This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

The Two-Modular Fourier Transform of Binary Functions

Yi Hong, *Senior Member, IEEE,* Emanuele Viterbo, *Fellow, IEEE,* and Jean-Claude Belfiore, *Member, IEEE*

***Abstract*—In this paper, we provide a solution to the open problem of computing the Fourier transform of a binary function defined over n-bit vectors taking m-bit vector values. In particular, we introduce the two-modular Fourier transform (TMFT) of a binary function $f : G \to \mathcal{R}$, where $G = (\mathbb{F}_2^n, +)$ is the group of n bit vectors with bitwise modulo two addition $+$, and $\mathcal{R}$ is a finite commutative ring of characteristic 2. Using the specific group structure of G and a sequence of nested subgroups of G, we define the fast TMFT and its inverse. Since the image $\mathcal{R}$ of the binary functions is a ring, we can define the convolution between two functions $f : G \to \mathcal{R}$. We then provide the TMFT properties, including the convolution theorem, which can be used to efficiently compute convolutions. Finally, we derive the complexity of the fast TMFT and the inverse fast TMFT.**

***Index Terms*—Two-modular Fourier transform, binary functions, binary groups, group ring**

I. Introduction

The Fourier transform is a fundamental tool in signal processing for spectral analysis and is often used to transform a convolution between two real- or complex-valued functions into the product of the respective transforms. In discrete-time signal processing, numerical evaluation of the Fourier transform is based on the fast-Fourier transform (FFT), which enables to efficiently compute convolutions [1].

More generally, 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 [5]. For complex valued functions, when the group G is cyclic, the Fourier transform is the well-known discrete Fourier transform [5]. For complex valued functions, and when G is the additive group of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the binary field, the Fourier transform is provided by the well known Hadamard transform, commonly used for analyzing Boolean functions [4]. In computer science, harmonic analysis of Boolean functions is a powerful tool, which is used in the theory of computational complexity (cf. the PCP Theorem in [3, Chap. 22]).

The Fourier transform of $f : G \to \mathbb{C}$, when G is finite and non-Abelian, is based on the complex matrix representations of the non-Abelian group [5]. This Fourier transform satisfies the convolution theorem, which converts time-domain convolutions between functions into the product of the corresponding transforms.

The concept of Fourier transform was also extended to functions $f : G \to K$ defined over finite group G taking values in a finite field K, except for the case where the characteristic of the field *divides* the order of the group. In general, for $f : G \to \mathcal{R}$, where G is an arbitrary group and $\mathcal{R}$ is a ring of prime characteristic p co-prime with the order of G, its Fourier transform is called the *p-modular Fourier transform*, which is similar to that of $f : G \to \mathbb{C}$, when G is non-Abelian, but uses finite field matrix representations of G [5].

An application of the p-modular Fourier transform, when G is Abelian, enables to describe Reed-Solomon codes and their decoding algorithms by a frequency domain interpretation [2]. In Reed-Solomon codes, $\mathcal{R}$ is the finite field $\mathbb{F}_{2^n}$ and the Abelian group G is the cyclic multiplicative group of $\mathbb{F}_{2^n}$. In this case, the order of G is $2^n - 1$, which is *not divisible* by the characteristic 2 of the field. However, when the order of the group is *divisible* by the characteristic p, and especially in the case of $p = 2$ and $|G| = 2^n$ (the order of G), the Fourier transform has never been defined before.

In this paper, we provide a solution to this problem by introducing the *two-modular Fourier transform* (TMFT) of a binary function $f : G \to \mathcal{R}$, where $G = (\mathbb{F}_2^n, +)$ is the group of n bit vectors with bitwise modulo two addition $+$ and $\mathcal{R}$ is a finite commutative ring of characteristic 2. Furthermore, using the specific group structure of G and a sequence of nested subgroups, we introduce the fast TMFT and its inverse TMFT (ITMFT).

The TMFT is based on the two-modular two-dimensional representations of the additive group of $\mathbb{F}_2$ and defines $n+1$ "spectral components" as matrices over "0" and "1" in $\mathcal{R}$ of size $2^k \times 2^k$, for $k = 0 \ldots, n$. To develop ITMFT, we introduce a new operator which extracts the top right corner element of these matrices, since the trace operator used in the traditional Fourier transform is not valid when the characteristic of the ring $\mathcal{R}$, $p = 2$, divides the order of the group $|G| = 2^n$.

When the ring $\mathcal{R} = \mathbb{F}_2 = \{0, 1\}$, the Hadamard transform for $f : G \to \mathbb{C}$ can be used for faster convolution computations, since we can map $\mathbb{F}_2$ to $\{+1, -1\} \subset \mathbb{C}$ by $y = 2x - 1$. However, if there is no such map from $\mathcal{R}$ to $\mathbb{C}$ then the traditional Fourier transform for $f : G \to \mathbb{C}$ cannot be used for computing convolutions of $f : G \to \mathcal{R}$ functions. With our TMFT, we can provide the convolution theorem, since the TMFT preserves the multiplicative structure of the ring $\mathcal{R}$, and enables efficient computations of multiplications in the group ring $\mathcal{R}[G]$ [10] of functions $f : G \to \mathcal{R}$. Finally, we discuss the implementation and complexity of the fast TMFT and its

Yi Hong and Emanuele Viterbo are with the Department of Electrical and Computer Systems Engineering, Faculty of Engineering, Monash University, VIC 3800, e-mail: {yi.hong, emanuele.viterbo}@monash.edu. Jean-Claude Belfiore is with Communications and Electronics Dept., Telecom ParisTech, Paris, France, email: jean-claude.belfiore@telecom-paristech.fr.
This paper was presented in part in the IEEE Information Theory workshop, April 2015, Jerusalem, Israel.

This work is supported by the Australian Research Council Discovery Project with ARC DP160101077.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

inverse.

We expect the TMFT to have broad applications to problems in coding theory and computer science, for example, in reliable computation of binary functions, network coding, cryptography, and classification of binary functions [11].

The rest of this paper is organized as follows. Section II reviews the classical concept of Fourier transforms of functions defined over additive groups taking values in complex or finite fields. In Section III, we present TMFT and *fast* TMFT of a binary function $f : G \to \mathcal{R}$ defined over a finite commutative ring $\mathcal{R}$ of characteristic 2. In Section IV we present the corresponding ITMFTs, and in Section V, we prove the convolution theorem. In Section VI, we discuss the implementation aspects and complexity of the proposed TMFT and ITMFT.

II. Background

In this section, we review the classical concept of Fourier transforms of functions defined over additive groups taking values in complex or finite fields. We highlight the essential mathematical ideas that are later used to define the TMFT. In the following we assume the reader is familiar with the basic notions of *group, subgroup, quotient group, homomorphism, the fundamental homomorphism theorem*, ring, and *field* [8].

A. Algebraic view of the discrete Fourier transform

The discrete Fourier transform (DFT) is defined for N samples of a real (or complex) discrete time function $f : \mathbb{Z}_N \to \mathbb{C}$, where $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ is the time axis. We can think of f as discrete-time periodic function by N samples. The DFT provides the well known discrete spectrum of such function. We observe that the time axis $\mathbb{Z}_N$ has an additive group structure given by $G \triangleq (\mathbb{Z}_N, +)$ with addition mod N. Hence we can think of $f : G \to \mathbb{C}$ as a complex valued function over the Abelian group G.

Let the vector $\mathbf{f} = (f[n])_{n=0}^{N-1}$ contain the N values of the *time-domain* function $f : G \to \mathbb{C}$. Then the DFT of $\mathbf{f}$ is given by the *frequency-domain* vector $\hat{\mathbf{f}} = (\hat{f}[k])_{k=0}^{N-1}$, where

$$\hat{f}[k] = \sum_{n=0}^{N-1} f[n] e^{-\jmath 2\pi \frac{nk}{N}}, \qquad k = 0, \ldots, N-1, \qquad (1)$$

represents the transform of f as a function $\hat{f} : G \to \mathbb{C}$. The corresponding frequency index k also ranges in $\mathbb{Z}_N$ and the frequency axis has the same group structure as G. The inverse discrete Fourier transform (IDFT) of $\hat{\mathbf{f}}$ is given by

$$f[n] = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}[k] e^{\jmath 2\pi \frac{nk}{N}}, \qquad k = 0, \ldots, N-1. \qquad (2)$$

The well known *DFT matrix* $\mathbf{F} = \{e^{-\jmath 2\pi \frac{nk}{N}}\}_{n,k=0}^{N-1}$ is a unitary matrix such that

$$\hat{\mathbf{f}}^T = \mathbf{F}\mathbf{f}^T \quad \text{and} \quad \mathbf{f}^T = \frac{1}{N}\mathbf{F}^H \hat{\mathbf{f}}^T \qquad (3)$$

where $(\cdot)^T$ and $(\cdot)^H$ denote transposition and Hermitian transposition of a matrix, respectively. The vectors $\mathbf{f}$ and $\hat{\mathbf{f}}$ are two 'descriptions' of the signal $f[n]$ in different coordinate systems, namely the *time basis* and the *frequency basis*.

We show how the group structure of the time axis can provide more insight into the DFT operation by using the notions of *group representations* and *characters* (see Appendix A for a brief review).

For the cyclic group $G = (\mathbb{Z}_N, +)$, the scalar representation ρ_k is the homomorphism from G to the unit circle in the complex plane $\mathcal{S} = \{z \in \mathbb{C} : |z| = 1\}$, given by

$$\rho_k : G \to S_k \subset \mathcal{S} \qquad \rho_k(n) \triangleq e^{-\jmath 2\pi \frac{nk}{N}}$$

for $k = 0, \ldots, N-1$, and the image of ρ_k is the set of distinct points on the unit circle

$$S_k \triangleq \mathrm{Im}(\rho_k) = \left\{1, e^{-\jmath 2\pi \frac{k}{N}}, e^{-\jmath 2\pi \frac{2k}{N}}, \cdots, e^{-\jmath 2\pi \frac{(N-1)k}{N}}\right\}.$$

The representation ρ_k is a group homomorphism transforming G into the group of complex roots of unity S_k, i.e., for any $g_1, g_2 \in G$

$$\rho_k(g_1 + g_2) = \rho_k(g_1)\rho_k(g_2)$$

since

$$e^{-\jmath 2\pi \frac{(g_1+g_2)k}{N}} = e^{-\jmath 2\pi \frac{g_1 k}{N}} e^{-\jmath 2\pi \frac{g_2 k}{N}}.$$

We now illustrate the relation between the DFT and the representation of a cyclic group using the example below with $G = (\mathbb{Z}_6, +)$.

Example 1: Using Definition A.2 (see Appendix A) in the scalar case, Table I illustrates all the inequivalent scalar representations $\rho_k : G \to \mathcal{S}_k$ for $k = 0, \ldots, 5$. Some representations are faithful (e.g., ρ_1 and ρ_5), the others are not. According to the *fundamental homomorphism theorem* of groups [8, Th. 1.5.6], the image S_k is isomorphic to the quotient group $G/\mathrm{Ker}(\rho_k)$, where $\mathrm{Ker}(\rho_k)$ is a normal subgroup of G. □

We can formally rewrite the DFT in (1) as

$$\hat{f}[k] = \sum_{g \in G} f[g]\rho_k(g) \quad k = 0, \ldots, N-1 \qquad (4)$$

Let $(\cdot)^*$ denote complex conjugation. Then we observe that the pairwise orthogonal complex vectors $\boldsymbol{\psi}_k = [\rho_k^*(g)]_{g \in G}$, form the discrete Fourier basis vectors in $\mathbb{C}^N$ (i.e., the columns of the DFT matrix $\mathbf{F}$ in (3)). This is shown in Table II for $G = (\mathbb{Z}_6, +)$. The formal DFT in (4) can also be interpreted as the complex scalar product

$$\hat{f}[k] = \langle \mathbf{f}, \boldsymbol{\psi}_k \rangle \quad k = 0, \ldots, N-1 \qquad (5)$$

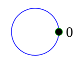
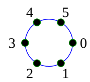
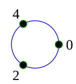
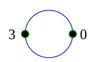
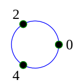
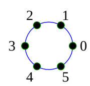
which gives the projection of the time domain vector $\mathbf{f}$ along the Fourier basis vector $\boldsymbol{\psi}_k$.

