AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **63(1)** (2015), Pages 170–181

Steiner loops satisfying Moufang's theorem

Charles J. Colbourn

School of CIDSE, Arizona State University
Tempe, AZ 85287
U.S.A.
colbourn@asu.edu

Maria De Lourdes Merlini Giuliani

Universidade Federal do ABC, Rua Santa Adlia
166 Santo André SP 09210-170
Brazil
lourdinha.gil@gmail.com

Alexander Rosa

Mathematics and Statistics
McMaster University, Hamilton, ON
Canada
rosa@mcmaster.ca

Izabella Stuhl*

University of São Paulo
05508-090 São Paulo, SP
Brazil
izabella@ime.usp.br

Abstract

A loop satisfies Moufang's theorem whenever the subloop generated by three associating elements is a group. Moufang loops (loops that satisfy the Moufang identities) satisfy Moufang's theorem, but it is possible for a loop that is not Moufang to nevertheless satisfy Moufang's theorem. Steiner loops that are not Moufang loops are known to arise from Steiner triple systems in which some triangle does not generate a subsystem of order 7, while Steiner loops that do not satisfy Moufang's theorem are shown to arise from Steiner triple systems in which some quadrilateral

* Also at University of Debrecen, H-4010 Debrecen, Hungary.

(Pasch configuration) does not generate a subsystem of order 7. Consequently, the spectra of values of v for which a Steiner loop exists are determined when the loop is also Moufang; when the loop is not Moufang yet satisfies Moufang's theorem; and when the loop does not satisfy Moufang's theorem. Furthermore, examples are given of non-commutative loops that satisfy Moufang's theorem yet are not Moufang loops.

1 Introduction

Let V be a finite set, and $\oplus$ be a binary operation $\oplus : V \times V \mapsto V$. When for every $a, b \in V$ there exists a unique x for which $a \oplus x = b$ and a unique y for which $y \oplus a = b$, $(V, \oplus)$ is a *quasigroup*. When there is an element $e \in V$ for which $e \oplus x = x = x \oplus e$ for all $x \in V$, $(V, \oplus)$ is a *loop* and e is its *identity element*. If the binary operation $\oplus$ satisfies the *associative property* $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ for all $x, y, z \in V$, the loop is a *group*. The operation $\oplus$ is *commutative* if $x \oplus y = y \oplus x$ for all $x, y \in V$. A *subloop* of loop $(V, \oplus)$ is a loop $(W, \oplus)$ with $W \subseteq V$. The *subloop generated by* $Y \subseteq V$ is the smallest subloop $(W, \oplus)$ for which $Y \subseteq W$. See [20] for related background.

A *Moufang identity* is any one of the identities $z \oplus (x \oplus (z \oplus y)) = ((z \oplus x) \oplus z) \oplus y$, $x \oplus (z \oplus (y \oplus z)) = ((x \oplus z) \oplus y) \oplus z$, $(z \oplus x) \oplus (y \oplus z) = (z \oplus (x \oplus y)) \oplus z$, or $(z \oplus x) \oplus (y \oplus z) = z \oplus ((x \oplus y) \oplus z)$. These are equivalent for loops [3, 12]. When a loop has the property that the Moufang identities hold for every choice of x, y, z, it is a *Moufang loop*. In 1935, Moufang [19] showed that in a Moufang loop, whenever three elements satisfy associativity $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, the subloop generated by $\{x, y, z\}$ is a group. Are there other loops for which the same conclusion holds? This is related closely to a question posed by Andrew Rajah at the *Loops'11* conference: "Is every variety that satisfies Moufang's theorem contained in the variety of Moufang loops?"

A loop *satisfies Moufang's theorem* if, for every three elements for which $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, the subloop generated by $\{x, y, z\}$ is a group. In this paper, we examine a large class of commutative loops, the Steiner loops, to establish that many non-Moufang loops nevertheless satisfy Moufang's theorem. A loop is *ruthless* if it is a Steiner loop, it is not a Moufang loop, and it satisfies Moufang's theorem. (In [8], a loop is said to *have Moufang's property* $\mathcal{MP}$ if it satisfies Moufang's theorem but is not a Moufang loop; hence ruthless loops are Steiner loops that have property $\mathcal{MP}$.)

