



**HAL**  
open science

# The build-up construction of quasi self-dual codes over a non-unital ring

Adel Alahmadi, Alaa Altassan, Hatoon Shoaib, Amani Alkathiry, Alexis Bonnetcaze, Patrick Solé

## ► To cite this version:

Adel Alahmadi, Alaa Altassan, Hatoon Shoaib, Amani Alkathiry, Alexis Bonnetcaze, et al.. The build-up construction of quasi self-dual codes over a non-unital ring. *Journal of Algebra and Its Applications*, 2021, 10.1142/S0219498822501432 . hal-03189828v2

**HAL Id: hal-03189828**

**<https://hal.science/hal-03189828v2>**

Submitted on 7 Apr 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Journal of Algebra and Its Applications  
 (2022) 2250143 (10 pages)  
 © World Scientific Publishing Company  
 DOI: 10.1142/S0219498822501432



## The build-up construction of quasi self-dual codes over a non-unital ring

Adel Alahmadi\*, Alaa Altassan† and Hatoon Shoaib‡

*The Department of Mathematics  
 King Abdulaziz University  
 Jeddah, Saudi Arabia  
 \*alahmadi@kau.edu.sa  
 †altassan@kau.edu.sa  
 ‡hashoaib@kau.edu.sa*

Amani Alkathiry

*The Department of Mathematics  
 King Abdulaziz University  
 Jeddah, Saudi Arabia  
 Umm Al-Qura University, Makkah, Saudi Arabia  
 aalkathiry@uqu.edu.sa*

Alexis Bonnecaze§ and Patrick Solé¶

*Aix Marseille Université, CNRS, Centrale Marseille  
 I2M, Marseille, France  
 §Alexis.Bonnecaze@univ-amu.fr  
 ¶sole@enst.fr*

Received 30 August 2019  
 Accepted 7 November 2019  
 Published

Communicated by S. K. Jain

There is a local ring  $E$  of order 4, without identity for the multiplication, defined by generators and relations as

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

We study a recursive construction of self-orthogonal codes over  $E$ . We classify, up to permutation equivalence, self-orthogonal codes of length  $n$  and size  $2^n$  (called here quasi self-dual codes or QSD) up to the length  $n = 12$ . In particular, we classify Type IV codes (QSD codes with even weights) up to  $n = 12$ .

*Keywords:* Non-unital rings; self-orthogonal codes; type IV codes.

Mathematics Subject Classification 2020: 94B05, 16A10

\*Corresponding author.

*A. Alahmadi et al.*

## 1. Introduction

The build-up method is a powerful technique to construct self-dual codes over fields and rings [7, 10]. Starting from a self-dual code of length  $n$ , it builds a self-dual code of length  $n + 2$  by a simple recursion. Under mild conditions, all codes sought for can be generated in that way.

In this paper, we adapt this method to generate quasi self-dual (QSD) codes over the ring  $E$ , a non-unital, non-commutative ring of order 4. While the four unital rings of order four  $\mathbb{F}_4, \mathbb{Z}_4, \mathbb{F}_2 + u\mathbb{F}_2, \mathbb{F}_2 \times \mathbb{F}_2$  have been used as alphabets in Coding Theory [14], the theory of codes over non-unital rings only started recently, in [1]. The ring  $E$  is one of the few non-unital rings of order 4 to study [4]. The importance of order 4 is the notion of Type IV codes. Over fields and unital rings, these are divisible self-dual codes over an alphabet of size 4. They have been studied over  $\mathbb{F}_4$  since the 1970s [9], and for the last three of the four rings mentioned above in [3]. To define them over  $E$  we need to replace self-dual codes by quasi self-dual codes. These are defined in [1] as self-orthogonal codes of length  $n$ , and size  $2^n$ . As explained in [1] some missing duality properties in non-unital rings make the study of self-dual codes over these rings intractable. Type IV codes can then be introduced as the subclass of QSD codes, all Hamming weights of which are even.

