Basefield Transforms with the Convolution Property

JONATHAN HONG, MARTIN VETTERLI, SENIOR MEMBER, IEEE, AND PIERRE DUHAMEL, MEMBER, IEEE

Invited Paper

We present a general framework for constructing transforms in the field of the input which have a convolution-like property. The construction is carried out over the reals, but is shown to be valid over more general fields. We show that these basefield transforms can be viewed as "projections" of the discrete Fourier transform (DFT). Furthermore, by imposing an additional condition on the projections, one may obtain self-inverse versions of the basefield transforms. Applying the theory to the real and complex fields, we show that the projection of the complex DFT results in the discrete combinational Fourier transform (DCFT) and that the imposition of the self-inverse condition on the DCFT yields the discrete Hartley transform (DHT). Additionally, we show that the method of projection may be used to derive efficient basefield transform algorithms by projecting standard FFT algorithms from the extension field to the basefield. Using such an approach, we show that many of the existing real Hartley algorithms are projections of well-known FFT algorithms.

I. Introduction

The discrete Hartley transform (DHT) has been proposed as a real transform with a convolution property and is thus an alternative to the discrete Fourier transform (DFT) for the convolution of real sequences [1]. While the Hartley transform offers no advantages over the Fourier transform in terms of computational complexity, it does offer certain structural advantages over the Fourier transform owing to the fact that the Hartley transform is a *real* transform that is also *involutionary* (self-inverse). This property avoids the storage of both the forward and the inverse transforms in applications where resources are scarce. Since its introduction by Bracewell in 1983, much work has gone into the analysis of the properties of the Hartley transform and its fast implementation [1], [2], [8], [10], [26]. Much of this work draws on the close relationship between the Hartley and Fourier transforms. A cursory examination of the two transforms reveals that the kernel of the Hartley transform is the difference of the real and imaginary parts of the Fourier transform kernel. While that is true and goes a long way toward developing the theory of the Hartley transform, it does not tell the whole story. There is in fact a deeper connection between the Hartley and the Fourier transform that unifies the two transforms along with other real transforms such as Ansari's discrete combinational Fourier transform (DCFT) [7]. In this paper, we will attempt to draw out the relations between these various transforms. Our approach will be from the point of view of field extensions and projections. This approach not only demonstrates the intimate connection between the various transforms, it also presents a framework for developing Hartley and other basefield transforms over fields other than the reals. Moreover, the approach permits easy development of fast algorithms based on standard FFT algorithms.

Uses of the Hartley transform as such are the same ones as those of the Fourier transform, the strongest difference being its involutionary property. Hence, the specific uses are not described in the paper. Several properties of the Hartley transform were obtained by trigonometric manipulations, which were at first thought to be specific to the Hartley domain. The strength of the approach explained in this paper is that not only does it show that these properties should be shared with the Fourier domain, but it also provides a way of deriving them. This is true for the fast algorithms where the search for FFT's with a reduced complexity when the data are real-valued was an active research area for a long time. The task of eliminating the redundancies in the computation while keeping a simple structure of the algorithm was quite involved. In this paper, we show that the real version of the Hartley Prime Factor Algorithm,

Manuscript received April 16, 1993; revised August 31, 1993.

J. Hong is with the Department of Electrical Engineering and Center for Telecommunications Research, Columbia University, New York, NY 10027-6699.

M. Vetterli was with the Department of Electrical Engineering and Center for Telecommunications Research, Columbia University, New York, NY 10027-6699. He is now with the Department of Electrical Engineering and Computer Science, University of California at Berkeley, Berkeley, CA 94720.

P. Duhamel is with Télécom Paris / URA 280, 75634 Paris, Cedex 13, France.

IEEE Log Number 9215538.

while difficult to obtain in a direct manner, can be straightforwardly derived using a projection method described later. Moreover, the spirit of the method can be applied to other domains: transforms which exist only in an extension field compared to the domain where the data are defined have applications, for example, in error-control coding.

We will confine the details in this paper to the real case. However, the discussion will purposely be left general so that the technique is easily extended to other fields of interest. In Section II, we set up the framework for our discussion with a quick summary of fields and field extensions. We will discuss the notion of a *normal basis* and a *dual basis* and present the *trace* function as a linear functional on the extension field. In Section III, we will use the apparatus developed in Section II to derive the discrete basefield transform (DBT) and its inverse as the "projection" of the Fourier transform from the field of complex numbers into the field of real numbers. It will be seen that the discrete basefield transform is essentially Ansari's discrete combinational Fourier transform. In Section IV, we will show that by imposing the "self-inverse" condition on the DBT, we obtain a class of involutionary transforms that includes among them, the conventional Hartley transform. In Section V, we will derive the convolution property of the Hartley transform via the method of projection. We will show that by mapping sequences between the Fourier and Hartley domain, one can deduce effortlessly Bracewell's Hartley Convolution Theorem. In Section VI, we will explain the use of the term "projection" and show why normal bases are the natural settings for expressing conjugacy relations. In Section VII, we consider fast algorithms for the Hartley transform. We will show that all existing fast Hartley transform algorithms may be derived as projections of existing fast Fourier transform algorithms. The technique bypasses the usual trignometric derivations and produces, in the Prime Factor case, a variant of an existing algorithm. Finally, in Section VIII, we briefly sketch how the technique presented may be extended to other fields of interest.

Due to the technical nature of the subject and our desire to maintain mathematical rigor, precise mathematical terms are used throughout the paper. In order to avoid disrupting the flow of the presentation, the definitions of many of the terms are given in the Appendix rather than in the body of the text. Such terms are *italicized* the first time they occur.

II. Fields and Field Extensions

In this section, we will review some simple facts from Algebra regarding fields and field extensions. By casting the DFT, the DCFT, and the DHT in the setting of fields, we will be able to draw out the connections between these heretofore unrelated transforms. That fields are the proper settings for discussing the various transforms will be seen in Section VIII, where we use the framework developed here to construct the counterparts of the aforementioned transforms in more general fields. We will confine our development here to the real/complex case with a brief mention of the general case at the end of the section.

Let $\boldsymbol{R}$ be the real numbers and $\boldsymbol{C}$ the field of complex numbers. Then in addition to being an extension of $\boldsymbol{R}$ of degree 2, $\boldsymbol{C}$ is also a vector space of dimension 2 over $\boldsymbol{R}$. As such, there exist 2 vectors α_0 and α_1 such that $\{\alpha_0, \alpha_1\}$ is a basis for $\boldsymbol{C}$ over $\boldsymbol{R}$ (notation: $\boldsymbol{C_R}$). The canonical basis for $\boldsymbol{C_R}$ is, of course, the usual basis $\{1, i\}$ (hence all elements in $\boldsymbol{C}$ may be written in the form $a+ib$, $a, b \in \boldsymbol{R}$). $\{1, i\}$, however, is not the only possible basis—any basis consisting of two linearly independent vectors over $\boldsymbol{R}$ will do just as well. Of particular importance to us are bases of the form $\{\alpha, \alpha^*\}$, i.e., the basis elements are *complex conjugates* of each other. Bases of this form are called *normal bases*. Examples of normal bases are $\{1+i, 1-i\}$ and $\{e+i\pi, e-i\pi\}$. More generally, it can be shown that all normal bases for $\boldsymbol{C_R}$ are of the form

$$\{\alpha, \alpha^*\} = \{a+ib, a-ib\}, \qquad a, b \in \boldsymbol{R},\ ab \neq 0. \quad (1)$$

Normal bases are important because (as we shall see later) they provide the natural setting for expressing conjugacy relations.

Considering $\boldsymbol{C_R}$ as a vector space, a *linear functional* on $\boldsymbol{C_R}$ is a linear map φ from $\boldsymbol{C}$ to $\boldsymbol{R}$. As we will show in the next section, all linear functionals on $\boldsymbol{C_R}$ are given by the *trace* function

$$\varphi(\zeta) = \mathrm{Tr}(\zeta) = \zeta + \zeta^*, \quad \forall \zeta \in \boldsymbol{C}. \quad (2)$$

The trace function, in addition to being linear, is also invariant under conjugates, i.e.

$$\mathrm{Tr}(\zeta) = \mathrm{Tr}(\zeta^*), \quad \forall \zeta \in \boldsymbol{C}. \quad (3)$$

The trace function will play the important role of a projection operator in subsequent constructions.

Given a basis $\{\alpha_0, \alpha_1\}$ for $\boldsymbol{C_R}$, the *dual basis* of $\{\alpha_0, \alpha_1\}$ is defined as the basis $\{\beta_0, \beta_1\}$ such that α_i and β_j are *trace-orthogonal* for all i and j, i.e.

$$\mathrm{Tr}(\alpha_i \beta_j) = \delta_{ij}, \quad \forall i, j. \quad (4)$$

It can be shown that the dual basis is unique. Moreover, if $\{\alpha_0, \alpha_1\}$ is normal then $\{\beta_0, \beta_1\}$ will be normal as well [17], [18]. It was shown above that the normal bases of $\boldsymbol{C_R}$ are of the form

$$\{\alpha, \alpha^*\} = \{a+ib, a-ib\}, \qquad a, b \in \boldsymbol{R}, ab \neq 0.$$

Applying the trace-orthogonality relation above (4)

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

we fing that the dual normal bases of $\boldsymbol{C_R}$ are of the form

$$\{\beta, \beta^*\} = \left\{ \frac{1}{4a} - i\frac{1}{4b}, \frac{1}{4a} + i\frac{1}{4b} \right\}, \qquad a, b \in \boldsymbol{R}, ab \neq 0. \quad (5)$$

Summarizing the facts relevant for later discussion, we have:

1) The trace function is a conjugate-invariant linear functional on $\boldsymbol{C_R}$, i.e.
   a) $\mathrm{Tr}(\zeta) \in \boldsymbol{R} \quad \forall \zeta \in \boldsymbol{C}$

b) $\mathrm{Tr}\ (c_1\zeta_1 + c_2\zeta_2) = c_1\,\mathrm{Tr}\,(\zeta_1) + c_2\,\mathrm{Tr}\,(\zeta_2)$ $\forall c_i \in \boldsymbol{R}, \forall \zeta_i \in \boldsymbol{C}$

c) $\mathrm{Tr}\ (\zeta) = \mathrm{Tr}\ (\zeta^*) \quad \forall \zeta \in \boldsymbol{C}.$

2) The normal bases of $\boldsymbol{C_R}$ are of the form

$$\{\alpha, \alpha^*\} = \{a + ib, a - ib\}, \qquad a, b \in \boldsymbol{R}, ab \neq 0.$$

3) The respective dual bases of the normal bases above are

$$\{\beta, \beta^*\} = \left\{\frac{1}{4a} - i\frac{1}{4b}, \frac{1}{4a} + i\frac{1}{4b}\right\}, \quad a, b \in \boldsymbol{R}, ab \neq 0.$$

We will conclude this section with a quick discussion of the general case. If $\boldsymbol{F}$ is a field and $\boldsymbol{K}$ is an extension of $\boldsymbol{F}$ of degree $m = [\boldsymbol{K} : \boldsymbol{F}] < \infty$, then $\boldsymbol{K}$ is a vector space of dimension m over $\boldsymbol{F}$ [21], [22]. As with the real/complex case, there exist m vectors $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ in $\boldsymbol{K}$ such that $\{\alpha_i\}$ is a basis for $\boldsymbol{K}$ over $\boldsymbol{F}$ (notation: $\boldsymbol{K_F}$). A basis $\{\alpha_i\}$ for $\boldsymbol{K_F}$ is called a *normal basis* if the α_i's are *conjugates* of each other with respect to the basefield $\boldsymbol{F}$. In contrast to the real/complex case, where normal bases are abundant, only under certain conditions on the field extension $\boldsymbol{K}$ do normal bases exist. If a normal basis $\{\alpha_i\}$ can be found, then its dual normal basis $\{\beta_i\}$ will also exist. The dual normal basis $\{\beta_i\}$ is defined as the basis $\{\beta_i\}$ such that

$$\mathrm{Tr}\,(\alpha_i\beta_j) = \delta_{ij}, \quad \forall i, j.$$

where Tr $(\cdot)$ is the linear function on $\boldsymbol{K_F}$ defined as

$$\mathrm{Tr}\,(\zeta) = \sum \text{ conjugates of } \zeta, \qquad \forall \zeta \in \boldsymbol{K}$$

III. Basefield Transforms and Conjugates

Before we proceed to derive the Hartley transform from the Fourier transform, let us cast the Fourier transform in the setting of fields and field extensions.

Let $\boldsymbol{F}$ be a field. Let $\{x_n\}_{n=0}^{N-1}$ be a sequence in $\boldsymbol{F}$. Then the Fourier transform of $\{x_n\}_{n=0}^{N-1}$ defined as

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

exists iff W_N, and element of order N (i.e. N is the lowest power of W_N such that $W_N^N = 1$), exists in $\boldsymbol{F}$. If $\boldsymbol{F}$ contains W_N, then the Fourier transform can be computed in $\boldsymbol{F}$ and the Fourier coefficients $\{X_n\}_{n=0}^{N-1}$ will reside in $\boldsymbol{F}$. If $\boldsymbol{F}$ does not contain an element of order N, then it is necessary to go an extension field $\boldsymbol{K}$ of $\boldsymbol{F}$ which contains such an element in order to compute the Fourier transform. Whether such an extension field exists depends on the value N and the *characteristic* of the field $\boldsymbol{F}$. If such an extension field can be found, then the Fourier coefficients $\{X_n\}_{n=0}^{N-1}$ will reside in the extension field but are constrained to satisfy a certain *conjugacy relation.*

To be specific for the field of immediate interest to us, if $\boldsymbol{F}$ is the field of real numbers, then $\boldsymbol{F}$ contains only elements of order 1 and 2 (1 and -1). Thus in order to compute a Fourier transform of size $N > 2$, it is necessary to go to an extension of $\boldsymbol{R}$ which contains an element of order N. The extension of $\boldsymbol{R}$ which contains such an element is the complex field $\boldsymbol{C}$. Over the field of complex numbers, the elements of order N are

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

where (m, N) denotes the greatest common divisor of m and N. Thus for $N > 2$, the Fourier transform of a real sequence is complex. However, because W_n^k and W_N^{-k} are conjugates of each other, the Fourier coefficients are constrained to satisfy the conjugacy relation [28]

$$X_k^* = X_{-k}, \quad \forall k. \tag{6}$$

It is worth noting that for the reals it is sufficient to go up to the complex field to find elements of every order. For more general fields, however, there may not be an extension that contains the element of the desired order. And even if the desired extension can be found, the extension will be different for different values of N. The motivation for constructing the Hartley and other basefield transforms is that since the input sequence is in the basefield $\boldsymbol{F}$, it would be desirable (as well as esthetically pleasing) to have a transform in which the transform coefficients would be in the same field. That there is such a transform is suggested by the conjugacy relation that the Fourier coefficients of the basefield sequence must satisfy. The conjugacy constraint implies a lack of freedom in the choice of the Fourier coefficients and hence a degree of redundancy which may be exploited.

Consider for a while the input as being members of the extension field. If we expand each input element with respect to a basis which contains 1 as a member, then each input element has $m - 1$ components equal to zero. Once transformed, each transform coefficient has in general no zero components. But due to the conjugacy constraint, one output characterizes a whole conjugacy class (i.e., m outputs in the most simple case). Thus in terms of independent components, there are just as many degrees of freedom in the transform domain as there were in the original basefield domain: the redundancy still exists and has only been changed. As a result, the transforms that we seek can be obtained by grouping the m outputs belonging to a conjugacy class, and combining them to obtain m basefield elements. Let M be the corresponding mapping. A basefield transform related to the Fourier transform can be obtained by applying to the output of a Fourier transform an operator $\mathcal{P}$ which is a direct sum of the operators M on the individual conjugacy classes of $\{X_n\}$. By appropriately permuting and/or repeating the elements of $\{X_n\}$, the operator $\mathcal{P}$ can be written as

$$P = \begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix}. \tag{7}$$

Schematically, the procedure is as shown in Fig. 1.

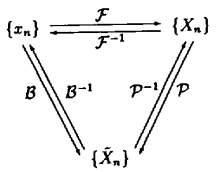


Fig. 1. Relations between$\{x_n\}$, DFT$\{x_n\}$, and DBT$\{x_n\}$.

In the figure, the input sequence is denoted by $\{x_n\}$, the Fourier transform of the sequence by $\{X_n\}$, and the (yet undefined) basefield transform by $\{\tilde{X}_n\}$. Note that $\{x_n\}$ and $\{\tilde{X}_n\}$ reside in the basefield $\boldsymbol{F}$ while $\{X_n\}$ is in the extension field $\boldsymbol{K}$ of $\boldsymbol{F}$. The function $\mathcal{F}$ between $\{x_n\}$ and $\{X_n\}$ is the usual DFT mapping. The function $\mathcal{B}$ is the basefield transform that we seek. Shown also is an intermediate map, $\mathcal{P}$, between $\{X_n\}$ and $\{\tilde{X}_n\}$. Since $\mathcal{F}$ and $\mathcal{B}$ (if it exists) are *bijections*, clearly the basefield transform exists iff the intermediate map $\mathcal{P}$ exists. It suffices therefore to construct the map $\mathcal{P}$ from $\{X_n\}$ to $\{\tilde{X}_n\}$, then the composition of $\mathcal{F}$ and $\mathcal{P}$ will yield a basefield transform.

This transform will have an inverse basefield transform if the map $\mathcal{P}$ is itself invertible. Since

$$\mathcal{P} = \begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix} \Longrightarrow$$

$$\mathcal{P}^{-1} = \begin{pmatrix} M^{-1} & & & \\ & M^{-1} & & \\ & & \ddots & \\ & & & M^{-1} \end{pmatrix}$$

it suffices that the mapping M be invertible.

How should we choose the mapping M? By construction, M must map the extension field to the basefield. Moreover, in order that $\mathcal{B} = \mathcal{P} \circ \mathcal{F}$ be linear, we will require that $\mathcal{P}$ be linear. Thus M should be a matrix with elements in $\boldsymbol{K}$.

Indeed, algorithms searching to eliminate the redundancy in the computation of the DFT of real-valued sequences already implicitly used this approach. If one chooses to compute separately the real part and the imaginary part of a set of conjugate pairs X_k and X_{-k} (done in early papers such as [15]), this amounts to considering the above scheme with M defined as

$$\begin{pmatrix} \tilde{X}_k \\ \tilde{X}_{-k} \end{pmatrix} = M \begin{pmatrix} X_k \\ X_{-k} \end{pmatrix} = \begin{pmatrix} 0.5 & 0.5 \\ i0.5 & -i0.5 \end{pmatrix} \begin{pmatrix} X_k \\ X_{-k} \end{pmatrix}.$$

Other choices of M are possible. See, for example, [12]–[14].

However, it is clear that not all choices of the matrix M will lead to structured transforms; some choices will invariably look contrived. Good choices of M will certainly be more mathematically structured. To that end, it is natural to search for an M which represents a separable mapping on the conjugacy classes. Ideally, M should induce the same linear functional on all X_k, viz. $\tilde{X}_k = \varphi(X_k)\ \forall X_k$.

