Filomat 37:12 (2023), 3985–3998
https://doi.org/10.2298/FIL2312985K

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Duadic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$

Raj Kumar[a], Maheshanand Bhaintwal[a]

[a] *Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee-247667, Uttarakhand, India*

Abstract. Duadic codes constitute a well-known class of cyclic codes. In this paper, we study the structure of duadic codes of length n over the ring $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, $u^2 = v^2 = 0$, $uv = vu$, where p is prime and $(n, p) = 1$. These codes have been studied here in the setting of abelian codes over R, and we have used Fourier transform and idempotents to study them. We have characterized abelian codes over R by studying their torsion and residue codes. It is shown that the Gray image of an abelian code of length n over R is a binary abelian code of length $4n$. Conditions for self-duality and self-orthogonality of duadic codes over R are derived. Some conditions on the existence of self-dual augmented and extended codes over R are presented. We have also studied Type II self-dual augmented and extended codes over R. Some results related to the minimum Lee distances of duadic codes over R are presented. We have also presented a sufficient condition for abelian codes of the same length over R to have the same minimum Hamming distance. Some optimal binary linear codes of length 36 and ternary linear codes of length 16 have been obtained as Gray images of duadic codes of length 9 and 4, respectively, over R using the computational algebra system Magma.

1. Introduction

The idea of finding good codes over a finite field via the Gray map has inspired many researchers to study codes over finite rings. This idea originated with the breakthrough paper of Hammons et al. [6], wherein it was shown that some well known binary non-linear codes are actually images of some linear codes over $\mathbb{Z}_4$ under the Gray map. Cyclic codes are among the most studied families of codes because of their rich algebraic structure and their relatively efficient encoding and decoding methods. Abelian codes are a generalization of cyclic codes. Berman [2] and MacWilliams [16] introduced abelian codes over finite fields. Speigel [25] studied abelian codes over the integer residue ring $\mathbb{Z}_m$ for some positive integer m. Rajan and Siddiqi [17, 18] studied cyclic codes and abelian codes over $\mathbb{Z}_m$ using the discrete Fourier transform approach. Duadic codes are an important class of abelian codes, and were introduced by Leon et al. [12] as a generalization of quadratic residue codes. They showed that every extended self-dual cyclic binary code is a duadic code. They also showed that in some cases Reed-Muller codes are also duadic codes. Further, it was shown that in several cases duadic codes are better than quadratic residue codes of the same length, and in some cases they have the best parameters among the codes of the same length. Tilborg [26] presented an important method to evaluate the minimum weights of binary quadratic residue codes. Li

2020 *Mathematics Subject Classification*. MSC 94B05, MSC 94B15
Keywords. Abelian codes, duadic codes, self-dual codes
Received: 26 June 2022; Revised: 05 December 2022; Accepted: 19 December 2022
Communicated by Paola Bonacini
Email addresses: raj.k1993@yahoo.com (Raj Kumar), maheshanand@ma.iitr.ac.in (Maheshanand Bhaintwal)

[11] generalized this result to duadic codes. Recently, Kumar and Bhaintwal [8] have studied duadic codes of odd length over $\mathbb{Z}_4 + u\mathbb{Z}_4$ using the Fourier transform approach.

In recent years there has been a lot of interest on linear codes over various rings of the form considered in this paper. Bonnecaze and Udaya [3] have studied cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$, and provided their basic framework. Dougherty et al. [4] have studied and classified Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Yildiz and Karadeniz have studied cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, where $u^2 = v^2 = 0, uv = vu$, and obtained some good binary codes as the images of these codes under two Gray maps. Ankur and Kewat [1] have studied Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. They have characterized the structure of self-dual, Type I codes and Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ with given generator matrix in terms of the structures of their torsion and residue codes. Kai et al. [7] studied $(1 + u)$-constacyclic codes of arbitrary length over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. In this paper, they have given a complete classification of self-dual constacyclic codes and enumerated them. Wang and Zhu [27] have studied repeated-root constacyclic codes over R and enumerated such self-dual codes for any given length n. Haifeng et al. studied $(1 - uv)$-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$ [5]. They have proved that a Gray image of $(1 - uv)$-constacyclic code over this ring is a distance invariant quasi-cyclic code of index p^2 and length p^3n over $\mathbb{F}_p$. Shi et al. have studied [24] the asymptotic behavior of quasi-cyclic codes on the same or similar rings. Shi et. al. [20] studied constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$. Shi et. al. [21] studied double circulant LCD codes over $\mathbb{Z}_4$. Many author [9, 14, 22, 23] have studied different classes of codes over similar structure of such type of rings.

In this paper, we study the structure of duadic codes of length n over the ring $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$ with $(n, p) = 1$, in the setting of abelian codes over R, and using the Fourier transform and idempotents. The torsion codes and residue codes of abelian codes have been studied. It is shown that the Gray image of an abelian code of length n over R is a binary abelian code of length $4n$. Conditions for self-duality and self-orthogonality of duadic codes are derived. Some conditions on the existence of self-dual augmented and extended codes over R are presented. We have also studied Type II augmented and extended codes over R. Some results related to the minimum Lee distances of duadic codes over R are obtained. We have presented a sufficient condition for abelian codes of the same length over R to have the same minimum Hamming distance. Some optimal binary linear codes of length 36 and ternary linear codes of length 16 have been obtained as Gray images of duadic codes of length 9 and 4, respectively, over R using the computational algebra system Magma.

The paper is organized as follows. Section 2 collects the relevant notations and definitions. Section 3 describes the algebraic structure of abelian codes over R. In Section 4, duadic codes and generalized duadic codes over R are introduced and some conditions for these codes to be self-dual, self-orthogonal or isodual are determined. A new Gray map is introduced and it is shown that the image of an abelian code under this map is also an abelian code. Section 5 presents some results on the minimum distance of abelian codes. In Section 6, the augmented and extended abelian codes over R are characterized in terms of self-duality, and some self-dual, self-orthogonal and isodual properties of these codes are discussed. In Section 7, Type II augmented and extended abelian codes over R have been studied. In Section 8, some optimal binary linear codes of length 36 and ternary linear codes of length 16 have been obtained as Gray images of duadic codes of length 9 and 4, respectively, over R using the computational algebra system Magma.

2. Preliminaries

Throughout the paper, R denotes the ring $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p = \{a + ub + vc + uvd \ : \ a, b, c, d \in \mathbb{F}_p\}$ with $u^2 = v^2 = 0, uv = vu$, where p is a prime and $\mathbb{F}_p = \{0, 1, \cdots, p - 1\}$ is the field of order p. The ring R can also be viewed as the quotient ring $\mathbb{F}_p[u, v]/\left\langle u^2, v^2, uv - vu\right\rangle$. An element $a + ub + vc + uvd \in R$ is a unit if and only if a is non-zero. The ring R is a local ring with the unique maximal ideal $\langle u, v\rangle$ and it has a total of p^4 elements. The ideals of R are $\langle 0\rangle, \langle 1\rangle, \langle u\rangle, \langle v\rangle, \langle uv\rangle, \langle u + v\rangle$, and $\langle u, v\rangle$. A linear code C of length n over R is an R-submodule of R^n. A linear code C of length n over R is called a cyclic code if it is invariant under the cyclic shift, i.e., $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$.

The Hamming distance $d(x, y)$ between any two elements $x, y \in R^n$ is the number of coordinate positions where x and y differ. The minimum Hamming distance $d_H(C)$ of a code C is given by

$$d_H(C) = \min\{d(x, y) \ : \ x, y \in C, \ x \neq y\} .$$

The Hamming weight $w_H(x)$ of any $x \in R^n$ is the total number of non-zero coordinates in x. If C is a non-zero linear code, $d_H(C)$ coincides with the smallest weight of a non-zero codeword in C.

