There exists no Steiner system $S(4, 5, 17)$

Patric R. J. Östergård [1], Olli Pottonen [1,2]

Department of Communications and Networking, Helsinki University of Technology, PO Box 3000, 02015 TKK, Finland

Abstract

If a Steiner system $S(4, 5, 17)$ exists, it would contain derived $S(3, 4, 16)$ designs. By relying on a recent classification of the $S(3, 4, 16)$, an exhaustive computer search for $S(4, 5, 17)$ is carried out. The search shows that no $S(4, 5, 17)$ exists, thereby ruling out the existence of Steiner systems $S(t, t + 1, t + 13)$ for $t \geq 4$.

Key words: Derived design; Exact cover problem; Steiner system

1 Introduction

For integers $2 \leq t < k < v$, a *Steiner system* $S(t, k, v)$ is a pair $(V, \mathcal{B})$, where V is a v-set of *points* and $\mathcal{B}$ is a collection of k-subsets of V, called *blocks*, such that every t-subset of V is contained in exactly one block. Steiner systems $S(2, 3, v)$, $S(3, 4, v)$ and $S(4, 5, v)$ are called Steiner triple, quadruple and quintuple systems, respectively. The parameter v is called the *order* of

Email addresses: patric.ostergard@tkk.fi (Patric R. J. Östergård), olli.pottonen@tkk.fi (Olli Pottonen).

[1] Supported in part by the Academy of Finland, Grant Numbers 107493 and 110196.

[2] Supported in part by the Graduate School in Electronics, Telecommunication and Automation and a grant from the Foundation of Technology, Finland (Tekniikan edistämissäätiö).

the system. The point set of a Steiner system $\mathcal{Q}$ is denoted by $V(\mathcal{Q})$ and the block set by $B(\mathcal{Q})$.

Steiner triple systems exist exactly when $v \equiv 1$ or $3 \pmod 6$, and Steiner quadruple systems exactly when $v \equiv 2$ or $4 \pmod 6$ [2]. Furthermore, by considering derived designs it is easy to see that $v \equiv 3$ or $5 \pmod 6$ is a necessary condition for the existence of Steiner quintuple systems. Also, since the number of blocks in a $S(4,5,v)$ is $\binom{v}{4}\Big/\binom{5}{4}$, which must be an integer, $v \not\equiv 4 \pmod 5$ is another necessary condition. It is still an open problem to find sufficient conditions for the existence of Steiner quintuple systems. For $v = 11$, there exists a unique Steiner quintuple system [1] and for $v = 15$, no Steiner quintuple systems exists [12]. By taking derived designs of known $S(5,6,v)$ [2], it follows that Steiner quintuple systems exist for $v = 23, 35, 47, 71, 83, 107, 131, 167, 243$. For $v = 17$ the existence problem is a longstanding open problem; attempts to extend an $S(3,4,16)$ to an $S(4,5,17)$ have not been successful [15]. However, there exists a unique $S(4,\{5,6\},17)$, that is, Steiner system containing blocks of 5 and 6 points [9]; see also [14]. It is known that an $S(4,5,17)$ could not have nontrivial automorphisms [4].

A bijection $f : V \to V'$ maps a design $\mathcal{Q} = (V, \mathcal{B})$ to the design $f(\mathcal{Q}) = (V', \mathcal{B}')$ with block set $\mathcal{B}' = \{f(B) : B \in \mathcal{B}\}$. The designs $\mathcal{Q}$ and $f(\mathcal{Q})$ are said to be *isomorphic* and f is called an *isomorphism*. An isomorphism that maps a design onto itself is an *automorphism*. For any set V, the set of all bijections of V onto itself is a group called the *symmetric group* on V and is denoted by $\mathrm{Sym}(V)$. Now the definition above of how these functions map designs is a group action. The *automorphism group* of a design $\mathcal{Q} = (V, \mathcal{B})$ is the group $\mathrm{Aut}(\mathcal{Q}) := \{\gamma \in \mathrm{Sym}(V) : \gamma(\mathcal{Q}) = \mathcal{Q}\}$.

