MATHEMATICS OF COMPUTATION
Volume 84, Number 296, November 2015, Pages 3051–3067
http://dx.doi.org/10.1090/mcom/2945
Article electronically published on April 7, 2015

ENUMERATION OF STEINER TRIPLE SYSTEMS WITH SUBSYSTEMS

PETTERI KASKI, PATRIC R. J. ÖSTERGÅRD, AND ALEXANDRU POPA

ABSTRACT. A Steiner triple system of order v, an STS(v), is a set of 3-element subsets, called blocks, of a v-element set of points, such that every pair of distinct points occurs in exactly one block. A subsystem of order w in an STS(v), a sub-STS(w), is a subset of blocks that forms an STS(w). Constructive and nonconstructive techniques for enumerating up to isomorphism the STS(v) that admit at least one sub-STS(w) are presented here for general parameters v and w. The techniques are further applied to show that the number of isomorphism classes of STS(21)s with at least one sub-STS(9) is 12661527336 and of STS(27)s with a sub-STS(13) is 1356574942538935943268083236.

1. INTRODUCTION

A *Steiner triple system* of order v, in short an STS(v), is a set of 3-element subsets, called *blocks*, of a v-element set of *points*, such that every pair of distinct points occurs in exactly one block. A necessary and sufficient condition for the existence of an STS(v) is that $v \equiv 1 \pmod 6$ or $v \equiv 3 \pmod 6$ [6, Sect. 0.2]. An STS(v) has $v(v-1)/6$ blocks and each point occurs in $(v-1)/2$ blocks. A *subsystem* of order w in an STS(v), in short a sub-STS(w), is a subset of blocks that forms an STS(w).

Two Steiner triple systems are *isomorphic* if there is a bijection between the point sets that takes the blocks of one system onto the blocks of the other system. The number of isomorphism classes of STS(v)s with admissible orders is known only up to $v = 19$. The orders $v = 7$ and $v = 9$ both have a unique STS(v). De Pasquale [8] and Brunel [2] established that there are two isomorphism classes for $v = 13$, and Cole, Cummings, and White [7, 28] showed that there are 80 isomorphism classes for $v = 15$. Kaski and Östergård [14] used an extensive computer search to conclude that there are 11084874829 isomorphism classes for $v = 19$.

The aforementioned studies do not only *count* the isomorphism classes of Steiner triple systems, but are constructive in the sense that specimens from each isomorphism class are obtained. The term *classification* is used for such constructive methods, whereas the term *enumeration* covers both constructive classification and nonconstructive counting.

For admissible orders greater than 19, where so far no attempts to count the number of isomorphism classes of Steiner triple systems have been successful, a more modest goal is to enumerate systems with a specific structure. One central type of systems are Steiner triple systems that admit subsystems. Indeed, a catalyst for the current work was a recent study [1], where it is shown that STS(21)s with

Received by the editor November 19, 2013 and, in revised form, March 4, 2014.
2010 *Mathematics Subject Classification.* Primary 05B07, 51E10.
Key words and phrases. Classification, enumeration, Steiner triple system, subsystem.

sub-STS(9)s form extremal objects for a certain switching construction that can be used to obtain new strongly regular graphs. It turned out that such systems had never been classified.

The objective of the current paper is to present constructive as well as nonconstructive enumeration techniques for STSs that admit subsystems. The work on nonconstructive techniques continues similar work carried out for other types of combinatorial objects in [12, 17, 24]. In particular, the techniques are applied to enumerate the isomorphism classes of STS(v)s that admit at least one sub-STS(w) for the parameters $v = 21$, $w = 9$ and $v = 27$, $w = 13$. The result is constructive for the former set of parameters and nonconstructive for the latter. The results obtained are summarized in the following theorem.

Theorem 1. *The number of isomorphism classes of* STS(21)*s that admit at least one sub*-STS(9) *is* 12661527336 *and of* STS(27)*s that admit a sub*-STS(13) *is* 1356574942538935943268083236.

The paper is organized as follows. Some (old and new) general results needed throughout the paper are presented in Section 2. The discussion of enumeration techniques for STS(v)s that admit at least one sub-STS(w) is divided into two parts. First, in Section 3, methods for enumerating possible complements of a sub-STS(w) in an STS(v) are considered. Second, in Section 4, the task of joining such complements with STS(w)s is discussed. Joining is discussed separately for the cases where the STS(v) has exactly one sub-STS(w) and when it has more than one sub-STS(w). The various cases are linked to earlier results in the literature, such as [18, 27]. The paper is concluded in Section 5.

2. Preliminaries

Here, we shall recall some well-known structural facts about Steiner triple systems that admit subsystems [6] and derive some further results needed in the sequel.

2.1. Decomposition of blocks induced by a subsystem.

We consider an STS(v) that has at least one sub-STS(w) and individualize one such sub-STS(w). We further write V for the point set of the STS(v) and $W \subseteq V$ for the point set of the individualized sub-STS(w).

Each point $p \in W$ occurs in $(w-1)/2$ blocks of the subsystem and in $(v-1)/2-(w-1)/2=(v-w)/2$ blocks outside the subsystem. Furthermore, each block is either contained in W (and hence part of the individualized subsystem) or intersects W in at most one point. Thus, there are $w(v-w)/2$ blocks that contain one point in W and two points in $V \setminus W$. Since there are $(v-w)(v-w-1)/2$ pairs of points outside the subsystem, we must have $w(v-w)/2 \leq (v-w)(v-w-1)/2$. This inequality immediately leads to the following standard observation.

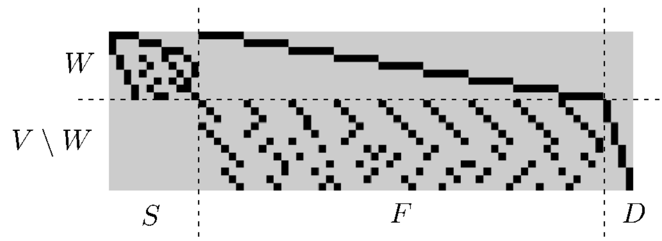
Theorem 2. *For an* STS(v) *with a sub*-STS(w)*, we have either* $2w+1 \leq v$ *or* $v = w$.

