Consta-Abelian Codes Over Galois Rings

Kiran. T and B. Sundar Rajan, *Senior Member, IEEE*

Abstract—We study n -length consta-Abelian codes (a generalization of the well-known Abelian codes and constacyclic codes) over Galois rings of characteristic p^a , where n and p are coprime. A twisted discrete Fourier transform (DFT) is used to generalize transform domain results of Abelian and constacyclic codes, to consta-Abelian codes. Further, we characterize consta-Abelian codes invariant under two kinds of monomials, whose underlying permutations are effected by: i) multiplying the coordinates with a unit in the appropriate mixed-radix representation of the coordinate positions and ii) shifting the coordinates by t positions. All the codes studied here belong to the class of quasi-twisted codes which are known to contain some good codes. We show that the dual of a consta-Abelian code invariant under the two monomials is also a consta-Abelian code closed under both monomials.

Index Terms—Abelian codes, consta-Abelian codes, constacyclic codes, Galois rings, quasi-twisted (QT) codes, twisted discrete Fourier transform.

I. INTRODUCTION AND PRELIMINARIES

The class of cyclic codes and its generalizations have been extensively studied, of which the following are the most important.

- *Abelian codes*: These are ideals in the group algebra $F_q[G]$, where G is an Abelian group of order n , with cyclic codes obtained as a special case (when G is cyclic).
- *Quasi-cyclic codes*: A code is t -quasi-cyclic if for every codeword $(c_0, c_1, \dots, c_{n-1})$, the cyclically shifted vector by t positions, $(c_{n-t}, \dots, c_{n-1}, c_0, \dots, c_{n-t-1})$ is also a codeword (cyclic if $t = 1$).
- *Constacyclic codes*: A code is β -constacyclic if for every codeword $(c_0, c_1, \dots, c_{n-1})$, the constacyclically shifted vector by one position, $(\beta c_{n-1}, c_0, \dots, c_{n-2})$ is also a codeword, where β is an element of $F_q^* = F_q \setminus \{0\}$ (cyclic if $\beta = 1$). These are the ideals in the ring $F_q[x]/\langle x^n - \beta \rangle$.

The motivation for studying each of these classes of generalizations is that better codes than cyclic codes in the sense of larger minimum distance have been found in these generalizations. The class of quasi-cyclic codes [1], [2] have been shown to contain asymptotically good codes [2]. They provide link between block codes and convolutional codes [3] and recently it has been shown that quasi-cyclic codes have close relationship with the tail-biting representations of general block codes [4]. Constacyclic codes over finite fields F_{p^l} (also known as pseudocyclic code) have been extensively studied [5]–[8]. The class of constacyclic codes includes as subclasses the important class of cyclic codes and the class of negacyclic codes. It was shown in [5] that constacyclic maximum-distance separable (MDS) codes exist for certain

Fig. 1. Generalizations of cyclic code.

parameters for which cyclic MDS codes do not exist. An attraction with constacyclic codes is that, these codes can be studied using the well-known “theory of cyclic codes.” Also, these codes can be decoded with slight modifications of efficient decoding algorithms for cyclic codes. Thus, constacyclic codes can be an alternative to cyclic codes for certain parameters.

Fig. 1 illustrates the various generalizations discussed above. Since a finite Abelian group G is a direct product of cyclic groups, we can view Abelian codes as multidimensional cyclic codes. This generalization of cyclic to Abelian codes can be carried over to constacyclic codes to give multidimensional constacyclic codes. Similarly, the generalization from cyclic to quasi-cyclic codes can be carried over to constacyclic codes to yield quasi-twisted (QT) codes [9]–[11], i.e., a code is (β, t) -QT if for every codeword $(c_0, \dots, c_{n-1})$, $(\beta c_{n-t}, \beta c_{n-t+1}, \dots, \beta c_{n-1}, c_0, \dots, c_{n-t-1})$ is also a codeword. Some QT codes with better parameters than any known codes were listed in [9] and [10].

In this correspondence, we investigate multidimensional constacyclic codes (henceforth referred to as consta-Abelian codes) using a twisted DFT and characterize codes that are invariant under two additional scaled permutations (called monomials in [2]).

For a prime p , Galois rings are residue class polynomial rings $Z_{p^a}[x]/\phi(x)$, where $Z_{p^a}[x]$ is the ring of polynomials over Z_{p^a} and $\phi(x)$ is a basic irreducible polynomial of degree l over $Z_{p^a}[x]$ [12]. This Galois ring denoted by $\text{GR}(p^a, l)$, coincides with the finite field F_{p^l} when $a = 1$ and the integer residue class ring Z_{p^a} when $l = 1$. Recently, various aspects of coding and cryptography have been dealt with in the general setting of Galois rings instead of finite fields. In view of this, in this correspondence, the codes we discuss are over Galois rings $\text{GR}(p^a, l)$.

Permutation groups of cyclic codes over Galois rings have been investigated in [13]. In [14], we used a transform approach to study Abelian codes over Galois rings closed under certain permutations. The results of this correspondence are generalizations of the results for Abelian codes discussed in [14]. Different decoding algorithms for codes over Galois rings have been studied [15]–[17]. In certain cases, the consta-Abelian codes belong to the class of Alternant codes and hence the algorithm discussed in [16] could be used for decoding such codes.

Manuscript received July 13, 2002; revised October 12, 2003. This work was supported in part by CSIR, India, under Research Grant 22(0298)/99/EMR-II to B. S. Rajan. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Yokohama, Japan, June/July 2003.

The authors are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore-560012, India (e-mail: kirant@protocol.ece.iisc.ernet.in; bsrajan@ece.iisc.ernet.in).

Communicated by C. Carlet, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.822619

Definition 1: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be codes of length n over $\text{GR}(p^a, l)$. We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if there are n permutations $\pi^{(0)}, \pi^{(1)}, \dots, \pi^{(n-1)}$ of $\text{GR}(p^a, l)$ and a permutation τ of $I_n = \{0, 1, \dots, n-1\}$ such that, if

$$\vec{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}_1$$

then

$$\pi\tau(\vec{c}) = (\pi^{(0)}(c_{\tau(0)}), \pi^{(1)}(c_{\tau(1)}), \dots, \pi^{(n-1)}(c_{\tau(n-1)})) \in \mathcal{C}_2.$$

When all $\pi^{(i)}$'s are identity permutations, we say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are *permutation equivalent* and when each $\pi^{(i)}$ is a multiplication by a nonzero scalar, $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *scalar multiple equivalent* or *monomial equivalent*. A code $\mathcal{C}$ is said to be $\pi\tau$ -invariant if $\pi\tau(\vec{c}) \in \mathcal{C}$ for all $\vec{c} \in \mathcal{C}$.

Monomially equivalent codes have the same weight enumerator, in particular they have the same minimum distance.

Example 1: A β -constacyclic code over $\text{GR}(p^a, l)$ is $\pi\tau$ -invariant where τ is a permutation of I_n which takes i to $(i+1)$ modulo n and π is such that

$$\pi(\vec{c}) = (\pi^{(0)}(c_0), \pi^{(1)}(c_1), \dots, \pi^{(n-1)}(c_{n-1}))$$

where $\pi^{(0)}(c_0) = \beta c_0$ and $\pi^{(\lambda)}(c_\lambda) = c_\lambda$ for $\lambda = 1, \dots, n-1$.

To generalize the class of constacyclic codes to consta-Abelian codes, we use the following notations. Let $m_0, m_1, \dots, m_{r-1}$ be nonzero positive integers and let $n = m_0 m_1 \cdots m_{r-2} m_{r-1}$. Using m_λ 's, $0 \leq \lambda \leq r-1$ as mixed radixes, any integer $i \in I_n$ can be uniquely expressed as

$$i = i_0 + i_1 m_0 + \cdots + i_{r-2} (m_0 m_1 \cdots m_{r-3}) + i_{r-1} (m_0 m_1 \cdots m_{r-2})$$

where $0 \leq i_\lambda < m_\lambda$. The mixed-radix representation of i is denoted by $i = [i] = [i_{r-1}, i_{r-2}, \dots, i_0]$ and the mixed-radix addition and subtraction, denoted by $\oplus$ and $\ominus$, respectively, are defined by

$$\begin{aligned} i \oplus j &= [a_{r-1}, a_{r-2}, \dots, a_0] \\ a_\lambda &= (i_\lambda + j_\lambda) \bmod m_\lambda, \quad \forall \lambda \end{aligned}$$

and

$$\begin{aligned} i \ominus j &= [a_{r-1}, a_{r-2}, \dots, a_0] \\ a_\lambda &= (i_\lambda - j_\lambda) \bmod m_\lambda, \quad \forall \lambda. \end{aligned}$$

Let G , a finite Abelian group (with $|G| = n$), be a direct product of r cyclic subgroups denoted by $C_{r-1}, \dots, C_0$ of orders $m_{r-1}, \dots, m_0$, respectively. If $g_{(m_{r-1})}, \dots, g_{(m_0)}$ are the generators of the corresponding cyclic subgroups, then any element $g \in G$ can be written as

$$g = g_{(m_{r-1})}^{i_{r-1}} g_{(m_{r-2})}^{i_{r-2}} \cdots g_{(m_0)}^{i_0}$$

for some $i_{r-1}, \dots, i_0$ where

$$0 \leq i_\lambda < m_\lambda \quad \text{for } \lambda = 0, 1, \dots, r-1.$$

This element is denoted by g_i or $g_{[i]}$, where

$$[i] = [i_{r-1}, i_{r-2}, \dots, i_0]$$

is the mixed-radix representation of $i \in I_n$ using $m_{r-1}, m_{r-2}, \dots, m_0$ as the mixed radixes. The group operation of G can thus be specified using mixed-radix indexing as $g_i g_j = g_{i \oplus j}$, where $i, j \in I_n$ and $i \oplus j$ and $i \ominus j$ are the mixed-radix addition and subtraction, respectively. Let e be the exponent of G and p be a prime such that $(e, p) = 1$ and, henceforth, let $n_\lambda = \prod_{i=0}^{\lambda-1} m_i$ for all $\lambda = 1, 2, \dots, r-1$; $n_0 = 1$ by convention and let $q = p^l$.

A group ring $\text{GR}(p^a, l)[G]$ is the set of all formal sums of the form $\sum_{g_i \in G} a_i g_i$, where $a_i \in \text{GR}(p^a, l)$, with the usual "polynomial

addition" and "polynomial multiplication." By associating a vector $\vec{a} = (a_0, a_1, \dots, a_{n-1}) \in \text{GR}(p^a, l)^n$ with the element of the group ring $\sum_{g_i \in G} a_i g_i$, an *Abelian code* corresponds to an ideal of a group ring $\text{GR}(p^a, l)[G]$. For every codeword $(c_0, c_1, \dots, c_{n-1})$ in the Abelian code, $(c_{0 \oplus j}, c_{1 \oplus j}, \dots, c_{(n-1) \oplus j})$ also belongs to the code for all values of $j = 0, 1, \dots, n-1$.

As in [18], we define the twisted group ring $\text{GR}(p^a, l)^\psi[G]$ by taking the $\text{GR}(p^a, l)$ -module $\text{GR}(p^a, l)[G]$ and imposing the following **twisted-multiplication** on each of the generators $g_{(m_\lambda)}$ of the cyclic subgroup C_λ , given by

$$g_{(m_\lambda)}^i \cdot g_{(m_\lambda)}^j = \psi_\lambda(g_{(m_\lambda)}^i, g_{(m_\lambda)}^j) g_{(m_\lambda)}^{i+j} = \beta_\lambda^k g_{(m_\lambda)}^t$$

where β_λ for all λ is an element of the unique cyclic subgroup $A \subset \text{GR}(p^a, l)^*$, $|A| = p^l - 1$, and ψ_λ is a map from $C_\lambda \times C_\lambda$ to A , which maps $(g_{(m_\lambda)}^i, g_{(m_\lambda)}^j)$ to β_λ^k , where k is such that $i + j = m_\lambda k + t$, $0 \leq t < m_\lambda$. Let $\vec{\beta} = (\beta_{r-1}, \beta_{r-2}, \dots, \beta_0)$ be the set of all β_λ 's used in defining the twisted-multiplication.

A $\vec{\beta}$ -**consta-Abelian code** is an ideal in the twisted group ring $\text{GR}(p^a, l)^\psi[G]$, with the twisted-multiplication defined by $\vec{\beta} = (\beta_{r-1}, \beta_{r-2}, \dots, \beta_0)$. For every codeword $\vec{c} = (c_0, c_1, \dots, c_{n-1})$ in the $\vec{\beta}$ -consta-Abelian code (corresponding to $\sum_{g_i \in G} c_i g_i$ in the corresponding ideal of $\text{GR}(p^a, l)^\psi[G]$), the element

$$\pi\tau(\vec{c}) = (\pi^{(0)}(c_{0 \oplus j}), \pi^{(1)}(c_{1 \oplus j}), \dots, \pi^{(n-1)}(c_{(n-1) \oplus j}))$$

(corresponding to twisted-multiplication of $\sum_{g_i \in G} c_i g_i$ by $g_j = g_{(m_{r-1})}^{j_{r-1}} g_{(m_{r-2})}^{j_{r-2}} \cdots g_{(m_0)}^{j_0}$) also belongs to the code for all values of $j = 0, 1, \dots, n-1$, where

$$\pi^{(i)}(c_{i \oplus j}) = \left(\prod_{\lambda=0}^{r-1} \beta_\lambda^{k_\lambda} \right) c_{i \oplus j} \quad (1)$$

and k_λ is such that

$$i_\lambda + j_\lambda = m_\lambda k_\lambda + (i_\lambda \oplus j_\lambda), \quad \text{for all } \lambda = 0, 1, \dots, r-1.$$

It is important to notice that the permutations $\pi^{(i)}$ are induced because of the permutation τ and the twisted multiplication defined in $\text{GR}(p^a, l)^\psi[G]$. In fact, $\pi^{(i)}$ used in (1) can be different for different values of j . Since we are concerned with codes which are ideals in the twisted group ring, for any other permutation on I_n also, there are a set of permutations on $\text{GR}(p^a, l)$ uniquely associated with it. Therefore, henceforth we denote the monomial $\pi\tau$ as π_τ , and the action of this monomial is denoted, as

$$\pi_\tau(\vec{a}) = (\pi_\tau^{(0)}(a_{\tau(0)}), \dots, \pi_\tau^{(n-1)}(a_{\tau(n-1)})).$$

In particular, the monomial associated with the permutation $i \mapsto i \oplus j$ in (1) is denoted as $\pi_{\oplus j}$ and the monomial for $i \mapsto i \ominus j$ as $\pi_{\ominus j}$.

