Duadic codes over F2 + uF2

Ling, San; Sole, Patrick

2001

Ling, S. & Solé, P. (2001). Duadic Codes over F2 + uF2. Applicable Algebra in Engineering, Communication and Computing, 12(5), 365-379.

https://hdl.handle.net/10356/95882

https://doi.org/10.1007/s002000100079

Duadic Codes over $\mathbf{F}_2 + u\mathbf{F}_2$

San Ling[1,*], Patrick Solé[2,]**

[1] Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: lings@math.nus.edu.sg)
[2] CNRS-I3S, ESSI, Route des Colles, 06 903 Sophia Antipolis, France (e-mail: ps@essi.fr)

Abstract. Duadic codes over $\mathbf{F}_2 + u\mathbf{F}_2$ are introduced as abelian codes by their zeros. This is the function field analogue of duadic codes over $\mathbf{Z}_4$ introduced recently by Langevin and Solé. They produce binary self-dual codes via a suitable Gray map. Their binary images are themselves abelian, thus generalizing a result of van Lint for cyclic binary codes of even length. We classify them in modest lengths and exhibit interesting non-cyclic examples.

Keywords: Abelian codes, Duadic codes, Self-dual, Isodual, Type II codes, Splitting.

1 Introduction

Duadic codes constitute a well-known class of cyclic codes. They provide a natural way to construct self-dual codes with a rich automorphism group. See the introduction section of [5] for references and historical perspective. They were generalized recently to $\mathbf{Z}_4$-codes [7]. In this article they are generalized to the context of abelian codes over $\mathbf{F}_2 + u\mathbf{F}_2$, the function field analogue of the former alphabet. While linear, the binary images of $\mathbf{F}_2 + u\mathbf{F}_2$-codes seem to perform just as well as their $\mathbf{Z}_4$-analogues. Furthermore they are shown here to be abelian for a double cover of the group from which their quaternary antecedent is defined. This extends an old result of van Lint for repeated roots cyclic binary codes [8].

*This work was done when the first named author was visiting CNRS-I3S, ESSI, Sophia Antipolis, France. The author would like to thank the institution for the kind hospitality. The research of this author is partially supported by MOE-ARF research grant R-146-000-018-112.
**The second named author is grateful to AGAT laboratory for its hospitality of nine months.

The material is organized as follows. Section 2 collects the relevant notations and definitions. Section 3 develops the algebraic machinery needed to study abelian codes. Section 4 introduces duadic codes and Section 5 studies their extensions by a parity-check with respect to self-duality and isoduality. Section 6 is concerned with Type II codes in the sense of [6]. Section 7 explores duadic codes of modest lengths with a special emphasis on non-cyclic examples.

2 Notations and Definitions

Let R be the commutative ring $\mathbf{F}_2 + u\mathbf{F}_2 := \mathbf{F}_2[X]/(X^2)$. This ring is endowed with the obvious addition and multiplication, with the property that $u^2 = 0$. The elements of R may be written as $0, 1, u$ and $1 + u$, where 1 and $1 + u$ are the only units in R. Therefore, R has three ideals: (0), (u) and (1).

A linear code C over R of length n is an R-submodule of R^n. An element of C is called a codeword. The Hamming weight $w_H(\mathbf{c})$ of a codeword $\mathbf{c}$ is the number of nonzero coordinates. The (Euclidean) inner product of two codewords $\mathbf{c} = (c_1, \ldots, c_n)$ and $\mathbf{c}' = (c'_1, \ldots, c'_n)$ of R^n is defined to be

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

Duality is understood with respect to this inner product. In particular, the dual code $C^\perp$ of C is defined to be

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

If $C \subseteq C^\perp$, we say that C is self-orthogonal. If $C = C^\perp$, then C is said to be self-dual. Two codes are equivalent if one can be obtained from the other by permuting the coordinates and exchanging 1 and $1 + u$ in some coordinates.

The Lee weights of $0, 1, u, 1+u \in R$ are defined to be 0, 1, 2, 1 respectively. The Lee weight of a codeword in R^n is the rational integer sum of the Lee weights of its coordinates. In other words, for a codeword $\mathbf{c} = (c_1, \ldots, c_n)$, if we let $n_0(\mathbf{c})$ denote the number of coordinates that are equal to 0, let $n_1(\mathbf{c})$ denote the number of coordinates equal to 1 or $1 + u$ and let $n_2(\mathbf{c})$ denote the number of coordinates equal to u, then the Lee weight $w_L(\mathbf{c})$ of $\mathbf{c}$ is defined to be $n_1(\mathbf{c}) + 2n_2(\mathbf{c})$. The Lee distance between two codewords $\mathbf{c}$ and $\mathbf{c}'$ is the Lee weight of $\mathbf{c} - \mathbf{c}'$.

The symmetrised weight enumerator (swe) of a code C over R is

$$swe_C(a, b, c) = \sum_{\mathbf{c} \in C} a^{n_0(\mathbf{c})} b^{n_1(\mathbf{c})} c^{n_2(\mathbf{c})}.$$

The MacWilliams identity for codes over R has been established by Bachoc [1, Theorem 4.2].