Now, as in [28], we define a Gray map ϕ from R to $\mathbb{F}_p^4$ as

$$\phi(a + ub + vc + uvd) = (a + b + c + d, c + d, b + d, d) .$$

The map ϕ can be extended to a map from R^n to $\mathbb{F}_p^{4n}$ component-wise. The Lee distance $d_L(C)$ of a linear code C over R is defined as the Hamming distance of $\phi(C)$. For a linear code C of length n over R, the dual of C is defined by

$$C^\perp = \{x \in R^n : \ x \cdot c = 0 \ \forall c \in C\} ,$$

where $x \cdot c$ denotes the usual inner product of x and c. If $C \subseteq C^\perp$, we say that C is self-orthogonal, and if $C = C^\perp$ then C is said to be a self-dual code. Two codes are equivalent if one can be obtained from the other by permuting and exchanging the coordinates.

Let $S = \mathbb{F}_p + u\mathbb{F}_p$. For a linear code C of length n over R, we define the residue code $Res(C)$ and the torsion code $Tor(C)$ of C as

$$\begin{aligned} Res(C) &= \{a' \in S^n : \ \exists\, b' \in S^n \text{ such that } a' + vb' \in C\} , \\ Tor(C) &= \{b' \in S^n \ : \ vb' \in C\} . \end{aligned}$$

The residue code and the torsion code are linear codes of length n over $\mathbb{F}_p + u\mathbb{F}_p$.

For a linear code C of length n over R, we define four binary linear codes associated to C in R, as

$$\begin{aligned} Res(Res(C)) &= C \ (\text{mod } \langle u, v\rangle) , \\ Tor(Res(C)) &= \{a_1 \in \mathbb{F}_p^n : \ ua_1 \in C \mod v\} , \\ Res(Tor(C)) &= \{a_2 \in \mathbb{F}_p^n : \ va_2 \in C \mod uv\} , \\ Tor(Tor(C)) &= \{a_3 \in \mathbb{F}_p^n : \ uva_3 \in C\} . \end{aligned}$$

For a linear code C of length n over R and $\epsilon \in R$, we define the extended code C_ϵ of C to be the code obtained by appending to each codeword $c = (c_1, \cdots, c_n)$ an overall parity-check coordinate $c_\infty = \epsilon \sum_{i=1}^n c_i$, i.e.,

$$C_\epsilon = \{(c, c_\infty) \mid \ c \in C\} .$$

By the augmented code $\overline{C}$ of C, we mean the code $C + span\{\mathbf{1}\}$, where $\mathbf{1}$ is the all-one vector and $span\{v\}$ denotes the R-span of any vector $v \in R^n$. The augmented and extended code $(\overline{C})_\epsilon$ of C is defined as

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

3. Abelian codes

In this section, we study the algebraic structure of abelian codes over $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$. Suppose G is a finite abelian group of odd order n. We assume that the operation in G is written additively. An abelian code of length n over R is defined to be an ideal in the group ring $R[G]$. Every element of $R[G]$ can be written uniquely as a formal polynomial $\sum_{g\in G} c_g Y^g$, $c_g \in R$. The addition in $R[G]$ is componentwise and the multiplication in $R[G]$ is the convolution product given by

$$\left(\sum_{h\in G} c_h Y^h\right)\left(\sum_{l\in G} c'_l Y^l\right) = \sum_{g\in G} d_g Y^g ,$$

where

$$d_g = \sum_{h+l=g} c_h c'_l \, .$$

Let α be an automorphism of G. Then the automorphism

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

of $R[G]$ is called a *multiplier* of $R[G]$. For convenience, we simply say that α is a multiplier of $R[G]$.

We have $\mathbb{F}_{p^t} + u\mathbb{F}_{p^t} + v\mathbb{F}_{p^t} + uv\mathbb{F}_{p^t} \simeq \mathbb{F}_{p^t}[u,v]/\langle u^2, v^2, uv - vu\rangle$ for every non-negative integer t. Let $\mathscr{R}_{u,v,t} = \mathbb{F}_{p^t}[u,v]/\langle u^2, v^2, uv - vu\rangle$. If $x = x_0 + ux_1 + v(y_0 + uy_1)$ represents any element of $\mathscr{R}_{u,v,t}$, then the Frobenius map F of $\mathscr{R}_{u,v,t}/R$ is defined by

$$F(x) = x_0^p + ux_1^p + v(y_0^p + uy_1^p) \, .$$

Exponent of a group G is the smallest positive integer n such that g^n gives identity of G for all $g \in G$. Let N denote the exponent of G, and let M be the smallest positive integer such that $p^M \equiv 1 \bmod N$. Then $\mathbb{F}_{p^M}$ contains a primitive Nth root of unity ξ. Now by the fundamental theorem of finite abelian groups,

$$G \simeq \times_{i=1}^{t} \mathbb{Z}_{n_i} \, ,$$

where n_i divides n_{i+1}, $1 \le i \le t-1$. Let a, b be any two elements of G and a_i, b_i be their respective factors in $\mathbb{Z}_{n_i}$. Then we define a character of G with values in $\mathbb{F}_{p^M}$ by

$$\chi_a(b) = \xi^{\sum_{i=1}^{t} a_i b_i (N/n_i)} \, .$$

Then

- For a fixed $a \in G$, χ_a is a homomorphism from G to $\mathbb{F}_{p^M}^{\times}$,
- $\chi_a(b) = \chi_b(a)$, and
- $\sum_{x\in G} \chi_a(x) = n\delta_{a,0}$, where $\delta_{a,0}$ is the Kronecker delta function.

The Fourier transform of any element $f = \sum_{g\in G} f_g Y^g \in \mathbb{F}_p[G]$ is defined by $\hat{f} = \sum_{g\in G} \hat{f}_g Y^g$, where $\hat{f}_g = \sum_{h\in G} f_h \chi_g(h)$. The inverse transform is given by $f_h = \frac{1}{n} \sum_{g\in G} \hat{f}_g \chi_h(-g)$. For any element $\mathbf{c} = a + ub + vc + uvd \in R[G]$, we define the Fourier transform of $\mathbf{c}$ as $\hat{\mathbf{c}} = \hat{a} + u\hat{b} + v\hat{c} + uv\hat{d}$.

Now, for any $a, b \in G$, we have

$$\chi_a(pb) = \chi_a(b)^p = F(\chi_a(b)) \, .$$

Also, for any $x \in R[G]$ and $g \in G$, we have

$$F(\hat{x}_g) = \hat{x}_{pg} \, .$$

Let $O_0, O_1, \cdots, O_s$ be the orbits of G under the map $x \mapsto px$ with $d_i = o(O_i), 1 \le i \le s$. Then using the same argument as in [8, Theorem 3.1], we get the following result.

Theorem 3.1. *Let G be a finite abelian group of odd order n. Then*

$$R[G] \simeq R \times \frac{\mathbb{F}_{p^{d_1}}[u,v]}{\langle u^2, v^2, uv - vu\rangle} \times \frac{\mathbb{F}_{p^{d_2}}[u,v]}{\langle u^2, v^2, uv - vu\rangle} \times \cdots \times \frac{\mathbb{F}_{p^{d_s}}[u,v]}{\langle u^2, v^2, uv - vu\rangle} \, .$$

Now we determine the ideal structure of $\mathscr{R}_{u,v,d} = \mathbb{F}_{p^d}[u,v]/\langle u^2, v^2, uv - vu\rangle$ for any non-negative integer d.

