BASEFIELD TRANSFORMS DERIVED FROM CHARACTER TABLES

Andreas Klappenecker, Student Member, IEEE*

Universität Karlsruhe, Institut für Algorithmen und Kognitive Systeme, Am Fasanengarten 5,
D–76 128 Karlsruhe, Germany; e-mail: klappi@ira.uka.de

ABSTRACT

We show that it is possible to define Hartley-like transforms for (generalized) character tables of finite groups. This large class of transforms include Hartley transforms for discrete Fourier transforms over abelian groups and Hartley-like transforms for the discrete cosine transform of type I.

INTRODUCTION

Calculating the Discrete Fourier Transform (DFT) of a real signal vector usually affords complex arithmetic. One can dispense with the complex arithmetic using the Discrete Hartley Transform (DHT) to compute the DFT.

Similar ideas can be applied to DFTs over arbitrary fields. Typically, computing the DFT of signal vectors over a basefield F amounts to a field extension, since in general the basefield F does not contain the required roots of unity. However, it is possible to define Hartley-like transforms (sharing many properties with the associated DFTs) that do not require an extension of the basefield.

Such transforms were first introduced in [4] under the name *Algebraic Discrete Fourier Transforms* (ADFTs) and later termed *basefield transforms with convolution property* in [7]. The DFT and corresponding basefield transforms over finite fields are discussed in [2,4,6].

We give a character theoretic explanation why the ADFT can be used to compute the DFT. Readers not familiar with the language of character theory are referred to [8,9]. In our terminology the previous results [2–7] can be derived from character tables of finite cyclic groups over some splitting field. The new transforms proposed here include basefield transforms for the DFT over abelian groups and for the Discrete Cosine Transform (and more).

CHARACTER TABLES

We recall the following facts and notions from representation theory of finite groups. Let E be a field of characteristic $p \geq 0$, V a finite dimensional vector space over E, and G a finite group. A linear representation ρ is a group homomorphism from G into $\mathrm{GL}(V)$. The representation ρ is called *irreducible* iff 0 and V are the only G-invariant linear subspaces of V. The *character* afforded by ρ is defined by $\chi : G \to E$ with $\chi(x)$ given by the trace $\mathrm{tr}(\rho(x))$ for all $x \in G$. The character of an irreducible representation is also called irreducible. There exists only a finite number of different irreducible characters $\chi_1, \cdots, \chi_n$ of G over a field E. Note that the irreducible characters $\chi_1, \cdots, \chi_n$ are linearly independent over E.

It turns out that the characters are constant on certain classes of group elements of G. We need some more terminology to describe these classes. Let p be a prime or zero. An element $g \in G$ is called *p-regular,* if p is zero or if p does not divide the order of g. A conjugacy class of p-regular elements is said to be *p-regular.* Every group element $g \in G$ can be written uniquely as $g = ab$, where a and b are commuting elements of G, the order of a is a power of p, and b is p-regular. Since the traces of $\rho(g)$ and $\rho(b)$ are always the same, it is sufficient to consider the values of the characters on the p-regular classes. Note that the value of a character is constant on every p-regular class.

The characters are constant on even large classes of group elements, provided E is not a splitting field of G. Denote by m the least common multiple of the orders of the p-regular elements of G. Let ω be a primitive mth root of unity over E. Two p-regular elements g and h of G are *E-conjugate*, if there exists some group element $x \in G$ such that $xgx^{-1} = h^{\nu}$, where ν is some integer modulo m of the set $\{ \nu \,|\, \sigma\omega = \omega^{\nu} \text{ for } \sigma \in \mathrm{Gal}\,(E(\omega)/E) \}$. The characters are constant on the E-conjugacy classes of p-regular elements $C_1, \ldots, C_r$. It was proved by Witt and Berman that the number of classes C_i and the number of irreducible characters χ_i coincide.

We define the (invertible) transform matrix X as the (generalized) character table:

$$X = (\chi_i(C_j))_{i,j=1,\ldots,r} .$$

In the next section we develop the conjugacy properties of these transforms.

