ALGEBRAIC COMBINATORICS

Jean Doyen & William M. Kantor

Automorphism groups of Steiner triple systems

Volume 5, issue 4 (2022), p. 593-608.
https://doi.org/10.5802/alco.240

Algebraic Combinatorics is published by The Combinatorics Consortium
and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

Algebraic Combinatorics
Volume 5, issue 4 (2022), p. 593–608
`https://doi.org/10.5802/alco.240`

Automorphism groups of Steiner triple systems

Jean Doyen & William M. Kantor

Abstract If G is a finite group then there is an integer M_G such that, for $u \geqslant M_G$ and $u \equiv 1$ or $3 \pmod 6$, there is a Steiner triple system U on u points for which $\mathrm{Aut}U \cong G$. If V is a Steiner triple system then there is an integer N_V such that, for $u \geqslant N_V$ and $u \equiv 1$ or $3 \pmod 6$, there is a Steiner triple system U on u points having V as an $\mathrm{Aut}U$-invariant subsystem such that $\mathrm{Aut}U \cong \mathrm{Aut}V$ and $\mathrm{Aut}U$ induces $\mathrm{Aut}V$ on V.

1. Introduction

Mendelsohn [5] proved that any finite group G is isomorphic to the automorphism group of some Steiner triple system. In his proof he modified the Steiner triple system of points and lines of a projective space $PG(n,2)$, producing a system having $2^{n+1}-1$ points for some n. This leads to the natural question: what restrictions are there on the number of points of a Steiner triple system U such that $\mathrm{Aut}U \cong G$? In order to admit G as a group of automorphisms, U cannot be too small:

Theorem 1.1. *If G is a finite group then there is an integer M_G such that, for $u \geqslant M_G$ and $u \equiv 1$ or $3 \pmod 6$, there is a Steiner triple system U on u points for which* $\mathrm{Aut}U \cong G$.

As with most theorems of this sort, the proof does not distinguish between cyclic groups and simple groups. It is known that $M_G = 15$ when $G = 1$ [4]. Our arguments cannot deal with such small Steiner triple systems.

The preceding theorem is an immediate consequence of [5] and the following more general result, which is the main theorem of this paper:

Theorem 1.2. *If $V_\star$ is a Steiner triple system then there is an integer $N_{V_\star}$ such that, for $u \geqslant N_{V_\star}$ and $u \equiv 1$ or $3 \pmod 6$, there is a Steiner triple system U on u points having $V_\star$ as an $\mathrm{Aut}U$-invariant subsystem such that $\mathrm{Aut}U \cong \mathrm{Aut}V_\star$ and $\mathrm{Aut}U$ induces $\mathrm{Aut}V_\star$ on $V_\star$.*

Manuscript received 10th August 2018, revised 25th March 2022 and 10th March 2020, accepted 26th March 2022.

Keywords. Steiner triple system, Automorphism group.

Acknowledgements. The research of the second author was supported in part by a grant from the Simons Foundation.

Cameron [1] considered a similar question. He proved that, if V is a Steiner triple system of order v (i.e. having v points), and if $u > 6v^2$ with $u \equiv 1$ or $3 \pmod 6$, then there is a Steiner triple system U of order u in which V can be embedded in such a way that every automorphism of V can be extended to U. His proof and ours use a familiar and wonderful construction of Moore [6] from the not-so-distant past that combines three Steiner triple systems to produce a fourth.

The proof of Theorem 1.2 first enlarges $V_\star$, without changing its automorphism group, as part of a process to obtain a Steiner triple system U having a rich geometry of $PG(m,2)$ subsystems for various m (cf. Remark 3.1). This process involves Lemma 2.3 and Proposition 2.5 (using [3]), and leads to our key tool: Proposition 3.8. The latter makes it straightforward in Proposition 3.9 to determine the automorphism group of the Steiner triple system U we construct.

The ugly bookkeeping parts of the proof (in Section 3.1.1 and especially in Section 3.1.2) ensure that we obtain all large u. Remark 3.10 contains poor bounds for M_G and $N_{V_\star}$, while Remark 3.11 comments on a difference between the bookkeeping approaches in [1] and here.

Results such as Theorem 1.1 are usually based on the action of G having many regular point-orbits. This is very much not the situation for Theorem 1.2: for our U the size of every point-orbit of $\mathrm{Aut}U$ is 1 or the size of a point-orbit of $\mathrm{Aut}V_\star$ on the original Steiner triple system $V_\star$.

There is also a result in [1] concerning a *partial Steiner triple system* V (a set of points, together with some triples of points, such that any two points are in at most one triple), and a partial Steiner triple U having V as a *subsystem* (so the points of V are among the points of U, and the triples of V are precisely those triples of U that are contained in V). It is shown in [1] that there is a function g such that, if V is a partial Steiner triple system of order v, and if $u > g(v)$ with $u \equiv 1$ or $3 \pmod 6$, then there is a Steiner triple system U of order u of which V is a subsystem such that every automorphism of V can be extended to U. In Section 4 we will use Theorem 1.2 to prove the following stronger result (along with variations):

Theorem 1.3. *If V is a partial Steiner triple system then there is an integer N'_V such that, for $u \geqslant N'_V$ and $u \equiv 1$ or $3 \pmod 6$, there is a Steiner triple system U on u points having V as an $\mathrm{Aut}U$-invariant subsystem such that $\mathrm{Aut}U \cong \mathrm{Aut}V$ and $\mathrm{Aut}U$ induces $\mathrm{Aut}V$ on V.*

2. Background

2.1. Moore's XYV.

We will use a 125 year old construction due to Moore [6, p. 276].(1) (This construction is in many sources, such as [7, p. 235] and [1].)

Let $X \subset Y$ and V be three STSs (i.e. Steiner triple systems), and label $Y - X$ in any way by the elements of a cyclic group A of order $|Y| - |X|$. (We always use $|Y|$ to denote the order of an STS Y.) Then $U := X \cup (V \times A)$ is (the set of points of) an STS, with triples

(M1) those of X,

(M2) $(v,a_1),(v,a_2)$ and $\begin{cases} x & \text{if } a_1,a_2,x \text{ is a triple in } Y,\ a_i \in Y-X,\ x \in X \\ (v,a_3) & \text{if } a_1,a_2,a_3 \text{ is a triple in } Y,\ a_i \in Y-X, \end{cases}$

and

(M3) $(v_1,a_1),(v_2,a_2),(v_3,a_3)$ if v_1,v_2,v_3 is a triple in V and $a_1a_2a_3 = 1$.

---

(1) Moore used it to produce two nonisomorphic STSs of any admissible order > 13. Unfortunately, his method for proving nonisomorphism [6, pp. 279–281] has a significant gap.

The fact that A is cyclic, not just abelian, is used in several places, most significantly in Lemma 3.4 and Proposition 3.9.

Clearly $|U| = |X| + |V|(|Y| - |X|)$.

2.2. Enlarging Y. The STSs X and Y in the preceding section have unknown structure. While this does not matter for X, we will use elementary constructions to enlarge Y in order to give it significant geometric structure (Lemmas 2.2 and 2.3).

Given an STS Y_0 there is a standard construction for an STS $2Y_0 + 1$ on $2|Y_0| + 1$ points, labeled using $Y_0 \dot\cup Y_0' \dot\cup *_0$ for a "distinguished" new point $*_0$ and a bijection $y \mapsto y'$ sending $Y_0 \to Y_0'$, and triples of the form

$$abc \text{ in } Y_0 \qquad *_0aa' \text{ etc.} \qquad a'b'c \text{ etc.}$$

Here $|2Y_0 + 1| \equiv 3 \pmod 4$ and Y_0 is a subsystem of $2Y_0 + 1$. If Y_0 is a hyperplane of a projective space $P = PG(n, 2)$ then $P \cong 2Y_0 + 1$. Thus, if Y_0 is a projective space then so is $2Y_0 + 1$.

Definition 2.1. *An STS is* $PG(2,2)$-pointed *with respect to a point* p *if any two triples containing* p *generate a* $PG(2,2)$ *subsystem.*

An STS with more than seven points is $PG(3,2)$-2-pointed *with respect to two points if any four points including these two generate a* $PG(k,2)$ *subsystem for* $k = 2$ *or 3.*

An STS is $PG(3,2)$-paired *if any two points are in a* $PG(3,2)$ *subsystem.* This is the key geometric property needed in the proof of *Proposition* 3.8*(i).*

Lemma 2.2. *If* Y_0 *is an STS with more than one point, then*

(i) $2Y_0 + 1$ *is* $PG(2,2)$*-pointed with respect to the distinguished point* $*_0$,

(ii) $Y_1 := 2(2Y_0 + 1) + 1$ *is* $PG(3,2)$*-2-pointed* (*with respect to some pair of its points*), *and*

(iii) Y_1 *is* $PG(3,2)$*-paired of order* $4|Y_0| + 3 \equiv 7 \pmod 8$.

