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

Tsonka Baicheva Svetlana Topalova

Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

June, 2012
Pomorie, Bulgaria

Introduction I

Constant weight (n, d, w) binary code (CW)

- Length n
- Minimum Hamming distance d
- All codewords have constant weight w

Cyclically permutable code (CPC)

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

- All codewords are cyclically distinct
- Have full cyclic order

Cyclically permutable constant weight (CPCW) code is both CW and CPC.

CPCW codes are also called optical orthogonal codes

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.

Applications of CPCW codes

- Optical code-division multiple-access communication systems
- Mobile radio
- Frequence-hopping spread spectrum communications
- Constructing protocol-sequence sets for the M-active-out-of-T users collision channel without feedback
- Radar and sonar signal design
- Public key algorithm for optical communication based on lattice cryptography

Introduction IV

CPCW codes were studied in

- 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.
- 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.
- 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.
- 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.

Basic definitions I

- Z_v the ring of integers modulo v
- $\oplus$ addition in Z_v

Definition

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

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

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

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

Basic definitions II

Definition

A (v, k, λ) binary CPCW code is a collection $\mathcal{C} = \{C_1, \ldots, C_s\}$ of k-subsets (*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:

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

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

- (1) or (3) is called the auto-correlation property
- (2) or (4) is called the cross-correlation property

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

Basic definitions III

$C = \{c_1, c_2, \ldots, c_k\}$ is a block

$\triangle' C$ is the multiset of the values of the differences

$$c_i - c_j,\ i \neq j,\ i, j = 1,\ 2,\ \ldots,\ k$$

$\triangle C$ is the underlying set of $\triangle' C$

- *Autocorrelation property* $\Rightarrow$ at most λ differences are the same
- *Cross-correlation property* $\Rightarrow$ if $\lambda = 1$ then $\Delta C_1 \bigcap \Delta C_2 = \emptyset$ for two blocks C_1 and C_2 of the $(v, k, 1)$ CPCW

Basic definitions IV

Multiplier equivalence is defined for cyclic combinatorial objects.

Definition

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.

Bound for the size of a $(v, k, 1)$ CPCW I

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

- $(v, k, 1)$ CPCWs for which $s = \left\lfloor \frac{(v-1)}{k(k-1)} \right\rfloor$ are called optimal
- If $s = \dfrac{(v-1)}{k(k-1)}$ the $(v, k, 1)$ CPCW is called perfect

A perfect $(v, k, 1)$ CPCW corresponds to

- a cyclic 2-(v,k,1) design
- a cyclic (v,k,1) difference family

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

Motivation and known results about $(v, 3, 1)$ CPCW codes I

CPCW codes can be used

- For direct applications
- In recursive constructions of CPCW codes of higher parameters

  !!! Classification results for CPCW codes of small lengths might contribute to future investigations on codes with other higher parameters.

- For the construction of other types of combinatorial structures

Motivation and known results about $(v, 3, 1)$ CPCW codes II

An optimal $(v, 3, 1)$ CPCW code exists for all v except for

$$v = 6t + 2 \text{ and } t \equiv 2 \text{ or } 3 \pmod 4.$$

E.F. Brickell, V.K. Wei, Optical orthogonal codes and cyclic block designs, *Congr. Numer.*, vol. 58, 1987, pp. 175-192.

Motivation and known results about $(v, 3, 1)$ CPCW codes III

We do not know classification results for $(v, 3, 1)$ CPCW codes.

There are classification results for cyclic Steiner triple systems of order v ($STS(v)$) with $v \leq 57$.

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

- The STSs with $v = 13, 19, 25, 31, 37, 43, 49$, and 55 are strictly cyclic and equivalent to $(v, 3, 1)$ CPCW codes.
- The STSs with $v = 15, 21, 27, 33, 39, 45, 51$, and 57 have one short orbit.

Our result

We classify up to multiplier equivalence optimal $(v, 3, 1)$ CPCW codes with $v \leq 61$.

This way we also

- repeat the classification of cyclic $STS(v)$ for $v \leq 57$;
- classify cyclic $STS(v)$ with $v = 61$.

The construction is implemented by back-track search with minimality test on the partial solutions

Classification algorithm I

- We order all the possibilities for the blocks with respect to
  - lexicographic order: for each block $C = \{c_1, c_2, c_3\}$: $c_1 < c_2 < c_3$.
  - the action of the automorphisms of the cyclic group of order v.
- If we replace a block $C \in \mathcal{C}$ with a translate $C + t \in \mathcal{C}$, we obtain an equivalent CPCW code.

Without loss of generality we assume that each block of the optimal $(v, 3, 1)$ CPCW code is lexicographically smaller than its translates.

- This means that $c_1 = 0$

Classification algorithm II

We create an array L of all 3-element subsets of Z_v which might become blocks of a CPCW code with these parameters.

- We construct the blocks of L in lexicographic order
- To each block we apply the automorphisms $\varphi_i, i = 1, 2, ...m - 1$ of Z_v and if some of them maps it to a smaller one, we do not add this block since it is already somewhere in the array
- If we add the current block C to the list, we also add after it the $m - 1$ blocks to which C is mapped by $\varphi_i, i = 1, 2, ...m - 1$.

This way we obtain the array L whose elements are all the possible blocks.

Classification algorithm III

Blocks with suitable autocorrelation

$\mathbf{L_0}$
$L_1 = \varphi_1 L_0$
$L_2 = \varphi_2 L_0$
$\vdots$
$L_{m-1} = \varphi_{m-1} L_0$
$\mathbf{L_m}$
$L_{m+1} = \varphi_1 L_m$
$L_{m+2} = \varphi_2 L_m$
$\vdots$
$L_{2m-1} = \varphi_{m-1} L_m$
$\vdots$
$\mathbf{L_{im}}$
$L_{im+1} = \varphi_1 L_m$
$L_{im+2} = \varphi_2 L_m$
$\vdots$
$L_{(i+1)m-1} = \varphi_{m-1} L_m$

Classification algorithm IV

We construct the CPCW code choosing its blocks among the elements of L by back-track search until we find the s blocks

$$L_{x_1}, L_{x_2}, \dots, L_{x_s}$$

In order to reject some parts of the search tree we use:

- Minimality test. If the current partial solution can be transformed to a lexicographicaly smaller one by some of the automorphisms of Z_v, we reject it.

Classification results I

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

v	s	# codes	v	s	# codes	v	s	# codes
13p	**2**	**1**	30	4	1376	46	7	231616
14m	*1*	*3*	**31p**	**5**	**80**	47	7	1137664
15	2	5	32	5	242	48	7	2712394
16	2	3	33	5	1212	**49p**	**8**	**157340**
17	2	5	34	5	1360	50	8	550528
18	2	12	35	5	6762	51	8	3642484
19p	**3**	**4**	36	5	12784	52	8	4204688
20m	*2*	*23*	**37p**	**6**	**820**	53	8	21282112
21	3	25	*38m*	*5*	*35120*	54	8	54243072
22	3	20	39	6	15678	**55p**	**9**	**3027456**
23	3	40	40	6	19794	56	9	8660480
24	3	107	41	6	68784	57	9	68638238
25p	**4**	**12**	42	6	185376	58	9	74974976
26	4	36	**43p**	**7**	**9508**	59	9	446472448
27	4	128	*44m*	*6*	*621888*	60	9	$\geq$ 455000000
28	4	164	45	7	257886	61p	10	42373196
29	4	400						