Fact 1: *φ is a linear functional on $\boldsymbol{C}_{\boldsymbol{R}}$ iff there exists an $\alpha \in \boldsymbol{C}$ such that*

$$\varphi(\zeta) = \mathrm{Tr}(\alpha\zeta), \qquad \forall \zeta \in \boldsymbol{C}.$$

Proof: ($\Longleftarrow$) By the linearity of the Trace function discussed in Section II $\mathrm{Tr}(\alpha\cdot)$ is a linear functional on $\boldsymbol{C}_{\boldsymbol{R}}$ for any α.

($\Longrightarrow$) If φ is a linear functional on $\boldsymbol{C}_{\boldsymbol{R}}$, then φ is completely determined by its action on a basis of $\boldsymbol{C}_{\boldsymbol{R}}$. Let the action of φ on the canonical basis $\{1, i\}$ of $\boldsymbol{C}_{\boldsymbol{R}}$ be $\varphi(1) = c$ and $\varphi(i) = d$, where c and d are arbitrary elements of $\boldsymbol{R}$. We will show that there is an element $\alpha = a + ib \in \boldsymbol{C}$ such that $\varphi(1) = \mathrm{Tr}(\alpha 1) = c$ and $\varphi(i) = \mathrm{Tr}(\alpha i) = d$.

$$\mathrm{Tr}(\alpha 1) = \alpha + \alpha^* = 2a = c \quad \Longrightarrow \quad a = \frac{c}{2}$$

$$\mathrm{Tr}(\alpha i) = \alpha i - \alpha^* i = -2b = d \quad \Longrightarrow \quad b = -\frac{d}{2}.$$

Thus

$$\alpha = \frac{c}{2} - i\frac{d}{2}$$

is the desired element. □

We have thus determined that the function φ must be of the form

$$\varphi(\zeta) = \mathrm{Tr}(\alpha\zeta), \quad \forall \zeta \in \boldsymbol{C}$$

for some $\alpha \in \boldsymbol{C}$. Applying it to the Fourier coefficients $\{X_n\}$, we have

$$\varphi(X_k) = \mathrm{Tr}(\alpha X_k) = \alpha X_k + \alpha^* X_k^*, \quad 0 \le k \le N-1.$$

The corresponding form of the matrix M is easily found. Consider the action of φ on a conjugacy class $\{X_k, X_{-k}\}$ of $\{X_n\}$

$$\varphi(X_k) = \mathrm{Tr}(\alpha X_k) = \alpha X_k + \alpha^* X_k^*$$
$$\varphi(X_{-k}) = \mathrm{Tr}(\alpha X_{-k}) = \alpha X_{-k} + \alpha^* X_{-k}^*.$$

Since $\{X_n\}$ is the Fourier transform of a real sequence, it satisfies the conjugacy (6), thus the above equations can alternately be written as

$$\varphi(X_k) = \mathrm{Tr}(\alpha X_k) = \alpha X_k + \alpha^* X_{-k}$$
$$\varphi(X_{-k}) = \mathrm{Tr}(\alpha X_{-k}) = \alpha^* X_k + \alpha X_{-k}$$

or, in matrix form

$$\begin{pmatrix} \alpha & \alpha^* \\ \alpha^* & \alpha \end{pmatrix} \begin{pmatrix} X_k \\ X_{-k} \end{pmatrix} = \begin{pmatrix} \varphi(X_k) \\ \varphi(X_{-k}) \end{pmatrix}.$$

We still have not specified the element α. α should be chosen so that $\mathcal{P}$ can be inverted. For the complex field, this places a rather mild constraint on α. Since (7) implies that $\mathcal{P}$ is invertible iff M is invertible, the restriction on the choice of α is simply that it must render the matrix M nonsingular. The following simple fact gives the precise condition on the element α.

Fact 2: The matrix

$$M = \begin{pmatrix} \alpha & \alpha^* \\ \alpha^* & \alpha \end{pmatrix} = \begin{pmatrix} a+ib & a-ib \\ a-ib & a+ib \end{pmatrix}$$

is invertible iff $ab \neq 0$, *i.e., iff* $\langle\alpha\rangle \stackrel{\text{def}}{=} \{\alpha, \alpha*\}$ *is a normal basis of* $\boldsymbol{C}_{\boldsymbol{R}}$.

The first part of the fact is easily verified by considering the determinant of M. The second part of the fact follows from the discussion of normal basis in Section II. The second part may seem an unnecessary formalism; it is included mainly to suggest the result for fields other than $\boldsymbol{C}$ and $\boldsymbol{R}$.

By taking α to be a *generator* of a normal basis of $\boldsymbol{C}_{\boldsymbol{R}}$, then, the map

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

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

To summarize, we have shown that this requirement for a more structured mapping allowing a one-to-one correspondence between each member of the conjugacy class and a basefield element involved the trace function discussed in Section II. Furthermore, the requirement for this mapping to be invertible was that the element α involved in the trace function generates a normal basis for the complex over the reals.

As a result of the imposed mathematical structure, the mapping $\mathcal{P}$, originally defined in a blockwise manner, also corresponds to a "pointwise" one. Using $\mathcal{P}$, the basefield transform $\mathcal{B}$ can be obtained as follows:

Consider the DFT of $\{x_n\}$

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

where $x_n \in \boldsymbol{R}$ and W_N has been choosen in its general form $W_N = e^{-i(2\pi/N)m}$, $1 \leq m < N$, $(m, N) = 1$, rather than restricting to the usual case $m = 1$. Since $\mathcal{B} = \varphi \circ \mathcal{F}$, composing the two functions using $\alpha = a + ib$ yields the following real transform:

$$\begin{aligned} \tilde{X}_k &= \mathrm{Tr}(\alpha X_k) \\ &= \sum_{n=0}^{N-1} x_n \mathrm{Tr}(\alpha W_N^{nk}) \qquad (8) \\ &= \sum_{n=0}^{N-1} x_n \left[2a \cos \frac{2\pi}{N} nmk + 2b \sin \frac{2\pi}{N} nmk \right]. \qquad (9) \end{aligned}$$

We note that, for the classical choice of the element of order N, i.e., $m = 1$, this reduces to Ansari's discrete combinational Fourier transform

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

We now consider the structure of the inverse transform. From the discussion above, the inverse mapping $\mathcal{P}^{-1}$, combined with the inverse Fourier transform, completely defines the inverse basefield transform. The question now is about the structure of the inverse of the matrix M, and to which one-to-one mapping between the basefield elements and the conjugacy class it corresponds.

Fact 3: If

$$M = \begin{pmatrix} \alpha & \alpha^* \\ \alpha^* & \alpha \end{pmatrix}$$

where $\alpha = a + ib$ *is a generator of a normal basis* $\langle\alpha\rangle$ *of* $\boldsymbol{C}_{\boldsymbol{R}}$, *then*

$$M^{-1} = \begin{pmatrix} \beta & \beta^* \\ \beta^* & \beta \end{pmatrix}$$

where

$$\beta = \frac{1}{4a} - i\frac{1}{4b}$$

is the generator of the normal basis $\langle\beta\rangle$ *dual to* $\langle\alpha\rangle$.

Proof:

$$\begin{aligned} \begin{pmatrix} \alpha & \alpha^* \\ \alpha^* & \alpha \end{pmatrix} \begin{pmatrix} \beta & \beta^* \\ \beta^* & \beta \end{pmatrix} &= \begin{pmatrix} \mathrm{Tr}(\alpha\beta) & \mathrm{Tr}(\alpha\beta^*) \\ \mathrm{Tr}(\alpha\beta^*) & \mathrm{Tr}(\alpha\beta) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

where the last equality follows from the trace-orthogonality of the two bases. □

It follows that

$$\begin{pmatrix} X_k \\ X_{-k} \end{pmatrix} = \begin{pmatrix} \beta & \beta* \\ \beta* & \beta \end{pmatrix} \begin{pmatrix} \tilde{X}_k \\ \tilde{X}_{-k} \end{pmatrix},$$

consequently,

$$\varphi^{-1} : \tilde{X}_k \longmapsto X_k = \beta\tilde{X}_k + \beta^*\tilde{X}_{-k}.$$

Since $\mathcal{B} = \varphi \circ \mathcal{F}$, $\mathcal{B}^{-1} = \mathcal{F}^{-1} \circ \varphi^{-1}$. Composing φ^{-1} and $\mathcal{F}^{-1}$ yields

$$\begin{aligned} x_k &= \frac{1}{N} \sum_{n=0}^{N-1} (\beta\tilde{X}_n + \beta^*\tilde{X}_{-n}) W_N^{-nk} \\ &= \frac{1}{N} \left(\sum_{n=0}^{N-1} \beta\tilde{X}_{-n} W_N^{-nk} + \sum_{n=0}^{N-1} \beta^*\tilde{X}_n W_N^{-nk} \right) \\ &= \frac{1}{N} \sum_{n=}^{N-1} \tilde{X}_n (\beta W_N^{-nk} + \beta^* W_N^{nk}) \\ &= \frac{1}{N} \sum_{n=0}^{N-1} \tilde{X}_n Tr(\beta W_N^{-nk}) \qquad (10) \\ &= \frac{1}{N} \sum_{n=0}^{N-1} X_n \left[\frac{1}{2a} \cos \frac{2\pi}{N} nmk + \frac{1}{2b} \sin \frac{2\pi}{N} nmk \right]. \end{aligned}$$

Thus the inverse to the basefield transform (9) is

$$x_k = \frac{1}{N} \sum_{n=0}^{N-1} \tilde{X}_n \left[\frac{1}{2a} \cos \frac{2\pi}{N} nmk + \frac{1}{2b} \sin \frac{2\pi}{N} nmk \right]. \qquad (11)$$

As before, for $m = 1$, this reduces to the inverse discrete combinational Fourier transform

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

IV. The Self-Inverse Property

In this section, we will show that the Hartley transform is the basefield transform of the previous sections with the added proviso that the transform be involutionary.