Proof. (i) Two triples $*_0aa'$, $*_0bb'$ of $2Y_0 + 1$ containing $*_0$ generate a $PG(2,2)$ subsystem with triples

$$abc \qquad *_0aa',\ *_0bb',\ *_0cc' \qquad a'b'c,\ a'bc',\ ab'c'.$$

(ii) The pair $\{*_0, *_1\}$ has the required property, where $*_1$ is the new point used to produce $Y_1 = 2(2Y_0 + 1) + 1$ from $2Y_0 + 1$. For, if $*_0, *_1, a, b$ are four points of Y_1 then $*_1, a$ and $*_1, b$ are in triples meeting $2Y_0 + 1$ at points $\bar a$ and $\bar b$, respectively. Then $*_0, \bar a, \bar b$ are in a $PG(2,2)$ subsystem Z of $2Y_0 + 1$, and $2Z + 1$ is a $PG(3,2)$ subsystem of Y_1 containing $*_0, *_1, a, b$.

(iii) This is immediate by (ii). ☐

Admissible integers are those $\equiv 1$ or $3 \pmod 6$; these are precisely the possible orders of STSs.

We use the standard *direct product* $A \times B$ of STSs A and B: the STS for which $A \times B$ is the set of points and whose triples have the form $\{(a, b_1), (a, b_2), (a, b_3)\}$, $\{(a_1, b), (a_2, b), (a_3, b)\}$ or $\{(a_1, b_1), (a_2, b_2), (a_3, b_3)\}$ for $a \in A$, $b \in B$, and ordered triples (a_1, a_2, a_3) from A and (b_1, b_2, b_3) from B. Clearly, if $a \in A$ and $b \in B$ then $a \times B$ and $A \times b$ are subsystems of $A \times B$.

Lemma 2.3.

(i) *If* A *and* B *are* $PG(3,2)$*-paired STSs then so is* $A \times B$.

(ii) *An integer is the order of a* $PG(3,2)$*-paired STS if it is admissible*, *at least* 15 *and* $\equiv 7 \pmod 8$, *or if it is a product of integers each of which behaves that way.*

Proof. (i) Given two points (a_1, b_1) and (a_2, b_2) of $A{\times}B$ there are $PG(3,2)$ subsystems A_0 of A containing a_1, a_2 and B_0 of B containing b_1, b_2.

If $a_1 \neq a_2$ and $b_1 \neq b_2$ there is an isomorphism $\phi\colon A_0 \to B_0$ sending $a_i \mapsto b_i$ for $i = 1, 2$. Then $\{(a, a^\phi) \mid a \in A_0\} \subset A_0{\times}B_0$ is a $PG(3,2)$ subsystem of $A{\times}B$ containing the given points.

If $a_1 = a_2$ then $a_1{\times}B_0$ is a $PG(3,2)$ subsystem containing (a_1, b_1) and (a_2, b_2). If $b_1 = b_2$ then $A_0{\times}b_1$ is a $PG(3,2)$ subsystem containing (a_1, b_1) and (a_2, b_2).

(ii) Any admissible integer $8n + 7 \geqslant 15$ can be written $2(2(2n + 1) + 1) + 1$ with $2n+1 > 1$ and admissible. By Lemma 2.2(iii) there is a $PG(3,2)$-paired STS of order $8n + 7$. Now use (i). ☐

2.3. Enlarging $V_\star$. The STS $V_\star$ in Theorem 1.2 has unknown structure. As we did with Y_0 in Section 2.2, we will enlarge $V_\star$ to STSs having significant geometric structure (Corollary 2.6). Since our arguments are based on finite geometry, we briefly describe how "close" each STS in [3] is to a projective space.

Let V be a vector space over $F = \mathbf{F}_{16}$ with basis $v_1, \dots, v_n$. This produces a vector space and a projective space over $\mathbf{F}_2$. Let $F^* = \langle\theta\rangle$. Suitably modify the $PG(3,2)$ subspaces determined by the $\mathbf{F}_2$-spaces Fv_i and $F(v_i + \theta v_j)$ for all i, j, in order to obtain an STS D. Only a tiny portion of the underlying $PG(4n - 1, 2)$ is altered: every subspace of that projective space meeting $U \coloneqq \bigcup_{i,j} \big(Fv_i \cup F(v_i + \theta v_j)\big)$ at most once is a subsystem of D. As in [3, Theorem 1.1 and Sec. 7(1c)], this provides the flexibility needed for the following

Remark 2.4. *If $n \geqslant 6$ then there is an STS D such that*

(i) $\mathrm{Aut}D = 1$,
(ii) *D has $16^n - 1$ points, and*
(iii) *given points a, b of D there is a point c such that each pair $\{a, c\}$ and $\{b, c\}$ is in some $PG(n - 1, 2)$ subsystem of D.*

See [3] for the modifications of the above $PG(3,2)$ subsystems needed to obtain (i). The subsystems in (iii) are crucial for our proof of Theorem 1.2; we will obtain them less tediously than similar ones in [3]. Let $c \notin \bigcup_{u\in U}(\langle a, u\rangle_{\mathbf{F}_2} \cup \langle b, u\rangle_{\mathbf{F}_2})$ and consider the pair $\{a, c\}$. For $2 \leqslant j < n$ inductively increase a j-dimensional $\mathbf{F}_2$-subspace $J \supset \{a, c\}$ of V with $J \cap U \subseteq \langle a\rangle_{\mathbf{F}_2}$ to a $j + 1$-dimensional $\mathbf{F}_2$-subspace $J' \supset J$ with $J' \cap U = J \cap U$, noting that $|\bigcup_{u\in U}\langle J, u\rangle_{\mathbf{F}_2}| < 2^{j+1}(n + n(n-1))16 < |V|$.

Choose $n \geqslant 6$ so that $2^n - 1 > |V_\star| \geqslant 2^{n-6}$. Then *the image of any map from $PG(n - 1, 2)$ into $V_\star$ sending every collinear triple to a triple or a point must have size* 1. (Otherwise, since the map cannot be 1-1, restrict to a plane mapping onto a triple in order to obtain a contradiction: the preimages of the points of the triple would have to be pairwise disjoint, cover the plane, and be such that the line through two points of a preimage is contained in the preimage.)

Proposition 2.5. *Let D be as in the preceding Remark, and let $d \in D$.*

(i) *Every point of $V_\star{\times}D$ is in a $PG(n - 1, 2)$ subsystem of $V_\star{\times}D$,*
(ii) *$V_\star{\times}d$ is isomorphic to $V_\star$,*
(iii) *$V_\star{\times}d$ is an $\mathrm{Aut}(V_\star{\times}D)$-invariant subsystem of $V_\star{\times}D$ on which $\mathrm{Aut}(V_\star{\times}D)$ induces $\mathrm{Aut}(V_\star{\times}d)$, and $\mathrm{Aut}(V_\star{\times}D) \cong \mathrm{Aut}(V_\star{\times}d) \cong \mathrm{Aut}V_\star$, and*
(iv) *$|V_\star{\times}D| \equiv \pm 3 \pmod{12}$ and $16^5 < |V_\star{\times}D| < 2^{24}|V_\star|^5$.*

Proof. For (i), if $v \in V_\star$ then $v{\times}D$ is isomorphic to D, so use Remark 2.4(iii). Statement (ii) is obvious. For (iii) we need to determine $\mathrm{Aut}(V_\star{\times}D)$.

Every $PG(n-1, 2)$ subsystem in $V_\star{\times}D$ is a set of ordered pairs that projects onto subsystems of $V_\star$ and D, and hence induces a map from $PG(n - 1, 2)$ to $V_\star$ sending every collinear triple to a point or triple. As noted above, since $2^n-1>|V_\star|$ the image of that map is a point of $V_\star$. Thus, *every $PG(n-1,2)$ subsystem in $V_\star{\times}D$ lies in some subsystem $v{\times}D$, $v\in V_\star$.*

Consider the graph whose vertices are the $PG(n-1,2)$ subsystems of $V_\star{\times}D$, with two such subsystems joined if and only if they meet. We have just seen that every such subsystem is contained in some subsystem $v{\times}D$, $v\in V$. Since no two subsystems $v{\times}D$ meet, every connected component C of our graph lies in some subsystem $v{\times}D$; by Remark 2.4(iii), C is the set of $PG(n-1,2)$ subsystems of $v{\times}D$ and generates $v{\times}D$. Since $\mathrm{Aut}(V_\star{\times}D)$ permutes the connected components of our graph it also permutes the subsystems $v{\times}D$.

