi \circ \mathcal{F}$, we have

$$\tilde{X}_k = \operatorname{tr}(\alpha\beta_0)X_k^{(0)} + \operatorname{tr}(\alpha\beta_1)X_k^{(1)} + \operatorname{tr}(\alpha\beta_2)X_k^{(2)} + \cdots + \operatorname{tr}(\alpha\beta_{m-1})X_k^{(m-1)}, \tag{6}$$

which is indeed a basefield transform. While this shows the existence of a basefield transform, expression (6) is not optimum. We can reduce the amount of computation significantly by a proper choice of basis. Instead of an arbitrary basis, choose $\{\beta_i\}$ to be the (unique) *dual basis* of $\langle \alpha \rangle$. With this choice of basis, $\{\beta_i\}$ is also normal. Furthermore, we have

$$\operatorname{tr}(\alpha_i\beta_j) = \delta_{ij},$$

i.e., α_i and β_j are trace-orthogonal; consequently, (6) simplifies to

$$\tilde{X}_k = X_k^{(0)} = \sum_{n=0}^{N-1} x_n w_{nk}^{(0)} = \sum_{n=0}^{N-1} x_n \operatorname{tr}(\alpha W_N^{nk}). \tag{7}$$

In other words, $\tilde{X}_k$ reduces to the 0th component, with respect to a normal basis, of the discrete Fourier transform X_k. We will henceforth call (7) a Hartley transform.

Remark 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.

Remark 2: Equation (7) 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 (7), where m is the dimension of $\boldsymbol{E_B}$, n is the number of normal bases in $\boldsymbol{E_B}$ and ϕ is the Euler totient 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.

III. The Inverse Transform

To find the inverse Hartley transform (equation (7)) we need to first invert the intermediate map φ. Since

$$\varphi_M = \begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix} \Rightarrow$$

$$\varphi_M^{-1} = \begin{pmatrix} M^{-1} & & & \\ & M^{-1} & & \\ & & \ddots & \\ & & & M^{-1} \end{pmatrix},$$

it suffices to find the inverse of the matrix M of Section II. 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 $\{\beta_i\}$ is also normal, i.e., $\{\beta_i\} = \langle\beta\rangle = \{\beta, \beta^q, \beta^{q^2}, \cdots, \beta^{q^{m-1}}\}$ for some $\beta \in \boldsymbol{E}$.

Fact 1:

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

Proof: See [18]. □

It follows from this that

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

therefore,

$$\varphi^{-1}: \tilde{X}_k \mapsto X_k = \beta\tilde{X}_k + \beta^q \tilde{X}_{kq^{m-1}} + \beta^{q^2}\tilde{X}_{kq^{m-2}} + \cdots + \beta^{q^{m-1}}\tilde{X}_{kq}. \quad (8)$$

$\mathcal{H} = \varphi \circ \mathcal{F}$ implies $\mathcal{H}^{-1} = \mathcal{F}^{-1} \circ \varphi^{-1}$. Composing the two functions we obtain the following inverse transform

$$x_k = N^{-1}\sum_{n=0}^{N-1}(\beta\tilde{X}_n + \beta^q\tilde{X}_{nq^{m-1}} + \beta^{q^2}\tilde{X}_{nq^{m-2}} + \cdots + \beta^{q^{m-1}}\tilde{X}_{nq})W_N^{-nk}. \quad (9)$$

While expression (9) will compute the correct inverse, this computation is performed in the extension field $\boldsymbol{E}$. Since we seek a transform in the basefield $\boldsymbol{B}$, we need an alternative to (9). To that end consider the first summand of (9)

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

Fact 2:

$$\sum_{n=0}^{N-1}X_n^{q^i}W_N^{-nk} \in \boldsymbol{B}, \qquad \forall i.$$

Proof: Recall that $\xi \in \boldsymbol{B} = \mathrm{GF}(q)$ iff $\xi^q = \xi$. We have

$$\left(\sum_{n=0}^{N-1}X_n^{q^i}W_N^{-nk}\right)^q = \sum_{n=0}^{N-1}X_n^{q^{i+1}}W_N^{-nkq} = \sum_{n=0}^{N-1}X_{nq}^{q^i}W_N^{-nkq} = \sum_{n=0}^{N-1}X_n^{q^i}W_N^{-nk},$$

where the first equality is a consequence of the fact that $\mathrm{char}\,\boldsymbol{B} = p$ and $q = p^l$ for some integer l and some prime p; the second equality follows from the conjugacy relation; and the last equality holds because $\gcd(N, q) = 1$. □

From Fact 2 and the trace-orthogonality of α_i and β_j, it follows immediately that

$$\mathrm{tr}\left(\sum_{n=0}^{N-1}\beta\tilde{X}_n W_N^{-nk}\right) = \sum_{n=0}^{N-1}X_n W_N^{-nk} = Nx_k.$$

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 $\mathrm{tr}\,(\beta W_N^{-nk}) = w_{-nk}^{(0)}$ and we have the following *basefield inverse* of (7)

$$x_k = N^{-1}\sum_{n=0}^{N-1}\tilde{X}_n w_{-nk}^{(0)} = N^{-1}\sum_{n=0}^{N-1}\tilde{X}_n\,\mathrm{tr}\,(\beta W_N^{-nk}). \quad (10)$$

TABLE I
$GF(2^4)^*$

vs	Index	Normal Dual	Order
0001	0		1
0010	1	3	15
0100	2	6	15
1000	3	1	5
1001	4	12	15
1011	5		3
1111	6	2	5
0111	7		15
1110	8	9	15
0101	9	8	5
1010	10		3
1101	11		15
0011	12	4	5
0110	13		15
1100	14		15

Example: Let $\boldsymbol{E} = GF(2^4)$ and $\boldsymbol{B} = GF(2)$, then $\boldsymbol{E}$ is a four-dimensional vector space over $\boldsymbol{B}$. Table I lists some information regarding $\boldsymbol{E}^*$, the nonzero elements of $\boldsymbol{E}$.

