Rigid Steiner triple systems obtained from projective triple systems

M. J. Grannell
Department of Mathematics and Statistics
The Open University
Walton Hall
Milton Keynes MK7 6AA
UNITED KINGDOM
(m.j.grannell@open.ac.uk)

M. Knor
Department of Mathematics
Faculty of Civil Engineering
Slovak University of Technology
Radlinského 11
813 68 Bratislava
SLOVAKIA
(knor@math.sk)

Abstract

It was shown by Babai in 1980 that almost all Steiner triple systems are rigid; that is, their only automorphism is the identity permutation. Those Steiner triple systems with the largest automorphism groups are the projective systems of orders $2^n - 1$. In this paper we show that each such projective system may be transformed to a rigid Steiner triple system by at most n Pasch trades whenever $n \geq 4$.

Running head: Rigid STS

AMS classifications: Primary: 05B07, Secondary: 05B25, 05E18.

Keywords: automorphism; Pasch configuration; projective triple system; rigid system; Steiner triple system; trade.

1 Introduction

A Steiner triple system of order v, STS(v), is an ordered pair $(V, \mathcal{B})$ where V is a v-element set (the *points*) and $\mathcal{B}$ is a set of triples from V (the *blocks*), such that each pair from V appears in precisely one block. The necessary and sufficient condition for the existence of an STS(v) is that $v \equiv 1$ or $3 \pmod 6$ [9]; such values of v are called *admissible*. We often omit set brackets and commas from triples of points so that $\{x, y, z\}$ may be written as xyz when no confusion is likely, and pairs (or n-tuples) may be treated similarly. An *automorphism* of an STS(v) $= (V, \mathcal{B})$ is a permutation on the points of V that preserves the set of blocks $\mathcal{B}$. An STS(v) is said to be *rigid* if its only automorphism is the identity permutation. Alternative terms to "rigid" are "automorphism-free" and "asymmetric".

It was shown by Lindner and Rosa [10] that a rigid STS(v) exists for admissible v if and only if $v \geq 15$. Subsequently, Babai [1] proved that at most $v^{v^2(\frac{5}{48}+o(1))}$ distinct STS(v)s have an automorphism group of order greater than 1. Since (for admissible v) the number of distinct STS(v)s is $v^{v^2(\frac{1}{6}-o(1))}$ [2, 12], it follows that the proportion of rigid STS(v)s tends to 1 as $v \to \infty$. Speaking colloquially, almost all Steiner triple systems are rigid.

The most symmetric STS(v)s are the projective systems; these exist when v is of the form $2^n - 1$. The projective STS(v) of order $v = 2^n - 1$ may be represented on the points of $\mathbb{Z}_2^n \setminus \{0\}$ by taking the block set to comprise all triples of points xyz such that $x \oplus y \oplus z = 0$ in $\mathbb{Z}_2^n$. Here and subsequently we use $\oplus$ to denote addition of points in $\mathbb{Z}_2^n$. We will identify the integer $2^{n-1}a_{n-1} + 2^{n-2}a_{n-2} + \ldots + 2a_1 + a_0$ with the point $(a_{n-1}, a_{n-2}, \cdots, a_1, a_0) \in \mathbb{Z}_2^n \setminus \{0\}$ so that, for example, $12 \oplus 5 = 9$ because 12 is identified with 1100, 5 with 0101 and 9 with $1001 = 1100 \oplus 0101$. (In the vector representation, leading zeros are suppressed so that, for example, 101 and 0101 are both identified with 5, and it is not necessary to specify n when using $\oplus$.) We use the symbol S_n to denote the projective STS($2^n - 1$). It is well-known that S_n has automorphism group PSL$(n, 2)$ of order $2^{\frac{n(n-1)}{2}} \prod_{i=2}^{n}(2^i - 1)$ [7, page 41].

It is an interesting question how close the most and the least symmetric systems can be to one another. In this paper we investigate how far S_n is from a rigid system of the same order. The systems S_2 and S_3 are, up to isomorphism, the unique Steiner triple systems of orders 3 and 7 (the latter being generally known as the Fano plane), so there are no rigid systems of these orders.

If T_1 and T_2 are disjoint sets of triples from a common point set V that cover the same pairs of points, then the pair $\mathcal{T} = \{T_1, T_2\}$ is called a *trade pair*, and T_1 and T_2 are called *tradeable configurations*. If an STS(v) contains a copy of T_1, then that copy may be replaced by the corresponding copy of T_2 to give another STS(v). This operation is called a $\mathcal{T}$-trade. The set of points covered by T_1 and T_2 is called the *foundation* of the trade, and the number of blocks in each T_i ($i = 1, 2$) is called the *volume* of the trade. A *Pasch configuration* or *quadrilateral* or *4-cycle* $P(a, b, c, d, e, f)$ is a set of four triples on six distinct points having the form $\{abc, ade, bdf, cef\}$. The *opposite* Pasch configuration is

$\overline{P}(a, b, c, d, e, f) = P(f, b, c, d, e, a)$, and this covers the same pairs with a disjoint set of triples. If P_1 and P_2 are opposite Pasch configurations then $\mathcal{P} = \{P_1, P_2\}$ is a trade pair and the corresponding replacement operation is called a *Pasch trade*. This is the smallest possible trade in an STS(v), both by foundation and volume.

It is sometimes impossible to transform one given STS(v) to another by any sequence of Pasch trades. For 79 of the 80 nonisomorphic STS(15)s, it is possible to transform any one system to an isomorphic copy of another by a sequence of Pasch trades [4]. It was shown in [5] that, by allowing more general k-cycle trades, all 80 STS(15)s are connected. More recently, it was shown in [8] that the same is true for STS(19)s. However, the existence of perfect Steiner triple systems [6, 3] establishes that such transformations are not possible for all admissible orders.

