Harmonic Analysis of Binary Functions

Jean-Claude Belfiore
Communications and Electronics Dept.
Telecom ParisTech
Paris, France
jean-claude.belfiore@telecom-paristech.fr

Yi Hong
ECSE Department
Monash University
Clayton, Australia
yi.hong@monash.edu

Emanuele Viterbo
ECSE Department
Monash University
Clayton, Australia
emanuele.viterbo@monash.edu

***Abstract*—In this paper we introduce the two-modular Fourier transform of a binary function $f : \mathcal{R} \to \mathcal{R}$ defined over a finite commutative ring $\mathcal{R} = \mathbb{F}_2[X]/\phi(X)$, where $\mathbb{F}_2[X]$ is the ring of polynomials with binary coefficients and $\phi(X)$ is a polynomial of degree n, which is not a multiple of X. We also introduce the corresponding inverse Fourier transform. We then prove the corresponding convolution theorem.**

***Index Terms*—two-modular Fourier transform, binary functions, binary groups**

I. Introduction

Harmonic analysis of binary functions is a powerful tool which allows to derive deep results in computational complexity (cf. the PCP problem in [1, Chap. 22]). When the function takes scalar binary values, then, this scalar value can be mapped to the set $\{+1, -1\}$ and we get a classical problem of harmonic analysis of complex-valued functions. When the function takes values in a binary vector space, then we can no more use the same method and we have to find a Fourier transform which complies with the characteristics 2.

The Fourier transforms of functions over finite abelian groups $f : G \to \mathbb{C}$ (complex field) or $f : G \to \mathbb{Z}$ (ring of integers) have been extensively studied [3]. For complex valued functions, and when the group is cyclic, the Fourier transform is the well-known discrete Fourier Transform [3]. For complex valued functions, and if the group G is C_2^n where C_2 is the cyclic group of order 2, the Fourier transform is the well known Hadamard transform, commonly used for analysing Boolean functions [2].

A less common case occurs for $f : G \to \mathcal{R}$, where $\mathcal{R}$ is a ring of characteristics p. For any prime p co-prime with the order of G, the p-modular Fourier transform is defined in a way similar to the case where f is complex-valued. However, when p is not coprime with the order of the group, and especially in the case of $p = 2$ and the order of G is 2^n, the Fourier transform cannot be handled in the same way.

In this paper, we introduce the *two-modular Fourier transform* of a binary function $f : \mathcal{R} \to \mathcal{R}$ defined over a finite commutative ring $\mathcal{R} = \mathbb{F}_2[X]/\phi(X)$, where $\mathbb{F}_2[X]$ is the ring of polynomials with binary coefficients and $\phi(X)$ is a polynomial of degree n, which is not a multiple of X. The function f can be viewed as a binary function over the elements of the additive group of $\mathcal{R}$, i.e., $f : G \to \mathcal{R}$, where $G = C_2^n = C_2 \times \cdots \times C_2$ is the direct product of n copies of C_2. We then introduce the corresponding inverse Fourier transform, and prove the corresponding convolution theorem.

Our two-modular Fourier transform is based on the two-modular indecomposable representations of the group C_2 in dimension two and defines $n+1$ "spectral coefficients" as matrices over $\mathcal{R}$ of size $2^k \times 2^k$, for $k = 0 \ldots, n$. Our two-modular Fourier transform preserves the structure of the ring $\mathcal{R}$, which is lost if the characteristic zero Fourier transform were used. This Fourier transform may have broad applications to problems, where binary functions need to be reliably computed or for classification of binary functions.

