Duadic codes over $\mathbb{Z}_2^k$

Ling, San; Solé, Patrick

2001

Ling, S. & Solé, P. (2001). Duadic codes over $\mathbb{Z}_2^k$. IEEE Transactions on Information Theory, 47(4), 1581-1588.

<https://hdl.handle.net/10356/95881>

<https://doi.org/10.1109/18.923740>

© 2001 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [DOI: <http://dx.doi.org/10.1109/18.923740>].

Downloaded on 26 Apr 2023 21:29:07 SGT

Duadic Codes over $\mathbf{Z}_{2k}$

San Ling and Patrick Solé, *Member, IEEE*

Abstract—Duadic codes constitute a well-known family of binary cyclic codes. They are generalized in this correspondence to the setting of Abelian codes over the ring $\mathbf{Z}_{2k}$. Self-duality, isoduality, and Type II properties are studied.

Index Terms—Abelian codes, duadic codes, isodual, self-dual, splitting, Type II codes.

I. INTRODUCTION

There has been much interest and research in codes over finite rings, especially the ring $\mathbf{Z}_4$ of integers modulo 4, over recent years. Much research has been done on cyclic codes over such rings, self-duality, Type II property, links to the construction of unimodular lattices, etc., [1], [3], [2], [7]–[10], [16]–[18]. More recently, Langevin and Solé [14] introduced the notion of duadic $\mathbf{Z}_4$ -codes and studied some properties of such codes. These codes generalize the class of supplemented quadratic residue codes over $\mathbf{Z}_4$ in the same way that duadic codes over fields generalize quadratic residue codes over fields.

In this correspondence, we extend the notion of duadic codes to the rings $\mathbf{Z}_{p^m}$ (p prime and m an integer) and $\mathbf{Z}_{2k}$ (k an integer), and study their properties as well as those of their augmented and extended codes. The organization of the correspondence is as follows. After some recollection of definitions in Section II, we define duadic codes and generalized duadic codes over $\mathbf{Z}_{p^m}$ in Section III, and study the problem of self-duality and isoduality of such codes. In Section IV, we characterize the augmented and extended Abelian codes over $\mathbf{Z}_{p^m}$ that are self-dual or isodual by a multiplier and link them to the generalized duadic codes. In Section V, the self-dual augmented and extended Abelian codes over $\mathbf{Z}_{2^m}$ which are of Type II are characterized. Finally, in Section VI, we define duadic codes and generalized duadic codes over $\mathbf{Z}_{2k}$ and prove some results on self-duality, isoduality, and Type II property of Abelian $\mathbf{Z}_{2k}$ codes. For completeness, an appendix containing some discussion on the Fourier transform is also included.

II. PRELIMINARIES

A code of length n over $\mathbf{Z}_r$ is simply a nonempty subset of $\mathbf{Z}_r^n$. A linear code C of length n over $\mathbf{Z}_r$ is an additive subgroup of $\mathbf{Z}_r^n$. In this correspondence, we consider only linear codes over $\mathbf{Z}_r$. An element of C is called a codeword of C . The Hamming weight $w_H(\mathbf{c})$ of a codeword $\mathbf{c}$ is the number of nonzero coordinates. The (Euclidean) inner product $\langle \mathbf{c}, \mathbf{c}' \rangle$ of two elements $\mathbf{c} = (c_1, c_2, \dots, c_n)$ and $\mathbf{c}' = (c'_1, c'_2, \dots, c'_n)$ of $\mathbf{Z}_r^n$ is defined as

$$\langle \mathbf{c}, \mathbf{c}' \rangle = \sum_{i=1}^n c_i c'_i \bmod r.$$

The dual code $C^\perp$ of C is defined as

$$C^\perp = \{\mathbf{x} \in \mathbf{Z}_r^n \mid \langle \mathbf{x}, \mathbf{c} \rangle = 0 \text{ for all } \mathbf{c} \in C\}.$$

If $C \subseteq C^\perp$, we say that C is self-orthogonal. If $C = C^\perp$, then C is said to be self-dual.

When $r = 2k$ is even, such codes were first introduced and studied in [1] and subsequently in [8]. Two codes over $\mathbf{Z}_{2k}$ are said to be equivalent if one can be obtained from another by permuting the coordinates and, if necessary, changing the signs of certain coordinates. A code over $\mathbf{Z}_{2k}$ is said to be isodual if it is equivalent to its dual.

When $r = 2k$, the Euclidean weight $w_E(\mathbf{c})$ of a codeword $\mathbf{c} = (c_1, c_2, \dots, c_n)$ is defined to be

$$w_E(\mathbf{c}) = \sum_{i=1}^n \min\{c_i^2, (2k - c_i)^2\}.$$

A Type II code over $\mathbf{Z}_{2k}$ is a self-dual code over $\mathbf{Z}_{2k}$ in which all the Euclidean weights are multiples of $4k$. A self-dual code over $\mathbf{Z}_{2k}$ that is not of Type II is said to be of Type I.

For any C over $\mathbf{Z}_r$ and $\epsilon \in \mathbf{Z}_r$, we define the extended code C_ϵ to be the code obtained by appending to each codeword $\mathbf{c} = (c_1, \dots, c_n) \in C$ an overall “parity-check” coordinate $c_{\infty, \epsilon} = \epsilon \sum c_i$. By the augmented code $\overline{C}$, we mean the code $C + \text{span}\{\mathbf{1}\}$, where $\mathbf{1}$ is the all-one vector and $\text{span}\{\mathbf{v}\}$ is the $\mathbf{Z}_r$ -span of the vector $\mathbf{v}$. The augmented and extended code $\overline{C}_\epsilon$ is

$$\overline{C}_\epsilon = \{(\mathbf{c}, c_{\infty, \epsilon}) + \lambda(\mathbf{1}, \epsilon n) \mid \mathbf{c} \in C, \lambda \in \mathbf{Z}_r\}.$$

It is obtained by first augmenting C and then extending the augmented code with the parity check corresponding to ϵ .

III. DUADIC CODES

An Abelian code over $\mathbf{Z}_r$ is defined to be an ideal in the group ring $\mathbf{Z}_r[G]$, where G is a finite Abelian group whose order is prime to r . The elements of $\mathbf{Z}_r[G]$ may be written as formal polynomials $\sum_{g \in G} c_g X^g$, where $c_g \in \mathbf{Z}_r$. The group ring $\mathbf{Z}_r[G]$ is equipped with the usual componentwise addition and convolution product.

Duadic $\mathbf{Z}_4$ -codes were introduced and studied in [14]. We extend and generalize this notion in this section to the rings $\mathbf{Z}_{p^m}$, where p is any prime and m is any positive integer.

We first recall some definitions and results in [14].

Let $\text{GR}(p^m, d)$ be the unique Galois extension of $\mathbf{Z}_{p^m}$ of degree d . Let $O_0, O_1, \dots, O_s$ be the orbits of G (of order prime to p) under the map $x \mapsto px$ and let d_i denote the size of O_i . Since $O_0 = \{0\}$, we see that $d_0 = 1$ and, therefore, that $\text{GR}(p^m, d_0) = \mathbf{Z}_{p^m}$. Let σ denote the permutation of $\{0, 1, \dots, s\}$ induced by the map $x \mapsto -x$ on G . We then have the following facts (cf. [14, Theorem 5.1, Corollary 5.2, Theorem 7.3]).

Theorem 3.1:

- 1) There is a ring isomorphism between $\mathbf{Z}_{p^m}[G]$ and the product of rings $\mathbf{Z}_{p^m} \times \text{GR}(p^m, d_1) \times \dots \times \text{GR}(p^m, d_s)$.
- 2) Every ideal of $\mathbf{Z}_{p^m}[G]$ can be expressed as $I_0 \times I_1 \times \dots \times I_s$, where I_i is one of the ideals $(1) \ (n) \ (n^2) \ \dots \ (n^{m-1}) \ (n)$

$I_{\sigma(1)} \times \dots \times I_{\sigma(s)}$, where $(0)^o := (1)$, $(1)^o := (0)$ and, for $1 \leq i \leq m-1$, $(p^i)^o := (p^{m-i})$.