Let I be any ideal of $\mathscr{R}_{u,v,d}$. Define a map $\Psi : I \to \mathbb{F}_{p^d}[u]/\langle u^2\rangle$ such that

$$\Psi(a + ub + vc + uvd) = a + ub\ .$$

Clearly Ψ is a ring homomorphism with the kernel

$$\ker\Psi = \{vb' \in I \mid b' \in \mathbb{F}_{p^d}[u]/\langle u^2\rangle\}\ .$$

Let $J = \{b' \in \mathbb{F}_{p^d}[u]/\langle u^2\rangle \mid vb' \in I\}$. Then J is an ideal of $\mathbb{F}_{p^d}[u]/\langle u^2\rangle$. So, $J = \langle 0\rangle$ or $\langle 1\rangle$ or $\langle u\rangle$, and hence $\ker\Psi = \langle 0\rangle$ or $\langle v\rangle$ or $\langle uv\rangle$. It is easy to verify that $\Psi(I)$ is also an ideal of $\mathbb{F}_{p^d}[u]/\langle u^2\rangle$. So, $\Psi(I) = \langle 0\rangle$ or $\langle 1\rangle$ or $\langle u\rangle$. Therefore, we have the following result.

Proposition 3.2. *For any non-negative integer d, the ideals of* $\mathbb{F}_{p^d}[u,v]/\langle u^2, v^2, uv - vu\rangle$ *are given by*

1. $\langle 0\rangle, \langle 1\rangle$,
2. $\langle u\rangle$,
3. $\langle v\rangle$,
4. $\langle uv\rangle$,
5. $\langle u + v\delta\rangle$, *where* $\delta \in \mathbb{F}_{p^d}^{\times}$,
6. $\langle u, v\rangle$.

It is clear that the total number of these ideals is $p^d + 5$.

Let $O_0, O_1, \cdots, O_s$ be the orbits of G under the mapping $x \mapsto px$. Let σ denote the permutation of $\{0, 1, \cdots, s\}$ induced by the map $x \mapsto -x$ in G. If for every orbit of G, σ maps the orbit to itself, then σ is called an identity map. We have the following results.

Theorem 3.3. 1. *Every ideal I of R[G] can be expressed as*

$$I = I_0 \times I_1 \times \cdots \times I_s,$$

where I_j *is one of the ideals* $\langle 0\rangle, \langle 1\rangle, \langle u\rangle, \langle v\rangle, \langle uv\rangle, \langle u+v\delta\rangle, \langle u, v\rangle$ *in the ring* $\mathbb{F}_{p^{d_j}}[u,v]/\langle u^2, v^2, uv-vu\rangle$, $\delta \in \mathbb{F}_{p^{d_j}}^{\times}$, $0 \le j \le s$. *In particular, there are a total of* $7(p^{d_1}+5)(p^{d_2}+5)\cdots(p^{d_s}+5)$ *ideals of R[G].*

2. *The dual* $I^{\perp}$ *of an ideal* $I = I_0 \times I_1 \times \cdots \times I_s$ *of R[G] is given by* $I^{\perp} = I^0_{\sigma(0)} \times I^0_{\sigma(1)} \times \cdots \times I^0_{\sigma(s)}$, *where* $\langle 0\rangle^0 = \langle 1\rangle, \langle u\rangle^0 = \langle u\rangle, \langle v\rangle^0 = \langle v\rangle, \langle u + v\delta\rangle^0 = \langle u + v\delta\rangle$ *for* $\delta \in \mathbb{F}_{p^{d_j}}^{\times}$, $0 \le j \le s$, *and* $\langle uv\rangle^0 = \langle u, v\rangle$.

Proof. Part 1 directly follows from Theorem 3.1 and Proposition 3.2. For part 2, we observe that the ideals of $\mathbb{F}_{p^d}[u,v]/\langle u^2, v^2, uv-vu\rangle$ are $\langle 0\rangle, \langle 1\rangle, \langle u\rangle, \langle v\rangle, \langle uv\rangle, \langle u+v\delta_j\rangle$, where $\delta_j \in \mathbb{F}_{p^{d_j}}^{\times}$, and $\langle u, v\rangle$. Using the annihilators of these ideals, we get part 2 of the theorem. □

Now onward, the ideals of $R[G]$ will be called abelian codes over R.

Proposition 3.4. *Let* $I = I_0 \times I_1 \times \cdots \times I_s \in R[G]$ *be an abelian code of length n over R, and*

$$\begin{aligned}
Res(I) &= R_0 \times R_1 \times \cdots \times R_s\ ,\\
Tor(I) &= T_0 \times T_1 \times \cdots \times T_s\ ,\\
Res(Res(I)) &= M_0 \times M_1 \times \cdots \times M_s\ ,\\
Tor(Res(I)) &= N_0 \times N_1 \times \cdots \times N_s\ ,\\
Res(Tor(I)) &= L_0 \times L_1 \times \cdots \times L_s\ ,\\
Tor(Tor(I)) &= K_0 \times K_1 \times \cdots \times K_s\ ,
\end{aligned}$$

where $R_j, T_j \subseteq I_j$ *are ideals of* $\mathbb{F}_{p^{d_j}}[u]/\langle u^2\rangle$ *and* $M_j, N_j, L_j, K_j \subseteq I_j$ *are ideals of* $\mathbb{F}_{p^{d_j}}$, $0 \le j \le s$. *Then*

1. $R_j = \langle 1\rangle \iff M_j = \langle 1\rangle \iff I_j = \langle 1\rangle$,
2. $T_j = \langle 0\rangle \iff K_j = \langle 0\rangle \iff I_j = \langle 0\rangle$,
3. *If* $I_j \neq \langle 1\rangle$*, then* $M_j = \langle 0\rangle$,
4. *If* $I_j \neq \langle 0\rangle$*, then* $K_j = \langle 1\rangle$.

Proof. Consider the maps $\Psi : R \to \mathbb{F}_p + u\mathbb{F}_p$ and $\Phi : R \to \mathbb{F}_p$ such that $\Psi(a + ub + vc + uvd) = a + ub$ and $\Phi(a+ub+vc+uvd) = a$. Then $Res(I), Res(Res(I))$ are the images of I under the map Ψ and Φ, respectively. Also, we have $Tor(I) = \{b : vb \in I\}$ and $Tor(Tor(I)) = \{d : uvd \in I\}$. It can be easily shown that $R_j = \Phi(I_j) = \langle 1\rangle$ if and only if $I_j = \langle 1\rangle$ if and only if $M_j = \langle 1\rangle$. Similarly, it can be shown that $T_j = \langle 0\rangle$ if and only if $I_j = \langle 0\rangle$ if and only if $K_j = \langle 0\rangle$. If $I_j \neq \langle 1\rangle$, then I_j contains only some non-unit elements of $\mathbb{F}_{p^{d_j}}[u, v]/\langle u^2, v^2, uv - vu\rangle$, which implies that $M_j = \langle 0\rangle$. If $I_j \neq \langle 0\rangle$, then $\langle uv\rangle \subseteq I_j$, i.e., $K_j = \langle 1\rangle$. Hence the result holds. □

In the next result, we have shown that, for $p = 2$, the Gray image $\phi(C)$ of an abelian code C over R is an abelian code in $\mathbb{F}_2[G \times \mathbb{Z}_2 \times \mathbb{Z}_2]$.

Theorem 3.5. *For* $p = 2$*, if* C *is an abelian code in* $R[G]$*, where* G *is an abelian group of order* n*, then the Gray image* $\phi(C)$ *of* C *is an* $\mathbb{F}_2$*-abelian code in* $\mathbb{F}_2[G \times \mathbb{Z}_2 \times \mathbb{Z}_2]$.