Our main result is that, for $n \geq 4$, the projective system S_n of order $2^n - 1$ may be converted to a rigid system of the same order by Pasch trades, and that n block-disjoint Pasch trades suffice. So, if the distance between systems is measured by Pasch trades, S_n is distance at most n from a rigid system whenever $n \geq 4$. If the distance is measured by blocks then S_n is distance at most $4n$ from a rigid system whenever $n \geq 4$.

2 Preliminaries

An STS($2^n - 1$) with point set $A_n = \{1, 2, \ldots, 2^n - 1\}$, may be extended to an STS($2^{n+1} - 1$) with point set A_{n+1} by adjoining new blocks. Put $B_n = \{2^n, 2^n + 1, \ldots, 2^{n+1} - 1\}$, so that $A_n \cup B_n = A_{n+1}$ and take the new blocks to be all triples of the form xyz, where $x \in A_n$, $y, z \in B_n$ and $x \oplus y \oplus z = 0$. If this construction is applied to the projective system S_n, then S_{n+1} is the result. We will apply the construction recursively, starting with a rigid STS(15) which may be obtained from the projective system of order 15 (that is, S_4) by applying four block-disjoint Pasch trades. At each stage of the recursion we will apply one further block-disjoint Pasch trade and show that the resulting system is rigid. Thus for $n \geq 4$ we obtain a rigid STS($2^n - 1$), which we denote by S_n^*, and which is n Pasch trades distant from S_n.

The rigid STS(15), S_4^*, with which we start the recursion is given in Table 1. In fact it is system number 23 in the standard listing of [11]. It follows from results in [5] that the minimum number of Pasch trades required to convert S_4 to a rigid STS(15) is 4. The blocks which result from the trades are indicated by asterisks. More generally, a block xyz of an STS($2^n - 1$) with point set A_n will be called a *projective* block (pr-block for short) if $x \oplus y \oplus z = 0$, otherwise it will be called a *non-projective* block (npr-block for short). Thus in Table 1, the asterisked blocks are the npr-blocks and all remaining blocks are pr-blocks. The number of Pasch configurations containing the point x in S_n^* will be denoted by $p_n(x)$, and $p_4(x)$ is also tabulated in Table 1. Altogether there are 18 Pasch configurations in S_4^*.

$\{1,2,4\}^*$	$\{1,3,5\}^*$	$\{1,6,12\}^*$	$\{1,7,13\}^*$	$\{1,8,10\}^*$	$\{1,9,11\}^*$
$\{1,14,15\}$	$\{2,3,6\}^*$	$\{2,5,7\}$	$\{2,8,9\}^*$	$\{2,10,11\}^*$	$\{2,12,14\}$
$\{2,13,15\}$	$\{3,4,13\}^*$	$\{3,7,14\}^*$	$\{3,8,11\}$	$\{3,9,10\}$	$\{3,12,15\}$
$\{4,5,6\}^*$	$\{4,7,9\}^*$	$\{4,8,12\}$	$\{4,10,14\}$	$\{4,11,15\}$	$\{5,8,13\}$
$\{5,9,12\}$	$\{5,10,15\}$	$\{5,11,14\}$	$\{6,7,10\}^*$	$\{6,8,14\}$	$\{6,9,15\}$
$\{6,11,13\}$	$\{7,8,15\}$	$\{7,11,12\}$	$\{9,13,14\}^*$	$\{10,12,13\}^*$	

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$p_4(x)$	5	5	9	7	6	5	9	8	7	9	11	8	7	6	6

Table 1. The rigid STS(15), S_4^*.

There are two important points to note about S_4^*. First, the Pasch configuration $P^* = P(6,2,3,4,5,1)$ is the only Pasch configuration in which all four blocks lie in one and only one Pasch configuration. Second, the block $\{1,14,15\}$ is the only pr-block containing the point 1. In general for $n \geq 4$, we will call the triple $D_n = \{1, 2^n - 2, 2^n - 1\}$ the *distinguished triple* of order n, so $\{1,14,15\}$ is the distinguished triple of order 4, D_4.

As previously indicated, the construction of S_{n+1}^* from S_n^* is in two stages. First we apply the recursive construction as described above, adding new points and new projective blocks to form an STS$(2^{n+1}-1)$, denoted by T_{n+1}. Then we apply a Pasch trade involving the distinguished triple of order n and three of the new triples. We take the Pasch configuration $P_{n+1} = P(1, 2^n - 2, 2^n - 1, 2^n + 1, 2^n, 2^{n+1} - 1)$ in T_{n+1} and trade it for the opposite Pasch configuration, $\overline{P}_{n+1}$. If $\{a,b,c\}$ is one of the four blocks of S_{n+1}^* lying in $\overline{P}_{n+1}$, then either all the points a,b,c are in B_n, or one is in B_n and two are in A_n. On the other hand, if this block is not in $\overline{P}_{n+1}$, then either all the points a,b,c are in A_n, or one is in A_n and two are in B_n.

It is easy to show that S_4^* is rigid. Examining Table 1, the only point lying in 11 Pasch configurations is the point 11, so any automorphism must fix this point. The points 8 and 12 are the unique points lying in 8 Pasch configurations, so they are either fixed or transposed, and consideration of the block $\{4,8,12\}$ establishes that 4 is a fixed point. Then 9 and 13 are either fixed or transposed, so consideration of $\{9,13,14\}$ gives 14 fixed. But then $\{4,11,15\}$ gives 15 fixed, $\{4,10,14\}$ gives 10 fixed and $\{5,11,14\}$ gives 5 fixed. From $\{1,14,15\}$ we deduce that 1 is fixed and from $\{1,2,4\}$, 2 must be fixed. It is now trivial to show that all the remaining points are fixed by any automorphism.