The entries under vs are the vector space representation of $\boldsymbol{E_B}$ with respect to a polynomial basis generated by a primitive element γ of $\boldsymbol{E}$. The entries under *index* are the representations of the same elements as powers of γ. If an element generates a normal basis for $\boldsymbol{E_B}$, then in the column under *normal dual* we list the generator of its dual basis. Finally, in the last column, we list the order of the elements. As an example, take $W_5 = \gamma^3$, $\langle\alpha\rangle = \langle\gamma^6\rangle$, then $W_5^{-1} = \gamma^{12}$, $\langle\beta\rangle = \langle\gamma^2\rangle$ and

$$H = (\operatorname{tr}(\alpha W_5^{nk})) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

$$H^{-1} = (\operatorname{tr}(\beta W_5^{-nk})) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

IV. The Self-Inverse Property

The real Hartley transform has the interesting property that it is its own inverse. In this section, we give a condition for the proposed transform to have the self-inverse property. We restate the Hartley transform and its inverse

$$\tilde{X}_k = \sum_{n=0}^{N-1} x_n w_{nk}^{(0)} = \sum_{n=0}^{N-1} x_n \operatorname{tr}(\alpha W_N^{nk}) \tag{11}$$

$$x_k = N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n w_{-nk}^{(0)} = N^{-1} \sum_{n=0}^{N-1} \tilde{X}_n \operatorname{tr}(\beta W_N^{-nk}). \tag{12}$$

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

Proposition 1: Let $\boldsymbol{E}$ be an extension field of $\boldsymbol{B}$. There exist a self-inverse $\boldsymbol{B}$-transform iff there is a normal basis $\langle\alpha\rangle$ of $\boldsymbol{E_B}$ such that

$$\operatorname{tr}(\alpha W_N^k) = \operatorname{tr}(\beta W_N^{-k}), \qquad \forall k, \tag{13}$$

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

While the utility of Proposition 1 is unclear when the underlying fields are finite fields,[1] it has direct implications for the real and complex fields. As shown in Appendix A, Proposition 1 allows us to determine all the self-inverse real transforms admissible under this type of construction.

V. The Convolution Property

The convolution property of the Hartley transforms can be deduced readily with the aid of the intermediate map φ. Since the convolution property is well-understood in the Fourier domain, to obtain the convolution in the Hartley domain we map the sequences we are convolving to the Fourier domain (via φ^{-1}), perform the convolution in the Fourier domain (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 notation of the previous sections, we have

$$\begin{aligned} X_k &= \varphi^{-1}(\tilde{X}_k) = \beta\tilde{X}_k + \beta^q \tilde{X}_{kq^{m-1}} \\ &\quad + \beta q^2 \tilde{X}_{kq^{m-2}} + \cdots + \beta^{q^{m-1}} \tilde{X}_{kq}, \\ H_k &= \varphi^{-1}(\tilde{H}_k) = \beta\tilde{H}_k + \beta^q \tilde{H}_{kq^{m-1}} \\ &\quad + \beta^{q^2} \tilde{H}_{kq^{m-2}} + \cdots + \beta^{q^{m-1}} \tilde{H}_{kq}, \end{aligned}$$

therefore,

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

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

$$\tilde{Y}_k = \varphi(Y_k) = \operatorname{tr}(\alpha Y_k) = \sum_{i,j=0}^{m-1} \operatorname{tr}(\alpha\beta^{q^i+q^j}) \tilde{X}_{kq^{m-i}} \tilde{H}_{kq^{m-j}}. \tag{14}$$

which has the form of a polynomial product.

VI. The Hartley Transform as a Projection

In this section, we give an interpretation of the proposed Hartley transform. It is shown that the construction is effectively a *decoupling* and *distribution* operation in which the mapping φ plays the role of a "projection operator."

[1] It does provide a brute force way of determining the self-inverse transforms when $\boldsymbol{E}$ and $\boldsymbol{B}$ are given.

Let $\{\beta^{q^i} i\}_{i=0}^{m-1}$ be a normal basis of $\boldsymbol{E_B}$ with dual $\{\alpha^{q^i}\}_{i=0}^{m-1}$. Expressing W^{nk} with respect to the basis $\{\beta^{q^i}\}$

$$W^{nk} = w_{nk}^{(0)}\beta + w_{nk}^{(1)}\beta^q + w_{nk}^{(2)}\beta^{q^2} + \cdots + w_{nk}^{(m-1)}\beta^{q^{m-1}},$$

we can write the DFT of x_n as

$$\begin{aligned} X_k &= \sum_n x_n W^{nk} \\ &= \beta\sum_n x_n w_{nk}^{(0)} + \beta^q \sum_n x_n w_{nk}^{(1)} \\ &\quad + \beta^{q^2}\sum_n x_n w_{nk}^{(2)} + \cdots + \beta^{q^{m-1}}\sum_n x_n w_{nk}^{(m-1)} \\ &= \beta X_k^{(0)} + \beta^q X_k^{(1)} + \beta^{q^2} X_k^{(2)} + \cdots + \beta^{q^{m-1}} X_k^{(m-1)}, \end{aligned} \tag{15}$$

where $X_k^{(i)} \stackrel{\text{def}}{=} \sum_n x_n w_{nk}^{(i)}$ is the ith vector space component of X_k with respect to the basis $\{\beta^{q^i}\}$.

Since the proposed Hartley transform is

$$\tilde{X}_k = \operatorname{tr}(\alpha X_k) = \sum_n x_n w_{nk}^{(0)} = X_k^{(0)}, \tag{16}$$

i.e., $\tilde{X}_k$ is assigned the 0th component of X_k, one may wonder what happened to the other components of X_k? Recall from Section III (8) that

$$\begin{aligned} X_k = \varphi^{-1}(\tilde{X}_k) = \beta\tilde{X}_k + \beta^q \tilde{X}_{kq^{m-1}} \\ + \beta^{q^2}\tilde{X}_{kq^{m-2}} + \cdots + \beta^{q^{m-1}}\tilde{X}_{kq}. \end{aligned} \tag{17}$$

Since the representation of an element with respect to a given basis is unique, comparing (15) and (17), we see that

$$\begin{aligned} \tilde{X}_k &= X_k^{(0)} \\ \tilde{X}_{kq} &= X_k^{(m-1)} \\ \tilde{X}_{kq^2} &= X_k^{(m-2)} \cdots \\ \tilde{X}_{kq^{m-1}} &= X_k^{(1)}. \end{aligned} \tag{18}$$

Thus, the proposed transform distributed the m components (with respect to the normal basis $\{\beta^{q^i}\}$) of X_k amongst $\tilde{X}_k, \tilde{X}_{kq}, \tilde{X}_{kq^2}, \cdots$. What is the significance of the normal basis? As we shall see, the choice of a normal basis is crucial in ensuring that the distribution operation is consistent. Its function is to decouple completely the m vector space components of X_k.

