THE BUILD-UP CONSTRUCTION OVER A COMMUTATIVE NON-UNITAL RING

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

Manuscript submitted to
AIMS' Journals
Volume **X**, Number **0X**, XX **200X**

doi:10.3934/xx.xx.xx.xx

pp. **X–XX**

THE BUILD-UP CONSTRUCTION OVER A COMMUTATIVE NON-UNITAL RING

Adel Alahmadi*

Math Dept, King Abdulaziz University
Jeddah, Saudi Arabia

Amani Alkathiry

Math Dept, King Abdulaziz University
also with Umm Al-Qura University, Makkah, Saudi Arabia
Jeddah, Saudi Arabia

Alaa Altassan

Math Dept, King Abdulaziz University
Jeddah, Saudi Arabia

Alexis Bonnecaze

Aix Marseille Univ, CNRS, Centrale Marseille
I2M, Marseille, France.

Hatoon Shoaib

Math Dept, King Abdulaziz University
Jeddah, Saudi Arabia

Patrick Solé

Aix Marseille Univ, CNRS, Centrale Marseille
I2M, Marseille, France.

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

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

We study a recursive construction of self-orthogonal codes over I. We classify self orthogonal codes of length n and size 2^n (called here quasi self-dual codes or QSD) up to the length $n = 6$. In particular, we classify Type IV codes (i.e. QSD codes with even weights) and quasi Type IV codes (i.e. QSD codes with even torsion code) up to $n = 6$.

2010 *Mathematics Subject Classification.* Primary: 49B05; Secondary: 16A10.
Key words and phrases. non-unital rings, self-orthogonal codes, Type IV codes.

1. **Introduction.** The build-up method is a powerful technique to construct self-dual codes over fields and rings [7, 8]. Starting from a self-dual code of length n, it builds a self-dual code of length $n+2$ by a simple recursion. This method was used successfully over a non-unital non commutative ring in [1].
In this article, we adapt this method to generate quasi self-dual (QSD) codes over the ring I, a non-unital, commutative ring of order 4 [3]. QSD codes are defined in that reference as self-orthogonal codes of length n, and size 2^n. This special concept plays an analogous role in I to that played by self-dual codes over fields and unital rings. Of special interest is the subclass of Type IV codes, namely QSD codes with all weights even, which exists for several rings of order four [10, 2]. A relaxation of that concept that is special to the ring I is that of quasi Type IV codes (QTIV), that is to say QSD codes with an even torsion code [3]. While the build up constructions do not seem to preserve the class of Type IV codes, they are shown here to preserve the wider class of QTIV codes. As a result, we classify QSD codes of length at most 6. We also classify Type IV codes and QTIV codes of length $n \leq 6$. The material is organized as follows. The next section collects some necessary facts and notations about codes, rings, modules, and duality. Section 3 derives the main construction. Section 4 contains numerical data. Section 5 concludes the article, 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: $C \subseteq C^\perp$. A code is **even** if all its codewords have even weight. All self-orthogonal binary codes are even, but not all even codes are self-orthogonal. Two binary codes are **equivalent** if there is a permutation of coordinates that maps one to the other.

2.2. **Rings.** Following [11] we define a ring on two generators a, b by its relations

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

Thus, I has characteristic two, and consists of four elements $I = \{0, a, b, c\}$, 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	b	0	b
b	0	0	0	0
c	0	b	0	b

From this table, we infer that this ring is commutative, and without an identity element for the multiplication. It is local with maximal ideal $J = \{0, b\}$, and residue field $\mathbb{F}_2 = \{0, 1\}$, the finite field of order 2. Thus we have a **b-adic decomposition** as follows. Every element $i \in I$ can be written

$$i = as + bt,$$

where $s, t \in \mathbb{F}_2$ and where we have defined a natural **action** of $\mathbb{F}_2$ on I by the rule $r0 = 0r = 0$ and $r1 = 1r = r$ for all $r \in I$. Thus $a = 1a, c = 1c$ and $c = a1+b1$. Note that for all $r \in I$, 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 $x \in \mathbb{F}_2^n$, $r \in I^n$ to denote

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

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

2.3. **Modules.** A **linear** I-code C of length n is an I-submodule of I^n. It can be described as the I-span of the rows of a **generator matrix**. 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 $tor(C) = \{x \in \mathbb{F}_2^n \mid bx \in C\}$.

