Serdica J. Computing **9** (2015), No 1, 83–92

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

CLASSIFICATION OF MAXIMAL OPTICAL ORTHOGONAL CODES OF WEIGHT 3 AND SMALL LENGTHS*

Tsonka Baicheva, Svetlana Topalova

Dedicated to the memory of the late professor Stefan Dodunekov on the occasion of his 70th anniversary

Abstract. We classify up to multiplier equivalence maximal $(v, 3, 1)$ optical orthogonal codes (OOCs) with $v \leq 61$ and maximal $(v, 3, 2, 1)$ OOCs with $v \leq 99$.

There is a one-to-one correspondence between maximal $(v, 3, 1)$ OOCs, maximal cyclic binary constant weight codes of weight 3 and minimum distance 4, $(v, 3; \lfloor (v-1)/6 \rfloor)$ difference packings, and maximal $(v, 3, 1)$ binary cyclically permutable constant weight codes. Therefore the classification of $(v, 3, 1)$ OOCs holds for them too. Some of the classified $(v, 3, 1)$ OOCs are perfect and they are equivalent to cyclic Steiner triple systems of order v and $(v, 3, 1)$ cyclic difference families.

ACM Computing Classification System (1998): D.1.0, G.2.1.

Key words: optical orthogonal codes, cyclic Steiner triple systems, binary cyclically permutable constant weight codes, code division multiple access system.

*This work was partially supported by the Bulgarian National Science Fund under Contract No. I01/0003. Part of the results were announced at the Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory, Pomorie, Bulgaria (2012).

1. Introduction. Optical code-division multiple access (OCDMA) systems attract much attention as they have several benefits such as asynchronous transmission, flexibility in network design, accommodation of burst traffic, etc. A main problem connected with the use of OCDMA systems is the search for powerful code structures that allow a large number of users to communicate simultaneously with a low error probability. Among the most famous codes considered to date are optical orthogonal codes (OOCs). They also have applications in mobile radio, frequency-hopping spread-spectrum communications, radar, sonar signal design, constructing protocol-sequence sets for the M-active-out-of T users collision channel without feedback, etc.

Since the introductory paper by Chung, Salehi and Wei [8] the optical orthogonal codes construction problem has been intensively studied in many papers, e.g., [1, 2, 5, 6, 7, 9, 14, 16]. The maximal size of a $(v, 3, 1)$ OOC is known for each v [4]. Constructions of $(v, 3, 2, 1)$ OOCs are known for many values of v [15]. We do not know, however, classification results about OOCs of weight 3. In our paper we classify maximal $(v, 3, 1)$ and $(v, 3, 2, 1)$ OOCs with small v.

2. Basic definitions and relations to other combinatorial objects. For the basic concepts and notations concerning the classified in this paper combinatorial objects we follow [5], [10] and [16]. We denote by Z_v the ring of integers modulo v and by $\oplus$ and $\odot$ addition and multiplication in it.

Definition 1. *A $(v, k, \lambda_a, \lambda_c)$ optical orthogonal code (OOC) $\mathcal{C}$ is a collection of $\{0, 1\}$ sequences of length v and Hamming weight k such that:*

$$\sum_{i=0}^{v-1} x(i)x(i \oplus j) \le \lambda_a, \ 1 \le j \le v-1 \tag{1}$$

$$\sum_{i=0}^{v-1} x(i)y(i \oplus j) \le \lambda_c, \ 0 \le j \le v-1 \tag{2}$$

for all pairs of distinct sequences $x, y \in \mathcal{C}$.

A $(v, k, \lambda_a, \lambda_c)$ OOC can also be defined in the following way:

Definition 2. *A $(v, k, \lambda_a, \lambda_c)$ OOC $\mathcal{C}$ is a collection $\mathcal{C} = \{C_1, \ldots, C_s\}$ of k-subsets (codeword-sets) of Z_v, such that any two distinct translates of a codeword-set share at most λ_a elements, and any two translates of two distinct codeword-sets share at most λ_c elements:*

$$|C_i \cap (C_i \oplus t)| \le \lambda_a, \quad 1 \le i \le s, \quad 1 \le t \le v-1 \tag{3}$$

$$|C_i \cap (C_j \oplus t)| \leq \lambda_c, \quad 1 \leq i < j \leq s, \quad 0 \leq t \leq v-1 \tag{4}$$

The second definition is more convenient for our construction method. When we further talk of codewords, we will actually mean codeword-sets.