To illustrate this decoupling mechanism, consider the following question: given that the input data is in the basefield $\boldsymbol{B}$ and hence the DFT of the data satisfies the conjugacy relation

$$X_{kq^i} = X_k^{q^i}, \qquad \forall i,$$

what is the choice of basis which expresses this conjugacy relation in the simplest form: The answer apparently, is a normal basis. Let $\{\beta^{q^i}\}$ be an ormal basis, then the conjugacy class of X_k with respect to $\{\beta^{q^i}\}$ is

$$\begin{aligned} X_k &= \beta X_k^{(0)} + \beta^q X_k^{(1)} + \beta^{q^2} X_k^{(2)} \\ &\quad + \cdots + \beta^{q^{m-1}} X_k^{(m-1)} \\ X_{kq} = X_k^q &= \beta X_k^{(m-1)} + \beta^q X_k^{(0)} + \beta^{q^2} X_k^{(1)} \\ &\quad + \cdots + \beta^{q^{m-1}} X_k^{(m-2)} \\ X_{kq^2} = X_k^{q^2} &= \beta X_k^{(m-2)} + \beta^q X_k^{(m-1)} + \beta^{q^2} X_k^{(0)} \\ &\quad + \cdots + \beta^{q^{m-1}} X_k^{(m-3)} \\ &\vdots \\ X_{kq^{m-1}} = X_k^{q^{m-1}} &= \beta X_k^{(1)} + \beta^q X_k^{(2)} + \beta^{q^2} X_k^{(3)} \\ &\quad + \cdots + \beta^{q^{m-1}} X_k^{(0)}. \end{aligned} \tag{19}$$

Thus, with respect to a normal basis, the conjugacy relation is simply a circular shift of the m components of X_k. This not only shows the decoupling nature of a normal basis, in addition it shows that there are (at most) m degrees of freedom within each conjugacy class. Clearly, if we know the m components of any element of the conjugacy class, or equivalently, the 0th component of each element of the conjugacy class, then we know the entire conjugacy class. Referring to (16), we see that the Hartley transform does precisely this: it picks out the 0th component of each element of the DFT.

While it is true that if one were to choose a non-normal basis then the components of a conjugacy class with respect to this basis still has (at most) m degrees of freedom and hence can be characterized by m components, the distribution of these components can be done consistently only then the basis is normal. Thus in order to ensure that (16) is well defined, it is necessary to use a normal basis $\{\beta^{q^i}\}$.

Finally, we note that the act of extracting a component of an element with respect to a basis is reminiscent of the action of projection operators in Hilbert spaces. We can thus view φ as a projection operator with domain $\boldsymbol{E}$ and range $\boldsymbol{B}$, and the Hartley transform as the image, under φ, of the DFT of $\{x_n\}$ onto the subspace spanned by β. We use the term "projection" loosely to convey the sense of the action of φ. We do not mean to imply that φ is a projection operator in the usual sense. For example $\varphi^2 \neq \varphi$.

VII. Fast Algorithms

As noted in the previous section, the Hartley transform can be viewed as a projection of the Fourier transform from the extension field $\boldsymbol{E}$ into the basefield $\boldsymbol{B}$ via the function φ,

$$\tilde{X}_k = \varphi(X_k) = \operatorname{tr}(\alpha X_k).$$

Thus, if $\mathcal{A}$ is a fast algorithm for the DFT, then by an abuse of notation, $\operatorname{tr}(\alpha\mathcal{A})$ will be a fast algorithm for the DHT. In what follows we will use this fact to derive fast algorithms for the Hartley transform. Specifically we will derive the Hartley equivalent of Cooley–Tukey, Radix-2(DIT), Radix-2(DIF), Rader, and the Prime Factor algorithms.

A. Cooley–Tukey Algorithm

Let W_N be an element of order $N = N_1N_2$, then $W_{N_1} \stackrel{\text{def}}{=} W_N^{N_2}$ is an element of order N_1 and $W_{N_2} \stackrel{\text{def}}{=} W_N^{N_1}$ is an element of order N_2. Write n and k as

$$n = n_1 + n_2N_1$$

$$k = k_2 + k_1N_2,$$

then the Cooley–Tukey FFT can be written as [8], [9],

$$X_{k_2+k_1N_2} = \sum_{n_1=0}^{N_1-1} W_{N_1}^{n_1k_1}\left\{W_N^{k_2n_1}\left(\sum_{n_2=0}^{N_2-1} x_{n_1+n_2N_1}W_{N_2}^{n_2k_2}\right)\right\}.$$

Let

$$W_N^{k_2n_1} = \sum_{l=0}^{m-1} w_{k_2n_1}^{(l)}\gamma_l$$

$$W_{N_1}^{n_1k_1} = \sum_{i=0}^{m-1} w_{n_1k_1}^{(i)}\beta^{q^i}$$

$$W_{N_2}^{n_2k_2} = \sum_{j=0}^{m-1} w_{n_2k_2}^{(j)}\beta^{q^j},$$

where $\{\gamma_l\}_{l=0}^{m-1}$ is an arbitrary basis of $\boldsymbol{E_B}$ and $\{\beta^{q^i}\}_{i=0}^{m-1}$ is a normal basis with dual $\{\alpha^{q^i}\}_{i=0}^{m-1}$, then

$$W_{N_2}^{k_2n_2}W_{N_1}^{k_1n_1}W_N^{k_2n_1} = \sum_{i,j,l=0}^{m-1}\gamma_l\beta^{q^i+q^j}w_{k_2n_1}^{(l)}w_{n_1k_1}^{(i)}w_{n_2k_2}^{(j)}.$$