Let $\mathcal{Q} = (V, \mathcal{B})$ be an $S(t,k,v)$ and $p \in V$. The *derived design* of $\mathcal{Q}$ induced by p is defined as $\mathcal{Q}_p = (V_p, \mathcal{B}_p)$ with

$$V_p = V \setminus \{p\}, \quad \mathcal{B}_p = \{B \setminus \{p\} : p \in B \in \mathcal{B}\}.$$

Clearly $\mathcal{Q}_p$ is an $S(t-1,k-1,v-1)$. Accordingly the existence of an $S(t,k,v)$ implies the existence of an $S(t-1,k-1,v-1)$. For two points p, q we can consider a derived design of a derived design, $(\mathcal{Q}_p)_q$, which we will denote by $\mathcal{Q}_{p,q}$. Derivation is commutative, that is, $\mathcal{Q}_{p,q} = \mathcal{Q}_{q,p}$.

In the rest of the paper we describe an exhaustive search for $S(4,5,17)$. By running the computer search we found that no $S(4,5,17)$ exists. Thus no $S(t,t+1,t+13)$ exists for $t \geq 4$, since such designs would have an $S(4,5,17)$ as a derived design. It is already known that no such design exists for $t \geq 12$, since the number of blocks in an $S(12,13,25)$ would be $\binom{25}{12}/\binom{13}{12}$, which is not an integer.

2 The Search

We assume that the point set of a putative $S(4,5,17)$ is $\mathbb{Z}_{17} = \{0,1,\ldots,16\}$.

Let $\mathcal{Q}$ be an $S(4,5,17)$. Then $\mathcal{Q}$ can be represented as a list $(\mathcal{Q}_{16}, \mathcal{Q}_{15}, \ldots, \mathcal{Q}_0)$ of derived designs. (Note that the list contains labelled designs, not arbitrary isomorphism class representatives.) In the search, we first construct a set of pairs $(\mathcal{Q}_{16}, \mathcal{Q}_{15})$, called *seeds*, of derived designs of a putative $S(4,5,17)$ such that any $S(4,5,17)$ has an isomorphic copy $\mathcal{Q}$ such that $(\mathcal{Q}_{16}, \mathcal{Q}_{15})$ is a seed. Note that the two designs of a seed have a common derived triple system, as $\mathcal{Q}_{16,15} = \mathcal{Q}_{15,16}$. The seeds are classified in two independent ways based on a recent classification [6] of $S(3,4,16)$. Using a straightforward exhaustive search we finally try to augment each seed to an $S(4,5,17)$.

Instead of using the straightforward exhaustive search in the final stage, we could use the classification of $S(3,4,16)$ to find all extensions of seeds $(\mathcal{Q}_{16}, \mathcal{Q}_{15})$ to triples $(\mathcal{Q}_{16}, \mathcal{Q}_{15}, \mathcal{Q}_{14})$, extend these to $(\mathcal{Q}_{16}, \mathcal{Q}_{15}, \mathcal{Q}_{14}, \mathcal{Q}_{13})$, and so on, finally ending up with a complete $S(4,5,17)$, if such a design exists. However, this alternative approach is harder to implement and possibly even slower than the method used.

2.1 Generating seeds

There are 80 nonisomorphic $S(2,3,15)$ [3,13] and 1,054,163 nonisomorphic $S(3,4,16)$ [6]. Let $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_{80}$ be isomorphism class representatives of the $S(2,3,15)$ such that each design has point set $\mathbb{Z}_{15}$. The isomorphism class representatives of the $S(3,4,16)$ are partitioned into 80 subsets $\mathscr{C}_i$, $i = 1,\ldots,80$, such that $\mathcal{R} \in \mathscr{C}_i$ exactly when i is the smallest integer for which $\mathcal{T}_i$ is isomorphic to some derived design of $\mathcal{R}$. By relabeling if necessary we can assume that for any $\mathcal{R} \in \mathscr{C}_i$ we have $V(\mathcal{R}) = \mathbb{Z}_{16}$ and $\mathcal{R}_{15} = \mathcal{T}_i$.