II. Background

A. Fourier Transform of $f : G \to \mathbb{C}$

The classical notion of Fourier transform over arbitrary finite groups is based on the degree-n representations of group elements by complex $n \times n$ matrices in $GL(n, \mathbb{C})$. It generalizes the well known discrete Fourier transform, which is naturally defined over a cyclic group, which has n distinct scalar representations ρ_k, given by the powers of the n-th roots of unity

$$\rho_k = \{\exp(i2\pi k\ell/n), \ell = 0, \ldots n-1\}$$

for $k = 0, \ldots n-1$. In the general case where G is not cyclic, the group representations are matrices and we have

Definition 1: ([3]) Given a finite group G, the Fourier transform of a function $f : G \to \mathbb{C}$ evaluated for a given representation $\rho : G \to GL(d_\rho, \mathbb{C})$ of G, of degree d_ρ, is given by the $d_\rho \times d_\rho$ matrix

$$\hat{f}(\rho) = \sum_{a \in G} f(a)\rho(a)$$

The complete Fourier transform is obtained by considering the set $\{\rho_k\}$ of all inequivalent representations of G. The matrix entries of ρ_k are mutually orthogonal matrix functions over G and $\{\rho_k\}$ form the Fourier basis. Since the dimension of the 'frequency domain' space is equal to the dimension of the 'time domain' space we have

$$\sum_k d_{\rho_k}^2 = |G|$$

Definition 2: ([3]) The inverse Fourier transform evaluated at $a \in G$ is given by

$$f(a) = \frac{1}{|G|} \sum_k d_{\rho_k} \text{ Tr } \left(\rho_k(a^{-1}) \hat{f}(\rho_k) \right)$$

where Tr$(\cdot)$ is the trace of the matrix.

The above Fourier transform is well defined for complex valued functions over finite groups G and can be used to transform convolution in the 'time-domain' defined as [3]

$$(f_1 * f_2)(a) = \sum_{b \in G} f_1(ab^{-1}) f_2(b) \tag{1}$$

into the product in the 'frequency domain' i.e., [3]

$$(\widehat{f_1 * f_2})(\rho) = \hat{f}_1(\rho) \hat{f}_2(\rho)$$

B. Fourier Transform of $f : G \to K$

If we are interested in computing the Fourier transform of functions over a finite group G taking values in a finite field K of prime characteristic p we need to modify the Definition 1 and work with p-modular representations of the group G. The representations $\rho(a)$ are now in $GL(n, K)$ i.e., $n \times n$ matrices with entries in K.

Definition 3: A p-modular representation of a group G over a field K of prime characteristic p is a group homomorphism π which associates group elements to $k \times k$ matrices over K, i.e., $\pi : G \mapsto GL(k, K)$, such that the addition of two group elements corresponds to the matrix multiplication of the corresponding representation matrices. ■

The case where $K = \mathbb{C}$ has characteristic zero and yields the well known representation theory [4]. Definitions 1 and 2 provide the Fourier transform pair only if p is co-prime with $|G|$.

III. The two-modular Fourier transform

In this paper, we focus on binary functions $f : \mathcal{R} \to \mathcal{R}$ defined over a finite commutative ring $\mathcal{R} = \mathbb{F}_2[X]/\phi(X)$, where $\phi(X)$ is a polynomial of degree n, which is not a multiple of X. The elements of $\mathcal{R}$ can be represented as binary coefficient polynomials of degree less than n, where the ring operations are polynomial addition and multiplication mod $\phi(X)$.

Note that $G = C_2 \times \cdots \times C_2$ (the direct product of n copies cyclic groups of order two) coincides with the additive group of $\mathcal{R}$, where the elements can also be represented as binary vectors $\mathbf{b}$ of length n with mod two addition (or bitwise exclusive-OR). This means that we are actually working with functions $f : G \to \mathcal{R}$. In the special case where $\phi(X)$ is an irreducible polynomial $\mathcal{R}$ is the finite field $K = \mathbb{F}_{2^n}$.