It is easy to check that $res(C) \subseteq tor(C)$ [3]. 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 [3], shows that

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

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 I-code C is attached an additive $\mathbb{F}_4$-code $\phi(C)$ by the alphabet substitution

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

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

We use the Magma notation (Cf. the Handbook section of [16])

$$[< 0, 1 >, \cdots, < i, A_i >, \cdots, < n, A_n >]$$

for the **weight distribution** of a quaternary code, where A_i is the number of codewords of weight i. Two I-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 I^n as $(x, y) = \sum_{i=1}^{n} x_i y_i$.

The **dual** $C^\perp$ of C is the module defined by

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

Thus the dual of a module is a module. A code is **self-dual** if it is equal to its dual.

Remark 1. *The repetition code of length* 2 *is defined by* $R_2 := \{00, aa, bb, cc\}$. *Its dual is* $R_2^\perp = \{00, aa, bb, cc, 0b, b0, ac, ca\}$, *a supercode of* R_2 *of size* 8. *In length one, we have* $J^\perp = I$.

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

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

Clearly, C is **self-orthogonal** iff $C \subseteq C^\perp$.

A code of length n is **quasi self-dual** if it is self-orthogonal and of size 2^n.

Following a terminology from [10], a quasi self-dual code over I with all weights even is called a **Type IV** code.

Remark 2. *The repetition code of length* 2 *is quasi self-dual over* I *and is of Type IV. This shows, by taking direct sums of codes, that Type IV codes over* I *exits for all even lengths. We see that* J *is a quasi self-dual code over* I. *This shows, again by taking direct sums, that QSD codes exist for all integer lengths.*

Following a terminology introduced in [3], we shall call a QSD code with an even torsion code **quasi Type IV** (QTIV). Every Type IV code is quasi Type IV but not conversely as the next example shows.

Example 1. *The code with the three generators* $\begin{pmatrix} a & b & a & b \\ 0 & b & b & 0 \\ b & 0 & 0 & b \end{pmatrix}$ *is QSD but not Type IV as the sum of first and second row has odd weight. But its torsion code with generator matrix* $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ *is an even code. Thus, it is quasi Type IV.*

3. **Construction.** In this section we discuss two kinds of construction methods for quasi self-dual codes over I. The following theorem is the first one, constructing quasi self-dual codes of length increased by two, with one more generator.

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

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

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

- the first vector is orthogonal to itself by definition of x, since $a^2 + a^2(x, x) = 0$.

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

Hence C is self-orthogonal. We claim that $|C| = 4|C_0| = 2^{n+2}$. Indeed define $\widehat{C_0}$ as the generator span of the last k generators. Write $S_y = (y, 0, yx)$, for all $y \in I$. Then it can be seen that the construction in the theorem is equivalent to

$$C = \dot{\cup}_{y\in I}(S_y + \widehat{C_0}),$$

where $\dot{\cup}$ denotes disjoint union. Thus C is quasi self-dual of length $n + 2$. □

The next result shows that this construction preserves the quasi Type IV property.

Corollary 1. *If C_0 is QTIV then C obtained from the previous theorem is also QTIV.*

Proof. Since C_0 is quasi Type IV, then $tor(C_0)$ is an even code. If $tor(C_0)$ is even so is $tor(\widehat{C_0})$, since we are only adding two equal coordinates. Because $S_b = b(1, 0, x)$ we see that $tor(C) = tor(\widehat{C_0})\dot{\cup}((1, 0, x) + tor(\widehat{C_0}))$. Since $(x, x) = 1$, the vector $(1, 0, x)$ has even weight. Thus $tor(C)$ is even, and C is quasi Type IV. □

The second kind of construction also constructs QSD codes of length two more, but with two more generators.