Isomorphism testing for $S(2,3,15)$ is straightforward as the multiset of 15 integers with the numbers of Pasch configurations each point intersects is a certificate; a *Pasch configuration* is a set of four triples isomorphic to $\{\{a,b,c\},\{a,d,e\},\{b,d,f\},\{c,e,f\}\}$. For computing isomorphisms and automorphisms we use the graph automorphism software *nauty* [11].

Let $\mathcal{Q}$ be an isomorphism class representative of a putative $S(4,5,17)$ and let i be the smallest integer for which some derived triple system of a derived quadruple system of $\mathcal{Q}$ is isomorphic to $\mathcal{T}_i$. By relabeling if necessary we can assume that the derived design $\mathcal{Q}_{16}$ is equal to some $\mathcal{R} \in \mathscr{C}_i$. The design $\mathcal{Q}_{15}$ is then a Steiner quadruple system satisfying the following conditions: it has point set $\mathbb{Z}_{17} \setminus \{15\}$, its derived triple system $(\mathcal{Q}_{15})_{16}$ is equal to $\mathcal{T}_i$, none of its

derived triple systems is isomorphic to any $\mathcal{T}_j$ with $j < i$, and it has no blocks in common with $\mathcal{Q}_{16}$. This implies that $\mathcal{Q}_{15}$ is isomorphic to some $\mathcal{G}' \in \mathscr{C}_i$. Now we define seeds as pairs $(\mathcal{Q}_{16}, \mathcal{Q}_{15})$ such that $\mathcal{Q}_{16} \in \mathscr{C}_i$ and $\mathcal{Q}_{15}$ satisfies the conditions listed in this paragraph.

Thus all seeds can be found by iterating over every i, $\mathcal{R}, \mathcal{G} \in \mathscr{C}_i$ and considering all pairs $(\mathcal{R}, \mathcal{G}')$ such that $\mathcal{G}'$ is isomorphic to $\mathcal{G}$ and $\mathcal{G}'_{16} = \mathcal{T}_i$. However all such pairs are not seeds since the two $S(3, 4, 16)$ may have common blocks.

We have yet to describe how to find every possible $\mathcal{G}'$. We give two different algorithms. Since $\mathcal{G}'$ has point set $\mathbb{Z}_{17} \setminus \{15\}$ and the algorithms use the more convenient set $\mathbb{Z}_{16}$, the point 15 need to be replaced with 16.

Algorithm 1 *Assume $\mathscr{C}_i$ and $\mathcal{T}_i$ are given, $V(\mathcal{G}) = \mathbb{Z}_{16}$ for every $\mathcal{G} \in \mathscr{C}_i$ and $V(\mathcal{T}_i) = \mathbb{Z}_{15}$. For each $\mathcal{G} \in \mathscr{C}_i$ and $k \in \mathbb{Z}_{16}$ such that $\mathcal{G}_k$ is isomorphic to $\mathcal{T}_i$, find a permutation γ_k such that $\gamma_k(\mathcal{G}_k) = \mathcal{T}_i$ and $\gamma_k(k) = 15$. For every $\mathcal{G}$, γ_k and $\alpha \in \mathrm{Aut}(\mathcal{T}_i)$, output the design $\alpha(\gamma_k(\mathcal{G}))$.*

All permutations act on $\mathbb{Z}_{16}$; we define $\alpha(15) = 15$ for $\alpha \in \mathrm{Aut}(\mathcal{T}_i) \subset \mathrm{Sym}(\mathbb{Z}_{15})$.

Theorem 1 *Algorithm 1 above outputs every $\mathcal{G}'$ such that $\mathcal{G}'$ is isomorphic to some $\mathcal{G} \in \mathscr{C}_i$, $V(\mathcal{G}') = \mathbb{Z}_{16}$ and $\mathcal{G}'_{15} = \mathcal{T}_i$.*

Proof. First note that for any Steiner system $\mathcal{Q}$, point q, and permutation $\delta \in \mathrm{Sym}(V(\mathcal{Q}))$, we have $\delta(\mathcal{Q}_q) = \delta(\mathcal{Q})_{\delta(q)}$.

