CLASSIFICATION RESULTS FOR $(v, k, 1)$ CYCLIC DIFFERENCE FAMILIES WITH SMALL PARAMETERS

Tsonka Baicheva and Svetlana Topalova

Abstract: *Classifications of $(v, k, 1)$ cyclic difference families (CDFs) by other authors are known for $k = 3$ and $v \leq 57$, $k = 4$ and $v \leq 64$, $k = 5$ and $v \leq 65$, $k = 6$ and $v = 91$ and $k = 7$ and $v = 91$. In this work we construct all inequivalent $(v, k, 1)$ CDFs (respectively all multiplier inequivalent cyclic 2-$(v, k, 1)$ designs) with $k \leq 11$ and some small v by a computer search and an algorithm similar to the one applied for the classification of optimal orthogonal codes in our previous works. We obtain the same number of inequivalent CDFs for all the parameters, for which previous classification results are known. The new parameters covered by our software for $k \leq 7$ are $(61, 3, 1)$, $(73, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$, and $(85, 5, 1)$ CDFs.*

Keywords*: cyclic difference set, Steiner triple system, optical orthogonal code*

ACM Classification Keywords*: Algorithms*

MSC*: 05B05, 05B07, 05B10*

Introduction

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

For general background on difference families we refer to [Abel, 1996] and [Beth, Jungnickel, Lenz, 1999]. Complete sets of CDFs are of interest in their own right, as well as for applications in the construction of other types of combinatorial structures. There are known applications to one-factorizations of complete graphs and to cyclically resolvable cyclic Steiner triple systems [Fuji-Hara, Miao, Shinohara, 2002], as well as to constructions of regular LDPC codes [Fujisawa, Sakata, 2005]. Very efficient constructions of new optimal perfect secrecy systems that are onefold secure against spoofing are obtained via CDF [Huber, 2012]. Optimal frequency-hopping sequences can also be constructed from $(v, k, 1)$ CDFs.

01 Related combinatorial structures

Differences can be considered as a measure of distance. That is why CDFs correspond to several different combinatorial structures, for which a distance condition is defined by means of scalar product, or Hamming distance. A very suitable example are the two different definitions that authors very often give for (v, k, λ) optical orthogonal codes (OOCs).

Definition 2. *A (v,k,λ) optical orthogonal code $\mathcal{C}$ is a collection of $\{0,1\}$ sequences of length v and Hamming weight k such that:*

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

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

for all pairs of distinct sequences $x, y \in \mathcal{C}$. The same definition holds for a (v,k,λ) binary cyclically permutable constant weight (CPCW) code.

Definition 3. *A (v,k,λ) optical orthogonal code (OOC) can be defined as 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 and any two translates of two distinct codeword-sets share at most λ elements:*

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

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

And if $(v,k,1)$ OOCs are considered, the latter definition is usually replaced by the following one.

Definition 4. *A $(v,k,1)$ optical orthogonal code (OOC) may be viewed as a set of k-subsets of Z_v whose list of differences has no repeated elements.*

A $(v,k,1)$ OOC is *optimal* when its size reaches the upper bound $\left\lfloor \frac{(v-1)}{k(k-1)} \right\rfloor$. If its size is exactly equal to $\frac{(v-1)}{k(k-1)}$, the code is *perfect* because its list of differences covers all nonzero elements of Z_v. A perfect $(v,k,1)$ OOC forms a $(v,k,1)$ CDF.

Next we supply definitions of other combinatorial structures related to difference families.

Definition 5. *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 permuting its points in one cycle.

Definition 6. *An (n,w,d) binary constant weight code (CWC) of length n, weight w and minimal 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 $(n,w,w-d/2)$ CPCW code.*

A $(v,k,1)$ CDF can be obtained from any optimal perfect $(v,k,1)$ CPCW code (optimal perfect $(v,k,1)$ OOC), and from any optimal cyclic binary CWC with weight k and minimal distance $2(k-1)$. CDFs with $v \equiv k\ (mod\, k(k-1))$ do not correspond to CPCW codes (OOCs) and cyclic binary CWCs.