3 Main result

In this section we prove that S_n^* is rigid for $n \geq 5$. The main step in our proof is Lemma 3.4, where we establish that any automorphism ϕ of S_n^* fixes the Pasch configuration $P^* = P(6, 2, 3, 4, 5, 1)$. In order to do this, in Lemmas 3.1, 3.2 and 3.3, we determine some lower bounds on the number of Pasch configurations containing each block of S_j^*. Note that if a Pasch configuration contains three pr-blocks and a fourth block xyz, then the sum of the three pr-blocks is both $x \oplus y \oplus z$ and $0 \oplus 0 \oplus 0 = 0$, so xyz is also a pr-block.

Lemma 3.1. *Suppose that $i \geq 4$ and that $B = xyz$ is an npr-block of S_i^* which appears in exactly k Pasch configurations in S_i^*. Then*

(i) B appears in at least $k-2$ Pasch configurations in S_{i+1}^*;

(ii) if $i \geq 5$ and $B \neq \{1, 2^{i-1}-2, 2^{i-1}+1\}$, $\{1, 2^{i-1}-1, 2^{i-1}\}$, $\{2^{i-1}-2, 2^{i-1}-1, 2^i-1\}$ or $\{2^{i-1}, 2^{i-1}+1, 2^i-1\}$ then B appears in at least k Pasch configurations in S_{i+1}^*;

(iii) if $i \geq 5$ then B appears in at least $k-2$ Pasch configurations in S_j^* for $j \geq i+1$ (at least k if B is not one of the four npr-blocks identified in (ii));

(iv) if $i = 4$ then B appears in exactly k Pasch configurations in S_j^* for $j \geq 4$.

Proof. (i) The distinguished triple $D_i = \{1, 2^i-2, 2^i-1\}$ of order i is the only block of S_i^* which is not a block of S_{i+1}^*. So B can only appear in fewer Pasch configurations in S_{i+1}^* if in S_i^* it lies in Pasch configurations with D_i. But two distinct blocks can lie together in at most two Pasch configurations, so B must appear in at least $k-2$ Pasch configurations in S_{i+1}^*.

(ii) Now suppose that $i \geq 5$ and that B and D_i lie together in a Pasch configuration Q in S_i^*. Without loss of generality, the block $B = xyz$ cannot lie with D_i in a Pasch configuration unless $x \in \{1, 2^i-2, 2^i-1\}$. But there are no npr-blocks of S_i^* containing the point 2^i-2. The only npr-blocks of S_i^* that contain the point 2^i-1 are $\{2^{i-1}-2, 2^{i-1}-1, 2^i-1\}$ and $\{2^{i-1}, 2^{i-1}+1, 2^i-1\}$. The only remaining possibility is that $x = 1$ and Q has blocks $B, D_i, \{2^i-2, y, w\}, \{2^i-1, z, w\}$. Since there are no npr-blocks in S_i^* containing the point 2^i-2, $\{2^i-2, y, w\}$ must be a pr-block and therefore $y = (2^i-2) \oplus w$. If $\{2^i-1, z, w\}$ were also a pr-block then Q would comprise three pr-blocks and one npr-block, which is impossible. Thus $\{2^i-1, z, w\}$ must be an npr-block, but the only npr-blocks containing the point 2^i-1 are $\{2^{i-1}-2, 2^{i-1}-1, 2^i-1\}$ and $\{2^{i-1}, 2^{i-1}+1, 2^i-1\}$. Hence $\{z, w\} = \{2^{i-1}-2, 2^{i-1}-1\}$ or $\{2^{i-1}, 2^{i-1}+1\}$. Examining the resulting four possibilities for the ordered pair (z, w), and computing y in each case, there are just two possibilities for B when $x = 1$, namely $\{1, 2^{i-1}-2, 2^{i-1}+1\}$ and $\{1, 2^{i-1}-1, 2^{i-1}\}$. (In fact, the four blocks B identified in this paragraph each lie in two Pasch configurations with D_i, but we do not use this result.)

(iii) By applying (i) and (ii) it follows that if $i \geq 5$ then B lies in at least $k-2$ Pasch configurations in S_j^* for $j \geq i+1$ (at least k if B is not one of the four npr-blocks identified in (ii)).

(iv) In the case $i = 4$, note that D_4 appears in no Pasch configurations in S_4^*. Hence B does not lie in any Pasch configurations with D_4 in S_4^*, so B appears in at least k Pasch configurations in S_5^* and also in S_i^* for $i > 5$. Suppose B lies in an additional Pasch configuration Q in S_5^*. At least one of the other blocks must be an npr-block. If this is an npr-block in S_4^*, then at least 5 points of Q lie in A_4, and in this case the remaining two blocks of Q must each contain two points from A_4 and one from B_4. But the only such blocks are three of the npr-blocks from $\overline{P}_5$, namely $\{1, 14, 17\}$, $\{1, 15, 16\}$ and $\{14, 15, 31\}$. Hence Q must contain an npr-block not in S_4^* and consequently B must contain one of the points 1, 14 and 15. From Table 1, there are six npr-blocks in S_4^* containing the point 1, two containing the point 14 and none containing the point 15. Pairing each of these eight npr-blocks in turn with an intersecting block from $\overline{P}_5$ gives 16 pairs. For each such pair there are two possibilities for the formation of a Pasch configuration, giving a total of 32 cases to be considered. In each of these cases one of the two additional blocks contains a point from A_4 and the other contains a point from B_4, and so these additional blocks cannot intersect one another and no Pasch configuration is formed. Thus if B is an npr-block which appears in exactly k Pasch configurations in S_4^*, then it appears in exactly k Pasch configurations in S_5^*. It only remains to prove that it lies in no additional Pasch configurations in S_j^* for $j \geq 6$.

