Classification of Cyclic Steiner Quadruple Systems

Yanxun Chang[*], Bingli Fan, Tao Feng[†]
Institute of Mathematics
Beijing Jiaotong University
Beijing 100044, P. R. China

Derek F. Holt
Mathematics Institute
University of Warwick
Coventry CV4 7AL, United Kingdom

Patric R. J. Östergård[‡]
Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 13000, 00076 Aalto, Finland

Abstract

The problem of classifying cyclic Steiner quadruple systems (CSQSs) is considered. A computational approach shows that the number of isomorphism classes of such designs with orders 26 and 28 is 52170 and 1028387, respectively. It is further shown that CSQSs of order $2p$, where p is a prime, are isomorphic iff they are multiplier equivalent. Moreover, no CSQSs of order less than or equal to 38 are isomorphic but not multiplier equivalent.

[*] Supported by NSFC under grant 11271042.
[†] Supported by NSFC under grant 11471032.
[‡] Supported in part by the Academy of Finland, Grant No. 289002.

1 Introduction

A *Steiner system* $S(t,k,v)$ is a pair $(X,\mathcal{B})$, where X is a set of v *points* and $\mathcal{B}$ is a set of k-subsets of X (called *blocks*) such that every t-subset of X is contained in a unique block. An $S(3,4,v)$ is called a *Steiner quadruple system* of order v, or briefly an SQS(v). A survey of Steiner quadruple systems can be found in [20]. It is known [18] that an SQS(v) exists if and only if

$$v \equiv 2,4 \pmod{6}. \tag{1}$$

Two Steiner systems $(X,\mathcal{A})$ and $(Y,\mathcal{B})$ are said to be *isomorphic* if there exists a bijection $\sigma : X \to Y$ such that $\{\{\sigma(x) : x \in A\} : A \in \mathcal{A}\} = \mathcal{B}$. Such a bijection from $(X,\mathcal{A})$ to itself is called an *automorphism*. The set of all automorphisms of a Steiner system forms a group under composition, the *automorphism group* of the system. Subgroups of the automorphism group are called *groups of automorphisms*.

A standard problem in design theory is that of classifying designs with specific parameters up to isomorphism [25]. Barrau [2] found the unique SQS(8) and SQS(10). Mendelsohn and Hung [34] showed that there are exactly four isomorphism classes of SQS(14)s, and Kaski, Östergård and Pottonen [26] computed the 1054163 isomorphism classes of SQS(16)s. When $v > 16$, only the asymptotic behaviour of the number of isomorphism classes is known [10, 32].

As the problem of classifying SQS(v)s for $v > 16$ does not seem feasible at the moment, one may consider the classification problem for a subset of those structures. An important class of Steiner systems (and designs in general) are the cyclic ones. A *cyclic* Steiner quadruple system, briefly CSQS(v), is an SQS $(X,\mathcal{B})$ of order v and with a cyclic group of automorphisms that acts regularly on X; in the sequel, such a group is called a regular cyclic group. Typically one lets $X = \{0,1,\ldots,v-1\}$ and considers the group $\mathbb{Z}_v$, the additive group of integers modulo v, as a group of automorphisms.

The necessary condition (1) for the existence of an SQS(v) is obviously also a necessary condition for the existence of a CSQS(v). However, the exact spectrum of parameters for which CSQS(v)s exist has not been determined; see [11] for recent results on the existence problem (for $v \le 100$, the only open case is currently $v = 94$). The following classification results are known. The unique SQS(10) found by Barrau [2] is cyclic, but the unique SQS(8) is not. By computer search, Guregová and Rosa [17] showed that neither a CSQS(14) nor a CSQS(16) exists. Phelps [36] proved that there are 29 isomorphism classes of CSQS(20)s. Finally, Frenz and Kreher [13] showed that there are 114 isomorphism classes of CSQS(22)s, thereby correcting an earlier erroneous result in [8]. One aim of the current paper is to extend these classification results.

The paper is organized as follows. In Section 2, the structure of CSQS(v)s is discussed. An algorithm for classifying CSQS(v)s up to multiplier equivalence is considered in Section 3, which also contains the results obtained by applying this algorithm to the cases of $v = 26$ and $v = 28$. The number of such structures is 52170 and 1028387, respectively. In Section 4, it is shown that there are no CSQS($2p$)s, p prime, that are isomorphic but not multiplier equivalent. Using this result and computational results based on a classification of transitive permutation groups, it is shown that no CSQSs of order less than or equal to 38 are isomorphic but not multiplier equivalent. Finally, some related combinatorial structures and particular subclasses of cyclic Steiner quadruple systems are discussed in Section 5.

2 Preliminaries

Consider a Steiner quadruple system $(\{0, 1, \ldots, v-1\}, \mathcal{B})$ with $\mathbb{Z}_v$ as a group of automorphisms. All blocks of this system are partitioned into orbits under the action of $\mathbb{Z}_v$, and the system is uniquely defined by taking one block, called a *base block*, from each orbit. We know by the Orbit–Stabilizer Theorem that the cardinality of such an orbit divides v. If the cardinality of the orbit is v, then the orbit is called *full*, otherwise it is called *short*. In the current work, we encounter short orbits of length $v/2$ and $v/4$; we call these *half* orbits and *quarter* orbits, respectively.

The normalizer of a subgroup $H \leq G$, denoted by $N_G(H)$, is defined as

$$N_G(H) = \{a \in G : aHa^{-1} = H\}.$$

When prescribing a group of automorphisms H of a design on v points, the normalizer of H in the symmetric group $G = S_v$ captures the remaining symmetries in the sense that elements of $N_G(H)$ map H-orbits onto H-orbits [25, Sect. 9.1].

The normalizer of $\mathbb{Z}_v$ in S_v, $N_{S_v}(\mathbb{Z}_v)$, is isomorphic to the semidirect product $\mathbb{Z}_v \rtimes \mathrm{Aut}(\mathbb{Z}_v)$ [9, Corollary 4.2B]. The automorphism group of $\mathbb{Z}_v$ is the multiplicative group of units in the ring of integers modulo v, which, for each $s \in \mathbb{Z}_v$ fulfilling $(s, v) = 1$, consists of a permutation $m_s : x \mapsto sx$. Such a permutation is called a *multiplier*, and if one Steiner quadruple system can be obtained from another by the action of a multiplier then the systems are said to be *multiplier equivalent.* An automorphism that is a multiplier is called a *multiplier automorphism.* Slightly abusing the language, we call both m_s and the parameter s multipliers. The multiplier 1 is called *trivial.*

Two multiplier equivalent cyclic Steiner quadruple systems are isomorphic, but isomorphic systems are not necessarily multiplier equivalent. The general question of existence of set systems that are isomorphic but not multiplier equivalent has been studied extensively.

Various sufficient condition for isomorphic structures to be multiplier equivalent have been obtained. For example, Bays [3] and Lambossy [31] showed that if p is a prime then isomorphic cyclic Steiner systems $S(t,k,p)$ are multiplier equivalent (a more general result was later obtained by Pálfy [35]). Examples of structures that are isomorphic but not multiplier equivalent have also been published: Brand [4] presented the first example of isomorphic cyclic Steiner systems that are not multiplier equivalent by finding such a family of $S(2,3,p^n)$s when $p \equiv 1 \pmod{6}$ is a prime and $n \geq 2$ (a simpler construction was later given by Phelps [37]).

For orders up to 22, for which the Steiner quadruple systems have been classified, isomorphic systems are multiplier equivalent [13, 36].

3 Classification Algorithm

An algorithm for classifying combinatorial structures consists of two main parts: constructing structures and removing isomorphs. We shall here discuss both parts and different approaches. For a general, in-depth consideration of these issues, see [25].

When a group of automorphisms has been prescribed, here $\mathbb{Z}_v$, one is facing the problem of selecting (all possible) sets of orbits under the action of the prescribed group that together form the desired structure. For designs with arbitrary parameters, this problem is conveniently formulated as a system of linear Diophantine equations (called the Kramer–Mesner method after the originators). The algorithm used in [13] is presented in this framework.