Here, we consider the two-modular representation of $C_2 = \{0, 1\}$ as 2×2 binary matrices, i.e., $\pi_1(C_2) = \{E_0, E_1\}$, where

$$\pi_1(0) = E_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \pi_1(1) = E_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Then, we can represent the n-fold direct product $G = C_2 \times \cdots \times C_2 = C_2^n$ as tensor product of the representations of C_2 [4], i.e.,

$$\pi_n(G) \triangleq \pi_1(C_2) \otimes \cdots \otimes \pi_1(C_2) = \pi_{n-1}(C_2^{n-1}) \otimes \pi_1(C_2) \tag{2}$$

Note that the elements of G are n-bit binary vectors $\mathbf{b}$ and the group operation $\oplus$ is bitwise exclusive-OR. The corresponding representation matrix of an element $\mathbf{b} = (b_1, \ldots, b_n)$ is ([4])

$$E_{\mathbf{b}} \triangleq \pi_1(b_1) \otimes \cdots \otimes \pi_1(b_n) \ . \tag{3}$$

We also define the representation of the trivial group $\{0\}$ as $\pi_0(\{0\}) \triangleq 1$.

Lemma 1: The representations π_k for $k = 0, \ldots, n$ are faithful. ■

Proof: For $k = 0$ and 1 it is straightforward. For $k \geq 2$ we prove it by induction using the recursion (2). Thus it is enough to consider the case $k = 2$ and show that π_2 is a group homomorphism between C_2^2 and $\pi_2(C_2^2)$, i.e., that

$$\pi_2(b_1 \oplus c_1, b_2 \oplus c_2) = \pi_2(b_1 b_2) \cdot \pi_2(c_1 c_2)$$

or equivalently,

$$E_{b_1 \oplus c_1, b_2 \oplus c_2} = E_{b_1 b_2} \cdot E_{c_1 c_2}.$$

From (2) we have $\pi_2 = \pi_1 \otimes \pi_1$ then

$$\begin{aligned} E_{b_1 b_2} \cdot E_{c_1 c_2} &= (E_{b_1} \otimes E_{b_2}) \cdot (E_{c_1} \otimes E_{c_2}) \\ &= (E_{b_1} E_{c_1}) \otimes (E_{b_2} E_{c_2}) \\ &= E_{b_1 \oplus c_1, b_2 \oplus c_2} \end{aligned} \tag{4}$$

■

We can think of the the Fourier transform as a unitary transformation of a vector representing the values of the function f on a given ordered set of elements of G. In the following, we assume that such order is determined by the decimal representation $D(g) \in \{0, \ldots, |G|-1\}$ corresponding to the binary representation of $g \in G$.

Next, we specialize the definition of convolution in (1) for the case of additive groups.

Definition 4: Given a pair of functions f_1 and $f_2 : G \to \mathcal{R}$ we define the convolution product $f_3 : G \to \mathcal{R}$ as

$$f_3(g) = f_1(g) * f_2(g) = \sum_{u \in G} f_1(u + g) f_2(u)$$

■

It can be easily shown that the convolution product is commutative.

The aim is to project the function $f : G \to \mathcal{R}$ on a specific 'Fourier basis' $\{\psi_k\}$ where k is the 'frequency index'. The Fourier basis vectors are made up of all the two-modular representations ($2^k \times 2^k$ matrices) of the elements of the nested subgroups of $G = C_2^n$, $(n = \log_2 |G|)$, namely

$$\{0\} \lhd H_1 \lhd \cdots \lhd H_k \lhd \cdots \lhd H_{n-1} \lhd G$$

where $H_1 = C_2$, $H_2 = C_2 \times C_2$, $H_3 = C_2 \times C_2 \times C_2$, etc.

Thus we have

$$\begin{aligned}
\boldsymbol{\psi}_0 &= 1 \\
\boldsymbol{\psi}_1 &= \{E_0, E_1\} \\
\boldsymbol{\psi}_2 &= \{E_{00}, E_{11}, E_{01}, E_{10}\} \\
\boldsymbol{\psi}_3 &= \{E_{000}, E_{111}, E_{001}, E_{110}, E_{010}, E_{101}, E_{011}, E_{100}\} \\
&\vdots
\end{aligned}$$

where the scalar 1 is the representation of the trivial group $\{0\}$. The projection of f on the k-th Fourier basis vector $\boldsymbol{\psi}_k$, for $k = 0, \ldots, n$, gives the corresponding Fourier coefficient $\hat{f}_k$.