As in [10], only codes with dimension of residue code  $k_1 > 1$  are guaranteed to be obtained by the build-up construction, but QSD codes with dimension of residue code  $k_1 \leq 1$  are easy to construct directly. In particular, this method preserves the Type IV property. As a result, we classify QSD codes of length at most 12. We also classify Type IV codes of length  $n \leq 12$ .

This paper is organized as follows. Section 2 collects some necessary facts and notations about rings, codes and duality. Section 3 derives the main construction. Section 4 contains numerical data. Section 5 concludes the paper, and points out some open problems.

## 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 [4] we define a ring on two generators  $a, b$  by the relations

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

*The build-up construction of quasi self-dual codes over a non-unital ring*

A model for this 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:

×	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  $\mathbb{F}_2 = \{0, 1\}$ , 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  $r(s \oplus t) = rs + rt$ , where  $\oplus$  denote the addition in  $\mathbb{F}_2$ . On occasion we will use the **inner product notation**  $(x, r)$  for  $x \in \mathbb{F}_2^n, r \in E^n$  to denote

$$(x, r) = \sum_{i=1}^n x_i r_i = \sum_{x_i=1} r_i.$$

Denote by  $\alpha : E \rightarrow E/J \simeq \mathbb{F}_2$  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  $\mathbb{F}_2^n$ .

### 2.3. Modules

A **linear  $E$ -code**  $C$  of length  $n$  is a *one-sided  $E$ -submodule* of  $E^n$ . With that code we associate two binary codes of length  $n$  :

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

A. Alahmadi et al.

It is easy to check that  $\text{res}(C) \subseteq \text{tor}(C)$  [1]. It is traditional to denote by  $k_1$  the dimension of the residue code and  $k_1 + k_2$  that of the torsion code.

A simple application of the first isomorphism theorem [1], shows that

$$|C| = |\text{res}(C)||\text{tor}(C)| = 2^{2k_1+k_2}.$$

An **additive code** of length  $n$  over  $\mathbb{F}_4$  is an additive subgroup of  $\mathbb{F}_4^n$ . It is an  $\mathbb{F}_2$  vector space 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 alphabet substitution

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

where  $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ , extended naturally to  $\mathbb{F}_4^n$ . It can be checked that for all  $x \in E^n$ , we have  $\text{Tr}(\phi(x)) = \alpha(x)$ , and thus  $\text{res}(C) = \text{Tr}(\phi(C))$ , where  $\text{Tr}()$  denotes the usual **trace** from  $\mathbb{F}_4$  down to  $\mathbb{F}_2$ . Similarly, we see that  $\text{tor}(C)$  is the so-called **subfield subcode** of  $\phi(C)$  that is  $\mathbb{F}_2^n \cap \phi(C)$ .

We use the Magma notation

$$[\langle 0, 1 \rangle, \dots, \langle i, A_i \rangle, \dots, \langle n, A_n \rangle]$$

for the **weight distribution** of a quaternary code, where  $A_i$  is the number of codewords of weight  $i$  [12]. 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  $E^n$  by  $(x, y) = \sum_{i=1}^n x_i y_i$ .

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 (respectively, right) dual of a left (respectively, right) module is a left (respectively, right) module. A code is **left** (respectively, **right**) **self-dual** if it is equal to its left (respectively, 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.** 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.

**Observation.** 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** (respectively, **right nice**) if  $|C||C^{\perp L}| = 4^n$  (respectively,  $|C||C^{\perp R}| = 4^n$ ). A code is **nice** if it is both left and right nice.

*The build-up construction of quasi self-dual codes over a non-unital ring*

**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 [3], a quasi self-dual code over  $E$  with all weights even is called a **Type IV** code.

### 3. Construction

The following result constructs a quasi self-dual code of length  $n + 2$  from a quasi self-dual code of length  $n$ .

