Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 41–46*

Optimal $(v, 3, 1)$ binary cyclically permutable constant weight codes with small v

Tsonka Baicheva, Svetlana Topalova tsonka,svetlana@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Bulgaria

Abstract. We classify up to multiplier equivalence optimal $(v, 3, 1)$ binary cyclically permutable constant weight (CPCW) codes with $v \leq 61$. There is a one-to-one correspondence between optimal $(v, 3, 1)$ CPCW codes, optimal cyclic binary constant weight codes with weight 3 and minimal distance 4, $(v, 3; \lfloor (v-1)/6 \rfloor)$ difference packings, and optimal $(v, 3, 1)$ optical orthogonal codes. Therefore the classification of CPCW codes holds for them too.
Some of the classified $(v, 3, 1)$ CPCW codes are perfect and they are equivalent to cyclic Steiner triple systems of order v ($STS(v)$) and $(v, 3, 1)$ cyclic difference families. This way we obtain a classification of cyclic $STS(61)$ and $(61, 3, 1)$ cyclic difference families which is new.

1 Introduction

An (n, d, w) code is a binary code of length n and minimum Hamming distance d, whose codewords have constant weight w. These codes are called *constant weight* and have been extensively studied (see for instance [4]). One of the most interesting classes of these codes are the constant weight cyclically permutable codes. Cyclically permutable codes were first defined by Gilbert [10]. In a *cyclically permutable code* (CPC) all codewords are cyclically distinct and have full cyclic order. Such codes are not only suitable for error-correction but also for synchronization and multiple access, mobile radio, frequence-hopping spread spectrum communications, radar and sonar signal design. A *cyclically permutable constant weight* (CPCW) code is a code which is both constant weight and CPC. These codes were studied in [3], [12], [13], and can be used for the construction of protocol sequences for a multiuser collision channel without feedback. They are also called optical orthogonal codes in connection with applications for optical code-division multiple-access channels.

2 Basic definitions

For the basic concepts and notations concerning the classified combinatorial objects we follow [5], [8] and [12]. We denote by Z_v the ring of integers modulo v and by $\oplus$ and $\odot$ addition and multiplication in it.

A (v, k, λ) binary cyclically permutable constant weight (CPCW) code $\mathcal{C}$ is a collection of $\{0, 1\}$ sequences of length v and Hamming weight k such that:

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

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

for all pairs of distinct sequences $x, y \in \mathcal{C}$. The same definition holds for a (v, k, λ) optical orthogonal code.

A (v, k, λ) binary cyclically permutable constant weight (CPCW) code can also be defined as a collection $\mathcal{C} = \{C_1, \ldots, C_s\}$ of k-subsets (*codeword-sets* or *blocks*) of Z_v, such that any two distinct translates of a block share at most λ elements, and any two translates of two distinct blocks also share at most λ elements:

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

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

Condition (1) or (3) is called the auto-correlation property and (2) or (4) the cross-correlation property. The size of $\mathcal{C}$ is the number s of its blocks.

Consider a block $C = \{c_1, c_2, \ldots, c_k\}$. Denote by $\triangle' C$ the multiset of the values of the differences $c_i - c_j$, $i \neq j$, $i, j = 1, 2, \ldots, k$. The auto-correlation property means that at most λ differences are the same. In particular all the differences of a block of a $(v, k, 1)$ CPCW code are different. For $\lambda = 1$ the cross-correlation property means that $\Delta C_1 \bigcap \Delta C_2 = \emptyset$ for two blocks C_1 and C_2.

A (v, k, λ) difference family is a set $\mathcal{C} = \{C_1, \ldots, C_s\}$ where $C_i = \{c_{i_1}, c_{i_2}, \ldots, c_{i_k}\}$ are k-element subsets of Z_v, such that each nonzero element of Z_v is obtained exactly λ times as a difference $c_{i_j} - c_{i_l}$ for $1 \leq i \leq s$ and $1 \leq j \neq l \leq k$

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 2-(v,3,1) design is also called a Steiner triple system and denoted by $STS(v)$.

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).

Two (v, k, λ) CPCW codes C and C' are *isomorphic* if there exists a permutation of Z_v, which maps the collection of translates of each block of C to the collection of translates of a block 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, λ) CPCW codes are *multiplier equivalent* if they can be obtained from one another by an automorphism of Z_v and replacement of blocks by some of their translates.

Two cyclic 2-(v, k, λ) designs (partial designs) D and D' are *multiplier equivalent* if there exists an automorphism of Z_v which maps each block of D to a block of D'.

Two CPCW codes (cyclic designs) can be isomorphic, but multiplier inequivalent.

Let $\Phi(v, k, \lambda)$ be the largest possible size of a (v, k, λ) CPCW code. For codes with $\lambda = 1$ we have the following upper bound [7]

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

CPCW codes which reach this bound are called *optimal*. If the size is exactly $(v-1)/k(k-1)$, the $(v, k, 1)$ CPCW code is called *perfect* and corresponds to a cyclic 2-$(v, k, 1)$ design and to a cyclic $(v, k, 1)$ difference family.

3 Motivation and main results

There exists an optimal $(v, 3, 1)$ CPCW code if and only if $v \not\equiv 14$ or 20 $(mod\ 24)$ [1], [7]. Except for direct applications, $(v, 3, 1)$ CPCW codes can also be used in constructions of CPCW codes with other parameters [7]. Sometimes for the construction of new infinite families, CPCW codes with certain parameters and some additional properties are needed and classification results can be very useful. In this sense classification results for CPCW codes of small lengths might contribute to future investigations on codes with other higher parameters.

