Type IV codes over a non-unital ring

Adel Alahmadi, Alaa Altassan, Widyan Basaffar, Alexis Bonnecaze, Hatoon Shoaib, Patrick Solé

Type IV codes over a non-unital ring

Adel Alahmadi[*], Alaa Altassan [†], Widyan Basaffar[‡], Alexis Bonnecaze[§], Hatoon Shoaib[¶], Patrick Solé[‖**]

Abstract

There is a special local ring E of order 4, without identity for the multiplication, defined by $E = \langle a, b \mid 2a = 2b = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$. We study the algebraic structure of linear codes over that non-commutative local ring, in particular their residue and torsion codes. We introduce the notion of quasi self-dual codes over E, and Type IV codes, that is quasi self-dual codes whose all codewords have even Hamming weight. We study the weight enumerators of these codes by means of invariant theory, and classify them in short lengths.

Keywords: rings, codes, additive codes, Type IV codes.
MSC(2010): Primary 94 B05, Secondary 16 A10.

[*]Email: adelnife2@yahoo.com
[†]Email: aaltassan@kau.edu.sa
[‡]Email: whbasaffar@kau.edu.sa
[§]Email: Alexis.Bonnecaze@univ-amu.fr
[¶]Email: hashoaib@kau.edu.sa
[‖]Email: sole@enst.fr
[**]AA,AA,WB,HS are with Math Dept, King Abdulaziz University, Jeddah, Saudi Arabia. AB and PS are with Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France.

1 Introduction

The rings of order 4 used as alphabets in coding theory are historically, and by order of importance, $\mathbb{F}_4$ [12], $\mathbb{Z}_4$ [10], $\mathbb{F}_2+u\mathbb{F}_2$ [7], and $\mathbb{F}_2\times\mathbb{F}_2$ [6]. A quick look at the classification of finite rings of order 4 shows that these four rings above are exactly all the rings, amongst the list of 9 rings of order 4, that possess an identity element for the multiplication [8, 14]. More generally, in the abundant literature of codes over rings no non-unital ring has ever been used as alphabet [17, 5].

In this paper, for the first time in the history of Coding Theory, codes over a non-unital ring are studied. This ring has order four, and is denoted by E in the classification of [8, 14]. The ring E turns out to be also non-commutative. Our original intention was to study self-dual codes over E. However, the usual relation between the size of the code and that of its dual does not hold in general (see the notion of nice code in the next section). This situation led us to introduce the notion of quasi self dual code (QSD), that is of an E-code of length n that is both self-orthogonal and of size 2^n. The aim of this paper is thus to study the structure of QSD codes. In particular we study a multilevel construction of a QSD code as a function of a pair of dual codes. Like in the case of other local rings of order 4, the notions of residue and torsion codes are fundamental [4]. They lead in particular, to a canonical form for the generator matrix of any E code of given residue and torsion codes dimensions. However, the characterization of Theorem 6 of a QSD code as a multilevel construction from its residue and torsion code would not be true over the four commutative rings of order 4. This characterization is strong enough to allow us to characterize Type IV codes by their residue code, and to classify them in short lengths.

An important computational tool is the connection with additive codes over $\mathbb{F}_4$, made possible by the fact that E and $\mathbb{F}_4$ share the same additive group. In analogy with [6], we introduce the notion of Type IV codes over E as those QSD codes, all codewords of which have even Hamming weight. While additive codes over $\mathbb{F}_4$ were introduced in a Quantum coding context [3], they enter the picture here as a computational tool. Thus, by forgetting the multiplicative structure, a linear E-code is, in particular an additive code over $\mathbb{F}_4$. The connection is close enough that there is a one-to-one correspondence between the residue and torsion code over E, and the Trace code and subfield subcode over $\mathbb{F}_4$. This allows in particular, efficient computation in the Magma package dedicated to additive codes [13]. While the additive

codes classified here are not, in general, strong error correcting codes, they can have an interesting combinatorial structure as evidenced by Example 3.

We also study the weight enumerators in two and four variables of Type IV codes from the standpoint of invariant theory. This study refines the theory of the joint weight enumerator of a binary code and its dual started in [1], to binary codes containing the all-one vector. This leads us to a Gleason formula for the weight enumerators of Type IV codes, in four variables (complete weight enumerator) and by specialization to the weight enumerator in two variables.

The material is organized as follows. The next section collects basic facts and definitions about rings, modules, and duality. Section 3 describes the structure of generator matrices of linear codes over E. Section 4 exploits this theory to construct QSD codes and derives a criterion for a QSD code to be Type IV. Section 5 studies the weight enumerators of QSD and Type IV codes. Section 6 classifies, up to equivalence, QSD codes of length $n < 7$. Section 7 concludes the article.

2 Background material

2.1 Binary codes

Denote by $wt(x)$ the Hamming weight of $x \in \mathbb{F}_2^n$. The dual of a binary linear code C is denoted by $C^\perp$ and defined as

$$C^\perp = \{y \in \mathbb{F}_2^n \mid \forall x \in C,\, (x, y) = 0\},$$

where $(x, y) = \sum_{i=1}^n x_i y_i$, denotes the standard inner product. A code C is **self-orthogonal** if it is included in its dual: $C \subseteq C^\perp$. Two binary codes are **equivalent** if there is a permutation of coordinates that maps one to the other.