We call subsystems with $v = w$ *trivial*. Doyen and Wilson [10] showed that the condition in Theorem 2 is sufficient for all admissible parameters v and w.

From the analysis above we also immediately conclude that we can decompose the set X of blocks of the STS(v) into three disjoint sets $X = S \cup F \cup D$:

(S) the $w(w-1)/6$ blocks in the individualized subsystem,
(F) the $w(v-w)/2$ blocks that meet W in exactly one point, and
(D) the $(v-w)(v-2w+1)/6$ blocks that are disjoint from W.

Example 3. Below we display an STS(21) with an individualized sub-STS(9) as a 21×70 incidence matrix. The points in W and the points in $V \setminus W$ have been separated by a horizontal dashed line, and two vertical dashed lines separate the three parts (S, F, D) in the induced decomposition of blocks.



Let us now study the blocks in part F in more detail. Fix a point $p \in W$ and consider the blocks in part F that contain p. Such blocks must be disjoint apart from the common point p, since otherwise we would have a pair of distinct points occurring in two blocks. Since there are $(v-w)/2$ such blocks, and each contains two points from $V \setminus W$, we conclude that the blocks form a partition of $V \setminus W$ into 2-subsets. Letting p vary in W, we obtain in total w such partitions F_p. Again no two such partitions may share a 2-subset, since otherwise we would have a pair of distinct points occurring in two blocks.

Equivalently, we may view the set $\mathcal{F} = \{F_p : p \in W\}$ as a one-factorization of the w-regular graph G with vertex set $V(G) = V \setminus W$ and edge set $E(G) = \bigcup_{p \in W} F_p$. Recall that a *one-factor* of a graph is a 1-regular spanning subgraph, and a *one-factorization* of a graph is a set of one-factors such that each edge of the graph appears in precisely one one-factor. Two one-factorizations of a graph are *isomorphic* if one can be obtained from the other via a permutation of the vertices.

Let us now turn to the blocks in part D. We use the conventional notation $\bar{G}$ for the complement of the graph G.

Theorem 4. *The graph $\bar{G}$ is regular with degree $v-2w-1$. Moreover, it decomposes into edge-disjoint triangles.*

Proof. Regularity follows because G is regular. The degree is $(v-w-1)-w = v-2w-1$. Each block in part D defines a triangle in $\bar{G}$. These triangles are edge-disjoint and cover the edges of $\bar{G}$ exactly once because every pair of distinct points occurs in a unique block. □

Corollary 5. *The graph $\bar{G}$ is (i) empty if and only if $2w+1 = v$, and (ii) a union of $(v-w)/3$ vertex-disjoint triangles if and only if $2w+3 = v$.*

In fact, the blocks in $D \cup F$ form the blocks of a 3-GDD of type $1^{v-w}w^1$. A *k-GDD* of type $g_1^{a_1} g_2^{a_2} \cdots g_p^{a_p}$ is a triple $(V, \mathcal{G}, \mathcal{B})$, where V is a set of $\sum_{i=1}^{p} a_i g_i$ *points*, $\mathcal{G}$ is a partition of V into a_i subsets, called *groups*, of size g_i for $1 \le i \le p$, and $\mathcal{B}$ is a collection of k-subsets of points, called *blocks*, such that every 2-subset of points occurs in exactly one block or one group, but not both.

The blocks in $D \cup F$ can also be studied in the context of *incomplete Steiner systems* [5]. The point set W is said to form a *hole* in such an incomplete system.

The framework of incomplete Steiner systems is more general than that of 3-GDDs, since there may be more than one hole. If subsystems are removed from a Steiner triple system, then we get incomplete Steiner systems with holes. The reverse operation is not always possible, as the size of a hole does not have to be an admissible order for a Steiner triple system.

In general, a Steiner triple system may admit more than one subsystem of a given order, whereby the decomposition (S, F, D) is not unique. However, using results from the theory of incomplete Steiner systems, it follows that the decomposition is necessarily unique for certain parameters.

Theorem 6. *A necessary condition for an* STS(v) *to have more than one sub-*STS$((v-1)/2)$ *is that* $v \equiv 7 \pmod{24}$ *or* $v \equiv 15 \pmod{24}$.

Proof. Consider an STS(v) with two sub-STS$((v-1)/2)$ that intersect at z points. From [5], we then have that $v \geq 2(v-1)/2 + (v-1)/2 - 2z$, that is, $z \geq (v-3)/4$. But according to Theorem 2, $z \leq ((v-1)/2 - 1)/2 = (v-3)/4$, so $z = (v-3)/4$. As the intersection of the two sub-STS$((v-1)/2)$ form a Steiner triple system, $(v-3)/4 \equiv 1 \pmod 6$ or $(v-3)/4 \equiv 3 \pmod 6$, which can be simplified to the given necessary conditions. □

The condition in Theorem 6 is strict as the results of [5] imply that there do exist STS(v)s with more than one sub-STS$((v-1)/2)$ for every $v \equiv 7 \pmod{24}$ and $v \equiv 15 \pmod{24}$.

We shall now proceed with the discussion of enumeration algorithms.

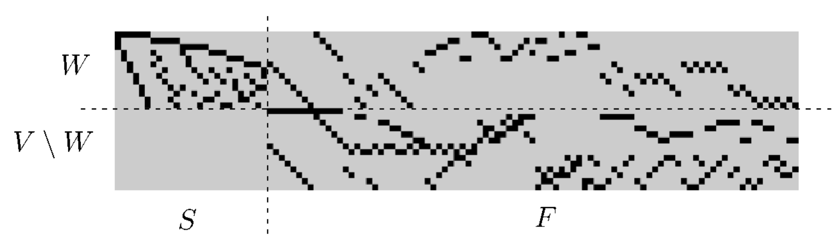
3. Enumerating complements of subsystems

It is clear from the decomposition (S, F, D) that the subsystem S and its complement (F, D) can be enumerated separately and joined together in the final stage. In all instances considered here and in earlier studies, the order of S is at most 13, so the involved Steiner triple systems have been classified (recall that this is the case even up to order 19). Consequently, we may focus on enumerating the parts (F, D). This task can further be split into the cases of $v = 2w + 1$ (Section 3.1) and $v > 2w + 1$ (Sections 3.2 and 3.3). The choice between the two methods to be presented in Sections 3.2 and 3.3 is basically a matter of computational efficiency and should be decided on a case-by-case basis.