A code C over R is isodual if it is equivalent to $C^{\perp}$. It is formally self-dual (fsd, for short) if its swe is invariant by the MacWilliams Transform.

A self-dual code over R is said to be of Type II if the Lee weight of every codeword is a multiple of 4. Otherwise we say that the self-dual code is of Type I.

For a code C over R, we denote by C_∞ the extended code, obtained from C by appending to each codeword $\mathbf{c} = (c_1, \ldots, c_n)$ an overall parity check coordinate $c_\infty = -\sum_{i=1}^{n} c_i$. The augmented code $\overline{C}$ is defined to be $C + span\{\mathbf{1}\}$, where $\mathbf{1}$ is the all-one vector and $span\{\mathbf{v}\}$ is the R-span of $\mathbf{v}$. Therefore, the augmented and extended code $\overline{C_\infty}$ is the code obtained by first extending C followed by augmentation. Whenever n is odd, $\overline{C_\infty}$ may also be obtained by first augmenting C followed by extension.

There is a natural isomorphism between (R^n, Lee distance) and ($\mathbf{F}_2^{2n}$, Hamming distance) that is an $\mathbf{F}_2$-linear isometry, called the Gray map. It is given by

$$\begin{aligned} \phi : R^n &\longrightarrow \mathbf{F}_2^{2n} \\ \mathbf{x} + u\mathbf{y} &\longmapsto (\mathbf{y}, \mathbf{x} + \mathbf{y}), \end{aligned}$$

where $\mathbf{x}, \mathbf{y} \in \mathbf{F}_2^n$.

There are two binary linear codes that are naturally associated with a given linear code C over R. They are the residue code

$$C_{(1)} = \{\mathbf{x} \in \mathbf{F}_2^n \mid \exists \mathbf{y} \in \mathbf{F}_2^n \quad \text{such that } \mathbf{x} + u\mathbf{y} \in C\}$$

and the torsion code

$$C_{(2)} = \{\mathbf{x} \in \mathbf{F}_2^n \mid u\mathbf{x} \in C\}.$$

Clearly, $C_{(1)} \subseteq C_{(2)}$. Let k_1 be the dimension of the binary code $C_{(1)}$ and let $k_1 + k_2$ be the dimension of the binary code $C_{(2)}$. We then say that the code C over R is of type $4^{k_1}2^{k_2}$.

3 Abelian Codes

An abelian code over R of length n is defined to be an ideal in the group ring $R[G]$, where G is a finite abelian group of order n. We assume throughout this paper that n is odd and that the group G is written additively. Every element of $R[G]$ can be written uniquely in the form $\sum_{g \in G} c_g X^g$ ($c_g \in R$). The addition in $R[G]$ is the obvious componentwise addition. This identifies $R[G]$ with R^n naturally as groups. The multiplication in $R[G]$ is the convolution product given by

$$\left(\sum_{h \in G} c_h X^h\right)\left(\sum_{\ell \in G} c'_\ell X^\ell\right) = \sum_{g \in G} d_g X^g,$$

where

$$d_g = \sum_{h+\ell=g} c_h c'_\ell.$$

Let $GR(R, d)$ be the unique Galois extension of R of degree d. This ring has been studied in [3, Section 2.1]. It may be regarded as a ring of the form $R[X]/(f)$, where f is a monic basic irreducible polynomial in $R[X]$ of degree d. For the definition and discussion of Galois extensions of local commutative rings in a more general setting, we refer the reader to [9, Chapter XV].

In particular, we recall that

$$GR(R, d) = \mathbf{F}_{2^d} + u\mathbf{F}_{2^d}, \tag{1}$$

where $\mathbf{F}_{2^d}$ is the unique finite field (up to isomorphism) of 2^d elements. The only ideals in $GR(R, d)$ are (0), (1) and (u). In the notation of (1), we may write these ideals as

$$\begin{aligned}(0) &= (0) + u(0),\\ (1) &= (1) + u(1),\\ (u) &= (0) + u(1).\end{aligned}$$

Here, the ideals on the left hand side are ideals in $GR(R, d)$, while the ideals on the right hand side are ideals in $\mathbf{F}_{2^d}$. Moreover, for $x = x_1 + ux_2 \in GR(R, d)$, the Frobenius map F is defined as

$$F(x) = x_1^2 + ux_2^2.$$

Let m denote the exponent of G. Let d be the order of 2 modulo m. Then $\mathbf{F}_{2^d}$ contains a primitive mth root of unity, which we fix and denote by ζ. By the Fundamental Theorem of finitely generated abelian groups, we may write

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

Every element $g \in G$ can hence be regarded as a t-uple $(a_1, \ldots, a_t)$, where $a_i \in \mathbf{Z}_{n_i}$. For elements $a, b \in G$, define

$$[a, b] = \zeta^e,$$

where

$$e = \sum_{i=1}^{t} a_i b_i (m/n_i).$$

Here, a_i, b_i, which are actually elements of $\mathbf{Z}_{n_i}$, are viewed as rational integers such that $0 \leq a_i, b_i \leq n_i - 1$. The sum e is computed as an integer sum. In fact, since ζ is an mth root of unity, the sum e may also be regarded as a sum modulo m.