2.2 Rings

Following [8] we define a ring on two generators a, b by its relations

$$E = \langle a, b \mid 2a = 2b = 0,\, a^2 = a,\, b^2 = b,\, ab = a,\, ba = b\rangle.$$

A model for that ring can be obtained by taking a, b to be matrices over $\mathbb{F}_2$ defined by

$$a = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Thus, E has characteristic two, and consists of four elements $E = \{0, a, b, c\}$, with $c = a + b$. The addition table is immediate from these definitions.

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

The multiplication table is as follows.

$\times$	0	a	b	c
0	0	0	0	0
a	0	a	a	0
b	0	b	b	0
c	0	c	c	0

From this table, we infer that this ring is not commutative, and without an identity element for the multiplication. It is local with maximal ideal $J = \{0, c\}$, and residue field $E/J = \mathbb{F}_2 = \{0, 1\}$, the finite field of order 2. Thus we have a **c-adic decomposition** as follows. Every element $e \in E$ can be written

$$e = as + ct,$$

where $s, t \in \mathbb{F}_2$ and where we have defined a natural action of $\mathbb{F}_2$ on E by the rule $r0 = 0r = 0$ and $r1 = 1r = r$ for all $r \in E$. Thus $a = 1a, c = 1c$ and $b = a1 + c1$. Note that for all $r \in E$, this action is "distributive" in the sense that $r(s \oplus_2 t) = rs + rt$, where $\oplus_2$ denote the addition in $\mathbb{F}_2$.

Denote by $\alpha : E \to E/J \simeq \mathbb{F}_2$ the **map of reduction modulo** J. Thus $\alpha(0) = \alpha(c) = 0$, and $\alpha(a) = \alpha(b) = 1$. This map is extended in the natural way in a map from E^n to $\mathbb{F}_2$.

2.3 Modules

A **linear** E-code of length n is a one-sided E-submodule of E^n. An **additive code** of length n over $\mathbb{F}_4$ is an additive subgroup of $\mathbb{F}_4^n$. It is a free $\mathbb{F}_2$ module

with 4^k elements for some $k \leq n$ (here $2k$ is an integer, but k may be half-integral). Using a **generator matrix** G, such a code can be cast as the $\mathbb{F}_2$-span of its rows. To every linear E code C is attached an **additive** $\mathbb{F}_4$ code $\phi(C)$ by the substitution

$$0 \to 0, a \to \omega, b \to \omega^2, c \to 1,$$

where $\mathbb{F}_4 = \mathbb{F}_2[\omega]$. Note that the reverse substitution attaches to every additive $\mathbb{F}_4$ code an additive subgroup of E^n, which may or may not be linear. Two E-codes are **permutation equivalent** if there is a permutation of coordinates that maps one to the other.

2.4 Duality

Define an **inner product** on E^n as $(x, y) = \sum_{i=1}^{n} x_i y_i$.

The **right dual** $C^{\perp_R}$ of C is the right module defined by

$$C^{\perp_R} = \{y \in E^n \mid \forall x \in C,\ (x, y) = 0\}.$$

The **left dual** $C^{\perp_L}$ of C is the left module defined by

$$C^{\perp_L} = \{y \in E^n \mid \forall x \in C,\ (y, x) = 0\}.$$

Thus the left (resp. right) dual of a left (resp. right) module is a left (resp. right) module. A code is **left self-dual** (resp. right self-dual) if it is equal to its left (resp. right) dual. A left self dual code C satisfies $C^{\perp_L} = C$. Likewise a right self dual code C satisfies $C^{\perp_R} = C$. A code is **self-dual** if it is equal to both of its duals.

Remark 1 *1. The repetition code of length 2 defined by $R_2 := \{00, aa, bb, cc\}$, is left self-dual. Its right dual is $R_2^{\perp_R} = \langle aa, bb, ab\rangle$, a supercode of R_2 of size 8.*

2. In length one, we have $J^{\perp_R} = J$. By taking direct sums of J with itself, we see that (right) self-dual codes over E exist for all lengths.

Remark 1 shows that the product of the sizes of a code and its dual is not always 4^n. A code C of length n is **left nice** (resp. **right nice**) if $|C||C^{\perp_L}| = 4^n$ (resp. $|C||C^{\perp_R}| = 4^n$). A code is **nice** if it is both left and right nice.

Remark 2 *J is a right nice code, but it is not a left nice code since $n = 1$, and $J^{\perp_L} = E$. Similarly, R_2 is not right nice since $R_2^{\perp_R}$ is of size* 8.

A code C is **self-orthogonal** if

$$\forall x, y \in C, (x, y) = 0.$$

Clearly, C is **self-orthogonal** iff $C \subseteq C^{\perp_L}$. Likewise, C is **self-orthogonal** iff $C \subseteq C^{\perp_R}$. Thus, for a self-orthogonal code C, we always have $C \subseteq C^{\perp_L} \cap C^{\perp_R}$. A code of length n is **quasi self-dual** if it is self-orthogonal and of size 2^n.

Remark 3 *Every one-sided nice self-dual code is quasi-self-dual but not conversely, as the next example shows.*

Example 1 *The code R_2 as a right module is quasi self-dual but not self-dual as $R_2 \subsetneq R_2^{\perp_R}$.*

Following a terminology from [6], a quasi self-dual code over E with all weights even is called a **Type IV** code.