**Theorem 1.** *Let  $C_0$  denote a quasi self-dual code of length  $n$  over  $E$ , with generating set  $r_1, \dots, r_k$ . Let  $x$  be a fixed vector in  $\mathbb{F}_2^n$  satisfying  $(ax, ax) = a$ . (Thus any  $x$  of odd Hamming weight works). Write  $y_i = (x, r_i)$  for  $1 \leq i \leq k$ . The row-span of the following  $k + 1$  vectors is a quasi self-dual code  $C$  of length  $n + 2$ .*

$$(a, 0, ax), (y_1, y_1, r_1), \dots, (y_k, y_k, r_k).$$

**Proof.** First, we check that  $C$  is self-orthogonal.

- the first vector is orthogonal to itself by definition of  $x$ , since  $a^2 + a = 0$ .
- the last  $k$  vectors are orthogonal to each other and to themselves by self-orthogonality of  $C_0$ , since  $y_i y_j + y_i y_j + (r_i, r_j) = 0$ .
- the first vector is orthogonal to the last  $k$  vectors by definition of the  $y_i$ 's since  $ay_i + (ax, r_i) = ay_i + ay_i = 0$ .
- Any of the last  $k$  vectors is orthogonal to the first vector since  $y_i a + (r_i, ax) = y_i + (r_i, x) = y_i + (x, r_i) = 0$ .

Hence  $C$  is self-orthogonal.

We claim that  $|C| = 4|C_0| = 2^{n+2}$ . Indeed define  $\widehat{C}_0$  as the row span of the last  $k$  generators. Write  $S_y = (y, 0, yx)$ , for all  $y \in E$ . Then it can be seen that the construction in the theorem is equivalent to the following disjoint union of four cosets of  $\widehat{C}_0$  :

$$C = \dot{\cup}_{y \in E} (S_y + \widehat{C}_0).$$

Thus  $C$  is quasi self-dual of length  $n + 2$ . □

A. Alahmadi et al.

**Remark 4.** For a given  $C_0$  by varying  $x$  we can construct  $2^{n-1}$  codes  $C$ .

**Corollary 1.** In the notation of the Theorem, if  $C_0$  is Type IV, so is  $C$ .

**Proof.** By [1] it is enough to check that  $\text{res}(C)$  contains the all-one vector. Let  $j_m$  denote the all-one vector of length  $m$ . By hypothesis  $\text{res}(C_0)$  contains  $j_n$ . Thus  $j_n = \sum_{i=1}^k a_i \alpha(r_i)$ , for some  $a_i \in \mathbb{F}_2$ . Consider the same linear combination of the last  $k$  generators of  $C$ .

$$\sum_{i=1}^k a_i \alpha((y_i, y_i, r_i)) = \left( \sum_{i=1}^k a_i \alpha(y_i), \sum_{i=1}^k a_i \alpha(y_i), j_n \right).$$

To check that this combination equals  $j_{n+2}$ , we note that

$$\sum_{i=1}^k a_i \alpha(y_i) = \left( x, \sum_{i=1}^k a_i \alpha(r_i) \right).$$

But, by the defining equation of the  $a_i$ 's we have

$$\left( x, \sum_{i=1}^k a_i \alpha(r_i) \right) = (x, j_n) = 1,$$

since  $x$  has odd Hamming weight. Thus  $j_{n+2} \in \text{res}(C)$ , showing that  $C$  is Type IV.  $\square$

The next result shows that all QSD codes can be obtained from the build-up construction, subject to a mild condition.

**Theorem 2.** If  $C$  is quasi self-dual code of length  $n + 2$  with  $k_1 > 1$ , then there is a quasi self-dual code  $C_0$  of length  $n$ , such that the construction of Theorem 1 applied to  $C_0$  produces  $C$ .

**Proof.** Let  $R_1, R_2, \dots, R_{k+1}$  denote the generators of  $C$  viewed as an  $E$ -module. Let  $R'_i$  be  $R_{i+1}$  with the first two columns removed for  $i = 0, \dots, k$ .

