J. Algebra Comb. Discrete Appl.
13(1) • 111–119

Received: 14 May 2025
Accepted: 20 September 2025

Journal of Algebra Combinatorics Discrete Structures and Applications

Construction of $(v, k, 1)$ cyclic difference families with small parameters

Research Article

Tsonka Baicheva* , Svetlana Topalova**, Ivan Hetman

Abstract: We construct all nonequivalent $(v, k, 1)$ cyclic difference families for 18 sets of parameters v and k for which classification results were not known. We also present the multipliers of all previously classified CDFs with small parameters. Most of the results are double-checked by two different backtrack search algorithms. The usage of an interesting property of the considered objects makes one of these algorithms faster than the other.

2020 MSC: 05-08, 05B10, 94B15

Keywords: Cyclic difference families, Multipliers, Cyclic Steiner systems, Cyclically permutable constant weight codes, Optical orthogonal codes

1. Introduction

Cyclic difference families (CDFs) are of particular interest because they are closely related to several other combinatorial structures [3] and have therefore numerous applications, for instance [20, 22, 26]. For general background on difference families we refer to [3].

We consider the additive group $\mathbb{Z}_v$ of integers modulo v. Let $B = \{b_0, b_1, \ldots, b_{k-1}\}$ be a k-element subset of $\mathbb{Z}_v$. Then $\Delta B = \{b_i - b_j |\ i, j = 0, 1, \ldots, k-1; i \neq j\}$ is the multiset of differences of B, and

* *The work of Tsonka Baicheva was partially supported by Grant No D01-98/26.06.2025 of the MES of the Republic of Bulgaria*
Tsonka Baicheva; Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria (email: tsonka@math.bas.bg).
** *The work of Svetlana Topalova was partially supported by the Centre of Excellence in Informatics and ICT under the Grant No BG16RFPR002-1.014-0018-C01, financed by the Research, Innovation and Digitalization for Smart Transformation Programme 2021-2027 and co-financed by the European Union.*
Ivan Hetman; Lviv, Ukraine (email: vespertilion@gmail.com).
Svetlana Topalova (Corresponding Author); 1) Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria, 2) Centre of Excellence in Informatics and Information and Communication Technologies, 1113 Sofia, Bulgaria (email: svetlana@math.bas.bg).

$B + t$ denotes a t-translate of B, where $B + t = \{b_0 + t, b_1 + t, \ldots, b_{k-1} + t\}$ for $t \in \mathbb{Z}_v$. The k-element subset B is called *full* if the number of its distinct translates is v, and *short* if it is less than v.

Definition 1.1. *A* $(v, k, 1)$ ***cyclic difference family*** *can be defined as a set* $D = \{B_1, B_2, \ldots, B_s\}$ *of* k*-element subsets of* $\mathbb{Z}_v$ *(blocks), such that* $B_n = \{b_{n0}, b_{n1}, \ldots, b_{nk-1}\}$ *and each nonzero element of* $\mathbb{Z}_v$ *either appears in the short block* $\{0, v/k, 2v/k, \ldots, (k-1)v/k\}$ *(possible if* k *divides* v*), or is obtained exactly once as a difference* $b_{ni} - b_{nj}$ *for* $1 \le n \le s$ *and* $i, j = 0, 1, \ldots, k-1; i \ne j$.

Definition 1.2. *Each* ***automorphism*** α ***of*** $\mathbb{Z}_v$ *is defined by an element* $m \in \mathbb{Z}_v$ *such that* $gcd(m, v) = 1$, *and* α *maps each* $a \in \mathbb{Z}_v$ *to* $ma \in \mathbb{Z}_v$. *The element* m *is a* ***multiplier*** *of the cyclic difference family* D *if* α *maps each block of* D *to a translate of a block of* D.

Most closely related to the difference families are the cyclic Steiner systems and the perfect $(v, k, 1)$ optical orthogonal codes (OOCs). The latter are equivalent to $(v, k, 1)$ cyclically permutable constant weight (CPCW) codes.

Definition 1.3. *A* $(v, k, 1)$ ***OOC (CPCW code)*** *may be viewed as a set* C *of* k*-subsets of* $\mathbb{Z}_v$ *(codewords) 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 $\mathbb{Z}_v$. A perfect $(v, k, 1)$ *OOC* corresponds to a $(v, k, 1)$ CDF without short blocks.