Remark: The isomorphism in Theorem 3.1, part 1) is obtained via the Fourier transform. The Fourier transform $\hat{\mathbf{c}} = \sum_{h \in G} \hat{c}_h X^h$ of a codeword $\sum_{g \in G} c_g X^g$ is defined in [14, Sec. 4]. Some elementary properties of the Fourier transform are also given there. Some further discussion on the Fourier transform is also included in the Appendix.

S. Ling is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: lings@math.nus.edu.sg).

P. Solé is with CNRS Laboratory I3S, ESSI, 06 903 Sophia Antipolis, France (e-mail: ps@essi.fr).

Communicated by I. F. Blake, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)02850-4.

We note in particular that, if $h \in O_j$, then $\hat{c}_h \in \text{GR}(p^m, d_j)$. Moreover,

$$\hat{c}_0 = \sum_{g \in G} c_g \in I_0 \subseteq \mathbf{Z}_{p^m}$$

for a codeword $\mathbf{c} \in I_0 \times I_1 \times \cdots \times I_s$. Therefore, the overall parity-check coordinate of a codeword $\mathbf{c}$ is $c_{\infty, \epsilon} = \epsilon \hat{c}_0 \in I_0$.

A *splitting* (X, A, B) of the group G is a partition of G such that X, A , and B are unions of orbits and $\alpha(A) = B$ and $\alpha(B) = A$, where α is an automorphism of G . In particular, $0 \in X$ and $\alpha(X) = X$. Let τ be the permutation on $\{0, 1, \dots, s\}$ induced by the map $x \mapsto \alpha x$. In particular, when $\alpha = -1$, we have $\tau = \sigma$. For any ideal $I = I_0 \times I_1 \times \cdots \times I_s$ of $\mathbf{Z}_{p^m}[G]$, we call the ideal $I^\alpha := I_{\tau(0)} \times I_{\tau(1)} \times \cdots \times I_{\tau(s)}$ the image of I under the multiplier α . It is the image of I under the isometry

$$\sum c_g X^g \mapsto \sum c_g X^{\alpha^* g}$$

where α^* , the adjoint of α , is an automorphism of G (see the Appendix). The ideal I is said to be isodual by the multiplier α if $I^\alpha = I^\perp$.

We define a *duadic code* over $\mathbf{Z}_{p^m}$ attached to the splitting (X, A, B) of G to be an ideal $I_0 \times I_1 \times \cdots \times I_s$ of $\mathbf{Z}_{p^m}[G]$ which satisfies the following: if $O_j \subseteq A \cup B$, then $I_j = (p^i)$ if and only if $I_{\tau(j)} = (p^{m-i})$, and if $O_j \subseteq X$, then $I_j = (p^{m/2})$. Obviously, this means that duadic codes over $\mathbf{Z}_{p^m}$ only exist if m is even. Note that when $p^m = 4$, this definition includes those duadic codes defined in [14]. When m is even, the ideal $I_0 \times I_1 \times \cdots \times I_s$ with $I_j = (p^{m/2})$, for all $0 \leq j \leq s$, is clearly self-dual. It is called the trivial self-dual ideal. It has been noted in [14, Proposition 7.5] that there is no nontrivial Abelian self-dual code in $\mathbf{Z}_{p^m}[G]$ with m even and $(n, p) = 1$ if and only if σ is the identity.

For any positive integer m , a *generalized duadic code* over $\mathbf{Z}_{p^m}$ is defined in the same way as a duadic code, except that the ideal I_0 is allowed to be any of the ideals $(1), (p), (p^2), \dots, (p^{m-1}), (0)$. In particular, when m is odd, a generalized duadic code exists if and only if there exists a splitting (X, A, B) with $X = \{0\}$. This also implies that n is odd when m is odd.

Theorem 3.2: Suppose that m is even and that there is a splitting (X, A, B) of G given by $\alpha = -1$. Then the duadic code attached to the splitting (X, A, B) is self-dual. Conversely, every self-dual Abelian code over $\mathbf{Z}_{p^m}$ is a duadic code attached to a splitting of G with $\alpha = -1$.

Proof: The first statement follows immediately from the definition of duadic codes and Theorem 3.1, part 3). For the second statement, given a self-dual Abelian code $C = I_0 \times I_1 \times \cdots \times I_s$, we first note that $I_0 = (p^{m/2})$. Set X to be the union of the orbits O_j where $I_j = (p^{m/2})$, set A to be the union of the orbits O_j where $I_j = (p^i)$ with $i < m/2$ and let B be the union of orbits O_j where $I_j = (p^i)$ with $i > m/2$. The self-duality of the given code C means that (X, A, B) is a splitting of G given by $\alpha = -1$ and that C is a duadic code attached to this splitting. This completes the proof of Theorem 3.2.

Remarks:

- 1) In Theorem 3.2, the trivial self-dual ideal where $I_j = (p^{m/2})$ for all $0 \leq j \leq s$ corresponds to the degenerate splitting $(G, \emptyset, \emptyset)$ of G .
- 2) Theorem 3.2 generalizes [14, Theorem 7.7].

The following theorem can be proved easily, so we omit the proof.

Theorem 3.3: Let $C = I_0 \times I_1 \times \cdots \times I_s$ be a generalized duadic code over $\mathbf{Z}_{p^m}$ attached to a splitting of G with $\alpha = -1$. If $I_0 = (p^i)$ where $i \geq m/2$, then C is self-orthogonal.

Using exactly the same technique as above, one can also obtain the following results on isodual codes.

Theorem 3.4: Assume that σ is the identity.

- 1) Suppose that m is even and that there is a splitting (X, A, B) of G . Then the duadic code attached to the splitting (X, A, B) is isodual. Conversely, every Abelian code over $\mathbf{Z}_{p^m}$ isodual by a multiplier is a duadic code attached to a splitting of G .
- 2) Let $C = I_0 \times I_1 \times \cdots \times I_s$ be a generalized duadic code over $\mathbf{Z}_{p^m}$ attached to a splitting of G given by α . If $I_0 = (p^i)$ where $i \geq m/2$, then $C^\alpha \subseteq C^\perp$.

IV. AUGMENTED AND EXTENDED ABELIAN CODES OVER $\mathbf{Z}_{p^m}$

A. Self-Duality

In this section, we begin by characterizing the self-dual augmented and extended codes of generalized duadic codes over $\mathbf{Z}_{p^m}$, where p is a prime. Then we show that any self-dual augmented and extended code of a given Abelian code over $\mathbf{Z}_{p^m}$ must, in fact, be the augmented and extended code of a generalized duadic code.

Let (X, A, B) be a splitting of G given by $\alpha = -1$ and let C be a generalized duadic code over $\mathbf{Z}_{p^m}$ attached to this splitting. We first study the augmented and extended code $\overline{C}_\epsilon$.

Theorem 4.1: Let G be an Abelian group of order n , let (X, A, B) be a splitting of G given by $\alpha = -1$, and let C be an attached generalized duadic code over $\mathbf{Z}_{p^m}$. Then, for $\epsilon \in \mathbf{Z}_{p^m}$, the code $\overline{C}_\epsilon$ is self-dual if and only if $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$.

Proof: If $\overline{C}_\epsilon$ is self-dual, then by considering the inner product $\langle (1, \epsilon n), (1, \epsilon n) \rangle = 0$, it follows that $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$.

Now we assume that $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$. We note first that $\overline{C}_\epsilon$ has exactly $p^{m(n+1)/2}$ elements. We also note that the choice of the ideal I_0 is irrelevant when we consider the augmented and extended code. Therefore, by Theorem 3.3, we may assume that C is self-orthogonal.

For codewords $\mathbf{c}, \mathbf{c}' \in C$, we have the following:

$$\langle (\mathbf{c}, c_{\infty, \epsilon}), (\mathbf{c}', c'_{\infty, \epsilon}) \rangle = 0 \quad (1)$$

$$\langle (\mathbf{c}, c_{\infty, \epsilon}), (1, \epsilon n) \rangle = 0 \quad (2)$$

$$\langle (1, \epsilon n), (1, \epsilon n) \rangle = 0. \quad (3)$$

Equation (1) is true because C is self-orthogonal and $c_{\infty, \epsilon}, c'_{\infty, \epsilon} \in (p^i)$ where $i \geq m/2$ (cf. Remark after Theorem 3.1); for (2), the left-hand side is equal to $(\epsilon^2 n + 1) \sum c_i$, while for (3), the left-hand side is $(\epsilon^2 n + 1)n$. Both give 0 because $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$.