3.1. The case $v = 2w + 1$.

When $v = 2w + 1$, it follows from Corollary 5 that $G \cong K_{w+1}$. Thus, part D of the decomposition (S, F, D) is empty, and part F defines a one-factorization of the complete graph K_{w+1}.

Example 7. Below we display an STS(27) with a sub-STS(13) as a 27×117 incidence matrix.



One-factorizations of complete graphs have been enumerated for graphs up to order 14. See [16, Sect. 8.1.1] for a survey of enumeration results for orders up to 12 and [17] for the case of order 14. Indeed, in the current work the one-factorizations of K_{14} will be needed.

3.2. **The cases $v > 2w+1$, point by point.** When $v > 2w+1$, the first possible case is $v = 2w+3$. For ease of exposition we restrict our discussion to this case, using the parameters $v = 21$, $w = 9$ as a running example (cf. Example 3). A generalization to arbitrary $v > 2w+3$ is discussed at the end of this section.

When $v = 2w+3$, we observe by Corollary 5 that the graph G is the complete graph K_{w+3} with $(w+3)/3$ vertex-disjoint triangles deleted, that is, $G \cong K_{w+3} \setminus ((w+3)/3)K_3$.

We classify the one-factorizations of $K_{w+3} \setminus ((w+3)/3)K_3$ via the following combinatorial correspondence, which is analogous to a correspondence due to Semakov and Zinov′ev [26]. Consider a one-factorization $\mathcal{F}$ of $K_{w+3} \setminus ((w+3)/3)K_3$. Augment $\mathcal{F}$ into a factorization $\mathcal{F}'$ of K_{w+3} consisting of (i) the 2-factor defined by the $(w+3)/3$ triangles in $((w+3)/3)K_3$, and (ii) all the one-factors in $\mathcal{F}$. It is immediate that $\mathcal{F}$ and $\mathcal{F}'$ determine each other uniquely. Now assign a label from $0, 1, \ldots, (w+1)/2$ to each connected component of each factor in $\mathcal{F}'$, so that no two connected components within a factor get the same label. Tabulating the labels of the $w+3$ vertices for each of the $w+1$ factors in $\mathcal{F}'$, we obtain a $(w+3) \times (w+1)$ array over the labels $0, 1, \ldots, (w+1)/2$.

Example 8. For parameters $v = 21$ and $w = 9$, below we display a 12×10 array obtained by labeling the factorization of K_{12} defined by the blocks in parts (F, D) in Example 3. The first column corresponds to the 2-factor defined by $4K_3$, or equivalently, the blocks in part D in Example 3.

```
0000000000
0111111111
0222222222
1012333333
1103244444
1230155555
2324401345
2441520453
2555315024
3353553210
3435434102
3544042531
```

We may view the rows of such an array as the codewords of a code $C_{\mathcal{F}'}$. From the properties of $\mathcal{F}'$ we readily observe that:

(P1) $C_{\mathcal{F}'}$ has $w+3$ codewords of length $w+1$,
(P2) any two distinct words differ in exactly w coordinates and agree in 1 coordinate, and
(P3) there is a unique coordinate with exactly $(w+3)/3$ symbols each occurring 3 times, and all the other w coordinates have $(w+3)/2$ symbols each occurring 2 times.

Conversely, any code with properties (P1)–(P3) corresponds to a factorization $\mathcal{F}'$ of K_{w+3} consisting of a 2-factor of triangles and w one-factors. This correspondence is one-to-one between isomorphism classes of factorizations and equivalence classes of codes, where two codes C and C' are said to be *equivalent* if one can be obtained from the other by a sequence of the following operations:

(E1) permutation of the codewords (rows of the array),
(E2) permutation of the coordinates (columns of the array), and
(E3) independent relabeling of the symbols in each coordinate.

We enumerate the one-factorizations of $K_{w+3} \setminus ((w+3)/3)K_3$ up to isomorphism by classifying the codes (arrays) that have properties (P1)–(P3) up to equivalence. We use an *orderly algorithm* [11, 25] relying on lexicographic order in this task. The following algorithm is an adaptation of algorithms used in two earlier studies [13, 15].

We order the set of all $M \times N$ arrays over an ordered alphabet of symbols Σ via the lexicographic order of the strings obtained by concatenating the rows of the array one after another. We say that an array is a *minimum representative* if it is the lexicographic minimum of its equivalence class.

By lexicographic order it is immediate that an $M \times N$ array is a minimum representative only if the $(M-1) \times N$ array obtained by deleting the last row is a minimum representative. This enables us to generate the $(w+3) \times (w+1)$ minimum representative arrays that have properties (P1)–(P3), recursively extending an $(M-1) \times (w+1)$ array one row at a time, and disregarding the result unless it is a minimum representative, $1 \leq M \leq w+3$. The minimality of a given array in its equivalence class can be tested using backtrack search over partial permutations of the rows; cf. [13].

When generating the arrays, we rely on the following observations to focus the backtrack search. First, each new row must satisfy (P2) relative to the old rows. Second, each new row must not violate (P3) relative to the old rows. Given (P2), we know that the first two rows of a minimum representative must be $000\cdots0$ and $011\cdots1$, which implies, by (P3), that the third row must be $022\cdots2$ and, consequently, that the first column must be $000111\cdots(w/3)(w/3)(w/3)$; cf. Example 8. Third, at some point we complete the structure to an $(w+3) \times (w+1)$ array using clique search in a compatibility graph with vertices as compatible rows; cf. [15]. For $w = 9$, the completion was carried out for $M = 7$ rows to 12 rows.

We find 15113085 isomorphism classes of one-factorizations of $K_{12} \setminus 4K_3$. Table 1 displays the number of one-factorizations N for each possible order $|\mathrm{Aut}(\mathcal{F})|$ of the automorphism group. The time required by the constructive enumeration was about nine core-hours on an Intel Xeon X5650 2.67GHz CPU.