Definition 1.4. *Let* V *be a finite set of* v *points, and* $\mathcal{B} = \{B_j\}_{j=1}^{b}$ *a finite collection of* k*-element subsets of* V, *called blocks.* $\mathcal{D} = (V, \mathcal{B})$ *is a* **2-*(*v*,*k*,1)** ***design*** *(**a Steiner system*** $S(2, k, v)$*) if any* 2*-subset of* V *is contained in exactly one block of* $\mathcal{B}$.

Definition 1.5. *An* ***automorphism of a*** **2-$(v, k, 1)$** ***design*** $\mathcal{D}$ *is a permutation of the points which maps each block of* $\mathcal{D}$ *to a block of* $\mathcal{D}$.

A 2-(v,k,1) design is *cyclic* if it has an automorphism 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). Each cyclic design corresponds to a $(v, k, 1)$ CDF and vice versa.

Definition 1.6. *A* ***multiplier automorphism*** *of a cyclic* 2-$(v, k, 1)$ *design* $\mathcal{D}$ *is an automorphism of* $\mathbb{Z}_v$ *which maps each block of* $\mathcal{D}$ *to a block of* $\mathcal{D}$.

A $(v, k, 1)$ CDF can exist for $v \equiv 1, k \ (mod\ k(k-1))$. If $v \equiv 1 \ (mod\ k(k-1))$ the CDF corresponds to a strictly cyclic 2-$(v, k, 1)$ design, and if $v \equiv k \ (mod\ k(k-1))$ to a cyclic design with one short orbit. We illustrate this by the following two examples, but if you are a reader familiar with the subject, please skip them.

Example 1.7. *Consider* $D = \{B_1, B_2\}$ *where* $B_1 = \{0, 1, 4\}$ *and* $B_2 = \{0, 2, 8\}$ *are subsets of* $\mathbb{Z}_{13}$. *Their multisets of differences are* $\Delta B_1 = \{1, 3, 4, 9, 10, 12\}$ *and* $\Delta B_2 = \{2, 5, 6, 7, 8, 11\}$. *Each nonzero element of* $\mathbb{Z}_{13}$ *appears exactly once in* $\Delta B_1 \cup \Delta B_2$. *That is why:*

- D *is a* $(13, 3, 1)$ *cyclic difference family. It has 3 multipliers:* $1, 3, 9$. *The nontrivial ones transform the blocks as:*
  $3B_1 + 1 = B_1,\ 3B_2 + 2 = B_2$
  $9B_1 + 4 = B_1,\ 9B_2 + 8 = B_2$
- D *is the set of base blocks of a strictly cyclic* 2-$(13, 3, 1)$ *design (Figure 1). The multipliers* 1, 3 *and* 9 *correspond to the design automorphisms* ϵ *(the identity),* α *and* β *respectively. They act on the points as:*

	B_1											B_2											
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	1	0	1	0	0	0	0	1	0	0	0	0
5	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	0
6	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0
7	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0
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

Figure 1. Incidence matrix of a strictly cyclic 2-$(13, 3, 1)$ design

$\alpha = (0)(1, 3, 9)(2, 6, 5)(4, 12, 10)(7, 8, 11)$, $\epsilon = (0)(1)\dots(12)$, $\epsilon = \alpha^3$.
$\beta = (0)(1, 9, 3)(2, 5, 6)(4, 10, 12)(7, 11, 8)$, $\beta = \alpha^2$,

Note that for the multipliers of the CDF it holds $9 = 3^2$, $1 = 3^3$, *and for the corresponding multiplier automorphisms of the design* $\beta = \alpha^2$ *and* $\epsilon = \alpha^3$.

- *D is an optimal perfect* $(13, 3, 1)$ *CPCW code (OOC) with codewords* B_1 *and* B_2.

Example 1.8. *Consider* $D' = \{B'_1, B'_2, B'_3\}$ *where* $B'_1 = \{0, 5, 10\}$, $B'_2 = \{0, 1, 4\}$ *and* $B'_3 = \{0, 2, 8\}$ *are subsets of* $\mathbb{Z}_{15}$. *Their multisets of differences are* $\Delta B'_1 = \{5^3, 10^3\}$, $\Delta B'_2 = \{1, 3, 4, 11, 12, 14\}$ *and* $\Delta B'_3 = \{2, 6, 7, 8, 9, 13\}$. *Each nonzero element of* $\mathbb{Z}_{15}$ *is either in the short block* B'_1, *or appears exactly once in* $\Delta B'_2 \cup \Delta B'_3$. *That is why:*