We now discuss how the fast Fourier transform (FFT) naturally stems from the group structure of $G = (\mathbb{Z}_N, +)$. From the fundamental homomorphism theorem [8, Th. 1.5.6], since $\mathrm{Ker}(\rho_k)$ is a subgroup of G, the direct product of $\mathrm{Ker}(\rho_k)$ and $G/\mathrm{Ker}(\rho_k)$ is isomorphic to G, i.e.,

$$\begin{aligned} G &= \{g = u + v | u \in \mathrm{Ker}(\rho_k), v \in G/\mathrm{Ker}(\rho_k)\} \\ &\cong \mathrm{Ker}(\rho_k) \times G/\mathrm{Ker}(\rho_k), \end{aligned} \qquad (6)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

TABLE I
DFT EXAMPLE WITH $G = (\mathbb{Z}_6, +)$.

k	$S_k = \mathrm{Im}(\rho_k) = \{\rho_k(g), g \in G = \{0,1,2,3,4,5\}\}$		$\mathrm{Ker}(\rho_k),\ G/\mathrm{Ker}(\rho_k)$
0		$\{1\}$	$\{0,1,2,3,4,5\}, \{0\}$
1		$\{1, e^{-\jmath\frac{2\pi}{6}}, e^{-\jmath\frac{4\pi}{6}}, e^{-\jmath\frac{6\pi}{6}}, e^{-\jmath\frac{8\pi}{6}}, e^{-\jmath\frac{10\pi}{6}}\}$	$\{0\}, \{0,1,2,3,4,5\}$
2		$\{1, e^{-\jmath\frac{4\pi}{6}}, e^{-\jmath\frac{8\pi}{6}}\}$	$\{0,3\}, \{0,2,4\}$
3		$\{1, -1\}$	$\{0,2,4\}, \{0,3\}$
4		$\{1, e^{\jmath\frac{4\pi}{6}}, e^{\jmath\frac{8\pi}{6}}\}$	$\{0,3\}, \{0,2,4\}$
5		$\{1, e^{\jmath\frac{2\pi}{6}}, e^{\jmath\frac{4\pi}{6}}, e^{\jmath\frac{6\pi}{6}}, e^{\jmath\frac{8\pi}{6}}, e^{\jmath\frac{10\pi}{6}}\}$	$\{0\}, \{0,1,2,3,4,5\}$

and

$$\rho_k(u) = \rho_k(0) = 1 \in S_k \quad \text{for all} \quad u \in \mathrm{Ker}(\rho_k)\ . \tag{7}$$

Then we can compute the DFT more efficiently as

$$\begin{aligned}\hat{f}[k] &= \sum_{g\in G} f[g]\rho_k(g)\\ &= \sum_{v\in G/\mathrm{Ker}(\rho_k)}\ \sum_{u\in\mathrm{Ker}(\rho_k)} f[u+v]\rho_k(u+v)\\ &= \sum_{v\in G/\mathrm{Ker}(\rho_k)}\left(\sum_{u\in\mathrm{Ker}(\rho_k)} f[u+v]\rho_k(u)\right)\rho_k(v)\\ &= \sum_{v\in G/\mathrm{Ker}(\rho_k)}\left(\sum_{u\in\mathrm{Ker}(\rho_k)} f[u+v]\right)\rho_k(v)\end{aligned} \tag{8}$$

for $k = 0, \ldots, N-1$. The last equality in (8) is due to (7). From (8), we observe how the number of multiplications reduces from $|G|^2 = N^2$ to

$$\sum_k |G/\mathrm{Ker}(\rho_k)|\ .$$

In the above example, the number of multiplications reduces from 36 to 21. Note that by taking advantage of the Hermitian symmetry of the DFT matrix $\mathbf{F}$, the number of multiplications can be further reduced to 12.

B. Fourier Transform of $f : G \to \mathbb{C}$ for arbitrary G

The classical notion of Fourier transform over arbitrary finite groups is based on the n-dimensional representations of group elements by complex $n \times n$ matrices in $GL(n, \mathbb{C})$ (see Appendix A). It generalizes the well known discrete Fourier transform, which is naturally defined over a cyclic group (additive Abelian group). In the general case where G is non-Abelian, the group element representations are matrices and we have

TABLE II
FOURIER BASIS VECTORS DFT EXAMPLE WITH $G = (\mathbb{Z}_6, +)$.

$g \in G$	0	1	2	3	4	5	
$\rho_0^*(g)$	1	1	1	1	1	1	$\boldsymbol{\psi}_0$
$\rho_1^*(g)$	1	$e^{+\jmath\frac{2\pi}{6}}$	$e^{+\jmath\frac{4\pi}{6}}$	$e^{+\jmath\frac{6\pi}{6}}$	$e^{+\jmath\frac{8\pi}{6}}$	$e^{+\jmath\frac{10\pi}{6}}$	$\boldsymbol{\psi}_1$
$\rho_2^*(g)$	1	$e^{+\jmath\frac{4\pi}{6}}$	$e^{+\jmath\frac{8\pi}{6}}$	1	$e^{+\jmath\frac{4\pi}{6}}$	$e^{+\jmath\frac{8\pi}{6}}$	$\boldsymbol{\psi}_2$
$\rho_3^*(g)$	1	-1	1	-1	1	-1	$\boldsymbol{\psi}_3$
$\rho_4^*(g)$	1	$e^{-\jmath\frac{4\pi}{6}}$	$e^{-\jmath\frac{8\pi}{6}}$	1	$e^{-\jmath\frac{4\pi}{6}}$	$e^{-\jmath\frac{8\pi}{6}}$	$\boldsymbol{\psi}_4$
$\rho_5^*(g)$	1	$e^{-\jmath\frac{2\pi}{6}}$	$e^{-\jmath\frac{4\pi}{6}}$	$e^{-\jmath\frac{6\pi}{6}}$	$e^{-\jmath\frac{8\pi}{6}}$	$e^{-\jmath\frac{10\pi}{6}}$	$\boldsymbol{\psi}_5$

Definition 1: ([5]) 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 dimension d_ρ, is given by the $d_\rho \times d_\rho$ matrix

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

The complete Fourier transform is obtained by considering all the ρ's in the set $\{\rho_k\}$ of all inequivalent irreducible representations of G (see Appendix A). □

Definition 2: ([5]) The inverse Fourier transform evaluated at $g \in G$ is given by

$$f(g) = \frac{1}{|G|}\sum_k d_{\rho_k}\,\mathrm{Tr}\left(\rho_k(g^{-1})\hat{f}(\rho_k)\right) \tag{9}$$

where $|G|$ is the order of the group G. □

Note that Definitions 1 and 2 generalize the DFT/IDFT for the Abelian group $G = (\mathbb{Z}_N, +)$. 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-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

domain' defined as[1] ([5])

$$(f_1 * f_2)(g) = \sum_{h \in G} f_1(h^{-1}g) f_2(h) \quad \text{for all} \quad g \in G \tag{10}$$

into the product of the 'frequency domain' transforms, i.e., [5]

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

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

We now consider the Fourier transform of functions over a finite group G taking values in a finite field $K = \mathbb{F}_{p^n}$ of prime characteristic p, where n is positive integer. Let α be a primitive element of K [12], then we can list all the elements in $\mathbb{F}_{p^n}$ as $\{0, 1, \alpha, \ldots, \alpha^{p^n-2}\}$.

Definition 3: ([12]) For an Abelian group $G = (\mathbb{Z}_N, +)$, where N is a divisor of $p^n - 1$ and p is coprime with N, we define the *finite field Fourier transform* of $f : \mathbb{Z}_N \to \mathbb{F}_{p^n}$ as

$$\hat{f}[k] = \sum_{n=0}^{N-1} f[n] \alpha^{nk}$$

and its *finite field inverse Fourier transform* as

$$f[n] = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}[k] \alpha^{-nk}.$$

□

The finite field inverse Fourier transform exists only if p is co-prime with $N = |G|$. This definition can be reformulated as in (4) using the scalar representations $\rho_k : G \to K$ that are defined by N vectors

$$[1, \alpha^k, \alpha^{2k}, \ldots, \alpha^{(N-1)k}] \qquad \text{for} \quad k = 0, \ldots, N-1.$$

We note that this Fourier transform is only defined when $G = (\mathbb{Z}_N, +)$ is isomorphic to a subgroup of the cyclic multiplicative group of $\mathbb{F}_{p^n}$. For any other non-Abelian group G, we need to modify Definition 1 by replacing the group representations with the *p-modular representations* of G defined below.

Definition 4: A *p-modular representation* of a group G over a field K of prime characteristic p is a group homomorphism $\pi : G \mapsto GL(n, K)$, such that the binary operation of two group elements corresponds to the matrix multiplication. □

III. The two-modular Fourier transform of binary functions

We now focus on binary functions (i.e., from n bit vectors to m bit vectors) $f : G \to \mathcal{R}$ where $G = (\mathbb{F}_2^n, +)$ is the group of n-bit binary vectors with bitwise mod two addition $+$, and $\mathcal{R}$ is a finite commutative ring of characteristic 2. For example, we can choose $\mathcal{R} = (\mathbb{F}_2^m, +, \wedge)$, where addition and multiplication are defined by bitwise $+$ (XOR) and $\wedge$ (AND) binary logic operators, respectively. Another example is a polynomial ring $\mathbb{F}_2[X]/\phi(X)$, where $\phi(X)$ is an arbitrary polynomial of degree m. In the special case where $\phi(X)$ is an irreducible polynomial, $\mathcal{R}$ is the finite field $K = \mathbb{F}_{2^m}$. The elements of $\mathcal{R}$ can be represented as binary coefficient polynomials of degree less than m, where the ring operations are polynomial addition and multiplication mod $\phi(X)$. In the following, we will denote the zero and one elements of the ring $\mathcal{R}$ as 0 and 1, and $1 + 1 = 0 \in \mathcal{R}$. In the special case of $\mathcal{R} = (\mathbb{F}_2^m, +, \wedge)$, we have $0 \to \mathbf{0}_m$ and $1 \to \mathbf{1}_m$, where $\mathbf{0}_m$ and $\mathbf{1}_m$ denote the m-bit all-zero and all-one vectors. Nevertheless, we use 0 and 1 in all cases for simplicity of notation.

For convenience of notation, we will label the n-bit vectors $\mathbf{b} = (b_1, \ldots, b_n) \in G$ using the corresponding decimal values $\{0, \ldots, 2^n - 1\}$, i.e.,

$$D(\mathbf{b}) = \sum_{k=1}^{n} b_k 2^{n-k} \tag{11}$$

and its inverse as

$$\mathbf{b} \triangleq D^{-1}(j) \tag{12}$$

for any decimal $j \in \{0, \ldots, 2^n - 1\}$. In the following, we will first introduce the *two-modular representations* of binary groups. Then we will introduce the TMFT and the fast TMFT.