CONJUGACY PROPERTIES

Assume that our signals v take values in a basefield F, a subfield of E. Exact computation of the vector-matrix-product vX affords computations in the field K obtained from F by adjoining the matrix entries of X. The value of a character is the sum of nth roots of unity, where n is a certain divisor of $|G|$. Therefore, the field extension K/F is normal. The Galois group $\mathrm{Gal}\,(K/F)$ acts on the character table by *row permutation,* since a Galois automorphism maps an irreducible character again onto an irreducible character. Moreover, since a Galois automorphism $\sigma \in \mathrm{Gal}\,(K/F)$ maps the

*This research was supported by DFG under grant Be 887/6-3 and SFB 414.

primitive nth root of unity ω onto a certain power ω^k, the value of $\sigma(\chi(g))$ can also be expressed by $\chi(g^k)$. This means that the Galois group also acts on the character table by *column permutation*.

BASEFIELD TRANSFORMS

In this section we introduce the basefield transforms associated to character tables and collect several important properties of these transforms. Roughly speaking, these transforms are obtained by projecting the matrix entries of the character table X onto values of the basefield F.

The elements of K can be expressed with respect to a basis $B = (b_1, \cdots, b_s)$ of the field extension K/F. Given an element $x = \sum_{i=1}^{s} x_i\, b_i$ of K, with $x_i \in F$, we define the projection on the kth component of the basis B by $P_k^B x = x_k$. Clearly, we can interchange permutation operations on the matrix X with the projection operator P_k^B, since P_k^B operates independently on each matrix entry.

We already noted that the Galois automorphisms of $\mathrm{Gal}\,(K/F)$ act on a character table X by row or column permutation. The permutation action of the Galois group on the character table induces a permutation action on $P_k^B X$. More precisely, there exist permutation representations ρ_L and ρ_R of $\mathrm{Gal}\,(K/F)$ such that the relations

$$\rho_L(\sigma)(P_k^B X) = P_k^B\, {}^{\sigma}X \qquad \text{and} \qquad (P_k^B X)\rho_R(\sigma) = P_k^B\, {}^{\sigma}X$$

hold for all $\sigma \in \mathrm{Gal}\,(K/F)$.

The operation of the Galois group $\mathrm{Gal}\,(K/F)$ is particularly transparent, if the elements of K are expressed with respect to a normal basis B. Such a basis[1] is given by the Galois orbit of some element k of the field K, that is, $B = (\sigma_1 k, \cdots, \sigma_s k)$. Normal bases have the feature that the projections on the different components $\left\{P_k^B(X) \,|\, k = 1, \ldots, r\right\}$ coincide with the projections of the conjugate matrices ${}^{\sigma}X$ on a fixed component $\left\{P_k^B({}^{\sigma}X) \,|\, \sigma \in \mathrm{Gal}\,(K/F)\right\}$. We already observed that the elements of the latter set are nothing but permuted versions of a *single* projection, namely they coincide with the set $\left\{\rho_L(\sigma) P_k^B(X) \,|\, \sigma \in \mathrm{Gal}\,(K/F)\right\}$ or alternatively with the set $\left\{P_k^B(X)\rho_R(\sigma) \,|\, \sigma \in \mathrm{Gal}\,(K/F)\right\}$.

To summarize, consider the product of a signal vector v over the basefield F with the character table X. If we express the result with respect to a normal base B, then vX is given by the r different vectors $vP_1^B(X), \ldots, vP_r^B(X)$. Instead of computing r different vector-matrix products, it is possible to compute a *single* vector matrix product $vP_k^B(X)$, since the other components are simply obtained by permutation of this result: $vP_m^B = vP_k^B(X)\rho_R(\sigma_m)$ for some $\sigma_m \in \mathrm{Gal}\,(K/F)$. Clearly, this leads to considerable savings.

We call $P_k^B X$ a basefield transform for X with respect to the normal basis B. The inverse transforms are derived in the next section.

INVERSE TRANSFORMS

The irreducible characters of a finite group satisfy certain orthogonality relations, which allow an explicit formulation of the inverse of a character table. We assume in this section that the field E is a splitting field for G of characteristic not dividing the order of the group G.