3 Structure of linear codes

Let C be code of length n over E. With that code we associate two binary codes of length n :

1. the **residue code** defined by $res(C) = \{\alpha(y) \mid y \in C\}$,
2. the **torsion code** defined by $tor(C) = \{x \in \mathbb{F}_2^n \mid cx \in C\}$.

It can be checked that for all $x \in E^n$, we have $Tr(\phi(x)) = \alpha(x)$, and thus $res(C) = Tr(\phi(C))$, where $\forall z \in \mathbb{F}_4$, $Tr(z) = z + z^2$. Similarly, we see that $tor(C)$ is the subfield subcode of $\phi(C)$.

Example 2 *The* dodecacode*, the most famous additive code [3], is not $\phi(C)$ for some E-code C, since it can be checked by electronic computation that the residue and torsion code would have dimensions* 6, *and* 2 *respectively, contradicting Lemma 1 below.*

Denote by α_C the restriction of α to C. We see that $tor(C)c = \text{ Ker}(\alpha_C)$, and that $res(C) = \text{Im}(\alpha_C)$. By the first isomorphism theorem applied to the map α_C, we see that $|C| = |res(C)||tor(C)|$. There is a relationship between these two codes.

Lemma 1 *If C is an E-linear code then $res(C) \subseteq tor(C)$.*

Proof. Write an arbitrary codeword in c-adic decomposition form as $ax + cy$, with x, y binary vectors. Since $\alpha(ax + cy) = x$, we have $x \in res(C)$. Note that, by definition of the residue code, any $x \in res(C)$ arises in that way. Multiplying the codeword $ax + cy$ on the left by c, we see that $cx \in C$, implying $x \in tor(C)$. ∎

We let $k_1 = \dim(res(C))$, and $k_2 = \dim(tor(C)) - k_1$, a nonegative quantity by Lemma 1, and say that C is of **type** (k_1, k_2). It can be seen that C is free as an E-module iff $k_2 = 0$. Further, by a previous observation, $|C| = |res(C)||tor(C)| = 2^{2k_1+k_2}$. We give a characterization of the generator matrix of a linear code as a function of these invariants.

Theorem 1 *Assume C is an E-linear code of length n and type (k_1, k_2). Then a generator matrix G of C is of the form*

$$G = \begin{pmatrix} aI_{k_1} & X & Y \\ 0 & cI_{k_2} & cZ \end{pmatrix},$$

where I_j denotes the identity matrix of order j, the matrices X, Y have entries in E, and Z is a binary matrix.

Proof. Write the generator matrices of $res(C)$ and $tor(C)$ as $G_1 = \begin{pmatrix} I_{k_1} & \alpha(X) & \alpha(Y) \end{pmatrix}$ and $G_2 = \begin{pmatrix} I_{k_1} & \alpha(X) & \alpha(Y) \\ 0 & I_{k_2} & Z \end{pmatrix}$, respectively, where X, Y are matrices of suitable dimensions with entries in E, and Z is a binary matrix. By the first isomorphism theorem applied to the map α_C, the matrix G can be written in the form $\begin{pmatrix} R \\ cT \end{pmatrix}$, where

$$tor(C) = res(C) \oplus \langle T \rangle,$$

and $\alpha(R) = G_1$. ∎

We give a left oriented result and leave the right leaning reader generalize it.

Theorem 2 *Assume C is a left nice E-linear code of length n and type (k_1, k_2). Then a parity check matrix H of C consistent with Theorem 1 is of the form*

$$H = \begin{pmatrix} Y^t + Z^t X^t & aZ^t & aI_{n-k_1-k_2} \\ cX^t & cI_{k_2} & 0 \end{pmatrix},$$

where I_j denotes the identity matrix of order j, and X, Y, Z are as in Theorem 1. In particular $C^\perp$ is of type $(n-k_1-k_2, k_2)$. If, furthermore C is self-dual, then $n = 2k_1 + k_2$.

Proof. A direct calculation shows that $HG^t = 0$. This shows that, as left modules, $\langle H \rangle = E^{n-k_1}H \subseteq C^\perp$. Equality follows by size comparison upon noticing that $\langle H \rangle$ has type $(n - k_1 - k_2, k_2)$, and upon observing that by the niceness hypothesis we have $|C||C^{\perp_L}| = 4^n$. The last assertion follows by unicity of the type $k_1 = n - k_1 - k_2$. ∎

4 Constructions of quasi self-dual codes

We call the next construction of E-codes from binary codes the **multilevel construction**.

Theorem 3 *Let B be a self-orthogonal binary code of length n. The code C defined by the relation*

$$C = aB + cB^\perp,$$

is a quasi-self-dual code. Its residue code is B and its torsion code is $B^\perp$.

Proof. The code C is closed under addition, by linearity of B. Note that $aC \subseteq aB \subseteq C$.

Since B is self-orthogonal, we see that $cC \subseteq cB \subseteq cB^\perp \subseteq C$. Again by self-orthogonality of B we get $bC \subseteq bB \subseteq aB + cB \subseteq aB + cB^\perp \subseteq C$.

Thus C is E-linear.

For all x, x' in B and y, y' in $B^\perp$ we have the inner products

$$(ax + cy, ax' + cy') = a(x, x') + c(y, x') = 0$$

since B is self orthogonal. Thus C is self-orthogonal.