Let $h\in\mathrm{Aut}(V_\star{\times}D)$. If $v\in V_\star$ then $(v{\times}D)^h=v^{h'}{\times}D$ for some $v^{h'}\in V_\star$, where $h'\colon V_\star\to V_\star$ is bijective. We claim that the map *$h'\colon V_\star\to V_\star$ is in* $\mathrm{Aut}V_\star$. For, if v_1,v_2,v_3 is a triple of $V_\star$ and $d\in D$ then $(v_1,d),(v_2,d),(v_3,d)$ is a triple of $V_\star{\times}D$. Then so is $(v_1,d)^h,(v_2,d)^h,(v_3,d)^h$; this is $(v_1^{h'},d_1),(v_2^{h'},d_2),(v_3^{h'},d_3)$ with $d_i\in D$, so $v_1^{h'},v_2^{h'}$, $v_3^{h'}$ is a triple of $V_\star$, as claimed.

Now $h'\in\mathrm{Aut}V_\star$ induces $h^\bullet\in\mathrm{Aut}(V_\star{\times}d)$ sending $(v,d)\mapsto(v^{h'},d)$ for $v\in V_\star$, $d\in D$. We thus have two automorphisms h and $h^\bullet$ of $V_\star{\times}d$ sending each $v{\times}D$ to $v^{h'}{\times}D$. Then $h^\bullet h^{-1}$ sends each subsystem $v{\times}D$ to itself, induces an automorphism of each such subsystem, and hence is 1 by (ii) and Remark 2.4(i). Thus, $h=h^\bullet$ sends each subsystem $V_\star{\times}d$ to itself, and hence so does $\mathrm{Aut}(V_\star{\times}D)$. This proves that $\mathrm{Aut}(V_\star{\times}D)=(\mathrm{Aut}V_\star)\times 1_D$.

(iv) $|V_\star{\times}D|=(16^n-1)|V_\star|\equiv(16-1)|V_\star|\equiv 3|V_\star|\equiv\pm3\pmod{12}$ and $16^5<(16^n-1)|V_\star|<(2^n)^4|V_\star|\leqslant(2^6|V_\star|)^4|V_\star|$ since $|V_\star|\geqslant 2^{n-6}$. ☐

Corollary 2.6. *For sufficiently large integers n and m there are STSs $V_\star{\times}D$ and $V_\star{\times}D{\times}D'$ such that one of them, V, has the following properties*:

(i) $|V|\equiv 3\pmod{12}$, $|V|>16^5$, *and either* $|V|=|V_\star||D|=|V_\star|(16^n-1)$ *or* $|V|=|V_\star||D||D'|=|V_\star|(16^n-1)(16^m-1)$,
(ii) *Every point of V is in a $PG(3,2)$ subsystem of V, and*
(iii) *V has an* $\mathrm{Aut}V$*-invariant subsystem $V_\star{}'\cong V_\star$ on which* $\mathrm{Aut}V$ *induces* $\mathrm{Aut}V_\star{}'$, *and* $\mathrm{Aut}V\cong\mathrm{Aut}V_\star{}'\cong\mathrm{Aut}V_\star$.

Proof. Apply the proposition to $V_\star{\times}D$ in place of $V_\star$, using in place of D an STS D' of order 16^m-1 where $2^m-1>|V_\star{\times}D|\geqslant 2^{m-6}$. Since $3|V_\star|\equiv\pm3\pmod{12}$ either $|V_\star|(16^n-1)\equiv 3\pmod{12}$ or $|V_\star|(16^n-1)(16^m-1)\equiv 3\pmod{12}$. ☐

3. PROOF OF THEOREM 1.2

The proof proceeds in three stages: construction of an STS U (Section 3.1.1), determining that we have obtained all sufficiently large admissible integers as the order of some such U (Section 3.1.2), and using geometry to determine $\mathrm{Aut}U$ (Sections 3.3 and 3.4).

3.1. PRELIMINARIES AND NOTATION.

We will describe STSs X, Y and V that will be used to construct our STS U via Section 2.1.

3.1.1. *Properties of X, Y and V.*

We begin with notation and properties of these STSs. We note that properties (P1)(b) and (P3)(d) will be essential (in Proposition 3.8) for studying subsystems of U isomorphic to V or Y.

Let V_* be as in Theorem 1.2. Property (P1) concerns an STS V that will replace V_* in our arguments and has a rich geometric structure.

(P1) *V and v.*

(a) Use Corollary 2.6 to obtain an STS V on v points, where
$v \equiv 3 \pmod{12}$ and $v > 16^5$,
having (a copy of) $V_\star$ as an $\mathrm{Aut}V$-invariant subsystem on which $\mathrm{Aut}V$ induces $\mathrm{Aut}V_\star$ and such that $\mathrm{Aut}V \cong \mathrm{Aut}V_\star$. (Here V is not uniquely determined: it depends on choices for D, n and possibly D' and m that are made just once in the proof of Corollary 2.6.)

(b) Every point of V is in a $PG(3,2)$ subsystem of V (Corollary 2.6(ii)).

In (P2) and (P4) we will introduce further admissible integers y_1, y_2, y, x and u; Lemma 3.3 concerns the existence of integers satisfying the conditions stated in (P1), (P2) and (P4).

(P2) δ, x, y_1, y_2 *and* y.

(a) Let $\delta = \pm 1$. (The admissible integer u in Theorem 1.2 will later be related to δ via the requirement $u \equiv \delta \pmod 4$.)
We will use an admissible integer $y \equiv \delta \pmod 4$:
let $y_1 \equiv 15 \pmod{24}$, which is admissible and $\equiv 7 \pmod 8$;
if $\delta = -1$ let $y \coloneqq y_1$; and
if $\delta = 1$ let $y \coloneqq y_1 y_2$ where $y_2 \equiv 15 \pmod{24}$.

(b) Let x be admissible.

(c) Assume that $y_1 \geqslant \sqrt{y} \geqslant 8x + 7$.

(d) Assume that $y > x + 6v$.

In (P3) and (P4) we provide a recipe that uses the integers in (P2) to obtain auxiliary STSs together with an STS U that behaves as required in Theorem 1.2.

(P3) X, Y_1, Y_2 *and* Y.

(a) Write $y_1 = 4y_0 + 3$, so that y_0 is admissible and $y_0 \geqslant 2x + 1$ (by (P2)(a) and (P2)(c)). Then [2] provides an STS Y_0 of order y_0 containing a subsystem X of order x.

(b) Let $Y_1 \coloneqq 2(2Y_0 + 1) + 1$, so $|Y_1| = 2(2|Y_0| + 1) + 1 = y_1$ (by (P3)(a)) and Y_1 is $PG(3,2)$-paired (by Lemma 2.2(iii)).
If $\delta = 1$ let Y_2 be a $PG(3,2)$-paired STS of order y_2 (Lemma 2.3(ii)).

(c) If $\delta = -1$ let $Y \coloneqq Y_1$, of order y.
If $\delta = 1$ let $Y \coloneqq Y_1 \times Y_2$, of order y.

(d) Any two points of Y are in a $PG(3,2)$ subsystem of Y (Lemma 2.3).

(P4) U, A *and* u.
Let $A \coloneqq Y - X$ be as in Section 2.1, so the STS $U \coloneqq X \cup (V \times A)$ has order $u \coloneqq x + v(y - x)$. In Lemma 3.3 we will see that all sufficiently large admissible integers arise here as u for the choice of v in (P1) and for suitable x, y, δ in (P2).

As noted in [1, p. 469], each $g \in \mathrm{Aut}V$ acts as an automorphism of U via
$$g = 1 \text{ on } X \text{ and } (p,q)^g = (p^g, q) \text{ for } p \in V,\ q \in Y - X.$$
This produces a subgroup of $\mathrm{Aut}U$ isomorphic to $\mathrm{Aut}V$ and inducing $\mathrm{Aut}(V \times 1)$ on the subsystem $V \times 1$ of U.

(P5) The cyclic group A has even order; let -1 denote its involution. For $a \in A$ let $-a \coloneqq (-1)a$.
Let $A_6 \coloneqq \{a \in A \mid a^6 = 1\}$.

(P6) *Labeling* $Y - X$. We assume that $Y - X$ behaves as in Lemma 3.4 below (which depends only on Section 2.1 and the fact that $|Y - X|$ is not tiny).

Remark 3.1. Section 1 mentions "*. . . a Steiner triple system U having a rich geometry of $PG(m,2)$ subsystems. . .* ". This refers to the geometry inherited by U from (P1)(b) and (P3)(d), which involves far more structure than the fact that U is generated by its $PG(3,2)$ subsystems.