We begin by restating the basefield transform equations. Over a general field $\boldsymbol{F}$, the basefield transform pair, is given by

$$\tilde{X}_k = \sum_{n=0}^{N-1} x_n \operatorname{Tr}(\alpha W_N^{nk}) \tag{12}$$

$$x_k = \frac{1}{N} \sum_{n=0}^{N-1} \tilde{X}_n \operatorname{Tr}(\beta W_N^{-nk}) \tag{13}$$

((8) and (10)), where W_N is an element of order N in a suitable extension $\boldsymbol{K}$ of $\boldsymbol{F}$ and α and β are generators of a set of mutually dual normal bases of $\boldsymbol{K}_{\boldsymbol{F}}$. Clearly, if a set of mutually dual bases can be found such that

$$\operatorname{Tr}(\alpha W_N^l) = \operatorname{Tr}(\beta W_N^{-l}), \quad \forall l \tag{14}$$

then the transform above would have the self-inverse property.

While (14) is difficult to apply for general fields $\boldsymbol{F}$ and $\boldsymbol{K}$ (though a brute force search is possible for some fields), for the real and complex fields, it is surprisingly easy to use. It yields, among other things, the conventional Hartley transform.

Recall that the real transform pair

$$\tilde{X}_k = \sum_{n=0}^{N-1} x_n \left[2a \cos \frac{2\pi}{N} nmk + 2b \sin \frac{2\pi}{N} nmk \right] \tag{15}$$

$$x_k = \frac{1}{N} \sum_{n=0}^{N-1} \tilde{X}_n \left[\frac{1}{2a} \cos \frac{2\pi}{N} nmk + \frac{1}{2b} \sin \frac{2\pi}{N} nmk \right] \tag{16}$$

((9) and (11)) is obtained by specializing (12) and (13) to the real and complex fields using the bases

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

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

with $a, b \in \boldsymbol{R}$, $ab \neq 0$. Condition (14) stipulates that, in order for the transform to have the self-inverse property, we must have

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

for all l. It is easy to verify that this is satisfied iff

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

Substituting these values of a and b into (15) and (16) yields the following self-inverse real transforms:

$$\tilde{X}_k = \sum_{n=0}^{N-1} x_n \left[(\pm)\cos \frac{2\pi}{N} nmk + (\pm)\sin \frac{2\pi}{N} nmk \right] \tag{17}$$

$$x_k = \frac{1}{N} \sum_{n=0}^{N-1} \tilde{X}_n \left[(\pm)\cos \frac{2\pi}{N} nmk + (\pm)\sin \frac{2\pi}{N} nmk \right]. \tag{18}$$

There are thus $4\phi(N)$ self-inverse transforms permissible under this type of construction (where ϕ is the *Euler Totient function*). Of these, the case $m = 1$, $a = b = 1/2$ corresponds to the conventional Hartley transform, representing the bases

$$\{\alpha, \alpha^*\} = \left\{ \frac{1}{2} + i\frac{1}{2}, \frac{1}{2} - i\frac{1}{2} \right\}$$

$$\{\beta, \beta^*\} = \left\{ \frac{1}{2} - i\frac{1}{2}, \frac{1}{2} + i\frac{1}{2} \right\}.$$

V. The Convolution Property

It would be difficult to derive the convolution property of the basefield transform directly from the transform equations (12) and (13). However, the convolution property can be deducted easily with the aid of the intermediate map φ. Since convolution has a simple expression in the Fourier domain, we can obtain the convolution property in the basefield domain as follows: map the convolving sequences to the Fourier domain (via φ^{-1}), perform the convolution in the Fourier domain (pointwise multiplication), then map the result back to the basefield (via φ).

To be specific, let us specialize to the reals. Let $\{x_n\}$ and $\{h_n\}$ be real sequences, of basefield transforms $\tilde{X}_{-k}$ and $\tilde{H}_{-k}$, respectively. Let $\{y_n\}$ be the convolution of $\{x_n\}$ and $\{h_n\}$. Then

$$X_k = \varphi_k^{-1}(\tilde{X}_k) = \beta \tilde{X}_k + \beta^* \tilde{X}_{-k}$$

$$H_k = \varphi_k^{-1}(\tilde{H}_k) = \beta \tilde{H}_k + \beta^* \tilde{H}_{-k}.$$

Therefore,

$$Y_k = H_k X_k = \beta\beta \tilde{H}_k \tilde{X}_k + \beta\beta^* \tilde{H}_k \tilde{X}_{-k} + \beta\beta^* \tilde{H}_{-k} \tilde{X}_k + \beta^*\beta^* \tilde{H}_{-k} \tilde{X}_{-k}.$$

To express $\tilde{Y}_k$ in terms of $\tilde{H}_k$ and $\tilde{X}_k$, we "project" Y_k to the reals by taking its trace with α. This yields the following convolution formula:

$$\begin{aligned} \tilde{Y}_k &= \varphi_k(Y_k) = \operatorname{Tr}(\alpha Y_k) \\ &= \operatorname{Tr}(\alpha\beta\beta) \tilde{H}_k \tilde{X}_k + \operatorname{Tr}(\alpha\beta\beta^*) \tilde{H}_k \tilde{X}_{-k} \\ &\quad + \operatorname{Tr}(\alpha\beta\beta^*) \tilde{H}_{-k} \tilde{X}_k + \operatorname{Tr}(\alpha\beta^*\beta^*) \tilde{H}_{-k} \tilde{X}_{-k} \\ &= \frac{1}{8}\left(\frac{3}{a} - \frac{a}{b^2} \right) \tilde{H}_k \tilde{X}_k + \frac{1}{8}\left(\frac{1}{a} + \frac{a}{b^2} \right) \\ &\quad \cdot (\tilde{H}_k \tilde{X}_{-k} + \tilde{H}_{-k} \tilde{X}_k - \tilde{H}_{-k} \tilde{X}_{-k}) \end{aligned}$$

where the coefficients are derived using the mutually dual normal bases for $\boldsymbol{C}_{\boldsymbol{R}}$ presented previously,

$$\langle\alpha\rangle = \{a + ib, a - ib\}$$

$$\langle\beta\rangle = \left\{ \frac{1}{4a} - i\frac{1}{4b}, \frac{1}{4a} + i\frac{1}{4b} \right\}, \quad a, b \in \boldsymbol{R},\ ab \neq 0.$$

To carry the specialization one step further, recall that the conventional Hartley transform corresponds to choosing the normal bases

$$\langle\alpha\rangle = \left\{ \frac{1}{2} + i\frac{1}{2}, \frac{1}{2} - i\frac{1}{2} \right\}$$

and

$$\langle\beta\rangle = \left\{\frac{1}{2} - i\frac{1}{2}, \frac{1}{2} + i\frac{1}{2}\right\}.$$

Setting $a = b = 1/2$ in the convolution equation above yields

$$\begin{aligned}\tilde{X}_k &= \frac{1}{2}\tilde{H}_k\tilde{X}_k + \frac{1}{2}(\tilde{H}_k\tilde{X}_{-k} + \tilde{H}_{-k}\tilde{X}_k - \tilde{H}_{-k}\tilde{X}_{-k}) \\ &= \tilde{H}_k\left(\frac{\tilde{X}_k + \tilde{X}_{-k}}{2}\right) + \tilde{H}_{-k}\left(\frac{\tilde{X}_k - \tilde{X}_{-k}}{2}\right) \\ &= \tilde{H}_k\tilde{X}_k^{(e)} + \tilde{H}_{-k}\tilde{X}_k^{(o)}.\end{aligned}$$

The equation is the original convolution equation given by Bracewell [1], [26].

VI. The Basefield Transform as a Projection

We have used the term "projection" several times in the preceding sections but somewhat loosely. In this section, we will try to give a precise meaning to the term. As before, the discussion will be confined to the real case, though the idea is applicable to other fields as well.

Consider the Fourier coefficients $\{X_n\}$. Since these coefficients reside in the complex field, they have unique representations with respect to any basis of $\boldsymbol{C}_{\boldsymbol{R}}$. Let $\{\gamma_0, \gamma_1\}$ be an arbitrary basis of $\boldsymbol{C}_{\boldsymbol{R}}$. Then for all k

$$X_k = \hat{X}_k^{(0)}\gamma_0 + \hat{X}_k^{(1)}\gamma_1 \tag{19}$$

for some $\hat{X}_k^{(01)}, \hat{X}_k^{(1)} \in \boldsymbol{R}$. If α is a generator of a normal basis $\{\alpha, \alpha^*\}$ of $\boldsymbol{C}_{\boldsymbol{R}}$, then by the linearity of the trace function

$$\begin{aligned}\tilde{X}_k &= \varphi(X_k) = \operatorname{Tr}(\alpha X_k) \\ &= \hat{X}_k^{(0)}\operatorname{Tr}(\alpha\gamma_0) + \hat{X}_k^{(1)}\operatorname{Tr}(\alpha\gamma_1).\end{aligned} \tag{20}$$

Consider what happens when $\{\gamma_0, \gamma_1\}$ is chosen to be the (unique) dual basis $\{\beta, \beta^*\}$ of $\{\alpha, \alpha^*\}$. Equation (20) becomes

$$\tilde{X}_k = \hat{X}_k^{(0)}\operatorname{Tr}(\alpha\beta) + \hat{X}_k^{(1)}\operatorname{Tr}(\alpha\beta^*) = \hat{X}_k^{(0)} \tag{21}$$

where the last equality follows from the trace-orthogonality relation of the two bases (4).

Consider now the quantity $\hat{X}_{-k} = \operatorname{Tr}(\alpha X_{-k})$. We have

$$\begin{aligned}\tilde{X}_{-k} &= \operatorname{Tr}(\alpha X_{-k}) \\ &= \operatorname{Tr}(\alpha^* X_{-k}^*) && (22) \\ &= \operatorname{Tr}(\alpha^* X_k) && (23) \\ &= \hat{X}_k^{(0)}\operatorname{Tr}(\alpha^*\beta) + \hat{X}_k^{(1)}\operatorname{Tr}(\alpha^*\beta^*) \\ &= \hat{X}_k^{(1)} && (24)\end{aligned}$$

where (22) follows from the conjugate-invariant property of the trace function (3), and (23) from the conjugacy relation of the Fourier coefficients (6), and (24) from the trace-orthogonality relation of the two bases (4).