Since $|C| = |B||B^\perp| = 2^n$, we see that $|C| = 2^n$. The residue and torsion codes are direct to derive from the definitions. ∎

Remark 4 *1. The same result would hold for the rule $C = bB + cB^{\perp}$, by symmetry of the multiplication table between a and b.*

2. A similar construction for right modules is immediate and left to the reader.

The above multilevel construction leads to the following result. Henceforth, $\oplus$ will denote the direct sum of vector spaces and modules.

Corollary 1 *If B_1, and B_2 are two binary codes of length n, with $B_1 \subseteq B_2$, then there is an E-code C with residue code B_1 and torsion code B_2. If, furthermore, B_1 is self-orthogonal and $B_2 \subseteq B_1^{\perp}$ then C is self-orthogonal. If, in addition, $B_2 = B_1^{\perp}$, then C is quasi self-dual.*

Proof. Take $C = aB_1 + cB_2$ and apply the construction of Theorem 3. Note that then $|C| = |B_1||B_2|$. ∎

The most general construction of self-dual E-codes from the Residue /Torsion viewpoint is given in the next theorem, which requires the two following lemmas.

Lemma 2 *For all self-orthogonal E-linear codes C we have*

1. $res(C) \subseteq res(C)^{\perp}$,
2. $tor(C) \subseteq res(C)^{\perp}$,
3. $tor(C) = res(C)^{\perp}$ *if* $|C| = 2^n$.

Proof.

The first statement follows by the fact that α is a ring morphism. Note that if $ax + cy, cz \in C$ for binary vectors x, y, z then $(cz, ax + cy) = 0$ yielding $c(x, z) = 0$, hence $(x, z) = 0$. This proves the second statement. The last statement follows by *2*, and dimension count, since $|C| = 2^{2k_1+k_2} = 2^n$ yields $n - k_1 = k_1 + k_2$.

∎

The following lemma does not hold over other rings of size 4.

Lemma 3 *If C is a QSD code, and an arbitrary codeword of C is $aS + cT$, with S, T binary vectors of length n, then $S \in res(C)$, and $T \in tor(C)$. In particular, $a\,res(C) \subseteq C$.*

Proof. Since $\alpha(aS + cT) = S$, we see that $S \in res(C)$. Since $res(C) \subseteq tor(C)$ any $S' \in res(C)$, satisfies $aS' \in C$. Using the self-orthogonality of C, we get, $(aS + cT, aS') = 0$, and by *1* of Lemma 2 $(T, S') = 0$, $\forall S' \in res(C)$. Thus $T \in res(C)^{\perp} = tor(C)$, by *3* of Lemma 2. Since $cT \in C$, we see that $aS = (aS + cT) + cT \in C$. ∎

Theorem 4 *If a left linear code C of length n is quasi self-dual then*

1. $res(C) \subseteq res(C)^{\perp}$,
2. $tor(C) = res(C)^{\perp}$,
3. $n = 2k_1 + k_2$.

Furthermore, a quasi self-dual code C is Type IV iff $res(C)$ contains the all-one codeword.

Proof. By Lemma 2, the first two conditions are necessary. The third condition follows by $|C| = 2^{2k_1+k_2} = 2^n$.

We claim that a quasi self-dual code C is Type IV iff $tor(C)$ has only even weight codewords. This happens iff $res(C) = tor(C)^{\perp}$ contains the all-one codeword. We now prove the claim.

The condition is necessary as $c\,tor(C) \subseteq C$.

To prove that the condition is sufficient, write S, T for binary vectors of length n, such that $aS + cT \in C$. We see that

$$wt(aS + cT) = wt(S) + wt(T) - wt(S \cap T),$$

where we let $S \cap T = (s_1 t_1, \ldots, s_n t_n)$.

By assumption, and Lemma 3, we know that $wt(T)$ is even. Similarly $wt(S)$ is even since $res(C) \in tor(C)$. Now $wt(S \cap T)$ is congruent to (S, T) modulo 2, which is zero since $T \in tor(C) = res(C)^{\perp}$. Thus $wt(aS + cT) \equiv 0 \pmod 2$, showing sufficiency. ∎

The power of Lemma 3 is best illustrated by the following three results.

Theorem 5 *If C is QSD of minimum Hamming distance d, then $d \leq \lfloor \frac{n}{2} \rfloor + 1$. If, furthermore, C is Type IV, then $d \leq 2\lfloor \frac{n+2}{4} \rfloor$.*

Proof. Denote by d_R and d_T, respectively, the minimum distances of the residue and torsion codes of C. By definition of $tor(C)$, we have $d \leq d_T$. By Lemma 3, we have $a\,res(C) \subseteq C$, implying $d \leq d_R$. The Singleton bound for binary codes applied to $res(C)$ and $tor(C)$ successively shows then that

$$\begin{aligned} d &\leq n - k_1 + 1, \\ d &\leq n - k_1 - k_2 + 1. \end{aligned}$$

Adding up these two inequalities and using $n = 2k_1 + k_2$ yields

$$2d \leq 2n - n + 2 = n + 2.$$

Since d is an integer this yields $d \leq \lfloor \frac{n}{2} \rfloor + 1$. For a Type IV code, both n and d are even. Since $2\lfloor x/2 \rfloor$ is the largest even integer less than a real x, we see that $d \leq 2\lfloor \frac{\frac{n}{2}+1}{2} \rfloor = 2\lfloor \frac{n+2}{4} \rfloor$. ∎

The next result shows that all QSD codes can be obtained by a multilevel construction.