We do not know classification results for $(v, 3, 1)$ CPCW codes, but there are classification results for cyclic Steiner triple systems of order v $(STS(v))$ with $v \leq 57$ [9], namely for $v = 19, 21, 25, 27, 31, 33, 37, 39, 43, 45, 49, 51, 55,$ and 57. Among them the designs with $v = 19, 25, 31, 37, 43, 49,$ and 55 are strictly cyclic and equivalent to $(v, 3, 1)$ CPCW codes, while the designs with $v = 121, 27, 33, 39, 45, 51,$ and 57 have one short orbit. Steiner triple systems are a particularly interesting class of designs with many different applications in Coding Theory (see for instance [14] for their connection with perfect codes).

In the present paper we classify up to multiplier equivalence optimal $(v, 3, 1)$ CPCW codes with $v \leq 61$. To the existing classification results for cyclic $STS(v)$ we add $v = 61$. We also repeat the classification of cyclic $STS(v)$ for $v \leq 57$.

4 Algorithm

Our algorithm is essentially different from those considered in [6], and [7] since our aim is not only to find one optimal CPCW code for each v, but to make a

classification too. We use a slight modification of the algorithm used in [2]. To classify optimal CPCW codes and cyclic designs up to multiplier equivalence we first order all the possibilities for blocks with respect to both lexicographic order and the action of the automorphisms of the cyclic group of order v, and then apply back-track search with minimality test on the partial solutions [11, section 7.1.2]. In this case the minimality test rejects the current partial solution if some of the automorphisms of Z_v can map it to a lexicographically smaller solution (that has already been constructed).

5 Classification results

We present in Table 1 the results of the classification up to multiplier equivalence of optimal (v,3,1) CPCW codes with $13 \leq v \leq 61$. The value of v is followed by p if the codes are perfect. As usual the number of blocks is denoted by s. If an optimal code does not exist for this length, a result about the codes of maximal size is presented and the value of v is followed by m. Files with all $(v, 3, 1)$ CPCW codes we construct can be obtained from the authors upon request.

All computer results are obtained by our own C++ programs. For the number of perfect CPCW codes we obtain exactly the number of the related cyclic $STS(v)$ with $v \leq 57$, presented in [9]. From the classification of perfect $(61, 3, 1)$ CPCW codes we obtain 42373196 inequivalent cyclic $STS(61)$ which is a new result.

In a similar way we construct cyclic $STS(v)$ with one short orbit (of length $v/3$). The base block of the short orbit is $\{0, v/3, 2v/3\}$. We repeat the classification of cyclic $STS(v)$ designs with one short orbit for $v = 15, 21, 27, 33, 39, 45$, 51, and 57. The number of multiplier inequivalent designs we obtain is the same as the number of nonisomorphic ones in [9].

The above presented complete classification of optimal $(v, 3, 1)$ CPCW codes with $v \leq 61$ shows that for some lengths there are thousands of nonisomorphic codes. All codes are available online to everybody who is interested and further investigations of their properties are possible. We believe that the classified codes will be of use both directly and as ingredients in constructions of new infinite families.

References

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

[2] T. Baicheva and 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(3)**, 224–231, 2011.

Table 1: Multiplier inequivalent optimal (v,3,1) CPCW codes

v	s	# (v,3,1) CPCW codes
13p	2	1
14m	1	3
15	2	5
16	2	3
17	2	5
18	2	12
19p	3	4
20m	2	23
21	3	25
22	3	20
23	3	40
24	3	107
25p	4	12
26	4	36
27	4	128
28	4	164
29	4	400
30	4	1376
31p	5	80
32	5	242
33	5	1212
34	5	1360
35	5	6762
36	5	12784
37p	6	820

v	s	# (v,3,1) CPCW codes
38m	5	35120
39	6	15678
40	6	19794
41	6	68784
42	6	185376
43p	7	9508
44m	6	621888
45	7	257886
46	7	231616
47	7	1137664
48	7	2712394
49p	8	157340
50	8	550528
51	8	3642484
52	8	4204688
53	8	21282112
54	8	54243072
55p	9	3027456
56	9	8660480
57	9	68638238
58	9	74974976
59	9	446472448
60	9	$\geq$ 455000000
61p	10	42373196

[3] S. Bitan, and T. Etzion, Constructions for optimal constant weight cyclically permutable codes and difference families, *IEEE Trans. on Inform. Theory*, **41**, 77–87, 1995.

[4] A. E. Brouwer, J. B. Shearer, N J. A. Sloane and W. D. Smith, A new table of constant weight codes, *IEEE Trans. Inform. Theory*, **36**, 1334–1380, 1990.

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

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

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

[8] Ch. Colbourn, and J. Dinitz, Eds, *Handbook of Combinatorial Designs*, 2nd edition (Discrete mathematics and its applications, ser. ed. K. Rosen), CRC Press, Boca Raton, FL., 2007.

[9] C. J. Colbourn, and A. Rosa, *Triple systems*, Oxford University Press, Oxford, 1999.

[10] E. N. Gilbert, Cyclically permutable error-correcting codes, *IEEE Trans. Inform. Theory,* **9**, 175–180, 1963.

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

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

[13] Q. A. Nguyen, L. Györfi and J. L. Massey, Constructions of binary constant-weight cyclic codes and cyclically permutable codes, *IEEE Trans. Inform. Theory,* **38**, 940–949, 1992.

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