ON THE CLASSIFICATION OF SELF-DUAL $\mathbb{Z}_k$-CODES
II

MASAAKI HARADA AND AKIHIRO MUNEMASA

Abstract. In this short note, we report the classification of self-dual $\mathbb{Z}_k$-codes of length $n$ for $k \leq 24$ and $n \leq 9$.

1. Introduction

Let $\mathbb{Z}_k$ be the ring of integers modulo $k$, where $k$ is a positive integer greater than 1. A $\mathbb{Z}_k$-code $C$ of length $n$ is a $\mathbb{Z}_k$-submodule of $\mathbb{Z}_k^n$. A code $C$ is self-dual if $C = C^\perp$, where the dual code $C^\perp$ of $C$ is defined as $C^\perp = \{ x \in \mathbb{Z}_k^n \mid x \cdot y = 0 \text{ for all } y \in C \}$ under the standard inner product $x \cdot y$. Two $\mathbb{Z}_k$-codes $C$ and $C'$ are equivalent if there exists a monomial $(\pm 1,0)$-matrix $P$ with $C' = C \cdot P$, where $C \cdot P = \{ xP \mid x \in C \}$. A Type II $\mathbb{Z}_{2k}$-code was defined in [2] as a self-dual code with the property that all Euclidean weights are divisible by $4k$ (see [2] for the definition of Euclidean weights). It is known that a Type II $\mathbb{Z}_{2k}$-code of length $n$ exists if and only if $n$ is divisible by eight [2]. A self-dual code which is not Type II is called Type I.

As described in [24], self-dual codes are an important class of linear codes for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes. Much work has been done towards classifying self-dual $\mathbb{Z}_k$-codes for small $k$ and modest $n$ (see [24]). Let $n_{\max}(k)$ denote the maximum integer $n$ such that self-dual $\mathbb{Z}_k$-codes are classified up to length $n$. For $k = 2, 3, \ldots, 10$, we list in Table 1 our present state of knowledge about $n_{\max}(k)$. We also list the reference for the classification of self-dual $\mathbb{Z}_k$-codes of length $n_{\max}(k)$.

| $k$ | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 |
|-----|----|----|----|----|----|----|----|----|----|
| $n_{\max}(k)$ | 40 | 24 | 19 | 16 | 12 | 12 | 12 | 12 | 10 |
| Reference | [5] | [11] | [12] | [10] | [12] | [12] | [12] | [12] | [12] |

Date: September 24, 2015.
2010 Mathematics Subject Classification. 94B05.
Key words and phrases. self-dual code, frame, unimodular lattice.
A classification method of self-dual \( \mathbb{Z}_k \)-codes based on a classification of \( k \)-frames of unimodular lattices was given by the authors and Venkov \[14\]. Then, in \[12\], using this method, self-dual \( \mathbb{Z}_k \)-codes were classified for \( k = 4, 6, 8, 9, 10 \) (see Table 1). Using the same method, in this short note, we complete the classification of self-dual codes \( \mathbb{Z}_k \)-codes of length \( n \) for \( k \leq 24 \) and \( n \leq 9 \). All computer calculations in this short note were done by Magma \[4\].

2. Classification of self-dual \( \mathbb{Z}_k \)-codes

2.1. Method for classifications. A classification method of self-dual \( \mathbb{Z}_k \)-codes based on a classification of \( k \)-frames of unimodular lattices was given by the authors and Venkov \[14\]. We describe it briefly here (see \[12\] and \[14\] for undefined terms and details).

