Interdisciplinary Information Sciences Vol. 22, No. 1 (2016) 81–85

ISSN 1340-9050 print/1347-6157 online
DOI 10.4036/iis.2015.R.01

On the Classification of Self-Dual $\mathbb{Z}_k$-Codes II

Masaaki HARADA[1,*] and Akihiro MUNEMASA[2]

[1]*Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan*
[2]*Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan*

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

KEYWORDS: self-dual code, frame, unimodular lattice

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 $k = 2, 3, \dots, 10$, 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 $n_{\max}(k)$.

Table 1. Known classification of self-dual $\mathbb{Z}_k$-codes.

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]	[16]	[12]	[15]	[12]	[12]	[12]

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 $\{f_1, \dots, f_n\}$ of n vectors $f_1, \dots, f_n$ in an n-dimensional unimodular lattice L with $(f_i, f_j) = k\delta_{i,j}$ is called a *k-frame* of L, where (x, y) denotes the standard inner product of $\mathbb{R}^n$, and $\delta_{i,j}$ 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

Received June 10, 2015; Accepted September 24, 2015; J-STAGE Advance published October 28, 2015
2010 Mathematics Subject Classification: Primary 94B05.
*Corresponding author. E-mail: mharada@m.tohoku.ac.jp

$$A_k(C) = \frac{1}{\sqrt{k}}\{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid (x_1 \bmod k, \dots, x_n \bmod k) \in C\}$$

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

$$\pi_{\mathcal{F}} : \frac{1}{k}\bigoplus_{i=1}^{n} \mathbb{Z}f_i \to \mathbb{Z}_k^n$$

$$\pi_{\mathcal{F}}(x) = ((x, f_i) \bmod k)_{1 \le i \le n}.$$

Then $\operatorname{Ker} \pi_{\mathcal{F}} = \bigoplus_{i=1}^{n} \mathbb{Z}f_i \subset L$, so the code $C = \pi_{\mathcal{F}}(L)$ satisfies $\pi_{\mathcal{F}}^{-1}(C) = L$. This implies $A_k(C) \simeq L$, and every code C with $A_k(C) \simeq L$ is obtained as $\pi_{\mathcal{F}}(L)$ for some k-frame $\mathcal{F}$ 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 $\mathcal{F} = \{f_1, \dots, f_n\}$, $\mathcal{F}' = \{f_1', \dots, f_n'\}$ be k-frames of L. Then the self-dual codes $\pi_{\mathcal{F}}(L)$ and $\pi_{\mathcal{F}'}(L)$ are equivalent if and only if there exists an automorphism P of L such that $\{\pm f_1, \dots, \pm f_n\} \cdot P = \{\pm f_1', \dots, \pm f_n'\}$ [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 $k \le 24$ and $n \le 9$. Our classification method of self-dual $\mathbb{Z}_k$-codes of length n requires a classification of n-dimensional unimodular lattices. For $n \le 7$, 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 $A_k(C) \simeq L$ for $k \in \{2, 3, \dots, 24\}$ and $L \in \{\mathbb{Z}^i \mid i = 1, 2, \dots, 9\} \cup \{E_8, E_8 \oplus \mathbb{Z}\}$. Note that all self-dual $\mathbb{Z}_k$-codes C with $A_k(C) \simeq E_8$ are Type II. A classification of self-dual $\mathbb{Z}_k$-codes of lengths $n \le 9$ 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.

Table 2. Classification of self-dual $\mathbb{Z}_k$-codes of lengths $n \le 9$.

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	1	0	1	0	1	1	0	0	[22]
3	0	0	0	1	0	0	0	1	0	0	0	[19]
4	1	1	1	2	2	3	4	7	4	7	4	[6, 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	[1, 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	
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	
15	0	0	0	2	0	0	0	51	0	0	0	
16	1	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	
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	

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.

Table 3. Classification of self-dual $\mathbb{Z}_k$-codes of length 4 ($25 \leq k \leq 200$).

k	$N_4(k)$	k	$N_4(k)$	k	$N_4(k)$	k	$N_4(k)$	k	$N_4(k)$	k	$N_4(k)$
25	5	55	5	85	10	115	9	145	14	175	20
26	3	56	1	86	6	116	5	146	11	176	2
27	4	57	7	87	7	117	15	147	18	177	14
28	3	58	5	88	2	118	8	148	8	178	13
29	2	59	3	89	5	119	8	149	7	179	8
30	5	60	5	90	19	120	5	150	30	180	19
31	2	61	4	91	9	121	9	151	7	181	9
32	1	62	4	92	3	122	9	152	3	182	19
33	4	63	8	93	8	123	11	153	20	183	15
34	4	64	2	94	6	124	6	154	15	184	3
35	3	65	8	95	8	125	13	155	12	185	17
36	6	66	9	96	1	126	20	156	14	186	20
37	3	67	4	97	6	127	6	157	8	187	14
38	3	68	4	98	10	128	1	158	10	188	6
39	5	69	5	99	13	129	12	159	12	189	26
40	2	70	9	100	12	130	21	160	2	190	23
41	3	71	3	101	5	131	6	161	10	191	8
42	5	72	4	102	14	132	9	162	27	192	2
43	3	73	5	103	5	133	11	163	8	193	10
44	2	74	6	104	3	134	9	164	7	194	14
45	7	75	11	105	16	135	22	165	25	195	31
46	3	76	5	106	8	136	4	166	11	196	16
47	2	77	5	107	5	137	7	167	7	197	9
48	2	78	10	108	9	138	15	168	5	198	33
49	6	79	4	109	6	139	7	169	15	199	9
50	10	80	2	110	14	140	9	170	26	200	10
51	6	81	12	111	10	141	10	171	21		
52	5	82	7	112	3	142	9	172	8		
53	3	83	4	113	6	143	10	173	8		
54	8	84	9	114	14	144	6	174	20		