Theorem 6 *If C is QSD, then $C = a\,res(C) \oplus c\,tor(C)$ as modules.*

Proof. By Lemma 3 we have the inclusion $C \subseteq a\,res(C) + c\,tor(C)$. Comparing sizes of both sides shows that equality holds. Indeed, by hypothesis C has size 2^n. Since by Lemma **??**, we have $res(C) = tor(C)^{\perp}$, the size of the right handside is at most 2^n. Thus $C = a\,res(C) + c\,tor(C)$, and the counting argument shows that the sum is direct. ∎

Theorem 7 *If C is QSD, and is left linear, then $\phi(C) = \overline{\phi(C)}$. If, furthermore, $\phi(C)$ is linear then it admits a binary basis.*

Proof. By Lemma 3, if $as + ct \in C$, then both as and ct are in C. By left multiplication, $bs = b(as) \in C$. Thus $bs + ct \in C$, yielding that $\overline{\phi(as + ct)} = \phi(bs + ct) \in \phi(C)$, if $\phi(as + ct) \in \phi(C)$. The first assertion follows. If $\phi(C)$ is linear, let $G = (I, M)$ be its generator matrix in systematic form. The fact that $\phi(C) = \overline{\phi(C)}$ implies that $M = \overline{M}$. The rows of G form the sought basis. ∎

Example 3 *If C is a QSD code with $res(C) = tor(C)$, then its residue code is self-dual. It is easy to check by Theorem 6 that $\phi(C)$ is obtained by extension of scalars from $res(C)$. Formally, $C = res(C) \otimes \mathbb{F}_4$. Thus, a QSD code of length 8 can be constructed in that way from the extended Hamming code, a self-dual code of parameters $[8, 4, 4]$. Its weight enumerator can be computed to be as follows.*

$$[< 0, 1 >, < 4, 42 >, < 6, 168 >, < 8, 45 >].$$

The columns of its check matrix form a triple sum set in the sense of [16], since the sum of the weights $(4 + 6 + 8)$ equals $3 \times 8 \times \frac{3}{4}$.

5 Weight enumerators

In this section we study the weight enumerators of QSD codes. If r denotes a vector of E^n, denote by $n_i(r)$ the number of components taking the value $i \in E$ it contains. The **complete weight enumerator** cwe_C of an E-code C can then be defined as the homogeneous polynomial in four variables.

$$cwe_C((x_i)_{i\in E}) = \sum_{r\in C} \prod_{i\in E} x_i^{n_i(r)}.$$

The **weight enumerator** $W_C(x, y)$ of C is then defined as $W_C(x, y) = cwe_C((x_i)_{i\in E})$, when $x_0 = x$ and $x_i = y$ for $i \neq 0$. The **joint weight enumerator** of two binary codes is defined as follows. Let u, v denote binary vectors of length n. We define the integers $i(u, v)$, $j(u, v)$, $k(u, v)$ and $l(u, v)$ to be the number of indices $\iota \in \{1, \cdots, n\}$ with $(u_\iota, v_\iota) = (0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$, respectively.

The joint weight enumerator $J(A, B)$ of, say, two binary linear codes A, B, is the four-variable polynomial defined by the formula

$$J(A, B)(w, x, y, z) = \sum_{u\in A,\, v\in B} w^{i(u,v)} x^{j(u,v)} y^{k(u,v)} z^{l(u,v)}.$$

The following result connects the complete weight enumerator of a QSD code with that of its residue and torsion codes.

Theorem 8 *Order E as $(0, c, a, b)$. If C is QSD, then $cwe_C(w, x, y, z) = J(res(C), tor(C))(w, x, y, z)$.*

Proof. By Theorem 6 we can write any element of C in unique fashion as $au + cv$, with $u \in res(C)$, and $v \in tor(C)$. Considering the four cases $(u_i, v_i) = (0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$ yields in succession

$$(au + cv)_i = au_i + cv_i = 0,\ c,\ a,\ b.$$

The result follows. ∎

We proceed to derive the matrix group G under which the cwe_C of a QSD code C of residue code R is invariant.

Proposition 1

$$J(R, R^{\perp})(w, x, y, -z) = J(R, R^{\perp})(w, x, y, z).$$

Proof.

By orthogonality of $u \in R$ and $v \in R^{\perp}$, we see that $l(u, v)$ is even. ∎

Proposition 2

$$J(R, R^{\perp})(w, x, y, z) = \tfrac{1}{2^n} J(R, R^{\perp})(w + x + y + z,$$
$$w + x - y - z, w - x + y - z, w - x - y + z).$$

Proof. Combine MacWilliams identity [12, (32) p.148] between $J(R, R^{\perp})$ and $J(R^{\perp}, R)$ with the relation [12, (29) p.148]. ∎

Further, there is the following relation for n even.

Proposition 3 *If n is even, then*

$$J(R, R^{\perp})(-w, -x, -y, -z) = J(R, R^{\perp})(w, x, y, z).$$

Proof. Follows by homogeneity of the polynomial. ∎

The polynomial $J(R, R^{\perp})$ is an invariant of degree n of a group $G = \langle H, J, -I \rangle$ of order 24, where

$$2H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

and

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

The three generators are implied by the three above propositions. The Molien series of G is

$$\frac{1 + 2t^2 + t^4}{(1 - t^2)^3(1 - t^6)}.$$

This is consistent with the Molien series of [1, §3]. The relevant primary and secondary invariants can be found in [1, Appendix]. If, furthermore, C is Type IV, we need to use the fact that, by Theorem 4, $R^\perp$ has only even weight codewords .