A set \( \{f_1, \ldots, f_n\} \) of \( n \) vectors \( f_1, \ldots, f_n \) in an \( n \)-dimensional unimodular lattice \( L \) with \( (f_i, f_j) = k \delta_{ij} \) is called a \( k \)-frame of \( L \), where \( (x, y) \) denotes the standard inner product of \( \mathbb{R}^n \), and \( \delta_{ij} \) is the Kronecker delta. The following construction of lattices from codes is called Construction A. If \( C \) is a self-dual \( \mathbb{Z}_k \)-code of length \( n \) then

\[
A_k(C) = \left\{ \left( x_1, \ldots, x_n \right) \in \mathbb{Z}^n \mid (x_1 \mod k, \ldots, x_n \mod k) \in C \right\}
\]

is an \( n \)-dimensional unimodular lattice. Moreover, \( C \) is Type II if and only if \( A_k(C) \) is even. Let \( F = \{f_1, \ldots, f_n\} \) be a \( k \)-frame of \( L \). Consider the mapping

\[
\pi_F : \frac{1}{\sqrt{k}} \bigoplus_{i=1}^n \mathbb{Z} f_i \to \mathbb{Z}_k^n
\]

\[
\pi_F(x) = ((x, f_i) \mod k)_{1 \leq i \leq n}.
\]

Then \( \text{Ker} \pi_F = \bigoplus_{i=1}^n \mathbb{Z} f_i \subset L \), so the code \( C = \pi_F(L) \) satisfies \( \pi_F^{-1}(C) = L \). This implies \( A_k(C) \simeq L \), and every code \( C \) with \( A_k(C) \simeq L \) is obtained as \( \pi_F(L) \) for some \( k \)-frame \( F \) of \( L \), where \( L \simeq L' \) means that \( L \) and \( L' \) are isomorphic lattices. Moreover, every Type I (resp. Type II) \( \mathbb{Z}_k \)-code of length \( n \) can be obtained from a certain \( k \)-frame in some \( n \)-dimensional odd (resp. even) unimodular lattice.

Let \( L \) be an \( n \)-dimensional unimodular lattice, and let \( F = \{f_1, \ldots, f_n\} \), \( F' = \{f'_1, \ldots, f'_n\} \) be \( k \)-frames of \( L \). Then the self-dual codes \( \pi_F(L) \) and \( \pi_{F'}(L) \) are equivalent if and only if there exists an automorphism \( P \) of \( L \) such that \( \{\pm f_1, \ldots, \pm f_n\} \cdot P = \{\pm f'_1, \ldots, \pm f'_n\} \) \[14\]. This implies that the classification of codes \( C \) satisfying \( A_k(C) \simeq L \) reduces to finding a set of representatives of \( k \)-frames in \( L \) up to the action of the automorphism group of \( L \).
2.2. Results. Here, we report the classification of self-dual $\mathbb{Z}_k$-codes of length $n$ for $k \leq 24$ and $n \leq 9$. Our classification method of self-dual $\mathbb{Z}_k$-codes of length $n$ requires a classification of $n$-dimensional unimodular lattices. For $n \leq 7$, any $n$-dimensional unimodular lattice is isomorphic to $\mathbb{Z}^n$. Up to isomorphism, there are two 8-dimensional unimodular lattices, one of which is the even unimodular lattice denoted by $E_8$ and the other is $\mathbb{Z}^8$. Also, up to isomorphism, there are two 9-dimensional unimodular lattices, $\mathbb{Z}^9$ and $E_8 \oplus \mathbb{Z}$ (see [7, p. 49]).

In Table 2, we list the number of inequivalent self-dual $\mathbb{Z}_k$-codes $C$ with $A_k(C) \cong L$ for $k \in \{2, 3, \ldots, 24\}$ and $L \in \{\mathbb{Z}^i \mid i = 1, 2, \ldots, 9\} \cup \{E_8, E_8 \oplus \mathbb{Z}\}$. Note that all self-dual $\mathbb{Z}_k$-codes $C$ with $A_k(C) \cong E_8$ are Type II. A classification of self-dual $\mathbb{Z}_k$-codes of lengths $n \leq 9$ was known for some $k$. In this case, we list the references in the last columns of the table. Generator matrices can be obtained electronically from [13]. All the zero entries in Table 2 are explained as follows. For $k \in \{3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24\}$, if there is a self-dual $\mathbb{Z}_k$-code of length $n$, then $n$ is divisible by four (see [9, Corollary 2.2]). For $k \in \{2, 5, 8, 10, 13, 17, 18, 20\}$, if there is a self-dual $\mathbb{Z}_k$-code of length $n$, then $n$ is even (see [8, Theorem 4.2], [9, Corollary 2.2]). If $k$ is a square, then there is a self-dual $\mathbb{Z}_k$-code for every length (see [6], [8]). If a self-dual $\mathbb{Z}_k$-code is Type II, then $k$ is even.

