The centre of a Steiner loop and the maxi-Pasch problem

Andrew R. Kozlik

Abstract. A binary operation "$\cdot$" which satisfies the identities $x \cdot e = x$, $x \cdot x = e$, $(x \cdot y) \cdot x = y$ and $x \cdot y = y \cdot x$ is called a Steiner loop. This paper revisits the proof of the necessary and sufficient conditions for the existence of a Steiner loop of order n with centre of order m and discusses the connection of this problem to the question of the maximum number of Pasch configurations which can occur in a Steiner triple system (STS) of a given order. An STS which attains this maximum for a given order is said to be *maxi-Pasch*. We show that loop factorization preserves the maxi-Pasch property and find that the Steiner loops of all currently known maxi-Pasch Steiner triple systems have centre of maximum possible order.

Keywords: Steiner loop; centre; nucleus; Steiner triple system; Pasch configuration; quadrilateral

Classification: 05B07, 20N05

1. Introduction

A *Steiner triple system* of order v, STS(v), is a pair $(V, \mathcal{B})$ where V is a set of v points and $\mathcal{B}$ is a collection of triples of distinct points taken from V such that every pair of distinct points from V appears in precisely one triple. Such systems exist if and only if $v \equiv 1$ or $3 \pmod 6$, see [14]. Given an STS $(V, \mathcal{B})$ one can define a binary operation "$\cdot$" on the set $L = V \cup \{e\}$ by assigning $x \cdot e = e \cdot x = x$, $x \cdot x = e$ for all $x \in L$ and $x \cdot y = z$ whenever $\{x, y, z\} \in \mathcal{B}$. The induced operation satisfies the identities

$$(1) \qquad x \cdot e = x, \qquad x \cdot x = e, \qquad (x \cdot y) \cdot x = y, \qquad x \cdot y = y \cdot x$$

for all x and y in L. Any binary operation satisfying these four identities is called a *Steiner loop*. The process described above is reversible. Given a Steiner loop one can obtain an STS by assigning $\{x, y, x \cdot y\} \in \mathcal{B}$ for all $x, y \in V$, $x \neq y$. There is therefore a one-to-one correspondence between Steiner triple systems and nontrivial Steiner loops. Thus a Steiner loop of order n exists if and only if $n = 1$ or $n \equiv 2$ or $4 \pmod 6$. In the remainder of this paper we replace the loop operation "$\cdot$" with juxtaposition.

DOI 10.14712/1213-7243.2020.035

The most well known examples of Steiner triple systems come from finite geometry. Let $V = \mathbb{F}_2^k \setminus \{\mathbf{0}\}$ and let $\mathcal{B}$ be the collection of all $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ such that $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ are pairwise distinct and $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. Then $(V, \mathcal{B})$ is a *projective* $\mathrm{STS}(2^k - 1)$. Its corresponding Steiner loop is $(\mathbb{F}_2^k, +)$. A Steiner loop is associative if and only if it is isomorphic to $(\mathbb{F}_2^k, +)$, see [5].

In a Steiner triple system, a collection of four triples on six points is called a *Pasch configuration* or *quadrilateral*. It is easily seen that this structure is necessarily of the form $\{a, b, c\}$, $\{a, d, f\}$, $\{b, f, g\}$, $\{c, d, g\}$ up to relabeling. For example an STS(7) contains seven distinct Pasch configurations. A Steiner triple system is said to be *anti-Pasch* if it does not contain a Pasch configuration.

Theorem 1.1 ([10], [15]). *An anti-Pasch* $\mathrm{STS}(v)$ *exists if and only if* $v \equiv 1$ *or* $3 \pmod 6$ *and* $v \neq 7$, 13.

A loop L with neutral element e is said to have the *inverse property* if for each $x \in L$ there exists an element x^{-1} such that $x^{-1}(xy) = y = (yx)x^{-1}$ for every $y \in L$. Every Steiner loop has the inverse property, since defining $x^{-1} := x$ satisfies the required condition.