Condition (1) or (3) is called the *auto-correlation property* and (2) or (4) the *cross-correlation property.*

A $(v, k, \lambda_a, \lambda_c)$ OOC with $\lambda_a = \lambda_c = \lambda$ is also denoted by (v, k, λ) OOC.

The *size* of $\mathcal{C}$ is the number s of its codewords.

Consider a codeword $C = \{c_1, c_2, \ldots, c_k\}$. Denote by $\triangle' C$ the multiset of the values of the differences $c_i - c_j$, $i \neq j$, $i, j = 1, 2, \ldots, k$ and by $\triangle C$ its corresponding set. The *type* of C is the number of elements of $\triangle C$, i.e., the number of different values of its differences. The auto-correlation property means that at most λ_a differences are the same. In particular all the differences of a codeword of a $(v, k, 1)$ OOC are different. For $\lambda_c = 1$ the cross-correlation property means that $\Delta C_1 \bigcap \Delta C_2 = \emptyset$ for two codewords C_1 and C_2.

A $(v, k, \lambda_a, 1)$ OOC is *perfect* if $\left| \bigcup_{i=1}^{s} \Delta C_i \right| = v - 1$, that is if all nonzero differences are covered. If $\lambda_a = \lambda_c = 1$ the size of a perfect $(v, k, 1)$ OOC is exactly $(v-1)/k(k-1)$.

Example. Codewords of a perfect $(13, 3, 1)$ OOC

$$\begin{array}{c} \{1100100000000\} \text{ or } \{0, 1, 4\} \\ \{1010000010000\} \text{ or } \{0, 2, 8\} \end{array}$$

$$\begin{array}{c} \triangle C_1 = \{1, 3, 4, 9, 10, 12\} \\ \triangle C_2 = \{2, 5, 6, 7, 8, 11\} \end{array}$$

We proceed with the definitions of combinatorial structures which are closely related to OOCs.

Definition 3. *A binary cyclically permutable constant weight (CPCW) (v, k, λ) code is a code of minimum Hamming distance $2(k - \lambda)$ whose codewords have weight k, length v, are cyclically distinct and of full cyclic order.*

A (v, k, λ) OOC is equivalent to a (v, k, λ) cyclically permutable constant weight (CPCW) code.

Definition 4. *An (n, w, d) binary constant weight code (CWC) of length n, weight w and minimum distance d is a collection of binary vectors of length n*

(codewords), which have exactly w nonzero positions and the Hamming distance between any two codewords is at least d.

A CWC is cyclic if the cyclic shift of each codeword is a codeword too. A cyclic CWC corresponds to an $(n, w, wd/2)$ OOC.

Definition 5. *Let B be a subset of an additive group G. We denote by ΔB the list of all possible differences $b - b'$ with (b, b') an ordered pair of distinct elements of B. More generally, if $F = B_1, B_2, \ldots, B_n$ is a collection of subsets of G, then the list of differences from F, denoted by ΔF, is the multiset obtained by joining $\Delta B_1, \ldots, \Delta B_n$. F is said to be a $(v, k, 1)$ difference family (DF) if G has order v, every B_i is of size $k \geq 3$, and ΔF covers every non-zero element of G exactly once. If further, $G = Z_v$, then this difference family is said to be cyclic (CDF).*

A $(v, k, 1)$ CDF can be obtained from any perfect $(v, k, 1)$ OOC.

Definition 6. *Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of points, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite collection of k-element subsets of V, called blocks. $D = (V, \mathcal{B})$ is a design with parameters t-(v,k,λ) if any t-subset of V is contained in exactly λ blocks of $\mathcal{B}$. A t-(v,k,λ) design is cyclic if it has an automorphism α permuting its points in one cycle, and it is strictly cyclic if each block orbit under this automorphism is of length v (no short orbits).*

A 2-$(v, 3, 1)$ design is also called a Steiner triple system and denoted by $STS(v)$. Steiner triple systems are a particularly interesting class of designs with many different applications in Coding Theory (see for instance [17] for their connection with perfect codes or [13] for their connection with conflict-avoiding codes).

A perfect $(v, k, 1)$ OOC corresponds to a cyclic 2-$(v, k, 1)$ design and to a cyclic $(v, k, 1)$ difference family. In particular perfect $(v, 3, 1)$ OOCs correspond to cyclic $STS(v)$.

Among the OOCs with given parameters those which have more codewords are more interesting from application point of view and research efforts are directed there.