In this correspondence, we are interested in the following two permutations on I_n .

Definition 2: For $n_0 = 1$ or some $n_s = \prod_{\lambda=0}^{s-1} m_\lambda$, let $Q_s : I_n \rightarrow I_n$, $i \mapsto (i + n_s)$ modulo n and let π_{Q_s} denote the associated monomial. If $\vec{a} = (a_0, a_1, \dots, a_{n-1}) \in \text{GR}(p^a, l)^n$, using the one to one mapping from $\text{GR}(p^a, l)^n$ to the twisted-group ring $\text{GR}(p^a, l)^\psi[G]$

$$\begin{aligned} & \sum_{i=0}^{n-1} \pi_{Q_s}^{(i)}(a_{(i-n_s)}) g_{(m_{r-1})}^{i_{r-1}} g_{(m_{r-2})}^{i_{r-2}} \cdots g_{(m_{s+1})}^{i_{s+1}} g_{(m_s)}^{i_s} \cdots g_{(m_0)}^{i_0} \\ &= \sum_{i=0}^{n-1} a_i g_{(m_{r-1})}^{i_{r-1} + \delta_{r-1}^{(s)}} \cdots g_{(m_{s+1})}^{i_{s+1} + \delta_{s+1}^{(s)}} g_{(m_s)}^{i_s + 1} \cdots g_{(m_0)}^{i_0} \\ &= \pi_{Q_s}(\vec{a}) \end{aligned}$$

where $\delta_\lambda^{(s)}$ appears as a "carry value" added to i_λ in the mixed-radix representation of $[i + n_s]$

$$[i + n_s] = [(i_{r-1} + \delta_{r-1}^{(s)})_{m_{r-1}}, \dots, (i_\lambda + \delta_\lambda^{(s)})_{m_\lambda}, \dots, (i_{s+1} + \delta_{s+1}^{(s)})_{m_{s+1}}, (i_s + 1)_{m_s}, i_{s-1}, \dots, i_0] \quad (2)$$

 Fig. 2. π_{U_b} -invariant, π_{Q_s} -invariant consta-Abelian codes.

(where $(x)_m$ denotes x modulo m), and $\pi_{Q_s}^{(i)}(a_{n-n_s+i})$ induced by the twisted-multiplication is given by

$$\begin{aligned} \pi_{Q_s}^{(i)}(a_{n-n_s+i}) &= \prod_{\lambda=1}^{r-1} \psi_{\lambda} \left(g_{(m_{\lambda})}^{i_{\lambda}}, g_{(m_{\lambda})}^{\delta_{\lambda}^{(s)}} \right) a_{n-n_s+i} \\ &= \left(\prod_{\lambda=1}^{r-1} \beta_{\lambda}^{k_{\lambda}} \right) a_{n-n_s+i} \end{aligned}$$

where k_{λ} is such that $i_{\lambda} + \delta_{\lambda}^{(s)} = m_{\lambda}k_{\lambda} + t_{\lambda}$, $0 \leq t_{\lambda} < m_{\lambda}$ for all $\lambda = 0, 1, \dots, r-1$,

Example 2: For $n = 2 \times 2 \times 3$ length codes over $Z_{25} = \{0, 1, \dots, 24\}$ and $\bar{\beta} = (24, 18, 24)$, the monomials defined above for different values of s are given by

$$\begin{aligned} \pi_{Q_2}(\vec{c}) &= (24c_6, 24c_7, 24c_8, 24c_9, 24c_{10}, 24c_{11}, c_0, c_1, \dots, c_5) \\ \pi_{Q_1}(\vec{c}) &= (7c_9, 7c_{10}, 7c_{11}, c_0, c_1, c_2, 18c_3, 18c_4, 18c_5, c_6, c_7, c_8) \\ \pi_{Q_0}(\vec{c}) &= (18c_{11}, c_0, c_1, 24c_2, c_3, c_4, 7c_5, c_6, c_7, 24c_8, c_9, c_{10}) \end{aligned}$$

where $\vec{c} = (c_0, c_1, c_2, \dots, c_{10}, c_{11}) \in Z_{25}^{12}$.

Definition 3: Let $b = [b_{r-1}, b_{r-2}, \dots, b_0]$ be such that $\gcd(b_{\lambda}, m_{\lambda}) = 1$ for all $\lambda = 0, 1, \dots, r-1$. Let $U_b: I_n \rightarrow I_n$ be a map, defined by

$$\begin{aligned} [i] &= [i_{r-1}, i_{r-2}, \dots, i_0] \\ &\rightarrow [(b_{r-1}i_{r-1})_{m_{r-1}}, (b_{r-2}i_{r-2})_{m_{r-2}}, \dots, (b_0i_0)_{m_0}] \end{aligned}$$

where $(x)_m$ denotes x modulo m . We call this permutation the Unit_b permutation. (Notice that every mixed-radix component of b is a unit

in the integer ring modulo the respective mixed radix.). The associated monomial is denoted as π_{U_b} , and the action of $\pi_{U_b}^{(i)}$ is scalar multiplication by

$$\prod_{\lambda=0}^{r-1} (\beta_{\lambda}^{k_{\lambda}}) \text{ where } k_{\lambda} \text{ satisfies } b_{\lambda}i_{\lambda} = m_{\lambda}k_{\lambda} + t_{\lambda}, \quad 0 \leq t_{\lambda} < m_{\lambda}.$$

Example 3: For $n = 2 \times 2 \times 3$ length codes over Z_{25} , $\bar{\beta} = (24, 18, 24)$ and $b = [1, 1, 5]$, the monomial defined above is given by

$$\begin{aligned} \pi_{U_b}(\vec{c}) &= (c_0, 24c_2, 24c_1, c_3, 24c_5, \\ &\quad 24c_4, c_6, 24c_8, 24c_7, c_9, 24c_{11}, 24c_{10}) \end{aligned}$$

for $\vec{c} = (c_0, c_1, c_2, \dots, c_{10}, c_{11}) \in Z_{25}^{12}$.

In this correspondence, we study $\bar{\beta}$ -consta-Abelian codes which are also invariant under the monomials π_{Q_s} and π_{U_b} . These codes are called π_{Q_s} -invariant $\bar{\beta}$ -consta-Abelian codes and π_{U_b} -invariant $\bar{\beta}$ -consta-Abelian codes, respectively. The classes of codes studied in this correspondence are best explained with Fig. 2, where, the class of $\bar{\beta}$ -consta-Abelian codes of length $n = m_{r-1}m_{r-2} \cdots m_1m_0$ is depicted by the ellipse in the figure. We show that, in the class of linear codes over $\text{GR}(p^a, l)$ of length $n = m_{r-1}m_{r-2} \cdots m_1m_0$, a π_{Q_s} -invariant code is also $\pi_{Q_{\lambda}}$ -invariant for every $s \leq \lambda \leq r-1$. We also show that every $\bar{\beta}$ -consta-Abelian code of length $n = m_{r-1}m_{r-2} \cdots m_1m_0$ is (β_{r-1}, n_{r-1}) -QT. Hence, the ellipse has not gone outside the concentric circles. The circle (shown in bold) represents n -length π_{U_b} -invariant linear codes (not necessarily $\bar{\beta}$ -consta-Abelian). The

horizontally hatched regions represent π_{Q_s} -invariant $\bar{\beta}$ -consta-Abelian codes for some value of s and double-hatched regions represent π_{U_b} -invariant and π_{Q_s} -invariant $\bar{\beta}$ -consta-Abelian codes.

The main result of this correspondence consists of: i) characterizing π_{Q_s} -invariant and π_{U_b} -invariant $\bar{\beta}$ -consta-Abelian codes over Galois rings and ii) finding the smallest value of such s and all values of b for every $\bar{\beta}$ -consta-Abelian code. We obtain these results using the DFT approach. DFT domain characterization of cyclic, Abelian, and quasi-cyclic codes over finite fields and rings Z_m have been previously discussed in the literature [19]–[22] and a similar technique has been used to characterize constacyclic codes in [23]. In this correspondence, we generalize the results of [23] for consta-Abelian codes over Galois rings and, then, characterize π_{Q_s} -invariant $\bar{\beta}$ -consta-Abelian codes and π_{U_b} -invariant $\bar{\beta}$ -consta-Abelian codes over Galois rings in the DFT domain defined over suitable Galois ring extensions. As a consequence, we characterize $\bar{\beta}$ -consta-Abelian codes that are both π_{Q_s} -invariant and π_{U_b} -invariant. Duals of these codes are shown to be invariant under both monomials π_{Q_s} and π_{U_b} .

If $\mathcal{C}$ is an arbitrary (β_{r-1}, n_{r-1}) -QT code of length $n = m_{r-1}m_{r-2} \cdots m_0$ over $\text{GR}(p^a, l)$, then the extension ring required for transform domain description of this code is $\text{GR}(p^a, lm)$ which should contain an n th root of unity as well as an n th root of β_{r-1} (in other words, m is the smallest integer such that both n and order $(\beta_{r-1}) \times n$ divide $p^{lm} - 1$). But, if this code $\mathcal{C}$ is $\bar{\beta}$ -consta-Abelian also (see Fig. 2), then an extension ring containing m_λ th roots of unity and m_λ th roots of β_λ for all $\lambda = 0, 1, \dots, r-1$ is enough, which is generally smaller than $\text{GR}(p^a, lm)$. Since algebraic decoding generally takes place in the extension ring, a smaller extension ring may lead to a simpler or more efficient decoding of code $\mathcal{C}$.

Throughout this correspondence, the length of the code is relatively prime to p , where p^a is the characteristic of the Galois ring $\text{GR}(p^a, l)$ over which the code is defined.

The remainder of this correspondence is organized as follows. In Section II, we define a twisted DFT and characterize consta-Abelian codes using this transform. Consta-Abelian codes invariant under π_{Q_s} and π_{U_b} are then characterized in Sections III and IV, respectively. Examples are given to illustrate each class of code. In Section V, we discuss duals of consta-Abelian codes and obtain nonexistence result for certain self-dual codes. Finally, the conclusions of this correspondence are presented in Section VI.

II. TWISTED-DFT CHARACTERIZATION OF CONSTA-ABELIAN CODES

For a $\bar{\beta}$ -consta-Abelian code over $\text{GR}(p^a, l)$, $\bar{\beta} = (\beta_{r-1}, \beta_{r-2}, \dots, \beta_0)$ is an r -tuple where each β_λ is an element of the cyclic subgroup of order $p^l - 1$ in $\text{GR}(p^a, l)$. Let d_λ be the order of element β_λ and let m be the smallest positive integer such that $m_\lambda d_\lambda \mid (q^m - 1)$ for all $\lambda = 0, 1, \dots, r-1$. Let α_λ be a primitive root of unity of order m_λ and γ_λ be an m_λ th root of β_λ , for all λ , belonging to the extension ring $\text{GR}(p^a, lm)$. Let $\text{GR}(p^a, lm)[G]$ be a group ring with “componentwise addition” (polynomial addition), i.e.,

$$\sum_{g_i \in G} a_i g_i + \sum_{g_i \in G} b_i g_i = \sum_{g_i \in G} (a_i + b_i) g_i$$

and “componentwise multiplication”

$$\left(\sum_{g_i \in G} a_i g_i \right) \cdot \left(\sum_{g_i \in G} b_i g_i \right) = \sum_{g_i \in G} (a_i b_i) g_i$$

and let $\text{GR}(p^a, l)^\psi[G]$ be the twisted group ring defined earlier (polynomial addition and polynomial multiplication). We now define a group ring homomorphism from $\text{GR}(p^a, l)^\psi[G]$ into $\text{GR}(p^a, lm)[G]$, and use this to characterize consta-Abelian codes over $\text{GR}(p^a, l)$.

A. Twisted DFT (TDFT)

Definition 4: Let $\vec{a} = (a_0, a_1, \dots, a_{n-1}) \in \text{GR}(p^a, l)^n$. Let α_λ and γ_λ for $\lambda = 0, 1, \dots, r-1$, be as defined earlier. The TDFT vector $\vec{A} = (A_0, A_1, \dots, A_{n-1}) \in \text{GR}(p^a, lm)^n$ of $\vec{a}$ is defined as

$$A_j = \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i_\lambda} \alpha_\lambda^{i_\lambda j_\lambda} \right) a_i, \quad \text{for all } j \in I_n \quad (3)$$

where $i = [i_{r-1}, i_{r-2}, \dots, i_0]$ and $j = [j_{r-1}, j_{r-2}, \dots, j_0]$ are mixed-radix representations of i and j . Let ζ_λ be a primitive $m_\lambda d_\lambda$ th root of unity in the cyclic group of order $p^{lm} - 1$ in $\text{GR}(p^a, lm)$ and $\gamma_\lambda = \zeta_\lambda^{h_\lambda}$, $\alpha_\lambda = \zeta_\lambda^{d_\lambda}$ for all $\lambda = 0, 1, \dots, r-1$. Then the above TDFT can be expressed as

$$A_j = \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \zeta_\lambda^{i_\lambda (h_\lambda + d_\lambda j_\lambda)} \right) a_i, \quad \text{for all } j \in I_n. \quad (4)$$

Henceforth, we refer to any $\vec{a} \in \text{GR}(p^a, l)^n$ as “time domain vector” and the corresponding $\vec{A} \in \text{GR}(p^a, lm)^n$ as TDFT vector of $\vec{a}$. Notice that, if $\beta_\lambda = 1$ for all λ , then the ideals correspond to $n = m_{r-1}m_{r-2} \cdots m_0$ length Abelian codes over $\text{GR}(p^a, l)$ and the TDFT reduces to the generalized DFT defined in [14]. The TDFT satisfies the following properties:

$$a_i = n^{-1} \prod_{\lambda=0}^{r-1} \gamma_\lambda^{-i_\lambda} \left\{ \sum_{j=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \alpha_\lambda^{-i_\lambda j_\lambda} \right) A_j \right\} \quad (5)$$

$$c_i = \sum_{k=0}^{n-1} \pi_{\ominus k}^{(i)} (a_{i \ominus k}) b_k \xleftrightarrow{\text{tdft}} A_j B_j \quad (6)$$

where $\xleftrightarrow{\text{tdft}}$ denotes a TDFT pair. In (6), the left-hand side is the twisted convolution, which corresponds to the “polynomial multiplication” of two elements in $\text{GR}(p^a, l)^\psi[G]$. This maps to the componentwise multiplication of the corresponding TDFT vectors in the group ring $\text{GR}(p^a, lm)[G]$.