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

$$AA^T = \left(\sum_{i=1}^{u} s_i x_i^2 \right) I_n,$$

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 $\mathcal{F}_{15}$ is obtained from $N(3,1,2,-1)$. We also found the following 21-frame $\mathcal{F}_{21}$:

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

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 $k \geq 2$.

Acknowledgments

This work is supported by JSPS KAKENHI Grant Number 26610032.

REFERENCES

[1] Balmaceda, J. M. P., Betty, R. A. L., and Nemenzo, F. R., "Mass formula for self-dual codes over $\mathbf{Z}_{p^2}$," *Discrete Math.*, **308**: 2984–3002 (2008).
[2] Bannai, E., Dougherty, S. T., Harada, M., and Oura, M., "Type II codes, even unimodular lattices, and invariant rings," *IEEE Trans. Inform. Theory*, **45**: 1194–1205 (1999).
[3] Betsumiya, K., Georgiou, S., Gulliver, T. A., Harada, M., and Koukouvinos, C., "On self-dual codes over some prime fields," *Discrete Math.*, **262**: 37–58 (2003).
[4] Bosma, W., Cannon, J., and Playoust, C., "The Magma algebra system I: The user language," *J. Symbolic Comput.*, **24**: 235–265 (1997).
[5] Bouyukliev, I., Dzhumalieva-Stoeva, M., and Monev, V., "Classification of binary self-dual codes of length 40," *IEEE Trans. Inform. Theory*, **61**: 4253–4258 (2015).
[6] Conway, J. H., and Sloane, N. J. A., "Self-dual codes over the integers modulo 4," *J. Combin. Theory Ser. A*, **62**: 30–45 (1993).
[7] Conway, J. H., and Sloane, N. J. A., Sphere Packing, Lattices and Groups (3rd ed.), Springer-Verlag (1999).
[8] Dougherty, S. T., Gulliver, T. A., and Wong, J., "Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$," *Des. Codes Cryptogr.*, **41**: 235–249 (2006).
[9] Dougherty, S. T., Harada, M., and Solé, P., "Self-dual codes over rings and the Chinese remainder theorem," *Hokkaido Math. J.*, **28**: 253–283 (1999).
[10] Gaborit, P., "Mass formulas for self-dual codes over Z_4 and $F_q + uF_q$ rings," *IEEE Trans. Inform. Theory*, **42**: 1222–1228 (1996).
[11] Harada, M., and Munemasa, A., "A complete classification of ternary self-dual codes of length 24," *J. Combin. Theory Ser. A*, **116**: 1063–1072 (2009).
[12] Harada, M., and Munemasa, A., "On the classification of self-dual $\mathbb{Z}_k$-codes," *Lecture Notes in Comput. Sci.*, **5921**: 78–90 (2009).
[13] Harada, M., and Munemasa, A., *Database of Self-Dual Codes*, http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm
[14] Harada, M., Munemasa, A., and Venkov, B., "Classification of ternary extremal self-dual codes of length 28," *Math. Comput.*, **78**: 1787–1796 (2009).
[15] Harada, M., and Östergård, P. R. J., "Self-dual and maximal self-orthogonal codes over $\mathbb{F}_7$," *Discrete Math.*, **256**: 471–477 (2002).
[16] Harada, M., and Östergård, P. R. J., "On the classification of self-dual codes over $\mathbb{F}_5$," *Graphs Combin.*, **19**: 203–214 (2003).
[17] Kitazume, M., and Ooi, T., "Classification of type II Z_6-codes of length 8," *AKCE Int. J. Graphs Comb.*, **1**: 35–40 (2004).
[18] Leon, J. S., Pless, V., and Sloane, N. J. A., "Self-dual codes over GF(5)," *J. Combin. Theory Ser. A*, **32**: 178–194 (1982).
[19] Mallows, C. L., Pless, V., and Sloane, N. J. A., "Self-dual codes over $GF(3)$," *SIAM J. Appl. Math.*, **31**: 649–666 (1976).
[20] Park, Y. H., "Modular independence and generator matrices for codes over $\mathbb{Z}_m$," *Des. Codes Cryptogr.*, **50**: 147–162 (2009).
[21] Park, Y. H., "The classification of self-dual modular codes," *Finite Fields Appl.*, **17**: 442–460 (2011).
[22] Pless, V., "A classification of self-orthogonal codes over GF(2)," *Discrete Math.*, **3**: 209–246 (1972).

[23] Pless, V. S., and Tonchev, V. D., "Self-dual codes over *GF*(7)," *IEEE Trans. Inform. Theory*, **33**: 723–727 (1987).
[24] Rains, E., and Sloane, N. J. A., Self-Dual Codes: Handbook of Coding Theory. In: V. S. Pless and W. C. Huffman (eds.), Elsevier, Amsterdam 1998, pp. 177–294.