



Quasi self-dual codes over non-unital rings of order six*

Adel Alahmadi¹ orcid.org/0000-0002-7758-3537

Amani Alkathiry² orcid.org/0000-0001-7920-859X

Alaa Altassan³ orcid.org/0000-0003-2729-7396

Widyan Basaffar⁴ orcid.org/0000-0003-1639-9186

Alexis Bonnetcaze⁵ orcid.org/0000-0002-9642-7222

Hatoon Shoaib⁶ orcid.org/0000-0002-1888-8154

Patrick Solé⁷ orcid.org/0000-0002-4078-8301

King Abdulaziz University, Dept. of Mathematics, Jeddah, Saudi Arabia.

¹ adelnife2@yahoo.com ; ³ aaltassan@kau.edu.sa ; ⁴ whbasaffar@kau.edu.sa ;

⁶ hashoaib@kau.edu.sa

² Umm Al-Qura University, Dept. of Mathematics, Makkah, Saudi Arabia

aalkathiry@uqu.edu.sa

Aix-Marseille Université, CNRS, Marseille, France.

⁵ alexis.bonnetcaze@univ-amu.fr ; ⁷ sole@enst.fr

Received: February 2020 | Accepted: June 2020

Abstract:

There exist two semi-local rings of order 6 without identity for the multiplication. We classify up to coordinate permutation self-orthogonal codes of length n and size $6^{n/2}$ over these rings (called here quasi self-dual codes or QSD) till the length $n=8$. To any such code is attached canonically a \mathbb{Z}_6 -code, which, when self-dual, produces an unimodular lattice by Construction A.

Keywords: Non-unital rings; Semi-local rings; Self-orthogonal codes; Unimodular lattices.

MSC (2020): 94B05, 16A10.

Cite this article as (IEEE citation style):

A. Alahmadi, A. Alkathiry, A. Altassan, W. Basaffar, A. Bonnetcaze, H. Shoaib, and P. Solé, "Quasi self-dual codes over non-unital rings of order six", *Proyecciones (Antofagasta, On line)*, vol. 39, no. 4, pp. 1083-1095, Aug. 2020, doi: 10.22199/issn.0717-6279-2020-04-0066.



Article copyright: © 2020 Adel Alahmadi, Amani Alkathiry, Alaa Altassan, Widyan Basaffar, Alexis Bonnetcaze, Hatoon Shoaib and Patrick Solé. This is an open access article distributed under the terms of the Creative Commons License, which permits unrestricted use and distribution provided the original author and source are credited.

*A preprint of this paper can be found at Archive ouverte HAL



1. Introduction

Codes over the ring of order six Z_6 have received some attention in the past due to their connection to euclidean lattices [11,13]. The main tool in this context is the Chinese Remainder Theorem (CRT) over the integers [8]. A classification technique for self-dual codes over this ring up to the permutation part of their monomial automorphism group was derived in [16], using the notion of double cosets in permutation groups. In a series of recent papers, the authors have studied self-orthogonal codes over non-unital rings of order 4 [1, 2, 4, 3]. This is a major innovation in the domain of codes over rings, where only unital rings were used as alphabets till then [18,19].

In the present paper, we combine these two strands of thought in the following way. We study self-orthogonal codes over two non-unital rings of order 6, denoted here by H_{32} and H_{23} . Both rings are semilocal with two maximal ideals of size two and three. There is a non multiplicative analogue of the CRT that allows to attach to any code over such a ring the ordered pair of a binary code and a ternary code. If the code is quasi self-dual (QSD) that is self-orthogonal of length n and size $6^{n/2}$, it can be shown that one of the two codes is self-dual and the other is a rate one-half code. Forgetting their multiplicative structure, we can regard the codes over either of these two non-unital rings as additive codes over Z_6 , or, equivalently Z_6 -linear codes. This simple observation allows us to use the Magma package for codes over rings [6] to compute weight distributions, and complete weight enumerators. We use the same classification methodology as that in [16] for codes over Z_6 . We are able to classify QSD codes over these two rings up to length $n = 8$.