- *D' is a* $(15, 3, 1)$ *CDF with 4 multipliers:* $1, 2, 4, 8$. *They transform the blocks as:*
  $2B'_1 = B'_1$, $2B'_2 = B'_3$, $2B'_3 = B'_2$
  $4B'_1 = B'_1$, $4B'_2 = B'_2$, $4B'_3 = B'_3$
  $8B'_1 = B'_1$, $8B'_2 = B'_3$, $8B'_3 = B'_2$
- *D' is the set of base blocks of a cyclic* 2-$(15, 3, 1)$ *design (Figure 2).*
  The multipliers 1, 2, 4 *and* 8 *correspond to design automorphisms* ϵ', α', β' *and* γ'*:*
  $\alpha' = (0)(1, 2, 4, 8)(3, 6, 12, 9)(5, 10)(7, 14, 13, 11)$, $\epsilon' = (0)(1)\dots(14)$, $\epsilon' = \alpha'^4$,
  $\beta' = (0)(1, 4)(2, 8)(3, 12)(5)(6, 9)(7, 13)(10)(11, 14)$, $\beta' = \alpha'^2$,
  $\gamma' = (0)(1, 8, 4, 2)(3, 9, 12, 6)(5, 10)(7, 11, 13, 14)$, $\gamma' = \alpha'^3$.
  The multipliers $4 = 2^2$, $8 = 2^3$, $1 = 2^4$, *the automorphisms* $\beta' = \alpha'^2$, $\gamma' = \alpha'^3$, $\epsilon' = \alpha'^4$.

A cyclic design corresponding to a $(v, k, 1)$ CDF with M multipliers, has M multiplier automorphisms and at least vM automorphisms. There are many examples of cyclic designs with more than vM automorphisms. The design from Example 1.8 has 20160 automorphisms.

Definition 1.9. *Two* $(v, k, 1)$ *cyclic difference families are* ***equivalent*** *if there is an automorphism of* $\mathbb{Z}_v$ *which maps each block of the first family to a translate of a block of the second family.*

Definition 1.10. *Two* $(v, k, 1)$ *OOCs (CPCW codes)* C *and* C' *are* ***isomorphic*** *if there exists a permutation* φ *of* $\mathbb{Z}_v$, *which maps the collection of translates of each codeword of* C *to the collection of translates of a codeword of* C'. *These two codes are* ***multiplier equivalent*** *if* φ *is an automorphism of* $\mathbb{Z}_v$.

Figure 2. **Incidence matrix of a cyclic 2-$(15, 3, 1)$ design**

	B'_1					B'_2													B'_3													
0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0
1	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1
2	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0
3	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0
4	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0
5	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0
6	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0
7	0	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0
8	0	0	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0
9	0	0	0	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0
10	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0
11	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0
12	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0
13	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0
14	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1

Multiplier nonequivalent perfect OOCs correspond to nonequivalent CDFs. That is why our classification results for $(v, k, 1)$ CDFs with $v \equiv 1 \ (mod\ k(k-1))$ correspond to classification results for multiplier nonequivalent perfect $(v, k, 1)$ OOCs.

Definition 1.11. *Two cyclic 2-$(v, k, 1)$ designs $\mathcal{D}$ and $\mathcal{D}'$ are* ***isomorphic*** *if there exists a permutation ψ of the points which maps each block of $\mathcal{D}$ to a block of $\mathcal{D}'$. The designs $\mathcal{D}$ and $\mathcal{D}'$ are* ***multiplier equivalent*** *if ψ is an automorphism of $\mathbb{Z}_v$.*

Equivalent $(v, k, 1)$ CDFs correspond to multiplier equivalent cyclic 2-$(v, k, 1)$ designs. The CDFs classification results from Table 1 are also classification results for multiplier nonequivalent cyclic 2-$(v, k, 1)$ designs. Usually two multiplier nonequivalent cyclic designs are nonisomorphic, but there are parameters v and k for which the nonequivalent $(v, k, 1)$ CDFs are more than the corresponding nonisomorphic cyclic 2-$(v, k, 1)$ designs. Infinite series of such design parameters are presented in [27].