For Steiner systems, the following approach via instances of the exact cover problem is more specific than the Kramer–Mesner method and naturally leads to a state-of-the-art algorithm [28]. The algorithm discussed and used in [6, 36] for the classification of cyclic Steiner quadruple systems is essentially of this type (although considered in a somewhat different framework).

Given a set S and a collection $\mathcal{C}$ of subsets of S, the *exact cover problem* asks for a partitioning of S using elements in $\mathcal{C}$. To search for a Steiner system $(X, \mathcal{B})$ with parameters $S(t,k,v)$ and a prescribed group of automorphisms G, we produce the following instance.

We let S have one element for each orbit of t-element subsets of X under the action of G; let $T_1, T_2, \ldots, T_m$ be base blocks. There is further one element in $\mathcal{C}$ for each orbit $\mathcal{K}$ of k-element subsets of X that fulfills

$$|\{K \in \mathcal{K} : T_i \subseteq K\}| \leq 1$$

for all i, $1 \leq i \leq m$. If this condition is fulfilled, then we let the corresponding element (which itself is a set) of $\mathcal{C}$ consist of the t-element orbits for which $|\{K \in \mathcal{K} : T_i \subseteq K\}| = 1$. To find all possible solutions to instances of the exact cover problem, the libexact software [27] can be used.

Isomorph rejection—considered with respect to multiplier equivalence or isomorphism—should be carried out amongst the systems constructed in the above mentioned way. Classifying cyclic Steiner quadruple systems up to multiplier equivalence is computationally more straightforward, but finding the isomorphism classes is usually the main goal. (For the structures and parameters considered in the current work, these turn out to coincide, but this can obviously not be assumed a priori.)

Isomorph rejection can also be used earlier in the search to prune the search tree. In [6, 36], isomorph rejection (with respect to multiplier equivalence) is carried out already after having added the first orbit of 4-element subsets to the set of orbits (which are chosen in a particular way).

Here, as in [36], we first construct all possible sets of short orbits in a CSQS, and carry out isomorph rejection (with respect to multiplier equivalence) amongst all such sets before completing the systems. We call a fixed set of short orbits a *seed* for the final search. Before going into the details of the classification of CSQS(26)s and CSQS(28)s, let us briefly state some known results on the occurrence of short orbits.

The possible short orbits of a CSQS(v) are the following: the half orbits are of the form $\{\{i, j+i, v/2+i, v/2+j+i\} : 0 \leq i < v/2\}$ for some j, $1 \leq j < v/4$ and the unique quarter orbit is $\{\{i, v/4+i, v/2+i, 3v/4+i\} : 0 \leq i < v/4\}$. We denote a half orbit with parameter j by O_j.

Following Lindner and Rosa [33], we partition the admissible orders of CSQS(v)s into four classes:

A. $v \equiv 2, 10 \pmod{24}$;

B. $v \equiv 4, 20 \pmod{24}$;

C. $v \equiv 14, 22 \pmod{24}$;

D. $v \equiv 8, 16 \pmod{24}$.

Cyclic quadruple systems in classes B and D contain the unique quarter orbit while those in classes A and C do not. Systems in A and B (and C and D, respectively) contain an even (and odd, respectively) number of

Table 1: Distributions of orbit lengths

Case	Quarter	Half	Full
26.1	0	0	25
26.2	0	2	24
26.3	0	4	23
26.4	0	6	22
28.1	1	0	29
28.2	1	2	28
28.3	1	4	27
28.4	1	6	26
32.1	1	1	38
32.2	1	3	37
32.3	1	5	36
32.4	1	7	35

half orbits. The possible distributions of orbit lengths for the parameters considered here are shown in Table 1.

We shall next have a look at details of our classification of CSQS(26)s and CSQS(28)s. In the development of the approach, the cases of CSQS(20)s and CSQS(22)s were considered; our results corroborate those in [36] and [13] (mentioned in the Introduction). Classification with respect to multiplier equivalence is considered in Sects. 3.1 and 3.2, and isomorphism is treated in Sect. 4.

3.1 Classification of CSQS(26)s

A cyclic Steiner system CSQS(26) is in class A and therefore contains no quarter orbit and an even number of half orbits. Since there are $\lfloor(26-1)/4\rfloor = 6$ possible half orbits, there are 0, 2, 4, or 6 half orbits in a CSQS(26). See Table 1.

For $i = 0$, 2, 4, and 6 there are clearly $\binom{6}{i}$ ways to choose i out of 6 orbits, that is, 1, 15, 15, and 1 ways, respectively. For $v = 26$, there are $\phi(26) = 12$ multipliers, and 7 can be taken as a generator of the multiplicative group of units in the ring of integers modulo 26 (the group is cyclic as 26 is of the form $2p^k$, where p is an odd prime).

The 15 2-subsets of half orbits are themselves partitioned into three orbits under the action of the above mentioned group of units. These orbits have representatives $\{O_1, O_5\}$, $\{O_1, O_2\}$, and $\{O_1, O_3\}$ with lengths 3, 6, and 6, respectively. The complements of these orbits with respect to $\{O_1, O_2, O_3, O_4, O_5, O_6\}$ will obviously form three orbits of the 15 4-subsets of half orbits. As representatives, we take $\{O_1, O_2, O_3, O_5\}$, $\{O_1, O_2, O_3, O_4\}$, and $\{O_1, O_2, O_3, O_6\}$ with orbit lengths 3, 6, and 6, respectively.

Running the exact cover algorithm for eight seed cases gave the numbers in Table 2, where we also list the orders of the multiplier automorphism groups of the seeds, |Stab|. This computation took just over 2 core-hours using a 3.1-GHz Intel i5-2400 processor.

Table 2: Number of completed CSQS(26)s

Seed	|Stab|	N
$\emptyset$	12	304578
$\{O_1, O_5\}$	4	17208
$\{O_1, O_2\}$	2	18338
$\{O_1, O_3\}$	2	16920
$\{O_1, O_2, O_3, O_5\}$	4	3560
$\{O_1, O_2, O_3, O_4\}$	2	3186
$\{O_1, O_2, O_3, O_6\}$	2	2466
$\{O_1, O_2, O_3, O_4, O_5, O_6\}$	12	10180

Theorem 1. *There are exactly* 622522 *distinct* CSQS(26)*s.*

Proof. From the numbers in Table 2 and the orbit lengths of the seeds, we get the total number $304578 + 3 \cdot 17208 + 6 \cdot 18338 + 6 \cdot 16920 + 3 \cdot 3560 + 6 \cdot 3186 + 6 \cdot 2466 + 10180 = 622522$. □

We next consider the task of finding the multiplier equivalence classes. Since a multiplier maps an orbit of blocks to another orbit of the same length, the systems coming from different seeds cannot be multiplier equivalent. Moreover, in this isomorph rejection, one need consider only multiplier automorphisms of the seeds (which clearly have size $12/i$, where i is the orbit length).

In some cases it is possible to use theoretical arguments.

Theorem 2. *A* CSQS(v) *that has a half orbit cannot have* -1 *as a multiplier automorphism.*

Proof. Assume that $v - 1 = -1$ is a multiplier automorphism of a given CSQS(v). A triple $\{0, a, -a\}$, where $1 \leq a < v/4$ must be covered by some block $\{0, a, -a, x\}$, which the multiplier -1 maps to $\{0, a, -a, -x\}$. Unless $x = -x$, a triple is covered twice. The solutions to $2x = 0$ are $x = 0$ (which is not possible) and $v/2$, so there must be a block $\{0, a, v/2, -a\}$. But this is not possible if the system has a half orbit O_a with $1 \leq a < v/4$. □

Corollary 1. *A necessary condition for a* CSQS(v) *to have* -1 *as a multiplier automorphism is that* $v \equiv 2, 4, 10, \text{ or } 20 \pmod{24}$.