Projecting $X_{k_2+k_1N_2}$ into the basefield via φ, we obtain

$$\begin{aligned}\tilde{X}_{k_2+k_1N_2} &= \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} x_{n_1+n_2N_1}\operatorname{tr}(\alpha W_{N_2}^{k_2n_2}W_{N_1}^{k_1n_1}W_N^{k_2n_1})\\ &= \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}\sum_{i,j,l=0}^{m-1}\operatorname{tr}(\alpha\gamma_l\beta^{q^i+q^j})x_{n_1+n_2N_1}\\ &\quad\cdot w_{k_2n_1}^{(l)}w_{n_1k_1}^{(i)}w_{n_2k_2}^{(j)}\\ &= \sum_{i,j,l=0}^{m-1}\operatorname{tr}(\alpha\gamma_l\beta^{q^i+q^j})\sum_{n_1=0}^{N_1-1} w_{n_1k_1}^{(i)}\\ &\quad\cdot\left\{w_{k_2n_1}^{(l)}\left(\sum_{n_2=0}^{N_2-1} x_{n_1+n_2N_1}w_{n_2k_2}^{(j)}\right)\right\}\\ &= \sum_{i,j,l=0}^{m-1}\operatorname{tr}(\alpha\gamma_l\beta^{q^i+q^j})\sum_{n_1=0}^{N_1-1} w_{n_1k_1q^{m-i}}^{(0)}\\ &\quad\cdot\left\{w_{k_2n_1}^{(l)}\left(\sum_{n_2=0}^{N_2-1} x_{n_1+n_2N_1}w_{n_2k_2q^{m-j}}^{(0)}\right)\right\}.\end{aligned}$$

Therefore, the Cooley–Tukey FHT is given by

$$\tilde{X}_{k_2+k_1N_2} = \sum_{i,j,l=0}^{m-1} c_{i,j,l}\sum_{n_1=0}^{N_1-1} w_{n_1k_1q^{m-i}}^{(0)}\cdot\left\{w_{k_2n_1}^{(l)}\left(\sum_{n_2=0}^{N_2-1} x_{n_1+n_2N_1}w_{n_2k_2q^{m-j}}^{(0)}\right)\right\}, \quad (20)$$

where

$$c_{i,j,l} \stackrel{\text{def}}{=} \operatorname{tr}(\alpha\gamma_l\beta^{q^i+q^j}) \qquad 0 \le i, j, l \le m-1$$

are constants that can be precomputed.

Though the expression looks complicated, we note that the inner parenthesis is simply the DHT of $\{x_{n_1+n_2N_1}\}_{n_2}$ evaluated at k_2q^{m-j}. Similarly, the outer paenthesis is the DHT of the sequence $\{w_{k_2n_1}^{(l)}(\sum_{n_2=0}^{N_2-1} x_{n_1+n_2N_1}w_{n_2k_2q^{m-j}}^{(0)})\}_{n_1}$ evaluated at k_1q^{m-i}. We thus have the following procedure for computing a Cooley–Tukey DHT.

1) Arrange the data in an N_2 by N_1 array.
2) Compute the DHT along each column.

$$C(n_1, k_2) = \sum_{n_2=0}^{N_2-1} x_{n_1+n_2N_1}w_{n_2k_2}^{(0)}.$$

3) For each j and l, $0 \le j,\ l \le m-1$, form

$$D_{j,l}(n_1, k_2) = w_{n_1k_2}^{(l)}C(n_1, k_2q^{m-j}).$$

4) For each j and l, $0 \le j,\ l \le m-1$, compute the DHT along each row of D.

$$E_{j,l}(k_1, k_2) = \sum_{n_1=0}^{N_1-1} D_{j,l}(n_1, k_2)w_{n_1k_1}^{(0)}.$$

5) For each k_1 and k_2, $0 \le k_1 \le N_1-1$ $0 \le k_2 \le N_2-1$, compute

$$\tilde{X}_{k_2+k_1N_2} = \sum_{i,j,l=0}^{m-1} c_{i,j,l}F_{i,j,l}(k_1, k_2),$$

where $F_{i,j,l}(k_1, k_2) \stackrel{\text{def}}{=} E_{j,l}(k_1q^{m-i}, k_2)$.

What is the (multiplicative) complexity of the Cooley–Tukey FHT? From the procedure, we see that step 2) requires N_1 DHT's of size N_2, step 4) requires m^2N_2 DHT's of size N_1, and steps 3) and 5) require m^2N and m^3N multiplications respectively. Denoting the complexity of a size N DHT by $\mu(N)$, we see that the complexity of the Cooley–Tukey DHT is

$$\mu(N_1N_2) = N_1\mu(N_2) + m^2N_2\mu(N_1) + m^2N + m^3N. \quad (21)$$

If N_1 and N_2 are composite, the above procedure can be repeated for the smaller transforms.

1) Radix-2 (DIT) Algorithm: An important special case of the Cooley–Tukey algorithm results when N is divisible by 2. By taking $N_1 = 2$ and $N_2 = N/2$, we have the following Radix-2 Decimation-In-Time algorithm:

$$\tilde{X}_k = \tilde{X}_k^{(\text{even})} + \sum_{j=0}^{m-1} c_{j,k}\tilde{X}_{kq^{m-j}}^{(\text{odd})}, \qquad 0 \le k \le N/2-1 \quad (22)$$

$$\tilde{X}_{k+N/2} = \tilde{X}_k^{(\text{even})} - \sum_{j=0}^{m-1} c_{j,k} \tilde{X}_{kq^{m-j}}^{(\text{odd})}, \quad 0 \le k \le N/2-1, \quad (23)$$

where

$$\tilde{X}_k^{(\text{even})} \stackrel{\text{def}}{=} \sum_{n=0}^{N/2-1} x_{2n} w_{nk}^{(0)}$$

is the DHT of the even-indexed input,

$$\tilde{X}_k^{(\text{odd})} \stackrel{\text{def}}{=} \sum_{n=0}^{N/2-1} x_{2n+1} w_{nk}^{(0)}$$

is the DHT of the odd-indexed input, and

$$c_{j,k} \stackrel{\text{def}}{=} \sum_{l=0}^{m-1} w_k^{(l)} \operatorname{tr}(\alpha\gamma_l \beta^{q^j})$$

are constants which can be precomputed.