The number of automorphisms of $\mathbb{Z}_v$ is given by the Euler function $\phi(v)$. It is proved in [25] that if $(v, \phi(v)) = 1$, then all isomorphic cyclic incidence structures on v points are multiplier equivalent. In addition it is shown in [27] that isomorphic cyclic 2-$(pq, k, 1)$ designs are always multiplier equivalent for primes p and q, such that $k = q$ and $p > q$, or an $(m, k, 1)$ CDF does not exist for either $m = p$ or $m = q$. In the cases listed above, in the cases with only one $(v, k, 1)$ CDF, and in the cases considered in [6] or [17], the classification results from Table 1 are classification results for the nonisomorphic cyclic 2-$(v, k, 1)$ designs. In the remaining cases the number of the nonisomorphic cyclic 2-$(v, k, 1)$ designs might be smaller than that of the nonequivalent $(v, k, 1)$ CDFs.

Numerous existence results on CDFs have been obtained. The first paper on the topic was published in 1939 [8]. Presently we know that there exists a $(v, 3, 1)$ difference family for every $v \equiv 1, 3 \ (mod\ 6)$ except for $v = 9$ [19] and there exists a $(v, 4, 1)$ difference family for every $v \equiv 1, 4 \ (mod\ 12)$ except for $v = 16, 25, 28$ [28]. A $(20t + 1, 5, 1)$ CDF exists for $1 \leq t \leq 50$ except possibly for $t = 16, 25, 31, 34, 40, 45$ [2], and a $(pq, 5, 1)$ CDF exists for primes p and q, such that $p \equiv q \equiv 11 \ (mod\ 20)$ [12]. For $k = 6$ and 7 we know that a $(q, 6, 1)$ CDF exists for any prime power $q \equiv 1 \ (mod\ 30)$ with the exception of $q = 61$ [15] and a $(q, 7, 1)$ CDF exists for any prime power $q \equiv 1 \ (mod\ 42)$ except for $q = 43$, possibly for $q = 127$ (nonexistence proved in [5]), $211, 31^6$, and primes $q \in [261239791,\ 1.236597 \cdot 10^{13}]$ such that $(-3)^{\frac{(q-1)}{14}} = 1$ in GF(q)[16]. An infinite family of parameters for which a CDF does not exist is presented in [13], namely: If k is an even integer whose prime decomposition contains a prime $p \equiv 3 \ (mod\ 4)$ raised to an odd power, then there does not exists a $(2k(k-1) + k, k, 1)$ CDF.

The fact that the blocks B and $-B$ of a difference family have $\Delta B = \Delta(-B)$ has been used in previous research in different ways (see [14], for instance). In [9] *similar* difference families are defined as

follows.

Definition 1.12. *Two difference families are* ***similar*** *if one can be obtained from the other by changing the sign of some base blocks.*

Similar difference families are used in [11] to derive a lower bound on the number of non isomorphic cyclic 2-$(v, k, 1)$ designs, and they are used in [10] to construct new designs. We do not know papers in which the similarity property is used in algorithms for classification of cyclic difference families. That is why one of the aims of the present paper is to promote such an algorithm, namely the algorithm A_2 presented in the next section.

In [11] it is proved that if there exists a 2-$(v, k, 1)$ cyclic design, then there are at least $\lceil \frac{2^n}{\phi(v)} \rceil$ nonisomorphic $(v, k, 1)$ cyclic designs (n is the number of full base blocks) and more precise lower bounds are derived for $k = 3$ and prime v. These bounds are quite far from the known results for small parameters, but give a good idea of the increase of the number of CDFs with definite k when v grows.

Constructive classification is only possible for relatively small values of v, but is very important for the possible usage of CDFs in different applications. Classification results have been obtained in [4, 6, 7, 17–19, 23] and a summary of them was presented in [4]. In the present work we update this summary by adding 18 new classification results and correcting the number of $(73, 4, 1)$ CDFs which was wrongly given in [4]. In addition we present here the number of multipliers of all the CDFs with small parameters which have been classified by now and provide files with the CDFs and their multipliers. They can be freely downloaded from http://www.moi.math.bas.bg/~tsonka/MainCDF.htm. Section 2 presents the construction algorithms, Section 3 the results and the open problems.

2. Construction methods

To obtain the new classification results we use two different backtrack search algorithms. Exhaustive backtrack search is exponential [24], so the computation time grows very fast with the parameters. Nevertheless it is often successfully used for the construction of combinatorial structures with relatively small parameters if rejection of some equivalent partial solutions is applied (big branches of the search tree are cut off) and parameter-specific restrictions are implemented. The first algorithm we use (A_1) is a parallelized version of the algorithm described in [4] and [6]. The second one (A_2) was recently suggested by the first author in [21] and improved by him later. Without going into details we shall outline here the main ideas of the two approaches and the differences between them.