In the case of $v > 2w+3$, Theorem 4 gives that $\bar{G}$ is regular with even degree greater than or equal to 4. Then parts F and D may be considered separately. For parts F and D, we are facing the general problems of classifying one-factorizations of regular graphs and decompositions of regular graphs into triangles, respectively. For the former problem, see [15]. Starting from a classification of regular graphs with given parameters, one may first classify the structures for part D, which gives a set of graphs G to consider for F. Isomorph rejection is simplified by the fact that the decomposition of (F, D) into F and D is unique, which makes the problem analogous to that of Section 4.1.

3.3. **The cases $v > 2w+1$, block by block.** The array in the previous section is constructed row by row. An alternative approach is that of constructing the array column by column, that is, block by block from the viewpoint of a design.

TABLE 1. The one-factorizations of $K_{12} \setminus 4K_3$

$\lvert\mathrm{Aut}(\mathcal{F})\rvert$	N	$\lvert\mathrm{Aut}(\mathcal{F})\rvert$	N
1	15032761	24	31
2	74174	27	1
3	839	36	3
4	4834	48	2
6	54	72	4
8	307	144	2
9	8	216	1
12	48	648	1
16	11	1296	1
18	3		

A classification of the arrays column by column can be carried out in a two-stage approach. In the first stage certain partial arrays are classified, and these partial arrays (called *seeds*) are completed to full arrays in the second stage.

There are various possible choices for the definition of a seed. One possibility is to define seeds as $(v-w)\times 3$ subarrays consisting of columns where each symbol occurs twice. The approach of [18] can, somewhat modified, be put into the framework of the current paper with such a seed (joining is not carried out in that work, but the STS(7) is fixed while forming the complement of it).

One may also define seeds analogous to those in the approach for classifying one-factorizations of complete graphs discussed in [15]; see also [16, Sect. 8.1.1]. A seed is then defined as a $(v-w)\times w$ subarray consisting of those columns of the final array where each symbol occurs twice, with the first column $0011\cdots((v-w-2)/2)((v-w-2)/2)$, the first row $000\cdots0$, the second row $011\cdots1$, and all other entries containing a 0 or a 1 filled out.

Example 9. For parameters $v = 21$ and $w = 9$, below we display a partial 12×9 array (seed), which can be extended to a structure isomorphic to the 12×10 array in Example 8.

0	0	0	0	0	0	0	0	0
0	1	1	1	1	1	1	1	1
1	1							
1	0							
2		1						
2		0						
3				0		1		
3					1			0
4					0			1
4				1			0	
5			1			0		
5			0				1	

Extension of seeds and rejection of isomorphs amongst the completed structures can be handled analogously to the basic situation of one-factorizations of complete graphs, with an exact cover algorithm [20] for the former subproblem and canonical augmentation [23] for the latter. Again we refer to [15] and [16, Sect. 8.1.1] for details. The difference compared with the basic case is obviously the D part of (F, D), but this difference is easily implemented in the algorithms.

4. Joining the parts

We consider joining for two situations: for STS(v)s with exactly one sub-STS(w) and for STS(v)s with at least one sub-STS(w). A general algorithm for the latter case obviously covers the previous case as well but will then be considerably slower than a tailored approach. Theorem 6 implies certain conditions under which there will be exactly one sub-STS(w).

Also the following observation can in some cases be used to deduce that there is exactly one sub-STS(w). Assume that an STS(v) has two sub-STS(w)s that intersect in w' points. If one of the subsystems has point set W, then the pairs of the other system induced by $V \setminus W$ form a one-factorization of $K_{w-w'}$. Consequently, a necessary condition for these subsystems to exist is that (F, D) contain such a subsystem.

4.1. **Exactly one sub-STS(w).** Earlier work on joining when there is exactly one sub-STS(w) has been carried out specifically for the case of STS($2w+1$)s with sub-STS(w)s by Déherder [9] and Stinson and Seah [27]. Stinson and Seah enumerated the STS(19)s with a sub-STS(9), a work that Déherder had started. Our discussion will to some extent follow that of Stinson and Seah [27]. We use the case of STS(27)s with exactly one sub-STS(13) as a running example. (For $w = 9$ and $w = 13$, there can be only one sub-STS(w) in an STS($2w + 1$) by Theorem 6.)

Focusing on cases with exactly one sub-STS(w), the decomposition (S, F, D) is unique for a given STS(v), and our task reduces to enumerating the number of pairs $(S, (F, D))$ up to isomorphism. We obtain yet another reduction by observing that we may fix the point set $W \subseteq V$ of S, in which case our task becomes to enumerate the number of orbits of formal pairs $(S, (F, D))$ under the diagonal action of the direct product $\mathrm{Sym}(W) \times \mathrm{Sym}(V \setminus W)$.

For STS(27)s with one sub-STS(13), there are two isomorphism classes of subsystems S [2, 8] and 1132835421602062347 isomorphism classes of one-factorizations F [17]; part D is empty. It is obvious that there are far too many orbits of one-factorizations in this case to support a constructive enumeration, and hence nonconstructive techniques are required. We shall now have a look at a convenient method for counting, which uses Burnside's lemma to count structures. In its basic version, as presented in [27], this method just gives the total number of objects and is in the general case not able to refine the number based on the order of the automorphism group.

Let S be an STS(w) with point set W and let (F, D) be a pair such that $S \cup F \cup D$ is an STS(v). All possible ways of joining S and (F, D) into an STS(v) can now be obtained by applying all possible permutations $\pi \in \mathrm{Sym}(W)$ to S. The objective of our enumeration is then to count or identify pairwise nonisomorphic structures obtained in this way.

We observe that two structures $(S, (F, D))$ and $(S', (F, D))$ are isomorphic under the diagonal action if and only if there is an automorphism of (F, D) restricted to the point set W that takes S onto S'.