Definition 5: We abstractly define the k-th Fourier coefficients as the $2^k \times 2^k$ matrix

$$\hat{f}_k = \langle f, \boldsymbol{\psi}_k \rangle = \sum_{g \in G} f(g) E_{\tau_k(g)} \tag{5}$$

where $E_{\tau_k(g)}$ is one of the elements in $\boldsymbol{\psi}_k$ selected by g according to a surjective group homomorphism $\tau_k : G \mapsto H_k$ and $H_k = C_2^k$ are the nested subgroups of $G = G_n = C_2^n$ for $k = 0, \ldots, n$. ■

We can represent the elements of H_k as n-bit vectors with the first $n-k$ bits set to zero i.e., $H_k = \{(0, \ldots, 0, b_{n-k+1}, \ldots, b_n) | b_i \in \{0,1\}\}$. Then we consider the quotient groups G_n/H_k whose elements are represented as n-bit vectors with the last k bits set to zero i.e., $G_n/H_k = \{(b_1, \ldots, b_{n-k}, 0, \ldots, 0) | b_i \in \{0,1\}\}$. Note that these representations yield the well-known standard array of G_n as the direct product of the subgroups H_k and G_n/H_k.

Let d_k be the element of G_n with an n-bit binary representation of the decimal number 2^{k-1} (i.e., the all-zero vector with a 1 in the $(n-k+1)$-th position). Let us consider the binary subgroups $C_2 = \langle d_k \rangle = \{0, d_k\}$ generated by d_k. Then we have the following decomposition

$$\underbrace{G}_{2^n} \approx \underbrace{H_k/\langle d_k \rangle}_{2^{k-1}} \times \underbrace{\langle d_k \rangle}_{2} \times \underbrace{G/H_k}_{2^{n-k}} \tag{6}$$

for $k = 1, \ldots, n-1$, where cardinalities of the subgroups are indicated below each group. In the following we will represent the elements of $G = C_2^n$ as the leafs of a binary tree of depth n, where the 2^n leafs are labeled with the n-bit binary vectors following (6). The intermediate nodes at level k in the tree can be labeled with the elements of the nested subgroups H_k.

In Definition 5, the k-th Fourier coefficients $\hat{f}_k$ can be explicitly computed by collecting the terms with the same $E_{\tau_k(g)}$, i.e.,

$$\begin{aligned}
\hat{f}_k = \sum_{u \in H_k/\langle d_k \rangle} \Bigg\{ &\left[\sum_{g \in G_n/H_k} f(u+g) \right] E_{\sigma_k(u)} \\
&+ \left[\sum_{g \in G_n/H_k} f(u+d_k+g) \right] E_{\overline{\sigma_k(u)}} \Bigg\}
\end{aligned} \tag{7}$$

for $k = 0, \ldots, n$, where $\sigma_k(u)$ maps the elements $u \in H_k/\langle d_k \rangle$ to binary labels consisting of the last k bits of the n-bit representation of u. The corresponding $\overline{\sigma_k(u)}$ is the binary complement of the bits of $\sigma_k(u)$.

Example 1: The Fourier coefficients for a function over $G_3 = C_2^3$ can be computed using $H_1 = C_2$ and $H_2 = C_2 \times C_2$

$$\begin{aligned}
\hat{f}_0 &= \sum_{g \in G_3} f(g) \boldsymbol{\psi}_0 = \sum_{g \in G_3} f(g) \\
\hat{f}_1 &= \sum_{g \in G_3/H_1} f(\underbrace{(000)}_{u} + g) E_0 + f(\underbrace{(000)}_{u} + \underbrace{(001)}_{d_1} + g) E_1 \\
\hat{f}_2 &= \sum_{u \in H_2/\langle d_2 \rangle} \sum_{g \in G_3/H_2} f(u+g) E_{\sigma_2(u)} + f(u + (010) + g) E_{\overline{\sigma_2(u)}} \\
\hat{f}_3 &= \sum_{u \in G_3/\langle d_3 \rangle} f(u) E_{\sigma_3(u)} + f(u + (100)) E_{\overline{\sigma_3(u)}}
\end{aligned}$$

Note that we can think of $\hat{f}_0$ as the 'DC-component' of f. For convenience we index the elements of G_n with integers from 0 to $2^n - 1$ derived from the binary representation, as demonstrated in the tables below when $n = 3$. The tables also list H_1, H_2, G_3/H_1, and G_3/H_2.