The material is layed out in the following way. The next section collects the notations and notions needed for the rest of the paper. Section 3 is an exposition of the classification technique that we used. Section 4 contains some numerical data pertaining to that classification in modest length.

2. Background material

2.1. Codes over fields

Let p be a prime. Denote by $wt(x)$ the Hamming weight of $x \in F_p^n$. The dual of a linear code C over F_p is denoted by C^\perp and defined as

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

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, i.e. $C \subseteq C^\perp$. A code is **even** if all its codewords have even weights. All binary self-orthogonal codes are even, but not all binary even codes are self-orthogonal. Two codes over F_p are **permutation equivalent** if there is a permutation of coordinates that maps one to the other.

2.2. Rings

Let C_p be the cyclic additive abelian group of order p and $C_p(0)$ be the ring with additive group C_p and trivial multiplication. We know (see for example [9, Lemma 2]) that, up to isomorphism, there are exactly two rings of order p , namely Z_p and $C_p(0)$ and, if p and q are distinct primes, there are exactly four rings of order pq . These are Z_{pq} , $C_{pq}(0)$, $H_{pq} := Z_p + C_q(0)$, and $H_{qp} := C_p(0) + Z_q$. The symbol $+$ denotes the direct product of rings. Since the first two rings are well known, we consider in this paper the last two rings which are semi-local non-unital rings of order pq . In order to effectively construct codes, we restrict ourselves to the case $p = 3$ and $q = 2$. We denote these rings by

$$H_{32} := Z_3 + C_2(0) = \langle a, b \mid 2a = 0, 3b = 0, a^2 = 0, ab = 0 = ba, b^2 = b \rangle,$$

and

$$H_{23} := Z_2 + C_3(0) = \langle a, b \mid 2a = 0, 3b = 0, a^2 = a, ab = 0 = ba, b^2 = 0 \rangle.$$

We denote by c, d, e the remaining three elements, which we define as

$$\begin{aligned} c &= a + b \\ d &= 2b \\ e &= a + 2b. \end{aligned}$$

The addition tables of H_{32} and H_{23} are identical up to isomorphism and given by the following table

+	0	a	b	c	d	e
0	0	a	b	c	d	e
a	a	0	c	b	e	d
b	b	c	d	e	0	a
c	c	b	e	d	a	0
d	d	e	0	a	b	c
e	e	d	a	0	c	b

The multiplication tables for respectively H_{32} and H_{23} are as follows.

\times	0	a	b	c	d	e
0	0	0	0	0	0	0
a	0	0	0	0	0	0
b	0	0	b	b	d	d
c	0	0	b	b	d	d
d	0	0	d	d	b	b
e	0	0	d	d	b	b

and

\times	0	a	b	c	d	e
0	0	0	0	0	0	0
a	0	a	0	a	0	a
b	0	0	0	0	0	0
c	0	a	0	a	0	a
d	0	0	0	0	0	0
e	0	a	0	a	0	a

From these tables, we infer that these two rings are commutative, and without an identity element for the multiplication. They are semi-local with the two maximal ideals $J_a = \{0, a\}$, and $J_b = \{0, b, d\}$. Let $z \in \{23, 32\}$. The following decomposition

$$H_z = J_a \oplus J_b,$$

can be checked directly from the defining relations of c, d, e .

This alphabet decomposition induces a code decomposition as follows.

The code C over H_z can be written as a direct sum (in the sense of modules)

$$C = aC_a \oplus bC_b,$$

where C_a is a binary code and C_b is a ternary code.

Denote by $\alpha_a : H_z \rightarrow F_2$ the **map of reduction modulo J_a** , and denote by $\alpha_b : H_z \rightarrow F_3$ the **map of reduction modulo J_b** , where J_a , and J_b are viewed as additive groups. Thus $\alpha_a(a) = \alpha_b(b) = 0$, and, by convention we choose $\alpha_a(b) = \alpha_b(a) = 1$. These maps are extended in the natural way into maps from H_z^n to F_2^n (resp. from H_z^n to F_3^n).

Thus, with these notations, we see that $C_a = \alpha_b(C)$ and $C_b = \alpha_a(C)$.