3.1.2. *Existence of y and x.* We first rephrase and slightly strengthen the numerical requirements in (P1), (P2) and (P4):

Lemma 3.2. *Assume that u, v, δ, y_1, y_2 and y are integers that behave as follows*:

(i) *u is admissible with* $u \equiv \delta \pmod 4$ *for* $\delta = \pm 1$, *and* $v \equiv 3 \pmod{12}$,
(ii) $u > 800^2 v^7$ *and* $v > 16^5$,
(iii) *$v-1$ is a factor of $u-y$,*
(iv) $y = y_1 y_2 \equiv \delta \pmod 4$ *with* $y_1 \equiv 15 \pmod{24}$, *where*
if $\delta = -1$ then $y_2 = 1$, while
if $\delta = 1$ then $y_2 \equiv 15 \pmod{24}$ *and* $y_1 \geqslant y_2$ *(so* $y_1 \geqslant \sqrt{y}$*), and*
(v) $u/v < y < u/v + \frac{1}{8}\{(v-1)/v\}\sqrt{u/v} - 1 < u$.

Then $u, v, \delta, y_1, y_2, y$ and $x \coloneqq (vy-u)/(v-1) = y - (u-y)/(v-1)$ are integers that satisfy all of the conditions in (P1), (P2) *and* (P4).

Remark. We have $y_1 \equiv 7 \pmod 8$, and $y_2 \equiv 7 \pmod 8$ if $y_2 \neq 1$. However, we do not need information about either u or $v \pmod 8$. What we need are u and $y \pmod 4$ in (i) and (iv) in order to have $u - y \equiv 0 \pmod 4$; this and $v - 1 \equiv 2 \pmod 4$ imply that $x = y - (u-y)/(v-1) \equiv y - 0 \equiv 1 \pmod 2$.

Proof. Note that u, v, y_1, y_2 and y are admissible. By (v), $vy - u > 0$ and $u - y > 0$, so $0 < x < y$.

(P1): See (i) and (ii).

(P2)(a): This is in (iv).

(P2)(b): Since $v \equiv 0 \pmod 3$ we have $x \equiv (0-u)/(0-1) = u \equiv 0$ or $1 \pmod 3$. We have already noted that x is odd, so it is admissible.

(P2)(c) and (P2)(d): By (v), $(vy-u)/v < \frac{1}{8}\{(v-1)/v\}\sqrt{u/v} - \frac{7}{8}\{(v-1)/v\}$. Then

$$\begin{aligned} x = (vy-u)/(v-1) &< \tfrac{1}{8}\sqrt{y} - \tfrac{7}{8} \quad \text{(which proves (P2)(c) using (iv))} \\ &< y/2 < y - 6v \end{aligned}$$

since $y > u/v > 12v$ by (v) and (ii); and this proves (P2)(d).

(P4): The relation $u = x + v(y-x)$ is just the present definition of x. □

Remark. Condition (v) places y in an interval of length roughly $\frac{1}{8}\sqrt{u/v}$, which is fairly large by (ii). We still need to verify the relatively obvious fact that this is large enough to make it possible to satisfy the remaining inequalities and congruences in the lemma.

Lemma 3.3. *Given admissible integers v and u such that* $v \equiv 3 \pmod{12}$, $v > 16^5$ *and* $u > 800^2 v^7$, *there are integers x, y_1, y_2 and y behaving as stated in* (P1), (P2) *and* (P4).

Proof. We will use (i)–(v) in the preceding lemma. Let $u \equiv \delta \pmod 4$ with $\delta = \pm 1$; the remaining requirements in (i) and (ii) are among the present hypotheses.

Since $v \equiv 3 \pmod{12}$ we can write $v = 3 + 12e + 24m$ with $e \in \{0, 1\}$.

When $\delta = -1$ let $y_2 \coloneqq 1$. When $\delta = 1$ let $y_2 \coloneqq v + (6-e)(v-1)$, so $y_2 \equiv 1 \pmod{v-1}$ and $y_2 \equiv 15 \pmod{24}$. Clearly $y_2 < 7v$.

We next define y_1. Let $0 < u' < v-1$ with $u' \equiv u \pmod{v-1}$, so u' is odd.

Let $y_1 \coloneqq u' + \Big(24\lceil u/\{24v(v-1)y_2\}\rceil + \frac{1}{2}\big((15-6e) + (23-6e)u'\big)\Big)(v-1)$. Since $(15-6e) + (23-6e)u'$ is even we have $y_1 \equiv u' \equiv u \pmod{v-1}$ and $y_1 \equiv u' + \big((15-6e) + (23-6e)u'\big)(1+6e) \equiv 15 \pmod{24}$.

We claim that y_1, y_2 and $y \coloneqq y_1 y_2$ behave as required in Lemma 3.2(iii)–(v).

(iii): $y = y_1 y_2 \equiv u \cdot 1 \pmod{v-1}$.

(iv): Most of this is in our definitions of y_1 and y_2, while $u > 24v(v-1)7v > 24v(v-1)y_2$ implies that $y_1 > 24(v-1) > 7v > y_2$.

(v): For the first part of (v), $y = y_1y_2 > \big(24u/\{24v(v-1)y_2\}\big)(v-1)y_2 = u/v$. Next, $u' < v-1,\ y_2 < 7v$ and $800^2v^6 < u/v$ imply that

$$\begin{aligned} y = y_1y_2 &< u'y_2 + \big(u/v + 24\cdot 1\cdot(v-1)y_2\big) + \tfrac{1}{2}(15+23v)(v-1)y_2 \\ &< (v-1)7v + \big(u/v + 24(v-1)7v\big) + \tfrac{1}{2}(15+23v)(v-1)7v \\ &< u/v + 100v^2(v-1) - 1 < u/v + \tfrac{1}{8}\{(v-1)/v\}\sqrt{u/v} - 1 \\ &< u/v + u/v < u; \end{aligned}$$

the ends of the last two lines take care of the remaining parts of (v). Now Lemma 3.2 provides us with the required integer x. ☐

3.1.3. *Labeling.* The structure of $Y-X$ as both a cyclic group and a partial STS have nothing to do with one another, as observed by Moore [6, p. 279]. This independence is seen in (M2) and (M3). This allows us to label the points of $Y-X$ in any way by the elements of A using an arbitrary bijection $\pi\colon Y-X \to A$; an element y of $Y-X$ is labeled by $a := y^\pi$, which we abbreviate by writing $y = a$.

Lemma 3.4. *The elements of $Y-X$ can be labeled by the elements of A in such a way that, if $k \in A_6$, $\alpha \in \mathrm{Aut}A$ and the permutation $y \mapsto ky^\alpha$ of A is an automorphism of the partial Steiner triple system $Y-X$, then $k=1$ and $\alpha = 1$.*

Proof. By (P1)(a) and (P2)(d), $|Y-X| > 6\cdot 16^5$. Then there are distinct points $y_1,\dots,y_9$ of $Y-X$, and $x_0 \in X$, such that the following are triples of Y:

$$y_1,y_2,y_3 \qquad y_3,y_4,y_5 \qquad x_0,y_6,y_7 \qquad x_0,y_8,y_9.$$

Let c be a generator of A. Label the y_i using $A_6 \cup \{c,-c,c^2\}$:

$$y_1 = 1 \;\; y_2 = -1 \;\; y_3 = c \quad y_4 = -c \quad y_5 = c^2; \text{ and also}$$

$$y_6 = \omega \;\; y_7 = -\omega \;\; y_8 = \omega^2 \;\; y_9 = -\omega^2 \text{ if some } \omega \in A \text{ has order 3.}$$

(The remaining points of $Y-X$ are labeled by the remaining elements of A in an arbitrary manner. Note that the points y_6, y_7, y_8 and y_9 are needed only if $|A|$ is a multiple of 3.) Thus, we have the following triples in Y:

$$1,-1,c \qquad c,-c,c^2 \qquad x_0,\omega,-\omega \qquad x_0,\omega^2,-\omega^2$$

(where the last two are omitted if $|A|$ is not a multiple of 3).

Now consider an automorphism $y \mapsto ky^\alpha$ of $Y-X$, where $k \in A_6$, $\alpha \in \mathrm{Aut}A$. This sends the triple $1,-1,c$ to $k,-k,kc^\alpha$. If $k \in A_6 - \{\pm1\}$ then this triple is $\omega^i, -\omega^i, kc^\alpha$ for $i = 1$ or 2; but the triple in Y containing ω^i and $-\omega^i$ is not contained in $Y-X$.

Thus, $k = \pm 1$, and $1,-1,c$ is sent to $1,-1,kc^\alpha$, so $kc^\alpha = c$.