A. Two-modular representations of binary groups

Definition 5: The *two-modular representation* of the binary group $C_2 = (\mathbb{F}_2, +) = \{0, 1\}$ is defined as 2×2 matrices over $\{0, 1\} \in \mathcal{R}$, i.e., $\pi_1(C_2) = \{E_0, E_1\}$, where

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

□

Lemma 1: The n-fold direct product group $C_2^n = (\mathbb{F}_2^n, +)$ can be faithfully represented as the Kronecker product of the representations of C_2, i.e.,

$$\begin{aligned} \pi_n(C_2^n) &\triangleq \pi_1(C_2) \otimes \cdots \otimes \pi_1(C_2) \\ &= \pi_{n-1}(C_2^{n-1}) \otimes \pi_1(C_2). \end{aligned} \tag{13}$$

Specifically, the matrix representation of a group element $\mathbf{b} = (b_1, \ldots, b_n)$ is,

$$E_{\mathbf{b}} \triangleq \pi_1(b_1) \otimes \cdots \otimes \pi_1(b_n). \tag{14}$$

□

Proof: We need to show that π_n is an injective homomorphism. For $n = 0$ and 1, it is straightforward. For $n \geq 2$, we prove it by induction using the recursion (13). Thus it is enough to consider the case $n = 2$ and show that π_2 is a group homomorphism between C_2^2 and $\pi_2(C_2^2)$, i.e., that

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

or equivalently,

$$E_{(b_1+c_1, b_2+c_2)} = E_{(b_1,b_2)} \cdot E_{(c_1,c_2)} \ .$$

From (13) we have $\pi_2 = \pi_1 \otimes \pi_1$ then

$$\begin{aligned} E_{(b_1,b_2)} \cdot E_{(c_1,c_2)} &= (E_{b_1} \otimes E_{b_2}) \cdot (E_{c_1} \otimes E_{c_2}) \\ &= (E_{b_1} E_{c_1}) \otimes (E_{b_2} E_{c_2}) \\ &= E_{(b_1+c_1, b_2+c_2)} \ . \end{aligned} \tag{15}$$

[1] We adopt the conventional multiplicative group notation for non-Abelian groups.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

Then, we note that $E_{\mathbf{b}} = \mathbf{I}_{2^n}$ holds only for $\mathbf{b} = \mathbf{0}_n$. This proves the homomorphism is injective, since the kernel of π_n is only the all zero binary vector. □

Finally we define the representation of the trivial group $\{0\}$ as $\pi_0(\{0\}) \triangleq 1 \in \mathcal{R}$.

Example 2: The two-modular representation of $G = \mathbb{F}_2^2$ is given by:

$$E_{00} = \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix} \quad E_{01} = \begin{pmatrix} 1&1&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1 \end{pmatrix}$$

$$E_{10} = \begin{pmatrix} 1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1 \end{pmatrix} \quad E_{11} = \begin{pmatrix} 1&1&1&1\\0&1&0&1\\0&0&1&1\\0&0&0&1 \end{pmatrix} .$$

□

We list below a few simple properties of the representation matrices.

Property 1: The 2×2 matrices E_0 and E_1 are upper triangular and have antidiagonal symmetry. Hence, any $E_{\mathbf{b}}$ defined by the Kroneker product in (14) is also upper triangular and antidiagonal symmetric. □

Property 2: Any linear combination of $E_{\mathbf{b}}$ matrices is upper triangular and antidiagonal symmetric. □

Property 3: From Lemma 1, we have $E_{\mathbf{b}} = \mathbf{I}_{2^n}$ only for $\mathbf{b} = \mathbf{0}_n$, where $\mathbf{I}_{2^n}$ denotes the $2^n \times 2^n$ identity matrix. □

Property 4: The top right corner element of $E_{\mathbf{b}}$ is 1 only for $\mathbf{b} = \mathbf{1}_n$. □

Property 5: The main diagonal of $E_{\mathbf{b}}$'s is all 1s, and hence the top left corner element is always 1.

B. The TMFT and the fast TMFT

Let us consider a sequence of nested subgroups $H_k \cong C_2^k$ of $G = C_2^n$, namely

$$H_0 = \{\mathbf{0}_n\} \lhd H_1 \lhd \cdots \lhd H_k \lhd \cdots \lhd H_{n-1} \lhd G \quad (16)$$

where $\{\mathbf{0}_n\}$ denotes the trivial group with only one element, the n-bit zero vector.

There are many possible choices for such sequence $H_k \cong C_2^k$ and we now choose a specific one, which results in a simpler notation. In particular, we choose H_k, $k = 1, \ldots, n$, to be the set of n-bit vectors with the first $n-k$ bits set to zero, i.e.,

$$H_k = \{(0, \ldots, 0, b_{n-k+1}, \ldots, b_n) | b_i \in \{0,1\}\} \cong C_2^k, \quad (17)$$

and $k = 1, \ldots, n$. Then we consider the quotient groups G/H_k, which are the sets of n-bit vectors with the last k bits set to zero, i.e.,

$$G/H_k = \begin{cases} \{(b_1, \ldots, b_{n-k}, 0, \ldots, 0) | b_i \in \{0,1\}\} & \\ & k = 1, \ldots n-1 \\ \{\mathbf{0}_n\} & k = n \end{cases} \quad (18)$$

Table III shows an example of G, H_1, H_2, G/H_1, and G/H_2 for $n = 3$ bits, where we index each element using its corresponding decimal value from (11). Let $d_k \in H_k$ be the n-bit all-zero vector except for its $(n-k+1)$-th bit set to 1, i.e.

TABLE III
NESTED SUBGROUPS AND CORRESPONDING QUOTIENT GROUPS OF C_2^3

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

	H_1
0	000
1	001

	G/H_1
0	000
2	010
4	100
6	110

	H_2
0	000
1	001
2	010
3	011

	G/H_2
0	000
4	100

$$d_k = (\underbrace{0, \ldots, 0}_{n-k}, \underbrace{1}_{n-k+1}, \underbrace{0, \ldots, 0}_{k-1})$$

Let us consider the binary subgroups of H_k generated by d_k, i.e., $\langle d_k \rangle = H_k/H_{k-1} = \{\mathbf{0}, d_k\} \cong C_2$ and $H_k/\langle d_k \rangle = H_{k-1}$. Then we have the following decomposition

$$\underbrace{G}_{2^n} = \underbrace{H_k/\langle d_k \rangle}_{2^{k-1}} \times \underbrace{\langle d_k \rangle}_{2} \times \underbrace{G/H_k}_{2^{n-k}} \quad k = 1, \ldots, n \quad (19)$$

where cardinalities of the component subgroups are indicated below each one and

$$H_k/\langle d_k \rangle = \begin{cases} \{\mathbf{0}_n\} & k = 1 \\ \{(0, \ldots, 0, b_{n-k+2}, \ldots, b_n) | & \\ \quad b_i \in \{0,1\}\} \cong C_2^{k-1} & k = 2, \ldots, n \end{cases} \quad (20)$$

For any $g = (b_1, \ldots, b_n) \in G$, we have $g = u + v$ or $g = u + v + d_k$, where $u = (0, \ldots, 0, b_{n-k+2}, \ldots, b_n) \in H_k/\langle d_k \rangle$ for $k = 2, \ldots, n$ (or $u \in \{\mathbf{0}_n\}$ for $k = 1$), and $v = (b_1, \ldots, b_{n-k}, 0, \ldots, 0) \in G/H_k$ for $k = 1, \ldots, n-1$ (or $v \in \{\mathbf{0}_n\}$ for $k = n$). The element d_k is the n-bit all-zero vector except for its $(n-k+1)$-th bit set to 1, as defined above.

We now define $\sigma_k : H_k/\langle d_k \rangle \to C_2^k$ as a map converting the n bit vectors in $H_k/\langle d_k \rangle$ to k bit vectors in C_2^k, which removes the first $n-k$ zero bits of the n bit vectors of $H_k/\langle d_k \rangle$. Specifically, for any $u \in H_k/\langle d_k \rangle$, we have

$$\sigma_k(u) \triangleq \begin{cases} 0 & k = 1. \\ (0, b_{n-k+2}, \ldots, b_n) & k = 2, \ldots, n \end{cases} \quad (21)$$

We note that $\mathrm{Im}(\sigma_k)$ does not contain any pair of complementary vectors. All the complementary vectors are in the $\mathrm{Im}(\sigma_k)$, where

$$\overline{\sigma_k(u)} \triangleq \begin{cases} 1 & k = 1. \\ (1, \bar{b}_{n-k+2}, \ldots, \bar{b}_n) & k = 2, \ldots, n \end{cases} \quad (22)$$

where $\bar{b}_i$ represents the binary complement of $b_i \in \{0,1\}$.

Lemma 2: The map σ_k is a homomorphism, i.e., given $u_1, u_2 \in H_k/\langle d_k \rangle$, we have $\sigma_k(u_1 + u_2) = \sigma_k(u_1) + \sigma_k(u_2)$ and $\sigma_k(\mathbf{0}_n) = \mathbf{0}_k$, but the map $\overline{\sigma_k}$ is not. □

Proof: The proof is straightforward. □

Let $\tau_k : G \mapsto C_2^k$, $k = 1, \ldots, n$, be a map with image $\mathrm{Im}(\tau_k) = C_2^k$, which defines the k-bit vector index $\mathbf{b} = \tau_k(g)$

of $E_{\mathbf{b}} = E_{\tau_k(g)}$, for all $g \in G$. In particular, for any $g \in G$, $\tau_k(g)$ is defined as

$$\tau_k(g) \triangleq \begin{cases} \sigma_k(u) & \text{if } g = u + v \text{ for some} \\ & u \in H_k/\langle d_k \rangle \text{ and } v \in G/H_k \\ \overline{\sigma_k(u)} & \text{if } g = u + v + d_k \text{ for some} \\ & u \in H_k/\langle d_k \rangle \text{ and } v \in G/H_k \end{cases} \tag{23}$$

Lemma 3: The map $\tau_k : G \mapsto C_2^k$ is a group homomorphism, i.e., $\tau_k(g + w) = \tau_k(g) + \tau_k(w)$, for $g, w \in G$, and $\text{Ker}(\tau_k) = G/H_k$. □

Proof: The proof is given in Appendix B. □

We now consider the two-modular representations $\pi_k(\tau_k(g)) = E_{\tau_k(g)}$ of G, with image $\text{Im}(\pi_k) = \pi_k(C_2^k) = \{E_{\tau_k(g)} : g \in G\}$ with 2^k elements isomorphic to the nested subgroups H_k, i.e.,

$$\begin{aligned} H_0 &\cong \text{Im}(\pi_0) = \{1\} \\ H_1 &\cong \text{Im}(\pi_1) = \{E_0, E_1\} \\ H_2 &\cong \text{Im}(\pi_2) = \{E_{00}, E_{01}, E_{10}, E_{11}\} \\ H_3 &\cong \text{Im}(\pi_3) = \{E_{000}, E_{001}, E_{010}, E_{011}, \\ & \qquad E_{100}, E_{101}, E_{110}, E_{111}\} \\ & \vdots \end{aligned}$$

the Fourier basis 'vectors' $\boldsymbol{\psi}_k = [E_{\tau_k(g)} : g \in G]$ are the 2^n-component vectors (indexed by g) of $2^k \times 2^k$ matrices from the set $\text{Im}(\pi_k)$.

The projection of f on the k-th Fourier basis vector $\boldsymbol{\psi}_k$, for $k = 0, \ldots, n$, gives the corresponding Fourier coefficient $\hat{f}_k$, which is a $2^k \times 2^k$ matrix.

