Abelian Codes Over Galois Rings Closed Under Certain Permutations

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

***Abstract*—We study n-length Abelian codes over Galois rings with characteristic p^a, where n and p are relatively prime, having the additional structure of being closed under the following two permutations: i) permutation effected by multiplying the coordinates with a unit in the appropriate mixed-radix representation of the coordinate positions and ii) shifting the coordinates by t positions. A code is t-quasi-cyclic (t-QC) if t is an integer such that cyclic shift of a codeword by t positions gives another codeword. We call the Abelian codes closed under the first permutation as unit-invariant Abelian codes and those closed under the second as quasi-cyclic Abelian (QCA) codes. Using a generalized discrete Fourier transform (GDFT) defined over an appropriate extension of the Galois ring, we show that unit-invariant Abelian and QCA codes can be easily characterized in the transform domain. For $t = 1$, QCA codes coincide with those that are cyclic as well as Abelian. The number of such codes for a specified size and length is obtained and we also show that the dual of an unit-invariant t-QCA code is also an unit-invariant t-QCA code. Unit-invariant Abelian (hence unit-invariant cyclic) and t-QCA codes over Galois field F_{p^l} and over the integer residue rings are obtainable as special cases.**

***Index Terms*—Abelian codes, dual codes, Galois rings, generalized discrete Fourier transform (GDFT), mixed-radix number system, quasi-cyclic codes.**

I. Introduction

The family of Abelian codes over finite fields F_{p^l} and integer rings modulo m, Z_m, have been extensively studied [1]–[8]. Abelian codes include the class of cyclic codes (hence, Bose–Chaudhuri–Hocquenghem (BCH), Reed–Solomon (RS) codes) as a special case and in some cases [1], [2], it has been shown that Abelian codes have better error-correcting capabilities compared to that of cyclic codes of the same length.

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 $Z_p[x]$ and, hence, over $Z_{p^a}[x]$ [9]. This Galois ring denoted by GR (p^a, l), throughout this correspondence, coincides with the finite field F_{p^l} when $a = 1$ and the integer residue class ring Z_{p^a} when $l = 1$. Linear codes over Z_{p^a} have been studied by several authors [10]–[13]. Renewed interest in codes over rings was due to Hammons *et al.* [14], who found that certain optimal nonlinear binary codes are binary images of certain linear codes over Z_4 under the Gray map. Recently, various aspects of coding and cryptography are dealt in the general setting of Galois rings instead of finite fields [15]–[20]. In view of this, in this correspondence, the Abelian codes we discuss are over Galois rings GR (p^a, l).

Recently, permutation groups of cyclic codes over Galois rings have been investigated in [15]. Different decoding algorithms for codes over Galois rings and Abelian codes have been studied [21]–[24]. In [22], a decoding algorithm for Alternant codes over Galois rings has been proposed. In certain cases, Abelian codes belong to the class of Alternant codes and, hence, the above algorithm could be used for decoding such codes. In [24], a permutation decoding algorithm was proposed for decoding binary Abelian codes using Gröbner bases. It was shown in [24] that the number of errors that can be corrected varies with the subgroup of the automorphism group of the code used in permutation decoding. The larger this group,the better the error-correcting capability. This motivates us to characterize Abelian codes closed under certain permutations. We achieve this for two kinds of permutations described in the following.

Let $m_0, m_1, \ldots, m_{r-1}$ be nonzero positive integers and let

$$n = \prod_{\lambda=0}^{r-1} m_\lambda.$$

Let $i \in I_n = \{0, 1, \ldots, n-1\}$. Using m_λ's as mixed radixes, any number $i \in I_n$ can be uniquely expressed as

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

where $0 \le i_\lambda < m_\lambda$. The mixed-radix representation of i is denoted by

$$i = \lceil i \rceil = \lceil i_{r-1}, i_{r-2}, \ldots, i_0 \rceil. \tag{2}$$

The mixed-radix addition and subtraction, denoted by $\oplus$ and $\ominus$, respectively, are defined by

$$i \oplus j = \lceil a_{r-1}, a_{r-2}, \ldots, a_0 \rceil, \quad a_\lambda = (i_\lambda + j_\lambda) \bmod m_\lambda, \ \forall \lambda.$$

and

$$i \ominus j = \lceil a_{r-1}, a_{r-2}, \ldots, a_0 \rceil, \quad a_\lambda = (i_\lambda - j_\lambda) \bmod m_\lambda, \ \forall \lambda.$$

Let G be an Abelian group of order

$$n = \prod_{\lambda=0}^{r-1} m_\lambda$$

which is a direct product of r cyclic subgroups of order m_i, $i = 0, 1, \ldots, r-1$. An n-length code is Abelian on G if, for every codeword $(c_0, c_1, \ldots, c_{n-1})$ in the code, $(c_{0\oplus j}, c_{1\oplus j}, \ldots, c_{(n-1)\oplus j})$ also belongs to the code for all values of $j = 0, 1, \ldots, n-1$.

In this correspondence we study Abelian codes that are also closed under the two permutations given in the following definition.

Definition 1:

i) Let $b = \lceil b_{r-1}, b_{r-2}, \ldots, b_0 \rceil \in I_n$ such that $\gcd(b_\lambda, m_\lambda) = 1$ for all $\lambda = 0, 1, \ldots, r-1$. Let $U_b: I_n \to I_n$, defined by

$$\lceil i \rceil = \lceil i_{r-1}, i_{r-2}, \ldots, i_0 \rceil \to \lceil (b_{r-1} i_{r-1})_{m_{r-1}}, (b_{r-2} i_{r-2})_{m_{r-2}}, \ldots, (b_0 i_0)_{m_0} \rceil$$

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.) Abelian codes closed under U_b are called U_b-invariant and the collection of such Abelian codes for various units b will be called unit-invariant Abelian codes.

ii) For some $t \in I_n$, let $Q_t: I_n \to I_n$, which takes $i \to i+t$ modulo n.

Abelian codes closed under Q_t are those which are t-quasi-cyclic as well. (A code is t-quasi-cyclic (t-QC) if t is an integer such that cyclic shift of a codeword by t positions gives another codeword belonging to the code.) Abelian codes closed under Q_t will be referred as **t-QC Abelian (t-QCA) codes**. For $t = 1$, we get **cyclic Abelian (CA) codes**.

Manuscript received March 28, 2002; revised January 25, 2003. This work was supported in part by CSIR, India, under Research Grant 22(0298)/99/EMR-II to B. S. Rajan.

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 R. Koetter, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.815816

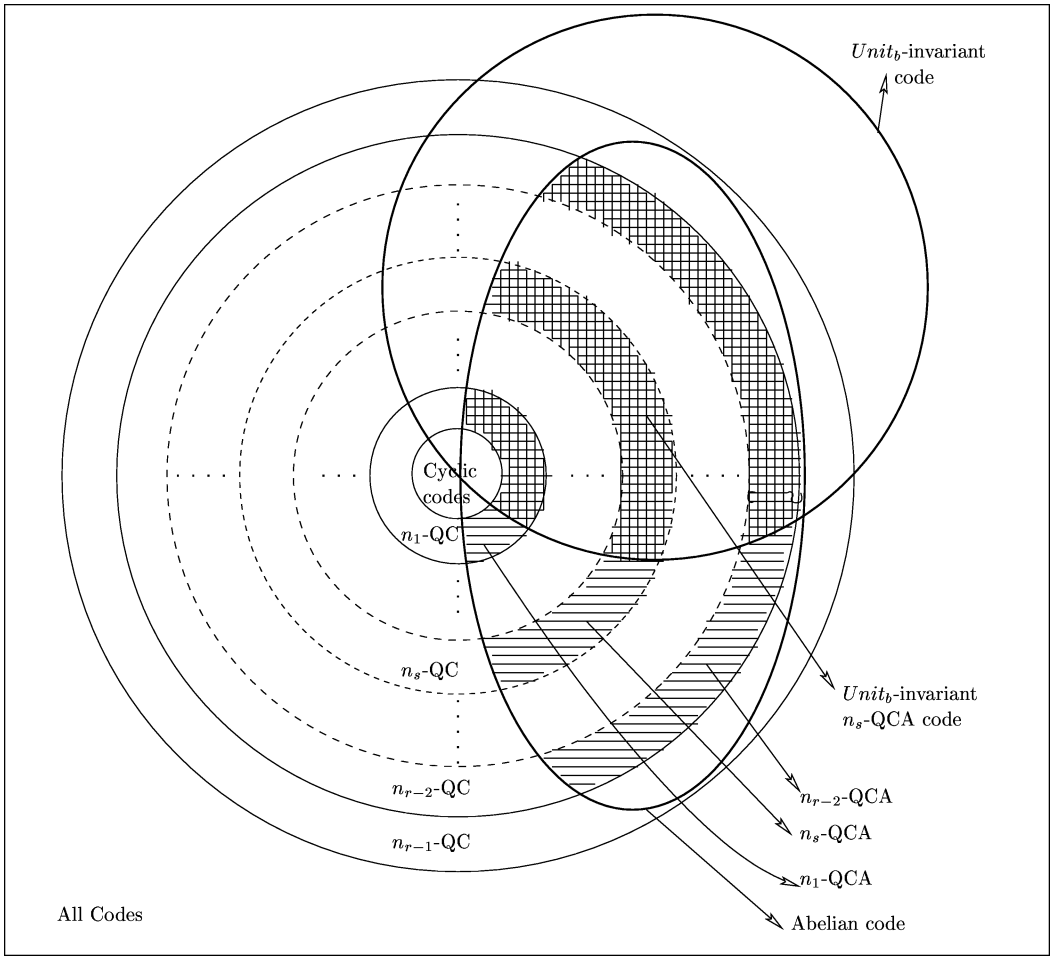

Fig. 1. U_b-invariant QCA codes.

The class of QC codes [25], [26] is important due to the following reasons: i) they contain asymptotically good codes [26], ii) they provide a link between block codes and convolutional codes [27], and iii) they recently have been shown to have a close relationship with the tail-biting representations of general block codes [28].

The classes of codes studied in this correspondence are best explained with Fig. 1. The class of length-$n = m_{r-1}m_{r-2}\cdots m_1 m_0$ Abelian codes is depicted by the ellipse in the figure. In the class of n-length QC codes every n_s-QC code is closed under n_λ-cyclic shifts also for all $s \leq \lambda \leq r-1$, where $n_\lambda = m_{\lambda-1}m_{\lambda-2}\cdots m_1 m_0$. Note that every length-$n = m_{r-1}m_{r-2}\cdots m_1 m_0$ Abelian code is necessarily an n_s-QC code for some $s \leq r-1$ where $n_0 = 1$ by convention. Hence, the ellipse has not gone outside the concentric circles. The circle (shown in bold) represents n-length unit-invariant linear codes (not necessarily Abelian). The horizontally hatched regions represent n_s-QCA codes for some value of s and the double-hatched regions represent Unit_b-invariant n_s-QCA codes. Observe that an Abelian code is either n_s-QCA or Unit_b-invariant n_s-QCA.

The main result of this correspondence consists of i) characterizing QCA and unit-invariant QCA codes over Galois rings, ii) finding the value s for every Abelian code, and iii) if the code is Unit_b-invariant also, then the value b.

We show that it is easy to obtain these results using the discrete Fourier transform (DFT) approach. DFT domain characterization of cyclic, Abelian, and QC codes over finite fields and rings Z_m have been previously discussed in the literature [6], [7], [29], [30]. In this correspondence, we characterize QCA codes and U_b-invariant Abelian codes over Galois rings in the DFT domain defined over suitable Galois ring extensions. Thus, we characterize U_b-invariant QCA codes as well. By inspecting the DFT domain description of an Abelian code, we are able to give all the values of n_s and b for which the code is n_s-QCA and U_b-invariant QCA. QCA codes have the advantage that they need a smaller Galois ring extension compared to *QC non-Abelian* codes for DFT domain characterization for some cases [31]. Efficient DFT domain encoding and decoding techniques exist for codes over fields [32]. Since algebraic decoding generally takes place in the extension ring, a smaller extension ring may lead to simpler or more efficient decoding.

Throughout the correspondence, the length of the code n is relatively prime to the characteristic p^a of the Galois ring over which the code is defined.

The content is organized as follows. In Section II, we give a brief introduction to codes over Galois rings and the concept of dimension of a code over a Galois ring. A generalized DFT is used to characterize Abelian codes in this section. This is a generalization of [6], where Abelian codes over rings Z_m were characterized in DFT domain. In Section III, we characterize U_b-invariant Abelian codes and in Section IV we present the characterization of QCA codes over Galois rings. In Section V, we discuss dual U_b-invariant and QCA codes and enumerate such invariant codes of a specified size.

II. Codes Over Galois Ring

Let GR (p^a, l) be the Galois ring $Z_{p^a}[x]/\phi(x)$, where $\phi(x)$ is a basic irreducible polynomial of degree l in $Z_{p^a}[x]$. We refer the readers

to [6], [35] where most of the properties of Galois rings relevant to us are listed. A GR (p^a, l)-linear code of length n is an GR (p^a, l)-submodule of GR $(p^a, l)^n$.