Let σ_0 be the Frobenius automorphism of $\text{GR}(p^a, lm)$ [12]. Using p -adic representation, an element $\gamma \in \text{GR}(p^a, lm)$ can be represented as $\gamma_0 + \gamma_1 p + \cdots + \gamma_{a-1} p^{a-1}$ where γ_i are elements from the Teichmüller set $T = \text{GR}(p^a, lm)/p \text{GR}(p^a, lm)$ (isomorphic to the field $F_{p^{lm}}$). Then $\sigma_0(\gamma)$ is equal to $\gamma_0^p + \gamma_1^p p + \cdots + \gamma_{a-1}^p p^{a-1}$. Alternately, if polynomial representation is used for elements of Galois ring, then each element of the set T is a polynomial in x . Therefore, σ_0 can be uniquely defined by defining its action on x . Let $\sigma = \sigma_0^l$, then σ is an automorphism of $\text{GR}(p^a, lm)$ that fixes $\text{GR}(p^a, l) \subseteq \text{GR}(p^a, lm)$.

Lemma 1: (Conjugate symmetry property) If

$$\vec{A} = (A_0, A_1, \dots, A_{n-1}) \in \text{GR}(p^a, lm)^n$$

is the TDFT vector of $(a_0, a_1, \dots, a_{n-1}) \in \text{GR}(p^a, l)^n$, then the following relation among $A_j, j \in I_n$, holds:

$$\sigma^k(A_j) = A_i \quad (7)$$

where $i = [i_{r-1}, i_{r-2}, \dots, i_0]$ with

$$i_\lambda = \left(\frac{(q^k - 1)h_\lambda}{d_\lambda} + q^k j_\lambda \right) \text{ modulo } m_\lambda$$

for all $\lambda = 0, 1, \dots, r-1$.

Let ϕ_λ^k denote a mapping from I_{m_λ} to I_{m_λ} which maps j_λ to

$$\left(\frac{(q^k - 1)h_\lambda}{d_\lambda} + q^k j_\lambda \right).$$

Let Φ^k denote the mapping from I_n to I_n , which maps $i = [i_{r-1}, i_{r-2}, \dots, i_0]$ to

$$\Phi^k(i) = [\phi_{r-1}^k(i_{r-1}), \phi_{r-2}^k(i_{r-2}), \dots, \phi_0^k(i_0)].$$

TABLE I
TDFT PARAMETERS FOR $n = 2 \times 2 \times 2$ AND $\bar{\beta} = (1, 1, 4)$

$\lambda \downarrow$	m_λ	α_λ	β_λ	d_λ	γ_λ	ζ_λ	h_λ
2	2	4	1	1	1	4	0
1	2	4	1	1	1	4	0
0	2	4	4	2	2	2	1

Definition 5: For every $j \in I_n$, the set

$$\widehat{[j]} = \{j, \Phi^1(j), \Phi^2(j), \dots, \Phi^{e_j-1}(j)\}$$

where e_j is the smallest integer such that $\Phi^{e_j}(j) = j$, is called the **cyclotomic coset modulo n** containing $[j]$ and e_j is called the exponent of $[j]$. Clearly, I_n is a disjoint union of such cyclotomic cosets. Let $\mathbf{L} \subseteq I_n$ be the set containing one element from each of the cyclotomic cosets. We call the set $\mathbf{L}$ the cyclotomic representative set. (For concreteness, we use the smallest element of a cyclotomic coset as a representative.)

Example 4:

i) Table I lists the TDFT parameters for $n = 2 \times 2 \times 2$ length $(1, 1, 4)$ -consta-Abelian codes over F_5 . The cyclotomic cosets each consist of a single element and hence the corresponding representative set $\mathbf{L} = I_8$.

ii) For $n = 2 \times 2 \times 3$ length $(24, 18, 24)$ -consta-Abelian codes over Z_{25} , the smallest extension required for the TDFT description is the Galois ring

$$\text{GR}(5^2, 2) = Z_{25}[x]/(x^2 + x + 2) = \{c + dx \mid c, d \in Z_{25}\}.$$

The Frobenius automorphism σ_0 is given by $\sigma_0(x) = 24 + 24x$. Z_{25} is the only nontrivial Galois subring of $\text{GR}(5^2, 2)$. It can be checked that all the elements of Z_{25} are invariant under the Frobenius automorphism. The only nontrivial ideal of Z_{25} is $5Z_{25}$ which is equal to $\{0, 5, 10, 15, 20\}$ and the only nontrivial ideal of $\text{GR}(5^2, 2)$ is

$$5 \text{GR}(5^2, 2) = \{c + dx \mid c, d \in 5Z_{25}\}.$$

The group of units

$$\text{GR}(5^2, 2)^* = \text{GR}(5^2, 2) \setminus 5 \text{GR}(5^2, 2).$$

The cyclic subgroup of order $p^{lm} - 1 = 24$, $G_1 \subset \text{GR}(5^2, 2)^*$ with elements listed in the increasing order of powers of generator element $6 + x$ is

$$\begin{aligned} G_1 = \{ & 6 + x, 9 + 11x, 7 + 14x, 14 + 2x, 5 + 24x, \\ & 7, 17 + 7x, 13 + 2x, 24 + 23x, 23 + 14x, \\ & 10 + 18x, 24, 19 + 24x, 16 + 14x, \\ & 18 + 11x, 11 + 23x, 20 + x, 18, 8 + 18x, \\ & 12 + 23x, 1 + 2x, 2 + 11x, 15 + 7x, 1 \}. \end{aligned}$$

Table II(a) lists the TDFT parameters, Table II(b) lists the cyclotomic cosets, and Table II(c) is the corresponding representative set $\mathbf{L}$.

The constraint due to the conjugate symmetry property given by (7) implies that: i) the set of transform components $\{A_{[j]} \mid [j] \in \widehat{[i]}\}$ denoted by $\widehat{A}_{[i]}$ are related (in other words, transform components indexed by elements of the same cyclotomic coset are related) and moreover ii) every element of $\widehat{A}_{[i]}$ belongs to the same Galois ring

$$\text{GR}(p^a, le_i) \subseteq \text{GR}(p^a, lm)$$

for some fixed e_i dividing m . The set $\widehat{A}_{[i]}$ will be called the **conjugacy class** containing $A_{[i]}$. For a code $\mathcal{C}$ over $\text{GR}(p^a, l)$, let $\mathbf{C}_j = \{A_j \mid \forall \vec{a} \in \mathcal{C}\}$ denote the set of distinct values taken by the j th transform component of all the codewords in $\mathcal{C}$ and let

$$\mathbf{C}_{i,j} = \{(A_i, A_j) \mid \forall \vec{a} \in \mathcal{C}\}.$$

Then, a $\bar{\beta}$ -consta-Abelian code $\mathcal{C}$ over $\text{GR}(p^a, l)$ is isomorphic to an ideal $\bigoplus_{i \in \mathbf{L}} \mathbf{C}_i$, where $\mathbf{C}_i = p^{\eta_i} \text{GR}(p^a, le_i)$ for some fixed value of η_i , $0 \leq \eta_i \leq a$ and transform components belonging to different

conjugacy classes take values *independently*. Here, A_i and A_j take values independently implies $\mathbf{C}_{i,j} = \mathbf{C}_i \times \mathbf{C}_j$.

In the remainder of this correspondence, we refer to the ideal $p^{\eta_i} \text{GR}(p^a, le_i)$ as the η_i -ideal of $\text{GR}(p^a, le_i)$. Also, for a $\bar{\beta}$ -consta-Abelian code, since $\widehat{A}_{[i]}$ can take values only from the ideals of Galois subring $\text{GR}(p^a, le_i)$, we will say $A_{[i]}$ takes values from the η_i -ideal to mean that $\mathbf{C}_i = p^{\eta_i} \text{GR}(p^a, le_i)$, since it is obvious which ring is meant. Hence, a $\bar{\beta}$ -consta-Abelian code is specified/characterized by specifying $\eta_{i_1}, \eta_{i_2}, \dots, \eta_{i_{|\mathbf{L}|}}$ corresponding to each element in $\mathbf{L} = \{[i_1], [i_2], \dots, [i_{|\mathbf{L}|}]\}$. In other words, a $\bar{\beta}$ -consta-Abelian code over $\text{GR}(p^a, l)$ can be characterized by a partition of I_n as given in the following Definition 6.

Definition 6: The **defining partition** of a $\bar{\beta}$ -consta-Abelian code is the partition $(T_0, T_1, \dots, T_a)$ of I_n , where

$$T_\eta = \{j \in I_n \mid \mathbf{C}_j = p^\eta \text{GR}(p^a, le_j)\}, \quad \text{for } 0 \leq \eta \leq a.$$

For a $\bar{\beta}$ -consta-Abelian code, every T_η is a union of some cyclotomic cosets or $T_\eta = \emptyset$ if $\mathbf{C}_j \neq p^\eta \text{GR}(p^a, le_j)$ for any $j \in I_n$. This partition uniquely specifies the $\bar{\beta}$ -consta-Abelian code.

Example 5:

- Some $(1, 1, 4)$ -consta-Abelian codes of length $n = 2 \times 2 \times 2$ over F_5 are listed in Table III. In the TDFT description of all codes, only the transform components A_j for which $\mathbf{C}_j \neq 0$ are listed. The corresponding TDFT parameters and cyclotomic cosets are given in the previous example.
- Table IV lists some $n = 2 \times 2 \times 3$ length $(24, 18, 24)$ -consta-Abelian codes over Z_{25} . The corresponding TDFT parameters and cyclotomic cosets are given in the previous example.
- $(24, 18, 24)$ -consta-Abelian codes over $\text{GR}(5^2, 2)$ of length $n = 2 \times 2 \times 3$ are listed in Table V. In these tables, an element $a + bx$ of the Galois ring $\text{GR}(5^2, 2)$ is listed as a 2-tuple adjacent to each other. For this case, the extension ring required is the Galois ring $\text{GR}(5^2, 2)$ (see Example 4, part ii)) over which the code is defined and hence all cyclotomic cosets contain single elements.

B. Constraints on $\mathbf{L}$

The main result of this correspondence is to identify the constraints on the values taken by transform components belonging to different conjugacy classes for the $\bar{\beta}$ -consta-Abelian code to be

- π_{U_b} -invariant for some particular values of

$$b = [b_{r-1}, b_{r-2}, \dots, b_0]$$

such that $\gcd(b_\lambda, m_\lambda) = 1$ for all $\lambda = 0, 1, \dots, r-1$ and

- π_{Q_s} -invariant for any s , $0 \leq s \leq r-1$.

Given the transform domain description of a $\bar{\beta}$ -consta-Abelian code, this result enables us to give the smallest value of s for which the code is π_{Q_s} -invariant and also all the values of b for which the code is π_{U_b} -invariant. Toward this end, we define a constraint in terms of a partition on $\mathbf{L}$ and $\bar{\beta}$ -consta-Abelian codes satisfying this constraint as follows.

Definition 7: A **constraint** $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_u\}$ is a partition of the set of cyclotomic coset representatives

$$\mathbf{L} = \{[i_1], [i_2], \dots, [i_{|\mathbf{L}|}]\}.$$

A $\bar{\beta}$ -consta-Abelian code over $\text{GR}(p^a, l)$ is said to satisfy the constraint $\mathcal{D}$ if $[i_c], [i_d] \in \mathcal{D}_j$ for some $j \in \{1, 2, \dots, u\}$ implies $\eta_{i_c} = \eta_{i_d}$, where $\mathbf{C}_{i_c} = p^{\eta_{i_c}} \text{GR}(p^a, le_{i_c})$ and $\mathbf{C}_{i_d} = p^{\eta_{i_d}} \text{GR}(p^a, le_{i_d})$. If a set $\mathcal{D}_j$ contains only one cyclotomic coset representative, we call the corresponding cyclotomic coset a **free cyclotomic coset**. Otherwise, $\mathcal{D}_j$ is called a **constrained set of cyclotomic coset representatives** and all the corresponding cyclotomic cosets of $\mathcal{D}_j$ are said to form a constrained set.

TABLE II
TDFT PARAMETERS FOR $n = 2 \times 2 \times 3$ AND $\bar{\beta} = (24, 18, 24)$

$\lambda \downarrow$	m_λ	α_λ	β_λ	d_λ	γ_λ	ζ_λ	h_λ
2	2	24	24	2	7	7	1
1	2	24	18	4	$24 + 23x$	$7 + 14x$	3
0	3	$13 + 2x$	24	2	$14 + 2x$	$14 + 2x$	1

(a) TDFT parameters.

$\widehat{[0]}$	$\widehat{[1]}$	$\widehat{[2]}$	$\widehat{[6]}$	$\widehat{[7]}$	$\widehat{[8]}$
$\begin{bmatrix} 000 \\ 012 \end{bmatrix}$	$\begin{bmatrix} 001 \\ 011 \end{bmatrix}$	$\begin{bmatrix} 002 \\ 010 \end{bmatrix}$	$\begin{bmatrix} 100 \\ 112 \end{bmatrix}$	$\begin{bmatrix} 101 \\ 111 \end{bmatrix}$	$\begin{bmatrix} 102 \\ 110 \end{bmatrix}$

(b) Cyclotomic cosets.

$\mathbf{L} \rightarrow$	$\begin{bmatrix} 000 \\ 100 \end{bmatrix}$	$\begin{bmatrix} 001 \\ 101 \end{bmatrix}$	$\begin{bmatrix} 002 \\ 102 \end{bmatrix}$	$\begin{bmatrix} 100 \\ 110 \end{bmatrix}$	$\begin{bmatrix} 101 \\ 111 \end{bmatrix}$	$\begin{bmatrix} 102 \\ 112 \end{bmatrix}$
--------------------------	--	--	--	--	--	--

(c) Cyclotomic coset representative set $\mathbf{L}$.