Combining (19), (21), and (24) we see that, with respect to the dual basis $\{\beta, \beta^*\}$ of $\{\alpha, \alpha^*\}$, the basis components of the Fourier coefficients of a real sequence $\{x_n\}$ *are* the basefield coefficients of $\{x_n\}$

$$X_k = \tilde{X}_k\beta + \tilde{X}_{-k}\beta^*, \quad \forall k. \tag{25}$$

The function φ thus *picks out* the β-component of the expansion; it is for this reason that we call φ a "projection." The terminology is used to draw an analogy between the action of φ and that of the familiar projection operators in Hilbert spaces. It should be noted, however, this analogy is not exact. The function φ is not a projection operator in the usual sense of the term. It is easy to verify, for instance, that $\varphi^2 \neq \varphi$.

We will conclude this section with a discussion of why normal bases are the natural settings for expressing conjugacy relations. Consider the conjugacy class $\{X_k, X_{-k}\}$. From the discussion above we have that the expansion of X_k and X_{-k} with respect to a normal basis is

$$\begin{aligned}X_k &= \tilde{X}_k\beta + \tilde{X}_{-k}\beta^* \\ X_{-k} &= \tilde{X}_{-k}\beta + \tilde{X}_k\beta^*.\end{aligned}$$

Note that the basis components of the conjugates are permutations of each other. In extracting the β-component of the conjugates, we thus have all the information required to reconstruct them. The above is an example of a more general fact that applies to all fields: with respect to a normal basis, the basis components of the elements of a conjugacy class are permutations of one another. For this reason, normal bases are particularly useful for expressing conjugacy relations.

VII. Fast Algorithms

In this section, we will consider fast algorithms for the discrete basefield transform. We will show that for any fast algorithm for the discrete Fourier transform, there is an equivalent fast algorithm for the discrete basefield transform. Moreover, the fast algorithm for the basefield transform may be obtained by *projecting* the equivalent Fourier algorithm from the extension field to the basefield. The technique may be briefly stated as follows: if $\mathcal{A}$ is a fast algorithm for the Fourier transform, then by an abuse of notation,

$$\varphi(\mathcal{A}) = \operatorname{Tr}(\alpha\mathcal{A}) \tag{26}$$

will be a fast algorithm for the basefield transform. The strengths of this technique lie in that it takes advantage of the well-developed area of fast Fourier transform algorithms and that it is applicable to all fields of interest.

We will demonstrate the above technique by deriving a few familiar fast algorithms for the conventional real Hartley transform. It will be seen that the technique is easy to apply and that it circumvents the use of trignometric identities endemic in the development of fast Hartley transform algorithms. Other standard algorithms such as Rader's and Winograd's algorithms may be derived the same way.

The subsequent discussions require new notations (the coefficients of the expansion of the various variables with respect to different bases), which we introduce now by

recapping the classical real Hartley results in terms of the previous discussion.

The real Hartley transform is obtained from the basefield transform by setting $m = 1$, $a = b = 1/2$. As pointed out earlier, this is equivalent to choosing the order-N element $W_N = e^{-i(2\pi/N)}$ and the set of bases

$$\{\alpha_0, \alpha_1\} = \{\alpha, \alpha^*\} = \left\{\frac{1}{2} + i\frac{1}{2}, \frac{1}{2} - i\frac{1}{2}\right\}$$

$$\{\beta_0, \beta_1\} = \{\beta, \beta^*\} = \left\{\frac{1}{2} - i\frac{1}{2}, \frac{1}{2} + i\frac{1}{2}\right\}$$

Thus if W_N^{nk} is expanded with respect to the basis $\{\beta_0, \beta_1\} = \{\beta, \beta^*\}$, then

$$\begin{aligned} W_N^{nk} &= w_{nk}^{(0)}\beta_0 + w_{nk}^{(1)}\beta_1 \\ &= w_{-nk}^{(1)}\beta_0 + w_{-nk}^{(0)}\beta_1 \\ &= \left(\cos\frac{2\pi}{N}nk + \sin\frac{2\pi}{N}nk\right)\left(\frac{1}{2} - i\frac{1}{2}\right) \\ &\quad + \left(\cos\frac{2\pi}{N}nk - \sin\frac{2\pi}{N}nk\right)\left(\frac{1}{2} + i\frac{1}{2}\right) \end{aligned}$$

$$\operatorname{Tr}(\alpha W_N^{(nk)}) = w_{nk}^{(0)} = w_{-nk}^{1} \tag{27}$$

$$= \cos\frac{2\pi}{N}nk + \sin\frac{2\pi}{N}nk. \tag{28}$$

Consequently

$$\hat{X}_k = \sum_{n=0}^{N-1} x_n \operatorname{Tr}(\alpha W_N^{nk}) \tag{29}$$

$$= \sum_{n=0}^{N-1} x_n w_{nk}^{(0)} \tag{30}$$

$$= \sum_{n=0}^{N-1} x_n \left[\cos\frac{2\pi}{N}nk + \sin\frac{2\pi}{N}nk\right]. \tag{31}$$

In addition to the set of bases above, we will need another basis with which to expand the twiddle factors. While the transform kernel must be expanded with respect to a normal basis, the twiddle factors can be expanded with respect to any basis. The particular choice $\{\gamma_0, \gamma_1\} = \{1, -i\}$ yields the familiar fast Hartley transform algorithms. Using this basis, the twiddle factor W_N^k has the expansion

$$W_N^k = w_k^{(0)}\gamma_0 + w_k^{(0)}\gamma_1 = \cos\frac{2\pi}{N}k - i\sin\frac{2\pi}{N}k. \tag{32}$$

The following equations relating the three bases are easily verified. They are stated here for future reference

$$\operatorname{Tr}(\alpha\gamma_0\beta_0) = \operatorname{Tr}(\alpha\gamma_1\beta_1) = 1 \tag{33}$$

$$\operatorname{Tr}(\alpha\gamma_1\beta_0) = \operatorname{Tr}(\alpha\gamma_0\beta_1) = 0 \tag{34}$$

$$\operatorname{Tr}(\alpha\beta_0\beta_0) = \operatorname{Tr}(\alpha\beta_0\beta_1) = \frac{1}{2} \tag{35}$$

$$\operatorname{Tr}(\alpha\beta_1\beta_1) = -1/2 \tag{36}$$

$$\operatorname{Tr}(\alpha\beta_j) = \delta_j. \tag{37}$$

The general procedure which will be used for obtaining a fast Hartley transform algorithm from its Fourier counterpart is as follows: Starting from the basic equation of the FFT algorithm, expand each kernel involved in terms of the dual basis $\{\beta_0, \beta_1\}$, and the twiddle factors (if any) in terms of the familiar basis $\{\gamma_0, \gamma_1\}$. Finally, "project" the algorithm into the reals by the trace function based on α to obtain the Hartley coefficients.

A. Radix-2 (DIT) Algorithm

The Radix-2 Decimation-In-Time (DIT) Fourier transform algorithm is given by[1]

$$X_k = \sum_{n=0}^{N/2-1} x_{2n} W_{N/2}^{nk} + W_N^k \sum_{n=0}^{N/2-1} x_{2n+1} W_{N/2}^{nk}.$$

Expanding $W_{N/2}^{nk}$ with respect to the basis $\{\beta_0, \beta_1\}$ (since it is used as a kernel in the DFT of length $N/2$) and W_N^k (the twiddle factor) with respect to the basis $\{\gamma_0, \gamma_1\}$, we have

$$\begin{aligned} X_k &= \sum_{n=0}^{N/2-1} x_{2n} \sum_{j=0}^{1} w_{nk}^{(j)}\beta_j + \sum_{l=0}^{1} w_k^{(l)}\gamma_l \sum_{n=0}^{N/2-1} x_{2n+1} \sum_{j=0}^{1} w_{nk}^{(j)}\beta_j \\ &= \sum_{j=0}^{1}\sum_{n=0}^{N/2-1} x_{2n} w_{nk}^{(j)}\beta_j + \sum_{l,j=0}^{1}\sum_{n=0}^{N/2-1} x_{2n+1} w_{nk}^{(j)} w_k^{(l)}\gamma_l\beta_j. \end{aligned}$$

Projecting the equation into the reals via φ yields

$$\begin{aligned} \tilde{X}_k &= \sum_{j=0}^{1}\sum_{n=0}^{N/2-1} x_{2n} w_{nk}^{(j)} \operatorname{Tr}(\alpha\beta_j) \\ &\quad + \sum_{l,j=0}^{1}\sum_{n=0}^{N/2-1} x_{2n+1} w_{nk}^{(j)} w_k^{(l)} \operatorname{Tr}(\alpha\gamma_l\beta_j). \end{aligned}$$

The values of the trace terms are given by (33), (34), and (37), thus the previous equation can be simplified to

$$\begin{aligned} \tilde{X}_k &= \sum_{n=0}^{N/2-1} x_{2n} w_{nk}^{(0)} + w_k^{(0)} \\ &\quad \cdot \sum_{n=0}^{N/2-1} x_{2n+1} w_{nk}^{(0)} + w_k^{(1)} \sum_{n=0}^{N/2-1} x_{2n+1} w_{nk}^{(1)} \\ &= \sum_{n=0}^{N/2-1} x_{2n} w_{nk}^{(0)} + w_k^{(0)} \\ &\quad \cdot \sum_{n=0}^{N/2-1} x_{2n+1} w_{nk}^{(0)} + w_k^{(1)} \sum_{n=0}^{N/2-1} x_{2n+1} w_{-nk}^{(0)} \end{aligned}$$

where the second equality follows from (27). Note that the first summation corresponds to the $N/2$-point Hartley transform of the even sequence and the second and third summations correspond to the $N/2$-point Hartley transform of the odd sequence (see (30)). Denoting the two half-sized transforms by $\tilde{X}_k^{(\text{even})}$ and $\tilde{X}_k^{(\text{odd})}$, respectively, and substituting the expresions for the twiddle factors (32), we have

$$\tilde{X}_k = \tilde{X}_k^{(\text{even})} + \tilde{X}_k^{(\text{odd})}\left(\cos\frac{2\pi}{N}k\right) + \tilde{X}_{-k}^{(\text{odd})}\left(\sin\frac{2\pi}{N}k\right) \tag{38}$$

[1] This is generally written as two equations, one for k and the other for $k + (N/2)$ [4], [9], [25]. We have chosen to write it as one equation, however, in order to retain Bracewell's original formulation.

which is the original radix-2 (DIT) algorithm proposed by Bracewell [2], [26].

