Journal of Algebra Combinatorics Discrete Structures and Applications

On the resolutions of cyclic Steiner triple systems with small parameters*

Research Article

Svetlana Topalova

Abstract: The paper presents useful invariants of resolutions of cyclic $STS(v)$ with $v \leq 39$, namely of all resolutions of cyclic $STS(15)$, $STS(21)$ and $STS(27)$, of the resolutions with nontrivial automorphisms of cyclic $STS(33)$ and of resolutions with automorphisms of order 13 of cyclic $STS(39)$.

2010 MSC: 05B07, 05E18

Keywords: Resolutions, Cyclic designs, Point-cyclically resolvable, Cyclic $STS(v)$, $KTS(v)$

1. Introduction

1.1. Basic definitions and notations

For the basic concepts and notations concerning combinatorial designs and their resolvability refer, for instance, to [2], [3], [13], [22].

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*. If any 2-subset of V is contained in exactly λ blocks of $\mathcal{B}$, then $D = (V, \mathcal{B})$ is a 2-(v,k,λ) *design*, or *balanced incomplete block design (BIBD)*. Each point of D is incident with r blocks.

Two designs are *isomorphic* if there exists a one-to-one correspondence between the point and block sets of the first design and respectively, the point and block sets of the second design, and if this one-to-one correspondence does not change the incidence. An *automorphism* is an isomorphism of the design to itself, i.e. a permutation of the points that maps each block to a block of the same design.

A 2-(v,k,λ) design is *cyclic* if it has an automorphism permuting its points in one cycle of length v.

A *resolution* of the design is a partition of the collection of blocks into *parallel classes*, such that each point is in exactly one block of each parallel class. A design is *resolvable* if it has at least one resolution.

Two resolutions are *isomorphic* if there exists an automorphism of the underlying design which maps each parallel class of the first resolution to a parallel class of the second one. An *automorphism* of a resolution is an automorphism of the underlying design which maps each parallel class to a parallel class of the same resolution.

A resolution is *point-cyclic* if it has an automorphism permuting the points in one cycle. Only designs which are cyclic can have point-cyclic resolutions. A design is *point-cyclically resolvable* if it has at least one point-cyclic resolution.

A 2-$(v,3,1)$ design is called a Steiner triple system of order v ($STS(v)$) and its resolutions are called Kirkman triple systems of order v ($KTS(v)$).

1.2. Motivation and known results

Design resolutions have various important applications (see, for instance, [4], [9], [11], [19], [20], [21], [23]). Resolutions with rich automorphism groups might be very useful for some of them (For instance, point-cyclic resolutions of Steiner systems are used in some constructions of regular low-density parity-check codes providing a fast decoding algorithm [11] and of systematic repeat-accumulate codes [8]). That is why resolutions of cyclic designs are of particular interest and have been the subject of many papers.

General constructions of resolutions of cyclic designs are presented in [7], [14], [17], [18]. Cyclic $STS(v)$ are resolvable iff $v \equiv 3 \pmod 6$ and $v \geq 15$. There are several computer-aided classifications of $KTS(v)$ from cyclic designs. All resolutions of $STS(15)$ [12] and of cyclic $STS(21)$ [16] are known. The point-cyclic $KTS(21)$ and $KTS(39)$ are subject of [15], $KTS(33)$ with automorphisms of order 11 and cyclic underlying designs are constructed in [24] and the point-cyclic $KTS(27)$ are part of the constructed in [5] transitive $KTS(27)$. There exist many other works on $KTS(v)$ with $v \leq 39$, but the author does not know classification results for the rest of the cyclic $STS(v)$ cases considered below.

Subject of the present work is the classification of the resolutions of cyclic $STS(v)$ with small v. As it can be seen from the previous paragraph, not all of the results are new. The aim of the paper is on the one hand to obtain new $KTS(v)$ and on the other to present the properties of all known resolutions of cyclic $STS(v)$ with $v \leq 39$ and to make all of them available at a web-page for possible future applications.

2. Classification method

Cyclic 2-$(v,k,1)$ designs with small parameters were first classified in [6]. This classification was extended for some of the next parameters in [1]. Since all necessary designs are available, the focus of the present paper is only the construction and study of their resolutions. The resolutions of each cyclic $STS(v)$ are found in the following two ways.

2.1. Construction of all nonisomorphic resolutions

The blocks of the design are first sorted in lexicographic order and then backtrack search is applied on them. The parallel classes are constructed block by block. If n blocks have been added to a class, the $n + 1$-st one is chosen among the blocks which

- contain the smallest point that is in none of the already added blocks and

- contain no points which are in any of the added blocks.