There is a one-to-one correspondence between $(v,k,1)$ CDFs and cyclic 2-$(v,k,1)$ designs. An example illustrating the relations between difference families and other combinatorial structures is presented in Figure 1.

02 Equivalence

The aim of our work is classification of CDFs. That is why we have to know when two CDFs are equivalent.

Figure 1: Relations of cyclic difference families
a) - Perfect $(13, 3, 1)$ OOC and $(13, 3, 1)$ CDF

codeword-sets(sets)	differences
{0,1,4}	1 3 4 9 10 12
{0,2,8}	2 5 6 7 8 11

b) - Related cyclic 2-(13,3,1) design and cyclic (13,3,4) CWC

0	1 0 0 0 0 0 0 0 0 1 0 0 1	1 0 0 0 0 1 0 0 0 0 0 1 0
1	1 1 0 0 0 0 0 0 0 0 1 0 0	0 1 0 0 0 0 1 0 0 0 0 0 1
2	0 1 1 0 0 0 0 0 0 0 0 1 0	1 0 1 0 0 0 0 1 0 0 0 0 0
3	0 0 1 1 0 0 0 0 0 0 0 0 1	0 1 0 1 0 0 0 0 1 0 0 0 0
4	1 0 0 1 1 0 0 0 0 0 0 0 0	0 0 1 0 1 0 0 0 0 1 0 0 0
5	0 1 0 0 1 1 0 0 0 0 0 0 0	0 0 0 1 0 1 0 0 0 0 1 0 0
6	0 0 1 0 0 1 1 0 0 0 0 0 0	0 0 0 0 1 0 1 0 0 0 0 1 0
7	0 0 0 1 0 0 1 1 0 0 0 0 0	0 0 0 0 0 1 0 1 0 0 0 0 1
8	0 0 0 0 1 0 0 1 1 0 0 0 0	1 0 0 0 0 0 1 0 1 0 0 0 0
9	0 0 0 0 0 1 0 0 1 1 0 0 0	0 1 0 0 0 0 0 1 0 1 0 0 0
10	0 0 0 0 0 0 1 0 0 1 1 0 0	0 0 1 0 0 0 0 0 1 0 1 0 0
11	0 0 0 0 0 0 0 1 0 0 1 1 0	0 0 0 1 0 0 0 0 0 1 0 1 0
12	0 0 0 0 0 0 0 0 1 0 0 1 1	0 0 0 0 1 0 0 0 0 0 1 0 1

Definition 7. *Two difference families* $\mathbf{F} = \{B_1, B_2, \ldots, B_n\}$ *and* $\mathbf{F}' = \{B'_1, B'_2, \ldots, B'_n\}$ *over a group* G *are equivalent if there is an automorphism* α *of* G *such that for each* $i = 1, 2, \ldots, n$ *there exists* B'_j *which is a translate of* $\alpha(B_i)$.

We are also interested in the equivalence definitions for the related to the CDFs combinatorial objects, because classifying CDFs we classify them too.

Definition 8. *Two* 2-(v, k, λ) *designs* D *and* D' *are isomorphic if there exists a permutation of the points which maps each block of* D *to a block of* D'.

Definition 9. *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'.

Multiplier equivalence is defined for cyclic combinatorial objects.

Definition 10. *Two* (v, k, λ) *CPCW codes (OOCs) 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.*

Definition 11. *Two cyclic* 2-(v, k, λ) *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 cyclic designs can be isomorphic, but multiplier inequivalent. The same holds for two CPCW codes.

The number of multiplier inequivalent perfect optimal 2-$(v, k, 1)$ CPCW codes (OOCs) is the same as the number of the inequivalent 2-$(v, k, 1)$ CDFs.

The number of inequivalent $(v, k, 1)$ CDFs is the same as the number of multiplier inequivalent cyclic 2-$(v, k, 1)$ designs, and vice versa.