Proof. For any element $a = \sum_{g\in G}(a_g + ub_g + vc_g + uvd_g)Y^g \in R[G]$, the Gray image of a is an element of the form $a' = \sum_{(g,k,l)\in G\times\mathbb{Z}_2\times\mathbb{Z}_2} m_{(g,k,l)}Y^gZ^kW^l$ in $\mathbb{F}_2[G \times \mathbb{Z}_2 \times \mathbb{Z}_2]$, where

$$m_{(g,k,l)} = \begin{cases} a_g + b_g + c_g + d_g, & \text{if } (k, l) = (0, 0)\ , \\ c_g + d_g, & \text{if } (k, l) = (1, 0)\ , \\ b_g + d_g, & \text{if } (k, l) = (0, 1)\ , \\ d_g, & \text{if } (k, l) = (1, 1)\ . \end{cases}$$

We show that $\phi(C) = \{a' : a \in C\}$ is an ideal of the group ring $\mathbb{F}_2[G \times \mathbb{Z}_2 \times \mathbb{Z}_2]$. The addition and multiplication by Y in $\mathbb{F}_2[G\times\mathbb{Z}_2\times\mathbb{Z}_2]$ correspond to the ones in $R[G]$. Now consider the following points.

- Multiplication by W in $\mathbb{F}_2[G\times\mathbb{Z}_2\times\mathbb{Z}_2]$ corresponds to the multiplication of elements by $1 + u$ in $R[G]$.
- Multiplication by Z in $\mathbb{F}_2[G\times\mathbb{Z}_2\times\mathbb{Z}_2]$ corresponds to the multiplication of elements by $1 + v$ in $R[G]$.
- Multiplication by ZW in $\mathbb{F}_2[G\times\mathbb{Z}_2\times\mathbb{Z}_2]$ corresponds to the multiplication of elements by $1+u+v+uv$ in $R[G]$.

Therefore $\phi(C)$ is closed under multiplication by Y, Z and W. Clearly $\phi(C)$ is closed under multiplication by elements of $\mathbb{F}_2$. Hence $\phi(C)$ is an ideal of $\mathbb{F}_2[G \times \mathbb{Z}_2 \times \mathbb{Z}_2]$. □

Now let $I = I_0 \times I_1 \times \cdots \times I_s \in R[G]$ be an abelian code of length n over R. Then for every $h \in O_i$, $\hat{f}_h \in \mathbb{F}_{p^{d_i}}[u, v]/\langle u^2, v^2, uv - vu\rangle$, $0 \le i \le s$, where O_i are the orbits of G under the mapping $x \mapsto px$. Moreover,

$$\hat{f}_0 = \sum_{g\in G} f_g \in I_0 \subseteq R\ ,$$

for any codeword $c \in I$.

Let α be an automorphism of G. Then a partition (X, A, B) of G is called a splitting of G if X, A and B are unions of the orbits $O_0, O_1, \ldots, O_s$ and $\alpha(A) = B$, $\alpha(B) = A$. Let τ be the permutation of $\{0, 1, \ldots, s\}$ induced by the map $x \mapsto \alpha x$ in G. In particular, when $\alpha = -1$, we have $\tau = \sigma$. For any ideal $I = I_0 \times I_1 \times \cdots \times I_s$, we define $I^\alpha = I_{\tau(0)} \times I_{\tau(1)} \times \cdots \times I_{\tau(s)}$, the image of I under the multiplier α. It is, in fact, the image of I under the isometry

$$\sum_{g\in G} f_gX^g \mapsto \sum_{g\in G} f_gX^{\alpha^* g}\ ,$$

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

4. Duadic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$

In this section, we assume that G is an additive abelian group of order n, where n is odd. We define duadic codes over $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$ and study their properties related to self-duality and self-orthogonality. We also study generalized duadic codes over R.

We define a duadic code of length n over R attached to a splitting (X, A, B) of G to be an ideal $I = I_0 \times I_1 \times \cdots \times I_s$ of $R[G]$ which satisfies the following conditions: if $O_j \subseteq X$, then I_j is one of the ideals $\langle u\rangle$, $\langle v\rangle$, and $\langle u + v\delta_j\rangle$ for some $\delta_j \in \mathbb{F}^{\times}_{p^{d_j}}$, and if $O_j \subseteq A$ or B, then I_j is any of the ideals of $\mathbb{F}_{p^{d_j}}[u, v]/\langle u^2, v^2, uv - vu\rangle$ satisfying $I_{\tau(j)} = I^0$.

For an ideal I_j of $\mathbb{F}_{p^{d_j}}[u, v]/\langle u^2, v^2, uv - vu\rangle$, $1 \le j \le s$, if $I_j = \langle u\rangle$ or $\langle v\rangle$ or $\langle u + v\delta_j\rangle$, where $\delta_j \in \mathbb{F}^{\times}_{p^{d_j}}$, then I_j is self-dual. We call these ideals as trivial self-dual ideals.

Theorem 4.1. *If no non-trivial self-dual code exists over $R[G]$, then σ is an identity map, where σ is as defined above. The converse need not be true.*

Proof. Assume that σ is not an identity map. Then there always exists a nontrivial self-dual code $I = I_0 \times I_1 \times \cdots \times I_s$ by taking $I_j = \langle 0\rangle$ if and only if $I_{\sigma(j)} = \langle 1\rangle$. For the converse, consider for example that G has exactly three orbits O_0, O_1 and O_2 under the map $x \mapsto px$. Let $X = O_0, A = O_1, B = O_2$, and $I = \langle u\rangle \times \langle uv\rangle \times \langle u, v\rangle$. Then σ is an identity map on the set $\{0, 1, 2\}$, but I is a nontrivial self-dual code. □

Theorem 4.2. *Suppose σ is not an identity map and (X, A, B) is a splitting of G given by $\alpha = -1$. Then the duadic code attached to (X, A, B) is self-dual. Conversely, every self-dual abelian code over R is a duadic code attached to a splitting of G with $\alpha = -1$.*

Proof. First part follows from the definition of duadic codes. Suppose $I = I_0 \times I_1 \times \cdots \times I_s$ is a self-dual abelian code. Then $I = I^0_{\sigma(0)} \times I^1_{\sigma(1)} \times \cdots \times I^s_{\sigma(s)}$. We have $\sigma(0) = 0$ as $\sigma(x) = -x$, which implies that $I^0_0 = I_0$. This in turn implies that $I_0 = \langle u\rangle$ or $\langle v\rangle$ or $\langle u + v\rangle$. Let $O_0, O_1, \ldots, O_s$ be the orbits of G. Define

$$\begin{aligned}
A_1 &= \cup O_j, \quad \text{where } I_j = \langle u\rangle\,,\\
A_2 &= \cup O_j, \quad \text{where } I_j = \langle v\rangle\,,\\
A_3 &= \cup O_j, \quad \text{where } I_j = \langle u + v\delta_j\rangle \text{ for some } \delta_j \in \mathbb{F}^{\times}_{p^{d_j}},\\
A_4 &= \cup O_j, \quad \text{where } I_j = \langle u, v\rangle\,,\\
A_5 &= \cup O_j, \quad \text{where } I_j = \langle uv\rangle\,,\\
A_6 &= \cup O_j, \quad \text{where } I_j = \langle 0\rangle\,,\\
A_7 &= \cup O_j, \quad \text{where } I_j = \langle 1\rangle\,.
\end{aligned}$$

Now let $X = A_1 \cup A_2 \cup A_3, A = A_4 \cup A_5, B = A_6 \cup A_7$. We have $O_0 \subset X$, as $I_0 = \langle u\rangle$ or $\langle v\rangle$ or $\langle u + v\rangle$. Then the self-dual abelian code I is a duadic code attached to the splitting (X, A, B) with $\alpha = -1$. □

4.1. Generalized duadic codes

We define generalized duadic codes in the same way as duadic codes, except that in generalized duadic codes there is no restriction on the ideal I_0, i.e., I_0 can be any of the ideals $\langle 0\rangle, \langle 1\rangle, \langle u\rangle, \langle v\rangle, \langle uv\rangle, \langle u + v\delta_j\rangle$ or $\langle u, v\rangle$.