Let $\mathcal{G}$ and $\mathcal{G}'$ satisfy the assumptions. Because $\mathcal{G}$ and $\mathcal{G}'$ are isomorphic, there exists an $\beta \in \mathrm{Sym}(\mathbb{Z}_{16})$ such that $\beta(\mathcal{G}) = \mathcal{G}'$. Let $k = \beta^{-1}(15)$. Since $\beta(\mathcal{G}_k) = \beta(\mathcal{G})_{\beta(k)} = \mathcal{G}'_{15} = \mathcal{T}_i$, the algorithm finds a permutation γ with $\gamma(\mathcal{G}_k) = \mathcal{T}_i$ and $\gamma(k) = 15$.

Since $\beta(\mathcal{G}_k) = \mathcal{T}_i = \gamma(\mathcal{G}_k)$, we have $\beta\gamma^{-1} \in \mathrm{Aut}(\mathcal{T}_i)$. Let $\alpha = \beta\gamma^{-1}$. The algorithm outputs $\mathcal{G}' = \beta(\mathcal{G}) = \alpha(\gamma(\mathcal{G}))$. □

Algorithm 2 *Assume $\mathscr{C}_i$ and $\mathcal{T}_i$ are given, $V(\mathcal{G}) = \mathbb{Z}_{16}$ for every $\mathcal{G} \in \mathscr{C}_i$ and $V(\mathcal{T}_i) = \mathbb{Z}_{15}$. Consider every $S(3, 4, 16)$ $\mathcal{G}'$ with $\mathcal{G}'_{15} = \mathcal{T}_i$ and output $\mathcal{G}'$ if none of its derived systems is isomorphic to $\mathcal{T}_j$ with $j < i$.*

In the classification of $S(3, 4, 16)$ [6], a search for every $\mathcal{G}'$ with $\mathcal{G}'_{16} = \mathcal{T}_i$ and $V(\mathcal{G}') = \mathbb{Z}_{16}$ was carried out using a method similar to that described in Section 2.2. Possibility to reuse the data made Algorithm 2 practical.

To gain more confidence in the results of our computer search, we searched for all seeds using both Algorithm 1 and Algorithm 2. The searches resulted

in isomorphic sets of seeds.

The isomorphism class representatives may be ordered in 80! different ways for the list $\mathcal{T}_1, \ldots, \mathcal{T}_{80}$. Furthermore, for each order, the isomorphism class representatives in the sets $\mathscr{C}_i$ may be chosen in a great number of ways and listing the choices here is infeasible. Since different choices lead to different sets of seeds, an independent verification might produce a different number of seeds. Regardless of these choices, however, the seeds will always have the crucial property that, up to isomorphism, each $S(4, 5, 17)$ can be obtained by extending a seed.

The computational requirements for finding the seeds depend on the order of the triple systems. The order used in this work is shown in Table 1, which lists the indices assigned to the designs $\mathcal{T}_1, \ldots, \mathcal{T}_{80}$ in [10]. That is, $\mathcal{T}_1$ is #77 in [10], $\mathcal{T}_2$ is #67, etc.

INSERT TABLE 1 ABOUT HERE

2.2 Extending seeds

The task of extending a seed to an $S(4, 5, 17)$ can be formulated as an instance of the exact cover problem. In the exact cover problem, we are given a finite set U and a set $\mathscr{S}$ of subsets of U. The task is to produce a partition of U consisting of sets in $\mathscr{S}$.

First consider the task of producing an $S(4, 5, 17)$. In this case the set U consists of all quadruples, and $\mathscr{S}$ of all candidate blocks. More formally, let $q(A) = \{S \subset A : |S| = 4\}$ be the set of all quadruples contained in a set A. Now $U = q(\mathbb{Z}_{17})$ and $\mathscr{S} = \{q(B) : B \subset \mathbb{Z}_{17},\ |B| = 5\}$.

Extending a seed is the same as producing an $S(4, 5, 17)$ containing a given set of blocks. This is formulated as an exact cover problem by suitably restricting the sets U and $\mathscr{S}$ defined above.