03 Existence Results

The known existence results for CDFs with $k = 3, 4, 5, 6, 7$ can be summarized as follows:

Theorem 1. *A $(v, k, 1)$ CDF can exist for $v \equiv 1, k \ (mod\ k(k-1))$.*

Theorem 2. *[Dinitz, Shalaby, 2002] There exists a $(v, 3, 1)$ difference family for every $v \equiv 1, 3 \ (mod\ 6)$ except $v = 9$.*

Theorem 3. *([Bose 1939],[Buratti, 1995],[Buratti, 1997],[Colbourn, Dinitz (eds.), 1996],[Lidl, Niederreiter, 1983])*

1. For any prime power $q \equiv 1 \ (mod\ 12)$ there exists a $(q, 4, 1)$ difference family in GF(q).

2. For any prime power $q \equiv 1 \ (mod\ 20)$ there exists a $(q, 5, 1)$ difference family in GF(q).

Theorem 4. *([Abel, Burati, 2004],[Abel, Costa, Finizio, 2004])*

1. A $(12t + 1, 4, 1)$ differnce family exists for $1 \leq t \leq 50$ except for $t = 2$.

2. A $(20t + 1, 5, 1)$ differnce family exists for $1 \leq t \leq 50$ except possibly for $t = 16, 25, 31, 34, 40, 45$.

Theorem 5. *([Chen, Zhu, 1998]) There exists a $(q, 6, 1)$ DF for any prime power $q \equiv 1 \ (mod\ 30)$ with one exception of $q = 61$.*

Theorem 6. *([Chen, Wei, Zhu, 2002]) There exists a $(q, 7, 1)$ DF for any prime power $q \equiv 1 \ (mod\ 42)$ except for $q = 43$, posibly for $q = 127, 211, 31^6$, and primes $q \in [261239791, 1.236597.10^{13}]$ such that $(-3)^{\frac{(q-1)}{14}} = 1$ in GF(q).*

04 On the classification problem

The classification and the public accessibility of the classified CDFs with small parameters is of particular interest, because it can help to choose, among CDFs with the same parameters, the one which is most suitable for some application (for optical code-division multiple-access channels for instance), or the one which is most suitable to serve as ingredient in some recursive construction of CDFs with higher parameters.

Classifications of cyclic difference families by other authors are known for $k = 3$ and $v \leq 57$ [Colbourn, Rosa, 1999], $k = 4$ and $v \leq 64$ [Colbourn, Mathon, 1980], $k = 5$ and $v \leq 65$ [Colbourn, Mathon, 1980], $k = 6$ and $v = 91$ [Colbourn, 1981], [Janko, Tonchev, 1991] and $k = 7$ and $v = 91$ [Bhat-Nayak, Kane, Kocay, Stanton, 1983]. In this work we construct all inequivalent cyclic difference families with $k \leq 11$ and some small v.

Construction method

We use a modification of our algorithm for classification of optimal $(v, k, 1)$ OOCs [Baicheva, Topalova, 2011].

We classify the $(v, k, 1)$ CDFs up to equivalence by back-track search with minimality test on the partial solutions [Kaski, Östergård, 2006, section 7.1.2]. Without loss of generality we can assume that $b_1 < b_2 < \cdots < b_s$ for each set $\mathbf{B} = \{b_1, b_2, \ldots, b_s\}$. We first arrange all possibilities for the sets B_i with respect to a lexicographic order defined on them. If a set $B_i \in \mathbf{F}$ is replaced by one of its translates, we obtain an equivalent CDF. That is why we can assume that each set of $\mathbf{F}$ is lexicographically smaller than its translates. This means that $b_1 = 0$ and when we say that B_1 is mapped to B_2 by the permutation φ, we mean that B_2 is the smallest translate of $\varphi(B_1)$.

Let $\varphi_0, \varphi_1, \ldots, \varphi_{m-1}$ be the automorphisms of Z_v, where φ_0 is the identity. We construct an array of all sets $\mathbf{B}$ of k elements of Z_v which might become sets of $\mathbf{F}$, i.e. they are smaller than all their translates and $\Delta\mathbf{B}$ does not contain repeated differences. We find them in lexicographic order. To each constructed set we apply the permutations $\varphi_i, i = 1, 2, \ldots, m-1$. If some of them maps it to a smaller set, we do not add the current set since it is already somewhere in the array. If we add the current set to the array, we also add after it the $m-1$ sets to which it is mapped by $\varphi_1, \varphi_2, \ldots, \varphi_{m-1}$.