If $k=-1$ then $c^\alpha = -c$. The triple $c,-c,c^2$ is sent to $-c^\alpha, -(-c)^\alpha, -(c^2)^\alpha$, which is $c,-c,-(c^\alpha)^2$. Since $-(c^\alpha)^2 = -(-c)^2 \neq c^2$, this is impossible.

Then $k=1$, so $\alpha = 1$ since $c = c^\alpha$ generates A. ☐

3.2. Location of $PG(2,2)$ subsystems. We need structural properties of the STS U defined in (P4). In this section we will not need any of the assumptions in Section 3.1: only the definitions in (P4) and the notation in (P5) are involved.

For $v \in V$ let

$$Y_v := X \cup (v \times A).$$

By (M2) this is a subsystem of U isomorphic to Y (via the isomorphism $x \mapsto x$, $y \mapsto (v,y)$ for $x \in X$, $y \in A = Y-X$).

There are $PG(2,2)$ subsystems contained in $V \times 1$, and ones contained in $Y_v \cong Y$ for $v \in V$. Another possible type of $PG(2,2)$ subsystem uses a triple v_1,v_2,v_3 in V, $x \in X$, and elements $a_i \in A$:

$$\begin{array}{ll} \text{points:} & x,\ (v_i,a_i),\ (v_i,-a_i) \text{ for } i=1,2,3,\\ & \quad \text{for } x\in X,\ a_i\in A,\ a_1a_2a_3=1 \text{ and triples } a_i,-a_i,x \text{ in } Y\\ \text{triples:} & (v_i,a_i),(v_i,-a_i),x \text{ for } i=1,2,3, \text{ and}\\ & \quad (v_1,\epsilon_1a_1),(v_2,\epsilon_2a_2),(v_3,\epsilon_3a_3) \text{ whenever } \epsilon_i=\pm1 \text{ and } \epsilon_1\epsilon_2\epsilon_3=1. \end{array}\tag{1}$$

Remark 3.5. *Two points $(v_1,a_1),(v_2,a_2)$ with $v_1\neq v_2$ lie in at most one subsystem* (1). For, these points determine the triple v_1,v_2,v_3 and then all $(v_i,\pm a_i)$.

Definition 3.6. *Let S be a subsystem of V and $f\colon S\to A_6$ (cf.* (P5)*) a function such that $f(v_1)f(v_2)f(v_3)=1$ whenever v_1,v_2,v_3 is a triple in S. Then*

$$V_{S,f}\coloneqq\{(s,f(s))\mid s\in S\}$$

is a subsystem of U, and $V_{S,1}=S\times 1\cong V_{S,f}$ via $(s,1)\mapsto(s,f(s))$, using (M3)*: these subsystems are just variations on the subsystem $V\times 1$.*

The subsystems Y_v and $V_{S,f}$ are basic tools in our proof of Theorem 1.2, and

$$|Y_v\cap V_{S,f}|\leqslant 1 \text{ for all } v,\ S \text{ and } f.\tag{2}$$

Lemma 3.7. *Every $PG(2,2)$ subsystem of U either is of type* (1)*, lies in some Y_v, or has the form $V_{S,f}$ for a $PG(2,2)$ subsystem S of V.*

Proof. If a $PG(2,2)$ subsystem Z has the form $\{(v_i,y_i)\mid 1\leqslant i\leqslant 7\}$ with distinct v_i, then the v_i form an STS S by (M3); we may assume that the triples in Z are

$$\begin{array}{ll} (v_1,a_1),(v_2,a_2),(v_3,a_3) & \text{so } a_1a_2a_3=1\\ (v_1,a_1),(v_4,a_4),(v_5,a_5) & \text{so } a_1a_4a_5=1\\ (v_1,a_1),(v_6,a_6),(v_7,a_7) & \text{so } a_1a_6a_7=1\\ (v_3,a_3),(v_5,a_5),(v_7,a_7) & \text{so } a_3a_5a_7=1\\ (v_3,a_3),(v_4,a_4),(v_6,a_6) & \text{so } a_3a_4a_6=1\\ (v_2,a_2),(v_4,a_4),(v_7,a_7) & \text{so } a_2a_4a_7=1\\ (v_2,a_2),(v_5,a_5),(v_6,a_6) & \text{so } a_2a_5a_6=1 \end{array}$$

with $a_i\in A$. Multiplying these equations, and also just the first three of them, we find that $(\prod_i a_i)^3=1$ and $a_1^3a_2a_3a_4a_5a_6a_7=1$. It follows that $\prod_i a_i=\omega$ with $\omega^3=1$ and $a_1^2=\omega^2$, so every $a_i^6=1$. Then $Z=V_{S,f}$ with $f(v_i)\coloneqq a_i\in A_6$.

If Z contains a triple $(v,a_1),(v,a_2),(v,a_3)$ but does not lie in Y_v, then it also contains a point (v_2,b_2) with $v_2\neq v$. By (M3), if v,v_2,v_3 is a triple of V then there are triples $(v_2,b_2),(v,a_1),(v_3,b_3)$ and $(v_2,b_2),(v,a_2),(v_3,c_3)$ and $(v_2,b_2),(v,a_3),(v_3,d_3)$, and hence another triple $(v,a_1),(v_3,c_3),(v_3,d_3)$, which contradicts (M2).

Assume that Z is not in any Y_v. If Z has a triple $T\subseteq X$, then some point (v,a) is in Z, the triples joining (v,a) to the points of T all lie in both Z and Y_v by (M2), and then $Z\subseteq Y_v$. The only other possibility is that Z is determined by three triples through some $x\in X$, and hence contains triples

$$\begin{array}{ll} (v_1,a_1),(v_2,a_2),(v_3,a_3) & \text{so } a_1a_2a_3=1\\ x,(v_1,a_1),(v_1,b_1) & \text{so } a_1,b_1,x \text{ is a triple in } Y\\ x,(v_2,a_2),(v_2,b_2) & \text{so } a_2,b_2,x \text{ is a triple in } Y\\ x,(v_3,a_3),(v_3,b_3) & \text{so } a_3,b_3,x \text{ is a triple in } Y\\ (v_1,a_1),(v_2,b_2),(v_3,b_3) & \text{so } a_1b_2b_3=1\\ (v_1,b_1),(v_2,b_2),(v_3,a_3) & \text{so } b_1b_2a_3=1\\ (v_1,b_1),(v_2,a_2),(v_3,b_3) & \text{so } b_1a_2b_3=1. \end{array}$$

The last three equations imply that $a_1a_2a_3b_1^2b_2^2b_3^2=1$, so $1=(b_1b_2b_3)^2=(b_ia_i^{-1})^2$ and hence $b_i=\pm a_i$ for each i (cf. (P5)). Since $x,(v_i,a_i),(v_i,b_i)$ is a triple we have $b_i=-a_i$ for each i, so we are in (1). ☐

For Moore [6, Sec. 10], the types of $PG(2,2)$ subsystems of U were isomorphism invariants of his STS construction.[2] He did not go into the detail involved in (1) or a function $f\colon S \to A_6$.

3.3. Finding critical subsystems. The following key result is based on (P1)(b) and (P3)(d) together with (2).

Proposition 3.8. *Let W be a subsystem of U.*

(i) *If $W \cong Y$ then W has the form Y_v for some $v \in V$.*
(ii) *If $W \cong V$, if W meets every subsystem in* (i) *in at most one point, and if W is disjoint from the intersection of the subsystems in* (i), *then W has the form $V_{V,f}$ for some $f\colon V \to A_6$.*

Proof. (i) Clearly $|W| = |Y| > |X|$. Let $(v_1, a_1) \in W - X$. We claim that $W \subseteq Y_{v_1}$.

Assume that $W \nsubseteq Y_{v_1}$. Let $(v_2, a_2) \in W$ with $v_1 \neq v_2$. Since $W \cong Y$, by (P3)(d) there is a $PG(3,2)$ subsystem containing (v_1, a_1) and (v_2, a_2). That subsystem has three $PG(2,2)$ subsystems containing (v_1, a_1) and (v_2, a_2), each of type $V_{S,f}$ or as in (1), by Lemma 3.7; and at least one has type $V_{S,f}$ by Remark 3.5. In particular, $a_1 \in A_6$. Thus, $W \subseteq X \cup (V \times A_6)$. Then $|Y| = |W| \leqslant |X| + 6|V|$, which contradicts (P2)(d).

(ii) The stated intersection is X, so $W \subseteq V \times A$. For $v \in V$, $|W \cap Y_v| \leqslant 1$ implies that v occurs in at most one pair $(v,a) \in W$. Since $|W| = |V|$, it follows that $W = \{(v, f(v)) \mid v \in V\}$ for some $f\colon V \to A$.