Both algorithms use the following facts about a block $B = \{b_0, b_1, \dots b_{k-1}\}$:

- a full block B can be part of a CDF if its multiset of differences $\Delta B = \{b_i - b_j | i, j = 0, \dots, k-1; i \neq j\}$ consists of $k(k-1)$ distinct integers. Only full blocks which meet this requirement are constructed.
- If $k|v$ the CDF has a short block $\{0, v/k, 2v/k, \dots, (k-1)v/k\}$ which is added first.
- For computing purposes we assume that $b_0 < b_1 < \dots < b_{k-1}$, and define a lexicographic order on the blocks, such that if $B' = \{b'_0, b'_1, \dots b'_{k-1}\}$, then $B < B'$ if $b_0 < b'_0$, or if $b_i = b'_i$ for $0 \leq i < c \leq k-1$ and $b_c < b'_c$.
- An equivalent CDF is obtained if the block B is replaced by its translate B'. Using this, both algorithms assume that $b_0 = 0$, but their assumptions on the other elements of the blocks are different. The full block B has $k-1$ distinct translates with $b_0 = 0$. Denote them B', B'', etc.

  Algorithm A_1 assumes that B is lexicographically smaller than each of its translates. For instance, $v = 13$, $B = \{0, 1, 4\}$, $B' = \{0, 3, 12\}$, $B'' = \{0, 9, 10\}$.

  A_2 assumes that b_1 is the biggest difference between two successive elements of the block B, namely $b_1 > b_i - b_{i-1}$ for all $i \in \{2, \dots, k-1\}$ and $b_1 > v - b_{k-1}$. For instance, $v = 13$, $B = \{0, 9, 10\}$, $B' = \{0, 3, 12\}$, $B'' = \{0, 1, 4\}$.

All assumptions above are without loss of generality.

A_1 first constructs all blocks which meet the assumptions and orders them in a way which is convenient for the equivalence checks (details can be found in [6]). It then performs an exhaustive backtrack search on these possible blocks.

A_2 implies a different strategy using the fact that $\Delta B = \Delta(-B)$, but defined for objects in the chosen lexicographic order, namely A_2 is based on the usage of mirrors.

Definition 2.1. *Consider a full block $B = \{0, b_1, \ldots, b_{k-1}\}$, such that $b_1 > b_i - b_{i-1}$ for all $i \in \{2, \ldots, k-1\}$ and $b_1 > v - b_{k-1}$. Its **mirror** block is defined as $B' = \{0, b_1, b_1 + (v - b_{k-1}), \ldots, b_1 + (v - b_2)\}$.*

For instance, $v = 13, B = \{0, 9, 10\}, B' = \{0, 9, 12\}$. Two mirror blocks B and B' have $\Delta B = \Delta B'$. That is why A_2 uses in the construction of CDFs only one of the blocks of each pair of mirrors, namely the lexicographically smaller one, which will further be referred to as *canonical*. For it $b_2 < b'_2$ and therefore $b_2 - b_1 < v - b_{k-1}$. More precisely:

Definition 2.2. *A full block $B = \{b_0, \ldots, b_{k-1}\}$ is in **canonical form** when $b_0 = 0$, $b_i > b_{i-1}$ and $b_1 > b_i - b_{i-1}$ for $i \in \{2, \ldots, k-1\}$, and $b_2 - b_1 < v - b_{k-1} < b_1$.*

Definition 2.3. *A CDF is **canonical** when all its full blocks are in canonical form.*

A_2 constructs first all canonical CDFs . The replacement of all canonical blocks by their mirrors results in an equivalent CDF. The replacement of some blocks of a canonical CDF by their mirrors in all other possible ways leads to $2^{\lfloor \frac{v-1}{k(k-1)} \rfloor} - 2$ different CDFs which the algorithm obtains and further tests for equivalence.

Example 2.4. *There are 2 nonequivalent 2-$(15, 3, 1)$ CDFs. One of them is presented in Example 1.8.*

A_1 obtains $D' = \{\{0, 5, 10\}, \{0, 1, 4\}, \{0, 2, 8\}\}$ and $D'' = \{\{0, 5, 10\}, \{0, 1, 4\}, \{0, 2, 9\}\}$.

A_2 obtains $\hat{D}' = \{\{0, 5, 10\}, \{0, 7, 9\}, \{0, 11, 12\}\}$ and $\hat{D}'' = \{\{0, 5, 10\}, \{0, 7, 13\}, \{0, 11, 12\}\}$.