TABLE III
 $n = 2 \times 2 \times 2$ LENGTH $(1, 1, 4)$ -CONSTA-ABELIAN CODES OVER F_5

Time Domain	TDFT	Time Domain	TDFT	Time Domain	TDFT	Time Domain	TDFT
CODE $C_0, T_0 = \{0\}$	A_0	CODE $C_1, T_0 = \{1\}$	A_1	CODE $C_2, T_0 = \{2\}$	A_2	CODE $C_3, T_0 = \{3\}$	A_3
0 0 0 0 0 0 0 0	0	0 0 0 0 0 0 0 0	0	0 0 0 0 0 0 0 0	0	0 0 0 0 0 0 0 0	0
2 1 2 1 2 1 2 1	1	2 4 2 4 2 4 2 4	1	2 1 3 4 2 1 3 4	1	2 4 3 1 2 4 3 1	1
4 2 4 2 4 2 4 2	2	4 3 4 3 4 3 4 3	2	4 2 1 3 4 2 1 3	2	4 3 1 2 4 3 1 2	2
1 3 1 3 1 3 1 3	3	1 2 1 2 1 2 1 2	3	1 3 4 2 1 3 4 2	3	1 2 4 3 1 2 4 3	3
3 4 3 4 3 4 3 4	4	3 1 3 1 3 1 3 1	4	3 4 2 1 3 4 2 1	4	3 1 2 4 3 1 2 4	4
CODE $C_4, T_0 = \{4\}$	A_4	CODE $C_5, T_0 = \{5\}$	A_5	CODE $C_6, T_0 = \{6\}$	A_6	CODE $C_7, T_0 = \{7\}$	A_7
0 0 0 0 0 0 0 0	0	0 0 0 0 0 0 0 0	0	0 0 0 0 0 0 0 0	0	0 0 0 0 0 0 0 0	0
2 1 2 1 3 4 3 4	1	2 4 2 4 3 1 3 1	1	2 1 3 4 3 4 2 1	1	2 4 3 1 3 1 2 4	1
4 2 4 2 1 3 1 3	2	4 3 4 3 1 2 1 2	2	4 2 1 3 1 3 4 2	2	4 3 1 2 1 2 4 3	2
1 3 1 3 4 2 4 2	3	1 2 1 2 4 3 4 3	3	1 3 4 2 4 2 1 3	3	1 2 4 3 4 3 1 2	3
3 4 3 4 2 1 2 1	4	3 1 3 1 2 4 2 4	4	3 4 2 1 2 1 3 4	4	3 1 2 4 2 4 3 1	4
CODE C_8				CODE C_9			
Time Domain	TDFT	Time Domain	TDFT	Time Domain	TDFT	Time Domain	TDFT
$T_0 = \{0, 2\}$	A_2, A_3	$T_0 = \{0, 2\}$	A_2, A_3	$T_0 = \{1, 3\}$	A_4, A_6	$T_0 = \{1, 3\}$	A_4, A_6
0 0 0 0 0 0 0 0	0 0	0 4 0 1 0 4 0 1	2 3	0 0 0 0 0 0 0 0	0 0	0 0 2 1 0 0 3 4	2 3
2 4 3 1 2 4 3 1	0 1	2 3 3 2 2 3 3 2	2 4	2 1 2 1 3 4 3 4	0 1	2 1 4 2 3 4 1 3	2 4
4 3 1 2 4 3 1 2	0 2	1 3 4 2 1 3 4 2	3 0	4 2 4 2 1 3 1 3	0 2	1 3 4 2 4 2 1 3	3 0
1 2 4 3 1 2 4 3	0 3	3 2 2 3 3 2 2 3	3 1	1 3 1 3 4 2 4 2	0 3	3 4 1 3 2 1 4 2	3 1
3 1 2 4 3 1 2 4	0 4	0 1 0 4 0 1 0 4	3 2	3 4 3 4 2 1 2 1	0 4	0 0 3 4 0 0 2 1	3 2
2 1 3 4 2 1 3 4	1 0	2 0 3 0 2 0 3 0	3 3	2 1 3 4 3 4 2 1	1 0	2 1 0 0 3 4 0 0	3 3
4 0 1 0 4 0 1 0	1 1	4 4 1 1 4 4 1 1	3 4	4 2 0 0 1 3 0 0	1 1	4 2 2 1 1 3 3 4	3 4
1 4 4 1 1 4 4 1	1 2	3 4 2 1 3 4 2 1	4 0	1 3 2 1 4 2 3 4	1 2	3 4 2 1 2 1 3 4	4 0
3 2 2 3 3 2 2 3	1 3	0 3 0 2 0 3 0 2	4 1	3 4 4 2 2 1 1 3	1 3	0 0 4 2 0 0 1 3	4 1
0 2 0 3 0 2 0 3	1 4	2 2 3 3 2 2 3 3	4 2	0 0 1 3 0 0 4 2	1 4	2 1 1 3 3 4 4 2	4 2
4 2 1 3 4 2 1 3	2 0	4 1 1 4 4 1 1 4	4 3	4 2 1 3 1 3 4 2	2 0	4 2 3 4 1 3 2 1	4 3
1 1 4 4 1 1 4 4	2 1	1 0 4 0 1 0 4 0	4 4	1 3 3 4 4 2 2 1	2 1	1 3 0 0 4 2 0 0	4 4
3 0 2 0 3 0 2 0	2 2			3 4 0 0 2 1 0 0	2 2		

From Definition 6, if $(T_0, T_1, \dots, T_a)$ is the defining partition of a $\bar{\beta}$ -consta-Abelian code $\mathcal{C}$, then, $\mathcal{C}$ satisfies the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_u\}$ if and only if every set T_η is either empty or a union of some constrained sets $\mathcal{D}_j$.

Remark 1: We had earlier introduced the notion of transform components belonging to different conjugacy classes taking values *independently* for a $\bar{\beta}$ -consta-Abelian code. The above definition implies that if a $\bar{\beta}$ -consta-Abelian code satisfies constraint $\mathcal{D}$, and if i_1 and i_2 from two different cyclotomic cosets belong to the same set $\mathcal{D}_j$, then $\eta_{i_1} = \eta_{i_2} = \eta_j$ but $\mathcal{C}_{i_1, i_2} = \mathcal{C}_{i_1} \times \mathcal{C}_{i_2}$ continues to be true. If i_1 and i_2 belong to different sets in $\mathcal{D}$, then η_{i_1}, η_{i_2} can be different and $\mathcal{C}_{i_1, i_2} = \mathcal{C}_{i_1} \times \mathcal{C}_{i_2}$.

III. π_{Q_s} -INVARIANT CODES

For the ideals in the twisted group ring $\text{GR}(p^a, l)^\psi[G]$, corresponding to the permutation Q_s , we have a monomial π_{Q_s} induced by the twisted-multiplication defined earlier. In this section, we characterize all $\bar{\beta}$ -consta-Abelian codes which are invariant under the monomial π_{Q_s} .

Proposition 1: A π_{Q_s} -invariant linear code $\mathcal{C}$ (over $\text{GR}(p^a, l)$) is $\pi_{Q_{s+1}}$ -invariant as well.

Proof: Let $(\pi_{Q_s})^t$ denote the composition of π_{Q_s} with itself, t times. Since $\mathcal{C}$ is π_{Q_s} -invariant, $(\pi_{Q_s})^t(\vec{a}) \in \mathcal{C}$ for any $\vec{a} \in \mathcal{C}$. For $t = m_s$

$$(\pi_{Q_s})^{m_s}(\vec{a}) = \pi_{Q_{s+1}}(\beta_s \vec{a}) = \beta_s(\pi_{Q_{s+1}}(\vec{a})) \in \mathcal{C}$$

where $\beta_s \vec{a} = (\beta_s a_0, \beta_s a_1, \dots, \beta_s a_{n-1})$. Since the code $\mathcal{C}$ is $\text{GR}(p^a, l)$ -linear, $\beta_s^{-1}(\pi_{Q_s})^{m_s}(\vec{a}) \in \mathcal{C}$. $\square$

For the special case when $\beta_k = 1$, for all $0 \leq k \leq r-1$, the π_{Q_s} -invariant $\bar{\beta}$ -consta-Abelian codes are exactly the n_s -QCA codes discussed in [14].

Theorem 1: All $n = m_{r-1}m_{r-2} \cdots m_0$ length $\bar{\beta}$ -consta-Abelian codes are $\pi_{Q_{r-1}}$ -invariant.

Proof: Let $\mathcal{C}$ be a $\bar{\beta}$ -consta-Abelian code over $\text{GR}(p^a, l)$. For any

$$\vec{a} = \sum_{i=0}^{n-1} a_i g_i \in \mathcal{C}$$

the codeword

$$\begin{aligned} g_{(m_{r-1})} \sum_{i=0}^{n-1} a_i g_i &= \sum_{i=0}^{n-1} \pi_{Q_{r-1}}^{(i)}(a_{i \oplus [m_{r-1}-1, 0, 0, \dots, 0]}) g_i \\ &= \pi_{Q_{r-1}}(\vec{a}) \in \mathcal{C}. \end{aligned} \quad \square$$

Notice that the action of the monomial $\pi_{Q_{r-1}}$ is

$\pi_{Q_{r-1}}(\vec{a}) = (\beta_{r-1} a_{n-n_{r-1}}, \dots, \beta_{r-1} a_{n-1}, a_0, a_1, \dots, a_{n-n_{r-1}-1})$ which is essentially β_{r-1} -constacyclic shifts by n_{r-1} positions. Hence, all $\bar{\beta}$ -consta-Abelian codes are (β_{r-1}, n_{r-1}) -QT as indicated in Fig. 2.

In the next few theorems, we will use the following notations.

For $\bar{\beta} = (\beta_{r-1}, \beta_{r-2}, \dots, \beta_0)$, let κ be the smallest integer ($0 \leq \kappa < r$) such that $\beta_{r-1} = \beta_{r-2} = \dots = \beta_{\kappa+1} = 1$ and $\beta_\kappa \neq 1$. By convention, $\kappa = -1$, if $\bar{\beta} = (1, 1, \dots, 1)$.

Definition 8: For every $j \in I_n$ such that

$$[j] = [0, 0, \dots, 0, j_\mu \neq 0, j_{\mu-1}, \dots, j_0]$$

TABLE IV
 $n = 2 \times 2 \times 3$ LENGTH $\bar{\beta}$ -CONSTA-ABELIAN CODES OVER Z_{25} FOR $\bar{\beta} = (24, 18, 24)$

Time Domain										TDFT		Time Domain										TDFT			
CODE C_0 $T_0 = \emptyset; T_1 = \{0, 5\};$										A_0	A_5	CODE C_1 $T_0 = \emptyset; T_1 = \{1, 4\};$										A_1	A_4		
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	15	10	0	5	5	15	20	5	0	15	10	15	0	0	0	15	10	15	0	0	0	5	0	5	0
10	5	20	0	10	10	5	15	10	0	5	10	10	15	0	0	0	5	20	5	0	0	0	10	0	10
15	20	5	0	15	15	20	10	15	0	20	15	15	10	15	0	0	20	5	20	0	0	0	15	0	15
20	10	15	0	20	20	10	5	20	0	10	20	20	5	20	0	0	10	15	10	0	0	0	20	0	20
10	10	0	10	15	5	5	5	0	5	20	15	0	5	20	5	5	20	5	5	20	5	0	5	20	20
15	0	10	10	20	10	20	0	5	5	10	5	5	0	20	15	10	15	10	20	5	5	5	0	20	5
20	15	20	10	0	15	10	20	10	5	0	20	10	5	0	20	10	15	10	15	10	5	10	5	20	5
0	5	5	10	5	20	0	15	15	5	15	10	15	0	0	10	15	10	0	0	5	20	5	15	5	10
5	20	15	10	0	15	10	20	5	5	0	20	5	15	20	5	10	15	10	15	10	15	5	20	5	20
20	20	0	20	5	10	10	0	10	15	5	0	10	15	15	0	15	10	15	10	15	10	0	10	15	15
0	10	10	20	10	15	0	5	5	10	5	20	5	10	20	15	0	0	0	10	15	10	5	10	20	15
5	0	20	20	15	20	15	0	10	10	20	10	10	10	0	15	10	15	10	15	10	10	10	0	15	10
10	15	5	20	20	0	5	20	15	10	10	0	15	10	15	10	20	5	20	5	10	15	10	15	10	5
15	5	15	20	0	5	20	15	20	10	0	15	20	10	15	10	20	5	20	20	5	10	15	10	15	10
5	5	0	5	20	15	15	15	0	15	10	20	0	15	10	20	5	15	10	15	10	15	0	15	10	10
10	20	10	5	0	20	5	10	5	15	0	10	15	10	15	0	5	20	5	15	10	15	10	15	10	10
15	10	20	5	5	0	20	5	10	15	15	15	10	15	10	15	5	20	5	20	15	10	15	10	15	10
20	0	5	5	10	5	10	0	15	15	5	15	15	10	15	5	20	5	10	15	10	15	10	15	10	10
0	15	15	5	15	10	0	20	20	15	20	5	0	0	0	5	20	5	0	0	15	10	15	20	15	10
15	15	0	15	10	20	20	0	20	5	10	0	20	5	10	0	15	10	15	10	15	10	0	20	5	5
20	5	10	15	15	0	10	15	5	20	20	0	5	20	15	10	15	10	15	10	15	10	5	20	10	15
0	20	20	15	20	5	0	10	10	20	10	15	10	15	10	15	10	0	20	5	20	10	15	10	15	10
5	10	5	15	0	10	15	5	15	20	0	5	15	10	15	10	15	10	15	10	15	10	15	20	20	5
10	0	15	15	5	15	5	0	20	20	15	20	10	15	10	15	10	15	10	15	10	15	10	15	10	5
CODE C_2 $T_0 = \emptyset; T_1 = \{2, 3\};$										A_2	A_3	CODE C_3 $T_0 = \emptyset; T_1 = \{6, 11\};$										A_6	A_{11}		
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	15	10	0	20	20	15	20	5	0	10	10	10	5	15	10	0	5	10	5	20	0	10	10	5	0
10	5	20	0	15	15	5	15	10	0	20	20	10	10	5	20	0	10	20	10	15	0	20	20	10	0
15	20	5	0	10	10	20	10	15	0	5	5	15	10	15	0	15	15	5	15	10	0	5	15	0	15
20	10	15	0	5	5	10	5	20	0	10	15	15	10	15	0	20	15	20	5	0	15	15	20	0	0
10	0	15	10	20	10	5	0	20	5	10	15	0	5	0	5	20	20	0	20	5	10	0	5	20	20
15	15	0	10	15	5	20	20	0	5	20	10	15	10	15	0	15	10	10	20	15	10	5	10	0	5
20	5	10	10	10	0	10	15	5	5	5	0	10	5	5	0	10	15	5	15	10	0	5	10	5	20
0	20	20	10	5	20	0	10	10	5	15	10	15	10	15	0	10	10	10	15	10	15	15	10	15	10
5	10	5	10	0	15	15	5	15	5	0	20	5	15	10	15	0	10	15	5	15	10	20	0	15	15
20	0	5	20	15	20	10	0	15	10	15	10	15	10	15	0	10	15	15	0	15	10	20	0	15	15
0	15	15	20	10	15	0	20	20	10	15	0	5	20	15	10	15	0	20	20	15	10	15	10	15	10
5	5	0	20	5	10	15	15	0	10	15	5	10	15	10	15	0	15	15	5	15	10	15	10	15	10
10	10	20	0	5	5	10	5	10	5	10	0	15	10	15	10	0	15	15	10	15	10	15	10	15	10
15	10	20	20	20	0	20	5	10	10	10	0	20	10	15	10	0	15	15	10	15	10	15	10	15	10
5	0	20	5	10	5	15	0	15	0	15	5	15	10	15	10	0	15	15	10	15	10	15	10	15	10
10	15	5	5	5	0	5	20	15	15	15	0	10	15	10	15	0	15	15	10	15	10	15	10	15	10
15	5	15	5	0	20	20	15	20	15	10	10	10	15	10	15	0	15	15	10	15	10	15	10	15	10
20	20	0	5	20	15	10	0	15	10	15	10	15	10	15	10	0	15	15	10	15	10	15	10	15	10
0	10	10	5	15	10	0	5	15	15	20	5	15	10	15	10	0	15	15	10	15	10	15	10	15	10
15	0	10	15	5	15	20	0	5	15	10	15	10	15	10	15	0	15	15	10	15	10	15	10	15	10
20	15	10	15	5	10	10	20	10	20	10	15	10	15	10	15	0	15	15	10	15	10	15	10	15	10
0	5	5	15	20	5	0	15	15	20	10	15	10	15	10	15	0	15	15	10	15	10	15	10	15	10
5	20	15	15	15	0	15	10	20	20	0	15	10	15	10	15	0	15	15	10	15	10	15	10	15	10
10	5	10	0	15	10	20	5	5	0	20	5	10	15	10	15	0	15	15	10	15	10	15	10	15	10
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CODE C_4 $T_0 = \emptyset; T_1 = \{7, 10\};$										A_7	A_{10}	CODE C_5 $T_0 = \emptyset; T_1 = \{8, 9\};$										A_8	A_9		
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	20	5	0	0	0	0	10	15	10	0	0	0	0	5	15	10	0	20	10	5	20	0	15	15	5
10	15	10	0	0	0	20	5	20	0	0	0	0	0	10	5	20	0	15	15	20	10	15	0	5	5
15	10	15	0	0	0	5	20	5	0	0	0	0	0	15	0	10	5	15	10	5	10	0	20	15	0
20	5	20	0	0	0	15	10	15	0	0	0	0	0	20	0	10	15	5	15	20	5	0	10	10	20
10	15	10	10	15	10	20	5	20	20	5	20	0	5	20	10	0	15	10	20	0	5	20	15	20	10
15	10	15	10	15	10	5	20	5	20	5	20	10	15	15	10	0	15	5	5	0	20	5	10	5	0
20	5	20	10	15	10	15	10	15	20	5	20	10	15	10	15	0	15	10	20	20	0	10	15	5	20
0	0	0	0	10	15	10	0	0	0	20	5	20	10	15	10	0	15	15	10	15	10	15	10	15	10
5	20	5	10	15	10	15	10	15	10	15	10	15	10	15	10	0	15	10	20	10					