By the $\mathbf{Z}_{p^m}$ -linearity of the inner product, it therefore follows that $\overline{C}_\epsilon$ is self-orthogonal. By considering the cardinality of $\overline{C}_\epsilon$, it follows, therefore, that $\overline{C}_\epsilon$ is self-dual. This completes the proof of Theorem 4.1.

Now let C be an Abelian code in $\mathbf{Z}_{p^m}[G]$ for some Abelian group G of order n . Suppose that $\overline{C}_\epsilon$ is self-dual. We show the following.

Theorem 4.2: Let C be an Abelian code in $\mathbf{Z}_{p^m}[G]$, for some Abelian group G of order n , such that $\overline{C}_\epsilon$ is self-dual for some ϵ . Then $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$ and C is a generalized duadic code attached to a splitting (X, A, B) of G given by $\alpha = -1$. In particular, when m is even, any self-dual augmented and extended Abelian code over $\mathbf{Z}_{p^m}$ is the augmented and extended code of a duadic code attached to a splitting (X, A, B) of G given by $\alpha = -1$.

Proof: Since $(1, \epsilon n) \in \overline{C}_\epsilon$, the self-duality of $\overline{C}_\epsilon$ implies that $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$.

Write C as $I_0 \times I_1 \times \cdots \times I_s$ as before. Consider the orbits in $G \setminus \{0\}$. Let X' denote the union of the orbits O_j where $I_j = (p^{m/2})$ (hence, X' is empty if m is odd); let A be the union of the orbits O_j

where $I_j = (p^i)$ with $i < m/2$; and let B denote the union of orbits O_j where $I_j = (p^i)$ with $i > m/2$. It is clear that $\overline{C} := C + \text{span}\{\mathbf{1}\}$ is also an ideal in $\mathbf{Z}_{p^m}[G]$. In fact, it is $\overline{I}_0 \times I_1 \times \cdots \times I_s$, where $\overline{I}_0 = (1)$. Recall that $C^\perp$ is the ideal $I_{\sigma(0)}^\circ \times \cdots \times I_{\sigma(s)}^\circ$.

For $\mathbf{c} \in C$ and $\mathbf{c}' \in C^\perp$, recall that $c_{\infty, \epsilon} = \epsilon \hat{c}_0 \in I_0$ and $c'_{\infty, \epsilon} = \epsilon \hat{c}'_0 \in I_0^\circ$. Then we have

$$\langle (\mathbf{c}, c_{\infty, \epsilon}), (\mathbf{c}', c'_{\infty, \epsilon}) \rangle = 0. \quad (4)$$

It is also easy to see that we have

$$\langle (\mathbf{1}, \epsilon n), (\mathbf{c}', c'_{\infty, \epsilon}) \rangle = 0. \quad (5)$$

Therefore, $(C^\perp)_\epsilon \subseteq (\overline{C}_\epsilon)^\perp = \overline{C}_\epsilon$, from which it follows that $C^\perp \subseteq \overline{C}$.

If $I_0 = (p^i)$, then the index $[\overline{C} : C] = p^i$. Moreover, since $C^\perp \subseteq \overline{C}$, by considering the cardinality of $C^\perp$ and $\overline{C}$, it follows that the index $[\overline{C} : C^\perp] = p^{m-i}$. This means in particular that $I_{\sigma(j)}^\circ = I_j$ for all $1 \leq j \leq s$. This implies that $(X' \cup \{0\}, A, B)$ gives a splitting of G with $\alpha = -1$ and C is a generalized duadic code attached to this splitting.

The last statement of the theorem is obvious, since taking the augmentation of a code renders irrelevant what I_0 is.

This completes the proof of Theorem 4.2.

Remark: The flexibility in the choice of I_0 is useful later when we consider which self-dual extended and augmented Abelian codes over $\mathbf{Z}_{p^m}$ are of Type II when $p = 2$.

B. Isoduality

For C an Abelian code in $\mathbf{Z}_{p^m}[G]$, a multiplier α acts on C by permutation of the coordinates. In particular, the parity-check coordinate of a codeword $\mathbf{c}$ is the same as that of its image $\mathbf{c}^\alpha$ under the multiplier. We define the action of a multiplier α on the augmented and extended code $\overline{C}_\epsilon$ by the rule $(\mathbf{c}, c_{\infty, \epsilon}) \mapsto (\mathbf{c}^\alpha, c_{\infty, \epsilon})$. Therefore, $(\overline{C}_\epsilon)^\alpha = ((\overline{C})^\alpha)_\epsilon$. We say that the augmented and extended code $\overline{C}_\epsilon$ is isodual by a multiplier α if $(\overline{C}_\epsilon)^\perp = ((\overline{C})^\alpha)_\epsilon$. We have the following results on isoduality. We continue to assume that σ is the identity.

Theorem 4.3: Let G be an Abelian group of order n , let (X, A, B) be a splitting of G given by α , and let C be an attached generalized duadic code over $\mathbf{Z}_{p^m}$. Then, for $\epsilon \in \mathbf{Z}_{p^m}$, the code $\overline{C}_\epsilon$ is isodual by the multiplier α if and only if $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$.

Theorem 4.4: Let C be an Abelian code in $\mathbf{Z}_{p^m}[G]$, for some Abelian group G of order n , such that, for some ϵ , $\overline{C}_\epsilon$ is isodual by a multiplier α . Then, $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$ and C is a generalized duadic code attached to a splitting (X, A, B) of G given by α . In particular, when m is even, any augmented and extended Abelian code over $\mathbf{Z}_{p^m}$ that is isodual by a multiplier α is the augmented and extended code of a duadic code attached to a splitting (X, A, B) of G given by α .

The proofs of these two theorems are essentially the same as those for Theorems 4.1 and 4.2, using the following observations:

- 1) a multiplier leaves the parity-check coordinate of every codeword unchanged while acts as a permutation on the other coordinates;
- 2) the $\mathbf{c}'$ in the proof of Theorem 4.1 should be taken to be in C^α ;
- 3) due to the isoduality of $\overline{C}_\epsilon$ by the multiplier α , the containment $C^\perp \subseteq \overline{C}$ in the proof of Theorem 4.2 is now replaced by $C^\perp \subseteq \overline{C}^\alpha$. The same argument then yields $I_{\tau(j)}^\circ = I_j^\circ$ for all $1 \leq j \leq s$, a condition needed for the existence of the required splitting given by α .

V. TYPE II CODES OVER $\mathbf{Z}_{2^m}$

We assume in this section that $p = 2$. Recall that a Type II code over $\mathbf{Z}_{2^m}$ is a self-dual code over $\mathbf{Z}_{2^m}$ in which all the Euclidean weights are multiples of 2^{m+1} . The main result in this section is as follows.

Theorem 5.1: A self-dual augmented and extended Abelian code $\overline{C}_\epsilon$ over $\mathbf{Z}_{2^m}$ of length n is of Type II if and only if

$$\epsilon^2 n + 1 \equiv 0 \pmod{2^{m+1}}.$$

Before we prove Theorem 5.1, we begin with a couple of preliminary results. Recall that the inner product $\langle \mathbf{c}, \mathbf{c}' \rangle$ of two words in a given $\mathbf{Z}_{2^m}$ -code is an element of $\mathbf{Z}_{2^m}$. By abuse of notation, we can also regard $\langle \mathbf{c}, \mathbf{c}' \rangle$ as one of the elements $0, 1, \dots, 2^m - 1$ of $\mathbf{Z}_{2^{m+1}}$.