Corollary 2. *A* CSQS(26) *that is constructed from any of the seeds* $\{O_1, O_5\}$, $\{O_1, O_2\}$, $\{O_1, O_3\}$, $\{O_1, O_2, O_3, O_5\}$, $\{O_1, O_2, O_3, O_4\}$, *and* $\{O_1, O_2, O_3, O_6\}$ *cannot have nontrivial multiplier automorphisms.*

Proof. The multiplier automorphism group of $\{O_1, O_5\}$ and $\{O_1, O_2, O_3, O_5\}$ is a cyclic multiplicative group of order 4 with multipliers $\{1, 5, 21, 25\}$. The multiplier automorphism group of $\{O_1, O_2\}$, $\{O_1, O_3\}$, $\{O_1, O_2, O_3, O_4\}$, and $\{O_1, O_2, O_3, O_6\}$ is a group of order 2 with multipliers $\{1, 25\}$. Any nontrivial subgroups of these two groups contain the multiplier $25 = -1$, so the result follows from Theorem 2. □

In general, carrying out isomorph rejection with respect to multiplier equivalence is straightforward. For each CSQS(26) constructed, one simply applies all possible multipliers (there are 12 in total here, but the multiplier 1 can obviously be ignored), and the original system is accepted whenever none of the systems produced is lexicographically smaller than the original one [7]. When starting the search from a seed, one should restrict to multiplier automorphisms of the seed. For accepted systems, the order of the multiplier automorphism group is given by the number of systems produced that are identical to the original one.

Theorem 3. *There are exactly* 52170 *multiplier equivalence classes of* CSQS(26)*s.*

Proof. For the seeds $\emptyset$ and $\{O_1, O_2, O_3, O_4, O_5, O_6\}$, computer search shows that there are, respectively, 25668 and 855 multiplier equivalence classes of CSQS(26)s amongst the constructed ones, so the total number is (utilizing Corollary 2) $25668 + 17208/4 + 18338/2 + 16920/2 + 3560/4 + 3186/2 + 2466/2 + 855 = 52170$. □

To gain confidence in the correctness of the isomorph rejection for the seeds $\emptyset$ and $\{O_1, O_2, O_3, O_4, O_5, O_6\}$, we perform a consistency check that is based on double counting. Amongst the systems obtained from $\emptyset$, 4 admit a multiplier automorphism group of order 12 (generated by 7), 7 admit a group of order 6 (generated by 17), 106 admit a group of order 4 (generated by 5), 15 admit a group of order 3 (generated by 3), 375 admit a group of order 2 (generated by 25), and the remaining 25161 systems have no nontrivial multiplier automorphisms. The Orbit–Stabilizer Theorem then gives $1 \cdot 4 + 2 \cdot 7 + 3 \cdot 106 + 4 \cdot 15 + 6 \cdot 375 + 12 \cdot 25161 = 304578$, which coincides with the value in Table 2.

Similarly, amongst the systems obtained from $\{O_1, O_2, O_3, O_4, O_5, O_6\}$, 10 admit a multiplier automorphism group of order 3 (generated by 3) and the remaining 845 systems have no nontrivial multipliers. The Orbit–Stabilizer Theorem then gives $4 \cdot 10 + 12 \cdot 845 = 10180$, which also coincides with the value in Table 2.

3.2 Classification of CSQS(28)s

The classification of CSQS(28)s follows the approach in Section 3.1, so we shall here just mention the details that are specific for the current case. The CSQS(28)s are in class B and therefore contain the unique quarter orbit and an even number of half orbits (out of $\lfloor (28-1)/4 \rfloor = 6$ possible ones). Also now we have four cases with 0, 2, 4, and 6 half orbits, respectively. See Table 1.

For $v = 28$, there are $\phi(28) = 12$ multipliers, which form a noncyclic group. The group is generated by the multipliers 3 and 13 and is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_6$.

The seeds of the search, the orders of the multiplier automorphism groups of the seeds, |Stab|, and the number of completed systems in the computer search are shown in Table 3. The quarter orbit is included in all seeds. The computation took approximately 5 core-days using a 3.1-GHz Intel i5-2400 processor.

Using Table 3 and the Orbit–Stabilizer Theorem, we can now compute the total number of CSQS(28)s.

Theorem 4. *There are exactly* 12298370 *distinct* CSQS(28)*s.*

Proof. From the numbers in Table 3 and the orbit lengths of the seeds, we get the total number $5709310 + 3 \cdot (369854 + 401504 + 330570 + 365994 + 324836 + 70476 + 52830 + 53648 + 74168 + 72972) + 238504 = 12298370$. □

Analytic arguments can also here be used to find the number of equivalence classes with respect to multiplier equivalence. We start with a result that is well known and easy to prove.

Lemma 1. *Let P be a set of points fixed by a group of automorphisms of an* SQS(v)*. If $|P| \geq 3$, then the points in P induce an* SQS($|P|$)*.*

Table 3: Number of completed CSQS(28)s

Seed	|Stab|	N
$\emptyset$	12	5709310
$\{O_1, O_2\}$	4	369854
$\{O_1, O_3\}$	4	401504
$\{O_1, O_4\}$	4	330570
$\{O_1, O_6\}$	4	365994
$\{O_2, O_4\}$	4	324836
$\{O_1, O_2, O_3, O_4\}$	4	70476
$\{O_1, O_2, O_3, O_5\}$	4	52830
$\{O_1, O_2, O_3, O_6\}$	4	53648
$\{O_1, O_2, O_4, O_6\}$	4	74168
$\{O_1, O_2, O_5, O_6\}$	4	72972
$\{O_1, O_2, O_3, O_4, O_5, O_6\}$	12	238504

Lemma 2. *There is a* CSQS(v) *with* $v/2 + 1$ *as a multiplier automorphism only if there is a* CSQS($v/2$).

Proof. Since $2w(v/2+1) = vw + 2w \equiv 2w \pmod{v}$ and $(2w+1)(v/2+1) = vw + 2w + 1 + v/2 \equiv (2w+1) + v/2 \pmod{v}$, the multiplier $v/2 + 1$ fixes precisely the points with even labels, which induce an SQS($v/2$) by Lemma 1. Since $x \mapsto x + 2$ is an automorphism of the CSQS(v), the SQS($v/2$) must be cyclic. □

Lemma 3. *A* CSQS(28) *that is constructed from any of the seeds* $\{O_1, O_3\}$, $\{O_2, O_4\}$, $\{O_1, O_2, O_3, O_4\}$, $\{O_1, O_2, O_3, O_6\}$, *and* $\{O_1, O_2, O_5, O_6\}$ *cannot have nontrivial multiplier automorphisms.*

Proof. The multiplier automorphism group of all the listed seeds is isomorphic to the Klein group of order 4 and contains the multipliers $H = \{1, 13, 15, 27\}$. Consequently, the elements of H are the only possible multipliers automorphisms of a CSQS(28) constructed from the seeds.

By Theorem 2, $27 = -1$ is not a possible multiplier automorphism. As $15 = 28/2 + 1$, it follows from the nonexistence of a CSQS(14) and Lemma 2 that 15 is not a possible multiplier automorphism either.

For the multiplier 13, we consider $\mathbb{Z}_7 \times \mathbb{Z}_4$, which is isomorphic to $\mathbb{Z}_{28}$ via the mapping $i \mapsto i(1, 1)$. Then $13 \mapsto (-1, 1)$, and each base block is of one of the forms

$$\begin{array}{ll} \text{A:} & \{(*,a),(*,a),(*,a),(*,a)\}, \\ \text{B:} & \{(*,a),(*,a),(*,a),(*,b)\}, \\ \text{C:} & \{(*,a),(*,a),(*,b),(*,b)\}, \\ \text{D:} & \{(*,a),(*,a),(*,b),(*,c)\}, \\ \text{E:} & \{(*,a),(*,b),(*,c),(*,d)\}, \end{array}$$

where a, b, c, d are distinct. We denote the number of base blocks of these forms by x, y, z, u and w, respectively. All orbits of types A, B, and D are full. The quarter orbit is of type E and the half orbits are of types C (O_k, k even) and E (O_k, k odd). Let $z = z_1 + z_2$, where z_1 and z_2 are the number of base blocks that have full and half orbits, respectively.