2.3. Remark on length 4. A classification of self-dual $\mathbb{Z}_k$-codes of length 4 was given in [3] for $k = 19, 23$, and in [21] for prime $k \leq 100$. We note that the definition of equivalence employed in [21] is different from our definition. Let $N_4(k)$ denote the number of inequivalent self-dual $\mathbb{Z}_k$-codes of length 4. We give in Table 3 the numbers $N_4(k)$ for integers $k$ with $25 \leq k \leq 200$. We remark that the classification can be extended to $k = 1000$. However, in order to save space, we do not list the result.

Let $s_1, s_2, \ldots, s_u$ be positive integers. An orthogonal design of order $n$ and of type $(s_1, s_2, \ldots, s_u)$, denoted $OD(n; s_1, s_2, \ldots, s_u)$, on the commuting variables $x_1, x_2, \ldots, x_u$ is an $n \times n$ matrix $A$ with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ such that

$$AA^T = \left( \sum_{i=1}^{u} s_i x_i^2 \right) I_n,$$
Table 2. Classification of self-dual \( \mathbb{Z}_k \)-codes of lengths \( n \leq 9 \)

| \( k \) | \( \mathbb{Z} \) | \( \mathbb{Z}^2 \) | \( \mathbb{Z}^3 \) | \( \mathbb{Z}^4 \) | \( \mathbb{Z}^5 \) | \( \mathbb{Z}^6 \) | \( \mathbb{Z}^7 \) | \( \mathbb{Z}^8 \) | \( E_8 \) | \( \mathbb{Z}^9 \) | \( E_8 \oplus \mathbb{Z} \) | Reference |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 2   | 0   | 1   | 0   | 0   | 1   | 0   | 1   | 0   | 0   |       |       | 22    |
| 3   | 0   | 0   | 0   | 1   | 0   | 0   | 1   | 0   | 0   |       |       | 19    |
| 4   | 1   | 1   | 1   | 2   | 2   | 3   | 4   | 7   | 4   | 7   | 4   |       | 5, 10 |
| 5   | 0   | 1   | 0   | 1   | 0   | 2   | 0   | 3   | 0   | 0   | 0   |       | 18    |
| 6   | 0   | 0   | 0   | 1   | 0   | 0   | 0   | 3   | 2   | 0   | 0   |       | 9, 12, 17, 20 |
| 7   | 0   | 0   | 0   | 1   | 0   | 0   | 0   | 4   | 0   | 0   | 0   |       | 23    |
| 8   | 0   | 1   | 0   | 1   | 0   | 3   | 0   | 20  | 9   | 0   | 0   |       | 8, 12  |
| 9   | 1   | 1   | 2   | 3   | 3   | 6   | 9   | 16  | 0   | 28  | 7   |       | 11, 12 |
| 10  | 0   | 1   | 0   | 2   | 0   | 5   | 0   | 16  | 11  | 0   | 0   |       | 12    |
| 11  | 0   | 0   | 0   | 1   | 0   | 0   | 0   | 8   | 0   | 0   | 0   |       | 3     |
| 12  | 0   | 0   | 0   | 2   | 0   | 0   | 0   | 73  | 22  | 0   | 0   |       | 3     |
| 13  | 0   | 1   | 0   | 2   | 0   | 5   | 0   | 21  | 0   | 0   | 0   |       | 3     |
| 14  | 0   | 0   | 0   | 1   | 0   | 0   | 0   | 27  | 18  | 0   | 0   |       | 3     |
| 15  | 0   | 0   | 0   | 2   | 0   | 0   | 0   | 51  | 0   | 0   | 0   |       | 3     |
| 16  | 1   | 1   | 2   | 3   | 7   | 23  | 295 | 63  | 697 | 141 |       |       |
| 17  | 0   | 1   | 0   | 2   | 0   | 6   | 0   | 47  | 0   | 0   | 0   |       | 3     |
| 18  | 0   | 1   | 0   | 4   | 0   | 12  | 0   | 178 | 69  | 0   | 0   |       |       |
| 19  | 0   | 0   | 0   | 2   | 0   | 0   | 0   | 57  | 0   | 0   | 0   |       | 3     |
| 20  | 0   | 1   | 0   | 2   | 0   | 17  | 0   | 725 | 176 | 0   | 0   |       |       |
| 21  | 0   | 0   | 0   | 3   | 0   | 0   | 0   | 208 | 0   | 0   | 0   |       |       |
| 22  | 0   | 0   | 0   | 2   | 0   | 0   | 0   | 166 | 75  | 0   | 0   |       |       |
| 23  | 0   | 0   | 0   | 1   | 0   | 0   | 0   | 120 | 0   | 0   | 0   |       |       |
| 24  | 0   | 0   | 0   | 1   | 0   | 0   | 0   | 3690| 456 | 0   | 0   |       |       |