Theorem 4.3. *Let $C = I_0 \times I_1 \times \cdots \times I_s$ be a generalized duadic code over R attached to a splitting of G with $\alpha = -1$. If $I_0 = \langle uv\rangle$ or $\langle 0\rangle$, then C is self-orthogonal.*

Proof. The result follows from the fact that $\langle 0\rangle \subset \langle 0\rangle^0 = \langle 1\rangle$, and $\langle uv\rangle \subset \langle uv\rangle^0 = \langle u, v\rangle$. □

Proposition 4.4. *Suppose σ is an identity map on G, i.e., $\sigma(i) = i$ for all i, $0 \le i \le s$. If $C = I_0 \times I_1 \times \cdots \times I_s$ is a duadic code attached to a splitting (X, A, B) of G, then C is isodual. Also, if C is a generalized duadic code and $I_0 = \langle 0\rangle$ or $\langle uv\rangle$, then $C^{\alpha} \subseteq C^{\perp}$, where α is the corresponding multiplier.*

Proof. We have $C^{\perp} = I^0_{\sigma(0)} \times I^0_{\sigma(1)} \times \cdots \times I^0_{\sigma(s)} = I^0_0 \times I^0_1 \times \cdots \times I^0_s = C$, as σ is an identity map on G. If C is a duadic code, then $I^0_0 = I_0$. We have $C^{\alpha} = I_{\tau(0)} \times I_{\tau(1)} \times \cdots \times I_{\tau(s)}$. Define τ such that $I_{\tau(j)} = I^0_j$. Then $C^{\alpha} = C^{\perp}$, i.e., C is isodual. If C is a generalized duadic code with $I_0 = \langle 0\rangle$ or $\langle uv\rangle$, then $I^0_0 = \langle 1\rangle$ or $\langle u, v\rangle$, respectively, i.e., $I^0_0 \subseteq I_0$, which implies that $C^{\alpha} \subseteq C^{\perp}$. □

5. The minimum Lee distance of the duadic code over R

In this section, we discuss some results about the Lee distance of duadic codes over R, and also discuss results related to Hamming distance of abelian codes over R. First we have the following elementary result for the case $p = 2$.

Theorem 5.1. *Let $p = 2$ and let $C = I_0 \times I_1 \times \cdots \times I_s$ be a duadic code of length n over $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, where $I_j \neq \langle 0\rangle$ for any j. Then the Lee distance $d_L(C)$ of C is even.*

Proof. From the definition of Lee weight on R, for any $a \in R$ we have $w_L(a)$ is odd if a is a unit and $w_L(a)$ is even when a is not a unit. Now $I_j \neq \langle 0\rangle\ \forall j$, then $I_j \neq \langle 1\rangle\ \forall j$. Therefore all coordinates in any codeword of C are non-units. The result follows. □

Theorem 5.2. *The Hamming distances of all the non-trivial codes (ideals) of the ring $\mathbb{F}_{p^d}[u, v]/\langle u^2, v^2, uv - vu\rangle$, as given in Proposition 3.2, are the same.*

Proof. The proof parallels that of [8, Theorem 5.1]. We show first that the Hamming distances of $\langle uv\rangle$ and $\langle u, v\rangle$ are the same. Let $d_1 = d_H(\langle uv\rangle)$ and $d_2 = d_H(\langle u, v\rangle)$. So, we have to show that $d_1 = d_2$. Clearly $\langle uv\rangle \subseteq \langle u, v\rangle$, which implies that $d_1 \geq d_2$. Now suppose $d_1 > d_2$. So, there exists a non-zero element $c = (c_0, c_1, \cdots, c_{n-1}) \in \langle u, v\rangle$ with the Hamming weight d_2 which is not in $\langle uv\rangle$. Then there must be a coordinate c_i in c such that c_i is of the form $c_i = u\alpha + vc'' + uvc'''$ or $c_i = uc' + v\alpha + uvc'''$ for some $c', c'', c''' \in \mathbb{F}_{p^d}$ and $\alpha \in \mathbb{F}^{\times}_{p^d}$. Now define β such that

$$\beta = \begin{cases} v, & \text{if } c_i = u\alpha + vc'' + uvc''' , \\ u, & \text{if } c_i = uc' + v\alpha + uvc''' . \end{cases}$$

It is easy to see that $\beta c \in \langle uv\rangle$, and $\beta c \neq 0$. Since $\beta c \in \langle uv\rangle$, we get $d_1 \leq w_H(\beta c) \leq w_H(c) = d_2 < d_1$, which is a contradiction. Therefore we must have $d_1 = d_2$. Now consider the ideals $\langle u\rangle$, $\langle v\rangle$ and $\langle u + v\delta\rangle$, where $\delta \in \mathbb{F}^{\times}_{2^d}$. Let $d_3 = d_H(\langle u\rangle)$, $d_4 = d_H(\langle v\rangle)$ and $d_5 = d_H(\langle u + v\delta\rangle)$. Clearly $\langle uv\rangle \subseteq \langle u\rangle$, $\langle uv\rangle \subseteq \langle v\rangle$ and $\langle uv\rangle \subseteq \langle u + v\delta\rangle$, which implies that $d_1 \geq d_3, d_1 \geq d_4$ and $d_1 \geq d_5$. Now suppose $d_1 > d_3, d_4, d_5$. Then there exist non-zero elements $v' = (v_0, v_1, \cdots, v_{n-1}) \in \langle u\rangle, w = (w_0, w_1, \cdots, w_{n-1}) \in \langle v\rangle$ and $t = (t_0, t_1, \cdots, t_{n-1}) \in \langle u + v\delta\rangle$ with Hamming weights d_3, d_4 and d_5, respectively, such that none of v', w and t is in $\langle uv\rangle$. Now $uv', uw, ut \in \langle uv\rangle$ and it is easy to see that vv', uw and ut all are non-zero elements of $\langle uv\rangle$. This implies that $d_1 \leq w_H(vv') \leq w_H(v') = d_3 < d_1$, $d_1 \leq w_H(vv') \leq w_H(v') = d_4 < d_1$ and $d_1 \leq w_H(vv') \leq w_H(v') = d_5 < d_1$, a contradiction in each case. Therefore, we must have $d_1 = d_2 = d_3 = d_4 = d_5$. □

The following result gives a sufficient condition for two abelian codes of same length over R to have the same minimum distance.

Theorem 5.3. *Let $C_1 = I_0 \times I_1 \times \cdots \times I_s$ and $C_2 = I'_0 \times I'_1 \times \cdots \times I'_s$ be two abelian codes of length n over R, where I_j and I'_j are ideals of $\mathbb{F}_{2^{d_j}}[u, v]/\langle u^2, v^2, uv - vu\rangle$, $0 \leq j \leq s$. If for every j, I_j and I'_j are both zero or both non-zero, then $d_H(C_1) = d_H(C_2)$.*

Proof. Since C_1 is a direct product of $I_0, I_1, \ldots, I_s$, the minimum distance of C_1 is equal to the minimum among the minimum distances of $I_0, I_1, \ldots, I_s$ with $I_j \neq 0$. Similarly, the minimum distance of C_2 is the minimum among the minimum distances of $I'_0, I'_1, \ldots, I'_s$ with $I'_j \neq 0$. Now I_j and I'_j are either both zero or both non-zero for all j. Also, from Theorem 5.2, $d_H(I_j) = d_H(I'_j)$ for $I_j, I'_j \neq \langle 0\rangle$. It follows that $d_H(C_1) = d_H(C_2)$. □

6. Augmented and extended abelian codes over R

Recall that for any linear code C of length n over R, and $\epsilon \in R$, the augmented and extended code $(\overline{C})_\epsilon$ is defined by

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

where $c_\infty = \sum_{i=0}^{n-1} c_i$ for any $c = (c_0, c_1, \ldots, c_{n-1}) \in C$.