Lemma 5.2: For any two codewords $\mathbf{c}$ and $\mathbf{c}'$ in a given $\mathbf{Z}_{2^m}$ -code, we have

$$w_E(\mathbf{c} + \mathbf{c}') \equiv w_E(\mathbf{c}) + w_E(\mathbf{c}') + 2\langle \mathbf{c}, \mathbf{c}' \rangle \pmod{2^{m+1}}.$$

Proof: It suffices to prove the lemma in the case where the length of $\mathbf{c}$ and $\mathbf{c}'$ is one. In this case, the lemma is easily verified to be true by considering all the possible values for $\mathbf{c}$ and $\mathbf{c}'$.

Proposition 5.3: Let C be a generalized duadic $\mathbf{Z}_{2^m}$ -code, with $I_0 = (0)$, attached to a splitting of G with $\alpha = -1$. Then the Euclidean weights of all the codewords in C are congruent to $0 \pmod{2^{m+1}}$.

Proof: Since C is self-orthogonal by Theorem 3.3, $\langle \mathbf{c}, \mathbf{c}' \rangle \equiv 0 \pmod{2^m}$ for all $\mathbf{c}, \mathbf{c}' \in C$. Therefore, for all $\mathbf{c}$ and $\mathbf{c}'$ in C , we have from Lemma 5.2

$$w_E(\mathbf{c} + \mathbf{c}') \equiv w_E(\mathbf{c}) + w_E(\mathbf{c}') \pmod{2^{m+1}}.$$

This implies that the map

$$\begin{aligned} w_E : C &\longrightarrow \mathbf{Z}_{2^{m+1}} \\ \mathbf{c} &\longmapsto w_E(\mathbf{c}) \end{aligned}$$

is a group homomorphism. The image of this homomorphism is in $2^m \mathbf{Z}_{2^{m+1}}$, since C is self-orthogonal implies that

$$w_E(\mathbf{c}) \equiv \langle \mathbf{c}, \mathbf{c} \rangle \equiv 0 \pmod{2^m}.$$

It is also easy to see that the kernel K of this map is an ideal in $\mathbf{Z}_{2^m}[G]$. Therefore, K is an ideal contained in C of index 1 or 2. Write C as $I_0 \times I_1 \times \cdots \times I_s$ and write K as $I'_0 \times I'_1 \times \cdots \times I'_s$, where $I'_j \subseteq I_j$ for all $0 \leq j \leq s$. Since the only orbit of G of size 1 is the orbit $\{0\}$, this means that $I_j = I'_j$ for all $1 \leq j \leq s$ and I'_0 is of index 1 or 2 in I_0 . However, $I_0 = (0)$ and hence cannot contain an ideal of index 2. Therefore, $K = C$, i.e., all the codewords in C have Euclidean weights congruent to $0 \pmod{2^{m+1}}$. This proves the proposition.

We are now ready to prove Theorem 5.1.

Proof of Theorem 5.1: Since a self-dual augmented and extended Abelian $\mathbf{Z}_{2^m}$ -code $\overline{C}_\epsilon$ contains $(\mathbf{1}, \epsilon n)$, the assumption that such a code is of Type II implies that $\epsilon^2 n + 1 \equiv 0 \pmod{2^{m+1}}$.

Conversely, suppose that $\epsilon^2 n + 1 \equiv 0 \pmod{2^{m+1}}$. Let the given self-dual augmented and extended Abelian $\mathbf{Z}_{2^m}$ -code be $\overline{C}_\epsilon$, where C is a generalized duadic code, attached to a splitting (X, A, B) of the underlying group G with $\alpha = -1$, and such that $I_0 = (0)$. We may make such an assumption on C because of Theorem 4.2.

We need to show that all words of the form $(\mathbf{c}, c_{\infty, \epsilon}) + \lambda(\mathbf{1}, \epsilon n)$ have Euclidean weights congruent to 0 mod 2^{m+1} , where $\mathbf{c} \in C$ and $\lambda \in \mathbf{Z}_{2^m}$. By the choice of C above, $c_{\infty, \epsilon} = 0$ for all $\mathbf{c} \in C$. We have

$$\begin{aligned} w_E((\mathbf{c}, 0) + \lambda(\mathbf{1}, \epsilon n)) \\ &\equiv w_E((\mathbf{c}, 0)) + w_E(\lambda(\mathbf{1}, \epsilon n)) + 2\langle (\mathbf{c}, 0), \lambda(\mathbf{1}, \epsilon n) \rangle \\ &\equiv 0 \pmod{2^{m+1}} \end{aligned}$$

since

$$w_E((\mathbf{c}, 0)) = w_E(\mathbf{c}) \equiv 0 \pmod{2^{m+1}}$$

by Proposition 5.3

$$w_E(\lambda(\mathbf{1}, \epsilon n)) \equiv 0 \pmod{2^{m+1}}$$

since $\epsilon^2 n + 1 \equiv 0 \pmod{2^{m+1}}$, and

$$\langle (\mathbf{c}, 0), \lambda(\mathbf{1}, \epsilon n) \rangle = \lambda \sum c_i \equiv 0 \pmod{2^m}.$$

This completes the proof of Theorem 5.1.

VI. ABELIAN CODES OVER $\mathbf{Z}_{2k}$

We return now to study Abelian codes over $\mathbf{Z}_{2k}$.

Let $2k = p_1^{m_1} \cdots p_t^{m_t}$ be the prime power decomposition of $2k$, where $p_1 = 2$ and the p_i ($2 \leq i \leq t$) are distinct odd primes.

Recall that an Abelian code over $\mathbf{Z}_{2k}$ is an ideal in the group ring $\mathbf{Z}_{2k}[G]$ for some finite Abelian group G of order n . By the Chinese Remainder Theorem

$$\mathbf{Z}_{2k} \simeq \prod_{i=1}^t \mathbf{Z}_{p_i^{m_i}}$$

so a code C over $\mathbf{Z}_{2k}$ can be regarded as the (Chinese) product of codes C_i for $1 \leq i \leq t$, where C_i is a code over $\mathbf{Z}_{p_i^{m_i}}$ [8]. The code C is self-dual over $\mathbf{Z}_{2k}$ if and only if each C_i is self-dual over $\mathbf{Z}_{p_i^{m_i}}$ for $1 \leq i \leq t$ [8, Theorem 2.1]. Using the same notation for augmented and extended codes, it is easy to observe that $\overline{C}_\epsilon$ is the Chinese product of $(\overline{C}_i)_\epsilon$ ($1 \leq i \leq t$). An Abelian code C over $\mathbf{Z}_{2k}$ is the Chinese product of C_i , where C_i is an Abelian code over $\mathbf{Z}_{p_i^{m_i}}$. It is clear that C is isodual by a multiplier α if and only if each C_i (for $1 \leq i \leq t$) is isodual by α .

We say that C is a *duadic code* (resp., *generalized duadic code*) over $\mathbf{Z}_{2k}$ if and only if each C_i is a duadic code (resp., generalized duadic code) over $\mathbf{Z}_{p_i^{m_i}}$ attached to a splitting (X_i, A_i, B_i) with α_i an automorphism of G_i for $1 \leq i \leq t$. By Section III, a duadic code over $\mathbf{Z}_{2k}$ exists only if $2k$ is a perfect square. If $\alpha_1 = \cdots = \alpha_t = \alpha$, we say that C is a duadic code (resp., generalized duadic code) *with* α .

Theorem 6.1:

- 1) Let C be a generalized duadic code over $\mathbf{Z}_{2k}$ with $\alpha = -1$. If every $C_i = I_{i,0} \times I_{i,1} \times \cdots \times I_{i,s}$ satisfies $I_{i,0} = (p_i^{e_i})$ with $e_i \geq m_i/2$, then C is self-orthogonal.
- 2) When $2k$ is a perfect square, every duadic code over $\mathbf{Z}_{2k}$ with $\alpha = -1$ is self-dual. Moreover, every self-dual Abelian code over $\mathbf{Z}_{2k}$ is a duadic code with $\alpha = -1$.
- 3) Let C be a generalized duadic code over $\mathbf{Z}_{2k}$ with $\alpha = -1$ of length n . Then $\overline{C}_\epsilon$ is self-dual if and only if $\epsilon^2 n + 1 \equiv 0 \pmod{2k}$.
- 4) Let C be an Abelian code in $\mathbf{Z}_{2k}[G]$ for some Abelian group G of order n whose augmented and extended code $\overline{C}_\epsilon$ is self-dual. Then, $\epsilon^2 n + 1 \equiv 0 \pmod{2k}$ and C is a generalized duadic code over $\mathbf{Z}_{2k}$ with $\alpha = -1$. In particular, when $2k$ is a perfect

square, any self-dual augmented and extended Abelian code over $\mathbf{Z}_{2k}$ is the augmented and extended code of a duadic code over $\mathbf{Z}_{2k}$ with $\alpha = -1$.