The following result can be found in [20], [33], [15].

Proposition 1 [20], [33]: A GR (p^a, l)-linear code $\mathcal{C}$ is permutation-equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \cdots & A_{0,a} \\ 0 & pI_{k_1} & pA_{1,2} & \cdots & pA_{1,a} \\ & & \vdots & & \\ 0 & 0 & \cdots & p^{a-1}I_{k_{a-1}} & p^{a-1}A_{a-1,a} \end{pmatrix}$$

where $A_{i,j}$ are matrices over GR (p^a, l) and the columns in the above generator matrix are grouped into blocks of size $k_0, k_1, \ldots, k_{a-1}$. The size of $\mathcal{C}$ is $p^{l\tau}$, where

$$\tau = \sum_{i=0}^{a-1} k_i(a-i)$$

$\mathcal{C}$ is said to be of type $(k_0, k_1, \ldots, k_{a-1})$, and $k_0, k_1, \ldots, k_{a-1}$ are called the dimensions of $\mathcal{C}$.

A. DFT Over Galois Rings

In this subsection, we define the generalized discrete Fourier transform (GDFT) over Galois rings and discuss its properties, used subsequently to characterize Abelian codes over Galois rings.

Throughout the correspondence, G will denote an Abelian group of order n which is a direct product of r cyclic subgroups, denoted by $C_{r-1}, C_{r-2}, \ldots, C_0$ of orders, respectively, $m_{r-1}, m_{r-2}, \ldots, m_0$. Clearly, $n = m_{r-1}m_{r-2}\cdots m_1 m_0$. If $g_{(m_{r-1})}, g_{(m_{r-2})}, \ldots, g_{(m_0)}$ 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 $i_{r-1}, i_{r-2}, \ldots, i_0$ where $0 \le i_k < m_k$ for $k = 0, 1, \ldots, r-1$. This element is denoted by g_i or $g_{\lceil i \rceil}$, where $\lceil i \rceil = \lceil i_{r-1}, i_{r-2}, \ldots, i_0 \rceil$ is the mixed-radix representation of $i \in I_n$ using $m_{r-1}, m_{r-2}, \ldots, m_0$ 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 $\gcd(e, p) = 1$ and henceforth, let

$$n_\lambda = \prod_{i=0}^{\lambda-1} m_i, \qquad \text{for all } \lambda = 1, 2, \ldots, r-1$$

$n_0 = 1$ by convention. We consider linear codes of length $n = m_{r-1}\cdots m_1 m_0$ over the Galois ring GR (p^a, l) and use q for p^l for notational simplicity. (Note that when $a = 1$, GR (p^a, l) becomes F_{p^l} which is generally denoted by F_q.) Let m be the smallest integer such that $e \mid (p^{lm} - 1)$. The polynomial $x^e - 1$ factors linearly in the group of units of the Galois ring GR (p^a, lm) denoted by GR $(p^a, lm)^*$. Hence, elements of order m_i exists in GR $(p^a, lm)^*$ for $i = 0, 1, \ldots, r-1$. The GDFT is defined as follows.

Definition 2 (GDFT): Let

$$\gcd(n, p) = 1 \quad \text{and} \quad \vec{a} = (a_0, \ldots, a_{n-1}) \in \text{GR}(p^a, l)^n.$$

The GDFT of $\vec{a}$, denoted by $\vec{A} = (A_0, \ldots, A_{n-1}) \in \text{GR}(p^a, lm)^n$, is given by

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

where $i = \lceil i_{r-1}, i_{r-2}, \ldots, i_0 \rceil$ and $j = \lceil j_{r-1}, j_{r-2}, \ldots, j_0 \rceil$ are mixed-radix representations of i and j with mixed radixes $m_0, m_1, \ldots, m_{r-1}$ and $\alpha_0, \alpha_1, \ldots, \alpha_{r-1}$ are elements of GR $(p^a, lm)^*$ of orders $m_0, m_1, \ldots, m_{r-1}$, respectively.

For a ring R, the group ring RG is the set of formal sums given by

$$RG = \left\{ \sum_{k=0}^{n-1} c_{\lceil k \rceil} g_{\lceil k \rceil} \colon c_{\lceil k \rceil} \in R \right\}.$$

Addition in RG is the component-wise addition and multiplication in RG can be defined in two ways [6]: i) as convolution in which case RG is a "convolution algebra" or ii) as point-wise multiplication in which case RG is a "point-wise product algebra."

The GDFT defined above is a generalization of the GDFT for codes over $Z_{p^a} = \text{GR}(p^a, 1)$ discussed in [6]. Naturally, all the properties of GDFT in [6] (convolution property, conjugate symmetry property, and the algebra-isomorphism property) hold for the GDFT in Definition 2.

In particular, the conjugate symmetry property is as follows. Let σ_0 be the Frobenius automorphism of GR (p^a, lm) and let $\sigma = \sigma_0^l$. Now, GR (p^a, l) is fixed under the automorphism σ and α_i, $i = 0, 1, \ldots, r-1$ in the definition of GDFT satisfy $\sigma(\alpha_i) = \alpha_i^q$. If

$$(A_{\lceil 0 \rceil}, A_{\lceil 1 \rceil}, \ldots, A_{\lceil n-1 \rceil}) \in \text{GR}(p^a, lm)^n$$

is the GDFT vector of

$$(a_{\lceil 0 \rceil}, a_{\lceil 1 \rceil}, \ldots, a_{\lceil n-1 \rceil}) \in \text{GR}(p^a, l)^n$$

then the following relation among $A_{\lceil j \rceil}$, $j \in I_n$ holds:

$$\sigma(A_{\lceil j \rceil}) = A_{q\lceil j \rceil} \tag{4}$$

where $q\lceil j \rceil = \lceil (qj_{r-1})_{m_{r-1}}, (qj_{r-2})_{m_{r-2}}, \ldots, (qj_0)_{m_0} \rceil$.

B. GDFT Characterization of Abelian Codes Over GR (p^a, l)

Definition 3: The set $\{\lceil i \rceil, q\lceil i \rceil, q^2\lceil i \rceil, \ldots, q^{(e_i-1)}\lceil i \rceil\} \subset I_n$ where $\lceil i \rceil = q^{e_i}\lceil i \rceil$ is called the ***cyclotomic coset*** containing $\lceil i \rceil$, denoted by $\widehat{\lceil i \rceil}$, and e_i is called the exponent of $\widehat{\lceil i \rceil}$. Clearly, I_n is a disjoint union of cyclotomic cosets. Let $\boldsymbol{L} \subset I_n$ be the set containing one element from each of the cyclotomic cosets. We call the set $\boldsymbol{L}$ as the cyclotomic representative set. (For concreteness, we use the smallest element of a cyclotomic coset as a representative.) Notice that cyclotomic cosets are independent of a.

Example 1:

i) For $n = 7 \times 3 \times 3$ and $q = 2$ the cyclotomic cosets are shown in Table I and

$$\boldsymbol{L} = \{\lceil 0 \rceil, \lceil 1 \rceil, \lceil 3 \rceil, \lceil 4 \rceil, \lceil 5 \rceil, \lceil 9 \rceil, \lceil 10 \rceil, \lceil 12 \rceil, \lceil 13 \rceil, \lceil 14 \rceil, \lceil 27 \rceil, \lceil 28 \rceil, \lceil 30 \rceil, \lceil 31 \rceil, \lceil 32 \rceil\}.$$

ii) Table II(a) shows the cyclotomic cosets for $n = 5 \times 2 \times 2$ and $q = 9$ and Table II(b) displays the corresponding $\boldsymbol{L}$.

iii) For $n = 3 \times 3 \times 3$ and $q = 4$, there are 27 cyclotomic cosets each consisting of one element i, $i = 0, 1, \ldots, 26$ which is same as $\boldsymbol{L}$.

The constraint due to the conjugate symmetry property given by (4) implies that i) the set of transform components

$$\hat{A}_{\lceil i \rceil} = \{A_{\lceil i \rceil}, A_{q\lceil i \rceil}, A_{q^2\lceil i \rceil}, \ldots, A_{q^{(e_i-1)}\lceil i \rceil}\}$$

TABLE I
CYCLOTOMIC COSETS FOR $n = 7 \times 3 \times 3$ AND $q = 2$

$\widehat{\lceil 0 \rceil}$	$\widehat{\lceil 1 \rceil}$	$\widehat{\lceil 3 \rceil}$	$\widehat{\lceil 4 \rceil}$	$\widehat{\lceil 5 \rceil}$	$\widehat{\lceil 9 \rceil}$	$\widehat{\lceil 10 \rceil}$	$\widehat{\lceil 12 \rceil}$	$\widehat{\lceil 13 \rceil}$	$\widehat{\lceil 14 \rceil}$	$\widehat{\lceil 27 \rceil}$	$\widehat{\lceil 28 \rceil}$	$\widehat{\lceil 30 \rceil}$	$\widehat{\lceil 31 \rceil}$	$\widehat{\lceil 32 \rceil}$
$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 012 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 300 \rceil$	$\lceil 301 \rceil$	$\lceil 310 \rceil$	$\lceil 311 \rceil$	$\lceil 312 \rceil$
	$\lceil 002 \rceil$	$\lceil 020 \rceil$	$\lceil 022 \rceil$	$\lceil 021 \rceil$	$\lceil 200 \rceil$	$\lceil 202 \rceil$	$\lceil 220 \rceil$	$\lceil 222 \rceil$	$\lceil 221 \rceil$	$\lceil 600 \rceil$	$\lceil 602 \rceil$	$\lceil 620 \rceil$	$\lceil 622 \rceil$	$\lceil 621 \rceil$
					$\lceil 400 \rceil$	$\lceil 401 \rceil$	$\lceil 410 \rceil$	$\lceil 411 \rceil$	$\lceil 412 \rceil$	$\lceil 500 \rceil$	$\lceil 501 \rceil$	$\lceil 510 \rceil$	$\lceil 511 \rceil$	$\lceil 512 \rceil$
						$\lceil 102 \rceil$	$\lceil 120 \rceil$	$\lceil 122 \rceil$	$\lceil 121 \rceil$		$\lceil 302 \rceil$	$\lceil 320 \rceil$	$\lceil 322 \rceil$	$\lceil 321 \rceil$
						$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$	$\lceil 212 \rceil$		$\lceil 601 \rceil$	$\lceil 610 \rceil$	$\lceil 611 \rceil$	$\lceil 612 \rceil$
						$\lceil 402 \rceil$	$\lceil 420 \rceil$	$\lceil 422 \rceil$	$\lceil 421 \rceil$		$\lceil 502 \rceil$	$\lceil 520 \rceil$	$\lceil 522 \rceil$	$\lceil 521 \rceil$

TABLE II
CYCLOTOMIC COSETS AND CONSTRAINED SETS FOR $n = 5 \times 2 \times 2$ LENGTH ABELIAN CODES OVER GR $(3^a, 2)$

$\widehat{\lceil i \rceil} \rightarrow$	$\widehat{\lceil 0 \rceil}$	$\widehat{\lceil 1 \rceil}$	$\widehat{\lceil 2 \rceil}$	$\widehat{\lceil 3 \rceil}$	$\widehat{\lceil 4 \rceil}$	$\widehat{\lceil 5 \rceil}$	$\widehat{\lceil 6 \rceil}$	$\widehat{\lceil 7 \rceil}$	$\widehat{\lceil 8 \rceil}$	$\widehat{\lceil 9 \rceil}$	$\widehat{\lceil 10 \rceil}$	$\widehat{\lceil 11 \rceil}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$
					$\lceil 400 \rceil$	$\lceil 401 \rceil$	$\lceil 410 \rceil$	$\lceil 411 \rceil$	$\lceil 300 \rceil$	$\lceil 301 \rceil$	$\lceil 310 \rceil$	$\lceil 311 \rceil$

(a) Cyclotomic cosets for $q = 9$

$\mathbf{L} \rightarrow$	$\lceil 0 \rceil$	$\lceil 1 \rceil$	$\lceil 2 \rceil$	$\lceil 3 \rceil$	$\lceil 4 \rceil$	$\lceil 5 \rceil$	$\lceil 6 \rceil$	$\lceil 7 \rceil$	$\lceil 8 \rceil$	$\lceil 9 \rceil$	$\lceil 10 \rceil$	$\lceil 11 \rceil$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$

(b) Cyclotomic coset representative set $\mathbf{L}$ for $q = 9$

$\lceil i \rceil_{(b)}$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 2 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 6 \rceil_{(b)}$	$\lceil 7 \rceil_{(b)}$
$b = \lceil 211 \rceil$	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$
					$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$

$\lceil i \rceil_{(b)}$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 2 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 6 \rceil_{(b)}$	$\lceil 7 \rceil_{(b)}$	$\lceil 8 \rceil_{(b)}$	$\lceil 9 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 11 \rceil_{(b)}$
$b = \lceil 411 \rceil$	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$