Theorem 6.1. *Suppose ϵ is a unit in R, G is an abelian group of order n, and (X, A, B) is a splitting of G given by $\alpha = -1$. Let C be the corresponding generalized duadic code over R. Then $(\overline{C})_\epsilon$ is self-dual if and only if $\epsilon^2 n + 1 \equiv 0 \mod p$.*

Proof. If $(\overline{C})_\epsilon$ is a self-dual code for some unit $\epsilon \in R$, then $(\mathbf{1}, \epsilon n) \cdot (\mathbf{1}, \epsilon n) = 0$ in R implies that $\epsilon^2 n + 1 \equiv 0 \mod p$. Conversely, it is easy to observe that $(\overline{C})_\epsilon$ contains exactly $p^{2(n+1)}$ elements. Note also that the choice of the ideal I_0 is irrelevant when we consider the augmented and extended code. Therefore, we may assume C to be a duadic code and take $I_0 = \langle v \rangle$. By Theorem 4.3, C is self-orthogonal. Then for any codewords $c = (c_0, c_1, \ldots, c_{n-1})$ and $c' = (c'_0, c'_1, \ldots, c'_{n-1})$ in C, the following conditions are satisfied:

$$(c, c_\infty) \cdot (c', c'_\infty) = 0\,, \quad (1)$$
$$(c, c'_\infty) \cdot (\mathbf{1}, \epsilon n) = 0\,, \quad (2)$$
$$(\mathbf{1}, \epsilon n) \cdot (\mathbf{1}, \epsilon n) = 0\,, \quad (3)$$

where $c_\infty = \epsilon \sum_{i=0}^{n-1} c_i$ and $c'_\infty = \epsilon \sum_{i=0}^{n-1} c'_i$. Equation (1) holds because C is self-orthogonal and $c_\infty, c'_\infty \in \langle v \rangle$, as $c_\infty = \epsilon \hat{c}_0, c'_\infty = \epsilon \hat{c}'_0 \in I_0$. For equation (2), the left hand side is equal to $(n+1) \sum_{i=0}^{n-1} c_i$, and for equation (3), the left hand side is equal to $n(\epsilon^2 n + 1)$. Since $(n, p) = 1$, therefore the result holds as $\epsilon^2 n + 1 \equiv 0 \mod p$. □

If $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, then for any $a \in R$, we have [29]

$$a^2 = \begin{cases} 0, & \text{if } a \text{ is a non-unit}\,, \\ 1, & \text{otherwise}\,. \end{cases}$$

The following result then follows immediately from Theorem 6.1.

Corollary 1. Let $p = 2$, i.e., $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Suppose ϵ is a unit in R, G is an abelian group of order n, and (X, A, B) is a splitting of G given by $\alpha = -1$. Let C be the corresponding generalized duadic code over R. Then $(\overline{C})_\epsilon$ is self-dual if and only if n is odd.

Theorem 6.2. *Let G be an abelian group of order n and C be an abelian code in $R[G]$. If $(\overline{C})_\epsilon$ is a self-dual code for unit $\epsilon \in R$, then $\epsilon^2 n + 1 \equiv 0 \mod p$ and C is a generalized duadic code attached to a splitting (X, A, B) of G given by $\alpha = -1$. In particular, any self-dual augmented and extended abelian code over R is the augmented and extended code of a duadic code.*

Proof. Since $(\overline{C})_\epsilon$ is self-dual, from Theorem 6.1, $\epsilon^2 n + 1 \equiv 0 \mod p$. Let the abelian code C be given by $C = I_0 \times I_1 \times \cdots \times I_s$. Consider the orbits of G. Let X' denote the union of the orbits O_i for which each I_i is one of the ideals $\langle u \rangle, \langle v \rangle$ and $\langle u + v \rangle$; A be the union of the orbits O_i for which each I_i is one of the ideals $\langle u, v \rangle$ and $\langle 1 \rangle$; and B be the union of the orbits O_i for which I_i is one of the ideals $\langle uv \rangle$ and $\langle 0 \rangle$. The augmented code $\overline{C}$ is given by $\overline{I}_0 \times I_1 \times \cdots \times I_s$, where $\overline{I}_0 = \langle 1 \rangle$. From Theorem 3.3, we know that the dual of C is given by $C^\perp = I^0_{\sigma(0)} \times I^0_{\sigma(1)} \times \cdots \times I^0_{\sigma(s)}$.

Let $c \in C$, and $c' \in C^\perp$. The from equation (1), we have

$$(c, c_\infty) \cdot (c', c'_\infty) = 0\,.$$

It is also easy to see that

$$(\mathbf{1}, \epsilon n) \cdot (c', c'_\infty) = 0 \,.$$

Therefore $(C^\perp)_\epsilon \subseteq ((\overline{C})_\epsilon)^\perp \subseteq (\overline{C})_\epsilon$, which implies that $C^\perp \subseteq \overline{C}$.

Now if $I_0 = \langle uv \rangle$, then we have $[\overline{C} : C] = |I_0^0| = p^3$, where $[\overline{C} : C]$ denotes the index of C in $\overline{C}$ as a subgroup. As $C^\perp \subseteq \overline{C}$, it can easily be shown that $[\overline{C} : C^\perp] = |I_0| = p$. This means in particular that $I^0_{\sigma(j)} = I_j$ for $0 \le j \le s$. This implies that $(X' \cup \{0\}, A, B)$ gives a splitting of G by $\alpha = -1$, and C is therefore a generalized duadic code attached to this splitting. □

6.1. Isoduality

For a given abelian code over R, a multiplier α acts on C by permutation of coordinates. We define the action of a multiplier α on the augmented and extended code $(\overline{C})_\epsilon$ by the rule $(c, c_\infty) \mapsto (c^\alpha, c_\infty)$. Hence $((\overline{C})_\epsilon)^\alpha = ((\overline{C})^\alpha)_\epsilon$. We say that $(\overline{C})_\epsilon$ is isodual with respect to α if $((\overline{C})_\epsilon)^\perp = ((\overline{C})^\alpha)_\epsilon$. Here we assume that σ is an identity map.

It can be observed that a multiplier α leaves the parity-check coordinate c_∞ of every codeword unchanged while acting as a permutation on the other coordinates. The following result follows from this observation.

Theorem 6.3. *Suppose ϵ is a unit in R. Let G be an abelian group of order n, and (X, A, B) be a splitting of G given by α. Let C be an attached generalized duadic code over R. Then $(\overline{C})_\epsilon$ is isodual by α if and only if $\epsilon^2 n + 1 \equiv 0 \mod p$.*

Furthermore, if we replace $\overline{C}$ by $\overline{C}^\alpha$ in Theorem 6.2, we get the following result.