Since $W \cong V$, by (P1)(b) every point of W is in a $PG(2,2)$ subsystem, which by Lemma 3.7 has the form $V_{S,f'}$ with $|S| = 7$ and $f'\colon S \to A_6$ (since $|W \cap Y_v| \leqslant 1$ for each v). Then $W \subseteq V \times A_6$, f maps to A_6, and by (M3) f must behave as in Definition 3.6. ☐

3.4. Aut$U$ and Aut$A$. Theorem 1.2 concerns Aut$U$:

Proposition 3.9. Aut$U \cong$ Aut$V$, *and* Aut$U$ *leaves* $V \times 1$ *invariant, inducing* Aut$(V \times 1) \cong$ Aut$U$ *on this subsystem of* U.

Proof. Let $h \in \mathrm{Aut}U$. We must show that h is induced by some element of $\mathrm{Aut}(V \times 1) \leqslant \mathrm{Aut}U$ (cf. (P4)).

Proposition 3.8(i) states that the subsystems Y_v are uniquely determined for U. Then Proposition 3.8(ii) states that the subsystems $V_{V,f}$ are also uniquely determined for U. It follows that h sends $V \times 1 = V_{V,1}$ to $V_{V,f} \subseteq V \times A_6$ for some $f\colon V \to A_6$, and h permutes the subsystems Y_v.

Since h sends $X = \bigcap_{v \in V} Y_v$ to itself it also sends $U - X = V \times A$ to itself. In view of (M3), restricting h to the first component in $V \times A$ induces an isomorphism $\bar{h}\colon V \to V$; by (P4), $\bar{h}$ is also induced by some $g \in \mathrm{Aut}(V \times 1) \leqslant \mathrm{Aut}U$. Then $\bar{h}\bar{g}^{-1} = 1$ on V. We will prove that $h = g$. Replace h by hg^{-1}, so $\bar{h} = 1$ on V. *The remainder of the proof consists of showing that $h = 1$.*

Since $(v \times A)^h = v^{\bar{h}} \times A = v \times A$ and $(V \times 1)^h = V_{V,f}$ we have $(v,1)^h = (v, f(v))$ for all $v \in V$.

Since h permutes the subsystems Y_v, from $(v,1), (v,1)^h = (v, f(v)) \in Y_v$ it follows that h leaves invariant every Y_v. Let $(v,a)^h = (v, f_v(a))$ where $a, f_v(a) \in A$. Then $(v, f_v(1)) = (v,1)^h = (v, f(v))$. Let $b_v := f_v(1) = f(v) \in A_6$.

We will show that h acts on $V \times A$ by

$$(v,a)^h = (v, b_v a^\alpha) \text{ for all } v \in V, a \in A, \text{ and some } \alpha \in \mathrm{Aut}A. \tag{3}$$

---

[2] See Footnote 1.

Let v_1, v_2, v_3 be a triple of V. Whenever $a_1a_2a_3 = 1$, $a_i \in A$, by (M3) we obtain a triple (v_1, a_1), (v_2, a_2), (v_3, a_3) and hence also its image under h: the triple $(v_1, f_{v_1}(a_1))$, $(v_2, f_{v_2}(a_2))$, $(v_3, f_{v_3}(a_3))$, so $f_{v_1}(a_1)f_{v_2}(a_2)f_{v_3}(a_3) = 1$. Then

$$f_{v_1}(a_1)f_{v_2}(a_2)f_{v_3}(a_1^{-1}a_2^{-1}) = 1 \quad \text{for all } a_1, a_2 \in A.$$

Let $a_1 = 1$ and deduce that $f_{v_2}(a_2) = b_{v_1}^{-1} f_{v_3}(a_2^{-1})^{-1}$; while $a_2 = 1$ yields $f_{v_1}(a_1) = b_{v_2}^{-1} f_{v_3}(a_1^{-1})^{-1}$. Then $b_{v_1}b_{v_2}b_{v_3} = f_{v_1}(1)f_{v_2}(1)f_{v_3}(1) = 1$ and (after replacing a_i^{-1} by a_i)

$$b_{v_3} f_{v_3}(a_1a_2) = f_{v_3}(a_1)f_{v_3}(a_2).$$

Now $b_{v_3}^{-1} f_{v_3}(a_1a_2) = b_{v_3}^{-1} f_{v_3}(a_1) b_{v_3}^{-1} f_{v_3}(a_2)$, so that $f_{v_3}(a_1) = b_{v_3}a_1^{\alpha}$ for some $\alpha \in \mathrm{Aut}A$ and all $a_1 \in A$. Moreover, $f_{v_2}(a_2) = b_{v_1}^{-1} f_{v_3}(a_2^{-1})^{-1} = b_{v_2}a_2^{\alpha}$: we have the same automorphism α for all $v \in V$. This proves (3).

By (3) and (M2), if $v \in V$ then $a \mapsto b_v a^{\alpha}$ is an automorphism of the partial Steiner triple system $Y - X$. By (P6), $\alpha = 1$ and $b_v = 1$ for all v. Then $h = 1$ on $V \times A$. Since every point of X is in a triple containing two points of $Y - X$, it follows that $h = 1$, as claimed. ☐

3.5. Completion of proof. In (P1)–(P4) we provided the ingredients for the construction of an STS U using Section 2.1. Proposition 3.9 determined $\mathrm{Aut}U$.

Moreover, by (P1)(a) and Proposition 3.9, U has $\mathrm{Aut}U$-invariant subsystems $V \times 1 \supset V_\star \times 1$ such that $\mathrm{Aut}U \cong \mathrm{Aut}(V \times 1) \cong \mathrm{Aut}(V_\star \times 1)$ and $\mathrm{Aut}U$ induces $\mathrm{Aut}(V \times 1)$ and $\mathrm{Aut}(V_\star \times 1)$ on the respective subsystems.

Lemma 3.3 states that we have dealt with all admissible $u > 800^2v^7$. ☐

Remark 3.10. **Bounding $N_{V_\star}$.** In Lemma 3.2 we had $u > 800^2v^7$, but the integer $v = |V|$ obtained in Corollary 2.6 is much larger than $|V_\star|$. By Proposition 2.5(iv), $|V_\star \times D|$ is $O(|V_\star|^5)$, so v is $O(|V_\star|^{5\cdot 5})$. Thus, $N_{V_\star}$ is $O(|V_\star|^{25\cdot 7})$.

Bounding M_G. In [5] and [3] an STS $V_\star$ is constructed for which $G \cong \mathrm{Aut}V_\star$ and $|V_\star|$ is $2^{O(|G|)}$. By the preceding paragraph the same is true for M_G.

This bound for M_G is ridiculously weak. It seems likely that M_G is polynomial in $|G|$, but entirely new methods would be needed to prove that.

Remark 3.11. The argument in [1] depended on using pairs $X \subset Y$ provided by [2], essentially for all possible $x = |X|$ and $y = |Y|$ for which $y \geqslant 2x + 1$. The argument used here only had access to a more limited choice (P2)(a) of orders y (cf. Lemma 2.3(ii)). In [1] first $y - x$ was dealt with, at which point x and y were uniquely determined for given v and u. This approach can be used in our situation when $u \equiv -1 \pmod 4$ but not when $u \equiv 1 \pmod 4$. Therefore we have started with a restricted choice of y, and then x is uniquely determined for given v and u (Lemmas 3.2 and 3.3). Our problem was to have a suitably geometric Y of order y with a subsystem of the required order $x \leqslant (y_0 - 1)/2 < (y - 1)/2$.

4. Partial Steiner triple systems

4.1. Theorem 1.3. We first note how our approach differs from that of Cameron [1]. He observes: "In the construction used to prove Theorem 1, if the subsystem contains no triples, its automorphism group is the symmetric group S_u, while that of the embedding system is the general linear group $GL(u-1, 2)$." In other words, the PSTS (partial Steiner triple system) might have too few triples. The first part of our proof eliminates this possibility (cf. Lemma 4.3(v)).

Definition 4.1. *Let the PSTS $Q_k(x), k \geqslant 2$, have the following triples (using two "paths" of k triples in the first two rows and an additional point $2k+1$):*

$$\begin{array}{lllll}
x,1,2 & 2,3,4 & 4,5,6 & \ldots & 2k-2,2k-1,2k \\
x',1',2' & 2',3',4' & 4',5',6' & \ldots & (2k-2)',(2k-1)',(2k)' \\
2k+1,x,x' & 2k+1,i,i' & \text{for } 1 \leqslant i \leqslant 2k & & \\
x,3,(2k)' & x,3',2k & & &
\end{array}$$

Remark 4.2. The following properties of $Q_k(x)$ are straightforward:

1. $Q_k(x)$ has $4k+3$ points,
2. every point is in at least two triples,
3. the point $2k+1$ is in $2k+1 \geqslant 5$ triples, x is in four triples and every other point is in at most three triples,
4. every point is in the union of the triples containing $2k+1$, and
5. $\mathrm{Aut}Q_k(x) = 1$.