Definition 6: (**TMFT**). We define the k-th Fourier coefficients of the TMFT for $k = 1, \ldots, n$ as the $2^k \times 2^k$ matrix

$$\hat{f}_k = \langle f, \boldsymbol{\psi}_k \rangle \triangleq \sum_{g \in G} f(g) E_{\tau_k(g)} \tag{24}$$

where $E_{\tau_k(g)}$ is the g-th element of the vector $\boldsymbol{\psi}_k$ and for $k = 0$ we define

$$\hat{f}_0 = \langle f, \boldsymbol{\psi}_0 \rangle \triangleq \sum_{g \in G} f(g) \tag{25}$$

and we refer to $\hat{f}_0$ as the 'DC-component' of f. □

We are now ready to define the *fast TMFT* to compute (24) more efficiently by collecting the terms with the same $E_{\tau_k(g)}$.

Lemma 4: (**fast TMFT**) The k-th Fourier coefficients $\hat{f}_k$ of the *fast TMFT* for $k = 1, \ldots, n$ can be efficiently computed as

$$\begin{aligned} \hat{f}_k &= \sum_{u \in H_k/\langle d_k \rangle} \left\{ \left[\sum_{v \in G/H_k} f(u + v) \right] E_{\sigma_k(u)} \right. \\ & \qquad \left. + \left[\sum_{v \in G/H_k} f(u + d_k + v) \right] E_{\overline{\sigma_k(u)}} \right\} \end{aligned} \tag{26}$$

For $k = 0$, (25) holds as is. □

Proof: We note that, in Definition 6, for $g \in G$, there are 2^n matrices $E_{\tau_k(g)}$ of size $2^k \times 2^k$ in the computation of $\hat{f}_k$, $k = 1, \ldots, n$. Among these matrices $E_{\tau_k(g)}$, there are 2^k distinct ones in pairs of $E_{\sigma_k(u)}$ and $E_{\overline{\sigma_k(u)}}$, where $u \in H_k/\langle d_k \rangle$, according to (26). Hence, the fast TMFT can collect the 2^{n-k} terms with the same $E_{\tau_k(g)}$, leading to a reduced computation complexity (see details on complexity analysis in Section VI). □

Example 3: The Fourier coefficients of the fast TMFT for a function over $G = C_2^3$ can be computed using H_1 and H_2 defined in (17) as

$$\hat{f}_0 = \sum_{g \in G} f(g) \tag{27}$$

$$\hat{f}_1 = \sum_{v \in G/H_1} f(\underbrace{(000)}_{u} + v) E_0 + f(\underbrace{(000)}_{u} + \underbrace{(001)}_{d_1} + v) E_1 \tag{28}$$

$$\hat{f}_2 = \sum_{u \in H_2/\langle d_2 \rangle} \sum_{v \in G/H_2} f(u + v) E_{\sigma_2(u)} + f(u + (010) + v) E_{\overline{\sigma_2(u)}} \tag{29}$$

$$\hat{f}_3 = \sum_{u \in H_3/\langle d_3 \rangle} f(u) E_{\sigma_3(u)} + f(u + (100)) E_{\overline{\sigma_3(u)}} \tag{30}$$

The sum indices in (27), (28), (29), and (30) are based upon these group elements listed in Table III. For example, in (29), given $\langle d_2 \rangle = \{000, 010\}$, according to (20) and (21), we choose $u \in H_2/\langle d_2 \rangle = \{000, 001\}$, and thus we obtain the corresponding $\sigma_2(u) \in \{00, 01\}$ with the associated matrices $\{E_{00}, E_{01}\}$. Then $\overline{\sigma_2(u)} \in \{11, 10\}$ and the associated matrices are $\{E_{11}, E_{10}\}$.

Similarly, in (30), given $\langle d_3 \rangle = \{000, 100\}$, we choose $u \in H_3/\langle d_3 \rangle = \{000, 001, 010, 011\}$, which yields $\sigma_3(u) \in \{000, 001\ 010, 011\}$ with the associated matrices $\{E_{000}, E_{001}, E_{010}, E_{011}\}$, and $\overline{\sigma_3(u)} \in \{111, 110,\ 101, 100\}$ with the associated matrices $\{E_{111}, E_{110}, E_{101}, E_{100}\}$.

In Fig. 1, we illustrate how to efficiently bit-label all the E matrices using a binary tree structure. At level k in the tree, let $\mathbf{b}^{(k)} = \tau_k(g)$ denote a k bit vector, then

$$E_{\mathbf{b}^{(k)}} \in \bigcup_{u \in H_k/\langle d_k \rangle} \{E_{\sigma_k(u)}, E_{\overline{\sigma_k(u)}}\} \quad k = 1, \ldots, n$$

where $g = u + v$ or $g = u + v + d_k$ for some $u \in H_k/\langle d_k \rangle$ and $v \in G/H_k$. At level k, a node labeled with $E_{\mathbf{b}^{(k)}}$ splits into two branches leading to an upper node labeled by $E_{0,\mathbf{b}^{(k)}}$ (prepend 0) and a lower node labeled by $E_{1,\overline{\mathbf{b}^{(k)}}}$ (complement bits of $\mathbf{b}^{(k)}$ and prepend 1). This pair of nodes with a common parent correspond to $E_{\sigma_{k+1}(u)}$ and $E_{\overline{\sigma_{k+1}(u)}}$, respectively.

From Definition 4, we note that the Fourier coefficient matrices $\hat{f}_k$ in the fast TMFT are linear combination of the $E_{\mathbf{b}_k}$ matrices, weighted by a sum of the time domain samples of the function f given in (26). Fig. 2 illustrates how we label the nodes for $v \in G/H_k$. For convenience of notation, the time domain samples in Fig. 2 are denoted by $f_j = f(g)$, $j = D(g)$, for any $g \in G$. At level k, in each pair of the nodes with a common parent, the upper binary vector represents the $u + v$ and the lower represents $u + v + d_k$, where $v \in G/H_k$ for a given u. This tree can be used to compute the sums over $v \in G/H_k$ in (26).

Combining the labels from both trees in Figs. 1 and 2 yields the combined tree structure illustrated in Fig. 3. For each pair

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

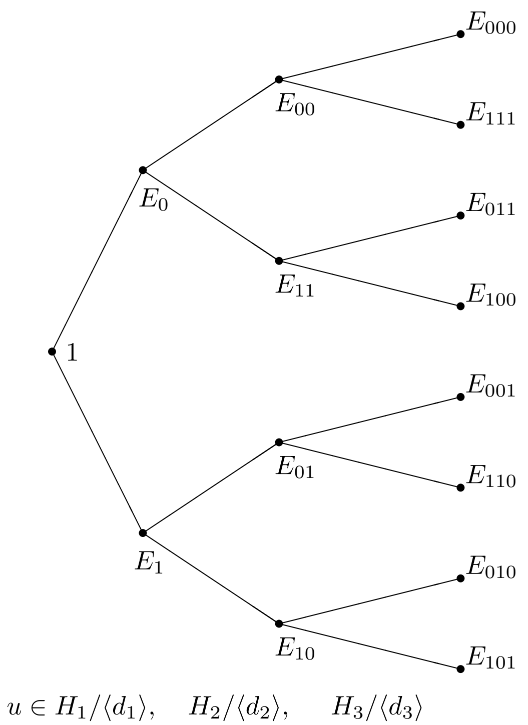


Fig. 1. Labeling tree the Fourier basis elements. The nodes in level k are labeled with the $2^k \times 2^k$ representations $E_{\tau_k(g)}$ of $u \in H_k/\langle d_k\rangle$.

of nodes at level k with the same parent node at level $k-1$, we compute

$$\left[\sum_{v \in G/H_k} f(u+v)\right] E_{\sigma_k(u)} \tag{31}$$

and

$$\left[\sum_{v \in G/H_k} f(u+d_k+v)\right] E_{\overline{\sigma_k(u)}} \tag{32}$$

respectively, where $E_{\sigma_k(u)}$ and $E_{\overline{\sigma_k(u)}}$ are the node labels from Fig. 1, while the arguments of f in the sums are given by the node labels from Fig. 2. Using Fig. 3, we can explicitly rewrite the fast TMFT coefficients in (27), (28), (29), and (30) as

$$\begin{aligned}
\hat{f}_0 &= f_0+f_1+f_2+f_3+f_4+f_5+f_6+f_7 \\
\hat{f}_1 &= (f_0+f_2+f_4+f_6)E_0+(f_1+f_3+f_5+f_7)E_1 \\
\hat{f}_2 &= (f_0+f_4)E_{00}+(f_2+f_6)E_{11} \\
&\quad +(f_1+f_5)E_{01}+(f_3+f_7)E_{10} \\
\hat{f}_3 &= f_0E_{000}+f_4E_{111}+f_2E_{011}+f_6E_{100} \\
&\quad +f_1E_{001}+f_5E_{110}+f_3E_{010}+f_7E_{101}
\end{aligned} \tag{33}$$

Alternatively, the Fourier basis vectors $\boldsymbol{\psi}_k$ in Definition 6 (non-fast TMFT) are shown in Table IV. □

Example 4: The TMFT of a Dirac function over G, i.e., $\delta_0(0)=1$ and 0 otherwise, is given by

$$\widehat{\delta_0(g)} = [1, E_0, \ldots, E_{\mathbf{0}_n}] = [1, \mathbf{I}_2, \ldots, \mathbf{I}_{2^n}]$$

i.e., the list of Fourier coefficient matrices is made up of identity matrices of increasing size. □

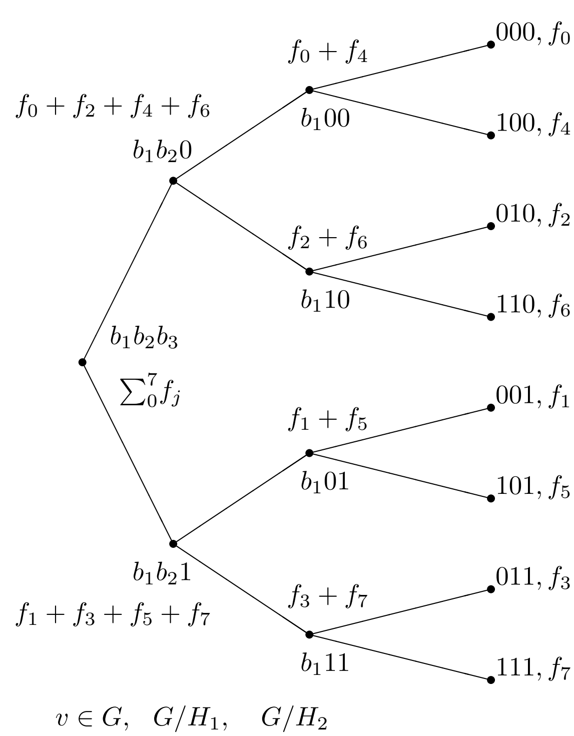


Fig. 2. Labeling tree of the arguments of f in the sums in (26) that multiply the Fourier basis elements. The bit vector labels of the elements in G are obtained by letting b_1, b_2, and b_3 vary in $\{0,1\}$.