W.L.O.G. we may assume that  $R_1$  contains only zeros and  $a$ 's, by using  $a^2 = ab = ac = a$ . We may also assume since  $k_1 > 1$ , that  $R_1 = (a, 0, R'_0), R_2 = (a, a, R'_1)$  and that, most importantly, that  $R_{i+1} = (0, 0, R'_i)$  for  $i \geq 2$ . The orthogonality relations  $(R_{i+1}, R_{j+1}) = 0$  imply  $(R'_i, R'_j) = 0$  for all  $1 \leq i, j \leq k$ . Thus  $C_0$ , spanned by  $R'_1, \dots, R'_k$ , is self-orthogonal.

It is also easy to check that, as in the proof of Theorem 1, we have  $|C_0| = \frac{|C|}{4} = 2^n$ .

The code obtained by applying Theorem 1 to the code  $C_0$  spanned by  $R'_1, \dots, R'_k$ , with  $x$  defined by  $R'_0 = ax$ , is row-equivalent to  $G$ . Indeed, with this definition of  $x$ , it can be checked that  $y_1 = a$ , and  $y_i = 0$  for  $i = 2, \dots, k$ . Indeed, the two conditions  $(R_1, R_2) = (R_2, R_1) = 0$  imply  $ay_1 = y_1a = a$ . Taken together these two conditions imply  $y_1 = a$ . Likewise, for  $2 \leq i \leq k$  the conditions  $(R_1, R_{i+1}) = (R_{i+1}, R_1) = 0$  imply  $ay_i = y_i a = 0$ . Taken together these two conditions imply  $y_i = 0$ .  $\square$

*The build-up construction of quasi self-dual codes over a non-unital ring*

It is easy to characterize codes where the hypothesis of this Theorem is not satisfied, as the next result shows.

**Theorem 3.** (1) *If  $C$  is QSD with  $k_1 = 0$ , then  $C = c\mathbb{F}_2^n$ . Such a code is not Type IV.*  
 (2) *If  $C$  is QSD with  $k_1 = 1$ , then  $C = aB \oplus cB^\perp$ , with  $B$  a self-orthogonal  $[n, 1]$  binary code. The code  $C$  is Type IV iff  $B$  is the repetition code of length  $n$  for some even  $n$ .*

**Proof.** By [1, Theorem 6], we know that  $C = a \operatorname{res}(C) \oplus c \operatorname{tor}(C)$ , with  $\operatorname{res}(C) \subseteq \operatorname{tor}(C)$ .

- (1) If  $C$  is QSD with  $k_1 = 0$ , then  $C = c \operatorname{tor}(C)$ . Since  $n$  is both its dimension and its length, the binary code  $\operatorname{tor}(C)$  has to be the  $[n, n, 1]$  “universe” code, denoted here by  $\mathbb{F}_2^n$ . The QSD code  $C$  is not Type IV as it contains codewords of odd weight.
- (2) If  $C$  is QSD with  $k_1 = 1$ , then  $C = a \operatorname{res}(C) \oplus c \operatorname{tor}(C)$ , with  $\operatorname{res}(C)$  a self-orthogonal code of dimension one. By [1, Theorem 4], the code  $C$  is Type IV iff  $\operatorname{res}(C)$  contains the all-one vector, iff  $\operatorname{res}(C)$  is the repetition code of length  $n$  for some even  $n$ .  $\square$

**Example 2.** • We obtain an infinite family of Type IV codes for each even  $n$  by letting  $K_n = aU_n + cU_n^\perp$ , with  $U_n$  denoting the repetition code of parameters  $[n, 1, n]$ . Thus  $K_n$  is the analogue of the Klemm code of [2].

