Resolutions of cyclic 2-(40,4,1) designs

Svetlana Topalova and Stela Zhelezova*
Bulgarian Academy of Sciences, Bulgaria

30th Applications of Computer Algebra - ACA 2025

Let V be a finite set of v *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite family of k-element subsets of V, called *blocks*. A pair $(V, \mathcal{B})$ is a *Steiner system* S$(2, k, v)$ (a 2-$(v, k, 1)$ design) if any 2-element subset of V is contained in exactly one block of $\mathcal{B}$. There are $|\mathcal{B}| = b = v(v-1)/k(k-1)$ blocks in an S$(2, k, v)$ and each point is in $r = (v-1)/(k-1)$ blocks.

Let $(V, \mathcal{B})$ and $(V', \mathcal{B}')$ be two Steiner systems S$(2, k, v)$. They are isomorphic if there is a permutation of the points $\phi : V \to V'$ which maps each block $B \in \mathcal{B}$ to a block $B' \in \mathcal{B}'$, $\phi(B) = B'$. An authomorphism of an S$(2, k, v)$ is an isomorphism to itself. A Steiner system S$(2, k, v)$ is cyclic if it has an authomorphism of order v permuting its points in one cycle.

The necessary condition for the existence of an S$(2, 4, v)$ is $v \equiv 1, 4 (\mathrm{mod}\ 12)$ and it is sufficient [4]. A cyclic S$(2, 4, v)$ exists for all possible v except for $v = 16, 25, 28$ [8].

A parallel class R_i, $i = \{1, \ldots, r\}$ in an S$(2, k, v)$ is a set of v/k blocks which partition the point set. An S$(2, k, v)$ is resolvable if the collection of its blocks can be partitioned to r parallel classes. Such a partition is called a resolution. Two resolutions are isomorphic if at least one automorphism of the underlying Steiner system maps each block of the first resolution to a block of the second one. An automorphism of a resolution is an isomorphism to itself. A resolvable Steiner system S$(2, 4, v)$ exists iff $v \equiv 4 (\mathrm{mod}\ 12)$ [5].

The most studied Steiner systems are the S$(2, 3, v)$s known as Steiner triple systems (STS(v)s). A considerable amount of research has been done on S$(2, 4, v)$s too. Their resolvability is in the focus of the present paper.

A cyclic Steiner system can be cyclically resolvable if at least one of its resolutions has an automorphism permuting the points in one cycle. Such a resolution is called point-cyclic and can exists for $v \equiv k (\mathrm{mod}\ k(k-1))$. The smallest set of parameters which fulfills the necessary conditions for the existence of cyclically resolvable S$(2, 4, v)$s is S$(2, 4, 40)$.

There is a construction of cyclically resolvable S$(2, k, v)$s for $v = ku$, u - a prime number [3]. The considered parameters do not match this construction. There are no cyclically resolvable Steiner systems among the cyclic S$(2, 4, 40)$s. Resolutions of S$(2, k, v)$s are of interest in connection with binary LDPC codes [6]. In that case cyclic Steiner systems are preferable because they might allow faster decoding. Thus when the point-cyclic resolutions are missing, the other resolutions of the cyclic S$(2, 4, v)$s are of particular interest.

There are 10 cyclic S$(2, 4, 40)$s. One of them is the point-line design of $PG(3, 3)$ with an automorphism group of order $12\,130\,560$. All its $73\,343$ resolutions have been recently constructed by Betten [1]. The other nine cyclic S$(2, 4, 40)$s are with automorphism groups of orders 40, 80, and

*This research is partially supported by the Bulgarian National Science Fund under Contract No KP-06-H62/2/13.12.2022.

160. We establish that three of them have altogether 1160 resolutions. We also investigate their automorphism groups and orbit structures.

Nowadays the role of computers in algebraic combinatorics is important. Computer algebra systems are used to generate new interesting combinatorial objects and to find some of their useful properties. GAP (Groups, Algorithms, Programs) [2] is a system designed to consider different problems in discrete mathematics. Information about some of the known examples of S$(2, 4, v)$s can be found in [7], where they are given in the format of the GAP Design package. We use the group theory functionality of GAP and our own C++ implementations of different algorithms for the construction of resolutions. This way we obtain all resolutions of the cyclic S$(2, 4, 40)$s.

References

[1] Betten, A. The packings of PG(3,3). *Des. Codes Cryptogr.* 79: 583–595, 2016.

[2] GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra, `http://www.gap-system.org/`. Last accessed: May 2025.

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

[4] Hanani, H. The existence and construction of balanced incomplete block designs. *Ann. Math. Stat.* 32: 361–386, 1961.

[5] Hanani, H., Ray-Chaudhuri, D.K., Wilson, R.M. On resolvable designs. *Discrete Math.* 3: 343–357, 1972.

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

[7] Krcadinac, V. Steiner 2-designs, `https://web.math.pmf.unizg.hr/~krcko/results/steiner.html`. Last accessed: May 2025.

[8] Zhang, M., Feng, T., Wang, X. The existence of cyclic $(v, 4, 1)$-designs. *Des. Codes Cryptogr.* 90: 1611–1628, 2022.