- 5) Let C be an Abelian code over $\mathbf{Z}_{2k}$ of length n such that $\overline{C}_\epsilon$ is self-dual. Then, $\overline{C}_\epsilon$ is of Type II if and only if $\epsilon^2 n + 1 \equiv 0 \pmod{4k}$.

Proof: The statement of 1) is an immediate consequence of Theorem 3.3 and the easy observation that C is self-orthogonal if and only if every C_i is self-orthogonal.

When $2k = p_1^{m_1} \cdots p_t^{m_t}$ is a perfect square, every m_i ($1 \leq i \leq t$) is even. Both statements of 2) then follow from Theorem 3.2 and the fact that C is self-dual if and only if each C_i is self-dual [8, Theorem 2.1].

Part 3) follows immediately from [8, Theorem 2.1] and Theorem 4.1, while part 4) is an easy consequence of [8, Theorem 2.1] and Theorem 4.2.

By [8, Theorem 2.3], a code C' over $\mathbf{Z}_{2k}$ is of Type II if and only if C'_1 is a Type II code over $\mathbf{Z}_{2^{m_1}}$ and C'_i is a self-dual code over $\mathbf{Z}_{p_i^{m_i}}$ for each $2 \leq i \leq t$. Using this result, as well as Theorems 4.1, 4.2, and 5.1, we obtain 5).

Remark : References [1, Corollary 3.3] and [8, Corollary 2.4] state that if there exists a Type II code of length n over $\mathbf{Z}_{2k}$, then n is a multiple of eight. Therefore, when k is odd, Theorem 6.1 5) can be refined to be: $\overline{C}_\epsilon$ is of Type II if and only if $\epsilon^2 n + 1 \equiv 0 \pmod{8k}$.

Using Theorems 3.4, 4.3, and 4.4, we obtain the following theorem.

Theorem 6.2: Assume that σ is the identity for each p_i .

- 1) Let C be a generalized duadic code over $\mathbf{Z}_{2k}$ with α . If every $C_i = I_{i,0} \times I_{i,1} \times \cdots \times I_{i,s}$ satisfies $I_{i,0} = (p_i^{e_i})$ with $e_i \geq m_i/2$, then $C^\alpha \subseteq C^\perp$.
- 2) When $2k$ is a perfect square, every duadic code over $\mathbf{Z}_{2k}$ with α is isodual. Moreover, every Abelian code over $\mathbf{Z}_{2k}$ isodual by a multiplier α is a duadic code with α .
- 3) Let C be a generalized duadic code over $\mathbf{Z}_{2k}$ with α of length n . Then $\overline{C}_\epsilon$ is isodual by a multiplier if and only if $\epsilon^2 n + 1 \equiv 0 \pmod{2k}$.
- 4) Let C be an Abelian code in $\mathbf{Z}_{2k}[G]$ for some Abelian group G of order n whose augmented and extended code $\overline{C}_\epsilon$ is isodual by a multiplier α . Then $\epsilon^2 n + 1 \equiv 0 \pmod{2k}$ and C is a generalized duadic code over $\mathbf{Z}_{2k}$ with α . In particular, when $2k$ is a perfect square, any augmented and extended Abelian code over $\mathbf{Z}_{2k}$ that is isodual by a multiplier α is the augmented and extended code of a duadic code over $\mathbf{Z}_{2k}$ with α .

VII. EXAMPLES OF CODES OVER $\mathbf{Z}_{2k}$ WITH SMALL LENGTHS

For a given integer n , all the finite Abelian groups G of order n can be easily determined. For each of such groups, for a given prime p not dividing n , the orbits of the map $x \mapsto px$ can then be easily determined. Once this is done, it is routine to observe if the group admits a splitting (X, A, B) with a given α . In the case where $2k$ is not a perfect square, to construct generalized duadic codes, the additional requirement that $X = \{0\}$ is needed.

A. When σ Is Not the Identity and $\alpha = -1$

For small k , we investigate the existence of duadic codes and generalized duadic codes for $n \leq 39$, $n = 47$ and 71 , as well as for the groups $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ ($n = 45$), $\mathbf{Z}_7 \times \mathbf{Z}_7$ ($n = 49$), and $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_7$ ($n = 63$). We only consider the cases for which σ is not the identity and α may be taken to be -1 . The existence of such codes, as well as

TABLE I
EXISTENCE OF (GENERALIZED) DUADIC CODES FOR SMALL k AND n (σ IS NOT IDENTITY AND $\alpha = -1$) AND PROPERTIES OF THEIR
AUGMENTED AND EXTENDED CODES

k	n	Remarks	Type II C_ϵ	Type I C_ϵ	References
2	7	QR	± 1		[4, 5, 9, 14, 16, 17]
2	15		± 1		[9, 14, 17]
2	21				[14, 17]
2	23	QR	± 1		[4, 5, 16, 17]
2	31	QR	± 1		[4, 5, 16, 17]
2	35			± 1	[17]
2	39		± 1		[17]
2	45	noncyclic			
2	47	QR	± 1		[4, 5]
2	49	noncyclic			
2	63	noncyclic	± 1		
2	71	QR	± 1		[4, 5]
3	23	g.d., QR	± 1		[1, 8]
3	47	g.d., QR	± 1		
3	71	g.d., QR	± 1		
4	7	g.d., QR	± 3	± 1	[5]
4	23	g.d., QR	± 3	± 1	[5]
4	31	g.d., QR	± 1	± 3	[4, 5]
4	47	g.d., QR	± 1	± 3	[4, 5]
4	49	g.d., noncyclic			
4	71	g.d., QR	± 3	± 1	[5]
5	31	g.d., QR	± 3		
5	71	g.d., QR	± 3		
6	23	g.d., QR	$\pm 1, \pm 5$		
6	47	g.d., QR	$\pm 1, \pm 5$		
6	71	g.d., QR	$\pm 1, \pm 5$		
8	7	QR	± 3	± 5	[5]
8	15		± 7	± 1	
8	21				
8	23	QR	± 5	± 3	[5]
8	31	QR	± 1	± 7	[5]
8	35				
8	39		± 3	± 5	
8	45	noncyclic			
8	47	QR	± 7	± 1	[5]
8	49	noncyclic			
8	63	noncyclic	± 1	± 7	
8	71	QR	± 3	± 5	[5]

the properties of their augmented and extended codes, is summarized in Table I. At the end of the section, we also list some examples of the augmented and extended codes which are extremal Type II codes.

Proposition 7.1: Let n be a prime.

- 1) There exist generalized duadic codes $C(2^m, n)$ over $\mathbf{Z}_{2^m}$ of length n , for all $m \geq 1$, if and only if $n \equiv \pm 1 \pmod 8$. Furthermore, if $n \equiv -1 \pmod 8$, then there exists ϵ such that $\overline{C}(2^m, n)_\epsilon$ is of Type II.
- 2) There exist generalized duadic codes $C(3^m, n)$ over $\mathbf{Z}_{3^m}$ of length n , for all $m \geq 1$, if and only if $n \equiv \pm 1 \pmod{12}$. Furthermore, if $n \equiv -1 \pmod{12}$, then there exists ϵ such that $\overline{C}(3^m, n)_\epsilon$ is self-dual.