The *left nucleus* N_λ, *middle nucleus* N_μ and *right nucleus* N_ϱ of a loop L are defined as

$$\begin{aligned} N_\lambda(L) &= \{x \in L \colon x(yz) = (xy)z \ \text{ for all } \ y, z \in L\}, \\ N_\mu(L) &= \{y \in L \colon x(yz) = (xy)z \ \text{ for all } \ x, z \in L\}, \\ N_\varrho(L) &= \{z \in L \colon x(yz) = (xy)z \ \text{ for all } \ x, y \in L\}. \end{aligned}$$

The *nucleus* of L, defined as $N(L) = N_\lambda(L) \cap N_\mu(L) \cap N_\varrho(L)$, is a subgroup of L. The *centre* of a loop L is defined as

$$Z(L) = N(L) \cap \{x \in L \colon xy = yx \ \text{ for all } \ y \in L\}.$$

The three nuclei coincide for any inverse property loop [1, Theorem VII.2.1]. Thus if L is a Steiner loop, then the three nuclei coincide and $N(L) = Z(L)$. Because the centre of a Steiner loop is an associative Steiner loop, its cardinality is a power of 2.

2. The centre of a Steiner loop

This section briefly revisits the proof of the necessary and sufficient conditions for the existence of a Steiner loop of order n with centre of order m published by D. Donovan and A. Rahilly, see [6] and [7]. In some cases simpler or alternative proofs of the original results are demonstrated.

A subloop K of L is said to be *normal* in L if $xK = Kx$, $x(yK) = (xy)K$ and $(xK)y = x(Ky)$ for all x, $y \in L$. The *factor loop* L/K is then defined in the usual way. Clearly, for any loop L the centre $Z(L)$ is normal in L.

Lemma 2.1. *Let L be a Steiner loop of order n with centre of order m and let k be the largest integer such that 2^k divides n. Then $m = 2^i$, where $i \in \{0, 1, \dots, k\}$. If $n \neq 2^k$, then $m \neq 2^k$.*

Proof: As noted in the introduction, m is a power of 2. Since the factor loop $L/Z(L)$ satisfies the identities (1), it is also a Steiner loop, and we either have $n/m = 1$ or we have $n/m \equiv 2$ or $4 \pmod 6$. In the former case the loop is associative, thus $n = 2^k$ and $m = 2^k$. In the latter case, in order for n/m to be even, m must be at most 2^{k-1}. □

Lemma 2.2. *If there exists a Steiner loop of order n with centre of order m, then there exists a Steiner loop of order $2n$ with centre of order $2m$.*

Proof: Let L be a Steiner loop of order n. Then $L \times \mathbb{F}_2$ is also a Steiner loop, since it satisfies the identities (1), and its centre is $Z(L) \times \mathbb{F}_2$. □

Proposition 2.3. *A Steiner loop of order n with a nontrivial centre exists if and only if $n \equiv 4$ or $8 \pmod{12}$ or $n = 2$.*

Proof: If $n \equiv 4$ or $8 \pmod{12}$ or $n = 2$, then there exists a Steiner loop of order $n/2$. By Lemma 2.2 there then exists a Steiner loop of order n with centre of order at least 2. If $n \equiv 2$ or $10 \pmod{12}$ and $n \neq 2$, then by Lemma 2.1 the centre of every Steiner loop of order n is trivial. □

With the help of a computer running the model builder Mace4, see [16], we can obtain a census of the centres of Steiner loops of order up to 20. The three unique Steiner triple systems of orders 1, 3 and 7 are projective, thus their corresponding loops all satisfy $Z(L) = L$. The Steiner loops of the unique STS(9) and of both STS(13)s all have trivial centre. There are only two STS(15)s up to isomorphism that induce a loop with a nontrivial centre. One is the projective STS(15) and the other is the system with automorphism group of order 192, i.e. System # 2 in [3]. The latter has centre of order 2. There are only three STS(19)s up to isomorphism that induce a loop with a nontrivial centre. They are the unique systems with automorphism groups of orders 108, 144 and 432. Each has centre of order 2. In light of the next theorem, it does not come as a surprise that these are precisely the three systems with 84 Pasch configurations, which is the maximum possible for any STS(19), see [13].

The next result is analogous to [6, Theorem 4]. We demonstrate a simpler proof by approaching the problem from a more algebraic perspective.