$D(g)$	G_3
0	000
1	001
2	010
3	011
4	101
5	101
6	110
7	111

	H_1
0	000
1	001

	H_2
0	000
1	001
2	010
3	011

	G_3/H_1
0	000
2	010
4	100
6	110

	G_3/H_2
0	000
4	100

Fig. 1 illustrates the binary tree for the $E_{\mathbf{b}}$, where $\mathbf{b}$ is a binary vector with k bits and k is the depth in the tree. This tree is constructed as follows. A node labeled with $E_{\mathbf{b}}$ at level $k-1$ (the number of bits in $\mathbf{b}$) splits into two branches leading to an upper node labeled by $E_{\mathbf{b},0}$ (append 0) and a lower node labeled by $E_{\overline{\mathbf{b}},1}$ (complement bits of $\mathbf{b}$ and append 1). This pair of nodes with a common father correspond to $E_{\sigma_k(u)}$ and $E_{\overline{\sigma_k(u)}}$, respectively.

Fig. 2 illustrates the binary tree with nodes labeled with the binary vectors corresponding to the subset of group elements, where the function f is evaluated in (7). At depth k, in each pair of the nodes with a common father, the upper binary vector represents the $u+g$ and the lower represents $u+g+d_k$, where $g \in G_3/H_k$ for a given u. This tree is used to compute the sums over $g \in G_n/H_k$ in (7).

Combining the labels from both trees, for each pair of nodes at level k with the same father node at level $k-1$, we are

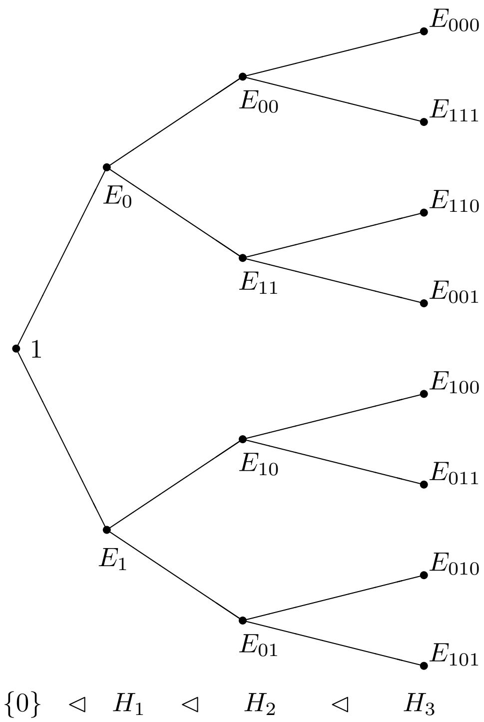

Fig. 1. Labeling tree the Fourier basis elements. The nodes level k are labeled with the representations of the elements of the subgroup H_k.

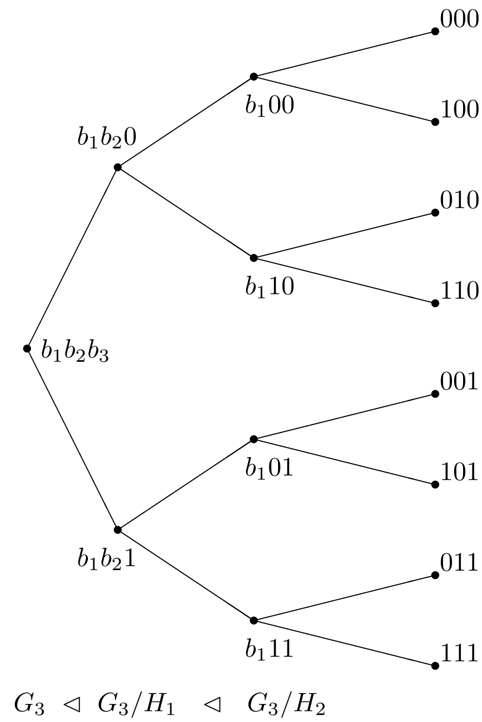

Fig. 2. Labeling tree of the arguments of f in the sums in (7) that multiply the Fourier basis elements. The bit vector labels of the elements in G are obtained by letting b_1, b_2, and b_3 vary in $\{0, 1\}$.