So, suppose that $j \geq 6$ and that B lies in an additional Pasch configuration Q in S_j^*, but not in S_{j-1}^*. As above, at least one of the other blocks must be an npr-block. If this is an npr-block in S_{j-1}^*, then at least 5 points of Q lie in A_{j-1}, and in this case the remaining two blocks of Q must each contain two points from A_{j-1} and one from B_{j-1}. But the only such blocks are the npr-blocks $\{1, 2^{j-1}-2, 2^{j-1}+1\}$, $\{1, 2^{j-1}-1, 2^{j-1}\}$ and $\{2^{j-1}-2, 2^{j-1}-1, 2^j-1\}$. Hence Q must contain an npr-block not in S_{j-1}^*. The only possible intersection that B can have with such a block is the point 1 so, without loss of generality, we may take $x = 1$ and the two blocks as $1yz$ (which implies that neither y nor z is 14 or 15) and either $\{1, 2^{j-1}-2, 2^{j-1}+1\}$ or $\{1, 2^{j-1}-1, 2^{j-1}\}$. Note there are no npr-blocks containing any pairs from $\{y, z\} \times \{2^{j-1}-2, 2^{j-1}-1, 2^{j-1}, 2^{j-1}+1\}$. Hence, in either case, the remaining two blocks of the Pasch configuration are pr-blocks. By adding the six entries in these two blocks in each case, it can be seen that $y \oplus z = 2^j - 1$. But this contradicts the fact that $y, z \in A_4$. Hence B does not appear in any additional Pasch configurations in S_j^* for $j \geq 6$. $\square$

Lemma 3.2. *For $i \geq 5$, all the blocks of the Pasch configuration $\overline{P}_i$ lie in at least 4 Pasch configurations in S_i^*, and hence in at least 2 Pasch configurations in S_j^* for $j \geq i+1$.*

Proof. The blocks of P_i lie in an STS(7) subsystem of T_i with the additional point $2^i - 2$ and the three additional blocks $\{2^{i-1} - 2, 2^{i-1}, 2^i - 2\}$, $\{2^{i-1} - 1, 2^{i-1} + 1, 2^i - 2\}$ and $\{1, 2^i - 2, 2^i - 1\}$. When P_i is traded for $\overline{P}_i$ to form S_i^*, the blocks of $\overline{P}_i$ continue to form an STS(7) subsystem with the same three additional blocks. Since every block of an STS(7) lies in 4 Pasch configurations within that STS(7), it follows that all the blocks of $\overline{P}_i$ lie in at least 4 Pasch configurations in S_i^*. ☐

Lemma 3.3. *For $i \geq 5$ every pr-block of S_i^* lies in at least 12 Pasch configurations in S_i^*.*

Proof. In S_4^* there are 6 npr-blocks through the point 1, so in S_i^* $(i \geq 4)$ there are $6 + 2(i - 4) = 2i - 2$ npr-blocks through the point 1. In S_4^* there are 2 npr-blocks through the point 14, none through the point 15 and at most 4 npr-blocks through every other point, so in S_i^* $(i \geq 4)$ there are at most 4 npr-blocks through any point other than 1.

Let xyz be any pr-block of S_i^*, where $i \geq 6$. First we estimate the number of other pr-blocks containing x. There are $(2^i - 2)/2 = 2^{i-1} - 1$ blocks of S_i^* that contain x. If $x = 1$, $2i - 2$ of these are npr-blocks, otherwise at most 4 of these are npr-blocks. So the number of pr-blocks through x other than xyz is $2^{i-1} - 2i$ if $x = 1$ and at least $2^{i-1} - 6$ otherwise. Potentially, each of these other pr-blocks xvw may be paired with xyz to give two Pasch configurations. A Pasch configuration will certainly result if the two blocks generated by the pairs yv and zw are pr-blocks (and likewise for the pairs yw and zv). But if $y \neq 1$ at most 8 pairs through y lie in an npr-block, and similarly for z. So, for $i \geq 6$, there are at least $2(2^{i-1} - 2i) - 16 = 2^i - 4i - 16 \geq 24$ Pasch configurations containing the block xyz.

Finally, in the case $i = 5$, direct computation establishes that for each pr-block of S_5^*, the minimum number of Pasch configurations in S_5^* containing it is 12. ☐

Lemma 3.4. *For $i \geq 4$ $P^* = P(6, 2, 3, 4, 5, 1)$ is the only Pasch configuration in S_i^* that has all four of its blocks lying in exactly one Pasch configuration. Consequently, any automorphism of S_i^* maps this Pasch configuration to itself.*

Proof. By computation, this is true for $i = 4$. Moreover, all four blocks of P^* are npr-blocks, so they continue to lie in exactly 1 Pasch configuration in S_i^* for $i \geq 5$. Apart from the four npr-blocks of P^*, every other npr-block in S_4^* lies in at least 2 Pasch configurations in S_4^* and hence also in S_i^* for $i \geq 5$. All npr-blocks of S_i^* other than those already present in S_4^* arise from $\overline{P}_j$ for some $j \geq 4$, and so these appear in at least 2 Pasch configurations in S_i^*. Finally, for $i \geq 5$, all pr-blocks of S_i^* appear in at least 12 Pasch configurations in S_i^*. ☐