Theorem 2.4. *Let $(V, \mathcal{B})$ be an* STS *and let L be its Steiner loop. For any $x \in L$ the following conditions are equivalent:*

(1) *The element x lies in the centre of L.*
(2) *If x, y and z are pairwise distinct elements of V, then the set $\{x, y, z\}$ generates a sub-*STS(3) *or a sub-*STS(7) *in $(V, \mathcal{B})$.*
(3) *For each $y, z \in L$, the subloop $\langle x, y, z\rangle$ is of order at most 8.*

Proof: Let $x \in Z(L) \setminus \{e\}$ and $y,\ z \in V$ be pairwise distinct elements such that $\{x, y, z\}$ does not lie in $\mathcal{B}$. By definition $\{x, y, xy\}, \{x, z, xz\}, \{y, z, yz\} \in \mathcal{B}$, and since $(xy)(xz) = ((xy)x)z = yz$, we also have $\{xy, xz, yz\} \in \mathcal{B}$. Furthermore $\{x, yz, xyz\}, \{y, xz, xyz\}, \{z, xy, xyz\} \in \mathcal{B}$. These seven triples form a sub-STS(7). Thus (1) implies (2).

Assume that (2) holds and let $x, y, z \in L$. If these three points are not pairwise distinct elements of V or if $\{x, y, z\} \in \mathcal{B}$, then $\langle x, y, z\rangle$ is a subloop of order 1, 2 or 4 in L. Otherwise, by assumption, $\langle x, y, z\rangle$ is a subloop of order 8 in L. Thus (2) implies (3).

In a Steiner loop every subloop of order at most 8 is necessarily a group. Thus (3) implies (1). □

It immediately follows from the previous theorem that every anti-Pasch STS(n), $n > 3$, gives rise to a Steiner loop with trivial centre. Taking into account the above census of the centres of Steiner loops of small orders, we have the following result.

Corollary 2.5. *A Steiner loop of order n with trivial centre exists if and only if $n = 1$ or $n \equiv 2$ or $4 \pmod 6$ and $n \notin \{2, 4, 8\}$.*

The following is an alternative proof of [7, Corollary 3.10].

Lemma 2.6 ([7]). *If L is a non-associative Steiner loop of order n with centre of order m, then $m < \frac{1}{4}n$.*

Proof: Since L is non-associative, it follows from Theorem 2.4 that there exist points $x, y, z \in L$ such that the order of the subloop $\langle x, y, z\rangle$ is strictly greater than 8. None of these three points lie in the centre and neither does the point xy, because $\langle xy, x, z\rangle = \langle x, y, z\rangle$. For any $u \in Z(L)$ we have $\langle u, x, y\rangle = \{e, x, y, xy, u, xu, yu, (xy)u\}$, where only e and u lie in the centre. Thus if $u, v \in Z(L)$, $u \neq v$, then $\langle u, x, y\rangle \neq \langle v, x, y\rangle$ and therefore $\langle u, x, y\rangle \cap \langle v, x, y\rangle = \langle x, y\rangle$. If $u \in Z(L) \setminus \{e\}$, then $\langle u, x, y\rangle$ is of order 8 and $\langle x, y\rangle$ is of order 4, thus the set $\bigcup_{u \in Z(L)} \langle u, x, y\rangle$ has cardinality $4(m-1)+4$. Finally, note that the point z does not lie in $\langle u, x, y\rangle$ for any $u \in Z(L)$. Thus there are at least $4m+1$ pairwise distinct points in L. □

The main result of D. Donovan and A. Rahilly now follows.

Theorem 2.7 ([7]). *Let $n = 2^k\eta$ be a positive integer, where η is odd. A non-trivial Steiner loop of order n with centre of order m exists if and only if $n \equiv 2$ or $4 \pmod 6$, and*

(a) $\eta = 1$, $(n, m) \neq (8, 1)$ *and* $m = 2^i$, *where* $i \in \{0, 1, \dots, k-3\} \cup \{k\}$, *or*
(b) $\eta > 1$ *and* $m = 2^i$, *where* $i \in \{0, 1, \dots, k-1\}$.

Proof: The necessity of the conditions follows from Lemmas 2.1 and 2.6 and from the fact that the unique STS(7) is projective.