D' and D'' are equivalent respectively to $\hat{D}'$ and $\hat{D}''$. This can be seen if three of the blocks are replaced by their translates, namely $\{0, 1, 4\}+11 = \{0, 11, 12\}$, $\{0, 2, 8\}+7 = \{0, 7, 9\}$ and $\{0, 2, 9\}+13 = \{0, 7, 13\}$.

A_1 constructs the two designs by the backtrack search.

A_2 constructs by backtrack search only the canonical CDF $\hat{D}'$. Then $\hat{D}''$ is obtained when $\{0, 7, 9\}$ is replaced by its mirror $\{0, 7, 13\}$.

The equivalence test in both algorithms is in fact a minimality test. It rejects a partial solution if there exists an automorphism of $\mathbb{Z}_v$ which maps it to a lexicographically smaller partial solution (because the latter should have already been considered).

A_2 is in general much faster than A_1, because during the construction of canonical CDFs, it uses only half of the possible blocks (the canonical ones), and handles the whole number of solutions only at the very end. That is why at each backtrack step A_2 has to deal with a smaller number of partial solutions than A_1. The latter constructs much more partial solutions that do not lead to a CDF, and tests twice more possibilities for the extension of each partial solution.

A_1 obtained most of the new results by a parallel implementation (in C++ and using MPI) on 96 processes (on six 16-core servers at 2.6 GHz) on the high performance computer Avitohol (see the acknowledgment at the end) and it needed one day for $(63, 3, 1)$, $(67, 3, 1)$ and $(133, 7, 1)$, two days for $(69, 3, 1)$, and five days for $(101, 5, 1)$ and $(105, 5, 1)$, while for $(121, 6, 1)$ and $(126, 6, 1)$ it would need more than 10 days. In the considered cases with $k = 5$ and 6 there is a tremendous number of solutions with one block less than the needed, which are not extendable to CDFs, but A_1 needs to handle them. A_1 works best when k is small and the number of all possible codewords is not very big, or when the number of the blocks is small (the uniqueness of $(133, 12, 1)$ was established in several minutes and $(113, 8, 1)$ and $(120, 8, 1)$ finished within 1 day by A_1 on a personal computer). In that case A_1 can gain of its fast minimality test.

Table 1. Number of multipliers of $(v, k, 1)$ CDFs

v	k	CDFs	$Aut_{\mathbb{Z}_v}$	Number of multipliers : Number of CDFs	pub	A_1	A_2
7	3	1	6	3: 1	[19]	✓	✓
13	3	1	12	3: 1	[19]	✓	✓
15	3	2	8	4: 2	[19]	✓	✓
19	3	4	18	1: 1 3: 2 9: 1	[19]	✓	✓
21	3	7	12	1: 1 2: 1 3: 2 6: 3	[19]	✓	✓
25	3	12	20	1: 12	[19]	✓	✓
27	3	8	18	1: 8	[19]	✓	✓
31	3	80	30	1: 63 3: 15 5: 1 15: 1	[19]	✓	✓
33	3	84	20	1: 78 2: 3 5: 2 10: 1	[19]	✓	✓
37	3	820	36	1: 777 3: 42 9: 1	[19]	✓	✓
39	3	798	24	1: 730 2: 4 3: 56 4: 2 6: 4 12: 2	[19]	✓	✓
43	3	9508	42	1: 9377 3: 129 7: 1 21: 1	[19]	✓	✓
45	3	11616	24	1: 11616	[19]	✓	✓
49	3	157340	42	1: 156852 3: 482 7: 4 21: 2	[19]	✓	✓
51	3	139828	32	1: 139808 2: 14 4: 3 8: 1 16: 2	[19]	✓	✓
55	3	3027456	40	1: 3027456	[19]	✓	✓
57	3	2353310	36	1: 2351359 2: 74 3: 1836 6: 33 9: 5 18: 3	[19]	✓	✓
61	3	42373196	60	1: 42368502 3: 4683 5: 10 15: 1	[4]	✓	✓
63	3	49526744	36	1: 49524476 2: 1656 3: 588 6: 24	here	✓	✓
67	3	893780730	66	1: 893764042 3: 16685 11: 2 33: 1	here	✓	
69	3	948359220	44	1: 948359121 2: 93 11: 5 22: 1	here	✓	
13	4	1	12	3: 1	[17]	✓	✓
37	4	2	36	1: 1 3: 1	[17]	✓	✓
40	4	10	16	1: 4 2: 2 4: 4	[17]	✓	✓
49	4	224	42	1: 216 3: 8	[17]	✓	✓
52	4	206	24	1: 195 3: 11	[17]	✓	✓
61	4	18132	60	1: 18123 3: 8 5: 1	[17]	✓	✓
64	4	12048	32	1: 12048	[17]	✓	✓
73	4	1428546	72	1: 1428410 3: 135 9: 1	[6]	✓	✓
76	4	1113024	36	1: 1112992 3: 32	[6]	✓	✓
85	4	228406824	64	1: 228399384 2: 7440	[6]	✓	✓
88	4	149494720	40	1: 149494720	[6]	✓	✓
21	5	1	12	6: 1	[17]	✓	✓
41	5	1	40	5: 1	[17]	✓	✓
61	5	10	60	1: 6 3: 2 5: 1 15: 1	[17]	✓	✓
65	5	2	48	4: 1 12: 1	[17]	✓	✓
81	5	528	54	1: 528	[4]	✓	✓
85	5	170	64	1: 160 2: 2 4: 4 8: 4	[4]	✓	✓
101	5	134632	100	1: 134630 5: 2	here	✓	✓
105	5	84924	48	1: 84909 2: 13 4: 2	here	✓	✓
31	6	1	30	3: 1	[3]	✓	✓
91	6	4	72	1: 1 3: 1 4: 1 12: 1	[18, 23]	✓	✓
121	6	48	110	1: 48	here		✓
126	6	64	36	1: 64	here		✓
91	7	2	72	12: 2	[7]	✓	✓
169	7	4	156	1: 2 3: 2	here		✓
57	8	1	36	3: 1	[4]	✓	✓
73	9	1	72	9: 1	[4]	✓	✓
91	10	1	72	6: 1	[4]	✓	✓