Consider orbits of types $\{(*,a),(*,a),(*,a)\}$ and $\{(*,a),(*,a),(*,b)\}$, where a and b are distinct. All these orbits have length 28. For the former type, there are 4 ways to choose a and $\binom{7}{3}$ ways to choose the starred values, so the number of orbits is $\binom{7}{3} \cdot 4/28 = 5$. For the latter type, we similarly get $4 \cdot \binom{7}{2} \cdot 3 \cdot 7/28 = 63$ orbits.

When considering how triple orbits are covered by quadruple orbits, for the above mentioned two types of triple orbits we get the equations

$$\begin{aligned} &4x + y = 5, \\ &3y + 4z_1 + 2z_2 + 2u = 63. \end{aligned}$$

By combining these, we get that $-6x + 2z_1 + z_2 + u = 24$, that is, $z_2 + u$ must be even. We shall now show that u is odd, which implies that z_2 must be odd (which is not the case for the five seeds listed in the theorem).

Let $\mathrm{Orb}(S)$ denote the orbit of a set $S \subseteq \mathbb{Z}_7 \times \mathbb{Z}_4$ under the additive action of $(1,1)$. If $(-1,1)$ stabilizes an orbit of type D, then w.l.o.g.,

$$\begin{aligned} &\mathrm{Orb}(\{(0,a),(r,a),(s,b),(t,c)\}) = \\ &\mathrm{Orb}(\{(0,a),(-r,a),(-s,b),(-t,c)\}) = \\ &\mathrm{Orb}(\{(0,a),(r,a),(-s+r,b),(-t+r,c)\}), \end{aligned}$$

so $-s + r = s$ and $-t + r = t$, that is, $2s = 2t = r$, and consequently the orbit can be written as $\mathrm{Orb}(\{(0,a),(2s,a),(s,b),(s,c)\})$, a, b, c distinct. We shall count the number of orbits of type D stabilized by the multiplier $(-1,1)$, which has the same parity as u. Let us now focus on triple orbits $\mathrm{Orb}(\{(0,a),(2s,a),(s,b)\}$ (where we may have $a = b$). Note that these triple orbits are stabilized by the multiplier $(-1,1)$.

The triple orbit $\mathrm{Orb}(\{(0,a),(s,b),(2s,a)\})$ is covered by an orbit with the general form $\mathrm{Orb}(\{(0,a),(s,b),(2s,a),(r,c)\})$. By letting the multiplier

$(-1,1)$ act on this orbit, we get

$$\begin{aligned}&\mathrm{Orb}(\{(0,a),(-s,b),(-2s,a),(-r,c)\}) = \\ &\mathrm{Orb}(\{(0,a),(s,b),(2s,a),(-r+2s,c)\}).\end{aligned}$$

Since we have a quadruple system, we must have $r = -r+2s$, that is, $r = s$. Consequently, (1) if $a = b$, then for each $s = 1,2,3$, the system contains $\mathrm{Orb}(\{(0,a),(s,a),(2s,a),(s,c)\})$, which is of type B; (2) no matter whether $a = b$, each triple orbit $\mathrm{Orb}(\{(0,a),(s,b),(2s,a)\})$ must be covered by an orbit of type B or D.

In total there are 9 orbits $\mathrm{Orb}(\{(0,a),(s,b),(2s,a)\})$, $a \neq b$, 3 of which are covered by orbits of type $\mathrm{Orb}(\{(0,a),(s,a),(2s,a),(s,b)\})$, $a \neq b$, and $9-3 = 6$ of which are covered by orbits of type $\mathrm{Orb}(\{(0,a),(s,b),(2s,a),(s,c)\})$, a,b,c distinct. Since each orbit of the latter type covers 2 such triple orbits, there are exactly $6/2 = 3$ orbits of that type. This shows that u is odd and thereby completes the proof. □

By using Lemma 3 and computer search, the following result is obtained.

Theorem 5. *There are exactly* 1028387 *multiplier equivalence classes of* CSQS(28)*s.*

Proof. A computer search shows that amongst the designs constructed from the seeds $\emptyset$, $\{O_1,O_2\}$, $\{O_1,O_4\}$, $\{O_1,O_6\}$, $\{O_1,O_2,O_3,O_5\}$, $\{O_1,O_2,O_4,O_6\}$, and $\{O_1,O_2,O_3,O_4,O_5,O_6\}$, there are, respectively, 478896, 92533, 82699, 91642, 13233, 18570, and 19955 multiplier equivalence classes of CSQS(28)s, so the total number is (utilizing Lemma 3 and Table 3) $478896 + 92533 + 401504/4 + 82699 + 91642 + 324836/4 + 70476/4 + 13233 + 53648/4 + 18570 + 72972/4 + 19955 = 1028387$. □

Now the validation using the Orbit–Stabilizer Theorem goes as follows (cf. Table 3).

Amongst the systems obtained from $\emptyset$, 41 admit a group of order 6 (generated by 3), 192 admit a group of order 3 (generated by 9), 5916 admit a group of order 2 (generated by 27), and the remaining 472747 systems have no nontrivial multipliers. The Orbit–Stabilizer theorem then gives $2 \cdot 41 + 4 \cdot 192 + 6 \cdot 5916 + 12 \cdot 472747 = 5709310$. Amongst the systems obtained from $\{O_1,O_2\}$, 139 admit a multiplier automorphism group of order 2 (generated by 13), and 92394 have no nontrivial multipliers: $369854 = 2 \cdot 139 + 4 \cdot 92394$. Amongst the systems obtained from $\{O_1,O_4\}$, 113 admit a multiplier automorphism group of order 2 (generated by 13), and 82586 have no nontrivial multipliers: $330570 = 2 \cdot 113 + 4 \cdot 82586$.

Amongst the systems obtained from $\{O_1, O_6\}$, 287 admit a multiplier automorphism group of order 2 (generated by 13), and 91355 have no nontrivial multipliers: $365994 = 2 \cdot 287 + 4 \cdot 91355$. Amongst the systems obtained from $\{O_1, O_2, O_3, O_5\}$, 51 admit a multiplier automorphism group of order 2 (generated by 13), and 13182 have no nontrivial multipliers: $52830 = 2 \cdot 51 + 4 \cdot 13182$. Amongst the systems obtained from $\{O_1, O_2, O_4, O_6\}$, 56 admit a multiplier automorphism group of order 2 (generated by 13), and 18514 have no nontrivial multipliers: $74168 = 2 \cdot 56 + 4 \cdot 18514$. Finally, amongst the systems obtained from $\{O_1, O_2, O_3, O_4, O_5, O_6\}$, 8 admit a multiplier automorphism group of order 6 (generated by 5), 99 admit a multiplier automorphism group of order 3 (generated by 9), 14 admit a multiplier automorphism of order 2 (generated by 13), and 19834 have no nontrivial multipliers: $238504 = 2 \cdot 8 + 4 \cdot 99 + 6 \cdot 14 + 12 \cdot 19834$.

4 Isomorphisms of Cyclic Steiner Quadruple Systems

In Section 3, we enumerate all CSQS(v)s for $v = 26, 28$ up to multiplier equivalence. In this section we continue with the task of determining the number of isomorphism classes.

Pálfy [35] proved that whenever $v = 4$ or $\gcd(v, \phi(v)) = 1$, isomorphic cyclic objects over a set of size v are multiplier equivalent. Unfortunately, from (1) and the fact that $\phi(v)$ is even for $v \geq 3$, it follows that Pálfy's result is not applicable in the current work. Neither is the result by Huffman *et al.* [22] that isomorphism of cyclic objects over a set of size p^2, where p is a odd prime, can be checked using at most $\phi(p^2)$ permutations.