B. Radix-2 (DIF) Algorithm

The Radix-2 Decimation-In-Frequency (DIF) Fourier transform is given by [4], [9], [25]

$$X_{2k} = \sum_{n=0}^{N/2-1} (x_n + x_{N/2+n}) W_{N/2}^{nk}$$

$$X_{2k+1} = \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) W_N^n W_{N/2}^{nk}.$$

Expanding the kernel $W_{N/2}^{nk}$ with respect to the basis $\{\beta_0, \beta_1\}$ and the twiddle factor W_N^n with respect to the basis $\{\gamma_0, \gamma_1\}$, we have

$$X_{2k} = \sum_{n=0}^{N/2-1} (x_n + x_{N/2+n}) \sum_{j=0}^{1} w_{nk}^{(j)} \beta_j$$

$$X_{2k+1} = \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) \sum_{l=0}^{1} w_n^{(l)} \gamma_l \sum_{j=0}^{1} w_{nk}^{(j)} \beta_j$$

$$= \sum_{l,j=0}^{1} \gamma_l \beta_j \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) w_n^{(l)} w_{nk}^{(j)}$$

$$= \sum_{l,j=0}^{1} \gamma_l \beta_j \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) w_n^{(l)} w_{(-1)^j nk}^{(0)}$$

where the last equality follow from (27). The projection of the first equation $\varphi(X_{2k})$ yields

$$\tilde{X}_{2k} = \sum_{n=0}^{N/2-1} (x_n + x_{N/2+n}) w_{nk}^{(0)} \tag{39}$$

which is the Hartley transform of the $N/2$-point sequence $\{x_n + x_{N/2+n}\}_{n=0}^{N/2-1}$. Projection of the second equation $\varphi(X_{2k+1})$ yields

$$\tilde{X}_{2k+1} = \sum_{l,j=0}^{1} \mathrm{Tr}(\alpha \gamma_l \beta_j) \cdot \sum_{n=0}^{N/2-1} (x_n - x_{N/2+n}) w_n^{(l)} w_{(-1)^j nk}^{(0)}.$$

The trace terms, as before, are given by (33), (34), and (37). Hence, the above equation reduces to

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

Note that the first summation is the kth Hartley coefficient of a modulated half-size sequence and the second summation is the $-k$th Hartley coefficient of another modulated half-size sequence. By substituting the variable n for $-n$ in the second summation, we can combine the two half-size transforms into one transform. Doing so and plugging in the values for the twiddle factors (32), we arrive at

$$\tilde{X}_{2k+1} = \sum_{n=0}^{N/2-1} \left[(x_n - x_{N/2+n}) \cos\left(\frac{2\pi}{N} n\right) + (x_{N/2-n} - x_{N-n}) \sin\left(\frac{2\pi}{N} n\right) \right] w_{nk}^{(0)}. \tag{40}$$

Equations (39) and (40) can be seen to be the radix-2 (DIF) algorithm of Sorensen *et al.* [8].

C. Prime Factor Algorithm

If $N = N_1 N_2$ with N_1 and N_2 relatively prime, then the one-dimensional Fourier transform can be written as a twiddle-factor-free two-dimensional Fourier transform [4], [25], [10]

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

Expanding $W_{N_1}^{n_1 k_1}$ and $W_{N_2}^{n_2 k_2}$ with respect to the normal basis $\{\beta_0, \beta_1\}$, we have

$$X_{k_1 k_2} = \sum_{n_1=0}^{N_1-1} \sum_{j=0}^{1} w_{n_1 k_1}^{(j)} \beta_j \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} \sum_{j=0}^{1} w_{n_2 k_2}^{(l)} \beta_l$$

$$= \sum_{j,l=0}^{1} \beta_j \beta_l \sum_{n_1=0}^{N_1-1} w_{n_1 k_1}^{(j)} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} w_{n_2 k_2}^{(l)}$$

$$= \sum_{j,l=0}^{1} \beta_j \beta_l \left\{ \sum_{n_1=0}^{N_1-1} w_{(-1)^j n_1 k_1}^{(0)} \cdot \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} w_{(-1)^l n_2 k_2}^{(0)} \right\}$$

where the last equality follows from (27). Note that the parenthesized term is a two-dimensional twiddle-factor-free Hartley transform (see (30)). If we denote this term by $\hat{X}$, then the above equation can be written more simply as

$$X_{k_1 k_2} = \sum_{j,l=0}^{1} \beta_j \beta_l \hat{X}_{(-1)^j k_1, (-1)^l k_2}.$$

Projecting this equation into the reals via φ yields

$$\tilde{X}_{k_1 k_2} = \sum_{j,l=0}^{1} \mathrm{Tr}(\alpha \beta_j \beta_l) \hat{X}_{(-1)^j k_1, (-1)^l k_2}.$$

Finally, substituting the values of the trace terms from (35) and (36), we arrive at the following prime factor Hartley algorithm:

$$\tilde{X}_{k_1 k_2} = \frac{1}{2} (\hat{X}_{k_1, k_2} + \hat{X}_{-k_1, k_2} + \hat{X}_{k_1, -k_2} - \hat{X}_{-k_1, -k_2}). \tag{41}$$

This is a new algorithm which is a variation of an existing algorithm due to Sorensen *et al.* [8].

VIII. Generalized Basefield Transform

Although we have confined the details of the discussion to the familiar real case, we have purposely kept the presentation general in order to facilitate the extension of the techinque to more general fields. We will, in this section, sketch the construction of basefield transforms over an arbitrary field. All the necessary ingredients have in fact been presented. We will merely put things in the proper context and detail some of the differences and difficulties in the general case vis à vis the real case. A more detailed treatment can be found in [16], [29].

The first problem that one has to address in constructing a basefield transform of a particular length N is that of finding the correct field extension. In the real case, there is one extension which will work for all N, namely, the *algebraically closed* complex field. This is a property peculiar to the reals that is not shared by other fields. For an arbitary field $\boldsymbol{F}$ there may not be an extension $\boldsymbol{K}$ which contains the requisite element W_N. Furthermore, for different values of N, the extension fields will be different. Whether an extension exists which contains the required element of order N depends on the *characteristic* of the field $\boldsymbol{F}$ [18]–[20].

It can be shown that if the characteristic of the field $\boldsymbol{F}$ divides N, then $\boldsymbol{F}$ does not admit an extension containing an element of order N [18]–[20]. In this case, neither the Fourier nor the basefield transform exists. If the characteristic of $\boldsymbol{F}$ does not divide N, then it will be possible to find an extension $\boldsymbol{K}$ that contains an element of order N [18]–[20]. For technical reasons we will take $\boldsymbol{K}$ to be the smallest of all such fields, namely the Nth *cyclotomic extension* of $\boldsymbol{F}$. In the cyclotomic extension $\boldsymbol{K}$, the elements of order N are simply the primitive Nth roots of unity.

Having found the proper extension of $\boldsymbol{F}$ containing an element of order N, one can obviously compute the Fourier transform of an $\boldsymbol{F}$ sequence. The formula is as in the real case

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

Because W_N resides in $\boldsymbol{K}$, $\{X_k\}$ will reside in $\boldsymbol{K}$ as well. The question then arises as to whether there is redundancy in the $\boldsymbol{K}$ sequence $\{X_k\}$ that one may exploit as the real case. The answer is yes; and as with the real case, the redundancy is manifested in the form of a conjugacy relation that the sequence $\{X_k\}$ must satisfy. To state this conjugacy constraint, we need to consider the *Galois group* associated with the fields $\boldsymbol{F}$ and $\boldsymbol{K}$. If $\boldsymbol{F}$ is a field and $\boldsymbol{K}$ is a finite extension of $\boldsymbol{F}$, then the Galois group of $\boldsymbol{K}$ and $\boldsymbol{F}$, $\mathrm{Aut}_F K = \{\sigma_i\}$, is the group of field *automorphisms* of $\boldsymbol{K}$ which leave $\boldsymbol{F}$ fixed. The effect of $\mathrm{Aut}_F K$ on the primitive Nth roots of unity is to permute them. Thus is W_N is a primitive Nth root of unity in $\boldsymbol{K}$, then

$$\sigma_i(W_N) = W_N^{j_i}$$

for some integer j_i relatively prime to N. It follows from this that

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

hence the conjugacy constraint on $\{X_k\}$ can be expressed as

$$\sigma_i(X_k) = X_{kj_i}. \tag{42}$$

Example 1: For $\boldsymbol{K} = \boldsymbol{C}$ *and* $\boldsymbol{F} = \boldsymbol{R}$, $\mathrm{Aut}_R C = \{\sigma_0, \sigma_1\}$, *where*

$$\sigma_0 : a + ib \longmapsto a + ib$$
$$\sigma_1 : a + ib \longmapsto a - ib.$$