where \( A^T \) denotes the transpose of \( A \) and \( I_n \) is the identity matrix of order \( n \). The following matrix

\[
M(x_1, x_2, x_3, x_4) = \begin{pmatrix}
x_1 & x_2 & x_3 & x_4 \\
-x_2 & x_1 & -x_4 & x_3 \\
-x_3 & x_4 & x_1 & -x_2 \\
-x_4 & -x_3 & x_2 & x_1
\end{pmatrix}
\]

is well known as an \( OD(4; 1, 1, 1, 1) \). From Lagrange’s theorem on sums of squares, for each positive integer \( k \), the matrix \( M \) gives a \( k \)-frame of \( \mathbb{Z}^4 \). However, there are \( k \)-frames which are not obtained in this way. Indeed, if \( k \) is a square, then a \( k \)-frame can be obtained from a \( k \)-frame of \( \mathbb{Z}^3 \), for example,

\[
\mathcal{F}_9 = \{(1, 2, 2, 0), (-2, -1, 2, 0), (-2, 2, -1, 0), (0, 0, 0, 3)\}\]
is a 9-frame. Although the following matrix

\[
N(x_1, x_2, x_3, x_4) = \begin{pmatrix}
  x_1 & x_2 & x_3 & x_4 \\
-x_2 & x_1 & -x_4 & x_3 \\
x_4 & -x_3 & x_1 & x_2 \\
x_3 & x_4 & -x_2 & x_1
\end{pmatrix}
\]

is not an orthogonal design, if \(x_1x_3 + x_1x_4 - x_2x_3 + x_2x_4 = 0\) then

\[
N(x_1, x_2, x_3, x_4)N(x_1, x_2, x_3, x_4)^T = \left(\sum_{i=1}^{4} x_i^2\right)I_4.
\]
A 15-frame $F_{15}$ is obtained from $N(3, 1, 2, -1)$. We also found the following 21-frame $F_{21}$:

$$F_{21} = \{(4, 1, 0, 2), (0, -4, 1, 2), (1, 0, 4, -2), (-2, 2, 2, 3)\}.$$ 

Note that $N_4(9) = 3$, $N_4(15) = 2$ and $N_4(21) = 3$. The two other 9-frames are obtained from $M(3, 0, 0, 0)$ and $M(2, 2, 1, 0)$. The other 15-frame is obtained from $M(3, 2, 1, 1)$. The two other 21-frames are obtained from $M(0, 1, 2, 4)$ and $M(2, 2, 2, 3)$.