Let $\Phi(v, k, \lambda_a, \lambda_c)$ be the largest possible size of a $(v, k, \lambda_a, \lambda_c)$ OOC. OOCs of size $\Phi(v, k, \lambda_a, \lambda_c)$ are called *maximal*.

For codes with $\lambda_a = \lambda_c = 1$ we know the following upper bound [8]

$$\Phi(v, k, 1) \leq \left\lfloor \frac{v-1}{k(k-1)} \right\rfloor.$$

OOCs which reach this bound are called *optimal*.

It has been proved in [4] that optimal $(v, 3, 1)$ OOCs exist iff $v \neq 6t + 2$ for $t \equiv 2$ or $3 \pmod 4$. For $v \equiv 6t+2$ and $t \equiv 2$ or $3 \pmod 4$ there exist $(v, 3, 1)$ OOCs of size $\left\lfloor \frac{v-1}{k(k-1)} \right\rfloor - 1$.

Since we want to classify all OOCs with given parameters, we need to define an equivalence relation on them.

Two $(v, k, \lambda_a, \lambda_c)$ OOCs C and C' are *isomorphic* if there exists a permutation of Z_v, which maps the collection of translates of each codeword of C to the collection of translates of a codeword of C'.

The automorphisms of the cyclic group of order v map each circulant matrix of order v to a circulant matrix of order v. That is why *multiplier equivalence* is defined for cyclic combinatorial objects.

Two $(v, k, \lambda_a, \lambda_c)$ OOCs are *multiplier equivalent* if they can be obtained from one another by an automorphism of Z_v and replacement of codewords by some of their translates.

There can exist OOCs which are isomorphic, but multiplier inequivalent.

3. Motivation and main results. Classification results about OOCs can be used in direct practical applications as well as in constructions of OOCs with other parameters [7, 8, 9]. Sometimes for the construction of new infinite families, OOCs with certain parameters and some additional properties are needed and classification results can also be very useful. In this sense classification results for OOCs of small lengths might contribute to future investigations on codes with other higher parameters.

We do not know classification results for $(v, 3, 1)$ OOCs, but there are classification results for cyclic Steiner triple systems of order v with $v \leq 57$ [11]. Among them the designs with $v = 19, 25, 31, 37, 43, 49,$ and 55 are strictly cyclic and equivalent to $(v, 3, 1)$ OOCs, so the number of maximal OOCs for these values of v is known. The number of maximal perfect $(61, 3, 1)$ OOCs and cyclic $STS(61)$ is known from the classification of $(61, 3, 1)$ CDFs in [3].

In the present paper we classify up to multiplier equivalence maximal $(v, 3, 1)$ and $(v, 3, 2, 1)$ OOCs. This way we also repeat the existing classification results for $(61, 3, 1)$ CDFs and for cyclic $STS(v)$ with $v = 19, 25, 31, 37, 43, 49,$ and 55.

4. Classification method. Computer search for constructing OOCs has been used by other authors before ([6, 8]). Our algorithm is essentially different from those considered in [6] and [8] since our aim is not only to find one

optimal OOC for each v, but to make a classification too. We classify the $(v, 3, 1)$ and $(v, 3, 2, 1)$ OOCs up to multiplier equivalence applying back-track search with minimality test on the partial solutions [12, section 7.1.2]. We use a modification of the algorithm used in [2].

All possibilities for codewords are first arranged with respect to a lexicographic order defined on them. We assume that $c_1 < c_2 < c_3$ for each codeword $C = \{c_1, c_2, c_3\}$. Let us define a lexicographic order on the codewords implying that: $C' = \{c'_1, c'_2, c'_3\}$ is lexicographically smaller than $C'' = \{c''_1, c''_2, c''_3\}$ if the type of C' is smaller than that of C'', or if the types of the two codewords are the same and $c'_i = c''_i$ for $i < j$ and $c'_j < c''_j$ for some j.

Without loss of generality we assume that each codeword is lexicographically smaller than the codewords of its translates. This means that $c_1 = 0$ and when we say that C_1 is mapped to C_2 by the permutation φ, we mean that C_2 is the smallest translate of $\varphi(C_1)$.

Classification algorithm

Step 1. We construct an array L - that contains all sets of 3 elements of Z_v which satisfy the auto-correlation property and are smaller than all their translates. They are found in lexicographic order.

• Let $\varphi_0, \varphi_1, \ldots, \varphi_{m-1}$ be the automorphisms of Z_v, where φ_0 is the identity. These automorphisms are applied to each constructed set.