The resolutions are thus constructed in lexicographic order. To make the classification feasible the algorithm is speeded up by performing a *minimality test* after adding each whole parallel class. This test checks if the current partial solution can be mapped to a lexicographically smaller one by some of the automorphisms of the design. If it can, an equivalent partial solution has already been considered and therefore the current one is rejected, namely a next possibility for the latest added block is looked for.

As a result all non isomorphic resolutions of the design are obtained.

2.2. Construction of all nonisomorphic resolutions with a given automorphism α of prime order p

There are two possibilities for the length of the parallel class orbits under α: length p and length 1 (fixed parallel classes). Since the number of parallel classes is $(v-1)/2$, there must be at least

$$c_f = \frac{v-1}{2} \ mod \ p$$

parallel classes which are fixed by α. The number of blocks in a parallel class is $v/3$ and therefore a fixed parallel class must contain at least

$$b_f = \frac{v}{3} \ mod \ p$$

fixed blocks. That is why with respect to α there must be

- at least $b_f c_f$ fixed blocks and

- at least $c_f(\left\lfloor \frac{v}{3p} \right\rfloor + b_f)$ block orbits such that any point is contained in at most one block of the orbit.

Therefore the algorithm starts with checking if these two conditions hold and stops if not. The construction algorithm itself is a modification of the general one described in the previous subsection. This modification adds more requirements, namely:

- Any two blocks of a non fixed parallel class should be from different orbits under α

- If a block is contained in a fixed parallel class, then all blocks of its orbit under α should be in the same parallel class

These requirements lead to a differently defined lexicographic order and respectively to a more complex minimality test which must take in account the orbit length (1 or p) under α of the added parallel classes.

3. Classification results

3.1. Resolution invariants

The blocks of all cyclic $STS(v)$ with $v \equiv 3 \pmod{6}$ are partitioned by the automorphism of order v in $(v-3)/6$ orbits of length v and one short block orbit of length $v/3$. Three types of point-cyclic resolutions of cyclic Steiner triple systems are defined in [17] with respect to the role of the short block orbit in the resolution. In a similar way we can define three types of resolutions (which may not be point-cyclic) as follows.

A resolution of a cyclic Steiner triple system is of type

- T_1 if the short orbit is a parallel class for all resolutions of the isomorphism class.

- T_2 if the short orbit is not a parallel class for any resolution of the isomorphism class.

- T_3 if the short orbit is a parallel class for some resolutions of the isomorphism class and is not a parallel class for the rest.

In the present paper the resolution type, the order of the full automorphism group and the orbits of this group on the parallel classes are found for each constructed resolution. The resolution properties are arranged in tables containing 8 columns. The first four of them contain the invariants which are computed for each resolution. Namely:

- $autD$ is the order of the full automorphism group of the design from which the resolution was obtained

- $autR$ is the order of the full automorphism group of the resolution

- T is the type of the resolution

- $orbR$ is the number of orbits of the parallel classes under the full automorphism group of the resolution

The number of solutions with such invariants is presented in the last four columns. Namely:

- D is the number of designs from which resolutions with these invariants are obtained

- $Dcyc$ is the number of those of the D designs which admit point-cyclic resolutions

- R is the number of resolutions with these invariants

- $Rcyc$ is the number of those of the R resolutions which are point-cyclic

Some comments on the properties of the constructed resolutions follow.

3.2. KTS(15)

All the 7 $KTS(15)$ are well known [12]. There are two cyclic $STS(15)$ with full automorphism groups of orders 60 and 20160. One of them is resolvable (Table 1) and this is the $STS(15)$ which can be obtained from the point-line incidence in $PG(3,2)$. There are two nonisomorphic resolutions which correspond to the two well-known doubly transitive parallelisms of $PG(3,2)$ [10]. The transitivity is, however, on the parallel classes ($orbR = 1$), while these resolutions are not point-cyclic.

Table 1.   **Resolutions of cyclic** $STS(15)$

autD	autR	T	orbR	D	Dcyc	R	Rcyc
20160	168	3	1	1	0	2	0

3.3. KTS(21)

There are 7 cyclic $STS(21)$ with full automorphism groups of orders 21, 42, 126(2), 504, 882 and 1008. Three of them are resolvable with 26 nonisomorphic resolutions constructed in [16] (Table 2). Two of them are point-cyclic and were obtained in [15] too. There are two other resolutions which have an automorphism group of order 21 but are not point-cyclic.