(For (5), every automorphism must fix x and $2k+1$, then also x', $1'$, 1, 2, $\ldots$.)

Let V be an n-point PSTS as in Theorem 1.3. We may assume that $n \geqslant 2$.

Lemma 4.3. *There is a PSTS V' such that*

(i) *V is an $\mathrm{Aut}V'$-invariant subsystem of V',*
(ii) *$\mathrm{Aut}V'$ induces $\mathrm{Aut}V$ on V,*
(iii) *$\mathrm{Aut}V' \cong \mathrm{Aut}V$,*
(iv) *$n' := |V'| \geqslant 22$, and*
(v) *every point of V' is in at least two triples of V'.*

Proof. For every point x of V, attach $Q_n(x)$ to V so that $V \cap Q_n(x) = x$ and the n PSTSs $Q_n(x)$ are pairwise disjoint. The union of V and these PSTSs (also using the union of their sets of triples) is a new PSTS V' having n' points, where $n' = n|Q_n(x)| = n(4n+3) \geqslant 22$, which proves (iv).

Condition (i) is clear, (v) holds in V' by Remark 4.2(2), and (ii) follows from the fact that all $Q_n(x)$ are isomorphic and are pairwise disjoint.

It remains to prove (iii). By Remark 4.2(3), any subsystem Q of V' isomorphic to $Q_n(x)$ has a point z in $2n+1$ triples of Q. Since $V' = \bigcup_{x \in V} Q_n(x)$, again by Remark 4.2(3) each point of V' is either in $2n+1$ triples of V', at most 3 triples, or (for points of V) between 4 and $4+(n-1)/2 < 2n+1$ triples. Then $z \notin V$ and $z \in Q_n(x)$ for a unique x. By Remark 4.2(4), the union of the triples of V' containing z is both Q and $Q_n(x)$, so $Q = Q_n(x)$.

Thus, V' determines the points of V, any element of $\mathrm{Aut}V'$ induces an element of $\mathrm{Aut}V$, and this yields a homomorphism from $\mathrm{Aut}V'$ onto $\mathrm{Aut}V$. Its kernel fixes every point x of V, and hence is 1 by Remark 4.2(5). ☐

In the rest of the proof we ignore V and work only with V'. By Theorem 1.2, *it suffices to construct one STS U having V' as an $\mathrm{Aut}U$-invariant subsystem such that $\mathrm{Aut}U \cong \mathrm{Aut}V'$ and $\mathrm{Aut}U$ induces $\mathrm{Aut}V'$ on V'.*

As in [1], we use the projective space $P = PG(n'-1,2)$ whose points are the $2^{n'}-1$ nonempty subsets of (the set of points of) V', the lines of P being all triples of subsets of V' whose symmetric difference is empty. Any permutation of the points of V' extends uniquely to an automorphism of P. Every point w of P has size $|w|$ as a subset of V'.

Again as in [1], we construct from the STS P and the PSTS V' an STS U whose points are those of P, as follows: for every triple a,b,c of V', replace the triples

$$ab, ac, bc \qquad a,b,ab \qquad a,c,ac \qquad b,c,bc \tag{4}$$

of P by the new triples

$$a, b, c \qquad a, ab, ac \qquad b, ab, bc \qquad c, ac, bc \tag{5}$$

(by abuse of notation, we write a and ab for $\{a\}$ and $\{a, b\}$, respectively). This produces a new STS U, because the new triples cover exactly the same pairs of points as the old ones.

Note that

(6) *Every point ab is in at most two triples of U that are not lines of P,*

and that $\mathrm{Aut}V'$ induces a subgroup of $\mathrm{Aut}U$ (as in [1, p. 468]). Moreover,

(7) *A line of P is also a triple of U if it contains a point w with $|w| > 2$.*

Lemma 4.4. *The lines of P can be determined using the triples in U.*

Proof. We will recover the line $\langle x, y\rangle$ of P determined by any given distinct points x, y of U. For every point p of U not in the triple of U determined by x and y there are distinct triples

$$p, x, x_1 \qquad p, y, y_1 \qquad x_1, y_1, z \qquad p, z, q$$

of U, producing a 7-set $U(p, x, y) := \{p, x, y, x_1, y_1, z, q\}$ of points of U.

There are at least $(2^{n'-2} - 1) - n' - \binom{n'}{2}$ planes of P containing x and y but containing no point w of P with $|w| \leqslant 2$. Every point $w \notin \langle x, y\rangle$ in such a plane has $|w| > 2$; by (7), every such plane has the form $U(p, x, y)$ for any of its four points $p \notin \langle x, y\rangle$. Thus, by Lemma 4.3(iv), if p is one of at least $4(2^{n'-2} - 1 - n' - \binom{n'}{2}) > \frac{3}{4}|U|$ points in the union S of these planes but not in $\langle x, y\rangle$, then

- (i) every set $U(p, x, y)$ occurs for at most four points p, and
- (ii) distinct sets $U(p, x, y)$ have the same intersection of size 3.

(The intersection in (ii) is the line $\langle x, y\rangle = \{x, y, z\}$.)

If S' is another set of more that $\frac{3}{4}|U|$ points satisfying (i)-(ii), then $|S \cap S'| \geqslant \frac{3}{4}|U| + \frac{3}{4}|U| - |U| = \frac{1}{2}|U| = \frac{1}{2}(2^{n'} - 1) \geqslant \frac{1}{2}(2^{22} - 1)$, and hence by (i) $S \cap S'$ contains distinct sets $U(p, x, y)$. Those sets produce the same set of size 3 in (ii). Thus, we have obtained the line $\langle x, y\rangle$ of P using the triples of U. □

Note that we have not yet used Lemma 4.3(v).

Proposition 4.5. $\mathrm{Aut}U \cong \mathrm{Aut}V' \cong \mathrm{Aut}V$.

Proof. We now have the triples in U and the triples in P. Let T denote the set of triples of U that are not triples in P (these are the triples in (5), and hence consist of points such as $a \in V'$ or ab). Let $x \in U$.

1. If x is in at least four triples in T, then $x \in V'$ by (6).
2. Every point of V' is in at least four triples in T, by Lemma 4.3(v) and (5).

Thus U *uniquely determines* V', so $\mathrm{Aut}U$ induces a subgroup of $\mathrm{Aut}V'$. Since $\mathrm{Aut}V'$ induces a subgroup of $\mathrm{Aut}U$, by Lemma 4.3(iii) we have $\mathrm{Aut}U \cong \mathrm{Aut}V' \cong \mathrm{Aut}V$, and we are done. □

Proof of Theorem 1.3. We have embedded the original PSTS V into an STS U such that $\mathrm{Aut}U$ leaves V invariant, induces $\mathrm{Aut}V$ on V, and is isomorphic to $\mathrm{Aut}V$. Now apply Theorem 1.2 to U (in place of V) in order to obtain STSs behaving as in Theorem 1.3. □

4.2. Corollaries. We note some consequences of Theorem 1.3. We will use a natural graph on the points of a PSTS W, with two points joined if they are in a triple. If this graph is not connected we can embed W in an arbitrarily large STS, which is clearly connected (preservation of the automorphism group is even possible by Theorem 1.3, but this will not be needed).

Corollary 4.6. *Given partial Steiner triple systems V and W, there is an integer $N_{V,W}$ such that, for each admissible $u \geqslant N_{V,W}$, there is a Steiner triple system U on u points having a subsystem $W' \cong W$ and an* $\mathrm{Aut}U$*-invariant subsystem $V' \cong V$ with $W' \cap V' = \varnothing$ such that* $\mathrm{Aut}U \cong \mathrm{Aut}V'$ *and* $\mathrm{Aut}U$ *induces* $\mathrm{Aut}V'$ *on V'.*

Proof. Here V and the desired U are as usual, the new aspect is to include W as well; we have no control over the PSTS $V\dot{\cup}W$. By the preceding remarks, we may assume that W is an STS and hence is connected, and that $W \cap V = \varnothing$, $n = |W| \geqslant 2$ and $n > |V|$. Let $x_1, \dots, x_n$ be the points of W. Then Definition 4.1 applies with $k = i + n \geqslant 3$; attach pairwise disjoint PSTSs $Q_{i+n}(x_i)$ to W in such a way that $Q_{i+n}(x_i) \cap W = x_i$ for every i. The union of W and all $Q_{i+n}(x_i)$ is a connected PSTS $\widehat{W}$.