The map $b \mapsto [a, b]$ is a character of G with values in $\mathbf{F}_{2^d}$. Moreover, we have

$$[a, b] = [b, a],$$
$$[a, 2b] = [2a, b] = [a, b]^2,$$
$$\sum_{x \in G} [a, x] = n\delta_{a,0}.$$

The Fourier Transform for binary codes is well-known. For a word $\mathbf{c} = \sum_{g \in G} c_g X^g \in \mathbf{F}_2[G]$, its Fourier Transform is defined to be $\hat{\mathbf{c}} = \sum_{h \in G} \hat{c}_h X^h$, where

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

For $R[G]$, we can write each word as

$$\mathbf{c} = \mathbf{c}_1 + u\mathbf{c}_2, \quad \mathbf{c}_1, \mathbf{c}_2 \in \mathbf{F}_2[G].$$

We define the Fourier Transform of $\mathbf{c}$ as $\hat{\mathbf{c}}_1 + u\hat{\mathbf{c}}_2$. It is easy to verify that the following hold:

- for all $\mathbf{c}, \mathbf{c}' \in R[G]$ and all $h \in G$, we have $\widehat{cc'}_h = \hat{c}_h \hat{c}'_h$;
- for all $\mathbf{c} \in R[G]$ and all $h \in G$, we have $F(\hat{c}_h) = \hat{c}_{2h}$.

Denote by $O_0, O_1, \ldots, O_s$ the orbits of G under the map $x \mapsto 2x$. Let d_i denote the size of O_i. Using exactly the same argument as in [7, Section 5], together with (1), we obtain the following results:

Theorem 3.1 *There is a ring isomorphism between $R[G]$ and the product*

$$R \times GR(R, d_1) \times \cdots \times GR(R, d_s).$$

Hence, $R[G]$ is isomorphic as a ring to

$$(\mathbf{F}_2 \times \mathbf{F}_{2^{d_1}} \times \cdots \times \mathbf{F}_{2^{d_s}}) + u(\mathbf{F}_2 \times \mathbf{F}_{2^{d_1}} \times \cdots \times \mathbf{F}_{2^{d_s}}).$$

Consequently, every ideal I of $R[G]$ can be expressed as

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

with $I_j = J_j + uK_j$, where J_j, K_j are ideals in $\mathbf{F}_{2^{d_j}}$ and $J_j \subseteq K_j$.

From Theorem 3.1, if a code C over R is identified with an ideal I of $R[G]$, we have $J_0 \times J_1 \times \cdots \times J_s \subseteq C_{(1)}$ and $K_0 \times K_1 \times \cdots \times K_s \subseteq C_{(2)}$, where $C_{(1)}$ and $C_{(2)}$ are the residue and torsion codes respectively. Since $|C| = |C_{(1)}||C_{(2)}|$, it follows that

$$C_{(1)} = J_0 \times J_1 \times \cdots \times J_s \subseteq \mathbf{F}_2[G]$$

and

$$C_{(2)} = K_0 \times K_1 \times \cdots \times K_s \in \mathbf{F}_2[G].$$

Moreover, $C = C_{(1)} + uC_{(2)}$.

We also have the following result on the Gray image of an abelian code over R:

Theorem 3.2 *If C is an abelian code in $R[G]$, where G is an abelian group of order n, then the Gray image $\phi(C)$ is a binary abelian code in $\mathbf{F}_2[G \times \mathbf{Z}_2]$. Moreover, if $C_{(1)}$ has minimum distance d_1 and $C_{(2)}$ has minimum distance d_2, then $\phi(C)$ has minimum distance* $\min\{d_1, 2d_2\}$. *If n is odd and G is cyclic, then $\phi(C)$ is a binary cyclic code.*

Proof. For an element $\mathbf{c} = \sum_{g\in G}(a_g + (1+u)b_g)X^g \in R[G]$, where $a_g, b_g \in \mathbf{F}_2$, consider $\mathbf{c}' = \sum_{(g,h)\in G\times \mathbf{Z}_2} c_{(g,h)} X^g Y^h$, where

$$c_{(g,h)} = \begin{cases} b_g & \text{if } h = 0 \\ a_g & \text{if } h = 1. \end{cases}$$

It is clear that $\mathbf{c}' \in \mathbf{F}_2[G \times \mathbf{Z}_2]$ and that it may be identified with the Gray image of $\mathbf{c}$. It remains to show that $\phi(C) = \{\mathbf{c}' \mid \mathbf{c} \in C\}$ forms an ideal in $\mathbf{F}_2[G \times \mathbf{Z}_2]$.

The addition and multiplication by X in $\mathbf{F}_2[G \times \mathbf{Z}_2]$ correspond to the ones in $R[G]$, so $\phi(C)$ is closed under these operations. Multiplication by Y corresponds to the "swap" map defined in [6, Section IX], which in turn corresponds to multiplication by $1+u$ in $R[G]$, so $\phi(C)$ is again closed under multiplication by Y. Hence, $\phi(C)$ is an ideal.

The second assertion follows immediately from the fact that $\phi(C)$ is equivalent to the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction (cf. [10, Section 2]) with $\mathbf{u} \in C_{(2)}$ and $\mathbf{v} \in C_{(1)}$.

The last assertion is obvious as $G \times \mathbf{Z}_2$ is cyclic in that case.