Proposition 4 *If C is Type IV, then*

$$J(R, R^\perp)(w, -x, y, -z) = J(R, R^\perp)(w, x, y, z).$$

Proof. By Theorem 4, the QSD code C is Type IV iff R contains the all-one vector, that is to say iff $R^\perp$ has only even weights. Since the weight of $v \in R^\perp$ in terms of exponents of $J(R, R^\perp)$ is $j + l$, we see that $j + l$ is an even number. The result follows. ∎

This means that cwe_C is invariant under K where

$$K = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Let $G_4 = \langle G, K \rangle$. It turns out that G_4 is a group of order 48 with Molien series

$$\frac{1 + t^4}{(1 - t^2)^2(1 - t^4)(1 - t^6)}.$$

Define the following four primary invariants, of respective degrees $2, 2, 4, 6$.

$$
\begin{aligned}
f_2 &= w^2+x^2+y^2+z^2,\\
f_2' &= wy-1/2x^2-1/2z^2,\\
f_4 &= w^4+6wx^2y+6wyz^2-1/2x^4+3x^2z^2+y^4-1/2z^4,\\
f_6 &= w^6+6/17w^5y+15/17w^4x^2+15/17w^4y^2+15/17w^4z^2+\\
&\quad 60/17w^3x^2y+20/17w^3y^3+60/17w^3yz^2+15/17w^2x^4+\\
&\quad 90/17w^2x^2y^2+90/17w^2x^2z^2+15/17w^2y^4+90/17w^2y^2z^2+\\
&\quad 15/17w^2z^4+30/17wx^4y+60/17wx^2y^3+180/17wx^2yz^2+\\
&\quad 6/17wy^5+60/17wy^3z^2+30/17wyz^4+1/17x^6+15/17x^4y^2+\\
&\quad 15/17x^4z^2+15/17x^2y^4+90/17x^2y^2z^2+15/17x^2z^4+y^6+\\
&\quad 15/17y^4z^2+15/17y^2z^4+1/17z^6.
\end{aligned}
$$

We also need the secondary invariant of degree four

$$h_4 = w^4+10w^2x^2-2w^2y^2-2w^2z^2+x^4-2x^2y^2-2x^2z^2+y^4+10y^2z^2+z^4.$$

After specialization of the variables ($w=x$ and $x=y=z=y$) we obtain polynomials in two variables x, y.

$$
\begin{aligned}
g_2 &= x^2+3y^2,\\
g_2' &= xy-y^2,\\
g_4 &= x^4+12xy^3+3y^4,\\
g_6 &= x^6+6/17x^5y+45/17x^4y^2+140/17x^3y^3+315/17x^2y^4+366/17xy^5+199/17y^6\\
h_4' &= x^4+6x^2y^2+9y^4.
\end{aligned}
$$

We summarize the above discussion in the following Theorem.

Theorem 9 *If C is a Type IV E-code then its complete weight enumerator is in the $\mathbb{C}[f_2,f_2',f_4,f_6]$-module $\mathbb{C}[f_2,f_2',f_4,f_6]+h_4\mathbb{C}[f_2,f_2',f_4,f_6]$. Its Hamming weight enumerator is in the algebra $\mathbb{C}[g_2,g_2',g_4,g_6]$-module $\mathbb{C}[g_2,g_2',g_4,g_6]+h_4'\mathbb{C}[g_2,g_2',g_4,g_6]$.*

Remark 5

1. *The repetition code R_2 has weight enumerator g_2.*
2. *The group G_4 has the same size and Molien series as the group appearing in [15, §7.7] acting on the cwe of trace self-dual additive even codes that contain the all-one vector.*
3. *It is an open problem to describe the invariant ring of Type IV codes by only using invariants that are weight enumerators.*

6 Short length classification ($n < 7$)

In the following, we classify, up to equivalence, QSD codes by means of the multilevel construction, and of the characterization of Theorem 6. To each binary self orthogonal code is attached a QSD code, it is the residue code of. The torsion code is then the dual of the self-orthogonal code. By Theorem 4 and Theorem 6, classifying QSD E-codes up to permutation equivalence is equivalent to classifying self-orthogonal binary codes up to equivalence. Likewise, classifying Type IV QSD E-codes up to permutation equivalence is equivalent to classifying self-orthogonal binary codes containing the all-one vector up to equivalence.

We thus construct self-orthogonal codes by hand in short lengths and rely on the classification of Hou [11] to know the maximum number of equivalence classes.

Some codes can be generated by triads or tetrads. Recall that an **isotropic vector** $x \in E^n$ is any vector satisfying $(x, x) = 0$. We define a **triad** as an isotropic vector of Hamming weight three in E^n with $n \geq 3$. Likewise we define a **tetrad** as an isotropic vector of Hamming weight four in E^n with $n \geq 4$.

We use the term **additive generator matrix** to mean that the code is obtained by taking sums of the rows. Thus, the additive generator matrix of a QSD code is always a square matrix.