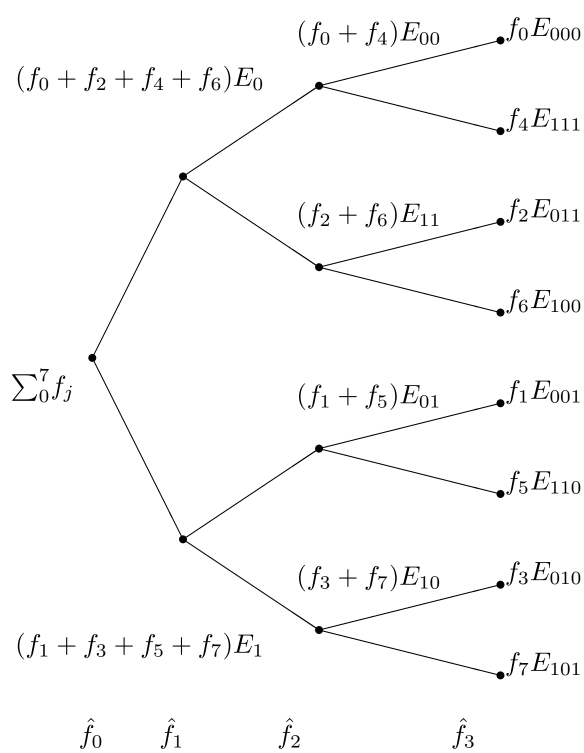


Fig. 3. Labeling tree of the multiplications of the arguments of f in the sums in (26) and the corresponding E matrices, resulting in the fast TMFT coefficients.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

TABLE IV
THE FOURIER BASIS VECTORS FOR $G = C_2^3$

$D(g)$	0	1	2	3	4	5	6	7	
$E_{\tau_0(g)}$	1	1	1	1	1	1	1	1	$\boldsymbol{\psi}_0$
$E_{\tau_1(g)}$	E_0	E_1	E_0	E_1	E_0	E_1	E_0	E_1	$\boldsymbol{\psi}_1$
$E_{\tau_2(g)}$	E_{00}	E_{01}	E_{11}	E_{10}	E_{00}	E_{01}	E_{11}	E_{10}	$\boldsymbol{\psi}_2$
$E_{\tau_3(g)}$	E_{000}	E_{001}	E_{011}	E_{010}	E_{111}	E_{110}	E_{100}	E_{101}	$\boldsymbol{\psi}_3$

Example 5: The TMFT of the indicator function of the element $g_0 \in G$, i.e.,

$$\delta_{g_0}(g) = \begin{cases} 1 & g = g_0 \\ 0 & \text{otherwise} \end{cases}$$

is given by

$$\widehat{\delta_{g_0}(g)} = \left[1, E_{\tau_1(g_0)}, \ldots, E_{\tau_n(g_0)}\right].$$

For example, $g_0 = (11) \in G = C_2^2$ yields $\widehat{\delta_{(11)}(g)} = \left[1, E_{\tau_1(11)}, E_{\tau_2(11)}\right] = [1, E_1, E_{10}]$. □

IV. THE INVERSE TWO-MODULAR FOURIER TRANSFORM

In the case of binary functions considered in this paper, Definition 2 cannot be applied since the $\frac{1}{|G|}\text{Tr}(\cdot)$ operator is undefined. In fact $|G|$ does not have an inverse and the trace of any representation matrix $E_{\mathbf{b}}$ is always zero, having an even number of ones on the diagonal (see Property 5). To overcome this problem, we introduce the matrix operator $\Phi_k : \pi_k(C_2^k) \to C_2$ from the set of two-modular representations of C_2^k to $\{0,1\}$, for $k = 1, \ldots, n$.

Definition 7: Let $E_{\mathbf{b}}$ be the $2^k \times 2^k$ representation of a k-bit binary vector $\mathbf{b} \in C_2^k$, then we define the matrix operator on $E_{\mathbf{b}}$ as

$$\Phi_k(E_{\mathbf{b}}) \triangleq E_{\mathbf{b}}[1, 2^k] \in \{0,1\}$$

i.e., Φ_k extracts the top-right corner element of the matrix $E_{\mathbf{b}}$. □

As observed in Property 4, only $\mathbf{b} = \mathbf{1}_k$ yields $\Phi_k(E_{\mathbf{b}}) = 1$, while any other binary vector representation is mapped to zero.

Lemma 5: The operator Φ_k is linear, i.e.,

$$\Phi_k(\alpha E_{\mathbf{a}} + \beta E_{\mathbf{b}}) = \alpha \Phi_k(E_{\mathbf{a}}) + \beta \Phi_k(E_{\mathbf{b}})$$

and

$$\Phi_k(E_{\mathbf{a}} E_{\mathbf{b}}) = \Phi_k(E_{\mathbf{b}} E_{\mathbf{a}}) \tag{34}$$

for any $\alpha, \beta \in \mathcal{R}$, and $\mathbf{a}, \mathbf{b} \in C_2^k$.
Proof: The proof is straightforward.

Lemma 6: Let $E_{\mathbf{a}}$ and $E_{\mathbf{b}}$ be the $2^k \times 2^k$ representation of the k-bit binary vectors $\mathbf{a}, \mathbf{b} \in C_2^k$, respectively. We have

$$\begin{aligned} \Phi_k(E_{\mathbf{a}} E_{\mathbf{b}}) &= \Phi_k(E_{\mathbf{a}+\mathbf{b}}) \\ &= \begin{cases} 1 & \text{iff } \mathbf{a} + \mathbf{b} = \mathbf{1} \text{ (or } \mathbf{a} = \bar{\mathbf{b}}) \\ 0 & \text{otherwise}. \end{cases} \end{aligned} \tag{35}$$

□

Proof: The proof is straightforward. □

Theorem 1: (**Inverse TMFT**). The *inverse TMFT* is given by

$$f_j = \hat{f}_0 + \sum_{k=1}^{n} \Phi_k\left(\hat{f}_k E_{\tau_k(D^{-1}(j))}\right) \quad j = 0, \ldots, 2^n - 1 \tag{36}$$

where $D^{-1}(j) = (c_n, \ldots, c_k, \ldots, c_1)$ [2], with $c_k \in \{0,1\}$ and τ_k is given in (23). □

Proof: Recalling (18), (19), (20), and $d_k = (0, \ldots, b_{n-k+1} = 1, 0, \ldots, 0)$ (the n-bit all-zero vector except for $b_{n-k+1} = 1$), we have

$$\begin{cases} u + v & = (b_1, \ldots, b_{n-k}, 0, b_{n-k+2}, \ldots, b_n) \\ u + v + d_k & = (b_1, \ldots, b_{n-k}, 1, b_{n-k+2}, \ldots, b_n) \end{cases} \tag{37}$$

for $k = 2, \ldots, n-1$, while in the special cases of $k = 1$ and $k = n$, we have respectively

$$\begin{cases} u + v & = (b_1, \ldots, b_{n-k}, 0) \\ u + v + d_1 & = (b_1, \ldots, b_{n-k}, 1) \end{cases} \tag{38}$$

and

$$\begin{cases} u + v & = (0, b_2, \ldots, b_n) \\ u + v + d_n & = (1, b_2, \ldots, b_n) \end{cases} \tag{39}$$

We then rewrite the right-hand side of (36) in its binary form as (40).

For any $k \in \{1, \ldots, n\}$, based on the binary representation $D^{-1}(j) = (c_n, \ldots, c_k, \ldots, c_1)$ and the definition of τ_k in (23), we have that:

- $E_{\tau_k(D^{-1}(j))} = E_{\sigma_k(\tilde{u})}$ holds when $D^{-1}(j) \in \{\tilde{u} + v \mid v \in G/H_k\}$, which implies $c_k = 0$ and $\tilde{u} = (0, \ldots, 0, c_{k-1}, \ldots, c_1)$. For such $\tilde{u}$, only the term $f(b_1, \ldots, b_{n-k}, \bar{c}_k = 1, c_{k-1}, \ldots, c_1)$ in the sum over u remains, since $\Phi_k(E_{\overline{\sigma_k(\tilde{u})}} E_{\tau_k(D^{-1}(j))}) = \Phi_k(E_{\overline{\sigma_k(\tilde{u})}} E_{\sigma_k(\tilde{u})}) = 1$. All the other terms cancel, since $\Phi_k(E_{\sigma_k(u)} E_{\sigma_k(\tilde{u})}) = 0$ for all u, and $\Phi_k(E_{\overline{\sigma_k(u)}} E_{\sigma_k(\tilde{u})}) = 0$ for all $u \neq \tilde{u}$.
- $E_{\tau_k(D^{-1}(j))} = E_{\overline{\sigma_k(\tilde{u})}}$ holds when $D^{-1}(j) \in \{\tilde{u} + v + d_k \mid v \in G/H_k\}$, which implies $c_k = 1$ and $\tilde{u} = (0, \ldots, 0, c_{k-1}, \ldots, c_1)$. For such $\tilde{u}$, only the term $f(b_1, \ldots, b_{n-k}, \bar{c}_k = 0, c_{k-1}, \ldots, c_1)$ in the sum over u remains, since $\Phi_k(E_{\sigma_k(\tilde{u})} E_{\overline{\sigma_k(\tilde{u})}}) = 1$, while the other terms cancel, since $\Phi_k(E_{\overline{\sigma_n(u)}} E_{\overline{\sigma_k(\tilde{u})}}) = 0$ for all u and $\Phi_k(E_{\sigma_k(u)} E_{\overline{\sigma_k(\tilde{u})}}) = 0$ for all $u \neq \tilde{u}$.

Then (40) simplifies to

$$\begin{aligned} & \sum_{b_1, \ldots, b_n} f(b_1, \ldots, b_n) \\ + & \sum_{b_1, \ldots, b_{n-1}}^{(v)} f(b_1, \ldots, b_{n-1}, \bar{c}_1) + \cdots \end{aligned} \tag{40}$$

$$+ \sum_{b_1, \ldots, b_{n-k}}^{(v)} f(b_1, \ldots, b_{n-k}, \bar{c}_k, c_{k-1}, \ldots, c_1) \tag{41}$$

$$+ \cdots + f(\bar{c}_n, c_{n-1}, \ldots, c_1). \tag{42}$$

[2]To simplify notation, we have reversed the order of the bit indices of c_k.

$$
\begin{aligned}
&\hat{f}_0 + \sum_{k=1}^{n} \Phi_k\left(\hat{f}_k E_{\tau_k(D^{-1}(j))}\right) \\
&= \sum_{b_1,\ldots,b_n}^{(v)} f(b_1,\ldots,b_n) + \sum_{b_1,\ldots,b_{n-1}}^{(v)} \left\{ f(b_1,\ldots,b_{n-1},\underbrace{0}_{c_1})\Phi_1(E_{\sigma_1(u)=0}E_{\tau_1(D^{-1}(j))}) \right. \\
&\qquad\qquad \left. + f(b_1,\ldots,b_{n-1},\underbrace{1}_{c_1})\Phi_1(E_{\overline{\sigma_1(u)}=1}E_{\tau_1(D^{-1}(j))}) \right\} + \cdots \\
&+ \sum_{b_1,\ldots,b_{n-k}}^{(v)} \sum_{b_{n-k+2},\ldots,b_n}^{(u)} \left\{ f(b_1,\ldots,b_{n-k},\underbrace{0}_{c_k},b_{n-k+2},\ldots,b_n)\Phi_k(E_{\sigma_k(u)}E_{\tau_k(D^{-1}(j))}) \right. \\
&\qquad\qquad \left. + f(b_1,\ldots,b_{n-k},\underbrace{1}_{c_k},b_{n-k+2},\ldots,b_n)\Phi_k(E_{\overline{\sigma_k(u)}}E_{\tau_k(D^{-1}(j))}) \right\} + \cdots \\
&+ \sum_{b_2,\ldots,b_n}^{(u)} \left\{ f(\underbrace{0}_{c_n},b_2,\ldots,b_n)\Phi_n(E_{\sigma_n(u)}E_{\tau_n(D^{-1}(j))}) + f(\underbrace{1}_{c_n},b_2,\ldots,b_n)\Phi_n(E_{\overline{\sigma_n(u)}}E_{\tau_n(D^{-1}(j))}) \right\}.
\end{aligned}
\tag{40}
$$