Table 2. **Resolutions of cyclic STS(21)**

autD	autR	T	orbR	D	Dcyc	R	Rcyc
126	9	2	4	1	0	3	0
126	63	2	2	1	1	1	1
882	3	2	4	1	0	1	0
882	9	3	4	1	0	1	0
882	21	2	2	1	0	1	0
882	63	3	2	1	1	1	1
1008	1	1	10	1	0	10	0
1008	3	1	6	1	0	7	0
1008	21	1	4	1	0	1	0
–	1	–	–	–	–	10	0
–	3	–	–	–	–	8	0
–	9	–	–	–	–	4	0
–	21	–	–	–	–	2	0
–	63	–	–	–	–	2	2
126	–	–	–	1	1	4	1
882	–	–	–	1	1	4	1
1008	–	–	–	1	0	18	0
–	–	–	–	3	2	26	2

3.4. KTS(27)

There are 8 cyclic $STS(27)$ with full automorphism groups of order 27. Four of them are resolvable yielding 19336 nonisomorphic resolutions (Table 3). None of them has a trivial automorphism group. Transitive $KTS(27)$ are constructed in [5] which intersect the constructed here $KTS(27)$ in the 4 point-cyclic ones.

Table 3. **Resolutions of cyclic STS(27)**

autD	autR	T	orbR	D	Dcyc	R	Rcyc
27	3	1	9	2	0	8	0
27	3	1	11	2	0	64	0
27	3	1	13	2	0	112	0
27	3	2	9	3	0	390	0
27	3	2	11	2	0	5088	0
27	3	2	13	2	0	13648	0
27	9	1	7	2	0	4	0
27	9	2	3	1	0	2	0
27	9	2	5	2	0	16	0
27	27	1	3	2	2	4	4
27	3	–	–	–	–	19310	0
27	9	–	–	–	–	22	0
27	27	–	–	–	–	4	4
27	–	–	–	4	2	19336	4

3.5. KTS(33)

There are 84 cyclic $STS(33)$ with full automorphism groups of orders 33(78), 66(3), 165(2) and 330(1). Seventy-nine of them possess altogether 28 resolutions with automorphisms of order 11 which were constructed in [24], 141022 resolutions with automorphisms of order 3 and 703296 resolutions with automorphisms of order 2. All the designs which have resolutions with automorphisms of order 11 possess resolutions with automorphisms of order 3 too, but they do not possess point-cyclic resolutions. The present investigation shows that all resolutions of cyclic $STS(33)$ have full automorphism groups of prime orders 11, 3 or 2 (Table 4). There are no resolutions with automorphisms of order 5.

Table 4. Resolutions of cyclic STS(33) with nontrivial automorphisms

autD	autR	T	orbR	D	Dcyc	R	Rcyc
33	11	1	6	13	0	18	0
33	11	2	6	8	0	10	0
33	3	2	8	76	0	127621	0
33	3	1	6	11	0	13	0
66	3	2	8	3	0	13388	0
66	2	1	11	3	0	7646	0
66	2	2	11	3	0	695650	0
–	11	–	–	–	–	28	0
–	3	–	–	–	–	141022	0
–	2	–	–	–	–	703296	0
33	–	–	–	76	0	127662	0
66	–	–	–	3	0	716684	0
–	–	–	–	79	0	844346	0

3.6. KTS(39)

There are 798 cyclic $STS(39)$ with full automorphism groups of orders 39(730), 78(4), 117(55), 156(2), 234(4), 468(2) and 3042(1). There are 375 of them which have resolutions with automorphisms of order 13 with no fixed points (Table 5). Note that an automorphism of order 13 with fixed points (one of the 798 cyclic designs possesses such a one) cannot fix any parallel class and thus cannot be an automorphism of a resolution. The number of resolutions with automorphisms of order 13 is 2827. There are 528 point-cyclic ones among them (constructed in [15]). Some of the other resolutions have a full automorphism group of order 39, but are not point-cyclic. Their underlying designs possess automorphism groups of orders 117, 234 and 3042. Only the resolutions of the design with an automorphism group of order 3042 are of type T_3.

4. Conclusion

The classified $KTS(v)$ with cyclic underlying designs can be of use both directly in relevant applications, and as parts of constructions of new infinite families. The results obtained in this paper coincide with those of other authors who have constructed part of the presented resolutions.

All computer results are obtained by C++ programs written by the author. Files with these resolutions can be downloaded from http://www.moi.math.bas.bg/∼ svetlana. They are available online to everybody who is interested and further investigations on their properties are possible.