(c) Constrained sets $\lceil i \rceil_{(b)}$ for different values of b

	$\lceil 0 \rceil_{<s>}$	$\lceil 1 \rceil_{<s>}$	$\lceil 2 \rceil_{<s>}$	$\lceil 3 \rceil_{<s>}$	$\lceil 4 \rceil_{<s>}$	$\lceil 5 \rceil_{<s>}$	$\lceil 6 \rceil_{<s>}$	$\lceil 7 \rceil_{<s>}$	$\lceil 8 \rceil_{<s>}$	$\lceil 9 \rceil_{<s>}$	$\lceil 10 \rceil_{<s>}$	$\lceil 11 \rceil_{<s>}$
$s = 2$	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$

	$\lceil 0 \rceil_{<s>}$	$\lceil 1 \rceil_{<s>}$	$\lceil 2 \rceil_{<s>}$	$\lceil 3 \rceil_{<s>}$	$\lceil 4 \rceil_{<s>}$	$\lceil 5 \rceil_{<s>}$	$\lceil 8 \rceil_{<s>}$	$\lceil 9 \rceil_{<s>}$
$s = 1$	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$
					$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$

	$\lceil 0 \rceil_{<s>}$	$\lceil 1 \rceil_{<s>}$	$\lceil 2 \rceil_{<s>}$	$\lceil 4 \rceil_{<s>}$	$\lceil 8 \rceil_{<s>}$
$s = 0$	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 100 \rceil$	$\lceil 200 \rceil$
			$\lceil 011 \rceil$	$\lceil 101 \rceil$	$\lceil 201 \rceil$
				$\lceil 110 \rceil$	$\lceil 210 \rceil$
				$\lceil 111 \rceil$	$\lceil 211 \rceil$

(d) Constrained sets $\lceil i \rceil_{<s>}$ for different values of s

are related (in other words, transform components indexed by elements of the same cyclotomic coset are related) and, moreover, ii) every element of $\hat{A}_{\lceil i \rceil}$ belongs to the same Galois ring

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

for some fixed e_i dividing m. The set $\hat{A}_{\lceil i \rceil}$ will be called the ***conjugacy class*** containing $A_{\lceil i \rceil}$. For a code $\mathcal{C}$ over GR $(p^a,\, l)$, let $\boldsymbol{C_j} = \{A_j \mid \vec{a} \in \mathcal{C}\}$ denote the set of distinct values taken by the jth transform component of all the codewords in $\mathcal{C}$ and let

$$\boldsymbol{C_{i,j}} = \{(A_i,\, A_j) \mid \vec{a} \in \mathcal{C}\}.$$

Using the conjugate symmetry and convolution property of the GDFT as in [6], it can be shown that the image of all n-tuples over GR $(p^a,\, l)$ under the GDFT, is isomorphic to a direct sum of Galois rings given by

$$\mathrm{GDFT}\,(\mathrm{GR}\,(p^a,\, l)^n) \cong \bigoplus_{i \in \boldsymbol{L}} \mathrm{GR}\,(p^a,\, le_i).$$

An Abelian code $\mathcal{C}$ over GR $(p^a,\, l)$ is isomorphic to an ideal of the ring $\bigoplus_{i \in \boldsymbol{L}} \mathrm{GR}\,(p^a,\, le_i)$, where $\boldsymbol{C_i} = p^{\eta_i}\mathrm{GR}\,(p^a,\, le_i)$ for some fixed value of η_i, $0 \leq \eta_i \leq a$, and transform components belonging to different conjugacy classes take values independently. By A_i and A_j take values independently, we mean $\boldsymbol{C_{i,j}} = \boldsymbol{C_i} \times \boldsymbol{C_j}$.

To be precise, we have the following GDFT domain characterization of Abelian codes over GR $(p^a,\, l)$.

- An Abelian code $\mathcal{C}$ over GR $(p^a,\, l)$ is the set of inverse GDFT vectors of a GR $(p^a,\, l)$-submodule of GDFT $(\mathrm{GR}\,(p^a,\, l)^n) \subset$

$\mathrm{GR}(p^a, lm)^n$ in which transform components indexed by elements of $\widehat{\lceil i \rceil}$, $i = 0, 1, \ldots, n-1$, take all the values from some ideal of $\mathrm{GR}(p^a, le_i)$ and transform components in disjoint cyclotomic cosets take values independently. Equivalently

- For any Abelian code $\mathcal{C}$ over $\mathrm{GR}(p^a, l)$, transform components of every codeword satisfy the conjugate symmetry property and for all $i \in \{0, 1, \ldots, n-1\}$, $\boldsymbol{C_i} = p^{\eta_i}\mathrm{GR}(p^a, le_i)$ for some $\eta_i \in \{0, 1, \ldots, a\}$ with transform components in disjoint cyclotomic cosets taking values *independently*.

In the remainder of this correspondence, we refer to the ideal $p^{\eta_i}\mathrm{GR}(p^a, le_i)$ as the η_i-ideal of $\mathrm{GR}(p^a, le_i)$. Also, for an Abelian code, since $\hat{A}_{\lceil i \rceil}$ can take values only from the ideals of Galois subring $\mathrm{GR}(p^a, le_i)$, we will say $A_{\lceil i \rceil}$ takes values from the η_i-ideal to mean that $\boldsymbol{C_i} = p^{\eta_i}\mathrm{GR}(p^a, le_i)$, since it is obvious the ideal of which ring is meant. Hence, an Abelian code is specified/characterized by specifying $\eta_{i_1}, \eta_{i_2}, \ldots, \eta_{i_{|\boldsymbol{L}|}}$ corresponding to each element in $\boldsymbol{L} = \{\lceil i_1 \rceil, \lceil i_2 \rceil, \ldots, \lceil i_{|\boldsymbol{L}|} \rceil\}$. In other words, an Abelian code over $\mathrm{GR}(p^a, l)$ can be characterized by a partition of I_n as given in Definition 4 that follows.

Definition 4: The ***defining partition*** of an Abelian code is the partition $(T_0, T_1, \ldots, T_a)$ of I_n, where

$$T_\eta = \{j \in I_n \mid \boldsymbol{C_j} = p^\eta \mathrm{GR}(p^a, le_j)\}, \qquad \text{for } 0 \le \eta \le a.$$

For an Abelian code, every T_η is a union of some cyclotomic cosets or $T_\eta = \emptyset$ if $\boldsymbol{C_j} \neq p^\eta \mathrm{GR}(p^a, le_j)$ for any $j \in I_n$.

Example 2: Let $G = C_3 \times C_3 \times C_3$, where C_3 is a cyclic group of order 3. Therefore, $n = 27$ and $e = 3$. We will consider codes over $\mathrm{GR}(2^2, 2)$. Since $e \mid (2^2 - 1)$, there is no need for an extended Galois ring and hence there are no conjugacy constraints on the transform components. All the transform components independently take values from the ideals of Galois ring $\mathrm{GR}(2^2, 2)$, where the ideals are $\{0\}$, $2\mathrm{GR}(2^2, 2)$ and $\mathrm{GR}(2^2, 2)$. All the codes $\mathcal{C}_0$ to $\mathcal{C}_5$ shown in Table III are Abelian codes where each element $a + bx \in \mathrm{GR}(2^2, 2)$ is denoted simply by ab. In all the codes, the transform components not listed take the value zero. For each code the defining partition is also shown.

Including the two trivial codes $\mathrm{GR}(p^a, l)^n$ and the all-zero codeword), there are $(a+1)^{|\boldsymbol{L}|}$ Abelian codes over $\mathrm{GR}(p^a, l)$, of length $n = m_{r-1}m_{r-2}\cdots m_0$. The cardinality of ideal $p^{\eta_i}\mathrm{GR}(p^a, le_i)$ is $p^{(a-\eta_i)le_i}$ and, hence, if $\mathcal{C} \subseteq \mathrm{GR}(p^a, l)^n$ is an $n = m_{r-1}m_{r-2}\cdots m_0$-length Abelian code of dimensions $(k_0, \ldots, k_{a-1})$ (refer to Proposition 1) such that each conjugacy class $\hat{A}_{\lceil i \rceil}$ takes values from the η_i-ideal, then the size of the code is $p^{l\tau}$ where

$$\tau = \sum_{i \in \boldsymbol{L}} e_i(a - \eta_i)$$

and

$$k_j = \sum_{i:\ \eta_i = j} e_i, \qquad \text{for all } j = 0, 1, \ldots, a-1.$$

The conjugacy class taking values from $p^{\eta_i}\mathrm{GR}(p^a, le_i)$ contributes to the dimension k_{η_i}.

C. Constraints on $\boldsymbol{L}$

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 Abelian code to be i) unit-invariant for any $b = \lceil b_{r-1}, b_{r-2}, \ldots, b_0 \rceil$ such that $\gcd(b_\lambda, m_\lambda) = 1$ for all $\lambda = 0, 1, \ldots, r-1$ and ii) n_s-QC for any s, $0 \le s \le r-1$.

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

Definition 5: A **constraint** $\mathcal{D}$ is a partition $\{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$ of the set of cyclotomic coset representatives

$$\boldsymbol{L} = \{\lceil i_1 \rceil, \lceil i_2 \rceil, \ldots, \lceil i_{|\boldsymbol{L}|} \rceil\}.$$

An Abelian code over $\mathrm{GR}(p^a, l)$ is **said to satisfy the constraint** $\mathcal{D}$ if $\lceil i_\alpha \rceil, \lceil i_\beta \rceil \in \mathcal{D}_j$ for some $j \in \{1, 2, \ldots, u\}$ implies $\eta_{i_\alpha} = \eta_{i_\beta}$, where $\boldsymbol{C}_{i_\alpha} = p^{\eta_{i_\alpha}}\mathrm{GR}(p^a, le_{i_\alpha})$ and $\boldsymbol{C}_{i_\beta} = p^{\eta_{i_\beta}}\mathrm{GR}(p^a, le_{i_\beta})$. 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.

Example 3: Table II(c) and (d) and Table IV(a) and (b) show two kinds of constrained sets defined by Definition 6 and Definition 8 ahead for the cases $n = 5 \times 2 \times 2$ with $q = 9$ and $n = 3 \times 3 \times 3$ with $q = 4$.

III. Unit-Invariant Abelian Code

In this section, we characterize U_b-invariant Abelian codes in the DFT domain. Let $b \in I_n$ such that $b = \lceil b_{r-1}, b_{r-2}, \ldots, b_0 \rceil$ and $\gcd(b_\lambda, m_\lambda) = 1$ for all $\lambda = 0, 1, \ldots, r-1$. Let U_b: $I_n \to I_n$, which sends

$$\lceil i \rceil = \lceil i_{r-1}, i_{r-2}, \ldots, i_0 \rceil \to \lceil b \rceil \lceil i \rceil = \lceil b_{r-1}i_{r-1}, b_{r-2}i_{r-2}, \ldots, b_0 i_0 \rceil.$$

Let $\lceil b \rceil^{-1} = \lceil b_{r-1}^{-1}, b_{r-2}^{-1}, \ldots, b_0^{-1} \rceil$, where b_λ^{-1} represents the inverse of b_λ in I_{m_λ} and let $\vec{a}^{\,(b)}$ denote the U_b-permuted version of $\vec{a}$, $\vec{A}^{\,(b)}$ denote the corresponding DFT vector. If $r = 1$, i.e., if G is a cyclic group, U_b-invariant codes generalize the class of cyclic codes over F_q which are invariant under the permutation $i \to qi$ modulo n studied in [26] and [29].

Definition 6: For any $i \in I_n$ and b as defined above, let

$$\widehat{\lceil i \rceil}^{(b^{-1})} = \{\lceil i \rceil, \lceil b \rceil^{-1}\lceil i \rceil, \lceil b \rceil^{-2}\lceil i \rceil, \ldots, \lceil b \rceil^{-e_i'+1}\lceil i \rceil\} \tag{5}$$

where e_i' is the smallest integer such that $\lceil b \rceil^{-e_i'}\lceil i \rceil = \lceil i \rceil$. Moreover, for every $\lceil i \rceil \in \boldsymbol{L} = \{\lceil i_1 \rceil, \lceil i_2 \rceil, \ldots, \lceil i_{|\boldsymbol{L}|} \rceil\}$, the associated subset of $\boldsymbol{L}$, denoted by $\lceil i \rceil_{(b)}$, is defined to be

$$\lceil i \rceil_{(b)} = \left\{ \lceil j \rceil \in \boldsymbol{L} \middle| \widehat{\lceil j \rceil} = \widehat{\lceil k \rceil} \text{ for some } k \in \widehat{\lceil i \rceil}^{(b^{-1})} \right\}. \tag{6}$$

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

Theorem 1: For any n and p such that $\gcd(n, p) = 1$, an $n = m_{r-1}m_{r-2}\cdots m_0$-length Abelian code over $\mathrm{GR}(p^a, l)$ is U_b-invariant iff it satisfies the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$, where $j \in \mathcal{D}_i \subset \boldsymbol{L} \Rightarrow \mathcal{D}_i = \lceil j \rceil_{(b)}$.