Remark. Theorem 3.2 generalises Theorem 1 of [8] and the proof is shorter.

3.1 Duality

Let σ denote the permutation on $\{0, 1, \ldots, s\}$ induced by the map $x \mapsto -x$ on G and, consequently, on the orbits $O_0, O_1, \ldots, O_s$ defined earlier. In particular, σ is the identity if and only if, for every $x \in G$, x and $-x$ lie in the same orbit. For the ideals (0), (1) and (u) in a Galois ring $GR(R, d)$, we define $(0)^o = (1)$, $(1)^o = (0)$ and $(u)^o = (u)$. By the same argument as in [7, Section 7] again, we have the following

Theorem 3.3 *The dual of the ideal $I = I_0 \times I_1 \times \cdots I_s \subseteq R[G]$ is the ideal $I^\perp = I^o_{\sigma(0)} \times I^o_{\sigma(1)} \times \cdots \times I^o_{\sigma(s)}$.*

Therefore, an ideal $I = I_0 \times I_1 \times \cdots \times I_s$ is self-dual if and only if we have $I^o_{\sigma(j)} = I_j$ for all $0 \le j \le s$.

Remark. There is always a trivial self-dual abelian code in $R[G]$ when the order n of G is odd, viz. the ideal I where $I_j = (u)$ for all $0 \le j \le s$. It is easy to observe that the following analog of [7, Proposition 7.5] is true: there is no nontrivial abelian self-dual code in $R[G]$ (where the order of G is odd) if and only if σ is the identity.

4 Duadic Codes over R

We say that (X, A, B) is a splitting of G given by α, where α is an automorphism of G, if $X \cup A \cup B$ is a partition of G such that X, A and B are unions of orbits and that $\alpha(A) = B$ and $\alpha(B) = A$. It follows therefore that $\alpha(X) = X$. We define a duadic code over R attached to the splitting (X, A, B) given by α to be the ideal $I_0 \times I_1 \times \cdots \times I_s$ in $R[G]$ where $I_j = (u)$ if $O_j \subseteq X$, $I_j = (0)$ if $O_j \subseteq A$ and $I_j = (1)$ if $O_j \subseteq B$. If we relax the condition on I_0 by allowing it to be any of the ideals (0), (u) or (1), then we say that the code thus obtained is a generalised duadic code attached to the splitting.

Theorem 4.1 *Assume that σ is not the identity and that (X, A, B) is a splitting of G given by -1. Then the duadic code attached to (X, A, B) is self-dual and the generalised duadic code with $I_0 = (0)$ is self-orthogonal. Conversely, every self-dual abelian code over R is a duadic code attached to some splitting of G given by -1.*

Proof. The first statement follows from the definitions of duadic codes and generalised duadic codes, as well as Theorem 3.3. Conversely, if $I = I_0 \times I_1 \times \cdots \times I_s$ is a self-dual abelian code in $R[G]$, by setting X to be the union of the O_j for which $I_j = (u)$, A to be the union of the O_j for which $I_j = (0)$ and B to be $G\backslash(A \cup X)$, it follows that (X, A, B) is a splitting of G given by -1.

Remark. Note that the trivial self-dual abelian code corresponds to the degenerate splitting $(G, \emptyset, \emptyset)$ of G.

Let τ be the permutation on $\{0, 1, \ldots, s\}$ induced by α. In particular, if $\alpha = -1$, we have $\tau = \sigma$. For any ideal $I = I_0 \times I_1 \times \cdots \times I_s$ of $R[G]$, 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 in fact the image of I under the isometry $\sum c_g X^g \mapsto \sum c_g X^{\alpha^* g}$, where α^*, an automorphism of G, is the adjoint of α with respect to the pairing $[,]$ defined in Section 3. The ideal I is said to be isodual by the multiplier α if $I^\alpha = I^\perp$.

Theorem 4.2 *Assume that σ is the identity 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 R isodual by a multiplier is a duadic code attached to a splitting of G.*

The proof of Theorem 4.2 is analogous to the one for Theorem 4.1.

5 Augmented and Extended Abelian Codes

5.1 Self-Duality

We first show in this section that the augmented and extended code of a generalised duadic code over R is self-dual. Then we show that if the augmented

and extended code of an abelian code C over R is self-dual, then C is actually a generalised duadic code.

Theorem 5.1 *Let G be an abelian group of order n, let (X, A, B) be a splitting of G given by -1 and let C be an attached generalised duadic code over R. Then $\overline{C_\infty}$ is self-dual.*

Proof. We first note that $\overline{C_\infty}$ has exactly 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 (hence $I_0 = (u)$). In particular, C is self-dual.

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

$$\langle (\mathbf{c}, c_\infty), (\mathbf{c}', c'_\infty) \rangle = 0, \tag{2}$$

$$\langle (\mathbf{c}, c_\infty), (\mathbf{1}, 1) \rangle = 0, \tag{3}$$

$$\langle (\mathbf{1}, 1), (\mathbf{1}, 1) \rangle = 0. \tag{4}$$

Equation (2) is true because C is self-dual and $c_\infty, c'_\infty \in (u)$; equation (3) follows from the definition of the extended code; while (4) is true because $n+1$ is even and R has characteristic 2.