Theorem 6.4. *Suppose ϵ is a unit in R. Let G be an abelian group of order n, and (X, A, B) be a splitting of G given by α. Let C be an attached generalized duadic code over R such that $(\overline{C})_\epsilon$ is isodual by a multiplier α. Then $\epsilon^2 n + 1 \equiv 0 \mod p$ and C is a generalized duadic code given by α. In particular, when I_0 is one of the ideals $\langle u \rangle, \langle v \rangle$ and $\langle u + v \rangle$, any augmented and extended abelian code over R 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.* □

7. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$

In this section, we consider $p = 2$, so that $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Here we give a criterion for self-dual augmented and extended abelian codes over R to be of Type II.

Definition 7.1. *[1] A self-dual code over R is said to be Type II if the Lee weight of every codeword is a multiple of* 4 *and Type I otherwise.*

In the following lemma, we use a constant $\mathcal{A}$. The value of this constant is given by the authors in [1].
Lemma 1 [1] If C is a linear code over R, then for any two codewords $c, c' \in C$, we have

$$w_L(c + c') = w_L(c) + w_L(c') - 2\mathcal{A} \mod 4,$$

where $\mathcal{A}$ is as defined in [Theorem 4, 1].

Theorem 7.2. *Let $C = I_0 \times I_1 \times \cdots \times I_s$ be a generalized duadic code over R attached to a splitting (X, A, B) of an abelian group G given by $\alpha = -1$ and with $I_0 = \langle 0 \rangle$. Then the Lee weights of all the codewords in C are multiples of* 4.

Proof. Define a map $f : C \to \mathbb{Z}_4$ such that

$$c \mapsto w_L(c) \mod 4 \,.$$

Since C is a self-orthogonal code, the number of units in every codeword must be even. Therefore $\mathcal{A}$ is even, where $\mathcal{A}$ is as defined above. Hence, from Lemma **1**.

$$f(c + c') = f(c) + f(c'),$$

i.e., f is a group homomorphism. As C is a self-orthogonal code, from Theorem 4.3 the Lee weight of any codeword in C is even. Therefore the image of f is contained in the ideal $\langle 2\rangle$ of $\mathbb{Z}_4$. Further, since $\ker f$ is an ideal of the ring $\mathbb{Z}_4[G]$, the index of $\ker f$ when considered as a subgroup of $\mathbb{Z}_4[G]$ is 1 or 2. Now suppose $C = I_0 \times I_1 \times \cdots \times I_s$, and $\ker f = I'_0 \times I'_1 \times \cdots \times I'_s$, where $I'_j \subseteq I_j$, $0 \le j \le s$. Since the only orbit of G of size 1 is the orbit $O_0 = \{0\}$, this means that $I_j = I'_j$ for all j, $1 \le j \le s$, and I'_0 is of index 1 or 2 in I_0. But $I_0 = \langle 0\rangle$ and hence cannot contain an ideal of index 2. Therefore, $\ker f = C$, i.e., all the codewords in C have Lee weights multiples of 4. Hence the result. □

We divide the units of R into two subsets U_1 and U_2 as follows.

$$\begin{aligned} U_1 &= \{1, 1+u, 1+v, 1+u+v+uv\}, \\ U_2 &= \{1+v+v, 1+u+uv, 1+v+uv, 1+uv\}. \end{aligned}$$

Then for any unit $a \in R$, we have

$$w_L(a) = \begin{cases} 1, & \text{if } a \in U_1, \\ 3, & \text{if } a \in U_2. \end{cases}$$

Theorem 7.3. *If $\epsilon \in U_1$, then a self-dual augmented and extended Abelian code $(\overline{C})_\epsilon$ of length n is of Type II if and only $n + 1 \equiv 0$ mod 4.*

Proof. Since $(\mathbf{1}, \epsilon n) \in (\overline{C})_\epsilon)$, the assumption that such a code is of *Type* II implies that $(\mathbf{1}, \epsilon n)\cdot(\mathbf{1}, \epsilon n) = n+1 \equiv 0$ mod 4.

Conversely, suppose that $n + 1 \equiv 0$ mod 4. From Theorem 6.2, C is a generalized duadic code attached to a splitting (X, A, B) of G given by $\alpha = -1$, such that $I_0 = \langle 0\rangle$. We need to show that all words of the form $(c, c_\infty) + \lambda(\mathbf{1}, \epsilon n)$ have Lee weights multiples of 4. For $I_0 = \langle 0\rangle$, we have $c_\infty = 0$. Now, as $n + 1 \equiv 0 \pmod 4$, from Theorem 7.2, we have

$$\begin{aligned} w_L((c, c_\infty)) &= w_L((c, 0)) \equiv 0 \pmod 4, \\ w_L((\mathbf{1}, \epsilon n)) &= w_L((\mathbf{1}, 1)) \equiv 0 \pmod 4, \text{ and} \\ w_L((c, c_\infty) + \lambda(\mathbf{1}, \epsilon n)) &= w_L((c, c_\infty)) + w_L(\lambda(\mathbf{1}, \epsilon n)) \equiv 0 \pmod 4. \end{aligned}$$

Hence the result holds. □

8. Examples

Now, we present some examples of abelian codes over R. All the computations to determine minimum distance of codes were performed in Magma [32].

Example 8.1. *Let $p = 2$, i.e., $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, and $n = 9$. Suppose $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.. Orbits of G are given by $O_0 = \{00\}$, $O_1 = \{01, 02\}$, $O_2 = \{10, 20\}$, $O_3 = \{11, 22\}$, and $O_4 = \{12, 21\}$. Hence*

$$R[G] \simeq R \times \mathscr{R}_{u,v,2} \times \mathscr{R}_{u,v,2} \times \mathscr{R}_{u,v,2} \times \mathscr{R}_{u,v,2},$$

the corresponding abelian codes of length 9 are presented in Table 1, where the codes are specified by their components in each of the five orbits. For example, $1-1-1-1-u$ represents the code whose components from the five orbits in the above order are $1, 1, 1, 1,$ and u, respectively. The codes with * denote binary optimal codes.

Example 8.2. *Let $p = 3$, i.e., $R = \mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$, and $n = 4$. Suppose $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Orbits of G are given by $O_0 = \{00\}$, $O_1 = \{01\}$, $O_2 = \{10\}$, $O_3 = \{11\}$. Hence*

$$R[G] \simeq R \times R \times R \times R,$$

the corresponding abelian codes of length 4 are presented in Table 2. The codes with * denote ternary optimal codes.

Table 1: Duadic codes of $R(\mathbb{Z}_3 \times \mathbb{Z}_3)$, $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$.

Abelian code(C)	$\phi(C)$	Comments for $\phi(C)$
$0-0-0-0-uv$	$[36,2,24]^*$	Self-orthogonal
$0-0-0-uv-0$	$[36,2,24]^*$	Self-orthogonal
$0-0-uv-0-0$	$[36,2,24]^*$	Self-orthogonal
$0-uv-0-0-0$	$[36,2,24]^*$	Self-orthogonal
$u-(u+v)-(u+v)-1-1$	$[36,26,4]^*$	
$u-(u+v)-v-1-1$	$[36,26,4]^*$	
$u-(u+v)-u-1-1$	$[36,26,4]^*$	
$v-1-1-u-v$	$[36,26,4]^*$	
$v-1-1-u-(u+v)$	$[36,26,4]^*$	
$v-1-1-v-(u+v)$	$[36,26,4]^*$	
$u-u-1-v-1$	$[36,26,4]^*$	
$u-u-v-1-1$	$[36,26,4]^*$	
$v-1-1-(u+v)-(u+v)$	$[36,26,4]^*$	
$1-u-1-1-1$	$[36,32,2]^*$	
$1-v-1-1-1$	$[36,32,2]^*$	
$1-1-(u+v)-1-1$	$[36,32,2]^*$	
$1-1-1-(u+v)-1$	$[36,32,2]^*$	
$(u+v)-u-u-u-u$	$[36,18,4]$	Self-dual
$v-u-u-u-u$	$[36,18,4]$	Self-dual
$u-u-v-v-u$	$[36,18,4]$	Self-dual
$v-u-v-v-u$	$[36,18,4]$	Self-dual
$(u+v)-u-v-v-u$	$[36,18,4]$	Self-dual
$u-u-u-u-u$	$[36,18,2]$	Self-dual

9. Conclusion

In this paper, we have studied duadic codes over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, $u^2 = v^2 = 0, uv = vu$. These codes have been studied here by considering them as a special class of abelian codes. Through their residue codes and torsion codes, we have determined some characterizations of these codes. Some conditions related to their self-orthogonality and self-duality are obtained. Also, some results related to minimum Lee distances of duadic codes over R are presented. We have also studied Type II self-dual augmented and extended codes over R. Some optimal binary linear codes of length 36 have been obtained as Gray images of duadic codes of length 9 over R.