Proof: From the GDFT expression

$$\begin{aligned} A_j^{(b)} &= \sum_{i=0}^{n-1}\left(\prod_{\lambda=0}^{r-1}\alpha_\lambda^{i_\lambda j_\lambda}\right)a_i^{(b)} = \sum_{i=0}^{n-1}\left(\prod_{\lambda=0}^{r-1}\alpha_\lambda^{i_\lambda j_\lambda}\right)a_{\lceil b \rceil \lceil i \rceil} \\ &= \sum_{i=0}^{n-1}\left(\prod_{\lambda=0}^{r-1}\alpha_\lambda^{(b_\lambda^{-1}i_\lambda)j_\lambda}\right)a_{\lceil i \rceil} \\ &= A_{\lceil b_{r-1}^{-1}j_{r-1}, b_{r-2}^{-1}j_{r-2}, \ldots, b_0^{-1}j_0 \rceil} = A_{\lceil b \rceil^{-1}\lceil j \rceil}. \end{aligned}$$

This implies that an Abelian code is U_b-invariant iff $\boldsymbol{C}_{\lceil j \rceil} = \boldsymbol{C}_{\lceil b \rceil^{-1}\lceil j \rceil}$. Also, if e_j' is the smallest integer such that $\lceil b \rceil^{-e_j'}\lceil j \rceil = \lceil j \rceil$, an Abelian code is U_b-invariant iff

$$\boldsymbol{C}_{\lceil j \rceil} = \boldsymbol{C}_{\lceil b \rceil^{-1}\lceil j \rceil} = \cdots = \boldsymbol{C}_{\lceil b \rceil^{-e_j'+1}\lceil j \rceil} = \boldsymbol{C}_{\lceil j \rceil}. \qquad \square$$

TABLE III
$n = 3 \times 3 \times 3$ LENGTH ABELIAN CODES OVER GR $(2^2, 2)$

Time domain vector	DFT
CODE $\mathcal{C}_0$ Defining partition: $T_0 = \emptyset; T_1 = \{0\}; T_2 = \overline{\{0\}}$	A_0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	20
02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02	02
22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22	22
CODE $\mathcal{C}_1$ Defining partition: $T_0 = \emptyset; T_1 = \{1\}; T_2 = \overline{\{1\}}$	A_1
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00
20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20	20
02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02	02
22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22	22
CODE $\mathcal{C}_2$ Defining partition: $T_0 = \emptyset; T_1 = \{2\}; T_2 = \overline{\{2\}}$	A_2
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00
20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20	20
02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02	02
22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22	22
CODE $\mathcal{C}_3$ Defining partition: $T_0 = \emptyset; T_1 = \{3\}; T_2 = \overline{\{3\}}$	A_3
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00
20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22	20
02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20	02
22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02	22
CODE $\mathcal{C}_4$ Defining partition: $T_0 = \emptyset; T_1 = \{1, 2\}; T_2 = \overline{\{1, 2\}}$	$A_1 A_2$
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00
20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20	00 20
02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02	00 02
22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22 20 02 22	00 22
20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20	20 00
00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00	20 20
22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22	20 02
02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02	20 22
02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02	02 00
22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22	02 20
00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00	02 02
20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20	02 22
22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22 02 20 22	22 00
02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02 00 02 02	22 20
20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20 20 00 20	22 02
00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00 22 22 00	22 22
CODE $\mathcal{C}_5$ Defining partition: $T_0 = \emptyset; T_1 = \{3, 6\}; T_2 = \overline{\{3, 6\}}$	$A_3 A_6$
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00
20 20 20 02 02 02 22 22 22 20 20 20 02 02 02 22 22 22 20 20 20 02 02 02 22 22 22 20 20 20 02	00 20
02 02 02 22 22 22 20 20 20 02 02 02 22 22 22 20 20 20 02 02 02 22 22 22 20 20 20 02 02 02 22	00 02
22 22 22 20 20 20 02 02 02 22 22 22 20 20 20 02 02 02 22 22 22 20 20 20 02 02 02 22 22 22 20	00 22
20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22	20 00
00 00 00 20 20 20 20 20 20 00 00 00 20 20 20 20 20 20 00 00 00 20 20 20 20 20 20 00 00 00 20	20 20
22 22 22 00 00 00 22 22 22 22 22 22 00 00 00 22 22 22 22 22 22 00 00 00 22 22 22 22 22 22 00	20 02
02 02 02 02 02 02 00 00 00 02 02 02 02 02 02 00 00 00 02 02 02 02 02 02 00 00 00 02 02 02 02	20 22
02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20	02 00
22 22 22 22 22 22 00 00 00 22 22 22 22 22 22 00 00 00 22 22 22 22 22 22 00 00 00 22 22 22 22	02 20
00 00 00 02 02 02 02 02 02 00 00 00 02 02 02 02 02 02 00 00 00 02 02 02 02 02 02 00 00 00 02	02 02
20 20 20 00 00 00 20 20 20 20 20 20 00 00 00 20 20 20 20 20 20 00 00 00 20 20 20 20 20 20 00	02 22
22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02 02 02 20 20 20 22 22 22 02	22 00
02 02 02 00 00 00 02 02 02 02 02 02 00 00 00 02 02 02 02 02 02 00 00 00 02 02 02 02 02 02 00	22 20
20 20 20 20 20 20 00 00 00 20 20 20 20 20 20 00 00 00 20 20 20 20 20 20 00 00 00 20 20 20 20	22 02
00 00 00 22 22 22 22 22 22 00 00 00 22 22 22 22 22 22 00 00 00 22 22 22 22 22 22 00 00 00 22	22 22

Corollary 1: For any n and p such that $\gcd(n, p) = 1$, all $n = m_{r-1} m_{r-2} \cdots m_0$-length Abelian codes over GR (p^a, l) are U_b-invariant for $b = \lceil q^{-1}, q^{-1}, \ldots, q^{-1} \rceil$.

Example 4: Table IV(a) lists for $n = 3 \times 3 \times 3$-length Abelian codes over GR $(2^2, 2)$, constrained sets for all possible values of b except $\lceil 1, 1, 1 \rceil$. For the same parameters, Table III lists codewords of several codes. The codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are U_b-invariant for $b = \lceil 2, 1, 1 \rceil$, $\lceil 1, 2, 1 \rceil$, and $\lceil 2, 2, 1 \rceil$; $\mathcal{C}_3$ is U_b-invariant for $b = \lceil 1, 1, 2 \rceil$, $\lceil 2, 1, 1 \rceil$, and $\lceil 2, 1, 2 \rceil$; and $\mathcal{C}_4$ is U_b-invariant for $b = \lceil 1, 1, 2 \rceil$, $\lceil 2, 1, 1 \rceil$, $\lceil 2, 1, 2 \rceil$, $\lceil 1, 2, 1 \rceil$, $\lceil 1, 2, 2 \rceil$, $\lceil 2, 2, 1 \rceil$, and $\lceil 2, 2, 2 \rceil$.

As an application of this result in the permutation decoding of Abelian codes, we use one of the examples used in [24].

The first code considered in [24] was the $[49 = 7 \times 7, 18, 12]$ code over GR $(2^1, 1) = F_2$. The set $\boldsymbol{L}$ for these parameters is as follows: $\{\lceil 0, 0 \rceil, \lceil 0, 1 \rceil, \lceil 0, 3 \rceil, \lceil 1, 0 \rceil, \lceil 1, 1 \rceil, \lceil 1, 2 \rceil, \lceil 1, 3 \rceil, \lceil 1, 4 \rceil, \lceil 1, 5 \rceil, \lceil 1, 6 \rceil, \lceil 3, 0 \rceil, \lceil 3, 1 \rceil, \lceil 3, 2 \rceil, \lceil 3, 3 \rceil, \lceil 3, 4 \rceil, \lceil 3, 5 \rceil, \lceil 3, 6 \rceil\}$. Further, it was mentioned in [24] that the zeros of this code

TABLE IV
CYCLOTOMIC COSETS AND CONSTRAINED SETS FOR $n = 3 \times 3 \times 3$ LENGTH ABELIAN CODES OVER GR $(2^a, 2)$

$b = \lceil 112 \rceil$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 6 \rceil_{(b)}$	$\lceil 7 \rceil_{(b)}$	$\lceil 9 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 12 \rceil_{(b)}$	$\lceil 13 \rceil_{(b)}$	$\lceil 15 \rceil_{(b)}$	$\lceil 16 \rceil_{(b)}$	$\lceil 18 \rceil_{(b)}$	$\lceil 19 \rceil_{(b)}$	$\lceil 21 \rceil_{(b)}$	$\lceil 22 \rceil_{(b)}$	$\lceil 24 \rceil_{(b)}$	$\lceil 25 \rceil_{(b)}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 020 \rceil$	$\lceil 021 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 120 \rceil$	$\lceil 121 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$	$\lceil 220 \rceil$	$\lceil 221 \rceil$
		$\lceil 002 \rceil$		$\lceil 012 \rceil$		$\lceil 022 \rceil$		$\lceil 102 \rceil$		$\lceil 112 \rceil$		$\lceil 122 \rceil$		$\lceil 202 \rceil$		$\lceil 212 \rceil$		$\lceil 222 \rceil$

$b = \lceil 121 \rceil$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 2 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 6 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 11 \rceil_{(b)}$	$\lceil 12 \rceil_{(b)}$	$\lceil 13 \rceil_{(b)}$	$\lceil 14 \rceil_{(b)}$	$\lceil 15 \rceil_{(b)}$	$\lceil 19 \rceil_{(b)}$	$\lceil 20 \rceil_{(b)}$	$\lceil 21 \rceil_{(b)}$	$\lceil 22 \rceil_{(b)}$	$\lceil 23 \rceil_{(b)}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 002 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 012 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 102 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 202 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$	$\lceil 212 \rceil$
				$\lceil 020 \rceil$	$\lceil 021 \rceil$	$\lceil 022 \rceil$				$\lceil 120 \rceil$	$\lceil 121 \rceil$	$\lceil 122 \rceil$				$\lceil 220 \rceil$	$\lceil 221 \rceil$	$\lceil 222 \rceil$

$b = \lceil 122 \rceil$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 6 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 11 \rceil_{(b)}$	$\lceil 13 \rceil_{(b)}$	$\lceil 14 \rceil_{(b)}$	$\lceil 15 \rceil_{(b)}$	$\lceil 19 \rceil_{(b)}$	$\lceil 20 \rceil_{(b)}$	$\lceil 22 \rceil_{(b)}$	$\lceil 23 \rceil_{(b)}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 012 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$	$\lceil 212 \rceil$
		$\lceil 002 \rceil$	$\lceil 020 \rceil$	$\lceil 022 \rceil$	$\lceil 021 \rceil$		$\lceil 102 \rceil$	$\lceil 120 \rceil$	$\lceil 122 \rceil$	$\lceil 121 \rceil$		$\lceil 202 \rceil$	$\lceil 220 \rceil$	$\lceil 222 \rceil$	$\lceil 221 \rceil$

$b = \lceil 211 \rceil$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 2 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 6 \rceil_{(b)}$	$\lceil 7 \rceil_{(b)}$	$\lceil 8 \rceil_{(b)}$	$\lceil 9 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 11 \rceil_{(b)}$	$\lceil 12 \rceil_{(b)}$	$\lceil 13 \rceil_{(b)}$	$\lceil 14 \rceil_{(b)}$	$\lceil 15 \rceil_{(b)}$	$\lceil 16 \rceil_{(b)}$	$\lceil 17 \rceil_{(b)}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 002 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 012 \rceil$	$\lceil 020 \rceil$	$\lceil 021 \rceil$	$\lceil 022 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 102 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 120 \rceil$	$\lceil 121 \rceil$	$\lceil 122 \rceil$
										$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 202 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$	$\lceil 212 \rceil$	$\lceil 220 \rceil$	$\lceil 221 \rceil$	$\lceil 222 \rceil$

$b = \lceil 212 \rceil$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 7 \rceil_{(b)}$	$\lceil 8 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 11 \rceil_{(b)}$	$\lceil 12 \rceil_{(b)}$	$\lceil 13 \rceil_{(b)}$	$\lceil 14 \rceil_{(b)}$	$\lceil 15 \rceil_{(b)}$	$\lceil 16 \rceil_{(b)}$	$\lceil 17 \rceil_{(b)}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 020 \rceil$	$\lceil 021 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 102 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 120 \rceil$	$\lceil 121 \rceil$	$\lceil 122 \rceil$
		$\lceil 002 \rceil$		$\lceil 012 \rceil$		$\lceil 022 \rceil$	$\lceil 200 \rceil$	$\lceil 202 \rceil$	$\lceil 201 \rceil$	$\lceil 210 \rceil$	$\lceil 212 \rceil$	$\lceil 211 \rceil$	$\lceil 220 \rceil$	$\lceil 222 \rceil$	$\lceil 221 \rceil$