6.1 $n = 2$ (2 codes)

A QSD code that is not type IV can be constructed by the multilevel construction from the binary self-orthogonal code $\{\begin{pmatrix}0 & 0\end{pmatrix}\}$ and its dual, $\mathbb{F}_2^2$. Its generator matrix is

$$cI_2 = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

and its weight distribution is $[< 0, 1 >, < 1, 2 >, < 2, 1 >]$.

The other one is a type IV E-code with residue code the binary self-orthogonal code generated by $\begin{pmatrix}1 & 1\end{pmatrix}$. Its generator matrix is $\begin{pmatrix}a & a\end{pmatrix}$ and its weight distribution is $[< 0, 1 >, < 2, 3 >]$. Its ϕ-image is $\mathbb{F}_4$-linear.

6.2 $n = 3$ (2 codes)

One QSD code can be constructed from the binary self-orthogonal code generated by $\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$. Its generator matrix is cI_3 and its weight distribution is $[< 0, 1 >, < 1, 3 >, < 2, 3 >, < 3, 1 >]$.

The other QSD code can be constructed from the binary self-orthogonal code generated by $\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$. Its additive generator matrix is $\begin{pmatrix} a & 0 & a \\ c & 0 & c \\ 0 & c & 0 \end{pmatrix}$ and its weight distribution is $[< 0, 1 >, < 1, 1 >, < 2, 3 >, < 3, 3 >]$.

6.3 $n = 4, 5, 6$

We summarize the information in the following four tables.

Table 1: codes of length 4

Residue code	Generator Matrix	weight distribution	Type IV
$\langle \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix} \rangle$	cI_4	$[<0,1>,<1,4>,<2,6>,<3,4>,<4,1>]$	no
$\langle \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \rangle$	$\begin{pmatrix} c & 0 & 0 & c \\ a & 0 & 0 & a \\ 0 & c & 0 & 0 \\ 0 & 0 & c & 0 \end{pmatrix}$,	$[<0,1>,<1,2>,<2,4>,<3,6>,<4,3>]$	no
$\langle \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \rangle$	$\begin{pmatrix} c & 0 & 0 & c \\ a & a & a & a \\ 0 & c & 0 & c \\ 0 & 0 & c & c \end{pmatrix}$,	$[<0,1>,<2,6>,<4,9>]$	no
$\langle \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \rangle$	$\begin{pmatrix} a & 0 & a & 0 \\ 0 & a & 0 & a \end{pmatrix}$	$[<0,1>,<2,6>,<4,9>]$	yes

Table 2: codes of length 5

Residue code	Generator Matrix	weight distribution	Type IV
$\langle \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rangle$	cI_5	$[<0,1>,<1,5>,<2,10>,<3,10>,<4,5>,<5,1>]$	no
$\langle \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \end{pmatrix} \rangle$	$\langle \begin{pmatrix} a & a & 0 & 0 & 0 \\ c & c & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & c & 0 \\ 0 & 0 & 0 & 0 & c \end{pmatrix} \rangle$	$[<0,1>,<1,3>,<2,6>,<3,10>,<4,9>,<5,3>]$	no
$\langle \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \end{pmatrix} \rangle$	$\begin{pmatrix} a & a & a & a & 0 \\ c & 0 & 0 & c & 0 \\ 0 & c & 0 & c & 0 \\ 0 & 0 & 0 & 0 & c \end{pmatrix}$	$[<0,1>,<1,1>,<2,6>,<3,6>,<4,9>,<5,9>]$	no
$\langle \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \rangle$	$\begin{pmatrix} c & 0 & c & 0 & 0 \\ a & 0 & a & 0 & 0 \\ 0 & c & 0 & 0 & c \\ 0 & a & 0 & 0 & a \\ 0 & 0 & 0 & c & 0 \end{pmatrix}$	$[<0,1>,<1,1>,<2,6>,<3,6>,<4,9>,<5,9>]$	no

Table 3: codes of length 6, part I

Residue code	Generator Matrix	weight distribution	Type IV
$\langle\begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0\end{pmatrix}\rangle$	cI_6	$[<0,1>,<1,6>,<2,15>,<3,20>,<4,15>,<5,6>,<6,1>]$.	no
$\langle\begin{pmatrix}1 & 1 & 0 & 0 & 0 & 0\end{pmatrix}\rangle$	$\begin{pmatrix} a & a & 0 & 0 & 0 & 0 \\ c & c & 0 & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 & c & 0 \\ 0 & 0 & 0 & 0 & 0 & c \end{pmatrix}$	$[<0,1>,<1,4>,<2,9>,<3,16>,<4,19>,<5,12>,<6,3>]$	no
$\langle\begin{pmatrix}1 & 1 & 1 & 1 & 0 & 0\end{pmatrix}\rangle$	$\begin{pmatrix} a & a & a & a & 0 & 0 \\ c & 0 & 0 & c & 0 & 0 \\ 0 & c & 0 & c & 0 & 0 \\ 0 & 0 & c & c & 0 & 0 \\ 0 & 0 & 0 & 0 & c & 0 \\ 0 & 0 & 0 & 0 & 0 & c \end{pmatrix}$	$[<0,1>,<1,2>,<2,7>,<3,12>,<4,15>,<5,18>,<6,9>]$	no
$\langle\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1\end{pmatrix}\rangle$	$\begin{pmatrix} a & a & a & a & a & a \\ c & 0 & 0 & 0 & 0 & c \\ 0 & c & 0 & 0 & 0 & c \\ 0 & 0 & c & 0 & 0 & c \\ 0 & 0 & 0 & c & 0 & c \\ 0 & 0 & 0 & 0 & c & c \end{pmatrix}$	$[<0,1>,<2,15>,<4,15>,<6,33>]$	no