Consider cyclic objects over $\{0, 1, \ldots, pq - 1\}$, where p and q are distinct primes and $q < p$. We further assume that $\gcd(pq, \phi(pq)) \neq 1$, so that Pálfy's result cannot be used. Then $q \mid (p-1)$. In the current work, these conditions are fulfilled for $q = 2$ (in particular, $26 = 2 \cdot 13$). Huffman [21] derived a sufficient set of permutations for checking whether two cyclic objects with the given parameters are isomorphic. In the sequel, we fix q to 2 when describing the details of the approach. We introduce some definitions before proceeding:

$$\begin{aligned} T &= (0\ 1\ 2\ \cdots\ 2p-1), \\ \sigma_0 &= (0\ 2\ 4\ \cdots\ 2p-2), \\ \sigma_1 &= (1\ 3\ 5\ \cdots\ 2p-1). \end{aligned}$$

Obviously $T^2 = \sigma_0\sigma_1$. For $0 \leq i \leq 1$, $j \not\equiv 0 \pmod{p}$, $j \equiv 1 \pmod{2}$, we further define $\mu_{i,j}$, which maps $x \mapsto jx \pmod{2p}$ if $x \equiv i \pmod{2}$ and $x \mapsto x$

otherwise. The following result is [21, Theorem 1.1] for $q = 2$.

Theorem 6. *Let $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ be cyclic Steiner quadruple systems of order $2p$, p prime, and with T as an automorphism. If -1 is not a multiplier for $(X, \mathcal{A})$, then $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are isomorphic iff they are multiplier equivalent.*

Theorem 6 already takes care of all but $4 + 7 + 106 + 375 = 492$ of the multiplier equivalence classes of CSQS(26)s. We need some further definitions to proceed with the case when -1 is a multiplier. Let g be an element of order $p - 1$ in the multiplicative group of units in the ring of integers modulo $2p$, and let s be the unique solution to $s \equiv (p + 1)/2 \pmod{p}$ when $s \in \{1, g, g^2, \ldots, g^{p-2}\}$. Further let $\nu_0 = m_s$ and $\nu_1 = \mu_{0,s}\mu_{1,-s}$.

Lemma 4. *A* CSQS($2p$)*, p an odd prime, cannot have σ_0 as an automorphism.*

Proof. The permutation σ_0 fixes exactly p elements. Those elements induce an SQS(p) by Lemma 1. However, Steiner quadruple systems of odd order do not exist by (1). □

We have the following useful result, based on the results of [21] and the presentation in [30].

Theorem 7. *Let $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ be cyclic Steiner quadruple systems of order $2p$, p prime, and with T as an automorphism. Assume that m_{-1} is a multiplier automorphism of $(X, \mathcal{A})$, and let α be the smallest positive integer such that m_g^α is a multiplier automorphism of $(X, \mathcal{A})$. To determine isomorphism of $(X, \mathcal{A})$ and $(Y, \mathcal{B})$, it suffices to let the following permutations act on $(X, \mathcal{A})$ and check whether the result is $(Y, \mathcal{B})$: $m_g^i \nu_j$, where $0 \leq i < \alpha$, $0 \leq j \leq 1$. Moreover, $\sigma_0^{-1}\sigma_1$ has to be an automorphism if $j = 1$.*

Proof. In [21], the general case of order pq is considered and split into two cases, depending on whether σ_0 is an automorphism [21, Theorem 1.3] or not [21, Theorem 1.2]. By Lemma 4 we know that σ_0 is not an automorphism, so the result is [21, Theorem 1.2] (and [30, Theorem 4.3]) for $q = 2$. □

Note that Theorem 7 finds isomorphisms also for objects that are multiplier equivalent. If we are only interested in checking automorphism for CSQSs that are not multiplier equivalent, then it suffices to consider the cases with $j = 1$ in the theorem. Actually, such a consideration leads to the following theorem:

Theorem 8. *Let $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ be cyclic Steiner quadruple systems that both have order $2p$, p prime, and T as an automorphism. Then $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are isomorphic iff they are multiplier equivalent.*

Proof. The permutations to test in Theorem 7 are multipliers if $j = 0$, so we may focus on the permutations for $j = 1$. For $j = 1$, there is the condition that $\sigma_0^{-1}\sigma_1$ be an automorphism of the CSQS $(X, \mathcal{A})$. Consider a triple $\{a, b, c\}$, with a, b, and c even. This triple must be covered by some block $\{a, b, c, d\}$.

Assume that d is odd. Since $\sigma_0^{-1}\sigma_1$ is an automorphism, $\{a-2, b-2, c-2, d+2\}$ must be a block, and since the system is cyclic this further implies that $\{a, b, c, d+4\}$ is a block. Then, since $d \neq d+4$, $\{a, b, c\}$ is covered by two blocks, which is not possible.

If all triples with even points are covered by blocks with only even points, then the even points induce a CSQS(p), p prime (Lemma 1; it is further clear that it must be cyclic). Such a design cannot exist by (1). □

Theorem 8 handles the case of $v = 26$ in the current work, as well as corroborates the earlier result [13] that CSQS(22)s are isomorphic iff they are multiplier equivalent.

For the order $v = 28$, which is of the form pq^2, p, q primes, we do not have results as strong as Theorem 8, so some investigation of the constructed systems is needed. However, instead of trying to find isomorphisms between constructed systems, we take a different approach and attack the problem of finding isomorphic multiplier inequivalent systems separately from the main computer search.

For isomorphic multiplier inequivalent systems, the automorphism group must have regular cyclic subgroups that are not conjugate. This result occurs in various forms in many places in the literature, such as [1, Lemma 3.1], [30, Lemma 4.4], and [35, Lemma 0.1], and it actually played a central role already in work by Bays [3].

For a given order v, the search now proceeds in the following way: for (i) each transitive permutation group G of degree v, we (ii) check whether it has regular cyclic subgroups that are not conjugate, and, if so, (iii) exhaustively search for systems with automorphism group G.

In (i), it suffices to consider the groups up to conjugacy in S_v. The transitive permutation groups have been classified up to degree 32, see [5, 23] (and this work has recently been extended to degree 47), so these groups are readily available. For (ii), we first use standard Magma functions to find the conjugacy classes of elements of order v in G, then we select those that consist of a single v-cycle, and hence generate a regular cyclic subgroup, and finally we test the subgroups that they generate for conjugacy in G. If there is more than one conjugacy class in G of regular cyclic subgroups, then we proceed to (iii).

The number of permutation groups with nonconjugate regular cyclic subgroups is given in column N of Table 4. In column N', we further show the number of permutation groups with several conjugate regular cyclic subgroups (but with no pair of nonconjugate such subgroups, that is, excluding the groups enumerated under N). For completeness, these numbers are listed for all degrees up to 32. Notice that N is 0 exactly when the degree $d = 4$ or d and $\varphi(d)$ are coprime [35].

Table 4: Permutation groups with more than one regular cyclic subgroup

Degree	N	N'	Degree	N	N'
1	0	0	17	0	5
2	0	0	18	130	135
3	0	0	19	0	2
4	0	1	20	102	222
5	0	2	21	22	92
6	1	6	22	5	26
7	0	3	23	0	3
8	5	10	24	1359	2043
9	8	8	25	53	53
10	5	15	26	17	31
11	0	4	27	304	118
12	12	79	28	84	507
13	0	3	29	0	2
14	5	28	30	575	1290
15	0	70	31	0	4
16	179	115	32	26655	4341

If the automorphism group of an CSQS(v) is larger than its multiplier automorphism group, then the group has more than one regular cyclic subgroup. Phelps [36] pointed out that the automorphism group of the unique CSQS(10) is the projective general linear group PGL(2,9). In general, for $k > 0$ there is an CSQS($3^k + 1$) with PGL$(2, 3^k)$ as the automorphism group. (Automorphism groups are not studied further in this paper.)

If there exist isomorphic multiplier inequivalent CSQS(28)s, they must have an isomorphism group that is one of the 84 groups listed in column N of Table 4. Moreover, by Lemma 1 it suffices to consider groups whose subgroups fulfill the property that the number of fixed points be less than 3 or according to (1). This leaves 8 groups, which have the following numbering amongst the transitive groups of degree 28 in GAP and Magma: 51, 91, 128, 131, 204, 205, 249, 326. For completeness, we list (generators of) the groups in the Appendix. An exhaustive search—which is fast as the groups are large—shows that there are no CSQS(28)s with such groups of automorphisms.