$b = \lceil 221 \rceil$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 2 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 9 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 11 \rceil_{(b)}$	$\lceil 12 \rceil_{(b)}$	$\lceil 13 \rceil_{(b)}$	$\lceil 14 \rceil_{(b)}$	$\lceil 15 \rceil_{(b)}$	$\lceil 16 \rceil_{(b)}$	$\lceil 17 \rceil_{(b)}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 002 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 012 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 102 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 120 \rceil$	$\lceil 121 \rceil$	$\lceil 122 \rceil$
				$\lceil 020 \rceil$	$\lceil 021 \rceil$	$\lceil 022 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 202 \rceil$	$\lceil 220 \rceil$	$\lceil 221 \rceil$	$\lceil 222 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$	$\lceil 212 \rceil$

$b = \lceil 222 \rceil$	$\lceil 0 \rceil_{(b)}$	$\lceil 1 \rceil_{(b)}$	$\lceil 3 \rceil_{(b)}$	$\lceil 4 \rceil_{(b)}$	$\lceil 5 \rceil_{(b)}$	$\lceil 9 \rceil_{(b)}$	$\lceil 10 \rceil_{(b)}$	$\lceil 11 \rceil_{(b)}$	$\lceil 12 \rceil_{(b)}$	$\lceil 13 \rceil_{(b)}$	$\lceil 14 \rceil_{(b)}$	$\lceil 15 \rceil_{(b)}$	$\lceil 16 \rceil_{(b)}$	$\lceil 17 \rceil_{(b)}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 012 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 102 \rceil$	$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 120 \rceil$	$\lceil 121 \rceil$	$\lceil 122 \rceil$
		$\lceil 002 \rceil$	$\lceil 020 \rceil$	$\lceil 022 \rceil$	$\lceil 021 \rceil$	$\lceil 200 \rceil$	$\lceil 202 \rceil$	$\lceil 201 \rceil$	$\lceil 220 \rceil$	$\lceil 222 \rceil$	$\lceil 221 \rceil$	$\lceil 210 \rceil$	$\lceil 212 \rceil$	$\lceil 211 \rceil$

(a) Constrained sets $\lceil i \rceil_{(b)}$ for several values of b

$s = 1$	$\lceil 0 \rceil_{<s>}$	$\lceil 1 \rceil_{<s>}$	$\lceil 2 \rceil_{<s>}$	$\lceil 3 \rceil_{<s>}$	$\lceil 4 \rceil_{<s>}$	$\lceil 5 \rceil_{<s>}$	$\lceil 6 \rceil_{<s>}$	$\lceil 7 \rceil_{<s>}$	$\lceil 8 \rceil_{<s>}$	$\lceil 9 \rceil_{<s>}$	$\lceil 10 \rceil_{<s>}$	$\lceil 11 \rceil_{<s>}$	$\lceil 18 \rceil_{<s>}$	$\lceil 19 \rceil_{<s>}$	$\lceil 20 \rceil_{<s>}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 002 \rceil$	$\lceil 010 \rceil$	$\lceil 011 \rceil$	$\lceil 012 \rceil$	$\lceil 020 \rceil$	$\lceil 021 \rceil$	$\lceil 022 \rceil$	$\lceil 100 \rceil$	$\lceil 101 \rceil$	$\lceil 102 \rceil$	$\lceil 200 \rceil$	$\lceil 201 \rceil$	$\lceil 202 \rceil$
										$\lceil 110 \rceil$	$\lceil 111 \rceil$	$\lceil 112 \rceil$	$\lceil 210 \rceil$	$\lceil 211 \rceil$	$\lceil 212 \rceil$
										$\lceil 120 \rceil$	$\lceil 121 \rceil$	$\lceil 122 \rceil$	$\lceil 220 \rceil$	$\lceil 221 \rceil$	$\lceil 222 \rceil$

$s = 0$	$\lceil 0 \rceil_{<s>}$	$\lceil 1 \rceil_{<s>}$	$\lceil 2 \rceil_{<s>}$	$\lceil 3 \rceil_{<s>}$	$\lceil 6 \rceil_{<s>}$	$\lceil 9 \rceil_{<s>}$	$\lceil 18 \rceil_{<s>}$
	$\lceil 000 \rceil$	$\lceil 001 \rceil$	$\lceil 002 \rceil$	$\lceil 010 \rceil$	$\lceil 020 \rceil$	$\lceil 100 \rceil$	$\lceil 200 \rceil$
				$\lceil 011 \rceil$	$\lceil 021 \rceil$	$\lceil 101 \rceil$	$\lceil 201 \rceil$
				$\lceil 012 \rceil$	$\lceil 022 \rceil$	$\lceil 102 \rceil$	$\lceil 202 \rceil$
						$\lceil 110 \rceil$	$\lceil 210 \rceil$
						$\lceil 111 \rceil$	$\lceil 211 \rceil$
						$\lceil 112 \rceil$	$\lceil 212 \rceil$
						$\lceil 121 \rceil$	$\lceil 221 \rceil$
						$\lceil 122 \rceil$	$\lceil 222 \rceil$

(b) Constrained sets for n_s–QCA codes

are $T_a = T_1 = \{\lceil \widehat{0, 0} \rceil, \lceil \widehat{0, 1} \rceil, \lceil \widehat{1, 0} \rceil, \lceil \widehat{1, 1} \rceil, \lceil \widehat{3, 3} \rceil, \lceil \widehat{0, 3} \rceil, \lceil \widehat{3, 0} \rceil, \lceil \widehat{3, 5} \rceil, \lceil \widehat{5, 3} \rceil, \lceil \widehat{1, 4} \rceil, \lceil \widehat{4, 1} \rceil\}$. It can be checked that both the sets T_1 and $T_0 = I_n \setminus T_1$ are such that $\widehat{\lceil i \rceil}^{(b^{-1})} \in T_1$ (resp., T_0) for any $i \in T_1$ (resp., T_0) and for the following values of $\lceil b \rceil^{-1} = \lceil 2, 2 \rceil, \lceil 3, 3 \rceil, \lceil 1, 2 \rceil, \lceil 2, 1 \rceil$. From our results, this code is U_b-invariant for $\lceil b \rceil = \lceil 4, 4 \rceil, \lceil 5, 5 \rceil, \lceil 1, 4 \rceil$, and $\lceil 4, 1 \rceil$. In [24], only the permutation subgroup corresponding to $\lceil b \rceil = \lceil 4, 4 \rceil$ was used whereas the permutation subgroup corresponding to $\lceil b \rceil = \lceil 5, 5 \rceil, \lceil 1, 4 \rceil, \lceil 4, 1 \rceil$ under which the code is invariant was not considered. Using these additional permutations, it could be possible to correct more errors, or it is possible that one of these permutations is more important than the others in the sense that using a lesser number of permutation subgroups (and, hence, lesser iterations) the decoding algorithm might be able to correct most of the errors.

IV. QCA CODES IN THE GDFT DOMAIN

In this section, for a given length $n = m_{r-1} m_{r-2} \cdots m_0$, we study the GDFT domain characterization of n_s-QCA codes for all $s = 0, 1, 2, \ldots, r-1$ and for a fixed ordering of the factors m_{r-1}, $m_{r-2}, \ldots, m_0$. To characterize the t-QCA code where t is any divisor of n, with a proper ordering of the factors of n, we can always have $t = m'_s m'_{s-1} \cdots m'_0$ for some integer s such that

$$n = m'_{r-1} m'_{r-2} \cdots m'_s m'_{s-1} \cdots m'_0.$$

Hence, the GDFT characterization of a t-QCA can be done where t is any divisor of n, but it is important to notice that, in this case, the mixed-radix addition $\oplus$ (and, hence, Abelian codes) will be defined with respect to the mixed radixes $m'_{r-1}, m'_{r-2}, \ldots, m'_0$. For instance, if G is of order $n = 36 = m_1 \times m_0$, where $m_1 = 9$, $m_0 = 4$, we can characterize all CA and 4-QCA codes (cyclic and 4-QC codes Abelian on $G = C_9 \times C_4$). For $n = 36 = m'_1 \times m'_0$, where $m'_1 = m'_0 = 6$, we can characterize all CA and 6-QCA codes (cyclic and 6-QC codes Abelian on $C_6 \times C_6$). In some cases, it might turn out that a given code $\mathcal{C}$ is Abelian on $G = C_9 \times C_4$ as well as $C_6 \times C_6$ (trivial examples are all-zero vector, repetition code and GR $(p^a, l)^n$) in which case we can characterize whether this code is t-QC for $t = 1, 4$, and 6.

Throughout this section, for a vector $\vec{a} \in \text{GR}(p^a, l)^n$, $\vec{a}^{(t)}$ will denote the t-cyclic shifted version of $\vec{a}$ and the corresponding GDFT vector will be denoted by $\vec{A}^{(t)}$.

Theorem 2: All $n = m_{r-1} m_{r-2} \cdots m_0$-length Abelian codes are n_{r-1}-QCA codes.

Proof: Let $\mathcal{C}$ be an $n = m_{r-1}m_{r-2}\cdots m_0$-length Abelian code. For any $\vec{a} = \sum_{i=0}^{n-1} a_i g_i \in \mathcal{C}$, the codeword

$$g_{(m_{r-1})} \sum_{i=0}^{n-1} a_i g_i = \sum_{i=0}^{n-1} a_{i \oplus \lceil m_{r-1}-1,\, 0,\, \ldots,\, 0 \rceil} g_i = \vec{a}^{\,(n_{r-1})}$$

also belongs to $\mathcal{C}$. □

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

Definition 7: For every $j \in I_n$ such that

$$\lceil j \rceil = \lceil 0,\, 0,\, \ldots,\, 0,\, j_\mu \neq 0,\, j_{\mu-1},\, \ldots,\, j_0 \rceil$$

(i.e., j_μ is the first nonzero mixed-radix component) and $\mu \geq h > s \geq 0$, let the set $J^{(h,\,s)}(j)$ be defined as in (7) at the bottom of the page.

If $h = s+1$, we denote the set in (7) as $J^{(s)}(j)$ for notational simplicity which is the set of all $\lceil i \rceil \in I_n$ with only the sth component running over I_{m_s}.

Definition 8: Let $\boldsymbol{L} = \{\lceil i_1 \rceil, \lceil i_2 \rceil, \ldots, \lceil i_{|\boldsymbol{L}|} \rceil\}$. For any s $(0 \leq s < r-1)$, and $\lceil i \rceil \in \boldsymbol{L}$ such that $i \geq n_{s+1}$ and

$$\lceil i \rceil = \lceil 0,\, \ldots,\, 0,\, i_\mu \neq 0,\, i_{\mu-1},\, \ldots,\, i_0 \rceil,$$

the subset $\lceil i \rceil_{\langle s \rangle}$ of $\boldsymbol{L}$ is defined as the set

$$\left\{ j \in \boldsymbol{L} \middle| \text{ an element of } \widehat{\lceil j \rceil} \in J^{(\mu,\,s)}(k) \text{ for some } k \in \widehat{\lceil i \rceil} \right\}. \quad (8)$$

Since for any pair $\lceil i_c \rceil$, $\lceil i_d \rceil \in \boldsymbol{L}$, $\lceil i_c \rceil_{\langle s \rangle}$ and $\lceil i_d \rceil_{\langle s \rangle}$ either coincide or disjoint, $\{\lceil i \rceil_{\langle s \rangle} | \lceil i \rceil \in \boldsymbol{L}\}$ constitute a partition of $\boldsymbol{L}$. This partition of $\boldsymbol{L}$ will be called the s-**partition of** $\boldsymbol{L}$.

Example 5: Table II(d) lists all the s-partitions for all values of s for the case $n = 5 \times 2 \times 2$ with $q = 9$ and Table IV(b) displays the same for the case $n = 3 \times 3 \times 3$ with $q = 4$.

The following two properties of Galois rings are used in the proof of Lemma 1.

1) The degree of any element $\beta \in \mathrm{GR}(p^a, l)$ is the smallest positive integer t such that $\sigma_0^t(\beta) = \beta$. It follows that if $\beta \in \mathrm{GR}(p^a, t)$ but not in any subring $\mathrm{GR}(p^a, t_1)$, where $t_1 < t$, then t is the degree of β. This helps to identify the elements of a subring $\mathrm{GR}(p^a, t)$ in the Galois ring $\mathrm{GR}(p^a, l)$.
2) For any $\beta \in \mathrm{GR}(p^a, l)$, and t, a divisor of l, such that $l = td$, the relative trace map T_l/t is defined as

$$T_{l/t}(\beta) = \beta + \sigma_0^t(\beta) + \sigma_0^{2t}(\beta) + \cdots + \sigma_0^{(d-1)t}(\beta).$$

Properties analogous to those for the trace function over finite fields [34] can be proved for $T_{l/t}$ as well.