Adding the first two summations in (40) yields $\sum_{b_1,\ldots,b_{n-1}} f(b_1,\ldots,b_{n-1},c_1)$ due to the characteristic 2 of $\mathcal{R}$ (bitwise XOR addition). Progressively adding the summations up to (41) yields $\sum_{b_1,\ldots,b_{n-k}} f(b_1,\ldots,b_{n-k},c_k,\ldots,c_1)$. Finally adding all summations up to (42) yields $f(c_n,\ldots,c_k,\ldots,c_1) = f_j$. This completes the proof. □

Example 6: Following Example 3, given Fourier coefficients $\hat{f}_0$, $\hat{f}_1$, $\hat{f}_2$ and $\hat{f}_3$ in (33) for a function over $G = C_2^3$, the inverse Fourier transform can be computed as

$$
\begin{aligned}
f_0 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_0) + \Phi_2(\hat{f}_2E_{00}) + \Phi_3(\hat{f}_3E_{000}) \\
f_1 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_1) + \Phi_2(\hat{f}_2E_{01}) + \Phi_3(\hat{f}_3E_{001}) \\
f_2 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_0) + \Phi_2(\hat{f}_2E_{11}) + \Phi_3(\hat{f}_3E_{011}) \\
f_3 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_1) + \Phi_2(\hat{f}_2E_{10}) + \Phi_3(\hat{f}_3E_{010}) \\
f_4 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_0) + \Phi_2(\hat{f}_2E_{00}) + \Phi_3(\hat{f}_3E_{111}) \\
f_5 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_1) + \Phi_2(\hat{f}_2E_{01}) + \Phi_3(\hat{f}_3E_{110}) \\
f_6 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_0) + \Phi_2(\hat{f}_2E_{11}) + \Phi_3(\hat{f}_3E_{100}) \\
f_7 &= \hat{f}_0 + \Phi_1(\hat{f}_1E_1) + \Phi_2(\hat{f}_2E_{10}) + \Phi_3(\hat{f}_3E_{101})
\end{aligned}
$$

□

V. TMFT Properties

Theorem 2: (**Linearity of TMFT**). Given a pair of functions r and $s : G \to \mathcal{R}$, let $\hat{r} = [\hat{r}_0,\ldots,\hat{r}_k,\ldots,\hat{r}_n]$ and $\hat{s} = [\hat{s}_0,\ldots,\hat{s}_k,\ldots,\hat{s}_n]$ be the lists of Fourier coefficients matrices of TMFT (i.e., $\hat{r}_k$ and $\hat{s}_k$ are $2^k \times 2^k$ matrices), the TMFT of the linear combination of r and s is given by

$$
\begin{aligned}
\widehat{\alpha r + \beta s} &= \alpha\hat{r} + \beta\hat{s} \\
&= [\alpha\hat{r}_0 + \beta\hat{s}_0,\ldots,\alpha\hat{r}_k + \beta\hat{s}_k,\ldots,\alpha\hat{r}_n + \beta\hat{s}_n]
\end{aligned}
$$

for $\alpha, \beta \in \mathcal{R}$. □

Proof: The proof is straightforward.

Next, we specialize the definition of convolution in (10) for the case of the additive group $G = C_2^n$.

Definition 8: Given a pair of functions r and $s : G \to \mathcal{R}$ we define the convolution product $f : G \to \mathcal{R}$ as

$$
f(g) = r(g) * s(g) = \sum_{g' \in G} r(g' + g)s(g') \quad \text{for } g \in G.
$$

□

It can be easily shown that the convolution product is commutative. Now we present the convolution theorem when using TMFT.

Theorem 3: (**Convolution Theorem**). Given a pair of functions r and $s : G \to \mathcal{R}$, let $\hat{r} = [\hat{r}_0,\ldots,\hat{r}_k,\ldots,\hat{r}_n]$ and $\hat{s} = [\hat{s}_0,\ldots,\hat{s}_k,\ldots,\hat{s}_n]$ be the lists of Fourier coefficients matrices of TMFT (i.e., $\hat{r}_k$ and $\hat{s}_k$ are $2^k \times 2^k$ matrices), we obtain Fourier transform of the convolution product as

$$
\widehat{r * s} = \hat{r} \odot \hat{s} \triangleq [\hat{r}_0\hat{s}_0,\ldots,\hat{r}_k\hat{s}_k,\ldots,\hat{r}_n\hat{s}_n] \;.
$$

□

Proof: Using Definition 6, we can simply write the product of the k-th Fourier coefficient matrices of r and s as

$$
\hat{r}_k\hat{s}_k = \sum_{g \in G} r(g)E_{\tau_k(g)} \sum_{g' \in G} s(g')E_{\tau_k(g')} \;.
$$

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

$$
\begin{aligned}
\hat{r}_k\hat{s}_k &= \sum_{w \in G}\sum_{g \in G} r(g)s(g+w)E_{\tau_k(g)}E_{\tau_k(g+w)} \\
&= \sum_{w \in G}\sum_{g \in G} r(g)s(g+w)E_{\tau_k(g)}E_{\tau_k(g)+\tau_k(w)} \\
&= \sum_{w \in G}\sum_{g \in G} r(g)s(g+w)E_{\tau_k(w)} \\
&= \sum_{w \in G} (r * s)(w)E_{\tau_k(w)} \;.
\end{aligned}
\tag{43}
$$

The second equality is based on the fact that τ_k is group homomorphism (see Lemma 3). □

Theorem 4: (**Shifting Property**). Given the function $f : G \to \mathcal{R}$ and its TMFT

$$\hat{f}_k = \sum_{g \in G} f(g) E_{\tau_k(g)} \quad k = 1, \ldots, n$$

and a given shift $a \in G$ then the Fourier transform of $f(g+a)$ is given by

$$\sum_{g \in G} f(g+a) E_{\tau_k(g+a)} = \sum_{g \in G} f(g+a) E_{\tau_k(g)} E_{\tau_k(a)} \ . \quad (44)$$

If $f(g+a) = f(g)$ for all $g \in G$, then the above Fourier transform becomes

$$\sum_{g \in G} f(g+a) E_{\tau_k(g+a)} = \hat{f}_k E_{\tau_k(a)} \ . \quad (45)$$

□

Proof: The proof is straightforward.

VI. Implementation and Complexity

The evaluation of the TMFT only requires additions (and no multiplications) in the ring $\mathcal{R}$, since the $E_{\mathbf{b}}$ matrices only contain zeros and ones in $\mathcal{R}$. Hence, we define the *complexity* as the number of additions in the ring $\mathcal{R}$. For convenience of exposition, we will begin by analyzing the complexity of the ITMFT.

A. Complexity of ITMFT

The following lemma enables us to count the number of ring additions needed to compute one term $\Phi_k(\hat{f}_k E_{\tau_k(D^{-1}(j))})$ in (36), for any $k = 0, \ldots, n$ and $j = 0, \ldots, 2^n - 1$. We note that the top right corner of the matrix product is given by the scalar product first row of $\hat{f}_k$ and the last column of $E_{\tau_k(D^{-1}(j))}$.

Lemma 7: Given an n-bit vector $\mathbf{b}$ and the corresponding representation matrix $E_{\mathbf{b}}$, let $\mathbf{v}$ be the first row (or the transposed last column) of the matrix $E_{\mathbf{b}}$ and let $w_H(\mathbf{b})$ and $w_H(\mathbf{v})$ be their Hamming weights, then

$$w_H(\mathbf{v}) = 2^{w_H(\mathbf{b})} \ . \quad (46)$$

□

Proof: We first prove this lemma when $\mathbf{v}$ is the first row of the matrix $E_{\mathbf{b}}$. For $n = 1$, (46) is true by definition of E_0 and E_1. By induction on the number of bits, we assume (46) is true for a k-bit vector $\mathbf{b}^{(k)}$, i.e., $w_H(\mathbf{v}^{(k)}) = 2^{w_H(\mathbf{b}^{(k)})}$, where $\mathbf{v}^{(k)}$ is the first row of $E_{\mathbf{b}^{(k)}}$. When one more bit b_{k+1} is appended to $\mathbf{b}^{(k)}$ the matrix representation becomes

$$E_{\mathbf{b}^{(k+1)}} = E_{\mathbf{b}^{(k)}} \otimes E_{b_{k+1}} \ .$$

From the definition of the Kroneker product and the matrices E_0 and E_1, we have:

$$w_H(\mathbf{v}^{(k+1)}) = \begin{cases} w_H(\mathbf{v}^{(k)}) & \text{if } b_{k+1} = 0 \\ 2 w_H(\mathbf{v}^{(k)}) & \text{if } b_{k+1} = 1 \end{cases}$$

Hence the weight of the first row doubles for every bit that is equal to one in $\mathbf{b}$.

Based on the anti-diagonal symmetry noted in Property 1, under the same assumptions, (46) is also valid when $\mathbf{v}^T$ is the last column of $E_{\mathbf{b}}$. □

Lemma 8: The total complexity of the ITMFT is given by

$$C_{\text{ITMFT}} = \frac{3^{n+1} + 1}{2} + (n-2) 2^n \ . \quad (47)$$

□

Proof: The total complexity of the ITMFT takes into accounts *i)* the number of terms in $\hat{f}_k$ to be added when computing $\Phi_k(\hat{f}_k E_{\tau_k(D^{-1}(j))})$, for $k = 1, \ldots, n$; and *ii)* the number of additions of terms $\Phi_k(\hat{f}_k E_{\tau_k(D^{-1}(j))})$ in (36).

Let $w = w_H(\mathbf{b})$ be the Hamming weight of the k-bit vector $\mathbf{b}$ associated with the matrix $E_{\tau_k(D^{-1}(j))}$. The number of elements of the matrix $\hat{f}_k$ to be added when computing $\Phi_k(\hat{f}_k E_{\tau_k(D^{-1}(j))})$ is determined by the number of ones in the last column of $E_{\tau_k(D^{-1}(j))}$, which is 2^w according to Lemma 7. Then the number of additions is one less, i.e., $2^w - 1$. Since there are only 2^k distinct $E_{\tau_k(D^{-1}(j))}$ for each k, we need to run over all the weights w of the k-bit vector corresponding to the matrix $E_{\tau_k(D^{-1}(j))}$ for $k = 1, \ldots, n$. This results in a complexity of

$$\sum_{k=1}^{n} \sum_{w=0}^{k} \binom{k}{w} (2^w - 1) \ . \quad (48)$$

We simplify (48) to

$$\sum_{k=1}^{n} \left[\sum_{w=0}^{k} \binom{k}{w} 2^w - \sum_{w=0}^{k} \binom{k}{w} \right] = \sum_{k=1}^{n} (3^k - 2^k) \ . \quad (49)$$

On the other hand, the number of additions of terms $\Phi_k(\hat{f}_k E_{\tau_k(D^{-1}(j))})$ in (36) is $n 2^n$. Finally, we obtain the total complexity

$$C_{\text{ITMFT}} = \sum_{k=1}^{n} (3^k - 2^k) + n 2^n = \frac{3^{n+1} + 1}{2} - 2^{n+1} + n 2^n \ . \quad (50)$$

□

B. Complexity of the fast TMFT

From Lemma 4, we note that the Fourier coefficient matrices $\hat{f}_k$ of the fast TMFT are linear combination of the matrices $E_{\mathbf{b}}$, weighted by the scalar values. Following (14) and Property 1, the matrices $E_{\mathbf{b}}$ are the k-fold Kroneker products of the 2×2 upper triangular and anti-diagonal symmetric matrices E_0, E_1. This provides a simple algorithm (see Fig. 4), in which any $\hat{f}_k$ can be entirely reconstructed from its first row entries. Hence, we only need to compute and store the first row of the matrices $\hat{f}_k$, which is a linear combination of the first rows of matrices $E_{\mathbf{b}}$. Then the complexity can be derived by counting the Hamming weights of the first rows of matrices $E_{\mathbf{b}}$. We have the following Lemma.