Theorem 3.1. *For $n \geq 4$, the Steiner triple system S_n^* is rigid.*

Proof. Let ϕ be an automorphism of S_n^*. When $n = 4$ we have already shown that ϕ is the identity permutation, so now assume $n \geq 5$. Consider $P^* = P(6,2,3,4,5,1)$. This has blocks $124, 135, 236, 456$ and it must be fixed by ϕ; in other words, ϕ is an extension of an automorphism of this Pasch configuration. A Pasch configuration has an automorphism group of order 24. Note that the pairs 16, 25 and 34 do not appear in the blocks of P^*, so $\phi(1)$ forces $\phi(6)$, and $\phi(2)$ forces $\phi(5)$. Table 2 lists all the automorphisms of P^* in two formats. For example, the entry labelled ϕ_1 indicates that ϕ_1 is the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix} = (1)(2,3)(4,5)(6)$. Our aim is to show that only ϕ_0 ex-

ϕ_0	123456	$(1)(2)(3)(4)(5)(6)$	ϕ_{12}	415263	$(1,4,2)(3,5,6)$
ϕ_1	132546	$(1)(2,3)(4,5)(6)$	ϕ_{13}	426153	$(1,4)(2)(3,6)(5)$
ϕ_2	145236	$(1)(2,4)(3,5)(6)$	ϕ_{14}	451623	$(1,4,6,3)(2,5)$
ϕ_3	154326	$(1)(2,5)(3,4)(6)$	ϕ_{15}	462513	$(1,4,5)(2,6,3)$
ϕ_4	213465	$(1,2)(3)(4)(5,6)$	ϕ_{16}	514362	$(1,5,6,2)(3,4)$
ϕ_5	231645	$(1,2,3)(4,6,5)$	ϕ_{17}	536142	$(1,5,4)(2,3,6)$
ϕ_6	246135	$(1,2,4)(3,6,5)$	ϕ_{18}	541632	$(1,5,3)(2,4,6)$
ϕ_7	264315	$(1,2,6,5)(3,4)$	ϕ_{19}	563412	$(1,5)(2,6)(3)(4)$
ϕ_8	312564	$(1,3,2)(4,5,6)$	ϕ_{20}	624351	$(1,6)(2)(3,4)(5)$
ϕ_9	321654	$(1,3)(2)(4,6)(5)$	ϕ_{21}	635241	$(1,6)(2,3,5,4)$
ϕ_{10}	356124	$(1,3,6,4)(2,5)$	ϕ_{22}	642531	$(1,6)(2,4,5,3)$
ϕ_{11}	365214	$(1,3,5)(2,6,4)$	ϕ_{23}	653421	$(1,6)(2,5)(3)(4)$

Table 2. Automorphisms of $P^* = P(1,2,4,3,5,6)$.

tends to an automorphism of S_n^*. Since $\phi_{21}^2 = \phi_{22}^2 = \phi_3$, showing that ϕ_3 cannot be extended will suffice to do the same for ϕ_{21} and ϕ_{22}. Similarly, elimination of ϕ_{20} (respectively, ϕ_{23}) eliminates ϕ_{10} and ϕ_{14} (respectively, ϕ_7 and ϕ_{16}). We also have $\phi_8^2 = \phi_5$, $\phi_{12}^2 = \phi_6$, $\phi_{17}^2 = \phi_{15}$, $\phi_{18}^2 = \phi_{11}$. So we need only consider ϕ_i for $i = 1,2,3,4,5,6,9,11,13,15,19,20,23$. In each case we assume that ϕ_i extends to an automorphism of S_n^* and derive a contradiction. Note that S_n^* contains all the blocks listed in Table 1, apart from the block $\{1,14,15\}$.

For $i = 1,2$, ϕ_i fixes the block $\{1,6,12\}$, and maps $\{2,5,7\}$ to $\{3,4,13\}$ and vice-versa. Hence ϕ_i fixes the point 12 and transposes 7 and 13. But then ϕ_i maps the block $\{7,12,11\}$ to $\{13,12,10\}$ and vice-versa, so it transposes the points 10 and 11. But consideration of the block $\{10,11,2\}$ then shows that ϕ_i fixes the point 2, a contradiction.

For $i = 4,19$, ϕ_i fixes the block $\{3,4,13\}$, and maps $\{2,5,7\}$ to $\{1,6,12\}$ and vice-versa. Hence ϕ_i fixes the point 13 and transposes 7 and 12. But then it must map the block $\{13,12,10\}$ to $\{13,7,1\}$, which implies that $\phi_i(10) = 1$, a contradiction.

For $i = 9,13$, ϕ_i fixes the block $\{2,5,7\}$, and maps $\{1,6,12\}$ to $\{3,4,13\}$ and vice-versa. Hence ϕ_i fixes the point 7 and transposes 12 and 13. But then it must map the block $\{7,12,11\}$ to $\{7,13,1\}$, which implies that $\phi_i(11) = 1$, a contradiction.

For $i = 3, 20, 23$, ϕ_i fixes the blocks $\{1,6,12\}$, $\{2,5,7\}$ and $\{3,4,13\}$. So ϕ_i fixes each of the points 7, 12 and 13. Hence ϕ_i fixes the block $\{7,13,1\}$, and consequently the point 1. The blocks $\{7,12,11\}$ and $\{12,13,10\}$ are fixed by ϕ_i, so the points 11 and 10 are also fixed. But then the block $\{2,10,11\}$ establishes that ϕ_i fixes the point 2. But points 1 and, 2 are not both fixed in any of these cases, so we have a contradiction.