Let $\Gamma \leq \mathrm{Sym}(W)$ be the automorphism group of (F, D) restricted to W. For $\pi \in \Gamma$, let us write $\mathrm{fix}(\pi)$ for the number of S' such that S' is isomorphic to S and π fixes S'. An application of Burnside's lemma gives the following [27, Lemma 2.1]:

Theorem 10. *The number of nonisomorphic Steiner triple systems that can be obtained by joining S and (F, D) is exactly*

$$\frac{1}{|\Gamma|}\sum_{\pi\in\Gamma}\mathrm{fix}(\pi)\,.$$

The *cycle type* of a permutation with n_i cycles of length l_i, $1 \le i \le m$, is $l_1^{n_1} l_2^{n_2} \cdots l_m^{n_m}$. The value of $\mathrm{fix}(\pi)$ is solely dependent on the cycle type of the permutation $\pi \in \Gamma$, as conjugates in $\mathrm{Sym}(W)$ have the same value.

In [27, Table 2], $\mathrm{fix}(\pi)$ is calculated for all cycle types of permutations in the automorphism group of the unique STS(9). There are two isomorphism classes of STS(13)s for which the same calculations are carried out in Tables 2 and 3. The column N gives the number of permutations in the automorphism group with the given cycle type, and the column C shows the number of conjugates, obtained by straightforward calculation. This enables us to determine

$$\mathrm{fix}(\pi) = \frac{w!N}{|\mathrm{Aut}|C}\,.$$

TABLE 2. Automorphism types for STS(13) with $|\mathrm{Aut}| = 6$

Cycle type	N	C	$\mathrm{fix}(\pi)$
$1^1 3^4$	2	3203200	648
$1^3 2^5$	3	270270	11520
1^{13}	1	1	1037836800

TABLE 3. Automorphism types for STS(13) with $|\mathrm{Aut}| = 39$

Cycle type	N	C	$\mathrm{fix}(\pi)$
13^1	12	479001600	4
$1^1 3^4$	26	3203200	1296
1^{13}	1	1	159667200

For the one-factorizations of K_{14}, we find that the automorphism groups A of the 1132835421602062347 isomorphism classes partition into 96 conjugacy classes under the diagonal action. Furthermore, each conjugacy class acts faithfully on the 13 one-factors. Let us now describe the procedure for determining the conjugacy classes in more detail.

For small group orders, $1 \le |A| \le 3$, the conjugacy class of A is uniquely determined by the order $|A|$ together with the numbers of one-factors and vertices fixed by A. There are eight such groups, up to conjugacy. In Table 4 we show some information about the cycle types of the elements in these groups. Specifically, we give the number of cycles for each type that occurs in Tables 2 and 3 (for the action on the 13 one-factors). For each group we also give the group order $|A|$ and the number of one-factorizations whose automorphism group is conjugate to this group. The data comes from the classification of one-factorizations of K_{14} published in [17] (but is not presented in such detail in the final paper).

For group orders $|A| \ge 4$, we are left with 118731 isomorphism classes of one-factorizations, which we have stored on disk as a result of a constructive enumeration [17]. We find the conjugacy classes and group elements by encoding the

TABLE 4. Cycle types of group elements, small groups

Number	1^{13}	$1^3 2^5$	$1^1 3^4$	13^1	$\lvert A\rvert$	N
1	1	0	0	0	1	1132835411296799774
2	1	0	0	0	2	91872798
3	1	1	0	0	2	908969907
4	1	1	0	0	2	1019084772
5	1	0	0	0	2	5777030660
6	1	0	0	0	2	24073651
7	1	0	0	0	2	2479614292
8	1	0	2	0	3	4497762

automorphism group A of each one-factorization as a vertex-colored graph $H(A)$ such that any two such graphs are isomorphic as colored graphs (that is, only color-preserving permutations of the vertices are considered) if and only if the groups are conjugate in $\mathrm{Sym}(W) \times \mathrm{Sym}(V \setminus W)$. We then find that there are 88 conjugacy classes by putting $H(A)$ into canonical form for each of the 118731 groups A using *nauty* [22]. The time required was about seven core-hours on an Intel Xeon X5650 2.67GHz CPU. We present the cycle types for these groups in Tables 5 and 6 with the same format as for small groups in Table 4.

The encoding of A as a colored graph $H(A)$ is as follows. We use five colors, which we represent by the characters P, Q, R, S, T. Start with the empty graph. Take one vertex p_w with color P for each $w \in W$, and take one vertex p_u with color Q for each $u \in V \setminus W$. Now, for each element $a \in A$, which we may view as a permutation $a : V \to V$, introduce the following subgraph gadget by taking one vertex $x_{a,v}$ with color R for each $v \in V$, one vertex $y_{a,v}$ with color S for each $v \in V$, and one vertex z_a with color T. Then insert the edges $\{p_v, x_{a,v}\}$, $\{p_v, y_{a,v}\}$, $\{x_{a,v}, y_{a,a(v)}\}$, $\{x_{a,v}, z_a\}$, and $\{y_{a,v}, z_a\}$ for each $v \in V$. This results in a graph with $|V| + |A|(2|V| + 1)$ vertices and $5|A||V|$ edges. Figure 1 illustrates the construction with $V = \{1, 2, 3, 4, 5, 6, 7\}$, $W = \{1, 2, 3\}$ and, in cycle notation, $A = \{(1)(2)(3)(4)(5)(6)(7), (1, 2)(3)(4, 5)(6, 7)\}$. Observe that the vertex colors are indicated in the figure with the labels P, Q, R, S, T inside the vertices.

Applying Theorem 10, we find exactly 1356574942538935943268083236 STS(27)s with a sub-STS(13). Unfortunately, Theorem 10 only gives the total number of isomorphism classes of structures, but does not give a subdivision based on the order of the automorphism group. To this aim, one may use a more sophisticated version of Burnside's lemma, where the action of subgroups of A rather than elements of A are considered. See [19, Chapter 4] for details. In this work we originally got the result with a general technique for double coset enumeration (which is much more general than what is needed in this current context and is therefore omitted).

Table 7 displays the number of STS(27)s X with a sub-STS(13) for each possible order of the automorphism group $|\mathrm{Aut}(X)|$.