Table 5.   Resolutions of cyclic STS(39) with automorphisms of order 13

autD	autR	T	orbR	D	Dcyc	R	Rcyc
39	13	1	7	187	0	769	0
39	13	2	7	44	0	601	0
39	39	2	3	252	252	462	462
117	13	1	7	21	0	327	0
117	13	2	7	13	0	354	0
117	39	1	7	20	0	33	0
117	39	1	5	28	0	50	0
117	39	2	7	9	0	14	0
117	39	2	5	19	0	23	0
117	39	2	3	22	8	42	20
117	117	2	3	27	27	41	41
234	13	1	7	4	0	39	0
234	13	2	7	4	0	55	0
234	39	1	7	3	0	3	0
234	39	1	5	2	0	2	0
234	39	2	5	2	0	3	0
234	39	2	3	2	2	2	2
234	117	2	3	1	1	2	2
3042	13	3	7	1	0	3	0
3042	39	3	7	1	0	1	0
3042	117	3	3	1	1	1	1
–	13	–	–	–	–	2148	0
–	39	–	–	–	–	635	484
–	117	–	–	–	–	44	44
39	–	–	–	322	252	1832	462
117	–	–	–	48	36	884	61
234	–	–	–	4	3	106	4
3042	–	–	–	1	1	5	1
–	–	–	–	375	292	2827	528

References

[1] T. Baicheva, S. Topalova, Classification results for (v, k, 1) cyclic difference families with small parameters, Mathematics of Distances and Applications. M. Deza, M. Petitjean, K. Markov (Eds.), in International book series: Information Science and Computing, 25 (2012), 24–30.

[2] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1993.

[3] C. J. Colbourn, J. H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 2007.

[4] C. J. Colbourn, J. H. Dinitz, D. R. Stinson, Applications of Combinatorial Designs to Communications, Cryptography, and Networking, Surveys in Combinatorics, 1999, Edited by J. D. Lamb and D. A. Preece, London Mathematical Society Lecture Note Series 267 (1999), 37–100.

[5] C. J. Colbourn, S. S. Magliveras, R. A. Mathon, Transitive Steiner and Kirkman triple systems of order 27, Math. Comp. 58(197) (1992) 441–449.

[6] M. J. Colbourn, R. A. Mathon, On cyclic Steiner 2-designs. Topics on Steiner systems, Ann. Discrete Math. 7 (1980) 215–253.

[7] M. Genma, M. Mishima, M. Jimbo, Cyclic resolvability of cyclic Steiner 2-designs, J. Combin. Des. 5(3) (1997) 177–187.

[8] A. Gruner, M. Huber, New combinatorial construction techniques for low-density parity-check codes and systematic repeat-accumulate codes, IEEE Trans. Commun. 60(9) (2012) 2387–2395.

[9] M. Huber, Combinatorial designs for authentication and secrecy codes, Found. Trends Commun. Inf. Theory 5(6) (2008) 581–675.

[10] N. L. Johnson, Two-transitive parallelisms, Des. Codes Cryptogr. 22(2) (2001) 179–189.

[11] S. J. Johnson, S. R. Weller, Resolvable 2-designs for regular low-density parity-check codes, IEEE Trans. Commun. 51(9) (2003) 1413–1419.

[12] S. Kageyama, A survey of resolvable solutions of balanced incomplete block designs, Int. Stat. Rev. 40(3) (1972) 269–273.

[13] P.Kaski, P.Östergård, Classification Algorithms for Codes and Designs, Springer, Berlin, 2006.

[14] C. Lam, Y. Miao, On cyclically resolvable cyclic steiner 2-designs, J. Combin. Theory Ser. A 85(2) (1999) 194–207.

[15] C. W. H. Lam, Y. Miao, Cyclically resolvable cyclic Steiner triple systems of order 21 and 39, Discrete Math. 219(1-3) (2000) 173–185.

[16] R. A. Mathon, K. T. Phelps, A. Rosa, A class of Steiner triple systems of order 21 and associated Kirkman systems, Math. Comp. 37(155) (1981) 209–222.

[17] M. Mishima, M. Jimbo, Some types of cyclically resolvable cyclic Steiner 2-designs, Congr. Numer. 123 (1997) 193–203.

[18] M. Mishima, M. Jimbo, Recursive constructions for cyclic quasiframes and cyclically resolvable cyclic Steiner 2-designs, Discrete Math. 211(1-3) (2000) 135–152.

[19] N. V. Semakov, V. A. Zinoviev, Equidistant $q-$ary codes with maximal distance and resolvable balanced incomplete block designs, Probl. Peredachi. Inf. 4(2) (1968) 3–10.

[20] T. Etzion, N. Silberstein, Codes and designs related to lifted MRD codes, IEEE Trans. Inform. Theory 59(2) (2013) 1004–1017.

[21] D. Stinson, Combinatorial Designs: Constructions and Analysis, Springer, New York, 2004.

[22] V. D. Tonchev, Combinatorial Configurations, Longman Scientific and Technical, New York, 1988.

[23] V. D. Tonchev, Steiner systems for two-stage disjunctive testing, J. Comb. Optim. 15(1) (2008) 1–6.

[24] V. D. Tonchev, S. A. Vanstone, On Kirkman triple systems of order 33, Discrete Math. 106/107 (1992) 493–496.