Table 2. Parameters for which no CDF exists

v	k	pub	A_1	A_2
9	3	[19]	✓	✓
16	4	[17]	✓	✓
25	4	[1, 2]	✓	✓
28	4	[17]	✓	✓
25	5	[17]	✓	✓
45	5	[17]	✓	✓
36	6	[4]	✓	✓
61	6	[15]	✓	✓
66	6	[4][13]	✓	✓
96	6	[4]	✓	✓

v	k	pub	A_1	A_2
43	7	[16]	✓	✓
49	7	[4]	✓	✓
85	7	[4]	✓	✓
127	7	[5]	✓	✓
133	7	here	✓	✓
175	7	here		✓
64	8	[4]	✓	✓
113	8	here	✓	✓
120	8	here	✓	✓
169	8	here		✓

v	k	pub	A_1	A_2
176	8	here		✓
81	9	[4]	✓	✓
145	9	here		✓
153	9	here		✓
100	10	[4]	✓	✓
181	10	here		✓
190	10	here		✓
111	11	[4]	✓	✓
121	11	[4]	✓	✓

A_2 obtained the new results by a parallel implementation in Java on the cores of a personal computer (with the AMD Ryzen 9 5900X 12-Core processor) within one day for all covered parameter sets except $(169, 7, 1)$ and $(175, 7, 1)$ each of which needed 2 weeks. A_2 works best when $k \geq 5$ and the number of the constructed CDFs is relatively small. In general it requires almost constant RAM being well parallelizable.

3. Results and open problems

The number of multipliers of the CDFs which have been classified by now is presented in Table 1, where $Aut_{\mathbb{Z}_v}$ is the number of automorphisms of $\mathbb{Z}_v$ and the papers which published the classification are presented in column *pub*, where *here* marks our new results. A mark in the column A_i means that we have repeated or obtained this result by the algorithm A_i. The whole number of CDFs with these parameters is given in column *CDFs* and the number of multipliers is presented as $M : N$, where N is the number of CDFs which have M multipliers (M is also the number of the multiplier automorphisms of the corresponding design). The small parameters for which no CDFs exist are presented in Table 2.

Since small errors in the software implementation of the algorithms are always possible, as a check for the correctness of the results, we repeat all previously known results from Tables 1 and 2, and obtain most of the new ones by each of the two different algorithms.

We think that the availability online of files with all nonequivalent CDFs with definite small parameters and their multipliers might be of particular interest for some possible applications, as well as for future theoretical research on the topic. The classification of CDFs with parameters not listed in Tables 1 and 2 is an open problem.

Acknowledgment: Part of the research that led to these results was carried out using the infrastructure purchased under the National Roadmap for RI, financially coordinated by the Ministry of Education and Science of the Republic of Bulgaria (grant No D01-98/26.06.2025).