Every $Q_{i+n}(x_i)$ has a unique point in $2(i+n)+1 \geqslant 2n+3 > \frac{1}{2}(n-1)+4$ triples (by Remark 4.2(3)), and $\widehat{W}$ has no other such points (x_i is in at most $\frac{1}{2}(n-1)+4$ triples of $\widehat{W}$, again by Remark 4.2(3)). Then W can be recovered from $\widehat{W}$ using Remark 4.2(3)-(4). The PSTSs $Q_{i+n}(x_i), 1 \leqslant i \leqslant n$, have different orders, so from Remark 4.2(5) it follows that $\mathrm{Aut}\widehat{W} = 1$.

Since $|\widehat{W}| > |V|$ and $\widehat{W}$ is a connected component of the graph on the disjoint union $\widehat{W}\dot{\cup}V'$ of $\widehat{W}$ and $V' \cong V$, $\mathrm{Aut}(\widehat{W}\dot{\cup}V')$ leaves $\widehat{W}$ invariant and hence acts on V'. Then $\mathrm{Aut}(\widehat{W}\dot{\cup}V') \cong \mathrm{Aut}V'$, so apply Theorem 1.3 to $\widehat{W}\dot{\cup}V'$. ☐

The first step in the above proof was to embed an arbitrary STS into one whose automorphism group is trivial. This suggests a strengthening of Theorem 1.1:

Corollary 4.7. *If $V_1, \dots, V_m$ are partial Steiner triple systems and G is a finite group, then there is an integer $N_{V_1,\dots,V_m,G}$ such that, for each admissible $u \geqslant N_{V_1,\dots,V_m,G}$, there is a Steiner triple system U on u points such that $V_1, \dots, V_m$ are isomorphic to pairwise disjoint subsystems of U and* $\mathrm{Aut}U \cong G$.

Proof. Let V be an STS with $\mathrm{Aut}V \cong G$ [5]. Apply the preceding corollary to V and W, where W is the disjoint union of (copies of) $V_1, \dots, V_m$. ☐

Corollary 4.8. *If G and H are finite groups then there is an integer $N_{G,H}$ such that, for each admissible $u \geqslant N_{G,H}$, there is a Steiner triple system U on u points having a subsystem W such that* $\mathrm{Aut}U \cong G$ *and* $\mathrm{Aut}W \cong H$.

Proof. Let V and W be STSs such that $\mathrm{Aut}V \cong G$ and $\mathrm{Aut}W \cong H$ [5]. Apply Corollary 4.6 to the pair V, W in order to obtain an STS U behaving as stated. ☐

This corollary can be iterated in two ways: one involves disjoint subsystems with arbitrary given automorphism groups; another involves a nested sequence of subsystems with arbitrary given automorphism groups.

Our final corollary concerns retaining a *subgroup* of the automorphism group of an STS but not the full automorphism group. Notation: If G is a group acting on a set X, and if $Y \subset X$, then the *set-stabilizer* G_Y is $\{g \in G \mid g \text{ sends } Y \text{ to itself}\}$. (In the corollary V_1 need not be $\mathrm{Aut}V$-invariant, and $\mathrm{Aut}V_1$ need not be a subgroup of $\mathrm{Aut}V$.)

Corollary 4.9. *If V_1 is a subsystem of order > 1 of a partial Steiner triple system V, then there is an integer N'_{V,V_1} such that, for each admissible $u \geqslant N'_{V,V_1}$, there is a Steiner triple system U on u points having V and V_1 as* $\mathrm{Aut}U$*-invariant subsystems such that* $\mathrm{Aut}U \cong (\mathrm{Aut}V)_{V_1}$ *and* $\mathrm{Aut}U$ *acts on V as* $(\mathrm{Aut}V)_{V_1}$.

Proof. First we replace V by an STS: use Theorem 1.3 to find an STS $\hat{V}$ containing V such that $\mathrm{Aut}\hat{V}$ leaves V invariant, induces $\mathrm{Aut}V$ on V and is isomorphic to $\mathrm{Aut}V$. Then $(\mathrm{Aut}\hat{V})_{V_1} \cong (\mathrm{Aut}V)_{V_1}$.

Let z be a new point, and let $x \mapsto x'$ be a bijection from V_1 to a set V_1' disjoint from $\hat{V} \cup \{z\}$; this bijection turns V_1' into a PSTS. Form a PSTS W, with $\hat{V} \cup \{z\} \cup V_1'$ as its set of points, by using the triples in $\hat{V} \cup V_1'$ and including a new triple x, z, x' for every $x \in V_1$. Every g in $(\mathrm{Aut}\hat{V})_{V_1}$ acts as an automorphism of W via $z^g = z$ and $(x')^g = (x^g)'$ for $x \in V_1$.

The set V_1 is uniquely determined as the set of points of W lying in triples with the maximal number of other points (namely, $(|\hat{V}| - 1) + 2$ points); $\hat{V} - V_1$ is uniquely determined as the set of points of W lying in triples with exactly $|\hat{V}| - 1$ points. Then $\mathrm{Aut}W$ induces $(\mathrm{Aut}\hat{V})_{V_1}$ on $\hat{V}$.

Let K denote the pointwise stabilizer of $\hat{V}$ in $\mathrm{Aut}W$. For distinct $x, y \in V_1$, the triples x, z, x' and y, z, y' meet at z, so K fixes z and then also all points of V_1'. Thus, $K = 1$ and $\mathrm{Aut}W = (\mathrm{Aut}\hat{V})_{V_1}$. Now apply Theorem 1.3 to W. ☐

Remark 4.10. *If G and H are finite groups with $G > H$, then there is an integer $N'_{G,H}$ such that, for each admissible $u \geqslant N_{G,H}$, there a Steiner triple system U on u points having a subsystem W such that* $\mathrm{Aut}U \cong G$ *and* $(\mathrm{Aut}U)_W \cong \mathrm{Aut}W \cong H$. The proof involves a few straightforward changes in [3, Sec. 2], which we briefly outline.

1. Let Γ be an n-vertex connected graph having a connected induced subgraph Γ' such that $\mathrm{Aut}\Gamma \cong G$, G acts semiregularly on the vertices of Γ, and $(\mathrm{Aut}\Gamma)_{\Gamma'} \cong \mathrm{Aut}\Gamma' \cong H$. (Use the standard colored Cayley graphs for G and H and replace colored edges by suitable graphs.)

2. Consider the vector space V in Section 2.3. In order to conform to the notation in [3, Sec. 2] let V_F and V denote this as an F-space and as an $\mathbf{F}_2$-space, respectively. Assume that G acts on the basis of V_F as it does on the vertices of Γ. Let V_F' denote the F-span of the vertices of Γ', and let V' be V_F' viewed as an $\mathbf{F}_2$-space.

3. In [3, Sec. 2] there is a construction of an STS U with $\mathrm{Aut}U \cong G$, using V_F, V and Γ, and two auxiliary STSs on 15 points. Restricting the construction to V_F', V' and Γ' produces a subsystem U' of U obtained using these ingredients in the same manner that U was. In particular, $(\mathrm{Aut}U)_{U'} \cong \mathrm{Aut}U' \cong H$, as required.

Acknowledgements. We are grateful to a perspicacious, precise and patient referee, whose comments led to significant improvements.

References

[1] Peter J. Cameron, *Embedding partial Steiner triple systems so that their automorphisms extend*, J. Combin. Des. **13** (2005), no. 6, 466–470.

[2] Jean Doyen and Richard M. Wilson, *Embeddings of Steiner triple systems*, Discrete Math. **5** (1973), 229–239.

[3] William M. Kantor, *Automorphism groups of designs with* $\lambda = 1$, Discrete Math. **342** (2019), no. 10, 2886–2892.

[4] Charles C. Lindner and Alexander Rosa, *On the existence of automorphism free Steiner triple systems*, J. Algebra **34** (1975), 430–443.

[5] Eric Mendelsohn, *On the groups of automorphisms of Steiner triple and quadruple systems*, J. Combin. Theory Ser. A **25** (1978), no. 2, 97–104.

[6] E. Hastings Moore, *Concerning triple systems*, Math. Ann. **43** (1893), no. 2-3, 271–285.

[7] Jacobus H. van Lint and Richard M. Wilson, *A course in combinatorics*, second ed., Cambridge University Press, Cambridge, 2001.

Jean Doyen, Université Libre de Bruxelles, Bruxelles 1050, Belgium
E-mail : `jdoyen@ulb.ac.be`

William M. Kantor, U. of Oregon, Eugene, OR 97403 and Northeastern U., Boston, MA 02115
E-mail : `kantor@uoregon.edu`