$$J^{(h,s)}(j) = \{[0, \dots, 0, j_\mu, j_{\mu-1}, \dots, j_h, x_{h-1}, x_{h-2}, \dots, x_s, j_{s-1}, \dots, j_0] | x_\lambda \in I_{m_\lambda}; \lambda = h-1, h-2, \dots, s\}. \quad (8)$$

$$[i]_{(s)} = \begin{cases} \{i\}, & \text{if } s \geq \kappa; \mu \leq s. \\ \{j \in \mathbf{L} \mid \text{an element of } \widehat{[j]} \in J^{(\mu,s)}(k) \text{ for some } k \in \widehat{[i]}\}, & \text{if } \mu > s \geq \kappa \text{ or } \mu \geq \kappa > s \\ \{j \in \mathbf{L} \mid \text{an element of } \widehat{[j]} \in J^{(\kappa,s)}(k) \text{ for some } k \in \widehat{[i]}\}, & \text{if } \mu < \kappa; s < \kappa \end{cases} \quad (9)$$

$$A_j^{(s)} = \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i_\lambda} \alpha_\lambda^{i_\lambda j_\lambda} \right) \pi_{Q_s}^{(i)}(a_{i-n_s}) \quad (10)$$

$$= \sum_{i=0}^{n-1} \left(\prod_{\lambda=s+1}^{r-1} (\gamma_\lambda \alpha_\lambda^{j_\lambda})^{(i_\lambda + \delta_\lambda^{(s)})} \right) (\gamma_s \alpha_s^{j_s})^{(i_s+1)} \left(\prod_{\nu=0}^{s-1} \gamma_\nu^{i_\nu} \alpha_\nu^{i_\nu j_\nu} \right) a_i \quad (11)$$

$$= \frac{1}{n} \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} \left(\prod_{\lambda=s+1}^{r-1} (\gamma_\lambda \alpha_\lambda^{j_\lambda})^{\delta_\lambda^{(s)}} \right) \gamma_s \alpha_s^{j_s} \left(\prod_{\nu=0}^{s-1} \alpha_\nu^{(j_\nu - k_\nu)} \right) A_k \quad (12)$$

$$= \frac{1}{n} \sum_{k \in J^{(\kappa,s)}(j)} \left\{ \sum_{i=0}^{n-1} \gamma_\kappa^{\delta_\kappa^{(s)}} \alpha_\kappa^{\delta_\kappa^{(s)} j_\kappa} \left(\prod_{\lambda=s+1}^{\kappa-1} \gamma_\lambda^{\delta_\lambda^{(s)}} \alpha_\lambda^{i_\lambda (j_\lambda - k_\lambda) + \delta_\lambda^{(s)} j_\lambda} \right) \gamma_s \alpha_s^{i_s (j_s - k_s) + j_s} \right\} A_k. \quad (13)$$

Using Lemma 2, we will next prove one of the main results (Theorem 2) of this correspondence. The outline of the proof is similar to [14, proof for Theorem 3] (we use induction on s) and, therefore, we give complete proof only for $s = r - 2$ in the Appendix and for Theorem 2, we give only a part of the proof that highlights the differences.

Theorem 2: For any n and p such that $\gcd(n, p) = 1$, a length $n = m_{r-1} m_{r-2} \dots m_0$ β -consta-Abelian code over $\text{GR}(p^a, l)$ is π_{Q_s} -invariant for $\vec{\beta} = (1, \dots, 1, \beta_\kappa \neq 1, \dots, \beta_0)$ and $0 \leq s \leq r - 2$, if and only if it satisfies the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_u\}$, where $j \in \mathcal{D}_i \subset \mathbf{L} \Rightarrow \mathcal{D}_i = [j]_{(s)}$.

Proof: Let $\mathcal{C}$ be a β -consta-Abelian code and let $\vec{a} \in \mathcal{C}$. For $\mathcal{C}$ to be π_{Q_s} -invariant, $\pi_{Q_s}(\vec{a}) \in \mathcal{C}$. Let $\vec{A}^{(s)} = (A_0^{(s)}, A_1^{(s)}, \dots, A_{n-1}^{(s)})$ be the TDFT-vector of $\pi_{Q_s}(\vec{a})$.

Let $[0, 0, \dots, 0, j_\mu, \dots, j_0] \in \mathbf{L}$. In the next set of equations, we assume that $\kappa > \mu; \kappa > s$. For the other cases, the procedure remains same. Using the TDFT, we can write $A_j^{(s)}$ as in (10) at the top of this page and then inverse TDFT is used to reduce (11) to (12), also at the top of the page.

For the particular case $s = r - 2$, continuing from (13) (at the top of the page), the complete proof for this Theorem is given in the Appendix. For $0 \leq s < r - 2$, (13) can be further reduced to (14) (see (14) and (15) at the top of the following page). In (14), since $\delta_{s+2}^{(s)} = 0$, if $\delta_{s+1}^{(s)} = 0$ or if $i_{s+1} \not\equiv -1 \pmod{m_{s+1}}$, we can further split the first part of the right-hand side of (14) and obtain (15). Observe that K is independent of j_s and K_1 is independent of both j_s and j_{s+1} .

Having proved Theorem 2 for $s = r - 2$ separately (see the Appendix), we can use this as the induction base together with Proposition 1, and the remaining part of the proof is similar to the corresponding proof of Theorem 3 in [14]. $\square$

Example 7:

- i) Table VI lists the constrained sets for $(1, 1, 4)$ -consta-Abelian codes. The monomial π_{Q_s} acting on a codeword for different values of s are:

$$\pi_{Q_2}(c_0, c_1, \dots, c_{n-1}) = (c_4, c_5, c_6, c_7, c_0, c_1, c_2, c_3).$$

$$\pi_{Q_1}(c_0, c_1, \dots, c_{n-1}) = (c_6, c_7, c_0, c_1, c_2, c_3, c_4, c_5).$$

$$\pi_{Q_0}(c_0, c_1, \dots, c_{n-1}) = (4c_7, c_0, 4c_1, c_2, 4c_3, c_4, 4c_5, c_6).$$

In Table III, codes $\mathcal{C}_0, \mathcal{C}_1$, and $\mathcal{C}_8$ are π_{Q_0} -invariant; codes $\mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_9$ are π_{Q_1} -invariant; and rest of the codes are π_{Q_2} -invariant.

- ii) Table IV lists some $(24, 18, 24)$ -consta-Abelian codes over Z_{25} for the constrained sets listed in Table VII(c). The monomial π_{Q_s} for different values of s are

$$\pi_{Q_2}(\vec{c})$$

$$= (24c_6, 24c_7, 24c_8, 24c_9, 24c_{10}, 24c_{11}, c_0, c_1, \dots, c_5).$$

$$\pi_{Q_1}(\vec{c})$$

$$= (7c_9, 7c_{10}, 7c_{11}, c_0, c_1, c_2, 18c_3, 18c_4, 18c_5, c_6, c_7, c_8).$$

$$\pi_{Q_0}(\vec{c})$$

$$= (18c_{11}, c_0, c_1, 24c_2, c_3, c_4, 7c_5, c_6, c_7, 24c_8, c_9, c_{10}).$$

Among codes in Table IV, $\mathcal{C}_1$ and $\mathcal{C}_4$ are π_{Q_1} -invariant and the remaining codes are π_{Q_2} -invariant.

- iii) Table V lists some π_{Q_2} -invariant $(24, 18, 24)$ -consta-Abelian codes over $\text{GR}(5^2, 2)$ for constrained sets in Table VIII(b). The monomials π_{Q_s} for different values of s are the same as those for codes over Z_{25} given above.

IV. π_{U_b} -INVARIANT CODES

Let $b = [b_{r-1}, b_{r-2}, \dots, b_0]$ be such that $\gcd(b_\lambda, m_\lambda) = 1$ for all $\lambda = 0, 1, \dots, r - 1$. Let $U_b : I_n \rightarrow I_n$, which takes

$$[i] = [i_{r-1}, i_{r-2}, \dots, i_0] \rightarrow [b_{r-1}i_{r-1}, b_{r-2}i_{r-2}, \dots, b_0i_0].$$

Let $[b]^{-1} = [b_{r-1}^{-1}, \dots, b_0^{-1}]$, where b_λ^{-1} represents the inverse of b_λ in I_{m_λ} . In this section, we characterize π_{U_b} -invariant β -consta-Abelian codes for a special case of b defined above, which also satisfies: $d_\lambda \mid (b_\lambda^{-1} - 1)$ for all $\lambda = 0, 1, \dots, r - 1$. For every $\lambda = 0, 1, \dots, r - 1$, let $\phi_\lambda^{k, b_\lambda}$ denote a mapping from I_{m_λ} to I_{m_λ} which maps j_λ to

$$\left(\frac{(b_\lambda^{-k} - 1)h_\lambda}{d_\lambda} + b_\lambda^{-k} j_\lambda \right)$$

and let $\Phi^{k, b}$ be a map which maps $[j]$ to

$$[\phi_{r-1}^{k, b_{r-1}}(j_{r-1}), \phi_{r-2}^{k, b_{r-2}}(j_{r-2}), \dots, \phi_0^{k, b_0}(j_0)].$$

Notice that for $[b] = [q, q, \dots, q]$ the maps $\phi_\lambda^{k, b_\lambda} = \phi_\lambda^k$ and $\Phi^{k, b} = \Phi^k$, which is used to define the cyclotomic cosets.

Definition 10: For any $i \in I_n$ and b as defined above, let

$$\widehat{[i]}^{(b^{-1})} = \{[i], \Phi^{1, b}([i]), \Phi^{2, b}([i]), \dots, \Phi^{e_i' - 1, b}([i])\} \quad (16)$$

where e_i' is the smallest integer such that $\Phi^{e_i', b}([i]) = [i]$.