Remark 1. These maps are additive morphisms but not ring morphisms. Still C_a (resp. C_b) is a vector space over F_2 (resp. F_3) because F_2 (resp. F_3) is a prime field and additive subgroups of F_2^n (resp. F_3^n) coincide with vector spaces over F_2 (resp. F_3).

2.3. Weight Enumerators

A **linear** H_z -code C of length n is an H_z -submodule of H_z^n . It can be described as the H_z -span of the rows of a **generator matrix**. Two H_z -codes are **permutation equivalent** if there is a permutation of coordinates that maps one to the other.

An **additive code** C of length n over Z_6 is an additive subgroup of Z_6^n . It is an Z_6 sub-module of Z_6^n . By the CRT over the integers we can attach two codes to C : a binary code C_2 , and a ternary code C_3 . We will write $C = CRT(C_2, C_3)$. Conversely, from every pair of a binary code B and a ternary code T of the same length a Z_6 -code C can be constructed by the formula $C = CRT(B, T)$.

If $C = aC_a + bC_b$ is an H_z -code, we can identify it with an additive Z_6 -code given by $C = CRT(C_a, C_b)$. We use the Magma notation

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

for the **weight distribution** of a senary code, where A_i is the number of codewords of Hamming weight i . The first index $i > 0$ for which A_i is nonzero is called the **Hamming distance** of the code. It is denoted by d_H . We will also require the **complete weight enumerator** in six variables cwe_C of a senary code C defined by

$$cwe_C(x_0, x_1, x_2, x_3, x_4, x_5) = \sum_{c \in C} \prod_{i=0}^5 x_i^{n_i(c)},$$

where $n_i(c)$ denotes for $i = 0, \dots, 5$, the number of coordinates j for which $c_j = i$. Thus, if n is the length of C , we have for all $c \in C$ the relation

$$\sum_{i=0}^5 n_i(c) = n.$$

We follow the notation of [15].

In view of the connection with lattices it makes sense to introduce **Euclidean weight enumerator** in one variable ewe_C of a senary code C

defined as

$$ewe_C(y) = \sum_{c \in C} y^{w_E(c)},$$

where the **Euclidean weight** of $x \in Z_6$ is defined as $w_E(x) = 0, 1, 4, 9$ if $x = 0, \pm 1, \pm 2, \pm 3$ respectively. This notation is extended to vectors in the obvious way. The following connection with the complete weight enumerator is immediate from the definitions.

$$ewe_C(y) = cwe(1, y, y^4, y^9, y^4, y).$$

The first exponent $i > 0$ for which the coefficient of y^i is nonzero is called the **Euclidean distance** of the code and is denoted by d_E .

For the next theorem we require some familiarity with lattices in the sense of the geometry of numbers [7, 11]. The following result is the so-called Construction A of lattices from codes over Z_m when $m = 6$. For a proof see [7] for $m = 2$, and [14] for $m = 4$.

Theorem 1. *If C is a Z_6 code of length n and size $6^{n/2}$, then the lattice $A(C)$ given by*

$$\sqrt{6}A(C) = \bigcup_{c \in C} (c + 6Z^n)$$

has determinant 1 and norm $\min(6, d_E/6)$. If, furthermore, the code C is self-dual, then $A(C)$ is unimodular.

Remark 2. *It is proved in [11, 13] that $C = CRT(B, T)$ is self-dual iff both B and T are self-dual. Thus the Z_6 -codes produced in this paper, in view of Lemma 1, and Lemma 2 are not always self-dual.*

2.4. Duality

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

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

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

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

A code C is said to be **self-orthogonal** if

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

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

Remark 3. Let the alphabet be H_{32} . The repetition code of length 2 is defined by $R_2 := \{00, aa, bb, cc, dd, ee\}$. We see that R_2 is self-orthogonal. Its dual contains also bc, cb, ed, de . (Note that the rows of c and b (resp. d and e) are the same). Thus R_2 is not self-dual.

A code of length n is said to be **quasi self-dual** (QSD) if it is self-orthogonal and of size 2^n .