Lemma 1: If $\gcd(n, p) = 1$ and if $\mathcal{C}$ is an $n = m_{r-1}m_{r-2}\cdots m_0$-length Abelian code over $\mathrm{GR}(p^a, l)$ such that $\boldsymbol{C}_k = p^{\eta_k}\mathrm{GR}(p^a, le_k)$ for each $k = \lceil j_{r-1}, j_{r-2}, \ldots, k_s, \ldots, j_0 \rceil \in J^{(s)}(j)$, then

$$\sum_{k \in J^{(s)}(j)} \alpha_s^{k_s} A_k \in p^\gamma \mathrm{GR}(p^a, le), \qquad \text{for every } \vec{A} \in \mathrm{GDFT}(\mathcal{C})$$

iff $\eta_k \geq \gamma$ for all $k \in J^{(s)}(j)$ and $e_k | e$ for the specific value

$$k = \lceil j_{r-1}, \ldots, j_{s+1}, 0, j_{s-1}, \ldots, j_0 \rceil.$$

Proof: If the degree of $\alpha_s^{k_s}$ is t, by definition t is the smallest integer such that $\sigma_0^t(\alpha_s^{k_s}) = \alpha_s^{p^t k_s} = \alpha_s^{k_s}$. Since α_s is an m_sth root of unity, this implies t is the smallest integer such that $k_s = (p^t k_s)_{m_s}$. In the summation $\sum_{k \in J^{(s)}(j)} \alpha_s^{k_s} A_k$, k_s is the sth component in the mixed-radix representation of k. Since $A_k \in \mathrm{GR}(p^a, le_k)$, e_k the exponent of the cyclotomic coset $\widehat{\lceil k \rceil}$ is the smallest integer such that $k_\lambda = (p^{le_k} k_\lambda)_{m_\lambda}$ for all $\lambda = 0, 1, \ldots, r-1$. This implies t divides le_k and from property 1) above, $\alpha_s^{k_s} \in \mathrm{GR}(p^a, le_k)$ and hence $\alpha_s^{k_s} A_k \in p^{\eta_k}\mathrm{GR}(p^a, le_k)$ for all $k \in J^{(s)}(j)$. We now partition the set $\{A_k \mid k \in J^{(s)}(j)\}$ into subsets such that all transform components belonging to the same subset are from the same conjugacy class. Let H be the number of such subsets and M_i, $0 \leq i < H$ the cardinality of each subset. We choose one transform component

$$\lceil k^{(i)} \rceil = \lceil j_{r-1}, j_{r-2}, \ldots, j_{s+1}, k_s^{(i)}, j_{s-1}, \ldots, j_0 \rceil$$

from the ith subset and write

$$\sum_{k \in J^{(s)}(j)} \alpha_s^{k_s} A_k \in p^\gamma \mathrm{GR}(p^a, le)$$

as

$$\sum_{i=0}^{H-1} \sum_{\lambda=0}^{M_i-1} \alpha_s^{q^{\hat{e}\lambda} k_s^{(i)}} A_{q^{\hat{e}\lambda}\lceil k^{(i)} \rceil} \in p^\gamma \mathrm{GR}(p^a, le)$$

where $\hat{e}$ is the size of the cyclotomic coset containing k with sth component, $k_s = 0$. If $d_i = l\hat{e}M_i$ for all i

$$\sum_{\lambda=0}^{M_i-1} \alpha_s^{q^{\hat{e}\lambda} k_s^{(i)}} A_{q^{\hat{e}\lambda}\lceil k^{(i)} \rceil} = \sum_{\lambda=0}^{M_i-1} \sigma_0^{l\hat{e}\lambda} \left(\alpha_s^{k_s^{(i)}} A_{\lceil k^{(i)} \rceil} \right) = T_{d_i/l\hat{e}} \left(\alpha_s^{k_s^{(i)}} A_{\lceil k^{(i)} \rceil} \right).$$

From the properties of relative trace

$$T_{d_i/l\hat{e}} \left(\alpha_s^{k_s^{(i)}} A_{\lceil k^{(i)} \rceil} \right) \in p^{\eta_k}\mathrm{GR}(p^a, l\hat{e}), \qquad \text{for all } k$$

and hence

$$\sum_{i=0}^{H} T_{d_i/l\hat{e}}(\alpha_s^{k_s^{(i)}} A_{\lceil k^{(i)} \rceil}) \in \mathrm{GR}(p^a, le)$$

iff $\hat{e} \mid e$. This summation belongs to γ-ideal of $\mathrm{GR}(p^a, le)$ iff $\eta_k \geq \gamma$ because transform components belonging to different conjugacy classes and, hence, the individual trace functions ($T_{d_i/l\hat{e}}$ for each i) take values independently. □

The following Lemma which denotes the mixed-radix representation of $i + n_s$ is used in the main theorem (Theorem 3).

Lemma 2: For every $\lceil i \rceil = \lceil i_{r-1}, i_{r-2}, \ldots, i_0 \rceil$ and n_s, $s = 1, 2, \ldots, r-1$, the mixed-radix representation of $\lceil i + n_s \rceil$ is given in (9) at the bottom of the page, where

$$\delta_k^{(s)} = \begin{cases} 1, & \text{if } i_\lambda \equiv -1 \bmod m_\lambda, \text{ for all } s \leq \lambda < k \\ 0, & \text{otherwise} \end{cases}$$

for $s+1 \leq k \leq r-1$.

The following theorem presents the main result of this correspondence that establishes the constraint set for an n_s-QCA code.

$$J^{(h,\,s)}(j) = \{\lceil 0, \ldots, 0, j_\mu, j_{\mu-1}, \ldots, j_h, x_{h-1}, x_{h-2}, \ldots, x_s, j_{s-1}, \ldots, j_0 \rceil\} | x_\lambda \in I_{m_\lambda};\ \lambda = h-1, h-2, \ldots, s\}. \quad (7)$$

$$\lceil i + n_s \rceil = \lceil (i_{r-1} + \delta_{r-1}^{(s)})_{m_{r-1}},\, (i_{r-2} + \delta_{r-2}^{(s)})_{m_{r-2}},\, \ldots,\, (i_{s+1} + \delta_{s+1}^{(s)})_{m_{s+1}},\, (i_s + 1)_{m_s},\, i_{s-1},\, \ldots,\, i_0 \rceil \quad (9)$$

Theorem 3: For any n and p such that $\gcd(n, p) = 1$, a length-$n = m_{r-1}m_{r-2}\cdots m_0$ Abelian code over $\mathrm{GR}(p^a, l)$ is n_s-QCA, $0 \le s \le r-2$, iff it satisfies the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$, where

$$j \in \mathcal{D}_i \subset \boldsymbol{L} \Rightarrow \mathcal{D}_i = \begin{cases} \{j\}, & \text{if } j \le n_{s+1} - 1 \\ \lceil j \rceil_{\langle s \rangle}, & \text{otherwise.} \end{cases}$$

In other words, an Abelian code is n_s-QCA iff for all $j \in \boldsymbol{L}$

i) the spectral component j is free if $0 \le j \le n_{s+1} - 1$;
ii) and spectral components belonging to $\lceil j \rceil_{\langle s \rangle}$ form a constrained set if $n_{s+1} \le j \le n-1$.

Proof: Let $\vec{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$. We have

$$\begin{aligned} A_j^{(n_s)} &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \alpha_\lambda^{i_\lambda j_\lambda} \right) a_{i-n_s} \\ &= \sum_{i=0}^{n-1} \left(\prod_{\lambda=s+1}^{r-1} \alpha_\lambda^{j_\lambda (i_\lambda + \delta_\lambda^{(s)})} \right) \alpha_s^{j_s(i_s+1)} \prod_{\nu=0}^{s-1} \alpha_\nu^{i_\nu j_\nu} a_i. \end{aligned} \quad (10)$$

Clearly, if $j \in \boldsymbol{L}$ such that $0 \le j \le n_{s+1} - 1$, $j_{r-1} = j_{r-2} = \cdots = j_{s+1} = 0$, and (10) becomes

$$A_j^{(n_s)} = \alpha_s^{j_s} \sum_{i=0}^{n-1} \left(\prod_{\lambda=0}^{r-1} \alpha_\lambda^{i_\lambda j_\lambda} \right) a_i = \alpha_s^{j_s} A_j.$$

The preceding equation implies j is free for all $0 \le j \le n_{s+1} - 1$, thus proving condition i). To prove condition ii) for $n_{s+1} \le j \le n-1$, we continue with (10).

If $\lceil j \rceil = \lceil 0, \ldots, 0, j_\mu \ne 0, j_{\mu-1}, \ldots, j_0 \rceil$, substituting the inverse GDFT

$$a_i = \frac{1}{n} \sum_{k=0}^{n-1} \prod_{\lambda=0}^{r-1} (\alpha_\lambda)^{-i_\lambda k_\lambda} A_k$$

in (10) we can reduce it to (11)–(13) as shown at the bottom of the page. In (12), since $\delta_{s+2}^{(s)} = 0$, if $\delta_{s+1}^{(s)} = 0$ or if $i_{s+1} \not\equiv -1 \bmod m_{s+1}$, we can further split the first part of the right-hand side of (12) and obtain (13).

Observe that K is independent of j_s and K_1 is independent of both j_s and j_{s+1}.

Proof for the "Only If" Part: Let $\mathcal{C}$ be an n_s-QCA code. Notice that in deriving (13), we have not assumed any fixed value for s. In this part of the proof, we will prove condition ii) by induction on s. To elaborate, we will first prove that condition ii) is true for $s = r-2$. Using the fact that every n_s-QC code is n_{s+1}-QC also, we will be through if we assume that the condition is true for $s+1$ and show that it is true for s.

To prove condition ii) for $s = r-2$, let $j \in \boldsymbol{L}$ such that $n_{r-1} \le j \le n-1$, and let $\boldsymbol{C_j} = p^\eta \mathrm{GR}(p^a, le_j)$. We need to prove that

$$\begin{aligned} A_j^{(n_s)} &= \frac{1}{n} \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} \left(\prod_{\lambda=s+1}^{\mu} \alpha_\lambda^{i_\lambda(j_\lambda - k_\lambda) + \delta_\lambda^{(s)} j_\lambda} \right) \alpha_s^{i_s(j_s-k_s)+j_s} \left(\prod_{\nu=0}^{s-1} \alpha_\nu^{i_\nu(j_\nu - k_\nu)} \right) A_k \\ &= \frac{1}{n} \sum_{k \in J^{(\mu,s)}(j)} \left\{ \sum_{i=0}^{n-1} \alpha_\mu^{\delta_\mu^{(s)} j_\mu} \left(\prod_{\lambda=s+1}^{\mu-1} \alpha_\lambda^{i_\lambda(j_\lambda-k_\lambda)+\delta_\lambda^{(s)} j_\lambda} \right) \alpha_s^{i_s(j_s-k_s)+j_s} \right\} A_k \qquad (11) \\ &= \frac{1}{n} \sum_{k \in J^{(\mu,s)}(j)} \left\{ \sum_{\substack{i=0; \\ \delta_{s+2}^{(s)}=0}}^{n-1} \alpha_s^{j_s} \alpha_{s+1}^{\delta_{s+1}^{(s)} j_{s+1}} \left(\prod_{\lambda=s}^{\mu-1} \alpha_\lambda^{i_\lambda(j_\lambda-k_\lambda)} \right) A_k \right\} \\ &\quad + \frac{1}{n} \sum_{k \in J^{(\mu,s)}(j)} \left\{ \sum_{\substack{i=0; \\ \delta_{s+2}^{(s)}=1}}^{n-1} \alpha_s^{k_s} \alpha_{s+1}^{k_{s+1}} \left(\prod_{\lambda=s+2}^{\mu-1} \alpha_\lambda^{i_\lambda(j_\lambda-k_\lambda)+\delta_\lambda^{(s)} j_\lambda} \right) \alpha_\mu^{\delta_\mu^{(s)} j_\mu} A_k \right\} \qquad (12) \\ A_j^{(n_s)} &= \alpha_s^{j_s} A_j + \left\{ \frac{1}{m_s} (\alpha_{s+1}^{j_{s+1}} - 1) \sum_{k \in J^{(s)}(j)} \alpha_s^{k_s} A_k \right\} \\ &\quad - \left\{ \frac{1}{m_s m_{s+1}} \sum_{k \in J^{(s+2,s)}(j)} \alpha_s^{k_s} \alpha_{s+1}^{k_{s+1}} A_k \right\} \\ &\quad + \left\{ \frac{1}{n} \sum_{k \in J^{(\mu,s)}(j)} \sum_{\substack{i=0; \\ \delta_{s+2}^{(s)}=1}}^{n-1} \alpha_s^{k_s} \alpha_{s+1}^{k_{s+1}} \left(\prod_{\lambda=s+2}^{\mu-1} \alpha_\lambda^{i_\lambda(j_\lambda-k_\lambda)+\delta_\lambda^{(s)} j_\lambda} \right) \alpha_\mu^{\delta_\mu^{(s)} j_\mu} A_k \right\} \\ &= \alpha_s^{j_s} A_j + K + K_1 \qquad (13) \end{aligned}$$

where

$$K = \frac{1}{m_s} (\alpha_{s+1}^{j_{s+1}} - 1) \sum_{k \in J^{(s)}(j)} \alpha_s^{k_s} A_k$$

and

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

all other spectral components in the set $\lceil j \rceil_{\langle r-2 \rangle}$ 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 $\lceil j \rceil_{\langle r-2 \rangle}$ will get connected through conjugacy constraints. Toward this end, we consider another transform component j' such that $j' \in J^{(r-2)}(j)$ and $\boldsymbol{C_{j'}} = p^{\eta'}\mathrm{GR}\,(p^a, le_{j'})$. All we need to show is that, if Abelian code $\mathcal{C}$ is n_{r-2}-QC then $\eta = \eta'$.