We now turn to the case of CSQS(32)s.

Theorem 9. *A* CSQS($8m$) *cannot have* $4m-1$ *as a multiplier automorphism.*

Proof. Let $v = 8m$. For the multiplier $4m-1$ to fix a point $2w$, we get by $2w(4m-1) = 8mw - 2w \equiv -2w \pmod{8m}$ that $4w \equiv 0 \pmod{8m}$. Consequently, exactly the points $2w = 0$ and $2w = 4m$ are fixed in this manner. On the other hand, for the multiplier $4m-1$ to fix $2w+1$, we get by $(2w+1)(4m-1) = 8mw + 4m - 2w - 1 \equiv -(2w+1) + 4m \pmod{8m}$ that $2(2w+1) \equiv 4m \pmod{8m}$. This equation has no solution since $2w+1$ is odd.

As $(4m-1)(4m-1) \equiv 1 \pmod{8m}$ and the multiplier $4m-1$ fixes exactly the points 0 and $4m$, the derived triple system associated with 0 must have an automorphism of order 2 with 1 fixed point. A necessary condition for the existence of such triple systems, called reverse, on u points is that $u \equiv 1, 3, 9,$ or $19 \pmod{24}$ [39]. See also [20, p. 213]. Hence $8m \equiv 2, 4, 10,$ or 20 (mod 24), which is impossible. □

The following result due to Phelps is mentioned without proof in [16].

Theorem 10. *A* CSQS(32) *cannot have a nontrivial multiplier automorphism.*

Proof. The units in the ring of integers modulo 32 are the odd numbers, and these form a multiplicative group of order 16 that is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_8$. Consequently, any nontrivial subgroup of this group has an element of order 2. This means that if the design has a nontrivial multiplier automorphism, then either 15, 17, or 31 is a multiplier automorphism.

The fact that multiplier automorphisms 15 and $31 = -1$ are not possible is taken care of by Theorem 9 and Corollary 1, respectively. Finally, it follows from the nonexistence of a CSQS(16) and Lemma 2 that 17 is not a possible multiplier automorphism either. □

An easy calculation in Magma shows that, in each of the 26655 groups G listed in column N for degree 32, all of the regular cyclic subgroups C

of order 32 are normalized by an element in G that induces a nontrivial automorphism of C. This can also be deduced from the even-easier-to-verify fact that these groups all have orders divisible by 64. So, in each case, C is properly contained in a Sylow 2-subgroup S of G [40, Theorems 4.12, 4.14] and then, by [40, Theorem 4.6], C is properly contained in its normalizer $N_S(C)$ in S. But, as we observed in Section 2, the normalizer of C in the symmetric group S_{32} is equal to the semidirect product $C \rtimes \mathrm{Aut}(C)$. So an element of $N_S(C) \setminus C$ must induce a nontrivial automorphism of C. We conclude that there are no isomorphic multiplier inequivalent CSQS(32)s.

Theorem 8 takes care of the orders 34 and 38, so we now have the following result.

Theorem 11. *There are no isomorphic multiplier inequivalent* CSQS(v)*s for* $v \leq 38$.

The next orders to consider in a search for isomorphic multiplier inequivalent CSQS(v)s are $v = 40$, $v = 44$, and $v = 50$. Phelps [38] proved that isomorphic multiplier inequivalent cyclic designs exist for many parameters, including $S(2, k, v)$s for $k \geq 3$ and infinitely many values of v. However, for $t = 3$, the question remains open.

5 Related Designs

Since there are no isomorphic multiplier inequivalent CSQS(v)s with the parameters considered in the current study, we need not separately address the issues of isomorphism and multiplier equivalence when discussing particular subsets of such systems.

There are several types of designs that are closely related to cyclic Steiner quadruple systems. One example of such designs are cyclic H-designs. The concept of H-designs originates from work by Hanani [19]. An *H-design* is a triple $(X, \mathcal{G}, \mathcal{B})$, where $\mathcal{G}$ is a partition of a set of points X into n subsets (called *groups*), each of cardinality g, and $\mathcal{B}$ is a collection of k-subsets of X (called *blocks*), such that each block intersects any given group in at most one point, and each t-subset of X with points from distinct groups is contained in a unique block. An H-design with these parameters is denoted by $H(n, g, k, t)$. An H-design is also known as a *group divisible t-design.*

An *automorphism* of an H-design $(X, \mathcal{G}, \mathcal{B})$ is a permutation on X leaving $\mathcal{G}$ and $\mathcal{B}$ invariant. An H-design with n groups of cardinality g is said to be *cyclic* if it admits an automorphism consisting of a cycle of length gn. Without loss of generality, we may identify X with $\mathbb{Z}_{gn}$ and $\mathcal{G}$ with $\{\{i, n + i, \ldots, (g-1)n + i\} : 0 \leq i \leq n-1\}$.

Let $v \equiv 2, 4 \pmod{6}$ and $\mathcal{A} = \{\{0, j, v/2, v/2 + j\} : 1 \leq j \leq \lfloor v/4 \rfloor\}$. Consider a cyclic $H(v/2, 2, 4, 3)$ with a set $\mathcal{C}$ of base blocks. It is readily checked that $\mathcal{A} \cup \mathcal{C}$ forms a set of base blocks of a CSQS(v) that has $\lfloor v/4 \rfloor$ short orbits. Conversely, by reversing the above process, a CSQS(v) having $\lfloor v/4 \rfloor$ short orbits yields a cyclic $H(v/2, 2, 4, 3)$. For example, the proofs of Theorems 3 and 5 can be utilized to classify cyclic H-designs corresponding to CSQS(26)s and CSQS(28)s.

We shall next prove a nonexistence result for H-designs. An H-design is said to be *semi-cyclic* if it admits an automorphism consisting of n cycles of length g.

Theorem 12. *There is no cyclic* $H(v/2, 2, 4, 3)$ *for* $v \equiv 14, 22 \pmod{24}$.

Proof. The strategy is to prove that there is no semi-cyclic $H(v/2, 2, 4, 3)$ for $v \equiv 14, 22 \pmod{24}$. If there is a cyclic $H(v/2, 2, 4, 3)$, then there is a semi-cyclic $H(v/2, 2, 4, 3)$, so nonexistence of semi-cyclic $H(v/2, 2, 4, 3)$s implies nonexistence of cyclic $H(v/2, 2, 4, 3)$s.

Let $(X, \mathcal{G}, \mathcal{B})$ be an $H(n, g, 4, 3)$. We identify X with $\mathbb{Z}_n \times \mathbb{Z}_g$ and $\mathcal{G}$ with $\{\{i\} \times \mathbb{Z}_g : i \in \mathbb{Z}_n\}$. In this case the automorphism can be taken as $(i, x) \mapsto (i, x + 1)$.

Let $v = 2n$ with $n \equiv 7, 11 \pmod{12}$. Consider a semi-cyclic $H(n, 2, 4, 3)$ on $\mathbb{Z}_n \times \mathbb{Z}_2$ with base blocks of the form $\{(i_1, *), (i_2, *), (i_3, *), (i_4, *)\}$. Note that i_1, i_2, i_3, i_4 are distinct as we have an H-design. Assuming that $i_1 < i_2 < i_3 < i_4$, each base block must be one of the following:

$$\begin{array}{l}
\{(i_1,0),(i_2,0),(i_3,0),(i_4,0)\},\ \{(i_1,0),(i_2,0),(i_3,0),(i_4,1)\},\\
\{(i_1,0),(i_2,0),(i_3,1),(i_4,0)\},\ \{(i_1,0),(i_2,1),(i_3,0),(i_4,0)\},\\
\{(i_1,1),(i_2,0),(i_3,0),(i_4,0)\},\ \{(i_1,0),(i_2,0),(i_3,1),(i_4,1)\},\\
\{(i_1,0),(i_2,1),(i_3,0),(i_4,1)\},\ \{(i_1,0),(i_2,1),(i_3,1),(i_4,0)\}.
\end{array}$$

Denote the number of base blocks of these forms by x_j, $j = 1, 2, \ldots, 8$, respectively. The number of triple orbits of the form $\mathrm{Orb}(\{(i, 0), (i', 1), (i'', 0)\})$, where $i < i' < i''$ are distinct, is now $\binom{n}{3} = n(n-1)(n-2)/6$, which is odd. The number is also obtained as $2x_3 + 2x_4 + 2x_7 + 2x_8$, which is even, so we have a contradiction. □

Corollary 3. *There is no* CSQS(v) *for* $v \equiv 14, 22 \pmod{24}$ *with* $(v-2)/4$ *half orbits.*

Corollary 3 shows, for example, that no CSQS(22) with 5 half orbits exists.