Clearly, this procedure requires $mN/2$ multiplications and 2 DHT's of size $N/2$. The multiplicative complexity of the Radix-2 DIT FHT is therefore

$$\mu(N) = 2\mu(N/2) + mN/2. \quad (24)$$

If N is a power of 2, the procedure can be recursively applied to the half-size DHT's.

2) Radix-2 (DIF) Algorithm: By reversing the roles of N_1 and N_2 in the Radix-2 Decimation-in-Time algorithm, we arrive at the following Radix-2 Decimation-in-Frequency algorithm:

$$\tilde{X}_{2k} = \sum_{n=0}^{N/2-1} (x_n + x_{N/2+n}) w_{nk}^{(0)}, \quad 0 \le k \le N/2-1 \quad (25)$$

$$\tilde{X}_{2k+1} = \sum_{l,j=0}^{m-1} c_{l,j} \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) w_n^{(l)} w_{nk}^{(0)}, \quad 0 \le k \le N/2-1, \quad (26)$$

where $c_{l,j} \stackrel{\text{def}}{=} \operatorname{tr}(\alpha\gamma_l \beta^{q^j})$ are constants which can be precomputed.

This procedure requires $(m+1)$ DHT's of size $N/2$ plus $(m+m^2)N/2$ multiplications. Thus the complexity of the Radix-2 DIF FHT is

$$\mu(2 \cdot N/2) = (m+1)\mu(N/2) + \left(\frac{m}{2} + \frac{m^2}{2}\right) N. \quad (27)$$

As before, the procedure can be applied recursively to the half-size DHT's when N is a power of 2.

B. Prime Factor Algorithm

Let $N = N_1 N_2$ with N_1 and N_2 relatively prime. Using the input mapping

$$n_1 = n (\text{mod}\, N_1)$$
$$n_2 = n (\text{mod}\, N_2)$$

and the output mapping

$$k = k_1 N_2 + k_2 N_1 (\text{mod}\, N),$$

the prime factor algorithm for the Fourier transform of $\{x_n\}$ can be expressed as [8]

$$X_{k_1 k_2} = \sum_{n_1=0}^{N_1-1} W_{N_1}^{n_1 k_1} \left\{ \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} W_{N_2}^{n_2 k_2} \right\}.$$

Let $\{\beta^{q^i}\}_{i=0}^{m-1}$ be a normal basis with dual $\{\alpha^{q^i}\}_{i=0}^{m-1}$. With respect to it, let $W_{N_1}^{k_1 n_1}$ and $W_{N_2}^{k_2 n_2}$ have the following expansions

$$W_{N_1}^{n_1 k_1} = \sum_{i=0}^{m-1} w_{n_1 k_1}^{(i)} \beta^{q^i}$$
$$W_{N_2}^{n_2 k_2} = \sum_{i=0}^{m-1} w_{n_2 k_2}^{(j)} \beta^{q^j}.$$

Then,

$$W_{N_1}^{n_1 k_1} W_{N_2}^{n_2 k_2} = \sum_{i,j=0}^{m-1} w_{n_1 k_1}^{(i)} w_{n_2 k_2}^{(j)} \beta^{q^i + q^j}.$$

The projection of the DFT into the basefield $\boldsymbol{B}$ is

$$\begin{aligned}
&\tilde{X}_{k_1 k_2} \\
&= \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} \operatorname{tr}(\alpha W_{N_1}^{n_1 k_1} W_{N_2}^{n_2 k_2}) \\
&= \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} \sum_{i,j=0}^{m-1} \operatorname{tr}(\alpha \beta^{q^i + q^j}) w_{n_1 k_1}^{(i)} w_{n_2 k_2}^{(j)} \\
&= \sum_{i,j=0}^{m-1} \operatorname{tr}(\alpha \beta^{q^i + q^j}) \sum_{n_1=0}^{N_1-1} w_{n_1 k_1}^{(i)} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} w_{n_2 k_2}^{(j)} \\
&= \sum_{i,j=0}^{m-1} \operatorname{tr}(\alpha \beta^{q^i + q^j}) \sum_{n_1=0}^{N_1-1} w_{n_1 k_1 q^{m-i}}^{(0)} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} w_{n_2 k_2 q^{m-j}}^{(0)}.
\end{aligned}$$

As before the trace term is but a constant while the expression following the trace is a true 2-D DHT (i.e., no twiddle factors) evaluated at $(k_1 q^{m-i}, k_2 q^{m-j})$. Thus, if we define $c_{i,j} \stackrel{\text{def}}{=} \operatorname{tr}(\alpha \beta^{q^i + q^j})$ and $\hat{X}_{k_1,k_2} \stackrel{\text{def}}{=} \sum_{n_1=0}^{N_1-1} w_{n_1 k_1}^{(0)} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} w_{n_2 k_2}^{(0)}$, then the prime factor DHT algorithm can be written as

$$\tilde{X}_{k_1 k_2} = \sum_{i,j=0}^{m-1} c_{i,j} \hat{X}_{k_1 q^{m-i}, k_2 q^{m-j}}. \quad (28)$$

We thus have the following procedure for computing a prime factor FHT.

1) Place data into an N_1 by N_2 array.
2) Compute the DHT along each row.
3) Compute the DHT along each column.
4) For each k_1 and k_2, compute

$$\tilde{X}_{k_1 k_2} = \sum_{i,j=0}^{m-1} c_{i,j} \hat{X}_{k_1 q^{m-i}, k_2 q^{m-j}}.$$

The procedure requires N_1 DHTs of size N_2, N_2 DHT's of size N_1 and $m^2 N$ multplications. The complexity of the prime factor algorithm is, therefore,

$$\mu(N_1 N_2) = N_1 \mu(N_2) + N_2 \mu(N_1) + m^2 N. \qquad (29)$$

C. Rader's Algorithm

It is well known that for p prime, a length p DFT can be computed by a $(p-1)$-point cyclic convolution using Rader's algorithm [8], [10]. Let π be a primitive element of GF(p). Then Rader's algorithm can be written as [8], [10],

$$X_0 = \sum_{n=0}^{p-1} x_n$$

$$X_{\pi^k} = x_0 + \sum_{n=0}^{p-2} W_p^{\pi^{k-n}} x_{\pi^{p-1-n}}, \qquad 1 \le k \le p-1.$$