By the R-linearity of the inner product, it follows that $\overline{C_\infty}$ is self-orthogonal. Since $\overline{C_\infty}$ has 2^{n+1} elements, it follows that it is self-dual. This completes the proof of Theorem 5.1.

Next we let C denote an abelian code over R of length n. Suppose that $\overline{C_\infty}$ is self-dual.

Theorem 5.2 *Let C be an abelian code in $R[G]$, where G is an abelian group of order n. Suppose that $\overline{C_\infty}$ is self-dual. Then n is odd and C is a generalised duadic code over R attached to a splitting (X, A, B) of G given by -1. In particular, any self-dual augmented and extended abelian code over R is the augmented and extended code of a duadic code over R attached to a splitting (X, A, B) of G given by -1.*

Proof. Since $(\mathbf{1}, 1)$ is in $\overline{C_\infty}$, the self-duality of $\overline{C_\infty}$ implies that $n+1$ is even.

Write C as $I_0 \times I_1 \times \cdots \times I_s$. It is clear that $\overline{C} = C + span\{\mathbf{1}\}$ is an ideal of $R[G]$. In fact, it is the ideal $\overline{I}_0 \times I_1 \times \cdots \times I_s$, where $\overline{I}_0 = (1)$. Recall also that $C^\perp$ is the ideal $I^o_{\sigma(0)} \times \cdots \times I^o_{\sigma(s)}$.

Consider the orbits in $G \backslash \{0\}$. Let X' denote the union of the orbits O_j where $I_j = (u)$; let A be the union of the orbits O_j with $I_j = (0)$ and let B be the union of the orbits O_j with $I_j = (1)$.

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

$$\langle (\mathbf{c}, c_\infty), (\mathbf{c}', c'_\infty) \rangle = 0. \tag{5}$$

By definition of the extension, we have

$$\langle (\mathbf{1}, 1), (\mathbf{c}', c'_\infty) \rangle = 0. \tag{6}$$

Therefore, $(C^\perp)_\infty \subseteq (\overline{C_\infty})^\perp = \overline{C_\infty}$, from which it follows that $C^\perp \subseteq \overline{C}$, since n is odd and hence augmentation and extension of a code commute.

The index of C in $\overline{C}$ is 1, 2 or 4, depending on whether $I_0 = (1), (u)$ or (0). The size of $\overline{C}$ is 2^{n+1} since $\overline{C_\infty}$ is self-dual. Therefore, together with the fact that $C^\perp \subseteq \overline{C}$, it follows that the index of $C^\perp$ in $\overline{C}$ is 4, 2 or 1 respectively. This means in particular that $I^o_{\sigma(j)} = I_j$ for all $1 \leq j \leq s$. This means that $(X' \cup \{0\}, A, B)$ is a splitting of G given by -1 and C is a generalised duadic code attached to this splitting.

The final statement of the theorem follows immediately since the choice of I_0 is irrelevant when we consider the augmented and extended code.

This completes the proof of Theorem 5.2.

5.2 Isoduality

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

Theorem 5.3 *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 generalised duadic code over R. Then $\overline{C_\infty}$ is isodual by the multiplier α.*

Theorem 5.4 *Let C be an abelian code in $R[G]$, for some abelian group G of order n, such that $\overline{C_\infty}$ is isodual by a multiplier α. Then n is odd and C is a generalised duadic code attached to a splitting (X, A, B) of G given by α. In particular, any augmented and extended abelian code over R that is isodual by a multiplier α is the augmented and extended code over 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 5.1 and 5.2, 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 5.1 should be taken to be in C^α;
3. due to the isoduality of $\overline{C_\infty}$ by the multiplier α, the containment $C^\perp \subseteq \overline{C}$ in the proof of Theorem 5.2 is now replaced by $C^\alpha \subseteq \overline{C}^\alpha$. The same argument then yields $I_{\tau(j)} = I_j^o$ for all $1 \leq j \leq s$, a condition needed for the existence of the required splitting given by α.

6 Type II Codes

In this section, we give a criterion for self-dual augmented and extended abelian codes over R to be of Type II.

Let $C = I_0 \times \cdots \times I_s$ be a generalised duadic code over R attached to a splitting (X, A, B) of an abelian group G given by -1, with $I_0 = (0)$. We recall from Section 3 and Theorem 3.1 that $C = C_{(1)} + uC_{(2)}$, where $C_{(1)}, C_{(2)}$ are the residue and torsion codes respectively. If we write $C_{(1)} = J_0 \times \cdots \times J_s$ and $C_{(2)} = K_0 \times \cdots \times K_s$, then $J_0 = (0)$. Moreover, note that $J_j = (0)$ whenever $O_j \subseteq X$. It is easy to verify that $C_{(1)}$ is a binary split group code attached to the splitting (X, A, B) of G given by -1, in the sense of [5, Section II.B]. (In the notation of [5], it is the code C_0^Z attached to the splitting (Z, X_0, X_1) of G.) [5, Theorem IV.4] shows that $C_{(1)}$ is self-orthogonal and that the Hamming weight of every codeword in $C_{(1)}$ is congruent to 0 modulo 4.