Theorem 2. *Let C_0 be a quasi self-dual code of length n over I and $G_0 = (r_i)$ be a $k \times n$ generator matrix for C_0, where r_i is the i-th generator of G_0 , $1 \le i \le k$. Let x be a fixed vector in $\mathbb{F}_2^n$. For $1 \le i \le k$, let $y_i = ((x, r_i), (x, r_i))$ be a vector of length 2. Then the following generators*

$$(b, 0, bx), (0, b, bx), (y_1, r_1), \ldots, (y_k, r_k).$$

generate a quasi self-dual code C over I of length $n + 2$

Proof. Firstly, we show that C is self-orthogonal.

- The first generator is orthogonal to itself since $b^2 + b^2(x, x) = 0$. Similarly the second generator is orthogonal to itself.
- The first generator is orthogonal to the second generator as $b^2(x, x) = 0$.
- The first (or, the second) generator is orthogonal to any one of the last k generators since $b(x, r_i) + (bx, r_i) = 0$.
- The last k generators are orthogonal to each other and to themselves by self-orthogonality of C_0 since $(y_i, y_j) + (r_i, r_j) = (x, r_i)(x, r_j) + (x, r_i)(x, r_j) = 0$

Hence, the set of k generators generates a self-orthogonal code C. 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 $S_y = (y, 0, yx)$, $T_y = (0, y, yx)$ for all $y \in I$. Then it can be seen that the construction in the theorem is equivalent to

$$C = \dot{\cup}_{y,z\in J}(S_y + T_z + \widehat{C_0}).$$

Therefore, C is quasi self-dual code of length $n + 2$ □

Like for the first construction, we have a result on quasi Type IV codes.

Corollary 2. *If C_0 is QTIV then C obtained from the previous theorem is also QTIV if $(x, x) = 1$.*

Proof. Since C_0 is quasi Type IV, $tor(C_0)$ is even. If $tor(C_0)$ is even so is $tor(\widehat{C_0})$. Because both $S_b = b(1, 0, x)$ and $T_b = b(0, 1, x)$ are multiples of a binary vector by b, we see that

$$tor(C) = tor(\widehat{C_0})\dot{\cup}((1, 0, x) + tor(\widehat{C_0}))\dot{\cup}((0, 1, x) + tor(\widehat{C_0})).$$

Since, by hypothesis, $(x, x) = 1$, the vectors $(1, 0, x)$ and $(0, 1, x)$ have even weight. Thus, $tor(C)$ is even, and C is QTIV. □

Remark 3. *The number of codes generated from a given C_0 depends on the number of choices for x. Thus Theorem 1 generates 2^{n-1} codes, and Theorem 2 generates 2^n codes.*

4. **Numerical results.** In this section, we continue the classification of inequivalent codes given in [3] for $n < 4$, by means of the methods described in this paper up to $n = 6$. It is an open problem to know if the build-up methode can produce enough inequivalent codes in higher lengths.

We take for granted that QSD codes containing odd weight vectors cannot be Type IV.

Recall from [3] the following results.

- For $n = 1$ there is just one code generated by the matrix (b).
- For $n = 2$ there are two Type IV codes with weight distribution $[< 0, 1 >, < 2, 3 >]$.
- For $n = 3$ there are four QSD codes with weight distributions $[< 0, 1 >, < 1, 2 >, < 2, 1 >, < 3, 4 >]$ (two codes), $[< 0, 1 >, < 1, 2 >, < 2, 5 >]$, $[< 0, 1 >, < 1, 1 >, < 2, 3 >, < 3, 3 >]$ (two codes), and two QTIV codes with weight distribution $[< 0, 1 >, < 2, 5 >, < 3, 2 >]$.

4.1. **Length 4.** For $k = 1$, we obtain 14 codes with weight distributions
$[< 0, 1 >, < 1, 2 >, < 2, 2 >, < 3, 2 >, < 4, 9 >]$ (2 codes)
$[< 0, 1 >, < 1, 1 >, < 2, 5 >, < 3, 7 >, < 4, 2 >]$ (2 codes)
$[< 0, 1 >, < 1, 2 >, < 2, 2 >, < 3, 10 >, < 4, 1 >]$
$[< 0, 1 >, < 1, 3 >, < 2, 3 >, < 3, 5 >, < 4, 4 >]$
$[< 0, 1 >, < 1, 2 >, < 2, 6 >, < 3, 2 >, < 4, 5 >]$
$[< 0, 1 >, < 1, 3 >, < 2, 7 >, < 3, 5 >]$
$[< 0, 1 >, < 1, 2 >, < 2, 4 >, < 3, 6 >, < 4, 3 >]$ (2 codes)
$[< 0, 1 >, < 2, 6 >, < 4, 9 >]$ (2 codes, Type IV)
$[< 0, 1 >, < 2, 8 >, < 3, 4 >, < 4, 3 >]$ (2 codes, QTIV).