able to compute

$$\left[\sum_{g \in G_n/H_k} f(u+g)\right] E_{\sigma_k(u)}$$

and

$$\left[\sum_{g \in G_n/H_k} f(u+d_k+g)\right] E_{\overline{\sigma_k(u)}}$$

respectively, where $E_{\sigma_k(u)}$ and $E_{\overline{\sigma_k(u)}}$ are the labels from Fig. 1, while the arguments of f in the sums are the labels given in Fig. 2. ■

Example 2: The Fourier coefficients for a Dirac function over G_3, i.e., $\delta(0) = 1$ and 0 otherwise, are given by

$$\widehat{\delta(g)} = [1, E_0, E_{00}, E_{000}]$$

■

IV. The inverse two-modular Fourier transform

In the case of binary functions considered in this paper, Definition 2 cannot be used and we need to replace the $\frac{1}{|G|}\mathrm{Tr}(\cdot)$ operator with the following group homomorphism $\Phi_k : \pi_k(C_2^k) \to \mathbb{F}_2$ from the set of two-modular representations of C_2^k to $\{0, 1\}$, for $k = 1, \ldots, n$.

Definition 6: Let $\pi_k(g) = E_{\tau_k(g)} = E_g$ be the $2^k \times 2^k$ representation of an element $g \in C_2^k$ then we define the character of g as

$$\Phi_k(E_g) \triangleq (E_g)_{(1,2^k)} \in \{0, 1\}$$

i.e., Φ extracts the top-right corner element of the matrix E_g. Note that only the representation of the all ones vector $\mathbf{1}$ yields $\Phi(E_{\mathbf{1}}) = 1$, while any other binary vector representation is mapped to zero. ■

Lemma 2: Let E_{g_1}, E_{g_2} be the $2^k \times 2^k$ representation of the elements $g_1, g_2 \in C_2^k$, respectively. We have

$$\begin{aligned} \Phi_k(E_{g_1} \cdot E_{g_2}) &= \Phi_k(E_{g_1 \oplus g_2}) \\ &= \begin{cases} 1 & \text{iff } g_1 \oplus g_2 = \mathbf{1} (\text{ or } g_1 = \bar{g}_2) \\ 0 & \text{otherwise} \end{cases} \end{aligned} \tag{8}$$

■

Proof: The first equality descends directly from (4) and from the fact that Φ is a group homomorphism, while the second from Definition 6. ■

Theorem 1: The inverse Fourier transform is given by

$$f_j = \hat{f}_0 + \sum_{k=1}^{n-1} \Phi_k\left(\widetilde{E}_{j,k} \hat{f}_k\right) \tag{9}$$

where $j = 0, \ldots, 2^n - 1$, and the $\widetilde{E}_{j,k}$ are given by

$$\widetilde{E}_{j,k} = \begin{cases} E_{\sigma_k(u)} & \text{if } j \in \{D(u+g) \mid \\ & \quad u \in H_k/\langle d_k \rangle,\ g \in G_n/H_k\} \\ E_{\overline{\sigma_k(u)}} & \text{if } j \in \{D(u+d_k+g) \mid \\ & \quad u \in H_k/\langle d_k \rangle,\ g \in G_n/H_k\} \end{cases} \tag{10}$$

■

Proof: Substituting (7) in (9) we have

$$\sum_{g\in G_n} f(g) +$$
$$\sum_{k=1}^{n-1}\sum_{u\in H_k/\langle d_k\rangle}\left[\sum_{g\in G_n/H_k} f(u+g)\Phi_k\left(\widetilde{E}_{j,k}E_{\sigma_k(u)}\right)\right.$$
$$\left. + \sum_{g\in G_n/H_k} f(u+d_k+g)\Phi_k\left(\widetilde{E}_{j,k}E_{\overline{\sigma_k(u)}}\right)\right] \tag{11}$$