Definition 11: Let

$$\mathbf{L} = \{[i_1], [i_2], \dots, [i_{|\mathbf{L}|}]\}.$$

For every $[i] \in \mathbf{L}$, the associated subset of $\mathbf{L}$, denoted by $[i]_{(b)}$, is defined to be

$$[i]_{(b)} = \left\{ [j] \in \mathbf{L} \mid \widehat{[j]} = \widehat{[i]} \text{ for some } k \in \widehat{[i]}^{(b^{-1})} \right\}. \quad (17)$$

Note that with the definition above, clearly, every b defines a partition on $\mathbf{L}$.

$$A_j^{(s)} = \frac{1}{n} \sum_{k \in J(\kappa, s)(j)} \left\{ \sum_{\substack{i=0; \\ \delta_{s+2}^{(s)}=0}}^{n-1} \gamma_s \alpha_s^{js} \gamma_{s+1}^{\delta_{s+1}^{(s)}} \alpha_{s+1}^{\delta_{s+1}^{(s)} j_{s+1}} \left(\prod_{\lambda=s}^{\kappa-1} \alpha_\lambda^{i_\lambda(j_\lambda - k_\lambda)} \right) \right\} A_k$$

$$+ \frac{1}{n} \sum_{k \in J(\kappa, s)(j)} \left\{ \sum_{\substack{i=0; \\ \delta_{s+2}^{(s)}=1}}^{n-1} \gamma_s \alpha_s^{ks} \gamma_{s+1}^{\delta_{s+1}^{(s)}} \alpha_{s+1}^{\delta_{s+1}^{(s)} j_{s+1}} \left(\prod_{\lambda=s+2}^{\kappa-1} \gamma_\lambda^{\delta_\lambda^{(s)}} \alpha_\lambda^{i_\lambda(j_\lambda - k_\lambda) + \delta_\lambda^{(s)} j_\lambda} \right) \gamma_{\kappa}^{\delta_\kappa^{(s)}} \alpha_{\kappa}^{\delta_\kappa^{(s)} j_\kappa} \right\} A_k. \quad (14)$$

$$A_j^{(s)} = \gamma_s \alpha_s^{js} A_j + \left\{ \frac{1}{m_s} (\gamma_{s+1} \alpha_{s+1}^{js+1} - 1) \sum_{k \in J^{(s)}(j)} \gamma_s \alpha_s^{ks} A_k \right\}$$

$$- \left\{ \frac{1}{m_s m_{s+1}} \sum_{k \in J^{(s+2, s)}(j)} \gamma_s \alpha_s^{ks} \gamma_{s+1}^{\delta_{s+1}^{(s)}} \alpha_{s+1}^{\delta_{s+1}^{(s)} j_{s+1}} A_k \right\}$$

$$+ \frac{1}{n} \sum_{k \in J(\kappa, s)(j)} \left\{ \sum_{\substack{i=0; \\ \delta_{s+2}^{(s)}=1}}^{n-1} \gamma_s \alpha_s^{ks} \gamma_{s+1}^{\delta_{s+1}^{(s)}} \alpha_{s+1}^{\delta_{s+1}^{(s)} j_{s+1}} \left(\prod_{\lambda=s+2}^{\kappa-1} \gamma_\lambda^{\delta_\lambda^{(s)}} \alpha_\lambda^{i_\lambda(j_\lambda - k_\lambda) + \delta_\lambda^{(s)} j_\lambda} \right) \gamma_{\kappa}^{\delta_\kappa^{(s)}} \alpha_{\kappa}^{\delta_\kappa^{(s)} j_\kappa} \right\} A_k.$$

$$= \gamma_s \alpha_s^{js} A_j + K + K_1 \quad (15)$$

where

$$K = \frac{1}{m_s} (\gamma_{s+1} \alpha_{s+1}^{js+1} - 1) \sum_{k \in J^{(s)}(j)} \gamma_s \alpha_s^{ks} A_k \text{ and}$$

$$K_1 = \left\{ \frac{1}{n} \sum_{k \in J(\kappa, s)(j)} \sum_{\substack{i=0; \\ \delta_{s+2}^{(s)}=1}}^{n-1} \gamma_s \alpha_s^{ks} \gamma_{s+1}^{\delta_{s+1}^{(s)}} \alpha_{s+1}^{\delta_{s+1}^{(s)} j_{s+1}} \left(\prod_{\lambda=s+2}^{\kappa-1} \gamma_\lambda^{\delta_\lambda^{(s)}} \alpha_\lambda^{i_\lambda(j_\lambda - k_\lambda) + \delta_\lambda^{(s)} j_\lambda} \right) \gamma_{\kappa}^{\delta_\kappa^{(s)}} \alpha_{\kappa}^{\delta_\kappa^{(s)} j_\kappa} A_k \right\}$$

$$- \left\{ \frac{1}{m_s m_{s+1}} \sum_{k \in J^{(s+2, s)}(j)} \gamma_s \alpha_s^{ks} \gamma_{s+1}^{\delta_{s+1}^{(s)}} \alpha_{s+1}^{\delta_{s+1}^{(s)} j_{s+1}} A_k \right\}$$

Theorem 3: For n and p such that $\gcd(n, p) = 1$, an $n = m_{r-1} m_{r-2} \cdots m_0$ length $\bar{\beta}$ -consta-Abelian code is π_{U_b} -invariant if and only if it satisfies the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_u\}$, where $j \in \mathcal{D}_i \subset \mathbf{L} \Rightarrow \mathcal{D}_i = [j]_{(b)}$.

Proof: Let $A_j^{(b)}$ denote the j th component of TDFT $(\pi_{U_b}(\vec{a}))$. From the TDFT expression

$$A_j^{(b)} = \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i_\lambda} \alpha_\lambda^{i_\lambda j_\lambda} \right) \pi_{U_b}^{(i)}(a_{U_b(i)})$$

$$= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i_\lambda} \alpha_\lambda^{i_\lambda j_\lambda} \right) a_{[b] \lceil i \rceil}$$

$$= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{(b_\lambda^{-1} i_\lambda)} \alpha_\lambda^{(b_\lambda^{-1} i_\lambda) j_\lambda} \right) a_{[i]}$$

$$= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \zeta_\lambda^{i_\lambda (b_\lambda^{-1} h_\lambda + b_\lambda^{-1} d_\lambda j_\lambda)} \right) a_{[i]}$$

$$= A_{[x_{r-1}, x_{r-2}, \dots, x_0]}$$

where

$$x_\lambda = \frac{(b_\lambda^{-1} - 1) h_\lambda}{d_\lambda} + b_\lambda^{-1} j_\lambda$$

for all $\lambda = 0, 1, \dots, r-1$. This implies that a $\bar{\beta}$ -consta-Abelian code is π_{U_b} -invariant if and only if $\mathbf{C}_{[j]} = \mathbf{C}_{[x]}$. $\square$

Corollary 1: All $\bar{\beta}$ -consta-Abelian codes over $\text{GR}(p^a, l)$ are π_{U_b} -invariant for $b = [q^{-1}, q^{-1}, \dots, q^{-1}]$.

Example 8: Table VII(c) lists constrained sets for π_{U_b} -invariance of $(24, 18, 24)$ -consta-Abelian codes over Z_{25} . For $b = [1, 1, 5]$, the action of monomial π_{U_b} for the above parameters is

$$\pi_{U_b}(\vec{c}) = (c_0, 24c_2, 24c_1, c_3, 24c_5, 24c_4, c_6, 24c_8, 24c_7, c_9, 24c_{11}, 24c_{10}).$$

. Similarly, for $b = [1, 5, 1]$, the corresponding vector is

$$\pi_{U_b}(\vec{c}) = (c_0, c_1, c_2, 24c_3, 24c_4, 24c_5, c_6, c_7, c_8, 24c_9, 24c_{10}, 24c_{11}).$$

In Table IV, all codes are π_{U_b} -invariant for

$$b = [5, 1, 1], [1, 5, 5], [5, 5, 5]$$

where as codes $\mathcal{C}_1$ and $\mathcal{C}_4$ are π_{U_b} -invariant for

$$b = [1, 1, 5], [1, 5, 1], [5, 1, 5], [5, 5, 1]$$

as well.

For $\bar{\beta} = (1, 1, \dots, 1)$, the results of this section match the characterization of U_b -invariant Abelian codes discussed in [14]. Notice that U_b -invariant Abelian codes for $b = [b_{r-1}, b_{r-2}, \dots, b_0]$ are also invariant under the permutation $\tau : [i] \mapsto [k]$, where $i_\lambda \mapsto k_\lambda = (b_\lambda i_\lambda + j_\lambda)_{m_\lambda}$ for all $j_\lambda \in I_{m_\lambda}$, and $0 \leq \lambda \leq r-1$ (i.e., an affine permutation in each mixed-radix component). Similarly, it is not difficult to see that the π_{U_b} -invariant consta-Abelian codes discussed in this section are also invariant under monomials π_τ , where τ is any permutation $[i] \mapsto [k]$ defined earlier.

TABLE V
 $n = 2 \times 2 \times 3$ LENGTH $\bar{\beta}$ -CONSTA-ABELIAN CODES OVER $\text{GR}(5^2, 2)$ FOR $\bar{\beta} = (24, 18, 24)$

Time Domain																TDFT
CODE C_0 $T_0 = \emptyset; T_1 = \{0\}$;																A_0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	5	20	15	20	15	0	20	5	5	20	0	15	10	10	15
5	0	10	15	5	15	5	0	15	10	10	15	0	5	20	15	5
20	0	15	10	20	10	20	0	10	15	15	10	0	20	5	10	0
10	0	20	5	10	5	10	0	5	20	20	5	0	10	15	5	20
0	15	10	10	10	20	5	10	5	15	0	0	20	5	5	10	15
15	15	5	0	15	15	20	10	0	20	5	20	20	15	0	20	15
5	15	20	0	15	10	10	10	20	0	10	15	10	0	20	5	5
20	15	0	20	5	5	5	0	10	15	5	15	10	20	0	10	15
10	15	5	15	20	0	15	10	10	20	5	20	15	10	0	20	5
0	5	20	20	15	15	10	20	10	5	0	15	10	10	20	5	10
15	5	0	15	10	10	0	20	5	10	5	20	15	0	20	5	10
5	5	10	0	5	5	15	20	0	15	10	15	15	5	0	15	10
20	5	10	5	15	0	5	20	20	15	10	15	5	15	0	10	15
10	5	15	0	5	20	20	15	0	20	5	15	20	0	15	10	10
0	20	5	5	10	10	15	5	15	20	0	10	15	15	5	20	10
15	20	10	0	20	5	5	5	10	0	5	20	10	5	0	15	5
5	20	15	10	0	0	20	5	5	10	15	10	20	10	0	15	15
20	20	15	0	20	10	5	0	10	15	10	10	20	0	10	5	20
10	20	0	10	15	15	0	5	20	15	20	5	10	0	5	20	15
0	10	15	15	5	5	20	15	10	0	0	5	20	20	15	10	20
15	10	20	10	5	0	10	15	15	5	20	5	15	0	5	20	20
5	10	0	5	20	20	0	15	10	15	5	0	15	10	10	5	10
20	10	5	0	10	15	15	5	0	15	10	10	10	0	20	5	10
10	10	5	0	10	15	15	5	0	15	10	5	15	0	20	5	10
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
0	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
15	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
5	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
20	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	20
10	10	10	20	0	10	10	5	15	0	5	20	20	20	15	0	2

TABLE VI
CONSTRAINED SETS $[i]_{\langle s \rangle}$ FOR $2 \times 2 \times 2$ LENGTH
(1, 1, 4)-CONSTA-ABELIAN CODES

	$[0]_{\langle s \rangle}$	$[1]_{\langle s \rangle}$	$[2]_{\langle s \rangle}$	$[4]_{\langle s \rangle}$
$s = 0$	$[000]$	$[001]$	$[010]$ $[011]$	$[100]$ $[101]$ $[110]$ $[111]$
$s = 1$	$[000]$	$[001]$	$[010]$	$[011]$ $[100]$ $[101]$ $[110]$ $[111]$
$s = 2$	$[000]$	$[001]$	$[010]$	$[011]$ $[100]$ $[101]$ $[110]$ $[111]$

TABLE VII
CYCLOTOMIC COSETS AND CONSTRAINED SETS FOR $n = 2 \times 2 \times 3$
LENGTH CODES OVER Z_{5^2}

$[0]$	$[1]$	$[2]$	$[6]$	$[7]$	$[8]$
$[000]$	$[001]$	$[002]$	$[100]$	$[101]$	$[102]$
$[012]$	$[011]$	$[010]$	$[112]$	$[111]$	$[110]$

(a) Cyclotomic cosets.

$\mathbf{L} \rightarrow$	$[000]$	$[001]$	$[002]$	$[100]$	$[101]$	$[102]$
--------------------------	---------	---------	---------	---------	---------	---------

(b) Cyclotomic coset representative set $\mathbf{L}$.

$s = 0$	$[0]_{\langle s \rangle}$	$[6]_{\langle s \rangle}$
	$[000]$	$[100]$
	$[001]$	$[101]$
	$[002]$	$[102]$

$s = 1$	$[0]_{\langle s \rangle}$	$[1]_{\langle s \rangle}$	$[6]_{\langle s \rangle}$	$[7]_{\langle s \rangle}$
	$[000]$	$[001]$	$[100]$	$[101]$
	$[002]$	$[102]$		

(c) Constrained sets $[i]_{\langle s \rangle}$ for different values of s .

$[i]_{(b)}$	$[0]_{(b)}$	$[1]_{(b)}$	$[6]_{(b)}$	$[7]_{(b)}$
$b = [115], [151], [515], [551]$	$[000]$	$[001]$	$[100]$	$[101]$
	$[002]$	$[102]$		

$[i]_{(b)}$	$[0]_{(b)}$	$[1]_{(b)}$	$[2]_{(b)}$	$[6]_{(b)}$	$[7]_{(b)}$	$[8]_{(b)}$
$b = [511], [155], [555]$	$[000]$	$[001]$	$[002]$	$[100]$	$[101]$	$[102]$

(d) Constrained sets $[i]_{(b)}$ for different values of b .

partition $(T_0^\perp, T_1^\perp, \dots, T_a^\perp)$ such that the dual cyclotomic coset of $[i]$ is a subset of $T_{a-\eta}^\perp$.