If the integers n and $m = 2^i$ satisfy the conditions given above, then $n/m = 1$ or $n/m \equiv 2$ or $4 \pmod 6$ but $n/m \notin \{2, 4\}$. If $n/m \neq 8$, then by Corollary 2.5 there exists a Steiner loop of order n/m with trivial centre, thus by applying Lemma 2.2 in i iterations we obtain a Steiner loop of order n with centre of order m. If $n/m = 8$, then start instead with the Steiner loop of order 16 that has centre of order 2 and apply Lemma 2.2 in $i - 1$ iterations. $\square$

3. Maxi-Pasch Steiner triple systems

Denote the number of Pasch configurations in an STS(v), $(V, \mathcal{B})$, by $P(\mathcal{B})$. Define

$$P(v) = \max\{P(\mathcal{B}) \colon (V, \mathcal{B}) \text{ is an } \mathrm{STS}(v)\}.$$

An STS(v), $(V, \mathcal{B})$, is said to be *maxi-Pasch* if $P(\mathcal{B}) = P(v)$. In [17] D. R. Stinson and Y. J. Wei undertook a preliminary investigation of the bounds on $P(v)$. An elementary counting argument yields $P(v) \leq v(v-1)(v-3)/24$. The authors show that an STS(v) achieves this bound if and only if it is projective. Currently the only known values when $v \neq 2^k - 1$ are $P(9) = 0$, $P(13) = 13$ and $P(19) = 84$. D. R. Stinson and Y. J. Wei present several recursive lower bounds on $P(v)$. B. D. Gray and C. Ramsay in [12] present another recursive lower bound which is given in Corollary 3.4 below. In [11] M. Grannell and G. Lovegrove give lower bounds on $P(v)$ for v of the form $2^{2k} + 3$ or $2^{2k} + 5$.

The Pasch configuration is just one of 16 possible four-line configurations in an STS(v). For 5 of these configurations, the number of occurrences depends only on v. For the other 11 configurations and fixed v, the number of occurrences of any one determines the number of occurrences of all the others, see [9]. Thus the results about the number of Pasch configurations given in this section could equally well be rewritten in terms of any of the other variable four-line configurations.

Let Q be a quasigroup of order n. An ordered triple (a, b, c) of elements of Q is said to be *associative* if $a \cdot bc = ab \cdot c$. Denote the set of associative triples by $A(Q)$. Thus Q is a group if and only if $|A(Q)| = n^3$. The number of Pasch configurations in an STS is directly related to the number of associative triples in its Steiner loop.

Proposition 3.1. *Let L be a Steiner loop of order n and let $(V, \mathcal{B})$ be the corresponding* STS. *Then*

$$|A(L)| = n^3 - (n-1)(n-2)(n-4) + 24P(\mathcal{B}).$$

Proof: In a Steiner loop, if the triple $(a, b, c) \in L^3$ generates a subloop of order at most 4, then it is associative. This happens if $e \in \{a, b, c\}$, if two or more elements of the ordered triple are identical or if $\{a, b, c\}$ is a block in $\mathcal{B}$.

Let $(a, b, c) \in V^3$ be an ordered triple of distinct elements such that $\{a, b, c\} \notin \mathcal{B}$. The number of such triples is $(n-1)(n-2)(n-4)$, because the third element needs to be chosen so as to avoid forming a block of $\mathcal{B}$. The set of blocks $\{\{a, b, ab\}, \{b, c, bc\}, \{ab, c, (ab)c\}, \{a, bc, a(bc)\}\} \subset \mathcal{B}$ is a Pasch configuration if and only if (a, b, c) is an associative triple. Now observe that for each Pasch configuration $\mathcal{P}$ there are 24 associative triples in L^3 from which $\mathcal{P}$ can arise in this way. There are six ways to select two blocks $B_1, B_2 \in \mathcal{P}$. The point of intersection of B_1 and B_2 is the middle element of an associative triple. Any of the four other points in $B_1 \cup B_2$ can be chosen as the first element of the associative triple and its third element is then determined so that the resulting triple gives rise to $\mathcal{P}$. Thus the number of triples in L^3 that are not associative is $(n-1)(n-2)(n-4) - 24P(\mathcal{B})$. □

Lemma 3.2. *Let K and L be loops. Then $|A(K \times L)| = |A(K)| \cdot |A(L)|$.*

Proof: Since multiplication in the loop product $K \times L$ is defined componentwise, we have $((a_1, a_2), (b_1, b_2), (c_1, c_2)) \in A(K \times L)$ if and only if $(a_1, b_1, c_1) \in A(K)$ and $(a_2, b_2, c_2) \in A(L)$. □