Using Lemma 2 and (10), either $f(u+g)$ or $f(u+d_k+g)$ remains in the inner sum of the second term in (11). For $k = 1,\ldots,n-2$, by adding modulo two with the first term in (11) yields,

$$\sum_{u\in H_k/\langle d_k\rangle}\sum_{g\in G_n/H_k} f(u+g)$$

if

$$j \in \{D(u+g) \mid u\in H_k/\langle d_k\rangle,\ g\in G_n/H_k\}$$

and

$$\sum_{u\in H_k/\langle d_k\rangle}\sum_{g\in G_n/H_k} f(u+d_k+g)$$

if

$$j \in \{D(u+d_k+g) \mid u\in H_k/\langle d_k\rangle,\ g\in G_n/H_k\}\ .$$

When $k = n-1$, we have $g = \mathbf{0}$ and f_j is given by

$$f_j = \begin{cases} f(u) & \text{if } j = D(u) \\ & \text{for some } u\in H_{n-1}/\langle d_{n-1}\rangle \\ f(u+d_{n-1}) & \text{if } j = D(u+d_{n-1}) \\ & \text{for some } u\in H_{n-1}/\langle d_{n-1}\rangle \end{cases}$$

This completes the proof. ■

V. The Convolution Theorem

Theorem 2: Given a pair of functions f and $h : G \to \mathcal{R}$ we obtain Fourier transform of the convolution product as

$$\widehat{f*h} = \hat{f}\odot\hat{h}$$

where $\odot$ represents the component wise product of the corresponding Fourier coefficient matrices. ■

Proof: Using (5) we can simply write the product of the k-th Fourier coefficient matrices of f and h as

$$\hat{f}_k\hat{h}_k = \sum_{g\in G} f(g)E_{\pi_k(g)}\sum_{g'\in G} h(g')E_{\pi_k(g')}$$

Substituting $w = g+g'$, we obtain

$$\begin{aligned}\hat{f}_k\hat{h}_k &= \sum_{w\in G}\sum_{g\in G} f(g)h(g+w)E_{\pi_k(g)}E_{\pi_k(g+w)} \\ &= \sum_{w\in G}\sum_{g\in G} f(g)h(g+w)E_{\pi_k(g)}E_{\pi_k(g)+\pi_k(w)} \\ &= \sum_{w\in G}\sum_{g\in G} f(g)h(g+w)E_{\pi_k(w)} \\ &= \sum_{w\in G}(f*h)(w)E_{\pi_k(w)} \end{aligned} \tag{12}$$

where $E_{\pi_k(g)}E_{\pi_k(g)+\pi_k(w)} = E_{\pi_k(w)}$ is due to the group homomorphism property. ■

VI. Conclusions

In this paper we defined the two-modular Fourier transform of a binary function $f : \mathcal{R} \to \mathcal{R}$ defined over a finite commutative ring $\mathcal{R} = \mathbb{F}_2[X]/\phi(X)$, where $\phi(X)$ is a polynomial of degree n, which is not a multiple of X. We also introduced the definition of the corresponding inverse Fourier transform. The major difference from the traditional modular inverse Fourier transform is that the trace is replaced by a group homomorphism extracting the top right corner element of a matrix. We finally proved the corresponding convolution theorem. This Fourier transform may have broad applications to problems where binary functions need to be reliably computed or in classification of binary functions.

References

[1] S. Arora and B. Barak, *Computational Complexity: A Modern Approach,* Cambridge University Press, 2009.

[2] R. O'Donnell, *Analysis of Boolean Functions,* Cambridge University Press, 2014.

[3] A. Terras, *Fourier Analysis on Finite Groups and Applications,* Cambridge University Press, 1999.

[4] D. Benson, *Modular Representation Theory. New Trends and Methods,* Lecture Notes in Mathematics 1081, 2nd edition 2006.