- 3) There exist generalized duadic codes $C(5^m, n)$ over $\mathbf{Z}_{5^m}$ of length n , for all $m \geq 1$, if and only if $n \equiv \pm 1 \pmod 5$. Furthermore, there always exists ϵ such that $\overline{C}(5^m, n)_\epsilon$ is self-dual.
- 4) There exist generalized duadic codes $C(2^{m_1}3^{m_2}, n)$ over $\mathbf{Z}_{2^{m_1}3^{m_2}}$ of length n , for all $m_1, m_2 \geq 1$, if and only if $n \equiv \pm 1 \pmod{24}$. Furthermore, if $n \equiv -1 \pmod{24}$, then there exists ϵ such that $\overline{C}(2^{m_1}3^{m_2}, n)_\epsilon$ is of Type II.
- 5) There exist generalized duadic codes $C(2^{m_1}5^{m_2}, n)$ over $\mathbf{Z}_{2^{m_1}5^{m_2}}$ of length n , for all $m_1, m_2 \geq 1$, if and only if $n \equiv \pm 1$ or $\pm 9 \pmod{40}$. Furthermore, if $n \equiv -1$ or $-9 \pmod{40}$, then there exists ϵ such that $\overline{C}(2^{m_1}5^{m_2}, n)_\epsilon$ is of Type II.

TABLE I (Continued)
EXISTENCE OF (GENERALIZED) DUADIC CODES FOR
SMALL k AND n (σ IS NOT IDENTITY AND $\alpha = -1$) AND PROPERTIES OF
THEIR AUGMENTED AND EXTENDED CODES

k	n	Remarks	Type II $\overline{C}_\epsilon$	Type I $\overline{C}_\epsilon$	References
9	23	g.d., QR	± 5		
9	47	g.d., QR	± 7		
9	71	g.d., QR	± 1		
10	31	g.d., QR	$\pm 3, \pm 7$		
10	71	g.d., QR	$\pm 3, \pm 7$		
12	23	g.d., QR	$\pm 5, \pm 11$	$\pm 1, \pm 7$	
12	47	g.d., QR	$\pm 1, \pm 7$	$\pm 5, \pm 11$	
12	71	g.d., QR	$\pm 5, \pm 11$	$\pm 1, \pm 7$	
16	7	g.d., QR	± 3	± 13	[5]
16	23	g.d., QR	± 5	± 11	[5]
16	31	g.d., QR	± 15	± 1	[5]
16	47	g.d., QR	± 7	± 9	[5]
16	71	g.d., QR	± 3	± 13	[5]
18	23	QR	$\pm 5, \pm 13$		
18	35			$\pm 1, \pm 17$	
18	47	QR	$\pm 7, \pm 11$		
18	71	QR	$\pm 1, \pm 17$		

Examples:

- 1) For all $m \geq 1$, there always exist generalized duadic codes over $\mathbf{Z}_{2^m}$ of lengths 7, 23, 31, 47, and 71, where, for each such length, some of the augmented and extended codes are of Type II.
- 2) For all $m_1, m_2 \geq 1$, there always exist generalized duadic codes over $\mathbf{Z}_{2^{m_1 3^{m_2}}}$ of lengths 23, 47, and 71, where, for each such length, some of the augmented and extended codes are of Type II.
- 3) For all $m_1, m_2 \geq 1$, there always exist generalized duadic codes over $\mathbf{Z}_{2^{m_1 5^{m_2}}}$ of lengths 31 and 71, where, for each such length, some of the augmented and extended codes are of Type II.

Proof of Proposition 7.1: The condition on the existence of the generalized duadic codes over $\mathbf{Z}_{p^m}$ is due to the fact that there exists a splitting (X, A, B) of $G = \mathbf{Z}_n$ with $X = \{0\}$ if and only if p is a square modulo n .

The condition on the existence of self-dual or Type II augmented and extended code follows from Theorem 6.1, as well as from the following observations:

- 1) for a given n , if the congruence $\epsilon^2 n + 1 \equiv 0 \pmod{8}$ has a solution, then so does the congruence $\epsilon^2 n + 1 \equiv 0 \pmod{2^m}$;
- 2) For a given n and an odd prime p , the congruence $\epsilon^2 n + 1 \equiv 0 \pmod{p^m}$ has a solution if and only if so does $\epsilon^2 n + 1 \equiv 0 \pmod{p}$.

In Table I, the abbreviation “g.d.” means “only generalized duadic codes are defined,” while the absence of “g.d.” means duadic codes also exist for the corresponding k and n ; the remark “noncyclic” means the (generalized) duadic code is noncyclic, while the absence of the word means the corresponding code is cyclic. The “QR” in the remarks means that one of the (generalized) duadic codes for the given k and n is a quadratic residue code. Note that it does not necessarily mean that the quadratic residue code is, up to equivalence, the only (generalized)

duadic code of that given k and n . In the column labeled “Type II $\overline{C}_\epsilon$,” we list the values of $\epsilon \in \mathbf{Z}_{2k}$ for which $\overline{C}_\epsilon$ is of Type II, and similarly for the column labeled “Type I $\overline{C}_\epsilon$.” Values of ϵ that do not appear in these two columns correspond to those for which $\overline{C}_\epsilon$ is not self-dual. Given the assumption that σ is not the identity and that α may be taken to be -1 , all the duadic codes listed in Table I are self-dual. Some of the examples have been discussed in the literature. Appropriate references are given in the last column of Table I.

It is known [1, Corollary 3.5], that the minimum Euclidean weight d of a Type II code of length n over $\mathbf{Z}_{2k}$ satisfies

$$d \leq 4k \left(\left\lfloor \frac{n}{24} \right\rfloor + 1 \right) \quad (6)$$

if $\lfloor n/24 \rfloor \leq k - 2$ or if $k = 1$ or 2 . For $k \geq 2$, a Type II code that meets the bound in (6) is said to be extremal. It turns out that a number of the Type II augmented and extended codes arising from the (generalized) duadic codes in Table I turn out to be extremal. Examples are as follows.

- 1) All the Type II augmented and extended (generalized) duadic codes over $\mathbf{Z}_{2k}$ of lengths 8 and 16 are extremal. This follows from the facts that $d \equiv 0 \pmod{4k}$ and the bound in (6) is $4k$. For example, such codes of length 8 exist over $\mathbf{Z}_{2^m}$ for all $m \geq 2$, while such codes of length 16 exist over $\mathbf{Z}_{2^{2m}}$ for all $m \geq 1$.
- 2) Over $\mathbf{Z}_4$, the augmented and extended quadratic residue codes of lengths 24, 32, and 48 have minimum Euclidean weights 16, 16, and 24, respectively, and they are hence extremal [3, Theorem 3.4] and [16, Theorem 12].
- 3) Over $\mathbf{Z}_4$, the Type II code of length 40 (the unique Type II augmented and extended cyclic code of this length) has minimum Euclidean weight 16 and is hence extremal [17, p. 61].
- 4) Over $\mathbf{Z}_6$, the code G_6^{24} in [1], which is the Chinese product of two extended cyclic quadratic residue codes of length 24 over $\mathbf{Z}_2$ and $\mathbf{Z}_3$, is an augmented and extended generalized duadic code. It has minimum Euclidean weight 24 and is hence extremal.
- 5) Over $\mathbf{Z}_6$, the code C_{48} in [12], which is the Chinese product of two extended cyclic quadratic residue codes of length 48 over $\mathbf{Z}_2$ and $\mathbf{Z}_3$, is an augmented and extended generalized duadic code. It is shown in [12] that C_{48} has minimum Euclidean weight 36 and is extremal. (Though (6) is not applicable in this case, it is shown in [12, Proposition 4] that $d \leq 36$ in this case.)
- 6) Over $\mathbf{Z}_8$, Calderbank (a private communication in [6]) has shown that the extended Hensel lifted quadratic residue code QR_{48} over $\mathbf{Z}_8$ of length 48 is extremal.

B. When σ Is the Identity

Now we consider the case when σ is the identity. Again, we investigate the existence of duadic codes and generalized duadic codes for $n \leq 39$.