For $s = r-2$, starting from (11) and following similar manipulation as in (12) and (13) we get

$$A_j^{(n_{r-2})} = \alpha_{r-2}^{j_{r-2}} A_j + K \tag{14}$$

where

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

From the preceding equality, $K = A_j^{(n_{r-2})} - \alpha_{r-2}^{j_{r-2}} A_j$. Since A_j takes values from the ideal $p^{\eta}\mathrm{GR}\,(p^a, le_j)$, we have $K \in p^{\eta}\mathrm{GR}\,(p^a, le_j)$ and since $\frac{1}{m_{r-2}}(\alpha_{r-1}^{j_{r-1}} - 1)$ is a unit, this implies

$$\sum_{k \in J^{(r-2)}(j)} \alpha_{r-2}^{k_{r-2}} A_k \in p^{\eta}\mathrm{GR}\,(p^a, le_j). \tag{15}$$

The transform component $j' \in J^{(r-2)}(j)$, and from Lemma 1, (15) implies $\eta' \geq \eta$.

Notice that $j \in J^{(r-2)}(j') = J^{(r-2)}(j)$ and, hence, in the counterpart of (15) for $A_{j'}^{(n_{r-2})}$, K is a constant, i.e.,

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

By a similar argument that we used to obtain (15)

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

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

Having proved condition ii) for $s = r-2$, we now assume that this condition is true for some $s+1$, i.e., we assume that the set $\lceil j \rceil_{\langle s+1 \rangle}$ is a constrained set for any $j \in \boldsymbol{L}$. We draw attention to the fact that, for $\lceil j \rceil = \lceil 0, \ldots, 0, j_\mu, j_{\mu-1}, \ldots, j_0 \rceil$, the set $J^{(\mu, s)}(j)$ is a union of sets $J^{(\mu, s+1)}(.)$ as shown in (16) at the bottom of the page.

From our definition of the s-partition of $\boldsymbol{L}$ in Definition 8, the set $\lceil j \rceil_{\langle s \rangle}$ will be a union of several $\lceil i \rceil_{\langle s+1 \rangle}$ for some $i \in \boldsymbol{L}$. Let

$$\lceil j \rceil_{\langle s \rangle} = \{ \lceil j_1 \rceil_{\langle s+1 \rangle} \cup \lceil j_2 \rceil_{\langle s+1 \rangle} \cup \cdots \cup \lceil j_d \rceil_{\langle s+1 \rangle} \}.$$

Following our hypothesis, let all transform components in $\lceil j_i \rceil_{\langle s+1 \rangle}$ take values from their respective η_{j_i}-ideal for all $i \in \{1, 2, \ldots, d\}$. Our aim is to prove that η_{j_i}'s are all equal for all $i \in \{1, 2, \ldots, d\}$.

Without loss of generality, we will first assume that $j = j_1 \in \lceil j \rceil_{\langle s \rangle}$ and let $\boldsymbol{C_j} = p^{\eta_{j_1}}\mathrm{GR}\,(p^a, le_j)$. Now we consider any $j' \in J^{(s+1)}(j)$. If $j' \notin \boldsymbol{L}$, a representative of $\widehat{\lceil j' \rceil}$ is in $\boldsymbol{L}$; in fact, it belongs to $\lceil j \rceil_{\langle s+1 \rangle}$ and hence $\boldsymbol{C_{j'}}$ is also a η_{j_1}-ideal. Let $\boldsymbol{C_{j'}} = p^{\eta_{j_1}}\mathrm{GR}\,(p^a, le_{j'})$. From (13)

$$A_j^{(n_s)} = \alpha_s^{j_s} A_j + K + K_1$$
$$A_{j'}^{(n_s)} = \alpha_s^{j_s} A_{j'} + K' + K_1.$$

Since $\mathcal{C}$ is n_s-QCA, both $A_j^{(n_s)}$ and A_j take values from $p^{\eta_{j_1}}\mathrm{GR}\,(p^a, le_j)$. Similarly, both $A_{j'}^{(n_s)}$ and $A_{j'}$ take values from $p^{\eta_{j_1}}\mathrm{GR}\,(p^a, le_{j'})$. This implies

$$K + K_1 \in p^{\eta_{j_1}}\mathrm{GR}\,(p^a, le_j)$$

and

$$K' + K_1 \in p^{\eta_{j_1}}\mathrm{GR}\,(p^a, le_{j'})$$

and, therefore, $K - K' \in p^{\eta_{j_1}}\mathrm{GR}\,(p^a, le)$ where $e = lcm(e_j, e_{j'})$. This implies

$$\sum_{k \in J^{(s)}(j)} \alpha_s^{k_s} A_k \in p^{\eta}\mathrm{GR}\,(p^a, le_1) \tag{17}$$

where $\eta \geq \eta_{j_1}$ and $e_1 \,|\, e$. For all $k \in J^{(s)}(j)$, if $\boldsymbol{C_k} = p^{\eta_k}\mathrm{GR}\,(p^a, le_k)$, from Lemma 1, $\eta_k \geq \eta \geq \eta_{j_1}$. But all transform components $k \in J^{(s)}(j)$ have their representatives in $\lceil j \rceil_{\langle s \rangle}$ and hence each η_k is equal to some η_{j_i} and, therefore, $\eta_{j_i} \geq \eta_{j_1}$ for all $i \in \{2, 3, \ldots, d\}$.

In our argument so far, we assumed that $\lceil j \rceil = \lceil j_1 \rceil$. But the entire argument holds good for $\lceil j \rceil = \lceil j_i \rceil, i \in \{2, 3, \ldots, d\}$. Hence, $\eta_{j_1} \geq \eta_{j_i}$ for all $i \in \{2, 3, \ldots, d\}$, which implies $\eta_{j_1} = \eta_{j_2} = \cdots = \eta_{j_d}$.

Proof for the "If" Part: Let the Abelian code $\mathcal{C}$ satisfy the constraint given in the statement of the theorem. Let $\boldsymbol{C}_j = p^{\eta_j}\mathrm{GR}\,(p^a, le_j)$. Because the code satisfies condition ii), all transform components $k \in J^{(\mu, s)}(j)$ take values from their respective η_j-ideal (i.e., $\boldsymbol{C}_k = p^{\eta_j}\mathrm{GR}\,(p^a, le_k)$). We need to show that $A_j^{(n_s)}$ also takes values from $p^{\eta_j}\mathrm{GR}\,(p^a, le_j)$.

For this, we continue from (11). Since A_k takes values from the ideal $p^{\eta_j}\mathrm{GR}\,(p^a, le_k) \subset p^{\eta_j}\mathrm{GR}\,(p^a, lm)$, the element

$$\left\{ \sum_{i=0}^{n-1} \alpha_\mu^{\delta_\mu^{(s)} j_\mu} \left(\prod_{\lambda=s+1}^{\mu-1} \alpha_\lambda^{i_\lambda (j_\lambda - k_\lambda) + \delta_\lambda^{(s)} j_\lambda} \right) \alpha_s^{i_s (j_s - k_s) + j_s} \right\} A_k$$

in (11), belongs to $p^{\eta_j}\mathrm{GR}\,(p^a, lm)$ for all $k \in J^{(\mu, s)}(j)$, and hence $A_j^{(n_s)}$ also takes values from $p^{\eta_j}\mathrm{GR}\,(p^a, lm)$. But since $p^{le_j}\lceil j \rceil = q^{e_j}\lceil j \rceil = \lceil j \rceil$

$$\sigma_0^{le_j}\left(A_j^{(n_s)}\right) = A_j^{(n_s)}$$

as shown at the bottom of the page, and hence $A_j^{(n_s)}$ is an element of $p^{\eta_j}\mathrm{GR}\,(p^a, le_j) \subset p^{\eta_j}\mathrm{GR}\,(p^a, lm)$. □

Example 6: Table IV(b) lists the constrained sets for the codes shown in Table III. Notice that, in Table III, all codes except $\mathcal{C}_3$ and $\mathcal{C}_5$ are CA codes whereas $\mathcal{C}_3$ and $\mathcal{C}_5$ are 3-QCA codes.

Definition 9: An Abelian code which is both t-QC as well as U_b-invariant is called an U_b-invariant t-QCA code.

Corollary 2: For any n and p such that $\gcd(n, p) = 1$, a length-$n = m_{r-1}m_{r-2}\cdots m_0$ Abelian code over $\mathrm{GR}\,(p^a, l)$ with defining partition $(T_0, T_1, \ldots, T_a)$ is U_b-invariant n_s-QCA iff for any $j \in \boldsymbol{L}$

1) $\lceil j \rceil_{(b)} \subset T_\eta$ for some η; and
2) $\lceil j \rceil_{\langle s \rangle} \subset T_\eta$ for some η if $j \geq n_{s+1}$.

Proof: Follows from Theorems 1 and 3. □

Given any $n = m_{r-1}m_{r-2}\cdots m_0$-length Abelian code, this result helps us to systematically identify the smallest value of s for which the code is n_s-QC and all values of b for which the code is U_b-invariant.

$$J^{(\mu, s)}(j) = \bigcup_{x_s \in I_{m_s}} J^{(\mu, s+1)}(\lceil 0, \ldots, 0, j_\mu, \ldots, j_{s+1}, x_s, j_{s-1}, \ldots, j_0 \rceil) \tag{16}$$

$$\sigma_0^{le_j}\left(A_j^{(n_s)}\right) = \frac{1}{n} \sum_{k \in J^{(\mu, s)}(j)} \left\{ \sum_{i=0}^{n-1} \alpha_\mu^{\delta_\mu^{(s)} j_\mu} \left(\prod_{\lambda=s+1}^{\mu-1} \alpha_\lambda^{i_\lambda (j_\lambda - (q^{e_j} k_\lambda)) + \delta_\lambda^{(s)} j_\lambda} \right) \alpha_s^{i_s (j_s - (q^{e_j} k_s)) + j_s} \right\} A_{q^{e_j}\lceil k \rceil}$$
$$= A_j^{(n_s)} \quad \text{since } \{ q^{e_j}\lceil k \rceil \mid k \in J^{(\mu, s)}(j) \} = J^{(\mu, s)}(j).$$

V. Enumeration of Codes and Dual Codes

In this section, we follow a general approach to enumerate all Abelian codes of a specified size satisfying a given constraint $\mathcal{D}$. Hence, we will be enumerating both n_s-QCA codes as well as U_b-invariant codes. We then show that using the transform domain characterization, it is easy to identify the dual of an n_s-QCA (resp., U_b-invariant Abelian) code which is also n_s-QCA (resp., U_b-invariant Abelian).

A. Enumeration of Abelian Codes Satisfying Constraint $\mathcal{D}$

Let a $n = m_{r-1}m_{r-2}\cdots m_0$-length Abelian code satisfy constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$. Including the two trivial codes (all-zero vector and GR$(p^a, l)^n$), there are $(a+1)^u$ Abelian codes over GR(p^a, l) satisfying the constraint $\mathcal{D}$.

In the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$, let $|\mathcal{D}_j| = d_j$. Therefore,

$$|\boldsymbol{L}| = \sum_{i=1}^{u} d_i.$$

Further, if $\mathcal{D}_j = \{j_1, j_2, \ldots, j_{d_j}\}$, let $e_{j1}, e_{j2}, \ldots, e_{jd_j}$ be the corresponding sizes of the cyclotomic cosets $\widehat{\lceil j_1 \rceil}, \widehat{\lceil j_2 \rceil}, \ldots, \widehat{\lceil j_{d_j} \rceil}$, respectively. For an $n = m_{r-1}m_{r-2}\cdots m_0$-length Abelian code of dimensions $k_0, \ldots, k_{a-1}$ satisfying the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$, the constrained set $\mathcal{D}_j$ contributes $e_{j1} + e_{j2} + \cdots + e_{jd_j}$ to the dimension k_{η_j}, when all the elements belonging to the constrained set $\mathcal{D}_j$ take values from η_j-ideal of their corresponding Galois subring.

Theorem 4: For any n and p such that $\gcd(n, p) = 1$, the number of Abelian codes over GR(p^a, l) of length $n = m_{r-1}m_{r-2}\cdots m_0$ and size $p^l\tau$ satisfying the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$, is the number of ways in which τ can be expressed as

$$\tau = \left\{(a-\eta_1)\sum_{i=1}^{d_1} e_{1i}\right\} + \cdots + \left\{(a-\eta_u)\sum_{i=1}^{d_u} e_{ui}\right\}$$

where $0 \le \eta_j \le a$ for all $j = 1, 2, \ldots, u$.