References

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

[2] 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) 43–53.
[3] R. J. R. Abel, M. Buratti, Difference families, in: Ch. Colbourn Ch, J. Dinitz (Eds.), Handbook of Combinatorial Designs, 2nd edition, CRC Press, Boca Raton, FL. (2007).
[4] T. Baicheva, S. Topalova, Classification results for $(v, k, 1)$ cyclic difference families with small parameters, In: M. Deza, M. Petitjean, K. Markov (Eds.), International book series: Information Science and Computing, book 25 (2012) 24–30.
[5] T. Baicheva, S. Topalova, Classification of optimal $(v, k, 1)$ binary cyclically permutable constant weight codes with $k = 5$, 6 and 7 and small lengths, Des. Codes Cryptogr. 87 (2019) 365–374.
[6] T. Baicheva, S. Topalova, An update on optimal $(v, 4, 1)$ binary cyclically permutable constant weight codes and cyclic 2-$(v, 4, 1)$ designs with small v, Probl. Inf. Transm. 60(3) (2024) 189–198.
[7] V. N. Bhat-Nayak, V. D. Kane, W. L. Kocay, R. G. Stanton, Settling some BIBD conjectures, Ars Combin. 16 (1983) 229–234.
[8] R. C. Bose, On the construction of balanced incomplete block designs, Ann. Eugenics 9 (1939) 353–399.
[9] E. Brugnoli, M. Buratti, New designs by changing . . . the signs, Electron. Notes Discrete Math. 40 (2013), 49–52, doi:10.1016/j.endm.2013.05.010.
[10] M. Buratti, F. Martinovic, A. Nakic, $(27, 6, 5)$ designs with a nice automorphism group, Australasian Journal of Combinatorics 92(1) (2025), 80–95.
[11] M. Buratti, M. Muzychuk, Some bounds on the number of cyclic Steiner 2-designs, The Art of Discrete and Applied Mathematics 8 (2025) P1.01.
[12] Buratti M., Pasotti A., Further progress on difference families with block size 4 or 5, Des. Codes Cryptogr. 2010, vol. 56, pp. 1–20.
[13] M. Buratti, D. Stinson, New results on modular Golomb rulers, optical orthogonal codes and related structures, Ars Mathematica Contemporanea 20 (2021), 1–27.
[14] M. Buratti, A. Wassermann, On decomposability of cyclic triple systems, Australas. J. Comb. 71(2) (2018), 184–195.
[15] K. Chen, L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, Des. Codes Cryptogr. 15 (1998) 167–173.
[16] K. Chen, R. Wei, L. Zhu, Existence of $(q, 7, 1)$ difference families with q a prime power, J. Combin. Des. 10(2) (2002) 126–138.
[17] M. J. Colbourn, R. A. Mathon, On cyclic Steiner 2-designs, Ann. Discrete Math. 7 (1980) 215–253.
[18] C. J. Colbourn, On cyclic Steiner systems $S(2, 6, 91)$, Abstracts Amer. Math. Soc. 2 (1981).
[19] C. J. Colbourn, A. Rosa, Triple systems, Oxford University Press, Oxford (1999).
[20] 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) 2290–2294.
[21] I. Hetman, Steiner systems $S(2, 6, 121/126)$ based on difference families, arXiv:2401.08274 [math.CO] 9 Apr 2025.
[22] M. Huber, Perfect Secrecy Systems Immune to Spoofing Attacks, International Journal of Information Security 11 (2012) 281–289.
[23] Z. Janko, V. D. Tonchev, Cyclic $2-(91, 6, 1)$ designs with multiplier automorphisms, Discrete Math. 97(1) (1991) 265–268.
[24] P. Kaski, P. Östergård, Classification algorithms for codes and designs, Springer, Berlin (2006).
[25] Pálfy P., Isomorphism problem for relational structures with a cyclic automorphism, European J. Combin. 8 (1987) 35–43.
[26] H. Park, S. Hong, J.-S. No, D.-J. Shin, Construction of high-rate regular quasi-cyclic LDPC codes based on cyclic difference families, IEEE Trans. Commun. 61(8) (2013) 3108–3113.
[27] K.T. Phelps, Isomorphism Problems for Cyclic Block Designs, North-Holland Mathematics Studies 149 (1987), 385–391.
[28] M. Zhang, T. Feng, X. Wang, The existence of cyclic $(v, 4, 1)$-designs, Des. Codes Cryptogr. 90 (2022), 1611–1628.