• If some of them maps it to a smaller set, the current set is not added.

• If the current set is added to the array, the $m - 1$ sets to which it is mapped by $\varphi_1, \varphi_2, \ldots, \varphi_{m-1}$ are added right after it.

Step 2. After the construction of the array, back-track search is applied to choose the codewords of the OOC among all these possibilities for them.

• At each stage of the back-track search we add a codeword to the current partial solution choosing it from the array L. In order to make the classification feasible we speed up the algorithm by performing a minimality test and a type test.

Minimality test: we check if the current partial solution can be mapped to a lexicographically smaller one by the automorphisms of Z_v. If it can, an equivalent partial solution has already been considered, and we look for the next possibility for the current codeword.

The ordering of all the possible codewords described above allows repeated sets in the array L, but makes the minimality test of the partial solutions very fast.

Type test: Suppose that r codewords of the code have already been found. Let T be the type of the r-th codeword, and let d be the number of distinct

differences covered by the r codewords. We only look for codes with a definite number s of codewords. The type of the remaining codewords (of the array we choose them from) is at least as big as that of the r-th chosen one. That is why $d + (s - r)T \leq v - 1$. If this does not hold, the next possibility for the $(r - 1)$-st codeword is considered.

5. Classification Results. We present in Table 1 the results of the classification up to multiplier equivalence of maximal (v,3,1) OOCs with $13 \leq v \leq 61$. The value of v is followed by p if the codes are perfect. The number of codewords of the maximal OOCs is denoted by s. We do not include in the classifications the codes with only one codeword and $v < 13$.

Table 1. Multiplier inequivalent maximal (v,3,1) OOCs

v	s	OOCs	v	s	OOCs	v	s	OOCs	v	s	OOCs
13p	2	1	25p	4	12	37p	6	820	49p	8	157340
14	1	3	26	4	36	38	5	35120	50	8	550528
15	2	5	27	4	128	39	6	15678	51	8	3642484
16	2	3	28	4	164	40	6	19794	52	8	4204688
17	2	5	29	4	400	41	6	68784	53	8	21282112
18	2	12	30	4	1376	42	6	185376	54	8	54243072
19p	3	4	31p	5	80	43p	7	9508	55p	9	3027456
20	2	23	32	5	242	44	6	621888	56	9	8660480
21	3	25	33	5	1212	45	7	257886	57	9	68638238
22	3	20	34	5	1360	46	7	231616	58	9	74974976
23	3	40	35	5	6762	47	7	1137664	59	9	446472448
24	3	107	36	5	12784	48	7	2712394	60	9	1450970880
									61p	10	42373196

The classification of maximal (v, 3, 2, 1) OOCs with $10 \leq v \leq 99$ is presented in Table 2 where for each v we give the size s of the maximal OOCs, the number of multiplier inequivalent maximal OOCs, and the number of the perfect ones among them. As in Table 1 we do not include codes with $s = 1$.

All computer results are obtained by our own C++ programs. For the number of perfect OOCs we obtain exactly the number of the related cyclic $STS(v)$ with $v \leq 57$, presented in [11] and of the $(61, 3, 1)$ CDFs obtained in [3].

Files with the OOCs we construct can be downloaded from `http://www.moi.math.bas.bg/~tsonka`. The classification presented above shows that for some lengths there are thousands of nonisomorphic codes. All of them are available online to everybody who is interested and further investigations of their properties are possible. The classified codes can be of use both directly in relevant applications, and as parts of constructions of new infinite families.