Proof: If $\mathcal{C}$ is a $\bar{\beta}$ -consta-Abelian code over $\text{GR}(p^a, l)$ with $j \in T_\eta$, let $\mathcal{C}^*$ be a $\bar{\beta}$ -consta-Abelian code over $\text{GR}(p^a, l)$ with defining set $(T_0^*, T_1^*, \dots, T_a^*)$ such that $j \in T_{a-\eta}^*$. If $\vec{a} \in \mathcal{C}$ and $\vec{b} \in \mathcal{C}^*$, clearly, $A_j B_j = 0$ for all $j \in I_n$. By the twisted-convolution property (6), this implies

$$\sum_{i=0}^{n-1} \pi_{\ominus i}^{(j)}(b_{j \ominus i}) a_i = 0, \quad \text{for all } j \in I_n.$$

In particular

$$\sum_{i=0}^{n-1} \pi_{\ominus i}^{(0)}(b_{-i}) a_i = 0.$$

Let $\vec{c} = (c_0, c_1, \dots, c_{n-1})$ be such that $c_i = \pi_{\ominus i}^{(0)}(b_{-i})$. Therefore,

$$\sum_{i=0}^{n-1} a_i c_i = 0.$$

Using the TDFT expression

$$\begin{aligned} C_j &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i\lambda} \alpha_\lambda^{i\lambda j\lambda} \right) c_i \\ &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i\lambda} \alpha_\lambda^{i\lambda j\lambda} \right) \pi_{\ominus i}^{(0)}(b_{-i}) \\ &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{-i\lambda} \alpha_\lambda^{-i\lambda j\lambda} \right) b_i \\ &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} (\gamma_\lambda^{-1})^{i\lambda} (\alpha_\lambda^{-1})^{i\lambda j\lambda} \right) b_i \end{aligned} \quad (18)$$

$$\begin{aligned} &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \zeta_\lambda^{i\lambda(-h_\lambda - d_\lambda j\lambda)} \right) b_i \\ &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \zeta_\lambda^{i\lambda(h_\lambda^\perp + d_\lambda k_\lambda)} \right) b_i = B_k \end{aligned} \quad (19)$$

where $k_\lambda = \left(\frac{-h_\lambda^\perp - h_\lambda}{d_\lambda} - j_\lambda \right)$ modulo m_λ for all $\lambda = 0, 1, \dots, r-1$. In (18), γ_λ^{-1} is an m_λ th root of β_λ^{-1} and α_λ^{-1} is a primitive m_λ th root of unity for all $\lambda = 0, 1, \dots, r-1$. This proves that the vector $\vec{C}$ is a $\bar{\beta}^{-1}$ -TDFT vector. Let $\mathcal{C}^\perp$ be the collection of all $\vec{c} = (c_0, c_1, \dots, c_{n-1})$ such that $c_i = \pi_{\ominus i}^{(0)}(b_{-i})$ for all $\vec{b} \in \mathcal{C}^*$. Equation (19) proves that the defining set $(T_0^\perp, T_1^\perp, \dots, T_a^\perp)$ of $\mathcal{C}^\perp$ is such that the dual cyclotomic coset of $[j]$ belongs to $T_{a-\eta}^\perp$ if $[j] \in T_\eta$ in $\mathcal{C}$. Further, the type (see [24]) of $\mathcal{C}^\perp$ and $\mathcal{C}^*$ are the same, with $|\mathcal{C}^\perp| = |\mathcal{C}^*| = |\text{GR}(p^a, l)^n|$. Hence, $\mathcal{C}^\perp$ is the dual of $\mathcal{C}$. $\square$

We next show that the dual of a π_{U_b} -invariant (resp., π_{Q_s} -invariant) $\bar{\beta}$ -consta-Abelian code is π_{U_b} -invariant (resp., π_{Q_s} -invariant). Before proving this, we would like to point out that there is an abuse of notation by using permutation π_{U_b} (resp., π_{Q_s}) for both $\bar{\beta}$ -consta-Abelian and its dual, which is actually a $\bar{\beta}^{-1}$ -consta-Abelian code. By definition, both π_{U_b} and π_{Q_s} depend on the actual value of $\bar{\beta} = (\beta_{r-1}, \dots, \beta_0)$ and, hence, strictly speaking we should have used different notations for the monomial π_{U_b} (resp., π_{Q_s}) acting on the $\bar{\beta}$ -consta-Abelian code and its dual. We avoid this by saying that the dual of a π_{U_b} -invariant (resp., π_{Q_s} -invariant) $\bar{\beta}$ -consta-Abelian code is a π_{U_b} -invariant (resp., π_{Q_s} -invariant) $\bar{\beta}^{-1}$ -consta-Abelian code.

Let $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_u\}$ be a constraint for a π_{U_b} -invariant $\bar{\beta}$ -consta-Abelian code defined in Definition 11. For any constrained set $\mathcal{D}_j$, the set $\mathcal{D}_j^\perp$, which is a collection of representative elements of the cyclotomic coset containing $k^\perp$, for all $k \in \mathcal{D}_j$, is a constrained set for a π_{U_b} -invariant $\bar{\beta}^{-1}$ -consta-Abelian code. This is because, from Definition 11, an element of $\mathcal{D}_j$ is a representative element of the cyclotomic coset containing an element of the form $\Phi^{t,b}(i) = [\phi_{r-1}^{t,b_{r-1}}(i_{r-1}), \dots, \phi_0^{t,b_0}(i_0)]$ for some $i \in \mathbf{L}$, $0 \leq t < e_i$, and since

$$\begin{aligned} \frac{-h_\lambda^\perp - h_\lambda}{d_\lambda} - \phi_\lambda^{t,b_\lambda}(i_\lambda) &= \frac{-h_\lambda^\perp - h_\lambda}{d_\lambda} - \frac{(b_\lambda^t - 1)h_\lambda}{d_\lambda} - b_\lambda^t i_\lambda \\ &= \frac{(b_\lambda^t - 1)h_\lambda^\perp}{d_\lambda} + b_\lambda^t \left(\frac{-h_\lambda^\perp - h_\lambda}{d_\lambda} - i_\lambda \right) \\ &= \phi_\lambda^{t,b_\lambda} \left(\frac{-h_\lambda^\perp - h_\lambda}{d_\lambda} - i_\lambda \right) \end{aligned}$$

is in $\bar{\beta}^{-1}$ -TDFT, the above set $\mathcal{D}_j^\perp$ is actually equal to the collection of representative elements of $\bar{\beta}^{-1}$ -TDFT cyclotomic coset containing $\Phi^{t,b}(i^\perp)$, $0 \leq t < e_i$. This set, according to Definition 11, is a valid constrained set for $\bar{\beta}^{-1}$ -consta-Abelian code.

TABLE VIII
CYCLOTOMIC COSETS AND CONSTRAINED SETS FOR $n = 2 \times 2 \times 3$ LENGTH CODES OVER $\text{GR}(5^2, 2)$

$\mathbf{L} \rightarrow$	$[000]$	$[001]$	$[002]$	$[010]$	$[011]$	$[012]$	$[100]$	$[101]$	$[102]$	$[110]$	$[111]$	$[112]$
--------------------------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

(a) Cyclotomic coset representative set $\mathbf{L}$.

	$[0]_{\langle s \rangle}$	$[6]_{\langle s \rangle}$
$s = 0$	$[000]$	$[100]$
	$[001]$	$[101]$
	$[002]$	$[102]$
	$[010]$	$[110]$
	$[011]$	$[111]$
	$[012]$	$[112]$

	$[0]_{\langle s \rangle}$	$[1]_{\langle s \rangle}$	$[2]_{\langle s \rangle}$	$[6]_{\langle s \rangle}$	$[7]_{\langle s \rangle}$	$[8]_{\langle s \rangle}$
$s = 1$	$[000]$	$[001]$	$[002]$	$[100]$	$[101]$	$[102]$
	$[010]$	$[011]$	$[012]$	$[110]$	$[111]$	$[112]$

	$[0]_{\langle s \rangle}$	$[1]_{\langle s \rangle}$	$[2]_{\langle s \rangle}$	$[3]_{\langle s \rangle}$	$[4]_{\langle s \rangle}$	$[5]_{\langle s \rangle}$	$[6]_{\langle s \rangle}$	$[7]_{\langle s \rangle}$	$[8]_{\langle s \rangle}$	$[9]_{\langle s \rangle}$	$[10]_{\langle s \rangle}$	$[11]_{\langle s \rangle}$
$s = 2$	$[000]$	$[001]$	$[002]$	$[010]$	$[011]$	$[012]$	$[100]$	$[101]$	$[102]$	$[110]$	$[111]$	$[112]$

(b) Constrained sets $[i]_{\langle s \rangle}$ for different values of s .

$[i]_{(b)}$	$[0]_{(b)}$	$[1]_{(b)}$	$[3]_{(b)}$	$[4]_{(b)}$	$[6]_{(b)}$	$[7]_{(b)}$	$[9]_{(b)}$	$[10]_{(b)}$
$b = [115], [151], [515], [551]$	$[000]$	$[001]$	$[010]$	$[011]$	$[100]$	$[101]$	$[110]$	$[111]$
	$[002]$		$[012]$		$[102]$		$[112]$	

(c) Constrained sets $[i]_{(b)}$ for different values of b .

Similarly, if $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_u\}$ is a constraint for a π_{Q_s} -invariant $\bar{\beta}$ -consta-Abelian code defined in Theorem 2, it is straightforward to check that, for any π_{Q_s} -invariant $\bar{\beta}$ -consta-Abelian constrained set $\mathcal{D}_j$, the corresponding set $\mathcal{D}_j^\perp$, which is a collection of representative elements of the cyclotomic coset containing $k^\perp$, for all $k \in \mathcal{D}_j$, is a valid constrained set for a π_{Q_s} -invariant $\bar{\beta}^{-1}$ -consta-Abelian code.

We call such a pair of constrained sets $\mathcal{D}_j$ and $\mathcal{D}_j^\perp$ a dual constrained set pair.

Theorem 5: If $(T_0, T_1, \dots, T_a)$ is the defining partition of a $n = m_{r-1}m_{r-2} \cdots m_0$ length π_{Q_s} -invariant (resp., π_{U_b} -invariant) $\bar{\beta}$ -consta-Abelian code $\mathcal{C}$ over $\text{GR}(p^a, l)$ and if the set $\mathcal{D}_j \subset T_\eta$, then its dual code is a π_{Q_s} -invariant (resp., π_{U_b} -invariant) $\bar{\beta}^{-1}$ -consta-Abelian code with defining partition $(T_0^\perp, T_1^\perp, \dots, T_a^\perp)$ such that the corresponding dual constrained set $\mathcal{D}_j^\perp \subset T_{a-\eta}^\perp$.

Proof: For both π_{Q_s} -invariant and π_{U_b} -invariant $\bar{\beta}$ -consta-Abelian code, since we have already shown that $\mathcal{D}_j^\perp$ is a valid constrained set for $\bar{\beta}^{-1}$ -consta-Abelian code, the result follows directly from Theorem 4 and Theorem 2 (resp., Theorem 3). $\square$

Self-dual $\bar{\beta}$ -consta-Abelian codes can be discussed only if $\bar{\beta} = \bar{\beta}^{-1}$ which implies self-dual $\bar{\beta}$ -consta-Abelian codes exist only for $\bar{\beta}$, with $\beta_\lambda = 1$ or -1 for all λ . If $\beta_\lambda = 1$, then $h_\lambda^\perp = h_\lambda = 0$, $d_\lambda = 1$ and if $\beta_\lambda = -1$, $h_\lambda^\perp = h_\lambda = 1$ and $d_\lambda = 2$. Two special cases are as follows.

- $\bar{\beta} = (1, 1, \dots, 1)$ which correspond to the Abelian codes over $\text{GR}(p^a, l)$. The dual-cyclotomic coset of $[i]$ reduces to the coset $[n \ominus i]$ as discussed in [14].
- $\bar{\beta} = (-1, -1, \dots, -1)$ which are nega-Abelian codes (generalization of negacyclic) over $\text{GR}(p^a, l)$. The dual-cyclotomic coset of $[i]$ is the coset containing

$$[-1 - i_{r-1}, -1 - i_{r-2}, \dots, -1 - i_0].$$

From Theorem 5, a π_{Q_s} -invariant (resp., π_{U_b} -invariant) $\bar{\beta}$ -consta-Abelian code with defining partition $(T_0, T_1, \dots, T_a)$ is self-dual if and only if whenever $\mathcal{D}_j \subset T_\eta$, the corresponding dual constrained set

is a subset of $T_{a-\eta}$. We have a nonexistence result for self-dual codes which is an extension of a similar result for Abelian codes.

Theorem 6: If $\gcd(p, n) = 1$, a is an odd integer and $\bar{\beta}$ is such that $\beta_\lambda = -1$ for all $\lambda \in S \subset I_r$, $\beta_\lambda = 1$ otherwise, then $n = m_{r-1}m_{r-2} \cdots m_0$ length self-dual $\bar{\beta}$ -consta-Abelian codes over $\text{GR}(p^a, l)$ do not exist if $\prod_{\lambda \in S} m_\lambda$ is an odd integer.

Proof: Consider the element $i = [i_{r-1}, i_{r-2}, \dots, i_0] \in I_n$ such that $i_\lambda = \frac{m_\lambda - 1}{2}$ for all $\lambda \in S$ and $i_\lambda = 0$ for all $\lambda \in I_r \setminus S$. The dual element is $i^\perp = [i_{r-1}^\perp, \dots, i_0^\perp]$ with $i_\lambda^\perp = -1 - \frac{m_\lambda - 1}{2} = i_\lambda$ for all $\lambda \in S$ and $i_\lambda^\perp = 0 = i_\lambda$ for all $\lambda \in I_r \setminus S$. Hence, the dual cyclotomic coset of $[i]$ is $[i]$ itself.

For the self-dual code $\mathcal{C}$, if A_i takes values from an η -ideal, then according to Theorem 5, the corresponding dual transform component which is A_i itself, should take values from $(a - \eta)$ -ideal. This implies $a - \eta = \eta \Rightarrow a = 2\eta$, and hence a must be even. $\square$

Corollary 2: If $\gcd(p, n) = 1$ and $n = m_{r-1}m_{r-2} \cdots m_0$ is an odd integer, self-dual nega-Abelian codes of length n over $\text{GR}(p^a, l)$ do not exist for odd values of a .

VI. CONCLUSION

In this correspondence, using a TDFT, we have characterized consta-Abelian codes invariant under two monomials π_{Q_s} and π_{U_b} . Codes invariant under π_{Q_s} generalize the class of QT codes which are known to contain some good codes. Consta-Abelian codes are also (β_{r-1}, n_{r-1}) -QT, and they have an advantage over (β_{r-1}, n_{r-1}) -QT codes that are not consta-Abelian, because they need a smaller extension ring for DFT characterization. We have also shown that the dual of a π_{Q_s} -invariant (resp., π_{U_b} -invariant) $\bar{\beta}$ -consta-Abelian code is a π_{Q_s} -invariant (resp., π_{U_b} -invariant) $\bar{\beta}^{-1}$ -consta-Abelian code.

In [18], it was shown that certain Abelian codes over a Galois ring are isomorphic to a direct sum of consta-Abelian codes. For such Abelian codes, knowledge of the automorphism group of individual consta-Abelian codes give valuable information about the automorphism group of the Abelian code itself. Thus, for such Abelian codes, the results of this correspondence can be used to get subgroups of automorphism group which were not considered in our earlier paper

[14]. Further, encoding and decoding of such Abelian codes can be efficiently performed in the DFT domain by using parallel TDFTs (one for each consta-Abelian code) instead of using a single generalized DFT for Abelian codes used in [14].