For $k = 2$, we obtain 10 codes with weight distributions
$[< 0, 1 >, < 2, 2 >, < 3, 8 >, < 4, 5 >]$ (3 codes)
$[< 0, 1 >, < 2, 4 >, < 3, 4 >, < 4, 7 >]$ (4 codes)
$[< 0, 1 >, < 2, 6 >, < 4, 9 >]$ (Type IV, 3 codes).

4.2. **Length 5.** The main properties are summarized in the following table.

k	d	# codes	# Type IV	# QTIV
1	1	20	0	0
1	2	4	0	4
2	1	26	0	0
2	2	36	0	26

4.3. **Length 6.** The main properties are summarized in the following table.

k	d	# codes	# Type IV	# QTIV
1	1	34	0	0
1	2	6	2	6
2	1	176	0	0
2	2	141	4	92
3	2	104	8	104

5. **Conclusion.** In this article, we have applied the build-up method of construction of self-dual codes to quasi self-dual codes over a commutative non-unital ring of order 4. As a result, we have been able to classify QSD codes, Type IV codes and QTIV codes of length at most 6 up to equivalence.

In view of the super-exponential number of codes generated by this method, more computing power might be needed to extend the numerical results to higher lengths .

REFERENCES

[1] A. Alahmadi, A. Alkathiry, A. Altassan, A. Bonnecaze, H. Shoaib, P. Solé, The build-up construction of quasi self-dual codes over a non-unital ring, to appear in JAA .https://hal.archives-ouvertes.fr/hal-02433508

[2] A. Alahmadi, A. Altassan, W. Basaffar, A. Bonnecaze, H. Shoaib, P. Solé, Type IV codes over a non-unital ring, to appear in JAA.https://hal.archives-ouvertes.fr/hal-02433480

[3] A. Alahmadi, A. Altassan, W. Basaffar, A. Bonnecaze, H. Shoaib, P. Solé, Quasi Type IV codes over a non-unital ring, submitted. https://hal.archives-ouvertes.fr/hal-02544399

[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] S. Dougherty, A. Leroy, Euclidean self-dual codes over non-commutative Frobenius rings, Applicable Algebra in Engineering, Communication and Computing, Volume 27 Issue 3, (2016) 185–203.

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

[7] S. Han, H. Lee, Y. Lee, Construction of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, Bull. Korean Math Soc. **49** (2012), 135–143.

[8] J-L. Kim, Y. Lee, Euclidean and hermitian self-dual MDS codes over large finite fields, J. Of Combinatorial Th. A **105** (2004) 79–95.

[9] J-L. Kim, Y. Lee, An efficient construction of self-dual codes, Bull. Korean Math Soc. **52** (2015), 915–923,

[10] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, P. Solé, Type IV self-dual codes over rings. IEEE Trans. Information Theory 45(7): 2345-2360 (1999).

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

[12] 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.

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

[14] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. 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).
[15] W.C. Hufman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge (2003).
[16] `http://magma.maths.usyd.edu.au/magma/`
[17] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland (1977).
[18] R. Raghavendran, A class of finite rings, Compositio Mathematica, vol. 21, pp. 195–229, 1969.
[19] P. Solé, *Codes over Rings*, World Scientific (2008).

E-mail address: analahmadi@kau.edu.sa
E-mail address: aakathiry@uqu.edu.sa
E-mail address: aaltassan@kau.edu.sa
E-mail address: Alexis.Bonnecaze@univ-amu.fr
E-mail address: hashoaib@kau.edu.sa
E-mail address: sole@enst.fr