Denote by $C_1, \ldots, C_r$ the conjugacy classes of G and let g_i be a representative of C_i. The character table is given by the matrix $X = (\chi_i(g_j))_{i,j=1,\ldots,r}$. The inverse of X is then given by $X^{-1} = |G|^{-1}(|C_i|\,\chi_j(g_i^{-1}))$, cf. [1].

We now derive an explicit inverse for the corresponding basefield transforms of X. Let F be the basefield and K the extension field of F obtained by adjoining the matrix entries of X. We already observed that K/F is a finite Galois extension, meaning in particular that there exists a normal basis $B = (b_1, \ldots, b_s)$ for K/F. Moreover, there exists another normal basis $C = (c_1, \ldots, c_s)$ which is dual in the sense that $\mathrm{tr}_{K/F}(c_i\, b_j) = \delta_{ij}$ holds. We claim that the inverse of $P_k^B(X)$ is given by $P_k^C(X^{-1})$.

We prove this claim by calculating the matrix product $P^B(X)P^C(X^{-1})$. We remark here first that the projection operator $P_k^B(x)$ can be written with the help of the dual basis C as $\mathrm{tr}_{K/F}(c_k\, x)$. Using this we obtain for the matrix entry $Y_{ij} := \left[P_k^B(X)P_k^C(X^{-1})\right]_{ij}$ the following expression:

$$\begin{aligned} Y_{ij} &= \frac{1}{|G|}\sum_{e=1}^{r} \mathrm{tr}(c_k\chi_i(g_e))\,|C_e|\,\mathrm{tr}(b_k\chi_j(g_e^{-1})) \\ &= \frac{1}{|G|}\sum_{g\in G} \mathrm{tr}(c_k\chi_i(g))\,\mathrm{tr}(b_k\,\chi_j(g^{-1})). \end{aligned}$$

Writing out the trace forms and reordering the sums gives

$$\frac{1}{|G|}\sum_{\sigma,\tau\in\mathrm{Gal}\,(K/F)} \underbrace{\left(\sum_{g\in G}\sigma(\chi_i(g))\tau(\chi_j(g^{-1}))\right)}_{S:=} (\sigma c_k)(\tau b_k).$$

As a consequence of the orthogonality relations of characters, the inner sum S is different from zero only if $\sigma\chi_i$ is the same character as $\tau\chi_j$; in that case S equals $|G|$.

Consequently, if χ_i is conjugate to χ_j, say $\chi_j = \kappa\chi_i$ for some $\kappa \in \mathrm{Gal}\,(K/F)$, then

$$\left[P_k^B(X)P_k^C(X^{-1})\right]_{ij} = \sum_{\substack{\sigma,\tau\in\mathrm{Gal}\,(K/F)\\ \tau^{-1}\sigma=\kappa}} (\sigma c_k)(\tau b_k).$$

This last sum can be simplified to

$$\sum_{\tau\in\mathrm{Gal}\,(K/F)} (\tau\kappa c_k)(\tau b_k) = \mathrm{tr}((\kappa c_k)b_k).$$

Since C and B are dual bases, the trace expression $\mathrm{tr}((\kappa c_k)b_k)$ is non-zero only if κ is the identity; in that case we have by definition $\mathrm{tr}(c_k b_k) = 1$. We observe further that in the case $\kappa = id$ the characters χ_i and χ_j have to be identical to give some non-zero sum S. Thereby we obtain

$$\left[P_k^B(X)P_k^C(X^{-1})\right]_{ij} = \delta_{ij},$$

which proves our claim.

[1] A normal basis exists, since K/F is Galois.

A CLASSICAL EXAMPLE: THE DISCRETE HARTLEY TRANSFORM

The character table of the cyclic group $\mathbb{Z}/N\mathbb{Z}$ over the complex numbers is given by

$$X = (\exp(2\pi i\, kl/N))_{k,l=0,\dots,N-1},$$

which is nothing but the DFT of length N. Consider the basefield $F = \mathbb{R}$ of real numbers, then a normal basis for the extension $\mathbb{C}/\mathbb{R}$ is given by $B = ((1+i)/2, (1-i)/2)$. Rewriting X as $(\cos(2\pi kl/N) + i\sin(2\pi kl/N))$, the DHT of length N is obtained by (see also [3,7]):

$$P_1^B X = \Big(\cos(2\pi kl/N) + \sin(2\pi kl/N)\Big)_{k,l=0,\dots,N-1}.$$

We get the projection on the second component $P_2^B X$ by permuting $P_1^B X$ with $\sigma : x \mapsto -x \bmod N$. Clearly, this reflects the conjugacy property of the DFT.