Lemma 9: The total complexity of the fast TMFT is given by

$$C_{\text{FTMFT}} = \frac{3^{n+1} + 1}{2} - 2^{n+1} \ . \quad (51)$$

□

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory


```
Input: v (first row of \hat{f}_k), k number of bits
for j = 0 : k − 1
    w = zeros(2^j, 2^k);
    for i = 1 : 2^{j+1} : 2^k − 2^j
        w(1 : 2^j, (i + 2^j) : (i + 2^j + 2^j − 1)) = v(1 : 2^j, i : i + 2^j − 1);
    end
    v = [v; w];
end
return v (complete matrix \hat{f})
```

Fig. 4. Algorithm to find the full $\hat{f}_k$ from its first row.

Proof: For each $\hat{f}_k$, $k = 1, \ldots, n$, given k bit vector $\mathbf{b}$ with Hamming weight $w = w_H(\mathbf{b})$, we let $\mathbf{v_b}$ denote the first row vector of a $E_\mathbf{b}$ matrix with Hamming weight $w_H(\mathbf{v_b}) = 2^w$, according to Lemma 7. We prove the complexity of the fast TMFT in the following steps.

1) We start from the leaf nodes at level n in the tree, as shown for example in Fig. 3. The total number of terms to be added is given by the sum of the Hamming weights of all vectors $\mathbf{v_b}$ at level n, i.e.,
$$\sum_{\mathbf{b}} w_H(\mathbf{v_b}) = \sum_{w=0}^{n} \binom{n}{w} 2^w = 3^n \ .$$
The corresponding addition count is given by
$$\mathrm{K}_1 = 3^n - 2^n \tag{52}$$
since we have 2^n separate sums to compute the first row elements. By direct computation, we note that the first term in the first row of $\hat{f}_n$ is $\hat{f}_0 = \sum_{j=0}^{2^n-1} f_j$. This needs to be computed only once and is used throughout the following steps.

2) At level k ($1 \le k < n$) in the tree, we only focus on the first row of each matrix $\hat{f}_k$, except for the first element in this row ($\hat{f}_0 = \sum_{j=0}^{2^n-1} f_j$), which has been already computed at level n. Since the first term in $\mathbf{v_b}$ is always one (see Property 5), for each $\hat{f}_k$, the total number of terms to be added is given by the sum of $w_H(\mathbf{v_b}) - 1$ of all vectors $\mathbf{v_b}$ at level k, i.e.,
$$\sum_{\mathbf{b}} (w_H(\mathbf{v_b}) - 1) = \sum_{w=0}^{k} \binom{k}{w} (2^w - 1) = 3^k - 2^k, \tag{53}$$
for $k = 1, \ldots, n-1$. The last equality is due to (49). The corresponding additions count is given by $(3^k - 2^k) - (2^k - 1)$, since we have $2^k - 1$ separate sums to compute the $2^k - 1$ elements of the first row.
At each level k, there are extra addition operations that are performed to compute the partial sum of the time domain samples, i.e., $\sum_{v \in G/H_k} f(u+v)$ in (31) and $\sum_{v \in G/H_k} f(u+v+d_k)$ in (32). Note that we can ignore the partial sum coefficient of $E_\mathbf{0}$ at level k, since, by excluding the first element of the first row of $E_\mathbf{0}$, the remaining elements are all zeros. Hence, the extra count for such addition is $2^k - 1$. This can be also interpreted using the tree structure in Fig. 3: the number of additions simply coincides with the number of nodes at level k, after excluding node $E_\mathbf{0}$. Then, the complexity at all level k is given by
$$\mathrm{K}_2 = \sum_{k=1}^{n-1} (3^k - 2^k) - (2^k - 1) + (2^k - 1) = \sum_{k=1}^{n-1} (3^k - 2^k) \ . \tag{54}$$

3) At $k = 0$, we have $\hat{f}_0$, already available at level n. Hence, the final complexity is
$$C_{\text{FTMFT}} = \mathrm{K}_1 + \mathrm{K}_2 = \sum_{k=1}^{n} (3^k - 2^k) = \frac{3^{n+1} + 1}{2} - 2^{n+1} \ .$$

□

C. Complexity of TMFT

Lemma 10: The total complexity of TMFT is given by
$$C_{\text{TMFT}} = 3^{n+1} - (n+4)2^n + n + 1 \ . \tag{55}$$

□

Proof: The proof is similar to that of the fast TMFT and can be derived by modifying (53) and (54).

1) At level n, the complexity of TMFT is the same as $\mathrm{K}_1 = 3^n - 2^n$ in (52) of the fast TMFT, since both methods have the same 2^n distinct matrices $E_\mathbf{b}$.

2) At level $k = 1, \ldots, n-1$, (53) becomes
$$\begin{aligned}\sum_{\mathbf{b}} (w_H(\mathbf{v_b}) - 1) &= 2^{n-k} \sum_{w=0}^{k} \binom{k}{w} (2^w - 1) \\ &= 2^{n-k}(3^k - 2^k) \ . \end{aligned} \tag{56}$$
and the corresponding additions count is given by $\sum_{k=1}^{n-1} 2^{n-k}(3^k - 2^k) - (2^k - 1)$, since we have $2^k - 1$ separate sums to compute the $2^k - 1$ elements of the first row.
Note that (56) has an extra 2^{n-k} scaling factor, when compared to (53). As observed in the proof of Lemma 4, $\hat{f}_k$ of TMFT is the linear combination of the 2^n matrices $E_\mathbf{b}$, weighted by the scalar values. Among all the 2^n matrices $E_\mathbf{b}$, there are 2^k distinct ones and 2^{n-k} repetitions of each distinct one, which causes the extra scaling factor in (56).
Note that, for TMFT, there is no partial sum of the time domain samples in (31) and (32), and thus no extra

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

addition count of 2^k+1 in (54). Then, the complexity in (54) becomes

$$\mathrm{K}_2 = \sum_{k=1}^{n-1} 2^{n-k}(3^k - 2^k) - (2^k - 1), \quad k = 1, \ldots, n-1 \; . \tag{57}$$

3) At level 0, as discussed in the fast TMFT, no extra computation complexity is needed, since f_0 is already available at level n. Hence, the final complexity of TMFT is

$$C_{\mathrm{TMFT}} = \mathrm{K}_1 + \mathrm{K}_2 = 3^{n+1} - (n+4)2^n + n + 1 \; .$$

□

Remark 1: Comparing the complexity of TMFT in (55) and the fast TMFT in (51), we obtain the asymptotic ratio of C_{TMFT} over C_{FTMFT} as

$$\lim_{n\to\infty} \frac{C_{\mathrm{TMFT}}}{C_{\mathrm{FTMFT}}} = 2 \tag{58}$$

□

Remark 2: We can now compare the complexity of a convolution in the time domain to the complexity when using the fast TMFT. The convolution in Definition 8 requires $|G|^2 = 4^n$ *multiplications* in the ring $\mathcal{R}$. On the other hand, if we apply the convolution theorem, we need to compute two fast TMFT's and one ITMFT for a total of

$$\frac{3}{2}\left(3^{n+1} - 2^{n+2} + 1\right) + n2^n$$

additions in the ring $\mathcal{R}$. □

VII. Conclusions

In this paper we have defined the two-modular Fourier transform of a binary function $f : G \to \mathcal{R}$ over $G = C_2^n$ with values in a finite commutative ring $\mathcal{R}$ of characteristic 2. This new Fourier transform is based on k-dimensional representations of a sequence of nested subgroups $H_k = C_2^k$ of G. Using the specific group structure of G, we have highlighted the steps that lead to the fast version of the two-modular Fourier transform and its inverse. In particular, this new inverse Fourier transform significantly deviates from the traditional modular inverse Fourier transform, which is only valid for the case where the characteristic of the ring $\mathcal{R}$ does not divide the order of the group G. The major difference is that the trace operator is replaced by a new operator, which extracts the top right corner element of a matrix.

We then provided the TMFT properties including linearity, shifting property and the convolution theorem, which enables to efficiently compute convolutions (multiplications in the group ring $\mathcal{R}[G]$). We also presented the exact complexity of fast TMFT and its inverse.

This Fourier transform may have broad applications to problems, where binary functions need to be reliably computed or in classification of binary functions.

Appendix

A. Basic Definitions of Group Representation and Characters

Definition A.1: An n–dimensional representation of a group G is a group homomorphism from G to the group of $n \times n$ invertible matrices over a field K, i.e.,

$$\rho : G \to GL(n, K)$$

such that

$$\rho(g_1 g_2) = \rho(g_1)\rho(g_2) \qquad \forall g_1, g_2 \in G \; .$$

If the homomorphism is injective, we say the representation is *faithful*. We also define the *kernel* of ρ as $\mathrm{Ker}(\rho) = \{g \in G \; : \; \rho(g) = \mathbf{I}_n\}$. □

Note that this homomorphism transforms the group operation on a pair of elements to matrix multiplication of the corresponding representation matrices. Since matrix multiplication is non-commutative these representations are useful to study non-Abelian groups. When dealing with Abelian groups scalar (one-dimensional) representations are commonly used [8].

Definition A.2: Given two representations of a group G

$$\rho_1 : G \to GL(n, K) \qquad \rho_1(g) = \mathbf{V}_g$$

and

$$\rho_2 : G \to GL(n, K) \qquad \rho_2(g) = \mathbf{W}_g$$

where $g \in G$, we say ρ_1 and ρ_2 are *equivalent*, if there exists an invertible matrix $\mathbf{A}$ such that $\rho_2(g) = \mathbf{A} \cdot \mathbf{V}_g \cdot \mathbf{A}^{-1} = \mathbf{W}_g$, for all $g \in G$. Otherwise, we say ρ_1 and ρ_2 are *inequivalent*. In the scalar case, two representations are equivalent only if they coincide, i.e., $\rho_1(g) = \rho_2(g)$ for all $g \in G$. □

Definition A.3: A finite dimensional complex representation $\rho : G \to GL(n, \mathbb{C})$ is *irreducible* if the only subspace $V \subseteq \mathbb{C}^n$ that is invariant under all the matrix transformations $\rho(g)$, for all $g \in G$, is either $V = \mathbb{C}^n$ or $V = 0$. □

Definition A.4: Given a representation ρ of a group G, the *character* of ρ is the function $\chi_\rho : G \to K$ given by

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)) \qquad \forall g \in G$$

where $\mathrm{Tr}(\cdot)$ is the trace of the matrix. □

Note that a one-dimensional representation coincides with its character and hence it is a group homomorphism. However, in general the character of a matrix representation is not a group homomorphism.