For $i = 5, 6$, consideration of the blocks $\{1,6,12\}, \{2,5,7\}$ and $\{3,4,13\}$ gives $\phi_i(12) = 7, \phi_i(7) = 13$, so ϕ_i maps the block $\{7,12,11\}$ to $\{13,7,1\}$, implying that $\phi_i(11) = 1$, a contradiction.

For $i = 11, 15$ consideration of the blocks $\{1,6,12\}, \{3,4,13\}$ and $\{2,5,7\}$ gives $\phi_i(12) = 13, \phi_i(13) = 7$, so ϕ_i maps the block $\{12,13,10\}$ to $\{13,7,1\}$, implying that $\phi_i(10) = 1$, a contradiction.

It now follows that any automorphism ϕ of S_n^* fixes each of the points $1, 2, \ldots, 6$. Consideration of the following blocks in the order given proves that the points $7, 8, \ldots, 15$ are also fixed by ϕ: $\{1,6,12\}$, $\{2,5,7\}$,$\{3,4,13\}$, $\{3,7,14\}$, $\{4,7,9\}$, $\{4,8,12\}$, $\{4,10,14\}$, $\{5,10,15\}$ and $\{5,11,14\}$. Note that the block $D_4 = \{1,14,15\}$ of S_4^* which is destroyed by a Pasch trade in creating S_5^* has not been employed in this argument.

Now suppose that for some i with $4 \leq i < n$, all the points of A_i are known to be fixed by ϕ; this has just been proven for $i = 4$. We will prove that all the points of B_i are also fixed by ϕ. The system S_n^* contains the Pasch configuration $\overline{P}_{i+1}$ and consequently the block $\{1, 2^i - 1, 2^i\}$. Hence the point 2^i is fixed by ϕ. The block $\{2, 2^i, 2^i + 2\}$ lies in S_n^*, so the point $2^i + 2$ is also fixed by ϕ. Now consider all the triples of the form $\{x, 2^i + 2, (2^i + 2) \oplus x\}$ for $x \in A_i$. These are all blocks of S_n^* and so all the points $(2^i + 2) \oplus x$ $(x \in A_i)$ are fixed points of ϕ. But these cover all points of $B_i \setminus \{2^i + 2\}$. Hence all the points of B_i are fixed by ϕ. Since $A_i \cup B_i = A_{i+1}$, we deduce that all the points of A_{i+1} are fixed by ϕ. Then, by induction, ϕ fixes all the points of A_n, and so ϕ is the identity permutation on A_n, and S_n^* is rigid. $\square$

4 Concluding remarks

In this section we investigate the scope for improvements to the result of Section 3. In the discussions below it is convenient to consider each system of order $2^n - 1$ as having point set $\mathbb{Z}_2^n \setminus \{\mathbf{0}\}$.

Theorem 4.1. *Suppose that S_n is converted to another STS, say S_n', of the same order by a trade $\mathcal{T}$ whose foundation lies in a subspace $V_d \subseteq \mathbb{Z}_2^n$ of dimension d. If $d < n$ then S_n' is not rigid.*

Proof. If $d < n - 1$, add points to the subspace V_d to form a subspace V_{n-1} of dimension $n - 1$ that contains the foundation of $\mathcal{T}$. Put $W = \mathbb{Z}_2^n \setminus V_{n-1}$ so that

$|W| = 2^n - 2^{n-1} = 2^{n-1}$. If w^* is any fixed point of W then all the points $w^* \oplus v$ for $v \in V_{n-1}$ must lie in W for otherwise we have $w^* = (w^* \oplus v) \oplus v \in V_{n-1}$, a contradiction. Hence $W = \{w^* \oplus v : \ v \in V_{n-1}\}$.

First suppose that xyz is a block of S'_n with $x, y \in V_{n-1}$. If it is an npr-block then it arose in the trade and so $z \in V_{n-1}$, while if it is a pr-block then $z = x \oplus y \in V_{n-1}$. So a block with two points in V_{n-1} has all three points in V_{n-1}.

Second suppose that xyz is a block of S'_n with $x, y \in W$ and consequently xyz is a pr-block. Then $z = x \oplus y = (w^* \oplus u) \oplus (w^* \oplus v)$ for some $u, v \in V_{n-1}$. This gives $z = u \oplus v \in V_{n-1}$, and so a block with two points in W has its third point in V_{n-1}.

Now choose a fixed point $v^* \neq 0 \in V_{n-1}$ and define a mapping ϕ on $\mathbb{Z}_2^n$ by

$$\phi(z) = \begin{cases} z & \text{if } \ z \in V_{n-1}, \\ z \oplus v^* & \text{if } \ z \in W. \end{cases}$$

If xyz is a block of S'_n with all three points in V_{n-1} then $\phi(xyz) = xyz$. On the other hand, if xyz is a block of S'_n with $x, y \in W$ then $z \in V_{n-1}$ and so $\phi(x, y, z) = \{(x \oplus v^*), (y \oplus v^*), z\}$ and this is a block of S'_n because $(x \oplus v^*) \oplus (y \oplus v^*) = x \oplus y = z$. Hence ϕ is a non-trivial automorphism of S'_n, which is therefore not rigid. □

Corollary 4.1. *Suppose that S_n is converted to another STS, say S'_n, of the same order by a trade $\mathcal{T}$ consisting of p Pasch trades. If $p < \frac{n}{3}$ then S'_n is not rigid.*

Proof. The points of a Pasch configuration generate a subspace of dimension 3. So, if $p < \frac{n}{3}$, then the foundation of $\mathcal{T}$ lies in a subspace of dimension $d < n$, and the result follows. □

Theorem 3.1 shows that for $n \geq 4$, we can convert the projective system S_n to a rigid system using n Pasch trades. Corollary 4.1 proves that any such conversion requires at least $n/3$ Pasch trades. Our next result shows that an incremental approach has some limitations if we wish to improve on Theorem 3.1. First we define a projective extension.