Example: The code R_2 over either H_{32} or H_{23} is self-orthogonal of cardinality 6, hence it is QSD.

3. Classification

The following characterization result is easy but essential to understand the classification technique.

Lemma 1. Every QSD code C of length n over H_{23} is of the form $aC_a \oplus bC_b$ where

1. C_a is a self-dual binary code,
2. C_b is an $[n, n/2]$ ternary code.

In particular n must be even.

Proof. The code C is self-orthogonal iff C_a is a self-orthogonal binary code because of the following identity

$$(ax + by, ax' + by') = a(x, x'),$$

where x, x' (resp. y, y') are arbitrary binary (resp. ternary) vectors of length n . Since by the QSD hypothesis $C = |C_a||C_b| = 6^{n/2}$, we see that both C_a and C_b have dimension $n/2$. ■

Lemma 2. Every QSD code C of length n over H_{32} is of the form $aC_a \oplus bC_b$ where

1. C_b is a self-dual ternary code,
2. C_a is an $[n, n/2]$ binary code.

In particular n must be doubly even.

Proof. The proof of the first statement is analogous to the proof of Lemma 1, and is not written. To prove the second statement we use the

fact that ternary self-dual codes only exist in doubly even lengths [15]. ■

To classify QSD codes, we thus have to find all codes that are permutation equivalent to $aC_a + bC_b$ for a given pair (C_a, C_b) . This is a similar situation to the classification of self-dual codes over Z_{pq} in [16], and we follow the method there. Here SDR stands for System of Distinct Representatives.

Theorem 2. *Let (C_a, C_b) be a pair of codes as defined in Lemma 1 or Lemma 2, with respective permutation groups A and B . Then, the set*

$$S_{C_a, C_b} := \{aC_a + b\sigma(C_b) \mid \sigma \text{ runs over an SDR of } A \setminus S_n/B\}$$

forms a set of inequivalent codes. In particular $|S_{C_a, C_b}| = |A \setminus S_n/B|$.

The next corollaries are immediate.

Corollary 1. *Let L_a be the set of all inequivalent self-dual binary codes of length n . Let L_b be the set of all inequivalent $[n, n/2]$ ternary codes. Then, the set of all QSD codes of length n over H_{23} is, up to coordinate permutation, the disjoint union $\coprod_{\substack{C_a \in L_a \\ C_b \in L_b}} S_{C_a, C_b}$.*

Corollary 2. *Let L_b be the set of all inequivalent self-dual ternary codes of length n . Let L_a be the set of all inequivalent $[n, n/2]$ binary codes. Then, the set of all QSD codes of length n over H_{32} is, up to coordinate permutation, the disjoint union $\coprod_{\substack{C_a \in L_a \\ C_b \in L_b}} S_{C_a, C_b}$.*

To apply Corollary 1 effectively to classify QSD H_{23} -codes, we thus need to know two lists of codes, for a given length n .

1. An SDR of equivalence classes of self-dual $[n, n/2]$ binary codes,
2. an SDR of equivalence classes of ternary $[n, n/2]$ codes.

To apply Corollary 2 effectively to classify QSD H_{32} -codes, we thus need to know two lists of codes, for a given length n .

1. An SDR of equivalence classes of self-dual $[n, n/2]$ ternary codes,
2. an SDR of equivalence classes of binary $[n, n/2]$ codes.

The first type of list can be found in [12]. The second type of list can be established by using the method in [5,10].

The classification algorithm for QSD H_{23} -codes can be described as follows. Given an even length $n \geq 1$, do the following steps.

1. Write a list L_a of self-dual $[n, n/2]$ binary codes.
2. Write a list L_b of ternary $[n, n/2]$ codes.
3. For all pairs (C_a, C_b) in $L_a \times L_b$ do the following.
 1. Compute the permutation groups A and B of C_a and C_b respectively.
 2. Find a list $\sigma_1, \dots, \sigma_s$ of representatives of $A \backslash S_n / B$.
 3. For $i = 1$ to s output $aC_a + b\sigma_i(C_b)$.

A similar description holds for QSD H_{32} -codes.