Table 2. Multiplier inequivalent maximal (v,3,2,1) OOCs

v	s	OOCs	perfect	v	s	OOCs	perfect	v	s	OOCs	perfect
10	2	1	0	40	8	3618	1896	70	17	1	0
11	2	1	0	41	10	1	1	71	17	4	3
12	2	5	0	42	10	2	1	72	15	8378752	5930240
13	3	1	1	43	10	2	2	73	17	205	160
14	3	1	0	44	9	5452	2464	74	18	1	0
15	3	2	0	45	10	40	32	75	18	8	0
16	3	6	2	46	11	1	0	76	16	18781060	12069564
17	4	1	1	47	11	2	1	77	18	192	156
18	4	2	1	48	10	5136	3416	78	19	2	1
19	4	3	2	49	11	70	44	79	19	6	5
20	4	15	8	50	12	1	0	80	17	10985704	8577912
21	4	14	4	51	12	4	0	81	18	258201	140240
22	5	1	0	52	11	7452	4956	82	20	1	0
23	5	2	1	53	13	1	1	83	20	5	4
24	5	8	8	54	13	2	1	84	18	17634048	13703296
25	6	2	2	55	13	2	0	85	21	16	16
26	6	1	0	56	12	1344	1344	86	21	1	0
27	5	90	16	57	13	79	56	87	21	2	0
28	6	14	10	58	14	1	0	88	19	1263616	1263616
29	7	1	1	59	14	3	2	89	21	305	250
30	7	2	1	60	13	7168	6176	90	22	2	1
31	7	2	2	61	15	1	1	91	22	8	4
32	7	4	4	62	15	1	0	92	20	7221248	6407168
33	7	21	8	63	14	2160	1152	93	22	86	80
34	8	1	0	64	13	6666368	3236352	94	23	1	0
35	8	4	2	65	16	10	10	95	23	6	4
36	8	8	8	66	16	2	1	96	21	245760	245760
37	9	1	1	67	16	5	4	97	24	1	1
38	9	1	0	68	15	1600	1600	98	24	1	0
39	9	2	0	69	16	102	72	99	23	4930	3930

REFERENCES

[1] Abel R. J. R., M. Buratti. Some progress on (v, 4, 1) difference families and optical orthogonal codes. *J. Combin. Theory*, Ser. A, **106** (2004), 59–75.

[2] Baicheva T., S. Topalova. Classification of optimal (v, 4, 1) binary cyclically permutable constant weight codes and cyclic S(2, 4, v) designs with $v \leq 76$. *Problems of Information Transmission*, **47** (2011), No 3, 224–231.

[3] Baicheva T., S. Topalova. Classification results for (v, k, 1) cyclic difference families with small parameters. In: Proceedings of the ITHEA Math-

ematics of Distances and Applications (Eds M. Deza, M. Petitjean, K. Markov), Sofia, 2012, 24–30.

[4] Brickell E. F., V. K. Wei. Optical orthogonal codes and cyclic block designs. *Congr. Numer.*, **58** (1987), 175–192.

[5] Buratti M., K. Momihara, A. Pasotti. New results on optimal (v, 4, 2, 1) optical orthogonal codes. *Designs Codes and Cryptography*, **58** (2011), 89–109.

[6] Chu W., C. J. Colbourn. Optimal (n, 4, 2)-OOC of small order. *Discrete Math.*, **279** (2004), 163–172.

[7] Chu W., S. W. Golomb. A new recursive construction for optical orthogonal codes. *IEEE Trans. Inform. Theory*, **49** (2003), No 11, 3072–3076.

[8] Chung F. R. K., J. A. Salehi, V. K. Wei. Optical orthogonal codes: Design, analysis, and applications. *IEEE Trans. Inform. Theory* **35** (1989), 595–604.

[9] Chunk H., P. V. Kumar. Optical orthogonal codes – new bounds and an optimal construction. *IEEE Trans. Inform. Theory*, **90** (1990), 866–873.

[10] Colbourn C. J., J. Dinitz, Eds. Handbook of Combinatorial Designs. 2nd Ed, CRC Press, Boca Raton, FL., 2007.

[11] Colbourn C. J., A. Rosa. Triple systems. Oxford University Press, Oxford, 1999.

[12] Kaski P., P. R. J. Östergård. Classification algorithms for codes and designs. Springer, Berlin, 2006.

[13] Levenstein V. I. Conflict-avoiding codes and cyclic triple systems. *Problems of Information Transmission*, **43** (2007), 199–212.

[14] Martirosyan S., A. J. Han Vinck. A construction for optical orthogonal codes with correlation 1. *IEICE Trans. Fundamentals*, **E85-A** (2002), 269–272.

[15] Momihara K. Existence and construction of difference families and their applications to combinatorial codes in multiple-access communications. Graduate School of Information Science, Nagoya University, Japan, 2009.

[16] Moreno O., Z. Zhang, P. V. Kumar, V. A. Zinoviev. New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. on Inform. Theory*, **41** (1995), 448–455.

[17] Solov'eva F. I. Designs and Perfect Codes, General Theory of Information Transfer and Combinatorics. *Lecture Notes in Computer Science*, **4123** (2006), 1104–1105.

Tsonka Baicheva
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: tsonka@math.bas.bg

Svetlana Topalova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: svetlana@math.bas.bg

Received August 12, 2015
Final Accepted October 10, 2015