2.4. Remark on length 8. Let $N_{8,I}(2k)$ (resp. $N_{8,II}(2k)$) be the number of inequivalent Type I (resp. Type II) $\mathbb{Z}_{2k}$-codes of length 8. From Table 2 we see $N_{8,I}(2) = N_{8,II}(2)$ and $N_{8,I}(2k) > N_{8,II}(2k)$ ($k = 2, 3, \ldots, 12$). We conjecture that $N_{8,I}(2k) > N_{8,II}(2k)$ for all integers $k$ with $k \geq 2$.

Acknowledgment. This work is supported by JSPS KAKENHI Grant Number 26610032.

References

[1] J.M.P. Balmaceda, R.A.L. Betty and F.R. Nemenzo, Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$, Discrete Math. 308 (2008), 2984–3002.
[2] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices, and invariant rings, IEEE Trans. Inform. Theory 45 (1999), 1194–1205.
[3] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada and C. Koukouvinos, On self-dual codes over some prime fields, Discrete Math. 262 (2003), 37–58.
[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997), 235–265.
[5] I. Bouyukliev, M. Dzhumalieva-Stoeva and V. Monev, Classification of binary self-dual codes of length 40, IEEE Trans. Inform. Theory, (to appear).
[6] J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, J. Combin. Theory Ser. A 62 (1993), 30–45.
[7] J.H. Conway and N.J.A. Sloane, Sphere Packing, Lattices and Groups (3rd ed.). Springer-Verlag, New York, 1999.
[8] S.T. Dougherty, T.A. Gulliver and J. Wong, Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$, Des. Codes Cryptogr. 41 (2006), 235–249.
[9] S.T. Dougherty, M. Harada and P. Solé, Self-dual codes over rings and the Chinese remainder theorem, Hokkaido Math. J. 28 (1999), 253–283.
[10] 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.
[11] M. Harada and A. Munemasa, A complete classification of ternary self-dual codes of length 24, J. Combin. Theory Ser. A 116 (2009), 1063–1072.
[12] M. Harada and A. Munemasa, On the classification of self-dual $\mathbb{Z}_k$-codes, Lecture Notes in Comput. Sci. 5921 (2009), 78–90.
[13] M. Harada and A. Munemasa, Database of Self-Dual Codes, http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm
M. Harada, A. Munemasa and B. Venkov, Classification of ternary extremal self-dual codes of length 28, *Math. Comput.* **78** (2009), 1787–1796.

M. Harada and P.R.J. Östergård, Self-dual and maximal self-orthogonal codes over $F_7$, *Discrete Math.* **256** (2002), 471–477.

M. Harada and P.R.J. Östergård, On the classification of self-dual codes over $F_5$, *Graphs Combin.* **19** (2003), 203–214.

M. Kitazume and T. Ooi, Classification of type II $Z_6$-codes of length 8, *AKCE Int. J. Graphs Comb.* **1** (2004), 35–40.

J.S. Leon, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(5)$, *J. Combin. Theory Ser. A* **32** (1982), 178–194.

C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$, *SIAM J. Appl. Math.* **31** (1976), 649–666.

Y.H. Park, Modular independence and generator matrices for codes over $Z_m$, *Des. Codes Cryptogr.* **50** (2009), 147–162.

Y.H. Park, The classification of self-dual modular codes, *Finite Fields Appl.* **17** (2011), 442–460.

V. Pless, A classification of self-orthogonal codes over $GF(2)$, *Discrete Math.* **3** (1972), 209–246.

V.S. Pless and V.D. Tonchev, Self-dual codes over $GF(7)$, *IEEE Trans. Inform. Theory* **33** (1987), 723–727.

E. Rains and N.J.A. Sloane, Self-Dual Codes: Handbook of Coding Theory. In: V.S. Pless and W.C. Huffman (eds.), Elsevier, Amsterdam 1998, pp. 177–294.

(Corresponding author) Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan

*E-mail address: mharada@m.tohoku.ac.jp*

Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan

*E-mail address: munemasa@math.is.tohoku.ac.jp*