1. Write a list L_b of self-dual $[n, n/2]$ ternary codes.
2. Write a list L_a of binary $[n, n/2]$ codes.
3. For all pairs (C_a, C_b) in $L_a \times L_b$ do the following.
 1. Compute the permutation groups A and B of C_a and C_b respectively.
 2. Find a list $\sigma_1, \dots, \sigma_s$ of representatives of $A \backslash S_n / B$.
 3. For $i = 1$ to s output $aC_a + b\sigma_i(C_b)$.

4. Numerical results

All the computations needed for this section were performed in Magma [6], except for the length 8 where we used Sage [17]. The Euclidean distance of the codes below is computed by inspection of the Euclidean weight enumerator, which is, most of the time, too long to be displayed. In the following sections Z_6 -codes are classified up to coordinate permutation, which is a weaker form of equivalence than that used in [12,13,16] where the permutation part of the monomial automorphism group of the codes is authorized. Thus, we find seventeen euclidean self-dual Z_6 -codes for $n = 8$, where only five are found in [12,16]. In general all the self-dual codes mentioned below are self-dual for the standard inner product over Z_6 like in [12,13,16].

4.1. The Ring H_{32}

The bijective correspondence $H_{32} \leftrightarrow Z_6$ is given informally by

$$0 = 0, e = 1, b = 2, a = 3, d = 4, c = 5.$$

4.1.1. Length 4 (13 codes)

The main properties are summarized in the following table.

# codes	4	6	1	2
d_H	1	1	2	2
d_E	6	3	6	3

There is a unique self-dual Z_6 -code of length 4. Its *ewe* is

$$y^{36} + 10y^{18} + 16y^{12} + 8y^6 + 1.$$

This is consistent with [16, Table 2]. Construction A yields the lattice Z^4 .

4.1.2. Length 8 (11 615 codes)

The Hamming distance distribution is summarized in the following table.

# codes	4516	6365	743
d_H	1	2	3

There are seventeen self-dual codes, eleven of Hamming weight 2 and Euclidean weight 6, and six of Hamming weight 3 and Euclidean weight 12. The six codes of Euclidean distance 12 yield the lattice E_8 by Theorem 1, the unique Type II lattice in dimension 8 [7].

yields the lattice Z^8 by construction A.

4.2. The Ring H_{23}

The bijective correspondence $H_{23} \leftrightarrow Z_6$ is given informally by

$$0 = 0, e = 1, b = 2, a = 3, d = 4, c = 5.$$

4.2.1. Length 2 (two codes)

We obtain two codes one with generator matrix $(1\ 3)$, $d_H = 1$, $d_E = 4$, and the other one with generator matrix $(1\ 1)$, $d_H = 2$, $d_E = 2$.

4.2.2. Length 4 (fourteen codes)

The metric properties are summarized in the following table.

# codes	2	3	3	5	1
d_H	1	1	2	2	2
d_E	2	4	2	4	6

The unique code with $d_E = 6$ is the self-dual code obtained in §4.1.1.

4.2.3. Length 6 (162 codes)

The metric properties are summarized in the following table.

# codes	16	34	25	56	31
d_H	1	1	2	2	2
d_E	2	4	2	4	6

4.2.4. Length 8 (10447 codes)

The metric properties are summarized in the following table.

# codes	209	1797	509	3690	11	3179	416	481	117	6	27	5
SD	N	N	N	N	Y	N	N	N	N	Y	N	N
d_H	1	1	2	2	2	2	2	3	3	3	4	4
d_E	2	4	2	4	6	6	8	4	8	12	4	8

Like for codes over H_{32} , there are 17 self-dual codes, 11 of Hamming weight 2 and Euclidean weight 6, and 6 of Hamming weight 3 and Euclidean weight 12. The 6 codes of Euclidean distance 12 yield the lattice E_8 by Theorem 1, the unique Type II lattice in dimension 8 [7].

Acknowledgement:

The authors are indebted to Prof. David Kohel for helping them with computations in the computer package Sage [17].