By defining $\hat{X}_k \stackrel{\text{def}}{=} X_{\pi^k}$ and $\hat{x}_k \stackrel{\text{def}}{=} x_{\pi^{p-1-k}}$, this can be put in the simpler form

$$X_0 = \sum_{n=0}^{p-1} x_n$$

$$\hat{X}_k = x_0 + \sum_{n=0}^{p-2} W_p^{\pi^{k-n}} \hat{x}_n, \qquad 1 \le k \le p-1.$$

Applying φ to each of the equations we obtain the following analog of Rader's algorithm for the Hartley transform

$$\tilde{X}_0 = \operatorname{tr}(\alpha) \left(\sum_{n=0}^{p-1} x_n \right)$$

$$\tilde{\hat{X}}_k = x_0 \operatorname{tr}(\alpha) + \sum_{n=0}^{p-2} w_{\pi^{k-n}}^{(0)} \hat{x}_n, \qquad 1 \le k \le p-1. \qquad (30)$$

Note that the summation in the second equation is a $(p-1)$-point cyclic convolution. We thus have the following procedure for computing a length p DHT.

1) Compute $\tilde{X}_0$ according to the first equation.
2) Compute the cyclic convolution of $\{w_{\pi^l}^{(0)}\}_l$ and $\{\hat{x}_l\}_l$.
3) Add $x_0 \operatorname{tr}(\alpha)$ to the result of Step 2).

Since steps 1) and 3) require one multiplication each and step 2) requires $2(p-1)-j$ where j is the number of divisors of $p-1$ [8], the algorithm thus has complexity

$$\mu(p) = 2 + 2(p-1) - j. \qquad (31)$$

VIII. Hartley Transform over R Revisited

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

$$\operatorname{tr}(\alpha) = \alpha + \alpha^*$$

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

We derive, in Appendix A, the classes of real transforms and self-inverse real transforms admissible under this type of construction. It is seen that the real transforms are essentially Ansari's discrete combinational Fourier transforms for real input [13] and the self-inverse real transforms are essentially the Hartley transforms.

In Appendix B, we apply the fast algorithms derived in Sectio VII to the case of real input. It is seen that the method of projection produces known fast Hartley algorithms without resorting to trigonometric identities and algebraic manipulations. In one instance (PFA), the method produces a new algorithm which is a variation of an existing algorithm.

IX. Conclusion

We have presented a general framework for constructing basefield transforms having a convolution propertry. The construction is carried out over finite fields but is shown to apply to the real case as well. Fast algorithms for the computation of this new transform were also derived.

The technique presented can be generalized to an arbitrary field $\boldsymbol{B}$ by taking $\boldsymbol{E}$ to be the Nth cyclotomic extension of $\boldsymbol{B}$. For details see [19].

Appendix A

In this appendix, we apply the techniques developed for finite fields to the real and complex fields. We will start by determining the normal bases of $\boldsymbol{C}_{\boldsymbol{R}}$. Since $\boldsymbol{C}$ is a two dimensional vector space over $\boldsymbol{R}$, a normal basis of $\boldsymbol{C}_{\boldsymbol{R}}$ 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

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

The constraint forces $c = 1/4a$ and $d = -1/4b$, consequently the normal bases of $\boldsymbol{C}_{\boldsymbol{R}}$ and their corresponding dual bases are exactly

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

$$B = \{\beta, \beta^*\} = \left\{ \frac{1}{4a} - i\frac{1}{4b}, \frac{1}{4a} + i\frac{1}{4b} \right\},$$

where $a, b \in \boldsymbol{R}$ are arbitrary.

Over the complex field, the elements of order N are

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

It follows that

$$\operatorname{tr}(\alpha W_N^k) = 2a\cos\frac{2\pi}{N}mk + 2b\sin\frac{2\pi}{N}mk$$
$$\operatorname{tr}(\beta W_N^{-k}) = \frac{1}{2a}\cos\frac{2\pi}{N}mk + \frac{1}{2b}\sin\frac{2\pi}{N}mk,$$

which yield the following real transforms

$$\tilde{X}_k = \sum_{n=0}^{N-1} x_n \operatorname{tr}(\alpha W_N^{nk})$$
$$= \sum_{n=0}^{N-1} x_n\left[2a\cos\frac{2\pi}{N}nmk + 2b\sin\frac{2\pi}{N}nmk\right] \quad (32)$$

$$x_k = N^{-1}\sum_{n=0}^{N-1}\tilde{X}_n \operatorname{tr}(\beta W_N^{-nk})$$
$$= N^{-1}\sum_{n=0}^{N-1}\tilde{X}_n\left[\frac{1}{2a}\cos\frac{2\pi}{N}nmk + \frac{1}{2b}\sin\frac{2\pi}{N}nmk\right]. \quad (33)$$

For $m = 1$, (32) and (33) reduce to Ansari's discrete combinational Fourier transforms for real input [13]

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

Let us now impose the self-inverse condition on (32) and (33). By Proposition 1, the transforms defined by (32) and (33) will have the self-inverse property iff equation (13) is satisfied. This means that we must have, for all k

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

which is satisfied only if

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

Substituting these values into (32) and (33) yields the following self-inverse real transforms

$$\tilde{X}_k = \sum_{n=0}^{N-1} x_n\left[(\pm)\cos\frac{2\pi}{N}nmk + (\pm)\sin\frac{2\pi}{N}nmk\right] \quad (34)$$

$$x_k = N^{-1}\sum_{n=0}^{N-1}\tilde{X}_n\left[(\pm)\cos\frac{2\pi}{N}nmk + (\pm)\sin\frac{2\pi}{N}nmk\right]. \quad (35)$$