Clearly, $j_0 = 1$ *and* $j_i = -1$, *therefore*

$$X_k = \sigma_0(X_k) = X_{kj^0} = X_k$$
$$X_k^* = \sigma_1(X_k) = X_{kj^1} = X_{-k}$$

as expected. □

Example 2: For $\boldsymbol{K} = GF(q^m)$ *and* $\boldsymbol{F} = GF(q)$, $\mathrm{Aut}_F K$ *is the cyclic group generated by the Frobenius automorphisim* $\sigma : \alpha \mapsto \alpha^q$, *i.e.*

$$\sigma_i = \sigma^i : \alpha \longmapsto \alpha^{q^i}, \qquad i = 0, 1, \cdots, m-1.$$

Thus $j_i = q^i$ *and we have*

$$X_k^{q_i} = \sigma_i(X_k) = X_{kj_i} = X_{kq^i}, \qquad i = 0, 1, \cdots, m-1$$

which is the conjugacy relation for finite field sequences. □

For elements in $\{X_k\}$, define $X_k \sim X_l$ if $\sigma_i(X_k) = X_l$ for some $\sigma_i \in \mathrm{Aut}_F K$. It is easy to verify that $\sim$ is an equivalence relation on $\{X_k\}$. Thus $\sim$ partitions $\{X_k\}$ into disjoint equivalence classes which are the conjugacy classes of $\{X_k\}$. The conjugacy class of a particular element X_k is simply its *orbit* under $\mathrm{Aut}_F K$

$$\mathrm{Orb}(X_k) = \{\sigma_i(X_k) \mid \sigma_i \in \mathrm{Aut}_F K\}.$$

Having specified the field extension $\boldsymbol{K}$ (the Nth cyclotimic extension of $\boldsymbol{F}$) and established the conjugacy relation ($\sigma_i(X_k) = X_{kj_i}$) and the conjugacy classes ($\mathrm{Orb}(X_k)$) of the Fourier transform of a basefield sequence, it remains to be shown that $\boldsymbol{K}_{\boldsymbol{F}}$ admits a normal basis and that there is a "projection operator" φ from $\boldsymbol{K}$ to $\boldsymbol{F}$ in order to carry out the construction outlined in the previous sections. We address each of these questions in turn.

A normal basis of $\boldsymbol{K}_{\boldsymbol{F}}$ is, as before, a basis consisting of an element $\alpha \in \boldsymbol{K}$ along with all its conjugates with respect to the basefield $\boldsymbol{F}$. A normal basis can be written as $\{\sigma_i(\alpha)\}$. While normal bases are abundant in $\boldsymbol{C}_{\boldsymbol{R}}$, the existence of a normal basis is not even assured in general field extensions. For one thing, in order for $\{\sigma_i(\alpha)\}$ to be a normal basis for $\boldsymbol{K}_{\boldsymbol{F}}$, the cardinality of the automorphism group must be the same as that of the extension degree $[\boldsymbol{K} : \boldsymbol{F}]$ (since $\boldsymbol{K}$ is a vector space of dimension $[\boldsymbol{K} : \boldsymbol{F}]$ over $\boldsymbol{F}$), a condition thst is not satisfied in general. Fortunately, for cyclotomic extensions, the condition does hold [18]–[20]. Furthermore,

because cyclotomic extensions are finite extensions, the equality of $|\mathrm{Aut}_F K|$ and $[\boldsymbol{K} : \boldsymbol{F}]$ not only is necessary, but also sufficient to guarantee the existence of a normal basis. Cyclotomic extensions are *finite Galois* extensions, i.e., *finite, separable, normal* extensions [18]–[20]. By a classical theorem in Algebra (the *Normal Basis Theorem*), all such extensions admit a normal basis [18]–[20].

Finally, we turn to the question of a linear functional on $\boldsymbol{K}_{\boldsymbol{F}}$. In Section II, we loosely defined φ as

$$\mathrm{Tr}\,(\zeta) = \sum \text{ conjugates of } \zeta.$$

A more precise definition is

$$\mathrm{Tr}\,\zeta = \sum_i \sigma_i(\zeta).$$

The difference between the two definitions is a small but important point; it has to do with the size of the conjugacy class of ζ. Given an element $\zeta \in \boldsymbol{K}$ (assume $[\boldsymbol{K} : \boldsymbol{F}] = |\mathrm{Aut}_F K|$), the cardinality of the conjugacy class of ζ divides $[\boldsymbol{K} : \boldsymbol{F}]$ (e.g., $[\boldsymbol{C} : \boldsymbol{R}] = 2 \Longrightarrow$ the conjugacy classes are of sizes 1 or 2). Thus the first definition would include only $|\mathrm{Orb}\,(\zeta)|$ terms in the sum whereas the second (correct) definition would include $[\boldsymbol{K} : \boldsymbol{F}]$ terms.

We now have all the ingredients necessary to construct a basefield transform. Given a sequence $\{x_n\}$ in $\boldsymbol{F}$, find its Nth cyclotomic extension $\boldsymbol{K}$. The extension is necessarily finite and Galois over $\boldsymbol{F}$. By the Normal Basis Theorem, there exists an element $\alpha \in \boldsymbol{K}$ such that $\{\sigma_i(\alpha)\}$ is a normal basis for $\boldsymbol{K}_{\boldsymbol{F}}$. Let $\beta \in \boldsymbol{K}$ be the generator of the dual basis $\{\sigma_i(\beta)\}$ of $\{\sigma_i(\alpha)\}$. Then, the basefield transform is given by

$$\tilde{X}_k = \sum_{n=0}^{N-1} x_n \,\mathrm{Tr}\,(\alpha W_N^{nk}), \qquad 0 \le k \le N-1$$

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

IX. Conclusion

In this paper we have attempted to draw out the close connections between various transforms widely reported in the engineering literature. We have shown that the discrete combinational Fourier transform may be obtained as a special case of the projection of the Fourier transform from the complex field to the real field. We have shown that by imposing the self-inverse condition on the discrete combinational Fourier transform, one arrives at the conventional Hartley transform. We have also shown that by projecting existing fast Fourier transform algorithms, one can derive the known fast Hartley transform algorithms without resorting to trignometric identities. While the development was confined to the familier real case, we have cast it in a general framework which we believe illuminates the relationship between the various transforms and also provides a foundation for the extension of the technique to more general fields. This has three main uses: First, by using the tools developed in this paper, it is possible to derive the Hartley equivalent of almost any Fourier domain property or algorithm. Thus one could devise, for example, sliding Hartley transforms, pruned Hartley algorithms, power spectrum computations, and so on. Second, the generality of the approach makes it possibe to find applications in situations where transform computations are performed in an extension field of the basic field where the data are given. Such situations occur, for example, in the area of error-control coding. Finally, the projection method provides an effortless way to develop efficient computational algorithms over any field.

X. Appendix
Definitions of Mathematical Terms

This Appendix contains the definitions of some of the mathematical terms that were used in the paper. The definitions may be found in any standard textbook on Algebra [19]–[22].

Injection, surjection, bijection: A function $f : A \to B$ is said to be an *injection* if it is one-to-one. f is said to be a *surjection* if it is onto. If f is both an injection and a surjection, then it is called a *bijection.*

Involutionary: A function f is said to be *involutionary* if it is its own inverse, i.e., $f^{-1} = f$.

Euler's totient function: Euler's *totient function* is the function which assigns to each positive integer n the number $\phi(n)$ defined as the number of integers between 1 and n that are relatively prime to n.

Characteristic: If $\boldsymbol{F}$ is a field and $\boldsymbol{F_0}$ is the minimal subfield contained in $\boldsymbol{F}$, then $\boldsymbol{F_0}$ is isomorphic to $\boldsymbol{Q}$ (the field of rationals) or $\boldsymbol{Z_p}$, p prime (the field of integers mod p). If $\boldsymbol{F_0}$ is isomorphic to $\boldsymbol{Q}$, then $\boldsymbol{F}$ is said to be a field of *characteristic 0.* If $\boldsymbol{F_0}$ is isomorphic to $\boldsymbol{Z_p}$, then $\boldsymbol{F}$ is said to be a field of *characteristic p.*

Basefield, extension field: If $\boldsymbol{F}$ is a field and $\boldsymbol{K}$ is field containing $\boldsymbol{F}$, then $\boldsymbol{F}$ is called the *base* or the *ground field* and $\boldsymbol{K}$ is called an *extension field* or simply an *extension* of $\boldsymbol{F}$.

Automorphism, Galois group, orbit: If $\boldsymbol{K}$ is a field, an *automorphism* of $\boldsymbol{K}$ is a field isomorphism of $\boldsymbol{K}$ into itself. If $\boldsymbol{K}$ is an extension of $\boldsymbol{F}$, the set of all automorphisms of $\boldsymbol{K}$ which leave the subfield $\boldsymbol{F}$ fixed forms a group called the *Galois group* or the *automorphism group* of $\boldsymbol{K}$ over $\boldsymbol{F}$ (notations: $\mathrm{Gal}\,(K/F)$ or $\mathrm{Aut}_F K$). If $\mathrm{Gal}\,(K/F) = \{\phi_i\}$ and $\alpha \in \boldsymbol{K}$, then the *orbit* of α under $\mathrm{Gal}\,(L/K)$ is the set $\{\phi_i(\alpha)\}$.