Suppose that U_n is an STS$(2^n - 1)$ on the point set $\mathbb{Z}_2^n \setminus \{0\}$. Then U_n may be embedded in an STS$(2^{n+1} - 1)$, say U_{n+1}, by the addition of a new coordinate so that a point $x \in \mathbb{Z}_2^n \setminus \{0\}$ generates two new points $0x, 1x \in \mathbb{Z}_2^{n+1} \setminus \{0\}$, and we also add a further new point $100 \cdots 0$. Each block $\{a, b, c\}$ of U_n generates the block $\{0a, 0b, 0c\}$ of U_{n+1}, and the remaining blocks of U_{n+1} are all the triples of the form $\{0x, 1y, 1z\}$ where $x \oplus y \oplus z = 0$ in $\mathbb{Z}_2^n$ and $y \neq z$. The system U_{n+1} will be called the *projective extension* of U_n. The process may be repeated to give successive projective extensions $U_{n+1}, U_{n+2}, \ldots$ of U_n.

Theorem 4.2. *Suppose that R_n is a rigid STS$(2^n - 1)$ on the point set $\mathbb{Z}_2^n \setminus \{0\}$ obtained from S_n by some sequence of block-disjoint Pasch trades. If T_{n+2} is the projective extension of R_n to a system of order $2^{n+2} - 1$, then T_{n+2} is not rigid and* *it cannot be converted to a rigid system by a single further block-disjoint Pasch trade.*

Proof. A block $\{a, b, c\}$ of R_n generates a block $\{00a, 00b, 00c\}$ of T_{n+2}. We will call blocks of this form *type 0* blocks. The remaining blocks, which are all pr-blocks, are of four further types:

$$\begin{array}{ll} \textit{type 1}: \{00x, 01y, 01z\}, & \textit{type 2}: \{00x, 10y, 10z\}, \\ \textit{type 3}: \{00x, 11y, 11z\}, & \textit{type 4}: \{01x, 10y, 11z\}, \end{array}$$

where, in each case, $x \oplus y \oplus z = 0$.

Using this classification of blocks, we may classify the Pasch configurations of T_{n+2}. If a Pasch configuration has an $00x$ point then it must have two blocks containing this point, so the four blocks have the block types 0000, 0111, 0222, 0333, 1111, 1244, 1344, 2222, 2344, or 3333. If the Pasch configuration has no $00x$ point then the only possibility is 4444. So there are 11 types of Pasch configuration to consider. The type 0000 Pasch configurations correspond to those present in R_n.

We only consider trading a block-disjoint Pasch configuration, that is to say one that does not include any blocks resulting from trades already made in generating R_n from S_n. Thus any type 0 block involved in such a trade will be a pr-block. We will denote the resulting system obtained from T_{n+2} by $\overline{T}_{n+2}$.

First we argue that T_{n+2} itself is not rigid. We may consider that T_{n+2} is formed directly from S_{n+2} by a sequence of Pasch trades all of whose points have their first two coordinates 0. All the points of these trades lie in the subspace of dimension $n + 1$ given by the equation $\xi_{n+2} = 0$, where ξ_{n+2} denotes the first coordinate of a point. So, by Theorem 4.1, T_{n+2} is not rigid.

Now consider the case when $\overline{T}_{n+2}$ is obtained from T_{n+2} by trading a type 0000 Pasch configuration. Again, all the points of all the trades used to convert S_{n+2} to $\overline{T}_{n+2}$ satisfy $\xi_{n+2} = 0$, so $\overline{T}_{n+2}$ is not rigid. The same argument applies when $\overline{T}_{n+2}$ is obtained from T_{n+2} by trading a type 0111 or a type 1111 Pasch configuration. For types 0222 and 2222, the argument is essentially the same but with the equation $\xi_{n+1} = 0$, where ξ_{n+1} denotes the second coordinate of a point. For types 0333 and 3333, the argument may be repeated but with the equation $\xi_{n+2} \oplus \xi_{n+1} = 0$.

Consider next trading a type 1244 Pasch configuration P. This has blocks of the form:

$$\begin{array}{ll} \{00a, 01b, 01c\} \;\; (a \oplus b \oplus c = 0), & \{00a, 10d, 10e\} \;\; (a \oplus d \oplus e = 0), \\ \{01b, 10d, 11f\} \;\; (b \oplus d \oplus f = 0), & \{01c, 10e, 11f\} \;\; (c \oplus e \oplus f = 0). \end{array}$$

The traded Pasch configuration $\overline{P}$ comprises the blocks:

$$\begin{array}{ll} \{11f, 01b, 01c\}, & \{11f, 10d, 10e\}, \\ \{01b, 10d, 00a\}, & \{01c, 10e, 00a\}. \end{array}$$

Define $\phi : 00x \to 00x$, $11x \to 11x$, $01x \to 10(x \oplus f)$, $10x \to 01(x \oplus f)$. This mapping stabilizes $\overline{P}$, maps the image of R_n in $\overline{T}_{n+2}$ to itself, and maps all the remaining blocks (which are pr-blocks) amongst themselves. So ϕ is a non-trivial automorphism of $\overline{T}_{n+2}$.