Table 2: Duadic codes of $R(\mathbb{Z}_2 \times \mathbb{Z}_2)$, $R = \mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$.

Abelian code(C)	$\phi(C)$
$0 - 0 - 0 - uv$	$[16, 1, 16]^*$
$0 - 0 - uv - 0$	$[16, 1, 16]^*$
$0 - uv - 0 - 0$	$[16, 1, 16]^*$
$0 - 0 - 0 - uv$	$[16, 1, 16]^*$
$1 - 1 - 1 - u$	$[16, 14, 2]^*$
$1 - 1 - 1 - v$	$[16, 14, 2]^*$
$1 - 1 - 1 - u * v$	$[16, 13, 2]^*$
$1 - 1 - u * v - 1$	$[16, 13, 2]^*$
$1 - u * v - 1 - 1$	$[16, 13, 2]^*$
$u * v - 1 - 1 - 1$	$[16, 13, 2]^*$
$1 - u - u - v$	$[16, 10, 4]^*$
$1 - u - u - (u + v)$	$[16, 10, 4]^*$
$1 - u - v - u$	$[16, 10, 4]^*$
$1 - u - v - v$	$[16, 10, 4]^*$
$1 - u - v - (u + v)$	$[16, 10, 4]^*$
$1 - u - (u + v) - (u + v)$	$[16, 10, 4]^*$
$1 - v - (u + v) - (u + v)$	$[16, 10, 4]^*$
$u - 1 - u - v$	$[16, 10, 4]^*$
$u - 1 - u - (u + v)$	$[16, 10, 4]^*$
$v - 1 - u - v$	$[16, 10, 4]^*$
$v - 1 - u - (u + v)$	$[16, 10, 4]^*$
$(u + v) - 1 - u - v$	$[16, 10, 4]^*$
$(u + v) - 1 - u - (u + v)$	$[16, 10, 4]^*$

References

[1] Ankur, P.K. Kewat, Type I and Type II codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Asian-European J. Math. 12(01) (2019) 1950025.

[2] S.D. Berman, Semisimple cyclic and abelian codes II Kibernetika, 03(03) (1967) 17-23.

[3] P. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ IEEE Trans. Inform. Theory 45(4) (1999) 1250-1255.

[4] S.T. Dougherty, P. Gaborit, M. Harada, P. Solé, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, 45(1) (1999) 32–45.

[5] Y. Haifeng, S. Zhu, X.Kai, $(1 - uv)$-Constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, J. Syst. Sci. Complex., 27(4) (2014) 811-816.

[6] A. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Slone, P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock Preparata Goethals and related codes, IEEE Trans. Inform. Theory 40(4) (1994) 301-319.

[7] X. Kai, S. Zhu, L. Wang, A family of constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Syst. Sci. Complex. 25(5) (2012) 1032-1040.

[8] R. Kumar, M. Bhaintwal, Duadic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ Adv. Math. Comm. (2021), doi: 10.3934/amc.2020135.

[9] R. Kumar, M. Bhaintwal, R.K. Bandi: Ideal structure of $\mathbb{Z}_q + u\mathbb{Z}_q$ and $\mathbb{Z}_q + u\mathbb{Z}_q$-cyclic codes, Filomat 34(12) (2020) 4199-4214.

[10] P. Langevin, P. Solé, Duadic $\mathbb{Z}_4$-codes Finite Fields Their Appl. 06(04) (2000) 309-326.

[11] P. Li, X. Guo, S. Zhu, Z. Shixin, K. Xiaoshan, Some results on linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$, J. Appl. Math. Comput. 54 (2017) 307-324.

[12] J. Leon, J. Masley, V. Pless, Duadic Codes IEEE Trans. Inform. Theory 30(5) (1984) 709-714.

[13] S. Ling, P. Solé, Duadic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, Appl. Algebra Engrg. Comm. Comput. 12(05) (2000) 365-389.

[14] Y. Liu, M. Shi, P. Solé, Two-weight and three weight codes from trace codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, Discrete Mathematics 341 (2018) 350-357.

[15] S. Ling, P. Solé, Duadic codes over $\mathbb{Z}_{2k}$ IEEE Trans. Inform. Theory 47(04) (2000) 1581-1588.

[16] F.J. MacWilliams, Binary codes which are ideals in the group algebra of an abelian group, Bell Syst. Tech. J. 49 (1970) 987-1011.

[17] B.S. Rajan, M.U. Siddiqui, Transform domain characterzation of cyclic codes over $\mathbb{Z}_m$, Appl. Algebra Engrg. Comm. Comput. 5 (1994) 261-275.

[18] B.S. Rajan, M.U. Siddiqui, A generalized DFT for abelian codes over $\mathbb{Z}_m$ IEEE Trans. Inform. Theory 40(06) (1994) 2082-2090.

[19] J. Rushanan, Duadic codes and difference sets, J. Combin. Theory Ser. 57 (1991) 254-261.

[20] M. Shi, L. Qian, L. Sok, N. Aydin, On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$ and their Gray images, Finite Fields Their Appl. 45 (2017) 86-95.

[21] M. Shi, D. Haung, L. Sok, P. Solé, Double circulant LCD codes over $\mathbb{Z}_4$ Finite Fields Their Appl. 58 (2019) 133-144.

[22] M. Shi, H. Zhu, L. Qian, S. Sok, P. Solé, On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$ Crypogr. Commun. 12 (2020) 53–70.
[23] M. Shi, C.C. Wang, R.S. Wu, Y.Q. Chang, One-weight and two-weight $\mathbb{Z}_2\mathbb{Z}_2[uv]$-additive codes Crypogr. Commun. 12 (2020) 443-454.
[24] M. Shi, L. Qian, P. Sole, On self-dual negacirculant codes of index two and four Des. Codes Cryptogr. 86(11) (2018) 2485-2494.
[25] E Speigel, Codes over $\mathbb{Z}_m$ Infrom. Control 35(6) (1977) 48-51.
[26] van Tilborg H.C.A, On weights in codes Rep. 71-WSK-03 Department of Math. Tech. University of Eindhoven Netherlands (1971).
[27] Wang L. Zhu S, Repeated-root constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Pure and Appl. Algebra 222(10) (2018) 2952-2963.
[28] B. Yildiz, S. Karadenniz, Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr. 54 (2010) 61-81.
[29] B. Yildiz, S. Karadenniz,, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr. 58(3) (2011) 221-234.
[30] B. Yildiz, S. Karadenniz,, Self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst. 347 (2010) 1888-1894.
[31] Wan Z.X, Finite fields and Galois rings World Scientific Pub. Co Inc. Singapore (2012).
[32] http://magma.maths.usyd.edu.au/magma/.