The *libexact* software [7], based on an algorithm suggested by Knuth [8], was used for this search.

3 Results

No $S(4, 5, 17)$ was found when running the search, and we conclude that none exists. Thus no $S(t, t + 1, t + 13)$ exists for $4 \leq t \leq 11$; for $t \geq 12$ the nonexistence was already known.

The computationally intensive part of this result was the earlier classification of $S(3,4,16)$ [6], which required several years of CPU time, while all searches described in this paper required less than two days. In total 5,194,881 seeds were obtained during this process.

We corroborated earlier classification results for $S(4,5,11)$ and $S(4,5,15)$. Indeed, no $S(4,5,15)$ was found and a unique $S(4,5,11)$ was obtained. Only a few seconds of CPU time were required in these cases.

The next v for which existence of $S(4,5,v)$ remains open is 21. As the number of Steiner triple systems of order 19 has been shown [5] to be 11,084,874,829, classification of $S(3,4,20)$ and $S(4,5,21)$ using the approaches in [6] and here, respectively, is not feasible.

Acknowledgments

The authors thank Petteri Kaski for helpful suggestions.

References

[1] J. A. Barrau, On the combinatory problem of Steiner, Proc. Sect. Sci. Konink. Akad. Wetensch. Amsterdam 11 (1908) 352–360.

[2] C. J. Colbourn, R. Mathon, Steiner systems, in: C. J. Colbourn, J. H. Dinitz (Eds.), Handbook of Combinatorial Designs, 2nd ed., Chapman & Hall/CRC, Boca Raton, 2007, pp. 101–109.

[3] F. N. Cole, L. D. Cummings, H. S. White, The complete enumeration of triad systems in 15 elements, Proc. Nat. Acad. Sci. U.S.A. 3 (1917) 197–199.

[4] R. H. F. Denniston, No $S(4,5,17)$ could have automorphisms, presented at the 6th British Combinatorial Conference, Royal Holloway College, London, 11–15 July 1977.

[5] P. Kaski, P. R. J. Östergård, The Steiner triple system of order 19, Math. Comp. 73 (2004) 2075–2092.

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

[7] P. Kaski, O. Pottonen, libexact user's guide, Version 1.0, in preparation.

[8] D. E. Knuth, Dancing links, in: J. Davies, B. Roscoe, J. Woodcock (Eds.), Millennial Perspectives in Computer Science, Palgrave Macmillan, Basingstoke, 2000, pp. 187–214.

[9] E. S. Kramer, R. Mathon, Proper $S(t, \mathscr{K}, \nu)$'s for $t \geq 3$, $\nu \leq 16$, $|\mathscr{K}| > 1$ and their extensions, J. Combin. Des. 3 (1995) 411–425.

[10] R. A. Mathon, K. T. Phelps, A. Rosa, Small Steiner triple systems and their properties, Ars Combin. 15 (1983) 3–110; and 16 (1983) 286.

[11] B. D. McKay, *nauty* user's guide (version 1.5), Technical Report TR-CS-90–02, Computer Science Department, Australian National University, Canberra, 1990.

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

[13] H. S. White, F. N. Cole, L. D. Cummings, Complete classification of triad systems on fifteen elements, Memoirs Nat. Acad. Sci. U.S.A. 14 (1919) 1–89.

[14] J. L. Yucas, Extending $AG(4, 2)$ to $S(4, \{5, 6\}, 17)$, J. Combin. Des. 7 (1999) 113–117.

[15] J. L. Yucas, Extensions of $PG(3, 2)$ with bases, Australas. J. Combin. 25 (2002) 125–131.

Table 1
Indexing of $S(2,3,15)$

77	67	72	68	73	42	71	66	65	78	79	80	69	50	37	49	46
57	48	56	51	60	38	45	55	74	52	75	44	43	47	54	41	53
40	35	58	39	62	70	64	36	59	63	76	33	34	32	30	28	27
24	23	31	25	29	26	21	22	61	11	20	12	19	9	10	18	15
8	13	14	17	4	6	5	16	3	7	2	1					