If all orbits of a CSQS(v) are full, then we have a *strictly cyclic* Steiner quadruple system of order v, briefly sSQS(v). It is known that sSQS(v)s exists only if $v \equiv 2, 10 \pmod{24}$; see [12] and the references therein for more information on strictly cyclic Steiner quadruple systems. The proof of Theorem 3 establishes a complete classification of sSQS(26)s, which is the next open case after $v = 10$. The unique sSQS(10) was found already by Barrau [2].

Theorem 13. *There are exactly* 25668 *isomorphism classes of* sSQS(26)*s.*

A CSQS(v) with -1 as a multiplier automorphism is said to be *R-cyclic*, cf. [20]. The unique CSQS(10) is R-cyclic, and there are exactly 4 isomorphism classes of R-cyclic CSQS(20)s [36].

Theorem 14. *There are exactly* 492 *isomorphism classes of R-cyclic* CSQS(26)*s and* 5957 *isomorphism classes of R-cyclic* CSQS(28)*s.*

Proof. By the discussion after Theorem 3 and Theorem 5, the number of isomorphism classes of R-cyclic CSQS(26)s and CSQS(28)s are $4 + 7 + 106 + 375 = 492$ and $41 + 5916 = 5957$, respectively. □

By Theorem 2, a CSQS(v) with a half orbit cannot have -1 as a multiplier automorphism, so CSQSs in Classes C and D cannot be R-cyclic. Thus $v \equiv 2, 4, 10, 20 \pmod{24}$ is a necessary condition for an R-cyclic SQS(v) to exist.

A CSQS(v) is said to be *S-cyclic* if the multiplier -1 fixes each block orbit. Obviously an S-cyclic system is R-cyclic. The following result is from [14].

Theorem 15. *An S-cyclic* CSQS(v) *can exist only if* $v = 2n$ *or* $4n$*, where every prime factor* p *of* n *satisfies* $p \equiv 1$ or $5 \pmod{12}$*.*

The unique CSQS(10) is S-cyclic. There is a unique S-cyclic SQS(20) [24]. By examining the 492 R-cyclic CSQS(26)s, we were able to corroborate the following result, originally published in [15].

Theorem 16. *There are exactly* 18 *isomorphism classes of S-cyclic* CSQS(26)*s.*

A CSQS(v) is said to be *affine-invariant* if it admits all elements of the multiplicative group of units in the ring of integers modulo v as multiplier automorphisms, cf. [29]. Obviously an affine-invariant CSQS(v) is R-cyclic. The unique CSQS(10) is affine-invariant. By [36], there is no affine-invariant CSQS(20). By the discussion after Theorem 3, there are exactly 4 isomorphism classes of affine-invariant CSQS(26)s.

Lemma 5. *If there exists an affine-invariant* CSQS(v) *for* $v \equiv 4, 20 \pmod{24}$*, then there exists an affine-invariant* CSQS$(v/2)$*.*

Proof. When $v \equiv 4, 20 \pmod{24}$, $v/2 + 1$ is coprime with v. By Lemma 2, a CSQS(v) with $v/2+1$ as a multiplier automorphism implies a CSQS$(v/2)$. □

Lemma 6. *Suppose that there exists an affine-invariant* CSQS(v) *for* $v \equiv 2, 10 \pmod{24}$*. Write* $v = 2pn$*, where* p *is an odd prime and* n *is an odd integer. Then there exists an affine-invariant* CSQS$(2n)$*.*

Proof. The triple orbit Orb$(\{0, ap, bp\})$, $a \neq b$, is covered by an orbit that has the general form Orb$(\{0, ap, bp, \alpha + \beta p\})$, where $0 \leq \alpha < p$ and $0 \leq \beta < 2n$. It is readily checked that there exists a c satisfying $\gcd(1 + 2cn, v) = 1$ and $\gcd(c, p) = 1$ (take $c = (p + 1)/2$ or $c = (p - 1)/2$). Thus $1 + 2cn$ can be taken as a multiplier automorphism and Orb$(\{0, ap, bp, \alpha + \beta p\}) =$ Orb$(\{0, ap, bp, \alpha + \beta p + 2cn\alpha)\})$. Since we have a quadruple system, we must have $2cn\alpha \equiv 0 \pmod{2pn}$, which implies $\alpha = 0$. This procedure induces an affine-invariant CSQS$(2n)$. □

Theorem 17. *An affine-invariant* CSQS(v) *can exist only if* $v = 2n$ *or* $4n$*, where every prime factor* p *of* n *satisfies* $p \equiv 1$ or $5 \pmod{12}$*.*

Proof. By Theorem 2, a CSQS(v) that has a half orbit cannot have -1 as a multiplier automorphism. Thus if an affine-invariant CSQS(v) exists, then $v \equiv 2, 4, 10, 20 \pmod{24}$. A combination of Lemmas 5 and 6 completes the proof. □

By Theorem 17, there is no affine-invariant CSQS(28) (which we already know from the discussion after Theorem 5). Theorem 10 implies that a CSQS(32) cannot be R-cyclic, and thereby it can be neither S-cyclic nor affine-invariant. It also follows from Theorems 15 and 17 that a CSQS$(8n)$ can be neither S-cyclic nor affine-invariant. The similarity between Theorems 15 and 17 brings about the question whether an affine-invariant CSQS(v) is always S-cyclic. However, it turns out that none of the affine-invariant CSQS(26)s is S-cyclic.

Appendix

The eight groups needed to determine whether there are isomorphic multiplier inequivalent SQS(28)s are as follows. For each group, we give the number in GAP and Magma, the order of the group, and generators of the group (acting on $\{1, 2, \ldots, 28\}$).

Number = 51
Order = 392
Generators:
(1,8,14,20,25,4,10,15,22,27,5,12,17,23,2,7,13,19,26,3,9,16,21,28,6,11,18,24),
(1,25)(2,26)(3,7)(4,8)(5,21)(6,22)(9,17)(10,18)(11,27)(12,28)(15,24)(16,23).

Number = 91
Order = 784
Generators:
(1,6)(2,5)(7,14)(8,13)(9,12)(10,11)(15,28)(16,27)(17,25)(18,26)(19,23)(20,24),
(1,11,7,4,14,10,6,2,12,8,3,13,9,5),
(1,21,14,24,12,25,9,28,7,15,6,17,3,20)(2,22,13,23,11,26,10,27,8,16,5,18,4,19).

Number = 128
Order = 1176
Generators:
(1,13,22,17,6,25)(2,14,21,18,5,26)(3,7,20,28,24,12)(4,8,19,27,23,11),
(1,27,21,15,17,23,2,28,22,16,18,24)(3,13,4,14)(5,20,9,11,26,7,6,19,10,12,25,8).

Number = 131
Order = 1176
Generators:
(1,8,18,3,6,27,21,24,9,19,26,15,13,11,2,7,17,4,5,28,22,23,10,20,25,16,14,12),
(1,20,10,27,17,7,26,16,6,24,14,4,22,12,2,19,9,28,18,8,25,15,5,23,13,3,21,11),
(1,25)(2,26)(3,12)(4,11)(5,21)(6,22)(9,17)(10,18)(15,28)(16,27)(19,23)(20,24).