B. Proof of Lemma 3

According to (23), for any $g, w, g+w \in G$, we have

$$\tau_k(g) = \begin{cases} \sigma_k(u_1) & \text{if } \; g = u_1 + v_1 \text{ for some} \\ & u_1 \in H_k/\langle d_k \rangle \text{ and } v_1 \in G/H_k \\ \overline{\sigma_k(u_1)} & \text{if } \; g = u_1 + v_1 + d_k \text{ for some} \\ & u_1 \in H_k/\langle d_k \rangle \text{ and } v_1 \in G/H_k \end{cases} \tag{59}$$

$$\tau_k(w) = \begin{cases} \sigma_k(u_2) & \text{if } \; w = u_2 + v_2 \text{ for some} \\ & u_2 \in H_k/\langle d_k \rangle \text{ and } v_2 \in G/H_k \\ \overline{\sigma_k(u_2)} & \text{if } \; w = u_2 + v_2 + d_k \text{ for some} \\ & u_2 \in H_k/\langle d_k \rangle \text{ and } v_2 \in G/H_k \end{cases} \tag{60}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

$$\tau_k(g+w)=\begin{cases} \sigma_k(u_1+u_2) & \begin{array}{l}\text{if } g+w=(u_1+u_2)+(v_1+v_2)\\ \text{for some}\\ u_1,u_2,(u_1+u_2)\in H_k/\langle d_k\rangle\\ \text{and } v_1,v_2,v_1+v_2\in G/H_k\end{array}\\ \overline{\sigma_k(u_1+u_2)} & \begin{array}{l}\text{if } g+w=(u_1+u_2)\\ \qquad\qquad +(v_1+v_2)+d_k\\ \text{for some}\\ u_1,u_2,(u_1+u_2)\in H_k/\langle d_k\rangle\\ \text{and } v_1,v_2,v_1+v_2\in G/H_k\end{array}\end{cases} \quad (61)$$

There are four combinations of g and w that we will analyze to prove it is a group homomorphism.

1) When $g=u_1+v_1$ and $w=u_2+v_2$ for some $u_1,u_2\in H_k/\langle d_k\rangle$ and $v_1,v_2\in G/H_k$, we have $g+w=(u_1+u_2)+(v_1+v_2)$, for some $u_1,u_2,(u_1+u_2)\in H_k/\langle d_k\rangle$ and $v_1,v_2,v_1+v_2\in G/H_k$. From (61), we have

$$\tau_k(g+w)=\sigma_k(u_1+u_2)\ . \quad (62)$$

On the other hand, based on (59), (60) and Lemma 2, we have

$$\tau_k(g)+\tau_k(w)=\sigma_k(u_1)+\sigma_k(u_2)=\sigma_k(u_1+u_2) \quad (63)$$

Comparing (62) and (63), we have $\tau_k(g+w)=\tau_k(g)+\tau_k(w)$.

2) When $g=u_1+v_1+d_k$, and $w=u_2+v_2+d_k$ for some $u_1,u_2\in H_k/\langle d_k\rangle$ and $v_1,v_2\in G/H_k$, we have $g+w=(u_1+u_2)+(v_1+v_2)$ for some $u_1,u_2,(u_1+u_2)\in H_k/\langle d_k\rangle$ and $v_1,v_2,v_1+v_2\in G/H_k$. From (61) and Lemma 2, we have

$$\tau_k(g+w)=\sigma_k(u_1+u_2)=\sigma_k(u_1)+\sigma_k(u_2) \quad (64)$$

and

$$\begin{aligned}\tau_k(g)+\tau_k(w) &= \overline{\sigma_k(u_1)}+\overline{\sigma_k(u_2)}\\ &= \mathbf{1}_k+\sigma_k(u_1)+\mathbf{1}_k+\sigma_k(u_2)\\ &= \sigma_k(u_1)+\sigma_k(u_2) \quad (65)\end{aligned}$$

Comparing (64) and (65), we have $\tau_k(g+w)=\tau_k(g)+\tau_k(w)$.

3) When $g=u_1+v_1$ and $w=u_2+v_2+d_k$ for some $u_1,u_2\in H_k/\langle d_k\rangle$ and $v_1,v_2\in G/H_k$, we have $g+w=(u_1+u_2)+(v_1+v_2)+d_k$, for some $u_1,u_2,(u_1+u_2)\in H_k/\langle d_k\rangle$ and $v_1,v_2,v_1+v_2\in G/H_k$. We have

$$\begin{aligned}\tau_k(g+w) &= \overline{\sigma_k(u_1+u_2)}\\ &= \mathbf{1}_k+\sigma_k(u_1+u_2)\\ &= \mathbf{1}_k+\sigma_k(u_1)+\sigma_k(u_2) \quad (66)\end{aligned}$$

and

$$\begin{aligned}\tau_k(g)+\tau_k(w) &= \sigma_k(u_1)+\overline{\sigma_k(u_2)}\\ &= \mathbf{1}_k+\sigma_k(u_1)+\sigma_k(u_2)\ . \quad (67)\end{aligned}$$

Comparing (66) and (67), we have $\tau_k(g+w)=\tau_k(g)+\tau_k(w)$.

4) When $g=u_1+v_1+d_k$ and $w=u_2+v_2$, for some $u_1,u_2\in H_k/\langle d_k\rangle$ and $v_1,v_2\in G/H_k$, we have $g+w=(u_1+u_2)+(v_1+v_2)+d_k$, for some $u_1,u_2,(u_1+u_2)\in H_k/\langle d_k\rangle$ and $v_1,v_2,v_1+v_2\in G/H_k$. We obtain the same result as the previous case by swapping g and w.

This proves τ_k to be group homomorphism. According to the fundamental homomorphism theorem, we have Ker$(\tau_k)=G/H_k$. □

ACKNOWLEDGEMENT

We thank Dr Lakshmi Natarajan for fruitful discussions and the anonymous reviewers for their valuable comments.

REFERENCES

[1] A.V. Oppenheim and R.W. Schafer, *Discrete-Time Signal Processing*, 3rd Edition, Prentice-Hall, Signal Processing Series, 2010.

[2] R.E. Blahut, "A Universal Reed-Solomon Decoder," *IBM J. Research & Development*, Vol. 28, No. 2, pp. 150–158, Mar. 1984.

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

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

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

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

[7] Krister hlander and Hans Munthe-Kaas, "Applications of the Generalized Fourier Transform in Numerical Linear Algebra" *BIT Numerical Mathematics* Dec. 2005, vol. 45, n. 4, pp. 819–850

[8] V.P. Snaith, *Groups, Rings and Galois Theory (Second Edition)* World Scientific Publishing Co. Pte. Ltd., 2003, ISBN 981-238-576-2.

[9] R.S. Stankovic, C. Moraga, and Jaakko T. Astola, *Readings in Fourier Analysis on Finite Non-Abelian Groups,* TICSP Series #5, September 1999, ISBN 952-15-0284-3.

[10] D.S. Passman, *The algebraic structure of group rings* New York: John Wiley & Sons, 1977, ISBN: 0471022721.

[11] Claude Carlet, "Vectorial Boolean Functions for Cryptography", Book Chapter in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* ed. by Yves Crama and Peter L. Hammer, Cambridge University Press, pp. 398-472, 2010.

[12] J. M. Pollard, "The Fast Fourier Transform in a Finite Field", *Mathematics of Computation*, vol. 25, no. 114, pp. 365-374, 1971.

Yi Hong (M'00–SM'10) is currently a Senior Lecturer at the Department of Electrical and Computer Systems Eng., at Monash University, Clayton, Australia. She received her Ph.D. degree in Electrical Engineering and Telecommunications from the University of New South Wales (UNSW), Sydney, Australia. She then worked at the Institute of Telecom. Research, University of South Australia, Australia; at the Institute of Advanced Telecom., Swansea University, UK; and at University of Calabria, Italy. During her PhD, she received an International Postgraduate Research Scholarship (IPRS) from the Commonwealth of Australia and a supplementary Engineering Award from the School of Electrical Engineering and Telecommunications, UNSW. She received the NICTA-ACoRN Earlier Career Researcher award for a paper presented at the Australian Communication Theory Workshop (AUSCTW), Adelaide, Australia, 2007. Dr. Hong is an Associate Editor for IEEE Wireless Communications Letters and European Transactions on Telecommunications, and an IEEE Senior member. She was the General Co-Chair of 2014 IEEE Information Theory Workshop, Hobart, Tasmania; and the Technical Program Committee Chair of 2011 Australian Communications Theory Workshop, Melbourne, Australia. She was the Publicity Chair at the 2015 International Conference on Telecommunications, Sydney, and the 2009 IEEE Information Theory Workshop, Sicily, Italy. She is a Technical Program Committee member for many IEEE conferences such as IEEE ICC, VTC, PIMRC and WCNC. Her research interests include communication theory, coding and information theory with applications to telecommunication engineering.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2016.2545678, IEEE Transactions on Information Theory

Emanuele Viterbo (M'95–SM'04–F'11) was born in Torino, Italy, in 1966. He received his degree (Laurea) in Electrical Engineering in 1989 and his Ph.D. in 1995 in Electrical Engineering, both from the Politecnico di Torino, Torino, Italy. From 1990 to 1992 he was with the European Patent Office, The Hague, The Netherlands, as a patent examiner in the field of dynamic recording and error-control coding. Between 1995 and 1997 he held a postdoctoral position and later became Assistant professor, then Associate Professor, in the Dipartimento di Elettronica of the Politecnico di Torino. In 2006 he was appointed Full Professor in DEIS at Università della Calabria, Italy, in 2006. Since 2010, he is a Full Professor at Department of Electrical and Computer Systems Engineering, Monash University, and the Associate Dean Graduate Research of the Faculty of Engineering at Monash. In 1993 he was visiting researcher in the Communications Department of DLR, Oberpfaffenhofen, Germany. In 1994 and 1995 he was visiting the E.N.S.T., Paris. In 1998 he was visiting researcher in the *Information Sciences Research Center, AT&T Research,* Florham Park, NJ. In 2003 he was visiting researcher at the Maths Department of EPFL, Lausanne, Switzerland. In 2004 he was visiting researcher at the Telecommunications Department of UNICAMP, Campinas, Brazil. In 2005 he was visiting researcher at the ITR of UniSA, Adelaide, Australia. Dr. Emanuele Viterbo was awarded a NATO Advanced Fellowship in 1997 from the Italian National Research Council. His main research interests are in lattice codes for the Gaussian and fading channels, algebraic coding theory, algebraic space-time coding, digital terrestrial television broadcasting, and digital magnetic recording. He was Associate Editor of *IEEE Transactions on Information Theory, European Transactions on Telecommunications* and *Journal of Communications and Networks;* and is now an Editor of *Foundations and Trends in Communications and Information Theory.*

Jean-Claude Belfiore (M'91) received the "Diplôme d'ingénieur" (Eng. degree) from Ecole Supérieure d'Electricité (Supelec) in 1985, the "Doctorat" (PhD) from ENST in 1989 and the "Habilitation à diriger des Recherches" (HdR) from Université Pierre et Marie Curie (UPMC) in 2001. In 1989, he was enrolled at the "Ecole Nationale Supérieure des Télécommunications", ENST, also called "Télécom ParisTech", where he is presently full Professor in the Communications and Electronics department. He is carrying out research at the Laboratoire de Traitement et Communication de l'Information, LTCI, joint research laboratories between ENST and the "Centre National de la Recherche Scientifique" (CNRS), UMR 5141, where he is in charge of research activities in the areas of digital communications, information theory and coding. Jean-Claude Belfiore has made pioneering contributions on modulation and coding for wireless systems (especially space-time coding) by using tools of number theory. He is also, with Ghaya Rekaya and Emanuele Viterbo, one of the co-inventors of the celebrated Golden Code. He is now working on wireless network coding, coding for physical security and coding for interference channels. He is author or co-author of more than 200 technical papers and communications and he has served as advisor for more than 30 Ph.D. students. Prof. Belfiore has been the recipient of the 2007 Blondel Medal. He was an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY FOR CODING THEORY.