A similar argument works for Pasch types 1344 and 2344.

Finally consider trading a type 4444 Pasch configuration P. This has blocks of the form:

$$\begin{array}{llll} \{01a, 10b, 11c\} & (a \oplus b \oplus c = 0), & \{01a, 11d, 10e\} & (a \oplus d \oplus e = 0), \\ \{10b, 11d, 01f\} & (b \oplus d \oplus f = 0), & \{11c, 10e, 01f\} & (c \oplus e \oplus f = 0). \end{array}$$

The traded Pasch configuration $\overline{P}$ comprises the blocks:

$$\begin{array}{ll} \{01f, 10b, 11c\}, & \{01f, 11d, 10e\}, \\ \{10b, 11d, 01a\}, & \{11c, 10e, 01a\}. \end{array}$$

Define $\phi : 00x \to 00x$, $11x \to 11x$, $01x \to 10(x \oplus c)$, $10x \to 01(x \oplus c)$. This mapping stabilizes $\overline{P}$, maps the image of R_n in $\overline{T}_{n+2}$ to itself, and maps all the remaining blocks (which are pr-blocks) amongst themselves. So ϕ is a non-trivial automorphism of $\overline{T}_{n+2}$.

It follows that we cannot apply a single (block-disjoint) Pasch trade to T_{n+2} to get a new rigid system of order $2^{n+2} - 1$. $\square$

Despite Theorem 4.2, the following example shows that it is possible to do better than the result of Theorem 3.1.

Example 4.1. *The projective system S_5 may be converted to a rigid system using three block-disjoint Pasch trades.*

Take the point set to be A_5 and the three block-disjoint Pasch configurations $P_1 = P(1, 2, 3, 4, 5, 6)$, $P_2 = P(1, 6, 7, 8, 9, 14)$, and $P_3 = P(2, 9, 11, 16, 18, 25)$. Trading all three gives a new system, say R_5. For each $x \in A_5$, Table 3 gives the number, $q_5(x)$, of Pasch configurations in R_5 containing the point x.

x	1	2	3	4	5	6	7	8	9	10	11
$q_5(x)$	113	117	146	146	143	110	154	150	117	178	147
x	12	13	14	15	16	17	18	19	20	21	22
$q_5(x)$	177	177	146	187	146	176	142	175	175	174	175
x	23	24	25	26	27	28	29	30	31		
$q_5(x)$	175	175	142	174	186	174	174	175	174		

Table 3. The number of Pasch configurations in R_5 containing x.

It follows from Table 3 that any automorphism of R_5 must fix the points 1, 5, 6, 7, 8, 10, 11, 15, 17, and 27. It is then easy to argue that all remaining points are fixed; for example the block $\{1,3,5\}$ must be stabilized, and so 5 is a fixed point. By exhaustive computer search we have also shown that it is not possible to convert S_5 to a rigid system using just two Pasch trades. We hope to publish a more comprehensive study of Pasch trades on S_5 in a future paper.

Example 4.1 is not an isolated case. For specific values of n it is easy to find examples which convert S_n to a rigid system by employing fewer than n Pasch trades. Thus the question of finding, as a function of n, the minimum number of Pasch trades necessary to convert S_n to a rigid system remains open. It seems likely that there is some constant c satisfying $\frac{1}{3} \leq c \leq 1$ such that the minimum number of Pasch trades required is asymptotic to cn. Given a collection of $k < n_0$ Pasch trades which convert S_{n_0} to a rigid system, we speculate that a modest generalization of our construction, albeit with a more complicated proof, might facilitate a result that for $n \geq n_0$, $n - (n_0 - k)$ Pasch trades suffice to convert S_n to a rigid system. But to obtain a result which is substantially better than our Theorem 3.1, that is to say one that improves the putative constant c, a new construction is likely to be required.

Acknowledgements Part of this work was done when the second author was visiting the first author and he thanks him for his hospitality. He also acknowledges partial support by Slovak research grants VEGA 1/0781/11 and APVV-0223-10.

References

[1] L. Babai, Almost all Steiner triple systems are asymmetric, in: Topics on Steiner systems (Ed; C. C. Lindner and A. Rosa), Ann. Discrete Math. **7** (1980), 37–39.

[2] C. J. Colbourn and A. Rosa, Triple Systems, Clarendon Press, Oxford, 1999.

[3] A. D. Forbes, M. J. Grannell and T. S. Griggs, On 6-sparse Steiner triple systems. J. Combin. Theory Ser. A **114** (2007), 235–252.

[4] P. B. Gibbons, Computing techniques for the construction and analysis of block designs, Ph.D. thesis, University of Toronto (Department of Computer Science, University of Toronto, Technical Report 92/76), 1976.

[5] M. J. Grannell, T. S. Griggs and J. P. Murphy, Switching cycles in Steiner triple systems, Utilitas Math. **56** (1999), 3–21.

[6] M. J. Grannell, T. S. Griggs and J. P. Murphy, Some new perfect Steiner triple systems, J. Combin. Des. **7** (1999), 327–330.

[7] J. W. P. Hirschfeld, Projective geometries over finite fields, second edition, Clarendon Press, Oxford, 1998.

[8] P. Kaski, V. Mäkinen and P. R. J. Östergård, The cycle switching graph of the Steiner triple systems of order 19 is connected, Graphs Combin. **27** (2011), 539–546.

[9] T. P. Kirkman, On a problem in combinations, Cambridge and Dublin Math. J. **2** (1847), 191–204.

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

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

[12] R. M. Wilson, Nonisomorphic Steiner triple systems, Math. Z. **135** (1974), 303–313.