Theorem 3.3. *Let $(V_1, \mathcal{B}_1)$ be an* STS(v_1) *and $(V_2, \mathcal{B}_2)$ be an* STS(v_2). *Then there exists an* STS$(v_1v_2 + v_1 + v_2)$, *$(V, \mathcal{B})$, such that*

$$\begin{aligned} P(\mathcal{B}) = {} & \frac{7}{12} v_1 v_2 (3v_1v_2 - v_1 - v_2 - 1) \\ & + P(\mathcal{B}_1)(7v_2^2 + 1) + P(\mathcal{B}_2)(7v_1^2 + 1) + 24P(\mathcal{B}_1)P(\mathcal{B}_2). \end{aligned}$$

Proof: Let K and L be the Steiner loops of $(V_1, \mathcal{B}_1)$ and $(V_2, \mathcal{B}_2)$, respectively, and let $(V, \mathcal{B})$ be the STS corresponding to the Steiner loop $K \times L$. Then $|K| = v_1 + 1$, $|L| = v_2 + 1$ and $|K \times L| = v_1v_2 + v_1 + v_2 + 1$. In the equation from the previous lemma $|A(K \times L)| = |A(K)| \cdot |A(L)|$ substitute each of the cardinalities using Proposition 3.1 and express $P(\mathcal{B})$ to obtain the result. □

Taking $(V_1, \mathcal{B}_1)$ to be a maxi-Pasch STS(u) and $(V_2, \mathcal{B}_2)$ to be an STS(1), i.e. $L = \mathbb{F}_2$ and $P(\mathcal{B}_2) = 0$, gives the Gray–Ramsay bound.

Corollary 3.4 ([12]). *If* $v = 2u + 1 \equiv 3$ *or* $7 \pmod{12}$, $u \geq 7$, *then*

$$P(v) \geq \frac{7(v-1)(v-3)}{24} + 8P(u).$$

Proposition 3.1 shows that the problem of maximizing the number of Pasch configurations in an STS is equivalent to maximizing the number of associative triples in the corresponding Steiner loop, which has been studied for quasigroups in general, see [8]. This indicates that a Steiner loop with large centre corresponds to a Steiner triple system with a large number of Pasch configurations. Theorem 2.4 allows us to determine a lower bound on the number of sub-STS(7)s and thus the number of Pasch configurations when the order of the centre is given.

Proposition 3.5. *Let L be a Steiner loop of order n with centre of order m. Then the number of sub-*STS*(7)s in the Steiner triple system corresponding to L is at least*

$$\frac{m-1}{168}\big((m-2)(m-4) + 7(n-m)(n-m-2)\big). \tag{2}$$

Proof: Let $(V, \mathcal{B})$ be the Steiner triple system which corresponds to L. By $\mathcal{F}_i$ denote the set of all sub-STS(7)s in $(V, \mathcal{B})$ such that exactly i points of the subsystem lie in the centre of L. The only admissible values of i are $0, 1, 3$ and 7. Consider three pairwise distinct points $x, y, z \in V$, which do not lie in a common block. These three points generate a system in $\mathcal{F}_7$ if and only if they all lie in the centre. The number of ways of choosing three points from $Z(L) \setminus \{e\}$, so that they do not lie in a common block, is $(m-1)(m-2)(m-4)$. This way each of the systems in $\mathcal{F}_7$ is counted 168 times, thus

$$|\mathcal{F}_7| = \frac{(m-1)(m-2)(m-4)}{168}.$$

It follows from Theorem 2.4 that if one of the points x, y or z lies in the centre and the other two do not, then they generate a system in $\mathcal{F}_1$ or $\mathcal{F}_3$. In fact every system in $\mathcal{F}_1 \cup \mathcal{F}_3$ can be generated in this manner. The number of ways of choosing three points such that the first is from $Z(L) \setminus \{e\}$ and the remaining two are from $V \setminus Z(L)$, but do not all lie in a common block, is $(m-1)(n-m)(n-m-2)$. This way each of the systems in $\mathcal{F}_1$ and $\mathcal{F}_3$ is counted 24 times, thus

$$|\mathcal{F}_1| + |\mathcal{F}_3| = \frac{(m-1)(n-m)(n-m-2)}{24}.$$

The sum $|\mathcal{F}_1| + |\mathcal{F}_3| + |\mathcal{F}_7|$ gives a lower bound on the number of sub-STS(7)s in $(V, \mathcal{B})$. $\square$

It is not immediately obvious from the previous proposition that the number of sub-STS(7)s is maximized by maximizing the order m of the centre. By Lemma 2.6 we only need to consider m in the interval $[0, \frac{1}{4}n]$. Formula (2) is a cubic function in m with a positive leading coefficient and with stationary points at $m = n(7 \pm \sqrt{7})/12$. The lesser of the two stationary points is clearly greater than $\frac{1}{3}n$. So on the interval $[0, \frac{1}{4}n]$ the function is indeed increasing.