Most of the sets of a CDF have $v-1$ translates. If $v \equiv k \ (mod\ k(k-1))$ one of the sets has v/k translates and is equal to $\{0, v/k, 2v/k, \ldots, (k-1)v/k\}$, so we first add this set to the CDF. We then apply back-track search to choose the sets with $v-1$ translates from the upper list of all possibilities for them. The above described ordering

of all the possible sets allows repeated sets in the array, but makes the minimality test of the partial solutions very fast. By the minimality test we check if the current solution can be mapped to a lexicographically smaller one by the automorphisms of Z_v and reject it if so.

In this way we classify the CDFs up to multiplier equivalence. We use our own software written in C++.

Classification results

CDFs correspond to the perfect optimal OOCs which we have classified in our papers on optimal OOCs with parameters $(v, 4, 1)$ [Baicheva, Topalova, 2011], $(v, 5, 1)$ [Baicheva, Topalova, 2012a] and $(v, 3, 1)$ [Baicheva, Topalova, 2012b]. Therefore, in these papers new results about CDFs are obtained too. In the present paper we repeat all previous results on CDFs (ours and of other authors) and add some new ones, which we obtain by the above described construction method. We find the same number of inequivalent CDFs for all the parameters, for which previous classification results are known. To the results of other authors for $k \leq 7$ we add classifications of $(61, 3, 1)$, $(73, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$ and $(85, 5, 1)$ CDFs. A summary is presented in Table 1.

Since previous classification results have been obtained by different authors for the different parameters, we think that collecting them together is of particular interest. We believe that both Table 1 and the files with all the inequivalent difference sets (available from the authors) will be very useful for applications and to people who will go on with research in this field.

Table 1: Inequivalent cyclic (v,k,1) difference families (Multiplier inequivalent cyclic 2-(v,k,1) designs)

v	k	CDFs
7	3	1
9	3	0
13	3	1
15	3	2
19	3	4
21	3	7
25	3	12
27	3	8
31	3	80
33	3	84
37	3	820
39	3	798
43	3	9508
45	3	11616
49	3	157340
51	3	139828
55	3	3027456
57	3	2353310
61	3	42373196

v	k	CDFs
13	4	1
16	4	0
25	4	0
28	4	0
37	4	2
40	4	10
49	4	224
52	4	206
61	4	18132
64	4	12048
73	4	1426986
76	4	1113024
21	5	1
25	5	0
41	5	1
45	5	0
61	5	10
65	5	2
81	5	528

v	k	CDFs
85	5	170
31	6	1
36	6	0
61	6	0
66	6	0
91	6	4
96	6	0
43	7	0
49	7	0
85	7	0
91	7	2
57	8	1
64	8	0
73	9	1
81	9	0
91	10	1
100	10	0
111	11	0
121	11	0

Bibliography

[Shannon, 1949] C.E.Shannon. The Mathematical theory of communication. In: The Mathematical Theory of Communication. Ed. C.E.Shannon and W.Weaver. University of Illinois Press, Urbana, 1949.

[Abel, 1996] R.J.R. Abel, *Difference families*, in: C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, pp. 270Ű-287.

[Beth, Jungnickel, Lenz, 1999] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, Cambridge (1999).

[Fuji-Hara, Miao, Shinohara, 2002] R. Fuji-Hara, Y. Miao and S. Shinohara, Complete Sets of Disjoint Difference Families and their Applications, *Journal of Statistical Planning and Inference*, Volume 106, Issues 1Ű2, 1 August 2002, pp. 87 Ű 103.

[Fujisawa, Sakata, 2005] Fujisawa, M., Sakata, S., A class of quasi-cyclic regular LDPC codes from cyclic difference families with girth 8 , *Proceedings International Symposium on Information Theory*, 4-9 Sept. 2005, pp. 2290 - 2294.

[Huber, 2012] M. Huber, Perfect Secrecy Systems Immune to Spoofing Attacks, arXiv:1205.4874v1.