- For  $n = 5$ , if we take  $\operatorname{res}(C) = \langle (1, 1, 0, 0, 0) \rangle$ , we obtain a non-Type IV QSD code with weight distribution:

$$[\langle 0, 1 \rangle, \langle 1, 3 \rangle, \langle 2, 6 \rangle, \langle 3, 10 \rangle, \langle 4, 9 \rangle, \langle 5, 3 \rangle].$$

#### 4. Numerical Results

All the calculations in this section were performed in Magma [12]. When classifying QSD codes or Type IV codes up to permutation equivalence, the following result will be used.

**Theorem 4.** *Two QSD E-codes  $C$  and  $C'$  are permutation equivalent iff their residue codes are.*

**Proof.** The condition is necessary, since the residue of the permuted code is a permutation of the residue code.

The condition is sufficient. If  $A, B$  are binary codes, and  $P$  is a permutation acting on their coordinate places, it is easy to check, by invariance of the inner product, that  $P(A) = B$  iff  $P(A^\perp) = B^\perp$  [9, Chap. 1, Example 35]. By [1, Theorem 6], we have  $C = a \operatorname{res}(C) \oplus c \operatorname{res}(C)^\perp$ . Thus, if  $P(\operatorname{res}(C)) = \operatorname{res}(C')$ , then, by that result with  $A = \operatorname{res}(C)$  and  $B = \operatorname{res}(C')$ , we obtain, by linearity of the action of  $P$ , that  $P(C) = C'$ .  $\square$



A. Alahmadi et al.

In order to obtain all QSD codes of a given length, we recursively apply Theorem 1 from different codes. For example, Theorem 1 applied to the code whose generator matrix is  $cI_2$  (where  $I_2$  is an identity matrix of order 2) yields two QSD-codes of length 4, not Type IV, and up to equivalence, it yields one QSD-code with  $k_1 = 1$ . Theorem 1 applied to these two codes yields sixteen QSD-codes of length 6 (not Type IV) and two QSD-codes up to equivalence with  $k_1 = 2$ . In this way, we obtain QSD-codes of length  $2n$  with  $k_1 = n - 1$ . The same construction using generator matrix  $cI_4$  (where  $I_4$  is an identity matrix of order 4) yields QSD-codes of length  $2n$  with  $k_1 = n - 2$ , and so on.

To make sure that enough equivalence classes of codes have been generated by our algorithms, we have consulted the tables of number of equivalence classes of self-orthogonal binary codes contained in [8].

The generator matrices of the classified codes up to  $n = 11$ , and the weight distributions of QSD-codes up to  $n = 12$  can be found at:

<http://alexis.bonnetcaze.perso.luminy.univ-amu.fr/publication/>.

#### 4.1. QSD codes of odd length

From one QSD code of length 3, the number of codes of length  $n$  generated by Theorem 1, by the remark following Theorem 1, is

$$2^{\sum_{m=0}^{(n-3)/2} (2m)} = 2^{((n-2)^2-1)/4}.$$

In the following tables, the rows indicate, in order, the length, the dimension of the residue code ( $k_1$ ), the number of equivalence classes of codes in that set, and the largest minimum distance obtained. This convention is maintained for the next tables.

$n$	3		5			7			9				11				
$k_1$	1	1	2	1	2	3	1	2	3	4	1	2	3	4	5		
$\# \sim$	1	2	1	3	3	2	4	6	6	3	5	10	14	12	4		
$d$	2	1	1	1	1	3	1	1	2	2	1	1	2	2	3		

#### 4.2. QSD codes of even length not Type IV

From one QSD code of length 2 (Type IV or not), the number of codes of length  $n$  generated by Theorem 1, by the remark following Theorem 1, is

$$2^{\sum_{m=0}^{(n-4)/2} (2m+1)} = 2^{n^2/4-n+1}.$$

For instance, we have for  $n = 2$ , a unique QSD non Type IV code with  $k_1 = 0$ , as described in Theorem 3. As for QSD non Type IV of even length, we have the following table:

$n$	4	6		8			10				12				
$k_1$	1	1	2	1	2	3	1	2	3	4	1	2	3	4	5
$\# \sim$	1	2	2	3	4	3	4	8	9	6	5	13	21	21	9
$d$	1	1	2	1	2	2	1	2	2	2	1	2	2	2	3