To gain confidence in the correctness of the enumeration, we count in two different ways the total number of distinct STS(27)s that admit a sub-STS(13). First, we recall that the total number of distinct one-factorizations of K_{14} is $\mathrm{LF}(K_{14}) =$ 98758655816833727741338583040 [17]. Over a fixed point set V, we claim that the

TABLE 5. Cycle types of group elements, part I

Number	1^{13}	$1^3 2^5$	$1^1 3^4$	13^1	$\|A\|$	N
1	1	2	0	0	4	11808
2	1	1	0	0	4	10126
3	1	2	0	0	4	3144
4	1	1	0	0	4	7680
5	1	2	0	0	4	1098
6	1	0	0	0	4	10480
7	1	0	0	0	4	6112
8	1	0	0	0	4	5376
9	1	0	0	0	4	8338
10	1	2	0	0	4	10920
11	1	2	0	0	4	880
12	1	0	0	0	4	6456
13	1	0	0	0	4	18904
14	1	0	0	0	4	1144
15	1	0	0	0	4	1980
16	1	0	0	0	4	114
17	1	0	0	0	5	2742
18	1	3	2	0	6	360
19	1	0	2	0	6	534
20	1	3	2	0	6	789
21	1	0	2	0	6	3099
22	1	0	2	0	6	4176
23	1	3	2	0	6	280
24	1	0	2	0	6	9
25	1	4	0	0	8	118
26	1	4	0	0	8	32
27	1	2	0	0	8	50
28	1	2	0	0	8	20
29	1	0	0	0	8	80
30	1	2	0	0	8	164
31	1	2	0	0	8	204
32	1	2	0	0	8	186
33	1	0	0	0	8	54
34	1	0	0	0	8	14
35	1	4	0	0	8	38
36	1	2	0	0	8	122
37	1	4	0	0	8	398
38	1	4	0	0	8	12
39	1	2	0	0	8	34
40	1	0	0	0	8	84
41	1	0	0	0	8	28
42	1	0	0	0	8	19
43	1	2	0	0	8	19
44	1	0	0	0	8	76

Table 6. Cycle types of group elements, part II

Number	1^{13}	$1^3 2^5$	$1^1 3^4$	13^1	$\lvert A\rvert$	N
45	1	0	0	0	8	12
46	1	0	0	0	8	12
47	1	0	0	0	8	8
48	1	0	0	0	8	2
49	1	0	0	0	8	4
50	1	0	0	0	10	108
51	1	0	0	0	10	48
52	1	5	0	0	10	12
53	1	0	2	0	12	27
54	1	0	2	0	12	10
55	1	0	2	0	12	31
56	1	6	2	0	12	6
57	1	3	2	0	12	2
58	1	0	0	12	13	10
59	1	6	0	0	16	32
60	1	2	0	0	16	8
61	1	4	0	0	16	4
62	1	4	0	0	16	10
63	1	4	0	0	16	20
64	1	4	0	0	16	4
65	1	4	0	0	16	4
66	1	8	0	0	16	10
67	1	6	0	0	16	12
68	1	2	0	0	16	3
69	1	0	0	0	16	2
70	1	0	14	0	21	1
71	1	0	8	0	24	1
72	1	6	8	0	24	1
73	1	0	8	0	24	1
74	1	12	0	0	32	1
75	1	4	0	0	32	2
76	1	12	0	0	32	2
77	1	0	0	0	32	2
78	1	8	0	0	32	2
79	1	8	0	0	32	2
80	1	4	0	0	32	2
81	1	0	26	12	39	3
82	1	0	14	0	42	1
83	1	0	14	0	42	1
84	1	6	8	0	48	1
85	1	16	0	0	64	3
86	1	0	14	0	84	1
87	1	0	26	12	156	1
88	1	24	32	0	192	1

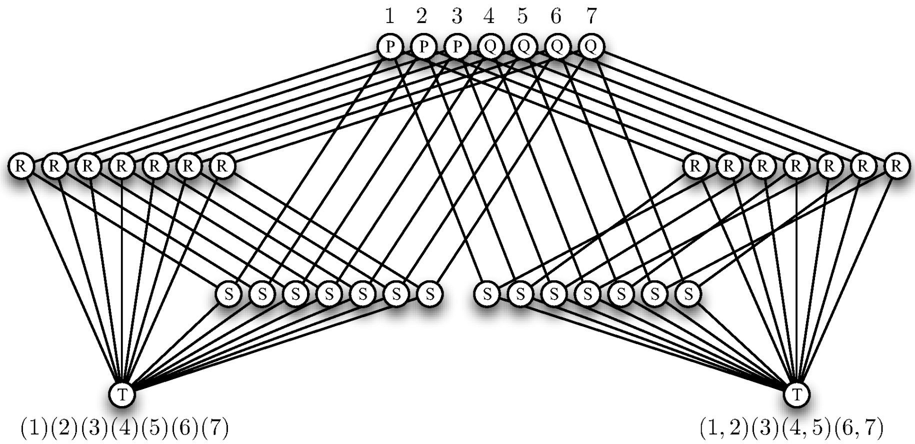


FIGURE 1. An illustration of the encoding $H(A)$

TABLE 7. The STS(27) with a sub-STS(13)

$\lvert\mathrm{Aut}(X)\rvert$	N
1	1356574942538913722873075856
2	22211642309784
3	8752680287
6	17256
13	40
39	13

number of distinct STS(27)s that admit a sub-STS(13) is

$$\sum_{[X]} \frac{27!}{|\mathrm{Aut}(X)|} = \binom{27}{13} \cdot \left(\frac{13!}{6} + \frac{13!}{39} \right) \cdot \mathrm{LF}(K_{14}) \cdot 13!\,, \tag{1}$$

where the sum on the left-hand side is over all isomorphism classes that admit a sub-STS(13); see Table 7. On the right-hand side, there are exactly $\binom{27}{13}$ ways to select the point set W, exactly $\frac{13!}{6} + \frac{13!}{39}$ ways to place one of the STS(13)s into W, and exactly $\mathrm{LF}(K_{14}) \cdot 13!$ ways to place a one-factorization of K_{14} between W and $V \setminus W$. Both the left-hand side and the right-hand side of (1) evaluate to

$$147715674490151300932389395741663921485092250240000000\,.$$

4.2. **At least one sub-STS(w).** Whenever joining is carried out such that more than one sub-STS(w) may arise, one has to be careful, since the assumption of a unique decomposition (S, F, D) is then no longer valid.