APPENDIX

THEOREM 2 FOR THE PARTICULAR CASE $s = r - 2$

For any n and p such that $\gcd(n, p) = 1$, a length $n = m_{r-1} m_{r-2} \cdots m_0$ $\bar{\beta}$ -consta-Abelian code over $\text{GR}(p^a, l)$ is $\pi_{Q_{r-2}}$ -invariant for $\bar{\beta} = (1, \dots, 1, \beta_\kappa \neq 1, \dots, \beta_0)$ if and only if it satisfies the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_u\}$, where $j \in \mathcal{D}_i \subset \mathbf{L} \Rightarrow \mathcal{D}_i = [j]_{\langle r-2 \rangle}$.

Proof: Let $\vec{a} \in \mathcal{C}$. For the $\bar{\beta}$ -consta-Abelian code $\mathcal{C}$ to be $\pi_{Q_{r-2}}$ -invariant, $\pi_{Q_{r-2}}(\vec{a}) \in \mathcal{C}$. Let

$$\vec{A}^{(r-2)} = (A_0^{(r-2)}, A_1^{(r-2)}, \dots, A_{n-1}^{(r-2)})$$

be the TDFT vector of $\pi_{Q_{r-2}}(\vec{a})$. From the TDFT expression, we have

$$\begin{aligned} A_j^{(r-2)} &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i\lambda} \alpha_\lambda^{i\lambda j\lambda} \right) \pi_{Q_{r-2}}^{(i)}(a_{i-n_{r-2}}) \\ &= \sum_{i=0}^{n-1} (\gamma_{r-1} \alpha_{r-1}^{j_{r-1}})^{\delta_{r-1}^{(r-2)}} (\gamma_{r-2} \alpha_{r-2}^{j_{r-2}}) \left(\prod_{\lambda=0}^{r-1} \gamma_\lambda^{i\lambda} \alpha_\lambda^{i\lambda j\lambda} \right) a_i. \end{aligned}$$

Using inverse TDFT expression

$$a_i = n^{-1} \prod_{\lambda=0}^{r-1} \gamma_\lambda^{-i\lambda} \left\{ \sum_{j=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \alpha_\lambda^{-i\lambda j\lambda} \right) A_j \right\}$$

we can further simplify the preceding equation, as shown at the bottom of the page and finally obtain (20), where

$$K = \left\{ \frac{1}{m_{r-2}} (\gamma_{r-1} \alpha_{r-1}^{j_{r-1}} - 1) \sum_{k \in J^{(r-2)}(j)} \gamma_{r-2} \alpha_{r-2}^{k_{r-2}} A_k \right\}.$$

Note that, in the equations at the bottom of this page, the second equality is reduced to the third equality using the fact that $\delta_{r-1}^{(r-2)} = 1$ if $i_{r-2} \equiv -1 \pmod{m_{r-2}}$ and $\delta_{r-1}^{(r-2)} = 0$ for other values of i_{r-2} .

Now, $j \in \mathbf{L}$ is free (the values of A_j does not influence the values that other transform components can take and *vice versa*) if and only if $K = 0$, which is true if and only if $\gamma_{r-1} \alpha_{r-1}^{j_{r-1}} = 1$ or

$$\sum_{k \in J^{(r-2)}(j)} \gamma_{r-2} \alpha_{r-2}^{k_{r-2}} A_k = 0.$$

But, from Lemma 2, the latter condition is possible if and only if $A_k = 0$ for all $A_k \in J^{(r-2)}(j)$, which means j is not free. Therefore, j is free if and only if

$$\begin{aligned} \gamma_{r-1} \alpha_{r-1}^{j_{r-1}} &= 1 \\ \Leftrightarrow h_{r-1} + d_{r-1} j_{r-1} &\equiv 0 \pmod{m_{r-1} d_{r-1}} \\ \Leftrightarrow d_{r-1} \mid h_{r-1} \text{ and } j_{r-1} &\equiv -\frac{h_{r-1}}{d_{r-1}} \pmod{m_{r-1}} \\ \Leftrightarrow \beta_{r-1} &= 1 \left(= \gamma_{r-1}^{m_{r-1}} = \zeta_{r-1}^{h_{r-1} m_{r-1}} \right) \\ \Leftrightarrow \kappa < r-1, h_{r-1} &= 0, d_{r-1} = 1 \text{ and } j_{r-1} = -h_{r-1} = 0. \end{aligned}$$

To prove the other cases,

($\Leftarrow$): Assume that the $\bar{\beta}$ -consta-Abelian code $\mathcal{C}$ satisfies the given constraint. That is, for all $i \in [j]_{\langle r-2 \rangle}$, A_i takes values from their respective η -ideal ($\mathcal{C}_i = p^\eta \text{GR}(p^a, l e_i)$). This implies all A_k , $k \in J^{(r-2)}(j)$ take values from their η -ideal (see Definition 9), and, therefore, K is definitely an element of the ideal $p^\eta \text{GR}(p^a, l m)$. It is straightforward to check that $\sigma_0^{l e_j}(K) = K$ (which implies $K \in p^\eta \text{GR}(p^a, l e_j)$) and hence,

$$\sigma_0^{l e_j}(A_j^{(r-2)}) = \sigma_0^{l e_j}(\gamma_{r-2} \alpha_{r-2}^{j_{r-2}} A_j + K) = A_j^{(r-2)}.$$

This means that if $\mathcal{C}$ is a $\bar{\beta}$ -consta-Abelian code with $\mathcal{C}_j = p^\eta \text{GR}(p^a, l e_j)$, then $\mathcal{C}_j^{(r-2)} = p^\eta \text{GR}(p^a, l e_j)$ for any j . Therefore, $\mathcal{C}$ is $\pi_{Q_{r-2}}$ -invariant.

($\Rightarrow$): Let the $\bar{\beta}$ -consta-Abelian code $\mathcal{C}$ be $\pi_{Q_{r-2}}$ -invariant, with $\mathcal{C}_j = p^\eta \text{GR}(p^a, l e_j)$ for $j \in \mathbf{L}$. We need to prove that all other spectral components in the set $[j]_{\langle r-2 \rangle}$ take values from the η -ideal of their corresponding Galois subrings. It is enough to prove this for the spectral components in $J^{(r-2)}(j)$ since the other components in $[j]_{\langle r-2 \rangle}$ will get connected through conjugacy constraints. Toward this end, we consider another transform component j' such that $j' \in J^{(r-2)}(j)$ and $\mathcal{C}_{j'} = p^{\eta'} \text{GR}(p^a, l e_{j'})$. All we need to show is that $\bar{\beta}$ -consta-Abelian code $\mathcal{C}$ is $\pi_{Q_{r-2}}$ -invariant if and only if $\eta = \eta'$.

From (20)

$$K = A_j^{(r-2)} - \alpha_{r-2}^{j_{r-2}} A_j.$$

Since A_j takes values from the ideal $p^\eta \text{GR}(p^a, l e_j)$ and the code is $\pi_{Q_{r-2}}$ -invariant, $A_j^{(r-2)}$ also takes values from $p^\eta \text{GR}(p^a, l e_j)$ and, hence, we have $K \in p^\eta \text{GR}(p^a, l e_j)$. Since $\frac{1}{m_{r-2}} (\alpha_{r-1}^{j_{r-1}} - 1)$ is a unit, this implies

$$\sum_{k \in J^{(r-2)}(j)} \alpha_{r-2}^{k_{r-2}} A_k \in p^\eta \text{GR}(p^a, l e_j). \quad (21)$$

$$\begin{aligned} A_j^{(r-2)} &= \frac{1}{n} \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} (\gamma_{r-1} \alpha_{r-1}^{j_{r-1}})^{\delta_{r-1}^{(r-2)}} (\gamma_{r-2} \alpha_{r-2}^{j_{r-2}}) \prod_{\lambda=0}^{r-1} (\alpha_\lambda)^{i\lambda(j\lambda-k\lambda)} A_k \\ &= \frac{\gamma_{r-2}}{n} \sum_{k \in J^{(r-2)}(j)} \sum_{i=0}^{n-1} (\alpha_{r-2})^{i_{r-2}(j_{r-2}-k_{r-2})+j_{r-2}} (\gamma_{r-1} \alpha_{r-1}^{j_{r-1}})^{\delta_{r-1}^{(r-2)}} A_k \\ &= \frac{\gamma_{r-2}}{n} \sum_{k \in J^{(r-2)}(j)} \left\{ \alpha_{r-2}^{j_{r-2}} \sum_{\substack{i=0; \\ \delta_{r-1}^{(r-2)}=0}}^{n-1} \alpha_{r-2}^{i_{r-2}(j_{r-2}-k_{r-2})} A_k \right\} + \left\{ \sum_{\substack{i=0; \\ \delta_{r-1}^{(r-2)}=1}}^{n-1} \gamma_{r-1} \alpha_{r-2}^{k_{r-2}} \alpha_{r-1}^{j_{r-1}} A_k \right\} \\ &= \gamma_{r-2} \alpha_{r-2}^{j_{r-2}} A_j + \left\{ \frac{1}{m_{r-2}} (\gamma_{r-1} \alpha_{r-1}^{j_{r-1}} - 1) \sum_{k \in J^{(r-2)}(j)} \gamma_{r-2} \alpha_{r-2}^{k_{r-2}} A_k \right\} \\ &= \gamma_{r-2} \alpha_{r-2}^{j_{r-2}} A_j + K \end{aligned} \quad (20)$$

The transform component $j' \in J^{(r-2)}(j)$ and, from Lemma 2, (21) implies $\eta' \geq \eta$.

Notice that $j \in J^{(r-2)}(j') = J^{(r-2)}(j)$ and, hence, in the counterpart of (20) for $A_{j'}^{(r-2)}$, K is a constant, i.e.,

$$A_{j'}^{(r-2)} = \alpha_{r-2}^{j'} A_{j'} + K.$$

By a similar argument to that which we used to obtain (21), we find that

$$\sum_{k \in J^{(r-2)}(j)} \alpha_{r-2}^{k_{r-2}} A_k \in p^{\eta'} \text{GR}(p^a, l_{e_{j'}})$$

which implies $\eta \geq \eta'$. Hence, $\eta = \eta'$.

ACKNOWLEDGMENT

The authors are grateful to the anonymous reviewers for their helpful comments.

REFERENCES

- [1] J. Conan and G. Seguin, "Structural properties and enumeration of quasi cyclic codes," *Applicable Alg. Eng., Commun. Computing*, vol. 4, pp. 25–39, 1993.
- [2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1988.
- [3] M. Esmaeili, T. A. Gulliver, N. P. Secord, and S. A. Mahmoud, "A link between quasi-cyclic codes and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 431–435, Jan. 1998.
- [4] A. R. Calderbank, G. D. Forney, and A. Vardy, "Minimal tail-biting trellises: The Golay code and more," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1435–1455, July 1999.
- [5] A. Krishna and D. V. Sarwate, "Pseudo-cyclic maximum-distance-separable codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 880–884, July 1990.
- [6] J. P. Pedersen and C. Dahl, "Classification of pseudo-cyclic MDS codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 365–370, Mar. 1991.
- [7] J. M. Jensen, "A class of constacyclic codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 951–954, May 1994.
- [8] G. Hughes, "Constacyclic codes, cocycles and a $u + v|u - v$ construction," *IEEE Trans. Inform. Theory*, vol. 46, pp. 674–680, Mar. 2000.
- [9] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, "New 1-generator quasi-twisted codes over GF(5)," in *Codes and Association Schemes*, A. Barg and S. Litsyn, Eds. Providence, RI: AMS/DIMACS, 2001, vol. 56, pp. 265–275.
- [10] —, "The structure of 1-generator QT codes and new linear codes," *Des., Codes Cryptogr.*, vol. 23, no. 3, pp. 313–326, Dec. 2001.
- [11] R. N. Daskalov and T. A. Gulliver, "New quasi-twisted quaternary linear codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2642–2643, Nov. 2000.
- [12] B. R. McDonald, *Finite Rings with Identity*. New York: Marcel Dekker, 1974.
- [13] J. T. Blackford and D. K. Ray-Chaudhuri, "A transform approach to permutation groups of cyclic codes over Galois rings," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2350–2358, Nov. 2000.
- [14] Kiran. T and B. S. Rajan, "Abelian codes over Galois rings closed under certain permutations," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2242–2253, Sept. 2003.
- [15] E. Byrne and P. Fitzpatrick, "Gröbner bases over Galois rings with an application to decoding," *J. Symb. Comp.*, vol. 31, pp. 565–584, 2001.
- [16] —, "Hamming metric decoding of alternant codes over Galois rings," *IEEE Trans. Inform. Theory*, vol. 48, pp. 683–694, Mar. 2002.
- [17] E. Byrne, "Lifting decoding schemes over a Galois ring," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-14 (Lecture Notes in Computer Science)*, S. Boztas and I. Shparlinski, Eds. Berlin, Germany: Springer-Verlag, 2001, vol. 2227, pp. 255–266.
- [18] G. Hughes, "Structure theorems for group ring codes with an application to self-dual codes," *Des., Codes Cryptogr.*, vol. 24, pp. 5–14, Sept. 2001.
- [19] B. S. Rajan and M. U. Siddiqi, "A generalized DFT for Abelian codes over Z_m ," *IEEE Trans. Inform. Theory*, vol. 40, pp. 2082–2090, Nov. 1994.
- [20] —, "Transform domain characterization of Abelian codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1817–1821, Nov. 1992.
- [21] R. M. Tanner, "A transform theory for a class of group-invariant codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 752–775, July 1988.
- [22] B. K. Dey and B. S. Rajan, " F_q -linear cyclic codes over F_{q^m} : DFT characterization," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-14 (Lecture Notes in Computer Science)*, S. Boztas and I. Shparlinski, Eds. Berlin, Germany: Springer-Verlag, 2001, vol. 2227, pp. 67–76.
- [23] S. Boztas, "Constacyclic codes and constacyclic DFTs," in *Proc. IEEE Int. Symp. Information Theory*, Cambridge, MA, June 1998, p. 235.
- [24] W. C. Huffman, "Decompositions and extremal type II codes over Z_4 ," *IEEE Trans. Inform. Theory*, vol. 44, pp. 800–809, Mar. 1998.