Table 4: codes of length 6, part II

Residue code	Generator Matrix	weight distribution	Type IV
$\langle \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \rangle$	$\begin{pmatrix} c & 0 & c & 0 & 0 & 0 \\ a & 0 & a & 0 & 0 & 0 \\ 0 & c & 0 & 0 & c & 0 \\ 0 & a & 0 & 0 & a & 0 \\ 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c \end{pmatrix}$	$[<0,1>,<1,2>,<2,7>,<3,12>,<4,15>,<5,18>,<6,9>]$	no
$\langle \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \rangle$	$\begin{pmatrix} c & 0 & 0 & 0 & c & c \\ a & 0 & a & a & 0 & a \\ 0 & c & 0 & 0 & c & 0 \\ 0 & a & 0 & a & a & a \\ 0 & 0 & c & 0 & c & c \\ 0 & 0 & 0 & c & 0 & c \end{pmatrix}$	$[<0,1>,<2,3>,<3,8>,<4,15>,<5,24>,<6,13>]$	no
$\langle \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \rangle$	$\begin{pmatrix} a & a & a & a & 0 & 0 \\ 0 & 0 & 0 & 0 & a & a \\ c & 0 & 0 & c & 0 & 0 \\ 0 & c & 0 & c & 0 & 0 \\ 0 & 0 & c & c & 0 & 0 \\ 0 & 0 & 0 & 0 & c & c \end{pmatrix}$	$[<0,1>,<2,9>,<4,27>,<6,27>$	no
$\langle \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \rangle$	$\begin{pmatrix} a & 0 & a & 0 & 0 & 0 \\ 0 & a & 0 & 0 & a & 0 \\ 0 & 0 & 0 & a & 0 & a \end{pmatrix}$	$[<0,1>,<2,9>,<4,27>,<6,27>]$	no

7 Conclusion and open problems

In this article we have studied quasi self-dual codes over the non-unital non-commutative ring E of order four. The existence of codes that are not nice preclude any attempt to derive a general MacWilliams formula, since this would imply a relation between the size of a code and that of its dual. We have thus introduced QSD codes as an alternative to the concept of self-dual codes. However, the special structure of QSD codes allowed us to use the invariant approach to the joint weight enumerator of the residue code and the torsion code.

Eventually, we gave a classification up to length 6 of the QSD codes, and of the Type IV QSD codes. Reference [11] allows us to reduce the classification problem for QSD codes to that of binary self-orthogonal codes. Since such a classification is not known in the literature for $n > 6$, another technique is needed in higher lengths. One possibility would be to derive a mass formula, as it exists already over certain rings [2, 9].

References

[1] A. Alahmadi, M. Deza, M. Dutour-Sikiric, P. Solé, Joint weight enumerator of an LCD code and its dual, Discrete Appl. Math, **257**, (2019) 12–18.

[2] J.M.L. Balmaceda, R.A.L. Betty,F. Nemenzo, Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$, Discrete Mathematics 308 (2008) 2984-3002.

[3] A.R. Calderbank, E.M. Rains, N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. on Information Th. **44**, (1998), 1369–1387.

[4] J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo four, J. Combinatorial Theory, Series A, **62** (1993), 30–45.

[5] M. Shi, A. Alahmadi, P. Solé, *Codes and Rings: Theory and Practice*, Acdemic Press (2017).

[6] Steven T. Dougherty, Philippe Gaborit, Masaaki Harada, Akihiro Munemasa, Patrick Solé, Type IV self-dual codes over rings. IEEE Trans. Information Theory 45(7): 2345-2360 (1999).

[7] T. Dougherty, Philippe Gaborit, Masaaki Harada, Patrick Solé, Type II Codes Over $F_2 + uF_2$. IEEE Trans. Information Theory 45(1): 32-45 (1999).

[8] B. Fine, Classification of finite rings of order p^2, Mathematics Magazine **66**, (4), (1993) 248–252.

[9] P. Gaborit, Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings, IEEE Trans. Inform. Theory 42 (1996) 1222–1228.

[10] A. Roger Hammons Jr., P. Vijay Kumar, A. Robert Calderbank, Neil J. A. Sloane, Patrick Solé, The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Information Theory 40(2): 301-319 (1994)

[11] X.D. Hou, On the Number of Inequivalent Binary Self-Orthogonal Codes, Trans. Inform. Theory 53 (2007), 2459–2479.

[12] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland (1977).

[13] `http://magma.maths.usyd.edu.au/magma/`

[14] R. Raghavendran, A class of finite rings, Compositio Mathematica, vol. 21, pp. 195–229, 1969.

[15] E.M. Rains, N.J.A. Sloane, Self-dual codes, in *Handbook of Coding Theory, I*, V.S. Pless, W.C. Hufman, eds, North Holland (1998).

[16] M. Shi, P. Solé, Three-weight codes, triple sum sets, and strongly walk regular graphs, Designs, Codes and Cryptography **87**, (10),(2019), 2395–2404.

[17] P. Solé, *Codes over Rings*, World Scientific (2008).