Here, we shall discuss an approach for joining with at least one sub-STS(w). Some case-by-case arguments can be used to tune the approach in specific situations, but here we shall omit such variants and put emphasis on general ideas.

When joining S and (F, D), we consider one representative from each isomorphism class of (F, D) and all labeled copies of S. To reject all but one representative from each isomorphism class of the structures $X = S \cup F \cup D$ thereby obtained, we apply the canonical augmentation method introduced by McKay [23]; see also [16, Sect. 4.2.3].

Let the point set V be fixed. Suppose we have constructed a Steiner triple system $X = S \cup F \cup D$ by extending (F, D). We accept X as the representative of its isomorphism class if and only if both (i) X is the minimum (with respect to lexicographic ordering of sets of 3-element subsets over V) of its orbit under the automorphism group $\mathrm{Aut}(F, D) = \{\sigma \in \mathrm{Sym}(V) : \sigma F = F, \sigma D = D\}$, and (ii) the subsystem $S = X \setminus (F \cup D)$ belongs to the canonical $\mathrm{Aut}(X)$-orbit $m(X)$ of sub-STS(w)s in X. We obtain a canonical orbit by putting X into canonical form $X' = \kappa(X)$ with X' and $\kappa \in \mathrm{Sym}(V)$ computed using *nauty* [22], finding the lexicographically least point set $W' \subseteq V$ of a sub-STS(w) in X', and returning the $\mathrm{Aut}(X)$-orbit of $\kappa^{-1}(W')$ as $m(X)$. In particular, the tests (i) and (ii) become trivial if both $\mathrm{Aut}(F, D)$ is trivial and the sub-STS(w) in X is unique.

For $w = 9$, we know that the automorphism group of the STS(9) has order 432, which results in $9!/432 = 840$ possibilities to complete the (S, F, D) decomposition given part (F, D). In total, $840 \cdot 15113085 = 12694991400$ STS(21)s are thus constructed in the process, which is guaranteed to construct at least one representative from each isomorphism class of STS(21)s that admit at least one sub-STS(9).

We find that there are 12661527336 isomorphism classes of STS(21) with a sub-STS(9). Table 8 displays the number of STS(21)s, N, for each possible order $|\mathrm{Aut}(X)|$ and each possible number $s_9(X)$ of sub-STS(9)s in X. The time required by the extension and isomorph rejection phase was about 150 core-days aggregated to a single Intel Xeon X5650 2.67GHz CPU.

TABLE 8. The STS(21)s with at least one sub-STS(9)

$\|\mathrm{Aut}(X)\|$	$s_9(X)$	N	$\|\mathrm{Aut}(X)\|$	$s_9(X)$	N
1	1	12657900680	14	7	1
1	3	101719	16	3	11
2	1	3492305	16	7	1
2	3	5316	18	1	9
3	1	15050	18	3	1
3	3	140	18	7	2
4	1	11128	24	1	12
4	3	339	24	3	7
6	1	210	27	1	3
6	3	55	36	1	4
6	7	1	36	3	1
8	1	154	48	3	2
8	3	67	54	7	1
8	7	1	72	3	1
9	1	21	72	1	4
9	7	1	108	7	1
12	1	73	144	3	1
12	3	11	504	7	1
12	7	1	1008	7	1

To gain confidence in the correctness of the enumeration, we carry out the following consistency check. Over a fixed point set V, we count in two different ways all the pairs (X, F) such that X is an STS(21) and $F \subseteq X$ is a one-factorization of $K_{12} \setminus 4K_3$ represented as a set of triples over V.

Taking the sum over the isomorphism classes, that is, the orbits of $\mathrm{Sym}(V)$, by the Orbit-Stabilizer Theorem we must have

$$\sum_{[F]} \frac{21!}{|\mathrm{Aut}(F)|} \cdot \frac{9!}{432} = \sum_{[X]} \frac{21!}{|\mathrm{Aut}(X)|} \cdot s_9(X)\,.$$

Using the computed data in Tables 1 and 8, both sides of this equality evaluate to

$$646809707516226677873049600000\,.$$

5. Conclusions

Steiner triple systems with subsystems of order greater than 3 have now been enumerated for STS(15)s with sub-STS(7)s (see [21, Table 1.29]), STS(19)s with sub-STS(7)s [18] (see also [4]), STS(19)s with sub-STS(9)s [27], STS(21)s with sub-STS(9)s (this work), and STS(27)s with sub-STS(13)s (this work). The (computational) effort needed to enumerate STS(v)s with sub-STS(w)s is to a large extent determined by the value of $v - w$. The open case with the smallest value of $v - w$ is that of enumerating STS(21)s with sub-STS(7)s.

Like various other problems, this enumeration problem can also be studied for two other types of combinatorial designs that form classes of 3-GDDs, namely Latin squares and one-factorizations of complete graphs. Latin squares with Latin subsquares are well-studied structures [3], while one-factorizations of complete graphs with sub-one-factorizations are maybe of less importance—but they do have applications, as we have seen in the current work.

Acknowledgements

This research was supported in part by the Academy of Finland, Grants 252083 and 256287 (P.K.) and Grant 132122 (P.Ö. and A.P.). We gratefully acknowledge use of computer resources funded by the project "Science-IT" at Aalto University.

References

[1] M. Behbahani, C. Lam, and P. R. J. Östergård, *On triple systems and strongly regular graphs*, J. Combin. Theory Ser. A **119** (2012), no. 7, 1414–1426, DOI 10.1016/j.jcta.2012.03.013. MR2925933

[2] G. Brunel, *Sur les deux systèmes de triades de trieze éléments*, Journal de Mathématiques Pures et Appliquées, Cinquième Série **7** (1901), 305–330.