To obtain a lower bound on the maximum number of sub-STS(7)s in a Steiner triple system of order v, we can set the order m of the centre in the previous proposition to the maximum value as given by Theorem 2.7. Multiplying the resulting bound by 7 gives a lower bound on the number of Pasch configurations, because there are seven Pasch configurations in each sub-STS(7) and no two sub-STS(7)s share a common Pasch configuration. This yields the following result.

Corollary 3.6. *Let* $v \equiv 1$ *or* $3 \pmod 6$ *and let* k *be the largest integer such that* 2^k *divides* $v+1$*. Then*

$$P(v) \geq \frac{2^{k-1}-1}{24}\big(2^{k-1}(2^{k-1}-6) + 7(v-2^{k-1})^2 + 1\big).$$

The next proposition gives insight into how Pasch configurations behave under loop factorization.

Theorem 3.7. *Let* L *be a Steiner loop with nontrivial centre and let* $(V, \mathcal{B})$ *be the corresponding* STS *of order* v*. Then for any* $z \in Z(L) \setminus \{e\}$ *the* STS $(V', \mathcal{B}')$ *corresponding to the factor loop* $L/\langle z\rangle$ *satisfies*

$$P(\mathcal{B}) \leq \frac{7(v-1)(v-3)}{24} + 8P(\mathcal{B}').$$

Proof: For any Pasch configuration $\mathcal{P} = \{\{a,b,c\},\{a,d,f\},\{b,f,g\},\{c,d,g\}\}$ in $\mathcal{B}$ denote its point set $V_{\mathcal{P}} = \{a,b,c,d,f,g\}$. There are two types of Pasch configuration in $\mathcal{B}$:

1. If $V_{\mathcal{P}} \cap zV_{\mathcal{P}} \neq \emptyset$, then without loss of generality $az = b$ or $az = g$.
   (a) If $az = b$ then $c = z$, $bd = (za)d = z(ad) = zf$ and $ag = (zb)g = z(bg) = zf$. Thus $K = V_{\mathcal{P}} \cup \{e, fz\}$ is a subloop of order 8.
   (b) If $az = g$ then $bz = (ca)z = c(az) = cg = d$ and $cz = (ba)z = b(az) = bg = f$. Thus $K = V_{\mathcal{P}} \cup \{e, z\}$ is a subloop of order 8.
2. If $V_{\mathcal{P}} \cap zV_{\mathcal{P}} = \emptyset$, then first let us show that in this case $zV_{\mathcal{P}} \subset V$. To see this, assume to the contrary that $e \in zV_{\mathcal{P}}$. Then $z \in V_{\mathcal{P}}$ and there exists some $x \in V_{\mathcal{P}}$ such that $\{x, z, xz\} \in \mathcal{P}$. Thus $x \in V_{\mathcal{P}} \cap zV_{\mathcal{P}}$, which is a contradiction. For any $\{w,x,y\} \in \mathcal{P}$ we also have $\{w, xz, yz\} \in \mathcal{B}$, because $w(xz) = (wx)z = yz$, and similarly $\{wz, x, yz\}$, $\{wz, xz, y\} \in \mathcal{B}$. Thus there are eight distinct Pasch configurations in $\mathcal{B}$, each of the form

$$\{\{az^i, bz^j, cz^{i+j}\},\ \{az^i, dz^{i+k}, fz^k\},$$
$$\{bz^j, fz^k, gz^{j+k}\},\ \{cz^{i+j}, dz^{i+k}, gz^{j+k}\}\},$$

where $i,\ j,\ k \in \{0, 1\}$, arithmetic in the exponents modulo 2.