*The build-up construction of quasi self-dual codes over a non-unital ring*

**4.3. Type IV codes of even length**

As observed in [1], Type IV codes can only exist in even length as the residue code must be self-orthogonal and contain the all-one vector. There is a unique Type IV code of length 2 namely  $R_2$  defined in Sec. 2, since for such a code the weights must be either 0 or 2. Theorem 1 applied to  $R_2$  gives two codes, whose images by  $\phi$  are  $\mathbb{F}_4$ -linear, and permutation equivalent to a  $[4, 2, 2]$  with generator matrix  $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ .

The other Type IV code can be constructed in the form

$$a\langle(1, 1, 1, 1)\rangle + c\langle(1, 1, 1, 1)\rangle^\perp.$$

Its image by  $\phi$  is an  $\mathbb{F}_4$ -additive code (not  $\mathbb{F}_4$ -linear) with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ w & w & w & w \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

and weight distribution  $[\langle 0, 1 \rangle, \langle 2, 6 \rangle, \langle 4, 9 \rangle]$ . Note that even though they possess the same weight distribution, these two codes are different, one being linear.

Information for lengths 4 to 12 is summarized in the following table:

$n$	4		6			8				10					12					
$k_1$	1	2	1	2	3	1	2	3	4	1	2	3	4	5	1	2	3	4	5	6
$\# \sim$	1	1	1	1	1	1	2	2	2	1	2	3	3	2	1	3	5	7	6	3
$d$	2	2	2	2	2	2	2	4	2	2	2	2	2	2	2	2	2	2	2	4

**5. Conclusion and Open Problems**

In this paper, we have applied the build-up method of construction of self-dual codes to quasi self-dual codes over a non-unital ring of order 4. As a result, we have been able to classify QSD codes, and Type IV QSD codes of length at most 12 up to equivalence.

To study higher lengths, a mass formula similar to what exists already over finite fields [11], or over  $\mathbb{Z}_4$  [5] might be needed. In view of the super-exponential number of codes generated by Theorem 1, more computing power might be needed to extend the numerical results to lengths larger than 12.

**References**

[1] A. Alahmadi, A. Altassan, W. Basaffar, A. Bonnecaze, H. Shoaib and P. Solé, Type IV codes over a non-unital ring, *J. Algebra and its Applications*, to appear.  
 [2] J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo four, *J. Combin. Theory Ser. A* **62** (1993) 30–45.  
 [3] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, Type IV self-dual codes over rings, *IEEE Trans. Inform. Theory* **45**(7) (1999) 2345–2360.  
 [4] B. Fine, Classification of finite rings of order  $p^2$ , *Math. Mag.* **66**(4) (1993) 248–252.

A. Alahmadi et al.

- [5] 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.
- [6] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank and N. J. A. Sloane, Patrick Solé: The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40**(2) (1994) 301–319.
- [7] S. Han, H. Lee and Y. Lee, Construction of self-dual codes over  $\mathbb{F}_2 + u\mathbb{F}_2$ , *Bull. Korean Math. Soc.* **49** (2012) 135–143.
- [8] X. D. Hou, On the number of inequivalent binary self-orthogonal codes, *Trans. Inform. Theory* **53** (2007) 2459–2479.
- [9] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes* (Cambridge University Press, Cambridge, 2003).
- [10] J.-L. Kim and Y. Lee, Euclidean and hermitian self-dual MDS codes over large finite fields, *J. Combin. Theory Ser. A* **105** (2004) 79–95.
- [11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).
- [12] <http://magma.maths.usyd.edu.au/magma/>.
- [13] R. Raghavendran, A class of finite rings, *Compos. Math.* **21** (1969) 195–229.
- [14] M. Shi, A. Alahmadi and P. Solé, *Codes and Rings: Theory and Practice* (Academic Press, Amsterdam, 2017).