There are thus $4\phi(N)$ 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 conclude this appendix by deriving the convolution property of the Hartley transform. By (14), the convolution property (adapted for the real field) is given by

$$\tilde{Y}_k = \operatorname{tr}(\alpha\beta\beta)\tilde{H}_k\tilde{X}_k + \operatorname{tr}(\alpha\beta\beta^*)\tilde{H}_k\tilde{X}_{-k}$$
$$+\operatorname{tr}(\alpha\beta^*\beta)\tilde{H}_{-k}\tilde{X}_k + \operatorname{tr}(\alpha\beta^*\beta^*)\tilde{H}_{-k}\tilde{X}_{-k}.$$

As previously indicated, 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

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

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

$$\tilde{Y}_k = \frac{1}{2}\tilde{H}_k\tilde{X}_k + \frac{1}{2}\tilde{H}_k\tilde{X}_{-k} + \frac{1}{2}\tilde{H}_{-k}\tilde{X}_k - \frac{1}{2}\tilde{H}_{-k}\tilde{X}_{-k}$$
$$= \tilde{H}_k\left(\frac{\tilde{X}_k + \tilde{X}_{-k}}{2}\right) + \tilde{H}_{-k}\left(\frac{\tilde{X}_k - \tilde{X}_{-k}}{2}\right)$$
$$= \tilde{H}_k\tilde{X}_k^{(\text{even})} + \tilde{H}_{-k}\tilde{X}_k^{(\text{odd})}$$

which is as expected [11].

Appendix B

In this appendix, we will apply the techniques of Sections VII to derive fast algorithms for Hartley transforms over the reals. The derivations consist of nothing more than recasting the formulae of Section VII in the setting of $\boldsymbol{R}$ since the methodology of the derivation there is independent of the underlying fields. Retracing the steps of the derivations, it is seen that the only property invoked which is particular to finite fields is the statement of the conjugacy relationship. By replacing such expressions with their counterparts in $\boldsymbol{C}_{\boldsymbol{R}}$, we have the equivalent fast algorithms for the real input case. More explicitly, to obtain fast algorithms for real Hartley transforms we substitute every occurrence of $\{\tilde{X}_{kq^i}\}_{i=0}^{m-1}$ in the formulae of Section VII with $\{\tilde{X}_{(-1)^i k}\}_{i=0}^{1} = \{\tilde{X}_k, \tilde{X}_{-k}\}$. We do this below for three cases: Radix-2(DIT), Radix-2(DIF), and PFA. The same technique can be applied to other algorithms.

As shown in Appendix A, the real Hartley transform corresponds to choosing the bases

$$\{\alpha_0, \alpha_1\} = \{\alpha, \alpha^*\} = \left\{\frac{1}{2}(1+i), \frac{1}{2}(1-i)\right\}$$
$$\{\beta_0, \beta_1\} = \{\beta, \beta^*\} = \left\{\frac{1}{2}(1-i), \frac{1}{2}(1+i)\right\}, \quad (36)$$

which we will assume for the remainder of the appendix. In addition, we will take the basis $\{\gamma_i\}$ to be

$$\{\gamma_0, \gamma_1\} = \{-1, -i\}, \quad (37)$$

with respect to which we have

$$w_k^{(0)} = \cos\frac{2\pi}{N}k, \qquad w_k^{(1)} = \sin\frac{2\pi}{N}k.$$

Radix-2(DIT) Algorithm

To obtain a real radix-w decimation-in-time algorithm[2] we recast equation (22) in $\boldsymbol{R}$ by reexpressing the conjugacy relation to obtain

$$\tilde{X}_k = \tilde{X}_k^{(\text{even})} + \sum_{j=0}^{1} c_{j,k} \tilde{X}_{(-1)^j k}^{(\text{odd})}, \tag{38}$$

where the constants $c_{j,k}$ are given by

$$c_{j,k} = \sum_{l=0}^{1} w_k^{(l)} \operatorname{tr}(\alpha\gamma_l\beta_j).$$

Using the bases (36),(37), it is easy to verify that

$$\operatorname{tr}(\alpha\gamma_0\beta_0) = \operatorname{tr}(\alpha\gamma_1\beta_1) = 1,$$
$$\operatorname{tr}(\alpha\gamma_1\beta_0) = \operatorname{tr}(\alpha\gamma_0\beta_1) = 0,$$

therefore,

$$c_{0,k} = \sum_{l=0}^{1} w_k^{(l)} \operatorname{tr}(\alpha\gamma_l\beta_0) = w_k^{(0)} = \cos\frac{2\pi}{N}k$$
$$c_{1,k} = \sum_{l=0}^{1} w_k^{(l)} \operatorname{tr}(\alpha\gamma_l\beta_1) = w_k^{(1)} = \sin\frac{2\pi}{N}k.$$

Substituting these values of $c_{j,k}$ into (38) yields the following radix-2 DIT algorithm

$$\tilde{X}_k = \tilde{X}_k^{(\text{even})} + \tilde{X}_k^{(\text{odd})}\left(\cos\frac{2\pi}{N}k\right) + \tilde{X}_{-k}^{(\text{odd})}\left(\sin\frac{2\pi}{N}k\right). \tag{39}$$

This we recognize as the radix-2 algorithm proposed originally by Bracewell [12].

Radix-2(DIF) Algorithm

To obtain a radix-2 decimation-in-frequency algorithm we proceed as before by recasting the finite field algorithm in $\boldsymbol{R}$. Restating the conjugacy relation in (25) and (26) we have

$$\tilde{X}_{2k} = \tilde{X}_k^{(\dagger)}$$
$$\tilde{X}_{2k+1} = \sum_{l,j=0}^{1} c_{l,j} \tilde{X}_{(-1)^j k}^{(l)}, \tag{40}$$

where

$$\tilde{X}_k^{(\dagger)} = \sum_{n=0}^{N/2-1} (x_n + x_{N/2+n}) w_{nk}^{(0)}$$
$$\tilde{X}_k^{(l)} = \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) w_n^{(l)} w_{nk}^{(0)}$$
$$c_{l,j} = \operatorname{tr}(\alpha\gamma_l\beta_j).$$

Using the bases (36) and (37), we have, from the previous section

$$c_{0,0} = c_{1,1} = \operatorname{tr}(\alpha\gamma_0\beta_0) = \operatorname{tr}(\alpha\gamma_1\beta_1) = 1,$$
$$c_{1,0} = c_{0,1} = \operatorname{tr}(\alpha\gamma_1\beta_0) = \operatorname{tr}(\alpha\gamma_0\beta_1) = 0,$$