It is straightforward to verify that, for σ to be the identity on the orbits of the map $x \mapsto px$ (where $p = 2, 3$, or 5), the only groups that admit a splitting (X, A, B) are as follows:

- 1) for $p = 2$:
 - i) $G = \mathbf{Z}_3 \times \mathbf{Z}_3$: the orbits are $O_0 = \{00\}$, $O_1 = \{11, 22\}$, $O_2 = \{12, 21\}$, $O_3 = \{10, 20\}$, and $O_4 = \{01, 02\}$, with a possible splitting given by $X = O_0$, $A = O_3 \cup O_4$, and $B = O_1 \cup O_2$ with

$$\alpha = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix};$$

ii) $G = \mathbf{Z}_{17}$: the orbits are

$$O_1 = \{1, 2, 4, 8, 16, 15, 13, 9\}$$

and

$$O_2 = \{3, 6, 12, 7, 14, 11, 5, 10\}$$

with a possible splitting given by $X = \{0\}$, $A = O_1$, and $B = O_2$ with $\alpha = 3$;

iii) $G = \mathbf{Z}_5 \times \mathbf{Z}_5$: the orbits, given by their representatives, are 00, 01, 10, 11, 12, 13, and 14, with a possible splitting given by $X = 00$, A the union of the orbits 01, 10, and 11, and B the union of 12, 13, and 14, with

$$\alpha = \begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix};$$

iv) $G = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$: the orbits are given by the representatives 000, 001, 010, 011, 012, 100, 101, 102, 110, 111, 112, 120, 121, and 122, and any splitting of G must have $X \neq \{0\}$;

v) $G = \mathbf{Z}_3 \times \mathbf{Z}_9$: the orbits are given by the representatives 00, 01, 03, 10, 11, 12, 13, and 16, three of which have size six and four have size two, so any splitting of G must again have $X \neq \{0\}$;

vi) $G = \mathbf{Z}_{33}$: the orbits are given by the representatives 0 (size 1), 1, 5, 3 (each of size 10) and 11 (size 2), where any splitting must have $X \neq \{0\}$;

2) for $p = 3$: only $G = \mathbf{Z}_5 \times \mathbf{Z}_5$ with the same orbits as for $p = 2$;

3) for $p = 5$

i) for $G = \mathbf{Z}_3 \times \mathbf{Z}_3, \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$, and $\mathbf{Z}_3 \times \mathbf{Z}_9$ with the same orbits as for $p = 2$;

ii) for $G = \mathbf{Z}_{33}$, with orbits given by the representatives 0, 1, 2, 3, and 11, and any splitting of G must have $X \neq \{0\}$.

Remarks:

- 1) The group $\mathbf{Z}_3 \times \mathbf{Z}_3$ may be identified as the underlying additive group for $\mathbf{F}_9 = \mathbf{F}_3(i)$, with $i^2 = -1$. Identifying $1 \in \mathbf{F}_9$ with $10 \in \mathbf{Z}_3 \times \mathbf{Z}_3$ and identifying $i \in \mathbf{F}_9$ with $01 \in \mathbf{Z}_3 \times \mathbf{Z}_3$, the A in the splitting given above then consists of all the nonzero squares while B contains all the nonsquares. Therefore, that splitting gives rise to a quadratic residue code.
- 2) The group $\mathbf{Z}_5 \times \mathbf{Z}_5$ may be identified as the underlying additive group for $\mathbf{F}_{25} = \mathbf{F}_5(j)$, with $j^2 + j + 1 = 0$. Identifying $1 \in \mathbf{F}_{25}$ with $10 \in \mathbf{Z}_5 \times \mathbf{Z}_5$ and $j \in \mathbf{F}_{25}$ with $01 \in \mathbf{Z}_5 \times \mathbf{Z}_5$, the A in the splitting given above again consists of all the nonzero squares while B contains all the nonsquares. Therefore, that splitting gives rise to a quadratic residue code.
- 3) The splitting for $\mathbf{Z}_{17}$ is precisely the one for quadratic residue codes of length 17.
- 4) In the cases of lengths 27 and 33, no quadratic residue code is obtained because the X in any admissible splitting of G is definitely nontrivial.

The existence of duadic codes and generalized duadic codes in this setting, together with some of the properties of their augmented and extended codes, is summarized in Table II. The remarks “g.d.,” “noncyclic,” and “QR” have the same meanings as in Table I. Since σ is assumed to be the identity, the duadic codes listed in Table II are isodual by some multiplier. When $k = 2$, the codes of lengths 9, 25, and 27 have been discussed in [14].

TABLE II
EXISTENCE OF (GENERALIZED) DUADIC CODES FOR SMALL k AND n (σ IS IDENTITY) AND PROPERTIES OF THEIR AUGMENTED AND EXTENDED CODES

k	n	Remarks	Isodual $\bar{C}_\epsilon$
2	9	noncyclic, QR	
2	17	QR	
2	25	noncyclic, QR	
2	27	noncyclic	± 1
2	33		
3	25	g.d., noncyclic, QR	
4	9	g.d., noncyclic, QR	
4	17	g.d., QR	
4	25	g.d., noncyclic, QR	
5	9	g.d., noncyclic, QR	± 1
6	25	g.d., noncyclic, QR	
8	9	noncyclic, QR	
8	17	QR	
8	25	noncyclic, QR	
8	27	noncyclic	
8	33		
9	25	g.d., noncyclic, QR	
10	9	g.d., noncyclic, QR	
12	25	g.d., noncyclic, QR	
16	9	g.d., noncyclic, QR	
16	17	g.d., QR	
16	25	g.d., noncyclic, QR	
18	25	noncyclic, QR	

VIII. OPEN PROBLEMS

We conclude with some problems left unanswered in this correspondence.

We have not discussed the weight enumerators of the codes studied in this correspondence. Except for a few examples of very small lengths, computation of the weight enumerators by brute force does not seem feasible. It is perhaps possible to determine the weight enumerators by using invariants and properties of the residue and torsion codes.

Recall that two codes over $\mathbf{Z}_{2k}$ are said to be equivalent if one can be obtained from another by permuting the coordinates and, if necessary, changing the signs of certain coordinates [1], [8]. In the examples of Tables I and II, we have not tried to classify the codes up to equivalence. For $k = 2$, the cyclic self-dual codes with $n \leq 39$ have been classified in [17]. The classification of such codes up to multiplier equivalence can be done by looking closely at the possible splittings for the given k and n , but it is coarser in general than the classification up to equivalence. It would be an interesting arithmetical problem to carry out such a classification for modest lengths. To convey an idea of the complexity of the problem, let it suffice to say that the noncyclic duadic codes of length 9 over $\mathbf{Z}_{10}$ correspond to 45 possible pairs of splittings, each pair consisting of one splitting over $\mathbf{Z}_2$ and another over $\mathbf{Z}_5$.

It is a well-known open problem in the theory of lattices to decide if there is an extremal Type II lattice in dimension 72. Of related interest is the following problem.

Question (cf. [13, Problem 6.12]): Is there a Type II $\mathbf{Z}_8$ -code in length 72 of minimum Euclidean distance 64?

We hope that some of the codes constructed in this correspondence might give an answer to this question.

APPENDIX

FINITE ABELIAN GROUPS AND THE FOURIER TRANSFORM

Let G be an Abelian group written additively in the form

$$G = \prod_{i=1}^t \mathbf{Z}_{n_i}$$

where n_i divides n_{i+1} for all $1 \leq i \leq t-1$. The exponent N of G is then n_t . An element g of G may then be written as $g = (g_1, \dots, g_t)$, with $g_i \in \mathbf{Z}_{n_i}$.

For $1 \leq i \leq t$, let $\mathbf{e}^{(i)}$ be the element of G with 1 in the component $\mathbf{Z}_{n_i}$ and 0 in the other components. Any element of G can then be uniquely written as $\sum_{i=1}^t g_i \mathbf{e}^{(i)}$, for $0 \leq g_i \leq n_i - 1$.

Define the following pairing $[\cdot, \cdot]$ on $G \times G$: for $g = (g_1, \dots, g_t)$ and $h = (h_1, \dots, h_t)$ in G

$$[\cdot, \cdot]: G \times G \longrightarrow \mathbf{Z}_N$$

$$[g, h] = \sum_{i=1}^t g_i h_i (N/n_i) \bmod N.$$

By taking g or h to be $\mathbf{e}^{(i)}$ for all $1 \leq i \leq t$, one shows readily that $[g, h] = 0$ for all h (resp., g) if and only if $g = 0$ (resp., $h = 0$), i.e., this pairing is nondegenerate.