For each Pasch configuration $\mathcal{P}$ of type 1, $V_{\mathcal{P}} \cup \{z\}$ is contained in some subloop K of order 8 in L. Since $K/\langle z\rangle$ is a subloop of order 4 in $L/\langle z\rangle$, the configuration $\mathcal{P}$ projects onto a single block of $\mathcal{B}'$. It follows from Theorem 2.4 that the number of Pasch configurations of type 1 is exactly determined by the order of $(V, \mathcal{B})$ and can be counted as 7 times the number of sub-STS(7)s containing z. These sub-STS(7)s are generated by z and any two points $x, y \in V \setminus \{z\}$, such that $\{x, y, z\} \notin \mathcal{B}$. The number of ways to choose such x and y is $(v-1)(v-3)$, but this way each sub-STS(7) is counted 24 times. Thus there are $7(v-1)(v-3)/24$ Pasch configurations of type 1 in $\mathcal{B}$.

The Pasch configurations of type 2 can be partitioned into p classes, each consisting of eight distinct Pasch configurations. All of the Pasch configurations in a given class project onto one Pasch configuration in $\mathcal{B}'$ and no two configurations from different classes project onto the same one. Thus the number of Pasch configurations in $\mathcal{B}'$ is at least p. □

Note that in the preceding proof there may indeed be more than p Pasch configurations in $\mathcal{B}'$. The simplest example of this can be seen by taking $(V, \mathcal{B})$ to be the STS(15) with 73 Pasch configurations and centre of order 2, i.e. System # 2 in [3]. Then $(V', \mathcal{B}')$ is an STS(7) with 7 Pasch configurations, yet $p = 3$. This demonstrates that a Pasch configuration in $\mathcal{B}'$ may also arise from the projection of a Pasch-free subset of $\mathcal{B}$ of the form $\{\{a, b, c\}, \{a, d, f\}, \{b, f, g\}, \{c, d, gz\}\}$.

Proposition 3.8. *Let L be the Steiner loop of a maxi-Pasch* STS(v).

- *For any $z \in Z(L)$ the factor loop $L/\langle z\rangle$ corresponds to a maxi-Pasch* STS.
- *If L has nontrivial centre, then*

$$P(v) = \frac{7(v-1)(v-3)}{24} + 8P\Big(\frac{1}{2}(v-1)\Big).$$

Proof: Let $(V, \mathcal{B})$ be the maxi-Pasch STS of order $v = 2u + 1$ corresponding to the Steiner loop L and let $(V', \mathcal{B}')$ be the STS(u) corresponding to $L/\langle z\rangle$, where $z \in Z(L) \setminus \{e\}$. Then by Corollary 3.4 and Theorem 3.7

$$\frac{7(v-1)(v-3)}{24} + 8P(u) \leq P(v) = P(\mathcal{B}) \leq \frac{7(v-1)(v-3)}{24} + 8P(\mathcal{B}').$$

Thus $P(u) \leq P(\mathcal{B}')$ and by maximality of $P(u)$ we have $P(u) = P(\mathcal{B}')$, which proves the first part of the proposition. The second part can be seen by substituting $P(\mathcal{B}')$ with $P(u)$ in the inequality. □

Applying the first part of the previous proposition iteratively until reaching a loop with trivial centre yields the following result.

Corollary 3.9. *Let L be a Steiner loop of a maxi-Pasch* STS*. Then $L/Z(L)$ corresponds to a maxi-Pasch* STS.

4. Concluding remarks

Call a Steiner loop *maxi-central* if its centre is of maximum possible order as given by Theorem 2.7. The property of a Steiner loop being maxi-central is not sufficient for the corresponding STS to be maxi-Pasch. The smallest Steiner loops for which this can be observed are those of order 22. These are all maxi-central, because by Theorem 2.7 they all have trivial centre. However, the number of Pasch configurations in STS(21)s varies. For example, there exists an anti-Pasch STS(21) and there also exists an STS(21) with 117 Pasch configurations, see [12].

The present paper does not improve the known lower bounds on $P(v)$, but shows that all known maxi-Pasch STSs have a maxi-central Steiner loop. For some values of v the maximum known lower bound on $P(v)$ is attained by a maxi-central Steiner triple system. These would most notably be the cases $v = 27$, 39, 43, 51 and 55 in [12]. For example, the STS(27) in [12] with 286 Pasch configurations is obtained by taking an STS(13) with 13 Pasch configurations and applying the standard $v \to 2v+1$ construction, which is equivalent to the doubling construction in Lemma 2.2. Thus the corresponding Steiner loop of order 28 has centre of order 2, which is the maximum possible.