The Discrete Hartley Transform can be viewed as a simple example of the basefield transforms considered in this paper.

ADFT OVER ABELIAN GROUPS

Let G be an abelian group. Recall that a finite abelian group is isomorphic to a direct product of cyclic groups. The complex irreducible characters of a direct product $G = H_1 \times H_2$ can be expressed with the help of the complex characters of H_1 and H_2. Namely, any irreducible character χ of G is obtained from irreducible characters χ_1, χ_2 of the groups H_1 and H_2 (resp.) by means of a product $\chi(h_1, h_2) = \chi_1(h_1)\chi_2(h_2)$. Therefore, the complex character table of an abelian group G is a Kronecker product of DFTs.

For example, the character table of the group $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is simply the Kronecker product of two DFTs of length three: $X = DFT_3 \otimes DFT_3$. If our signals are rational vectors of length nine, then a vector-matrix product vX would require an extension to the field $\mathbb{Q}(\omega)$, where $\omega = \exp(2\pi i/3)$. A normal base for the extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is given by $B = (-\omega, -\omega^2)$, since

$$-\omega = \frac{1}{2} - \frac{1}{2}i\sqrt{3}, \qquad -\omega^2 = \frac{1}{2} + \frac{1}{2}i\sqrt{3}.$$

Hence, the ADFT or basefield transform $P_1^B(X)$ is given by the following matrix:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & -1 \\
1 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\
1 & -1 & 0 & -1 & 0 & 1 & 0 & 1 & -1 \\
1 & 0 & -1 & -1 & 1 & 0 & 0 & -1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & -1 & -1 & -1 \\
1 & -1 & 0 & 0 & 1 & -1 & -1 & 0 & 1 \\
1 & 0 & -1 & 0 & -1 & 1 & -1 & 1 & 0
\end{pmatrix}.$$

An advantage of ADFTs is that they can be realized with simple arithmetic (the example shown here completely avoids any multiplications).

BASEFIELD TRANSFORMS FOR THE DCT

Let $G = \langle a \,|\, a^{2n} = 1\rangle$ be the cyclic group of order $2n$. The $\mathbb{C}$-irreducible characters of this group are given by $X_1 = (\chi_k(a^l))_{k,l=0,\dots,2n-1}$, where $\chi_k(a^l) = \exp(2\pi i\, kl/2n)$. We want to derive the $\mathbb{R}$-irreducible characters of this group. In general, each $\mathbb{R}$-irreducible character can be obtained from some $\mathbb{C}$-irreducible character χ by an expression of the form

$$m_{\mathbb{R}}(\chi) \sum_{\sigma \in \mathrm{Gal}(\mathbb{R}(\chi)/\mathbb{R})} {}^{\sigma}\chi,$$

where $m_{\mathbb{R}}(\chi)$ is a positive integer – the so-called Schur index. It is known that the Schur index divides $\chi(1)$. Therefore, we get $m_{\mathbb{R}}(\chi) = 1$, since G is abelian. It remains to determine the real-valued $\mathbb{C}$-irreducible characters. Aside from the trivial character $\chi(a^l) = 1$, there exists only one non-trivial real character, namely $\chi_n(a^l) = \exp(\pi i\, l)$. Consequently, we obtain the real character table for G :

$$X_2 = (v_k 2\cos(\pi k\, l/n))_{k,l=0,\dots,n},$$

where $v_k = 1$ except for $k = 0$ and $k = n$, where $v_k = 1/2$. The character table X_2 is the transform matrix for the DCT-I.[2]