[3] C. J. Colbourn, J. H. Dinitz, and I. M. Wanless, *Latin squares*, In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, pages 135–152. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[4] C. J. Colbourn, A. D. Forbes, M. J. Grannell, T. S. Griggs, P. Kaski, P. R. J. Östergård, D. A. Pike, and O. Pottonen, *Properties of the Steiner triple systems of order 19*, Electron. J. Combin. **17** (2010), no. 1. MR2661401 (2011g:05041)

[5] C. J. Colbourn, M. A. Oravas, and R. S. Rees, *Steiner triple systems with disjoint or intersecting subsystems*, J. Combin. Des. **8** (2000), no. 1, 58–77, DOI 10.1002/(SICI)1520-6610(2000)8:1⟨1::AID-JCD1⟩3.0.CO;2-N. MR1728889 (2000j:05021)

[6] C. J. Colbourn and A. Rosa, *Triple Systems*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1999. MR1843379 (2002h:05024)

[7] F. N. Cole, L. D. Cummings, and H. S. White, *The complete enumeration of triad systems in* 15 *elements*, Proceedings of the National Academy of Sciences of the United States of America, **3** (1917), 197–199.

[8] V. De Pasquale, *Sui sistemi ternari di* 13 *elementi*, Rendiconti. Reale Istituto Lombardo di Science e Lettere. Serie II. **32** (1899), 213–221.

[9] R. Déherder, *Recouvrements*, PhD thesis, Université Libre de Bruxelles, 1976.

[10] J. Doyen and R. M. Wilson, *Embeddings of Steiner triple systems*, Discrete Math. **5** (1973), 229–239. MR0327539 (48 #5881)

[11] I. A. Faradžev, *Constructive enumeration of combinatorial objects* (English, with French summary), Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976), Colloq. Internat. CNRS, vol. 260, CNRS, Paris, 1978, pp. 131–135. MR539959 (80i:05049)

[12] A. Hulpke, P. Kaski, and P. R. J. Östergård, *The number of Latin squares of order 11*, Math. Comp. **80** (2011), no. 274, 1197–1219, DOI 10.1090/S0025-5718-2010-02420-2. MR2772119 (2011m:05064)

[13] P. Kaski and P. R. J. Östergård, *There exists no* $(15, 5, 4)$ *RBIBD*, J. Combin. Des. **9** (2001), no. 5, 357–362, DOI 10.1002/jcd.1016. MR1849618 (2002f:05030)

[14] P. Kaski and P. R. J. Östergård, *The Steiner triple systems of order 19*, Math. Comp. **73** (2004), no. 248, 2075–2092, DOI 10.1090/S0025-5718-04-01626-6. MR2059752 (2005b:05035)

[15] P. Kaski and P. R. J. Östergård, *One-factorizations of regular graphs of order 12*, Electron. J. Combin. **12** (2005), Research Paper 2, 25 pp. (electronic). MR2134165 (2005m:05179)

[16] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs*, Algorithms and Computation in Mathematics, vol. 15, Springer-Verlag, Berlin, 2006. With 1 DVD-ROM (Windows, Macintosh and UNIX). MR2192256 (2008a:05002)

[17] P. Kaski and P. R. J. Östergård, *There are* $1,132,835,421,602,062,347$ *nonisomorphic one-factorizations of* K_{14}, J. Combin. Des. **17** (2009), no. 2, 147–159, DOI 10.1002/jcd.20188. MR2489440

[18] P. Kaski, P. R. J. Östergård, S. Topalova, and R. Zlatarski, *Steiner triple systems of order 19 and 21 with subsystems of order 7*, Discrete Math. **308** (2008), no. 13, 2732–2741, DOI 10.1016/j.disc.2006.06.038. MR2413971 (2009f:05032)

[19] A. Kerber, *Applied Finite Group Actions*, 2nd ed., Algorithms and Combinatorics, vol. 19, Springer-Verlag, Berlin, 1999. MR1716962 (2000j:05129)

[20] D. E. Knuth, *Dancing links*, In J. Davies, B. Roscoe, and J. Woodcock, editors, Millennial Perspectives in Computer Science, pages 187–214, Palgrave, Basingstoke, England, 2000.

[21] R. Mathon and A. Rosa, *2-*(v, k, λ) *designs of small order*, In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, pages 25–58. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[22] B. D. McKay. *nauty* User's Guide (Version 1.5), Technical Report TR-CS-90-02, Computer Science Department, Australian National University, Canberra, 1990.

[23] B. D. McKay, *Isomorph-free exhaustive generation*, J. Algorithms **26** (1998), no. 2, 306–324, DOI 10.1006/jagm.1997.0898. MR1606516 (98k:68132)

[24] B. D. McKay, A. Meynert, and W. Myrvold, *Small Latin squares, quasigroups, and loops*, J. Combin. Des. **15** (2007), no. 2, 98–119, DOI 10.1002/jcd.20105. MR2291523 (2007j:05030)

[25] R. C. Read, *Every one a winner; or how to avoid isomorphism search when cataloguing combinatorial configurations*, Algorithmic aspects of combinatorics (Conf., Vancouver Island, B.C., 1976), 1978, pp. 107–120. MR0491273 (58 #10537)

[26] N. V. Semakov and V. A. Zinov′ev, *Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs* (Russian), Problemy Peredači Informacii **4** (1968), no. 2, 3–10; English transl., Problems of Information Transmission **4** (1968), no. 2, 1–7 (1971). MR0347445 (49 #12165)

[27] D. R. Stinson and E. Seah, 284 457 *Steiner triple systems of order* 19 *contain a subsystem of order* 9, Math. Comp. **46** (1986), no. 174, 717–729, DOI 10.2307/2008010. MR829642 (87c:05027)

[28] H. S. White, F. N. Cole, and L. D. Cummings, *Complete classification of triad systems on fifteen elements*, Memoirs of the National Academy of Sciences **14** (1919) no. 2, 1–89.

Helsinki Institute for Information Technology HIIT, Department of Information and Computer Science, Aalto University, P.O. Box 15400, 00076 Aalto, Finland

Department of Communications and Networking, Aalto University School of Electrical Engineering, P.O. Box 13000, 00076 Aalto, Finland

Department of Communications and Networking, Aalto University School of Electrical Engineering, P.O. Box 13000, 00076 Aalto, Finland