[2]We have elected to combine (22) and (23) into one equation in order to retain Bracewell's original formulation [12]. In practice, the computation should be performed as indicated by (22) and (23) in order to avoid unnecessary multiplications.

thus (40) becomes

$$\tilde{X}_{2k} = \tilde{X}_k^{(\dagger)}$$
$$\tilde{X}_{2k+1} = \tilde{X}_k^{(0)} + \tilde{X}_{-k}^{(1)}.$$

Since

$$\tilde{X}_k^{(\text{even})} = \sum_{n=0}^{N/2-1} (x_n + x_{N/2+n}) \operatorname{cas}\left(\frac{2\pi}{N/2}nk\right)$$
$$\tilde{X}_k^{(0)} = \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) \cos\left(\frac{2\pi}{N}n\right) \operatorname{cas}\left(\frac{2\pi}{N/2}nk\right)$$
$$\tilde{X}_k^{(1)} = \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) \sin\left(\frac{2\pi}{N}n\right) \operatorname{cas}\left(\frac{2\pi}{N/2}nk\right)$$

where

$$\operatorname{cas} x \overset{\text{def}}{=} \cos x + \sin x,$$

the previous equations can be rearranged to yield the following decimation-in-frequency algorithm

$$\tilde{X}_{2k} = \sum_{n=0}^{N/2-1} (x_n + x_{N/2+n}) \operatorname{cas}\left(\frac{2\pi}{N/2}nk\right) \tag{41}$$

$$\tilde{X}_{2k+1} = \sum_{n=0}^{N/2-1} \left[(x_n - x_{N/2+n}) \cos\left(\frac{2\pi}{N}n\right) + (x_{N/2-n} - x_{N-n}) \sin\left(\frac{2\pi}{N}n\right)\right] \operatorname{cas}\left(\frac{2\pi}{N/2}nk\right) \tag{42}$$

These equations we recognize as the radix-2 DIF algorithm of Sorensen *et al.* [16].

Prime Factor Algorithm

Finally, let us derive a prime factor algorithm for real Hartley transforms. With all the necessary assumptions the prime factor algorithm can be written as

$$\tilde{X}_{k_1 k_2} = \sum_{i,j=0}^{1} c_{i,j} \hat{X}_{(-1)^i k_1, (-1)^j k_2}, \tag{43}$$

where

$$c_{i,j} = \operatorname{tr}(\alpha\beta_i\beta_j)$$
$$\hat{X}_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} w_{n_1 k_1}^{(0)} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} w_{n_2 k_2}^{(0)}.$$

Using the bases (36) and (37), it is easy to verify that

$$c_{0,0} = \operatorname{tr}(\alpha\beta_0\beta_0) = \frac{1}{2}$$
$$c_{0,1} = c_{1,0} = \operatorname{tr}(\alpha\beta_0\beta_1) = \frac{1}{2}$$
$$c_{1,1} = \operatorname{tr}(\alpha\beta_1\beta_1) = -\frac{1}{2},$$

which when substituted into (43) gives the following real prime factor algorithm

$$\tilde{X}_{k_1 k_2} = \frac{1}{2}[\hat{X}_{k_1,k_2} + \hat{X}_{-k_1,k_2} + \hat{X}_{k_1,-k_2} - \hat{X}_{-k_1,-k_2}], \tag{44}$$

where

$$\hat{X}_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} \operatorname{cas}\left(\frac{2\pi}{N_1} n_1 k_1\right) \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} \operatorname{cas}\left(\frac{2\pi}{N_2} n_2 k_2\right). \tag{45}$$

This is a new algorithm that is a variation of an existing algorithm (see [16]).Note that it is a true two-dimensional DHT (45) followed by a linear combination of elements at the four conjugate locations (44).

REFERENCES

[1] R. Lidl and H. Neiderreiter, *Finite Fields* (Encyclopedia of Mathematics and Its Applications, Vol.20). Reading, MA: Addison-Wesley, 1983.

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

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

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

[5] ——, *Topics in Algebra.* New York: Xerox Publishing, 1975.

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

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

[8] ——, *Fast Algorithms for Digital Signal Processing.* Reading, MA: Addison-Wesley, 1986.

[9] J. W. Cooley and J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series," *Math. of Computat.*, vol. 19, no. 2, pp. 297–301, Apr. 1965.

[10] C. M. Rader, "Discrete Fourier transforms when the number of data samples is prime," *Proc. IEEE*, vol. PROC-56, pp. 1107–1108, June 1968.

[11] R. N. Bracewell, "Discrete Hartley transforms," *J. Opt. Soc. Amer.*, vol. 73, no. 12, pp. 1832–1835, Dec. 1983.

[12] ——, "The fast Hartley transform," *Proc. IEEE*, vol. 72, no. 8, pp. 1010–1018, Aug. 1984.

[13] R. Ansari, "An extension of the discrete Fourier transform," *IEEE Trans. Circuits Syst.*, vol. CS-32, no. 6, pp. 618–619, June 1985.

[14] P. Duhamel and M. Vetterli, "Fast Fourier transforms: A tutorial review and a state of the art," *Signal Processing*, vol. 19, no. 4, pp. 259–299, Apr. 1990.

[15] ——, "Improved Fourier and Hartley transform algorithms. Application to cyclic convolution of real data," *IEEE Trans. on Acoust., Speech, Signal Processing*, vol. 35, no. 6, pp. 818–824, June 1987.

[16] H. V. Sorensen, D. L. Jones, C. S. Burrus, and M. T. Heideman, "On computing the discrete Hartley transform," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. 33, no. 5, pp. 1231–1238, Oct. 1985.

[17] J. J. Hong and M. Vetterli, "Hartley transforms over finite fields," in *Proc. 24th Asilomar Conf. Signals, Syst., and Comput.*, Nov. 1989, pp. 103–107.

[18] ——, "Computing m DFT's over GF(q) with one DFT over GF(q^m)," *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 271–274, Jan. 1993.

[19] J. J. Hong, "Finite field transforms for signal processing," Ph.D. dissertation, in preparation, Columbia Univ., 1993.