Lemma 6.1 *Suppose $n + 1 \equiv 0 \bmod 4$. Then $\overline{(C_{(1)})_\infty}$ is self-orthogonal, contains the codeword* $(\mathbf{1}, 1)$ *and the Hamming weight of every word in $\overline{(C_{(1)})_\infty}$ is a multiple of* 4.

Proof. By definition, $(\mathbf{1}, 1) \in \overline{(C_{(1)})_\infty}$.

Let $\langle \cdot, \cdot \rangle$ denote the usual Euclidean inner product in $\mathbf{F}_2^n$. (We allow ourselves this abuse of notation in this proof since we work strictly over $\mathbf{F}_2$ and hence no confusion will arise.)

For $\mathbf{c}, \mathbf{c}' \in C_{(1)}$, since $c_\infty = -\hat{c}_0 \in J_0 = (0)$, by the self-orthogonality of $C_{(1)}$, we have

$$\langle (\mathbf{c}, c_\infty), (\mathbf{c}', c'_\infty) \rangle = 0. \tag{7}$$

The definition of the extended code yields

$$\langle (\mathbf{c}, c_\infty), (\mathbf{1}, 1) \rangle = 0. \tag{8}$$

Since $n + 1$ is even,

$$\langle (\mathbf{1}, 1), (\mathbf{1}, 1) \rangle = 0. \tag{9}$$

As the inner product is $\mathbf{F}_2$-linear, it therefore follows from (7), (8) and (9) that $\overline{(C_{(1)})_\infty}$ is self-orthogonal.

As we have already observed, every word $\mathbf{c} \in C_{(1)}$ has Hamming weight congruent to 0 modulo 4, hence so does every word $(\mathbf{c}, c_\infty) = (\mathbf{c}, 0) \in (C_{(1)})_\infty$. Since $n+1 \equiv 0 \bmod 4$, every word of the form $(\mathbf{c}, c_\infty) + (\mathbf{1}, 1)$ also has Hamming weight congruent to 0 modulo 4. Hence Lemma 6.1 is proved.

Lemma 6.2 *We have* $\overline{C_\infty} = \overline{(C_{(1)})_\infty} + u\overline{(C_{(2)})_\infty}$.

Proof. Since $C = C_{(1)} + uC_{(2)}$, we have $C_\infty = (C_{(1)})_\infty + u(C_{(2)})_\infty \subseteq \overline{(C_{(1)})_\infty} + u\overline{(C_{(2)})_\infty}$. Since $(\mathbf{1}, 1) \in \overline{(C_{(1)})_\infty} + u\overline{(C_{(2)})_\infty}$ clearly, together with cardinality consideration, the lemma follows.

Lemma 6.3 *We have* $\overline{(C_{(2)})_\infty} = (\overline{(C_{(1)})_\infty})^\perp$ *as binary codes.*

Proof. As in the proof of Lemma 6.1, we abuse notation by using $\langle \cdot, \cdot \rangle$ to denote the usual Euclidean inner product in $\mathbf{F}_2^n$.

From the description of $C_{(1)}$ and $C_{(2)}$ in Section 3, it is clear that $C_{(2)} \subseteq (C_{(1)})^\perp$. Therefore, for $\mathbf{c} \in C_{(1)}$ and $\mathbf{c}' \in C_{(2)}$, noting that $c_\infty = 0$, we have the following identities:

$$\begin{aligned} &\langle (\mathbf{c}', c'_\infty), (\mathbf{c}, c_\infty) \rangle = 0, \\ &\langle (\mathbf{1}, 1), (\mathbf{1}, 1) \rangle = 0, \\ &\langle (\mathbf{1}, 1), (\mathbf{c}, c_\infty) \rangle = 0. \end{aligned}$$

Hence, $\overline{(C_{(2)})_\infty} \subseteq (\overline{(C_{(1)})_\infty})^\perp$. The equality required in the lemma follows by considering cardinalities of these two codes.

We are now ready to prove the main result of this section:

Theorem 6.4 *A self-dual augmented and extended abelian code over R of length n is of Type II if and only if $n + 1 \equiv 0 \bmod 4$.*

Proof. If C is an abelian code over R of length n such that its augmented and extended code is of Type II, then by considering the Lee weight of $(\mathbf{1}, 1)$, we must have $n + 1 \equiv 0 \bmod 4$.

Conversely, suppose that $n + 1 \equiv 0 \bmod 4$ and that C is an abelian code over R of length n such that $\overline{C_\infty}$ is self-dual. By Theorem 5.2, we may assume that C is a generalised duadic code $I_0 \times I_1 \times \cdots \times I_s$, where $I_0 = (0)$. We need to show that every codeword in $\overline{C_\infty}$ has Lee weight congruent to 0 modulo 4.

From Lemmas 6.2 and 6.3, $\overline{C_\infty} = \overline{(C_{(1)})_\infty} + u(\overline{(C_{(1)})_\infty})^\perp$. From Lemma 6.1, $\overline{(C_{(1)})_\infty}$ is a binary self-orthogonal code containing $(\mathbf{1}, 1)$ and whose codewords all have Hamming weights congruent to 0 modulo 4. It then follows from [6, Proposition 5.1] that $\overline{C_\infty}$ is a self-dual Type II code over R.