Now let α be an endomorphism of G . For each $1 \leq i \leq t$, we may write

$$\alpha \mathbf{e}^{(i)} = (\alpha_{i1}, \dots, \alpha_{ij}, \dots, \alpha_{it})$$

where, for each $1 \leq j \leq t$, $\alpha_{ij} \in \mathbf{Z}_{n_j}$. For an element $g = \sum g_i \mathbf{e}^{(i)}$ of G , αg is given by $(\sum g_i \alpha_{i1}, \dots, \sum g_i \alpha_{it})$. Note that, since $n_i \mathbf{e}^{(i)} = 0$, it follows that $n_i \alpha_{ij} = 0 \in \mathbf{Z}_{n_j}$ for all $1 \leq j \leq t$. In particular, if n_i divides n_j , then $\alpha_{ij} \equiv 0 \bmod (n_j/n_i)$. For all $1 \leq i, j \leq t$

$$[\alpha \mathbf{e}^{(i)}, \mathbf{e}^{(j)}] = \alpha_{ij} \frac{N}{n_j} \in \mathbf{Z}_N.$$

Let α^* be an endomorphism of G defined as follows: for all $1 \leq j \leq t$

$$\alpha^* \mathbf{e}^{(j)} = (\alpha_{j1}^*, \dots, \alpha_{ji}^*, \dots, \alpha_{jt}^*)$$

where the α_{ji}^* are defined in the following way:

- 1) if n_i divides n_j , write $n_j = n_i n'_{ij}$, and set α_{ji}^* to satisfy

$$\alpha_{ji}^* n'_{ij} \equiv \alpha_{ij} \bmod n_j;$$

- 2) if n_j divides n_i , write $n_i = n_j n'_{ji}$, and set

$$\alpha_{ji}^* \equiv \alpha_{ij} n'_{ji} \bmod n_i.$$

One checks readily that α_{ji}^* is well-defined in $\mathbf{Z}_{n_i}$. For $g = (g_1, \dots, g_t) \in G$, we have

$$\alpha^* g = \left(\sum g_j \alpha_{j1}^*, \dots, \sum g_j \alpha_{jt}^* \right).$$

This makes α^* a well-defined endomorphism of G . Moreover,

$$[\mathbf{e}^{(i)}, \alpha^* \mathbf{e}^{(j)}] = \alpha_{ji}^* \frac{N}{n_i} \in \mathbf{Z}_N.$$

The conditions on α_{ji}^* implies that

$$\alpha_{ji}^* \frac{N}{n_i} \equiv \alpha_{ij} \frac{N}{n_j} \bmod N$$

hence yields the equality

$$[\alpha \mathbf{e}^{(i)}, \mathbf{e}^{(j)}] = [\mathbf{e}^{(i)}, \alpha^* \mathbf{e}^{(j)}]$$

for all $1 \leq i, j \leq t$. Consequently, we obtain

$$[\alpha g, h] = [g, \alpha^* h] \quad (7)$$

for all $g, h \in G$.

The nondegeneracy of the pairing $[\cdot, \cdot]$ implies that, for any endomorphism α of G , there exists a unique endomorphism α^* of G that satisfies (7). The endomorphism α^* is called the adjoint of α .

Moreover, for any two endomorphisms α, β of G , we have $(\alpha\beta)^* = \beta^* \alpha^*$. This, in turn, implies that, if α is an automorphism of G , then so is α^* .

Let p be a prime not dividing the exponent N of G . Let $\text{GR}(p^m, M)$ be the smallest Galois ring extension of $\mathbf{Z}_{p^m}$ that contains the roots of unity of order N . Here, M is the order of p modulo N . Denote by ζ an element of order N in the group of invertible elements of $\text{GR}(p^m, M)$. For $g, h \in G$, we define the duality bracket of g and h to be

$$\langle g, h \rangle = \zeta^{[g, h]}.$$

Writing an element c of $\mathbf{Z}_{p^m}[G]$ formally as $c = \sum_{g \in G} c_g X^g$, we define its Fourier transform $\hat{c}$ as $\hat{c} = \sum_{h \in G} \hat{c}_h X^h$, where

$$\hat{c}_h = \sum_{g \in G} c_g \langle g, h \rangle.$$

It also follows that we have the following inversion formula:

$$c_g = \frac{1}{|G|} \sum_{h \in G} \hat{c}_h \langle -h, g \rangle.$$

If α is an automorphism of G , the above formulas enable one to check readily that $\sum_{h \in G} \hat{c}_{\alpha h} X^h$ is the Fourier transform of $\sum_{g \in G} c_g X^{\alpha^* g}$.

For α an automorphism of G , the map

$$\sum_{g \in G} c_g X^g \mapsto \sum_{g \in G} c_g X^{\alpha^* g}$$

is just a permutation on the coefficients, hence it is an isometry of $\mathbf{Z}_{p^m}[G]$. It is called a multiplier.

ACKNOWLEDGMENT

The authors wish to thank M. Harada for sending them a copy of [12]. They are also grateful to the anonymous referees and the Associate Editor for very helpful comments on the manuscript. This work was performed when S. Ling was visiting CNRS-I3S, ESSI, Sophia-Antipolis, France. This author would like to thank the institution for their kind hospitality. P Solé is grateful to AGAT laboratory for its hospitality of nine months.

REFERENCES

- [1] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, "Type II codes, even unimodular lattices, and invariant rings," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1194–1205, May 1999.
- [2] A. Bonnetcaze, P. Solé, C. Bachoc, and B. Mourrain, "Type II codes over $\mathbf{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 43, pp. 969–976, May 1997.
- [3] A. Bonnetcaze, P. Solé, and A. R. Calderbank, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory*, vol. 41, pp. 366–377, Mar. 1995.
- [4] A. R. Calderbank, W.-C. W. Li, and B. Poonen, "A 2-adic approach to the analysis of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 977–986, May 1997.
- [5] A. R. Calderbank and N. J. A. Sloane, "Modular and p -adic cyclic codes," *Des., Codes Cryptogr.*, vol. 6, pp. 21–35, 1995.

- [6] R. Chapman and P. Solé, "Universal codes and unimodular lattices," *J. Th. Nombres Bordeaux*, vol. 8, pp. 369–376, 1996.
- [7] J. H. Conway and N. J. A. Sloane, "Self-dual codes over the integers modulo 4," *J. Comb. Theory Ser. A*, vol. 62, pp. 30–45, 1993.
- [8] S. T. Dougherty, M. Harada, and P. Solé, "Self-dual codes over rings and the Chinese Remainder Theorem," *Hokkaido Math J.*, vol. 28, pp. 253–283, 1999.
- [9] J. Fields, P. Gaborit, J. Leon, and V. Pless, "All self-dual $\mathbf{Z}_4$ codes of length 15 or less are known," *J. Comb. Theory Ser. A*, vol. 78, pp. 32–50, 1997.
- [10] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbf{Z}_4$ -linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–319, Mar. 1994.
- [11] M. Harada, "On the existence of extremal Type II codes over $\mathbf{Z}_6$," *Discr. Math.*, vol. 223, pp. 373–378, 2000.
- [12] —, "Extremal type II codes over $\mathbf{Z}_6$ and their lattices," paper, preprint, 2000.
- [13] M. Harada, P. Solé, and P. Gaborit, "Self-dual codes over $\mathbf{Z}_4$ and unimodular lattices: A survey," in *Algebra and Combinatorics (Proc. Int. Congr., ICAC'97)*, K. P. Shum, E. J. Taft, and Z.-X. Wan, Eds. Singapore: Springer-Verlag, 1999, pp. 255–275.
- [14] P. Langevin and P. Solé, "Duadic $\mathbf{Z}_4$ -codes," *Finite Fields Their Appl.*, vol. 6, no. 4, pp. 309–326, 2000.
- [15] J. S. Leon, J. M. Masley, and V. Pless, "Duadic codes," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 709–714, Sept. 1984.
- [16] V. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbf{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1594–1600, Sept. 1996.
- [17] V. Pless, P. Solé, and Z. Qian, "Cyclic self-dual $\mathbf{Z}_4$ -codes," *Finite Fields Their Appl.*, vol. 3, pp. 48–69, 1997.
- [18] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: North-Holland, 1998.