References

- [1] A. Alahmadi, A. Alkathiry, A. Altassan, A. Bonnecaze, H. Shoaib, and P. Solé, “The build-up construction of quasi self-dual codes over a non-unital ring”, *Journal of algebra and applications*, accepted preprint, 2020. [On line]. Available: <https://bit.ly/38HMJ8t>

- [2] A. Alahmadi, A. Alkathiry, A. Altassan, A. Bonnecaze, H. Shoaib, and P. Solé, "The build-up construction of quasi self-dual codes over a commutative non-unital ring", submitted preprint, 2020.
- [3] A. Alahmadi, A. Altassan, W. Basaffar, A. Bonnecaze, H. Shoaib, and P. Solé, "Quasi Type IV codes over a non-unital ring", submitted preprint, 2020. [On line]. Available: <https://bit.ly/3gozCvo>
- [4] A. Alahmadi, A. Altassan, W. Basaffar, A. Bonnecaze, H. Shoaib, and P. Solé, "Type IV codes over a non-unital ring", *Journal of algebra and applications*, accepted preprint, 2020. [On line]. Available: <https://bit.ly/3f5D8ue>
- [5] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann, *Error correcting-linear codes*. Berlin: Springer, 2006, doi: 10.1007/3-540-31703-1
- [6] Computational Algebra Group. and University of Sydney, "Magma computational algebra system", *Magma computer algebra*, 2010. [Online]. Available: <http://magma.maths.usyd.edu.au/magma/>
- [7] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 2nd ed. New York, NY: Springer, 2003, doi: 10.1007/978-1-4757-2249-9
- [8] S. T. Dougherty, M. Harada, and P. Solé, "Self-dual codes over rings and the chinese remainder theorem", *Hokkaido mathematical journal*, vol. 28, no. 2, pp. 253-283, 1999, doi: 10.14492/hokmj/1351001213
- [9] B. Fine, "Classification of Finite rings of order p^2 "; *Mathematics magazine*, vol. 66, no. 4, pp. 248-252, Oct. 1993, doi: 10.1080/0025570X.1993.11996133
- [10] H. Fripertinger, "Enumeration of isometry classes of linear (n, k) -codes over $GF(q)$, SYMMETRICA", *Bayreuther mathematische schriften*, vol. 49, pp. 215-223, 1999. [On line]. Available: <https://bit.ly/31QmYRC>
- [11] M. Harada and M. Kitazume, " Z_6 -code constructions of the Leech lattice and the Niemeier lattices", *European journal of combinatorics*, vol. 23, no. 5, pp. 573-581, Jul. 2002, doi: 10.1006/eujc.2002.0557

- [12] M. Harada and A. Munemasa, "Database of self-dual codes", *Tohoku University Graduate School of Information Science, Department of Mathematics/Center for Pure and Applied Mathematics*, 15-Nov-2007. [Online]. Available: <http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm>.
- [13] M. Harada and A. Munemasa, "On the classification of self-dual open image in new window \mathbb{Z}_k -codes", in *Cryptography and coding*, M. G. Parker, Ed. Berlin: Springer, 2009, pp. 78–90, doi: 10.1007/978-3-642-10868-6_6
- [14] W. C. Huffman and V. Pless, *Fundamentals of error correcting codes*, Cambridge: Cambridge University Press, 2003, doi: 10.1017/CBO9780511807077
- [15] F. J. MacWilliams and N. J. A. Sloane, Eds., *The theory of error-correcting codes*, North-Amsterdam: North-Holland, 1977, doi: 10.1016/s0924-6509(08)x7030-8
- [16] Y-H. Park, "The classification of self-dual modular codes", *Finite fields and their applications*, vol. 17, no. 5, pp. 442–460, Sep. 2011, doi: 10.1016/j.ffa.2011.02.010
- [17] SageMath Mathematical Software System, "Sage", 2007. [Online]. Available: <https://www.sagemath.org/>
- [18] M. Shi, A. Alahmadi, and P. Solé, *Codes and rings: theory and practice*, Cambridge, MA: Academic Press, 2017, doi: 10.1016/C2016-0-04429-7
- [19] P. Solé, Ed., *Codes over rings*, Singapore: World Scientific, 2008, doi: 10.1142/7140.