[Dinitz, Shalaby, 2002] H.J. Dinitz, N. Shalaby, Block disjoint difference families for Steiner tripple systems: $v \equiv 3 \ (mod \ 6)$, *J. Stat. Plann. Infer.*, 106, 2002, pp. 77 - 86.

[Bose 1939] 3. R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics*, Vol. 9, 1939, pp. 353 - 399.

[Buratti, 1995] M. Buratti, Constructions for $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, *Discrete Mathematics*, Vol. 138, 1995, pp. 169 - 175.

[Buratti, 1997] M. Buratti, From a $(G, k, 1)$ difference family to a $(C_k \oplus G, k, 1)$ difference family, *Designs, Codes and Cryptography*, Vol. 11, 1997, pp. 5 - 9.

[Colbourn, Dinitz (eds.), 1996] C. J. Colbourn and J. H. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, New York, 1996.

[Lidl, Niederreiter, 1983] R. Lidl and H. Niederreiter, *Finite fields, Encyclopedia of Mathematics and Its Applications*, Vol. 20, Cambridge University Press, Cambridge, 1983.

[Abel, Burati, 2004] R.J.R. Abel, M. Burati, Some progress on $(v, 4, 1)$ diffrence families and optical orthogonal codes, *J. Combin Theory* A, 106, 2004, pp. 59 - 75.

[Abel, Costa, Finizio, 2004] R.J.R. Abel, S. Costa, N.j. Finizio, Directed-ordered whist tournaments and $(v, 5, 1)$ difference families: Existence results and some new classes of Z-cyclic solutions, *Discrete Appl. Math.*, 143, 2004, pp. 43 - 53.

[Chen, Zhu, 1998] K. Chen, L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, *Designs, Codes and Cryptography*, 15, 1998, pp. 167 - 173.

[Chen, Wei, Zhu, 2002] K. Chen,R. Wei, L. Zhu, Existence of $(q, 7, 1)$ difference families with q a prime power, *Journal of Combinatorial Designs*, 10, Issue 2, 2002, pp. 126 - 138.

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

[Baicheva, Topalova, 2011] 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*, vol. 47(3), 2011, pp. 224 - 231.

[Colbourn, Mathon, 1980] Colbourn M.J., Mathon R.A., On cyclic Steiner 2-designs, *Ann. Discrete Math.*, vol. 7, 1980, pp. 215 - 253.

[Colbourn, 1981] C. J. Colbourn, On cyclic Steiner systems S(2,6,91), *Abstracts Amer. Math. Soc.*, 2, 1981.

[Janko, Tonchev, 1991] Z. Janko, V. D. Tonchev, Cyclic 2-(91, 6, 1) designs with multiplier automorphisms, *Discrete Mathematics*, Volume 97, Issues 1Ű3, 1991, pp. 265 - 268.

[Bhat-Nayak, Kane, Kocay, Stanton, 1983] V. N. Bhat-Nayak, V. D. Kane, W. L. Kocay, R. G. Stanton, Settling some BIBD conjectures, *Ars Combin.*, 16, 1983, pp. 229 - 234.

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

[Baicheva, Topalova, 2012a] T. Baicheva and S. Topalova, Optimal optical orthogonal codes of weight 5 and small lengths, International Conference on Applications of Computer Algebra, Sofia, Bulgaria, 2012.

[Baicheva, Topalova, 2012b] T. Baicheva and S. Topalova, Optimal $(v, 3, 1)$ binary cyclically permutable constant weight codes with small v, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Pomorie, Bulgaria, 2012, pp. 41 - 46.

Authors' Information

Tsonka Stefanova Baicheva *- associate professor, Institute of Mathematics and Informatics Bulgarian Academy of Sciences, P.O.Box 323, 5000 V. Tarnovo, Bulgaria*
e-mail: tsonka@math.bas.bg

Svetlana Todorova Topalova *- associate professor, Institute of Mathematics and Informatics Bulgarian Academy of Sciences, P.O.Box 323, 5000 V. Tarnovo, Bulgaria*
e-mail: svetlana@math.bas.bg