Minimal polynomial, algebraic extension, algebraic closure: Let $\boldsymbol{K}$ be an extension of $\boldsymbol{F}$ and let $\alpha \in \boldsymbol{K}$. If there exists a nonzero polynomial $f(x) \in \boldsymbol{F}[x]$ such that $f(\alpha) = 0$, then α is said to be *algebraic* over $\boldsymbol{F}$. The unique monic polynomial of the minimal degree such that $f(\alpha) = 0$ is called the *minimial polynomial* of α. If no polynomial exists such that $f(\alpha) = 0$, then α is said to be *transcendental* over $\boldsymbol{F}$. If every element in $\boldsymbol{K}$ is algebraic over $\boldsymbol{F}$, then $\boldsymbol{K}$ is said to be an *algebraic extension* of $\boldsymbol{F}$. A field $\boldsymbol{F}$ that admits no proper algebraic extensions is said to be *algebraically closed.*

Separable, normal, cyclotomic and Galois extensions: Let $\boldsymbol{K}$ be an algebraic extension of $\boldsymbol{F}$. If for every $\alpha \in \boldsymbol{K}$ the minimal polynomial of α has distinct roots in a splitting field, then $\boldsymbol{K}$ is said to be a *separable extension* of $\boldsymbol{F}$. If every irreducible polynomial in $\boldsymbol{F}[x]$ that has a root in $\boldsymbol{K}$ splits over $\boldsymbol{K}$ then $\boldsymbol{K}$ is called a *normal extension* of $\boldsymbol{F}$. An algebraic extension that is both normal and separable is called a *Galois extension* (of $\boldsymbol{F}$). Examples of Galois extensions are the *cyclotomic extensions* which are the splitting fields of the polynomials $x^n - 1$, $n \in \boldsymbol{Z}$.

Finite extension, trace orthogonality, dual and normal basis, generator: If $\boldsymbol{K}$ is an extension of $\boldsymbol{F}$, then $\boldsymbol{K}$ is a vector space over $\boldsymbol{F}$. If, as a vector space, $\boldsymbol{K}$ is finite-dimensional, then $\boldsymbol{K}$ is said to be a *finite extension* of $\boldsymbol{F}$. Given a finite Galois extension $\boldsymbol{K}$ of $\boldsymbol{F}$ of dimension m, there exists $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ in $\boldsymbol{K}$ such the $\{\alpha_i\}$ is a basis for the vector space $\boldsymbol{K}$ over $\boldsymbol{F}$. The *dual basis* of $\{\alpha_i\}$ is defined as the basis $\{\beta_j\}$ such that

$$\mathrm{tr}\,(\alpha_i \beta_j) = \delta_{ij} \qquad \forall i, j$$

where $\mathrm{tr}\,(\cdot)$ is the linear function from $\boldsymbol{K}$ to $\boldsymbol{F}$ defined as

$$\mathrm{tr}\,(\zeta) = \sum_{\phi_i \in \mathrm{Gal}\,(K/F)} \phi_i(\zeta).$$

In other words, the bases $\{\beta_j\}$ and $\{\alpha_i\}$ are *trace-orthogonal*. If the basis $\{\alpha_i\}$ consists of the orbit under $\mathrm{Gal}\,(K/F)$ of a single element $\alpha \in \boldsymbol{K}$, i.e., $\{\alpha_i\} = \{\phi_i(\alpha) | \phi_i \in \mathrm{Gal}\,(K/F)\}$ for some $\alpha \in \boldsymbol{K}$, then $\{\phi_i, (\alpha)\}$ is called a *normal basis* and α is called the *generator* of the basis.

Conjugates, conjugacy class: Given an element α in $\boldsymbol{K}$, an element β in $\boldsymbol{K}$ is said to be a *conjugate* of α over $\boldsymbol{F}$ is α and β have the same minimal polynomial over $\boldsymbol{F}$. The set of all elements in $\boldsymbol{K}$ that are conjugates of α over $\boldsymbol{F}$ is called the *conjugacy class* of α.

ACKNOWLEDGMENT

The authorswish to thank Dr. A. M. Krot of the Belarusian Academy of Sciences for his careful reading of the paper and his many helpful comments and suggestions.

REFERENCES

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

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

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

[4] J. W. Cooley, "The structure of FFT and convolution algorithms," in *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*, Apr. 1990.

[5] I. J. Good, "The relationship between two fast Fourier transforms," *IEEE Trans. Comput.*, vol. C-20, pp. 310–317, 1971.

[6] J. M. Pollard, "The fast Fourier transform in a finite field," *Math. of Comput.*, vol. 25, no. 114, pp. 365–374, Apr. 1971.

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

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

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

[10] ——, "Improved Fourier and Hartley transform algorithms. application to cyclic convolution of real data," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. ASSP-35, no. 6, pp. 818–824, June 1987.

[11] M. Vetterli and H. J. Nussbaumer, "Simple FFT and DCT algorithms with reduced number of operations," *Signal Process.*, vol. 6, pp. 267–278, Aug. 1984.

[12] A. M. Krot and H. B. Minervina, "FFT algorithms for real-valued and Hermitian symmetric sequences," *Radiotekh. Elektron.*, vol. 34, no. 2, pp. 369–376, 1989.

[13] ——, "Synthesis of FFT split-radix algorithms for real-valued and Hermitian-symmetrical series," *Radioelectron. Commun. Syst.*, no. 12, pp. 10–15, 1989.

[14] A. M. Krot, "A single approach to the convolution and DFT calculations on the basis of the Eigen transforms in rational and real fields," *Radiotekh. Elektron.*, vol. 35, no. 4, pp. 805–815, 1990.

[15] G. D. Bergland, "A fast Fourier transform algorithm using base 8 iterations," *Math. of Computat.*, vol. 22, pp. 275–279, Apr. 1968.

[16] J. Hong and M. Vetterli, "Hartley transforms over finite fields," to appear in *IEEE Trans. Informat. Theory*, Sept. 1993.

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

[18] J. R. Bastida, *Field Extensions and Galois Theory (Encyclopedia of Mathematics and Its Applications)*, vol. 22. Reading, MA: Addison-Wesley, 1984.

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

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

[21] J. B. Fraleigh, *A First Course in Abstract Algebra*, 3rd ed. Reading, MA: Addison-Wesley, 1982.

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

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

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

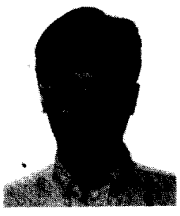
[25] R. E. Blahut, *Fast Algorithms for Digital Signal Processing*. Reading, MA: Addison-Wesley, 1986.

[26] R. N. Bracewell, *The Hartley Transform*. Oxford, UK: Oxford Univ. Press, 1985.

[27] J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing*. Englewood Cliffs, NJ: Prentice-Hall, 1979.

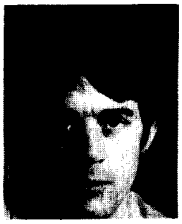
[28] A. V. Oppenheim and R. W. Schafer, *Digital Signal Processing* Englewood Cliffs, NJ: Prentice Hall, 1975.

[29] J. Hong, Ph.D. dissertation, Columbia University, New York, NY, 1999.



Jonathan Hong received the B.A. degree in mathematics from the University of California at Berkeley in 1985, the M.S. degrees in mathematics and computer science in 1988, and both from the University of Illinois at Urbana-Champaign, and the Ph.D. degree in electrical engineering from Columbia University, New York, NY, in 1993.

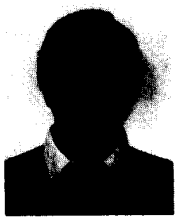
His research interests include finite field transforms, computational complexity, and coding theory.



Martin Vetterli (Senior Member, IEEE) received the Dipl. El.-Ing. degree from the ETH Zürich, Switzerland, in 1981, the M.S. degree from Stanford University, Stanford, CA, in 1982, and the Doctorat ès Science degree from EPF Lausanne, Switzerland, in 1986.

He was a Research Assistant at Stanford and EPFL, and worked for Siemens and AT&T Bell Laboratories. In 1986, he joined Columbia University, New York, where he is currently Associate Professor of Electrical Engineering. Since July 1993, he has also been an Acting Associate Professor in the Department of Electrical Engineering and Computer Science at the University of California at Berkeley. His research interests include wavelets, multirate signal processing, computational complexity, signal processing for telecommunications, as well as digital video processing and compression. He is a member of the editorial boards of *Signal Processing, Image Communication, Annals of Telecommunications, Applied and Computational Harmonic Analysis*, and *The Journal of Fourier Analysis and Applications*. He received the Best Paper Award of EURASIP in 1984 for his paper on multidimensional subband coding, the Research Prize of the Brown Bovery Corporation (Switzerland) in 1986 for his thesis, and the IEEE Signal Processing Society's 1991 Senior Award for the 1989 TRANSACTIONS paper with D. LeGall. He was a plenary speaker at the 1992 IEEE ICASSP, and is the co-author, with J. Kovacevic, of the forthcoming book *Wavelets and Subband Coding* (Englewood Cliffs, NJ: Prentice-Hall, 1994).

Dr. Vetterli is a member of SIAM and ACM.



Pierre Duhamel (Member, IEEE) was born in France in 1953. He received the Ing. degree in electrical engineering from the National Institute for Applied Sciences (INSA), Rennes, France, in 1975, the Dr. Ing. degree in 1978, and the Doctorat ès Sciences degree in 1986, both from Orsay University, Orsay, France.

From 1975 to 1980, he was with Thomson-CSF, Paris, France, where his research interests were in circuit theory and signal processing, including digital filtering and analog fault diagnosis. In 1980, he joined the National Research Center in Telecommunications (CNET), Issy les Moulineaux, France, where his activities were first concerned with the design of recursive CCD filters. Later, he worked on fast Fourier transforms and convolution algorithms, and now applies similar techniques to adaptive filtering, spectral analysis, and wavelet transforms, with applications in channel equalization and source coding. Since June 1993, he has been Professor at Télécom Paris (ENST) with research activities in the same areas.

Dr. Duhamel is vice-chairman of the DSP Committee, was an Associate Editor of the IEEE TRANSACTIONS ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING from 1989 to 1991, and is Associate Editor for the IEEE SIGNAL PPROCESSING LETTERS.