Number = 204
Order = 2352
Generators:
(15,16)(17,18)(19,20)(21,22)(23,24)(25,26)(27,28),
(1,9,12)(2,10,11)(3,14,6)(4,13,5)(15,18,21,16,17,22)(19,25,23,20,26,24)(27,28),
(1,13)(2,14)(3,11)(4,12)(5,9)(6,10)(7,8)(15,17)(16,18)(19,27)(20,28)(21,25)(22,26),
(1,22,2,21)(3,23,4,24)(5,25,6,26)(7,27,8,28)(9,16,10,15)(11,17,12,18)(13,20,14,19).

Number = 205
Order = 2352
Generators:
(1,11,14,5,9,8)(2,12,13,6,10,7)(3,4)(15,24,21,25,17,20)(16,23,22,26,18,19),
(1,21,2,22)(3,17,4,18)(5,27,6,28)(7,24,8,23)(9,20,10,19)(11,16,12,15)(13,26,14,25),
(1,28,10,16,3,17,11,19,6,21,13,23,7,25,2,27,9,15,4,18,12,20,5,22,14,24,8,26).

Number = 249
Order = 3528
Generators:
(1,5)(2,6)(3,4)(7,23,20,27,12,16)(8,24,19,28,11,15)(9,26)(10,25)(13,21)(14,22)(17,18),
(1,24,14,19,25,15,10,11,22,7,5,4,17,28,2,23,13,20,26,16,9,12,21,8,6,3,18,27).

Number = 326
Order = 7056
Generators:
(1,13)(2,14)(3,11)(4,12)(5,9)(6,10)(7,8)(17,21,20,28,24,25)(18,22,19,27,23,26),
(1,22,7,26,14,16,6,19,12,23,3,27,9,18)(2,21,8,25,13,15,5,20,11,24,4,28,10,17),
(1,26,6,19,14,22)(2,25,5,20,13,21)(3,16,9,27,7,23)(4,15,10,28,8,24)(11,17)(12,18).

References

[1] L. Babai, Isomorphism problem for a class of point-symmetric structures, Acta Math Acad Sci Hungar 29 (1977), 329–336.

[2] J. A. Barrau, Over de combinatorische opgave van Steiner, Kon Akad Wetensch Amst Verslag Wis- en Natuurk Afd 17 (1908), 318—326. (= On the combinatory problem of Steiner, Kon Akad Wetensch Amst Proc Sec Sci 11 (1908), 352–360.)

[3] S. Bays, Sur les systèmes cycliques de triples de Steiner differents pour N premier (où puissance de nombre premier) de la forme $6n+1$, I, Comment Math Helv 2 (1930), 294–305; II–VI, Comment Math Helv 3 (1931), 22-41, 122–147, 307–325.

[4] N. Brand, On the Bays–Lambossy theorem, Discrete Math 78 (1989), 217–222.

[5] J. J. Cannon and D. F. Holt, The transitive permutation groups of degree 32, Experiment Math 17 (2008), 307–314.

[6] C. J. Colbourn, M. J. Colbourn, and K. T. Phelps, Combinatorial algorithms for generating cyclic Steiner quadruple systems, Discrete Mathematical Analysis and Combinatorial Computation, Proc Conf New Brunswick, Univ New Brunswick, Fredericton, N.B., 1980, pp. 25–39.

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

[8] I. Diener, I, On cyclic Steiner systems $S(3,4,22)$, Ann Discrete Math 7 (1980), 301–313.

[9] J. D. Dixon and B. Mortimer, Permutation Groups, Springer, New York, 1996.

[10] J. Doyen and M. Vandensavel, Non-isomorphic Steiner quadruple systems, Bull Soc Math Belg 23 (1971), 393–410.

[11] T. Feng and Y. Chang, Constructions for cyclic 3-designs and improved results on cyclic Steiner quadruple systems, J Combin Des 19 (2011), 178–201.

[12] T. Feng, Y. Chang, and L. Ji, Constructions for strictly cyclic 3-designs and applications to optimal OOCs with $\lambda = 2$, J Combin Theory Ser A 115 (2008), 1527–1551.

[13] T. C. Frenz and D. L. Kreher, An algorithm for enumerating distinct cyclic Steiner systems, J Combin Math Combin Comput 11 (1992), 23–32.

[14] M. J. Grannell and T. S. Griggs, On the structure of S-cyclic Steiner quadruple systems, Ars Combin 9 (1980), 51–58.

[15] M. J. Grannell and T. S. Griggs, An enumeration of S-cyclic SQS(26), Utilitas Math 20 (1981), 249–259.

[16] M. J. Grannell and T. S. Griggs, A cyclic Steiner quadruple system of order 32, Discrete Math 38 (1982), 109–111.

[17] M. Guregová and A. Rosa, Using the computer to investigate cyclic Steiner quadruple systems, Mat Casopis Sloven Akad Vied 18 (1968), 229–239.

[18] H. Hanani, On quadruple systems, Canad J Math 12 (1960), 145–157.

[19] H. Hanani, On some tactical configurations, Canad J Math 15 (1963), 702–722.

[20] A. Hartman and K. T. Phelps, Steiner quadruple systems, Contemporary Design Theory, J. H. Dinitz and D. R. Stinson (Editors), Wiley, New York, 1992, pp. 205–240.

[21] W. C. Huffman, The equivalence of two cyclic objects on pq elements, Discrete Math 154 (1996), 103–127.

[22] W. C. Huffman, V. Job, and V. Pless, Multipliers and generalized multipliers of cyclic objects and cyclic codes, J Combin Theory Ser A 62 (1993), 183–215.

[23] A. Hulpke, Constructing transitive permutation groups, J Symbolic Comput 39 (2005), 1–30.

[24] R. K. Jain, On cyclic Steiner quadruple systems, M.Sc. Thesis, McMaster University, Hamilton, 1971.

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

[26] P. Kaski, P. R. J. Östergård, and O. Pottonen, The Steiner quadruple systems of order 16, J Combin Theory Ser A 113 (2006), 1764–1770.

[27] P. Kaski and O. Pottonen, libexact user's guide, version 1.0, HIIT Technical Reports 2008-1, Helsinki Institute for Information Technology HIIT, 2008.

[28] D. E. Knuth, Dancing links, Millennial Perspectives in Computer Science, J. Davies, B. Roscoe, and J. Woodcock (Editors), Palgrave, Houndmills, 2000, pp. 187–214.

[29] E. Köhler, Quadruple systems over $\mathbf{Z}_p$ admitting the affine group, Combinatorial Theory, D. Jungnickel and K. Vedder (Editors), LNM 969, Springer, Berlin, 1982, pp. 212–228.

[30] H. Koike, I. Kovács, and T. Pisanski, The number of cyclic configurations of type (v_3) and the isomorphism problem, J Combin Des 22 (2014), 216–229.

[31] P. Lambossy, Sur une manière de differencier les fonctions cycliques d'une forme donnée, Comment Math Helv 3 (1931), 69–102.

[32] H. Lenz, On the number of Steiner quadruple systems, Mitt Math Seminar Giessen 169 (1985), 55–71.

[33] C. C. Lindner and A. Rosa, Steiner quadruple systems—A survey, Discrete Math 22 (1978), 147–181.

[34] N. S. Mendelsohn and S. H. Y. Hung, On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$, Util Math 1 (1972), 5–95.

[35] P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, European J Combin 8 (1987), 35–43.

[36] K. T. Phelps, On cyclic Steiner systems $S(3,4,20)$, Ann Discrete Math 7 (1980), 277–300.

[37] K. T. Phelps, A construction of cyclic Steiner triple systems of order p^n, Discrete Math 67 (1987), 107–110.

[38] K. T. Phelps, Isomorphism problems for cyclic block designs, Ann Discrete Math 34 (1987), 385–391.

[39] A. Rosa, On reverse Steiner triple systems, Discrete Math 2 (1972), 61–71.

[40] J. J. Rotman, An Introduction to the Theory of Groups, 4th ed., Springer, New York, 1995.