7 Examples

For a given integer n, all the finite abelian groups G of order n can be easily determined. For each of such groups, the orbits of the map $x \mapsto 2x$ can then be easily computed. It is then routine to observe if the group admits a splitting (X, A, B) with a given α. We explore the duadic code over R for lengths up to 31.

7.1 Cyclic Self-Dual Codes

For lengths up to 31, such codes have been studied and classified by Bonnecaze and Udaya [3]. We note that there are four, not three as said in [3, Section 3.1.1], nontrivial cyclic self-dual codes in length 21. This "missing" code is obtained, in the notation of [3], by letting $f = f_3 f_6$, $g = f_4 f_5$ and $h = f_1 f_2$. The Lee distance of this code is 8, yielding by the Gray map a [42, 21, 8] binary extremal (in the sense of [4] where it is mentioned) cyclic self-dual code, with an automorphism group of order $2^{14} \cdot 3^5 \cdot 5^2 \cdot 7^2$.

7.2 Cyclic Isodual Codes

For $n \leq 31$, the only length that gives rise to cyclic isodual duadic codes is $n = 17$. In this case, the only code obtained is the quadratic residue code over R of length 17.

7.3 Noncyclic Isodual Codes

For $n \leq 31$, there are 3 values of n, viz. $n = 9$, 25 and 27, which are of interest.

7.3.1 $n = 9$

For $n = 9$, only $\mathbf{Z}_3 \times \mathbf{Z}_3$ gives rise to duadic codes. This group can be realised as the underlying additive group for $\mathbf{F}_9 = \mathbf{F}_3(i)$, with $i^2 = -1$. The orbits are then

$$\{(0), (\pm 1), (\pm i), (\pm(1+i)), (\pm(1-i))\}.$$

Here $Q = \{\pm 1, \pm i\}$, and $N = \{(\pm(1+i)), (\pm(1-i))\}$. In Table 1 the codes are specified by their components on each of the 5 orbits which are labelled in the above order. For instance $2 - 1 - 1 - 0 - 0$ is the supplemented quadratic residue (SQR) code $\mathscr{S}_Q$. We denote by q, r, s, t the following elements of $GL(2, 3)$.

$$q = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

There are nine nontrivial duadic codes. The four nontrivial orbits can be thought of as the points of $PG(1, 3)$. It is known that $PGL(2, 3)$ is 3-transitive on $PG(1, 3)$ ([2, Theorem 6.6]). This shows that the codes listed in Table 1 are all isodual. In fact, it can be shown that the first, fourth and sixth codes are multiplier-equivalent to one another, and that the remaining six codes are again multiplier-equivalent to one another. Hence, there are only two non multiplier-equivalent duadic codes.

7.3.2 $n = 25$

For $n = 25$, only $\mathbf{Z}_5 \times \mathbf{Z}_5$ gives rise to duadic codes. This group can be realised as the underlying additive group of $\mathbf{F}_{25} = \mathbf{F}_5(j)$ with $j^2 + j + 1 = 0$. There are six nonzero orbits all of size 4 and of the shape $C_a := (\pm a, \pm 2a)$ with a ranging over $\{1, j, 1 \pm j, 1 \pm 2j\}$. With these notations the squares and nonsquares are:

$$Q = C_1 \bigcup C_j \bigcup C_{1+j}$$

$$N = C_{1-j} \bigcup C_{1+2j} \bigcup C_{1-2j}.$$

It is easy to observe that there are only three types of codes, viz. those of types $4^{12}2^1$, $4^4 2^{17}$ and $4^8 2^9$, depending on the number of orbits in X of the splitting (X, A, B) of $\mathbf{Z}_5 \times \mathbf{Z}_5$.

The six nontrivial orbits can be thought of as the points of $PG(1, 5)$. The zeros of a code of type $4^{12}2^1$ comprise exactly three such projective points. The same is true for its nonzeros. Since $PGL(2, 5)$ is 3-transitive ([2, Theorem 6.6]) there is a multiplier that takes the zeros to the nonzeros. This shows that the code is duadic and hence isodual. Similarly, there is a multiplier that takes

Table 1. Duadic Codes of length 9

Code C	Type	$d_L(C)$	α
$2-1-1-0-0$	$4^4 2^1$	4	q
$2-0-2-2-1$	$4^2 2^5$	4	r
$2-2-0-2-1$	$4^2 2^5$	4	s
$2-1-0-1-0$	$4^4 2^1$	4	s
$2-2-2-0-1$	$4^2 2^5$	4	t
$2-1-0-0-1$	$4^4 2^1$	4	s
$2-0-2-1-2$	$4^2 2^5$	4	s
$2-2-1-0-2$	$4^2 2^5$	4	r
$2-0-1-2-2$	$4^2 2^5$	4	t

Table 2. Duadic Codes of length 25

Code C	Type	$d_L(C)$
Class 1	$4^{12}2^1$	6
Class 2	$4^4 2^{17}$	4
Class 3	$4^8 2^9$	8

one such code to another of the same type. Hence all such codes of this type are equivalent.