B. Dual Codes

If $\mathcal{C}$ is a GR(p^a, l)-linear code, its dual $\mathcal{C}^\perp$ is defined using the normal inner product

$$\mathcal{C}^\perp = \left\{\vec{y} \in \mathrm{GR}(p^a, l)^n \colon \sum_{i=0}^{n-1} x_i y_i = 0,\ \forall\, \vec{x} \in \mathcal{C}\right\}.$$

The following notion of dual cyclotomic cosets is used in describing the dual code pairs. For a given cyclotomic coset $\widehat{\lceil i \rceil}$, the cyclotomic coset $\widehat{\lceil n \ominus i \rceil}$ is called the dual cyclotomic coset. For any $i \in \boldsymbol{L}$, let $i^\perp \in \boldsymbol{L}$ denote the representative element of the dual cyclotomic coset $\widehat{\lceil n \ominus i \rceil}$. The dual of an Abelian code is also Abelian and the proof follows from the reasoning in [6], [35]. If $(T_0, T_1, \ldots, T_a)$ is the defining partition of an Abelian code $\mathcal{C}$, we use the notation $(T_0^\perp, T_1^\perp, \ldots, T_a^\perp)$ for the defining set of the dual code $\mathcal{C}^\perp$. If $\widehat{\lceil i \rceil} \subset T_\eta$ in $\mathcal{C}$, then for $\mathcal{C}^\perp$, the dual cyclotomic coset $\widehat{\lceil n \ominus i \rceil}$ is a subset of $T_{a-\eta}^\perp$.

Now, if an Abelian code satisfies the constraint $\mathcal{D}$, to prove that the dual code also satisfies the same constraint, we need to observe the following.

- If $\lceil j \rceil_{(b)}$ is a constrained set defined in Definition 6, then the set $\{i^\perp \mid i \in \lceil j \rceil_{(b)}\}$ is also a valid constrained set for U_b-invariant codes and it is actually equal to $\lceil j^\perp \rceil_{(b)}$.
- For $j \le n_{s+1} - 1$, i.e., if j is free then $j^\perp$ is also free and for $n_{s+1} \le j < n$, if $\lceil j \rceil_{\langle s \rangle}$ is a constrained set defined in Definition 8, then the set $\{i^\perp \mid i \in \lceil j \rceil_{\langle s \rangle}\}$ is also a valid constrained set for n_s-QCA codes and is equal to $\lceil j^\perp \rceil_{\langle s \rangle}$.

Example 7:

i) In Table IV(a), for $b = \lceil 1, 1, 2 \rceil$, $\lceil 1^\perp \rceil_{(b)} = \lceil 1 \rceil_{(b)}$, $\lceil 4^\perp \rceil_{(b)} = \lceil 7 \rceil_{(b)}$.

ii) For $b = \lceil 2, 2, 2 \rceil$, $\lceil j^\perp \rceil_{(b)} = \lceil j \rceil_{(b)}$ for all $j \in \boldsymbol{L}$.

iii) In Table IV(b), for $s = 1$, $\lceil 4^\perp \rceil_{\langle s \rangle} = \lceil 8 \rceil_{\langle s \rangle}$, $\lceil 9^\perp \rceil_{\langle s \rangle} = \lceil 18 \rceil_{\langle s \rangle}$ and for $s = 0$, $\lceil 3^\perp \rceil_{\langle s \rangle} = \lceil 6 \rceil_{\langle s \rangle}$, $\lceil 9^\perp \rceil_{\langle s \rangle} = \lceil 18 \rceil_{\langle s \rangle}$.

With this, and the characterization of dual Abelian codes, it is clear that if $\mathcal{C}$ is an Abelian code satisfying the constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$ such that $\mathcal{D}_k = \lceil j \rceil_{(b)} \subset T_\eta$ for U_b-invariance ($\mathcal{D}_k = \lceil j \rceil_{\langle s \rangle} \subset T_\eta$ for n_s-QC), the dual code is also an Abelian code satisfying the same constraint with $\mathcal{D}_{k'} = \lceil j^\perp \rceil_{(b)} \subset T_{a-\eta}^\perp$ (resp., $\mathcal{D}_{k'} = \lceil j^\perp \rceil_{\langle s \rangle} \subset T_{a-\eta}^\perp$) for some $k' \in \{1, 2, \ldots, u\}$.

Example 8: For the parameters discussed in Example 2, the code corresponding to $\boldsymbol{C_j} = 2\mathrm{GR}(2^2, 2)$ for all $j \in I_n$ is a self-dual code. This self-dual Abelian code corresponds to the defining partition (T_0, T_1, T_2) where $T_0 = T_2 = \emptyset$ and $T_1 = I_n$. It is interesting to note that this Abelian code is cyclic as well as U_b-invariant for all b. In fact, this code should satisfy any general constraint $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_u\}$ (more than the two mentioned in this correspondence) since $T_1 = I_n = \mathcal{D}$.

VI. Discussion

In this correspondence, we have characterized Abelian codes over Galois rings using a generalized DFT defined over a suitable extension of the Galois ring. We have then characterized Abelian codes which are also n_s-QC and U_b-invariant. QCA codes have the advantage over QC-only codes in the sense that, in certain cases they need a smaller extension field for DFT characterization. It would be interesting to see if this additional structure in the code could be exploited to develop good or more efficient decoding algorithms. We have enumerated all the QCA codes and U_b-invariant Abelian codes of a given length and we have shown that the dual of a QCA code or a U_b-invariant Abelian code is also a QCA code or a U_b-invariant Abelian code, respectively.

In [36], a Gray isometry (from GR$(p^a, l)^n$ to F_q^n) for codes over Galois rings was defined and using this map, a nonlinear $(36, 3^{12}, 15)$ code, the best known code for these parameters, was constructed as the image of a Z_9-lift of the ternary Golay code. It is interesting to see if the Gray image of codes over GR(p^a, l) discussed in this correspondence give any good codes over the base field F_q.

Acknowledgment

The authors are grateful to the reviewers for their suggestions and comments which helped to improve the content as well as the presentation of this correspondence.

References

[1] S. D. Berman, "On the theory of group codes," *Kibernetika*, vol. 3, no. 1, pp. 31–39, 1967.

[2] ——, "Semi-simple cyclic and Abelian codes," *Kibernetika*, no. 3, pp. 21–30, 1967.

[3] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an Abelian group," *Bell Syst. Tech. J.*, vol. 49, pp. 987–1011, 1970.

[4] P. Delsarte, "Automorphisms of Abelian codes," *Philips Res. Rep.*, vol. 25, pp. 389–402, 1970.

[5] P. Camion, "Abelian codes," Univ. Wisconsin, Madison, Math. Res. Ctr., Tech. Rep 1059, 1971.
[6] 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.
[7] ——, "Transform domain characterization of Abelian codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1817–1821, Nov. 1992.
[8] H. Chabanne, "Gröbner bases and Abelian codes," in *EUROCODE*, P. Chappin, P. Camion, and S. Harari, Eds. Berlin, Germany: Springer-Verlag, Oct. 1992, pp. 255–266.
[9] B. R. McDonald, *Finite Rings With Identity*. New York: Marcel Dekker, 1974.
[10] I. F. Blake, "Codes over certain rings," *Inform. Contr.*, vol. 20, pp. 396–404, 1972.
[11] ——, "Codes over integer residue rings," *Inform. Contr.*, vol. 29, pp. 295–300, 1975.
[12] E. Spiegel, "Codes over Z_m," *Inform. Contr.*, vol. 35, pp. 48–51, 1977.
[13] ——, "Codes over Z_m, revisited," *Inform. Contr.*, vol. 37, pp. 100–104, 1978.
[14] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–319, Mar. 1994.
[15] 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.
[16] A. Ashikhmin, "On generalized Hamming weights for Galois ring linear codes," *Des., Codes, Cryptogr.*, vol. 14, no. 2, pp. 107–126, May 1998.
[17] 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.
[18] C. Carlet, "More correlation-immune and resilient functions over Galois fields and Galois rings," in *EUROCRYPT'97, Advances in Cryptology (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, vol. 1233, pp. 422–433.
[19] D. K. Ray-Chaudhuri and Q. Xiang, "Constructions of partial difference sets and relative difference sets using Galois rings," *Des., Codes, Cryptogr.*, vol. 8, pp. 215–227, May 1996.
[20] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic codes," *Des., Codes, Cryptogr*, vol. 6, pp. 21–35, 1995.
[21] E. Byrne and P. Fitzpatrick, "Gröbner bases over Galois rings with an application to decoding," *J. Symb. Comp.*, vol. 31, pp. 565–584, 2001.
[22] ——, "Hamming metric decoding of alternant codes over Galois rings," *IEEE Trans. Inform. Theory*, vol. 48, pp. 683–694, Mar. 2002.
[23] 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.
[24] H. Chabanne, "Permutation decoding of Abelian codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1826–1829, Nov. 1992.
[25] J. Conan and G. Seguin, "Structural properties and enumeration of quasi cyclic codes," *Applic. Alg. in Eng., Commun. and Comput.*, pp. 25–39, 1993.
[26] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1988.
[27] M. Esmaeili, T. A. Gulliver, N. P. Secord, and S. A. Mahmoud, "A link between quasicyclic codes and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 431–435, Jan. 1998.
[28] 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.
[29] R. M. Tanner, "A transform theory for a class of group—Invariant codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 752–775, July 1988.
[30] 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, Nov. 2001, vol. 2227, pp. 67–76.
[31] B. S. Rajan and M. H. Lee, "Quasicyclic dyadic codes in Walsh–Hadamard transform domain," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2406–2412, Aug. 2002.
[32] R. E. Blahut, *Theory and Practice of Error Control Codes*. Reading, MA: Addison-Wesley, 1982.
[33] W. C. Huffman, "Decompositions and extremal Type II codes over Z_4," *IEEE Trans. Inform. Theory*, vol. 44, pp. 800–809, Mar. 1998.
[34] R. Lidl and H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and Its Applications Vol. 20)*. Cambridge, U.K.: Cambridge Univ. Press.
[35] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of cyclic codes over Z_m," *Appl. Alg. in Eng., Commun. and Comput.*, vol. 5, no. 5, pp. 261–276, 1994.
[36] M. Greferath and S. E. Schmidt, "Gray isometries for finite chain rings and a nonlinear ternary code $(36, 3^{12}, 15)$ code," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2522–2524, Nov. 1999.

Cubic Self-Dual Binary Codes

Alexis Bonnecaze, *Member, IEEE*, Anne Desideri Bracco, Steven T. Dougherty, Luz R. Nochefranca, and Patrick Solé, *Member, IEEE*

***Abstract*—We study binary self-dual codes with a fixed point free automorphism of order three. All binary codes of that type can be obtained by a cubic construction that generalizes Turyn's. We regard such "cubic" codes of length 3ℓ as codes of length ℓ over the ring $\mathbb{F}_2 \times \mathbb{F}_4$. Classical notions of Type II codes, shadow codes, and weight enumerators are adapted to that ring. Two infinite families of cubic codes are introduced. New extremal binary codes in lengths ≤ 66 are constructed by a randomized algorithm. Necessary conditions for the existence of a cubic $[72, 36, 16]$ Type II code are derived.**

***Index Terms*—Automorphism group, codes over rings, self-dual codes.**

I. Introduction

The construction of binary self-dual codes with an automorphism of given odd order has received a lot of attention over the years [14].

In this correspondence, we consider the case of an automorphism of order three without a fixed point. It was shown in [15] that all such codes can be obtained by a generalized cubic construction from a binary code and a quaternary code both of length ℓ. From now on, we will call such codes "**cubic**."

We view cubic codes as codes of length ℓ over the ring $\mathbb{F}_2 \times \mathbb{F}_4$. We study self-dual codes over that alphabet and adapt to that ring the classical tools in the study of self-dual codes: Type II codes, shadow codes, weight enumerators, and invariant theory. We give two infinite families of cubic self-dual codes related to quadratic residue (QR) codes and Reed–Muller (RM) codes, respectively. We give examples of extremal self-dual cubic codes for $\ell \leq 22$, and thereby examples of the application of the tools developed. Necessary conditions for the existence of a putative cubic Type II $[72, 36, 16]$ are derived.

Manuscript received October 3, 2001; revised April 8, 2003. This work was performed while A. Bonnecaze was visiting INRIA project GALAAD at Sophia Antipolis, France.

A. Bonnecaze is with the IAAI, 13003 Marseille, France (e-mail: Alexis.Bonnecaze@iaai.fr).

A. Desideri Bracco and P. Solé are with the CNRS, I3S ESSI, 06 903 Sophia Antipolis, France (e-mail: adbracco@essi.fr; ps@essi.fr).

S. T. Dougherty is with the Department of Mathematics, University of Scranton, Scranton, PA 18510 USA (e-mail: doughertys1@uofs.edu).

L. R. Nochefranca is with the Department of Mathematics, University of the Philippines, Diliman, 1101 Quezon City, Philippines (e-mail: sole@diamant.unice.fr).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.815800