More concretely, consider the cyclic group of order 10. The real character table X_2 for this group is given by the matrix:

$$\frac{1}{2}\begin{pmatrix}
2 & 2 & 2 & 2 & 2 & 2 \\
4 & \sqrt{5}+1 & \sqrt{5}-1 & -\sqrt{5}+1 & -\sqrt{5}-1 & -4 \\
4 & \sqrt{5}-1 & -\sqrt{5}-1 & -\sqrt{5}-1 & \sqrt{5}-1 & 4 \\
4 & -\sqrt{5}+1 & -\sqrt{5}-1 & \sqrt{5}+1 & \sqrt{5}-1 & -4 \\
4 & -\sqrt{5}-1 & \sqrt{5}-1 & \sqrt{5}-1 & -\sqrt{5}-1 & 4 \\
2 & -2 & 2 & -2 & 2 & -2
\end{pmatrix}$$

Assume that our signals are rational vectors, i. e., $F = \mathbb{Q}$. Adjoining the matrix entries of X_2 to F gives the quadratic extension field $K = \mathbb{Q}(\sqrt{5})$. A normal basis for K/F is for example given by $B := 1/2\,(\sqrt{5}-1, -\sqrt{5}-1)$. The projection $P_1^B(X_2)$ with respect to this basis is:

$$P_1^B(X) = \begin{pmatrix}
-1 & -1 & -1 & -1 & -1 & -1 \\
-2 & 0 & 1 & -1 & 0 & 2 \\
-2 & 1 & 0 & 0 & 1 & -2 \\
-2 & -1 & 0 & 0 & 1 & 2 \\
-2 & 0 & 1 & 1 & 0 & -2 \\
-1 & 1 & -1 & 1 & -1 & 1
\end{pmatrix}$$

We obtain the projection on the second component by per-

[2] The reader may be more familiar with the DCT-I obtained by the following base change: pDX_2D^{-1}, where D is the diagonal matrix $D = \mathrm{diag}(1, 1/\sqrt{2}, \dots, 1/\sqrt{2}, 1)$ and p is a prefactor $1/\sqrt{2n}$.

muting the columns with $\sigma = (24)(35)$:

$$P_2^B(X) = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 & -1 \\ -2 & -1 & 0 & 0 & 1 & 2 \\ -2 & 0 & 1 & 1 & 0 & -2 \\ -2 & 0 & 1 & -1 & 0 & 2 \\ -2 & 1 & 0 & 0 & 1 & -2 \\ -1 & 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

CONCLUSION

We outlined a general theory of basefield transforms for generalized character tables. It should be noted that these transforms have a convolution property, provided that they are derived from character tables of finite abelian groups over splitting fields of characteristic coprime to the group order. Avoiding field extensions is particularly attractive for integrated circuit implementations. We demonstrated this in [5] for the classical ADFT.

ACKNOWLEDGEMENT

It is a pleasure to thank Professor Thomas Beth for introducing me to the Algebraic Discrete Fourier Transform.

REFERENCES

[1] M. Aschbacher. *Finite group theory.* Cambridge University Press, 1986. Corr. Reprint 1994.

[2] T. Beth. *Verfahren der schnellen Fourier-Transformation.* Teubner-Verlag, 1984.

[3] T. Beth. Generating Fast Hartley Transforms – another application of the Algebraic Discrete Fourier Transform. In *Proceedings URSI-ISSSE '89, Erlangen, Deutschland*, pages 688–692, 1989.

[4] T. Beth, W. Fumy, and R. Mühlfeld. Zur Algebraischen Diskreten Fourier-Transformation. *Arch. Math.*, 40:238–244, 1983.

[5] T. Beth, A. Klappenecker, T. Minkwitz, and A. Nückel. The ART behind IDEAS. In *Computer Science Today*, volume LNCS 1000, pages 141–158. Springer Verlag, 1995.

[6] J. Hong and M. Vetterli. Hartley transforms over finite fields. *IEEE Trans. on Information Theory*, 39(5):1628–1638, 1993.

[7] J. Hong, M. Vetterli, and P. Duhamel. Basefield transforms with the convolution property. *Proc. of the IEEE*, 82(3):400–412, 1994.

[8] G. Karpilovsky. *Group representations*, volume I, part B. North-Holland, 1992.

[9] J.-P. Serre. *Linear Representations of Finite Groups.* Springer-Verlag, 1977.