The spectrum of a code of type $4^4 2^{17}$ comprises exactly an orbit of nonzeros and another of zeros. By the 2-transitivity of PGL(2,5) we can swap these two. This shows that such a code is indeed duadic and hence isodual. Similarly, this shows that there is a multiplier that takes a code of this type to another code of the same type. Hence all such codes of this type are equivalent.

As for codes of type $4^8 2^9$, calculations on Magma show that this class splits into two subclasses under the action of $PGL(2,5)$, and both orbits consist of duadic and hence isodual codes. Moreover, the codes in each subclass are multiplier equivalent. It is also possible to show the same result by using the 2-transitivity of $PGL(2,5)$ and some more tedious analysis, which we omit here.

7.3.3 $n = 27$

For $n = 27$, there are two groups that give rise to duadic codes.

(A) $G = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$.

Table 3. Duadic Codes of $R[\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3]$

Code C	Type	$d_L(C)$
$2-2-0-0-0-0-0-0-1-1-1-1-1-1-1$	$4^{12}2^3$	4
$2-2-0-0-0-0-0-0-2-2-1-1-1-1-1$	$4^{10}2^7$	6
$2-0-0-0-2-0-0-1-0-1-1-1-1-1-1$	$4^{12}2^3$	6
$2-2-0-0-0-0-0-2-2-2-2-1-1-1-1$	$4^8 2^{11}$	6
$2-0-0-2-2-0-0-1-0-2-1-1-1-1-1$	$4^{10}2^7$	6
$2-0-0-1-0-0-0-1-0-2-1-1-1-1-1$	$4^{12}2^3$	6
$2-2-0-0-0-2-2-2-0-2-1-1-1-1-1$	$4^8 2^{11}$	6
$2-2-0-0-0-2-2-2-2-2-2-1-1-1-1$	$4^6 2^{15}$	4
$2-2-2-0-0-2-0-0-2-1-1-2-1-1-1$	$4^8 2^{11}$	6
$2-0-2-0-2-2-0-2-0-1-1-2-1-1-1$	$4^8 2^{11}$	6
$2-0-2-0-2-2-0-2-2-2-1-2-1-1-1$	$4^6 2^{15}$	6
$2-2-0-2-0-2-0-2-2-2-1-2-1-1-1$	$4^6 2^{15}$	6
$2-2-0-0-2-2-2-2-2-2-2-2-2-1-1$	$4^4 2^{19}$	4
$2-0-2-2-2-2-2-2-2-2-2-2-0-1-1$	$4^4 2^{19}$	4
$2-0-2-2-2-2-2-2-2-2-2-2-2-2-1$	$4^2 2^{23}$	4

Table 4. Duadic Codes of $R[\mathbf{Z}_3 \times \mathbf{Z}_9]$

Code C	Type	$d_L(C)$
$2-0-2-0-2-1-2-1$	$4^8 2^{11}$	6
$2-2-2-0-0-1-2-1$	$4^8 2^{11}$	6
$2-2-2-0-2-2-2-1$	$4^2 2^{23}$	4
$2-0-2-2-2-1-2-2$	$4^6 2^{15}$	4

All the 14 nonzero orbits are of the shape $C_a = \{\pm a\}$ for some nonzero a. In Table 3 the a's are listed in order

$$000, 001, 010, 011, 012, 100, 101, 102, 110, 111, 112, 120, 121, 122.$$

There are no quadratic residue codes here because $2 = -1$ is not a quadratic residue in $\mathbf{F}_{27}$.

(B) $G = \mathbf{Z}_3 \times \mathbf{Z}_9$.

There are 7 nonzero orbits. Three have size six and four have size two. The orbits are by order of representatives

$$00, 01, 03, 10, 11, 12, 13, 16.$$

We list in Table 4 the four nontrivial non multiplier-equivalent duadic codes.

References

1. Bachoc, C.: Applications of coding theory to the construction of modular lattices. J. Comb. Theory Ser. A **78**, 92–119 (1997)
2. Beth, T., Jungnickel, D., Lenz, H.: Design Theory, Mannheim: B.I. Wissenschaftverlag, 1985
3. Bonnecaze, A., Udaya, P.: Cyclic codes and self-dual codes over $\mathbf{F}_2 + u\mathbf{F}_2$. IEEE Trans. Inform. Theory **45**, 1250–1254 (1999)
4. Conway, J. H., Sloane, N. J. A.: A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory **36**, 1319–1333 (1990)
5. Ding, C., Kohel, D., Ling, S.: Split group codes. IEEE Trans. Inform. Theory **46**, 485–495 (2000)
6. Dougherty, S. T., Gaborit, P., Harada, M., Solé, P.: Type II codes over $\mathbf{F}_2 + u\mathbf{F}_2$. IEEE Trans. Inform. Theory **45**, 32–45 (1999)
7. Langevin, P., Solé, P.: Duadic $\mathbf{Z}_4$-codes. Finite Fields Their Appls. **6**, 309–326 (2000)
8. van Lint, J. H.: Repeated-root cyclic codes. IEEE Trans. Inform. Theory **37**, 343–345 (1991)
9. McDonald, B. R.: Finite rings with identity. New York: Marcel Dekker 1974
10. Pless, V.: Coding constructions, In: Handbook of Coding Theory, Vol. 1 pp. 141–176, Amsterdam: Elsevier 1998