This brings us to the conjecture that if an STS is maxi-Pasch, then its Steiner loop is maxi-central. Nevertheless, even proving a weaker statement that for every $v \equiv 1 \text{ or } 3 \pmod 6$ there exists a maxi-Pasch STS(v) whose Steiner loop is maxi-central, would be of tremendous value. It follows from Proposition 3.8 that if this statement were true, then applying the doubling construction to a maxi-Pasch STS would produce an STS which is also maxi-Pasch. Thus by Proposition 2.3 it would suffice to solve the maxi-Pasch problem for STS(v) such that $v \equiv 1$ or $9 \pmod{12}$.

Determining the number of occurrences of various configurations in an STS(v) has been a significant area of investigation. In particular [4] gives the formulas for all five-line configurations in terms of v and in terms of the number of occurrences of the Pasch configuration and the so called *mitre configuration.* The latter being any configuration of the form $\{a, b, c\}$, $\{a, d, e\}$, $\{a, f, g\}$, $\{b, d, f\}$, $\{c, e, g\}$. This problem has been further explored in [2] for l-line configurations in general, where the minimum and maximum counts of each configuration are also examined. Just like the Pasch configuration has its counterpart in the associative identity in

Steiner loops, other configurations may have interesting algebraic counterparts of their own. The present paper warrants further research into Steiner loops satisfying such identities as these may provide new results about the maximality of the corresponding configurations in Steiner triple systems.

References

[1] Bruck R. H., *A Survey of Binary Systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, 20, Reihe: Gruppentheorie, Springer, Berlin, 1971.

[2] Colbourn C. J., *The configuration polytope of l-line configurations in Steiner triple systems*, Math. Slovaca **59** (2009), no. 1, 77–108.

[3] Colbourn C. J., Rosa A., *Triple Systems*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1999.

[4] Danziger P., Mendelsohn E., Grannell M. J., Griggs T. S., *Five-line configurations in Steiner triple systems*, Utilitas Math. **49** (1996), 153–159.

[5] Di Paola J. W., *When is a totally symmetric loop a group?*, Amer. Math. Monthly **76** (1969), 249–252.

[6] Donovan D., *The centre of a sloop*, Combinatorial Mathematics and Combinatorial Computing, Australas. J. Combin. **1** (1990), 83–89.

[7] Donovan D., Rahilly A., *The central spectrum of the order of a Steiner loop*, Southeast Asian Bull. Math. **16** (1992), no. 2, 115–121.

[8] Drápal A., *On quasigroups rich in associative triples*, Discrete Math. **44** (1983), no. 3, 251–265.

[9] Grannell M. J., Griggs T. S., Mendelsohn E., *A small basis for four-line configurations in Steiner triple systems*, J. Combin. Des. **3** (1995), no. 1, 51–59.

[10] Grannell M. J., Griggs T. S., Whitehead C. A., *The resolution of the anti-Pasch conjecture*, J. Combin. Des. **8** (2000), no. 4, 300–309.

[11] Grannell M. J., Lovegrove G. J., *Maximizing the number of Pasch configurations in a Steiner triple system*, Bull. Inst. Combin. Appl. **69** (2013), 23–35.

[12] Gray B. D., Ramsay C., *On the number of Pasch configurations in a Steiner triple system*, Bull. Inst. Combin. Appl. **24** (1998), 105–112.

[13] Kaski P., Östergård P. R. J., *The Steiner triple systems of order 19*, Math. Comp. **73** (2004), no. 248, 2075–2092.

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

[15] Ling A. C. H., Colbourn C. J., Grannell M. J., Griggs T. S., *Construction techniques for anti-Pasch Steiner triple systems*, J. London Math. Soc. (2) **61** (2000), no. 3, 641–657.

[16] McCune W., *Mace4 Reference Manual and Guide*, Tech. Memo ANL/MCS-TM-264, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, 2003.

[17] Stinson D. R., Wei Y. J., *Some results on quadrilaterals in Steiner triple systems*, Discrete Math. **105** (1992), no. 1–3, 207–219.

A. R. Kozlik:

Department of Algebra, Charles University, Sokolovská 83,
186 75 Praha 8, Czech Republic

E-mail: andrew.kozlik@gmail.com

(*Received* February 2, 2020, *revised* May 7, 2020)