Let V be a finite set, and $\mathcal{B}$ be a set of subsets of V each of cardinality three (*triples*), so that every subset of V of cardinality two is a subset of exactly one of the triples in $\mathcal{B}$. Then $(V, \mathcal{B})$ is a *Steiner triple system* of *order* v, denoted STS(v). See [7] for extensive background on triple systems. Existence of STSs was settled in 1847 by Kirkman [17], who showed that an STS(v) exists if and only if $v \equiv 1, 3 \pmod 6$. A *configuration* in an STS(v) $(V, \mathcal{B})$ is a pair $(W, \mathcal{D})$ with $W \subseteq V$, $\mathcal{D} \subseteq \mathcal{B}$, and $B \subseteq W$ whenever $B \in \mathcal{D}$. Configuration $(W, \mathcal{D})$ is a

- *subdesign* or sub-STS($|W|$) if it is a Steiner triple system of order $|W|$;

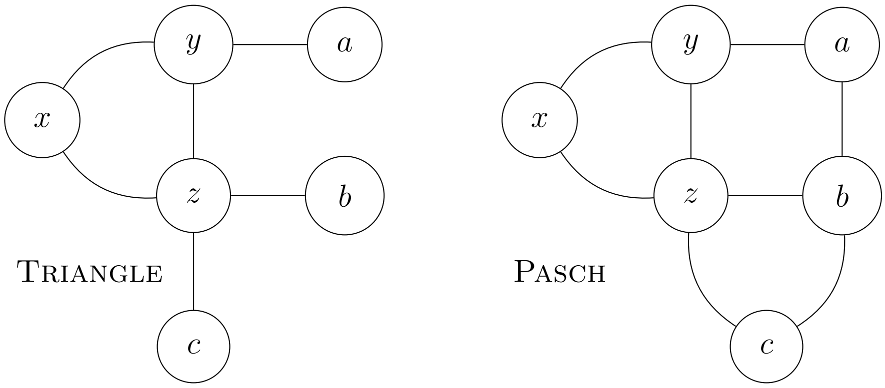
- *triangle configuration* if $\mathcal{D}$ is isomorphic to

$$\{\{x, y, a\}, \{x, z, b\}, \{y, z, c\}\};$$

- *Pasch configuration* or *quadrilateral* if $\mathcal{D}$ is isomorphic to

$$\{\{x, y, a\}, \{x, z, b\}, \{y, z, c\}, \{a, b, c\}\}.$$

The smallest subdesign that contains all triples in $\mathcal{D} \subseteq \mathcal{B}$ is the *subdesign generated by $\mathcal{D}$*.



Every STS(v) with $v > 3$ contains triangles. The situation is different for quadrilaterals and subsystems:

Theorem 1.1 [10] *For every $v \equiv 1, 3 \pmod 6$, there exists a (subsystem-free) STS(v) having no sub-STS(w) for any $3 < w < v$.*

Theorem 1.2 [13, 18] *For every $v \equiv 1, 3 \pmod 6$, there exists a (quadrilateral-free or anti-Pasch) STS(v) containing no quadrilateral except when $v \in \{7, 13\}$.*

From an STS(v), we can form a *Steiner loop* on $V \cup \{e\}$ with binary operation $\oplus$, so that whenever $\{x, y, z\} \in \mathcal{B}$, we have $x \oplus y = z$, $y \oplus x = z$, $x \oplus z = y$, $z \oplus x = y$, $y \oplus z = x$, and $z \oplus y = x$; and for every $x \in V \cup \{e\}$ we have $x \oplus x = e$, $x \oplus e = x$, and $e \oplus x = x$. A Steiner loop is commutative.

One particular class of Steiner triple systems plays an important role. Treat the $2^n - 1$ nonzero binary vectors of length n as elements, and form a triple containing three such vectors whenever their vector sum is the zero vector. The Steiner triple system that results is the *projective triple system*, and its Steiner loop is the *boolean loop*. Boolean loops are precisely the Steiner loops that are also groups [9]. The characterization of loops that are both Steiner and Moufang is in [3, Lemma 3.2]; see also [16].

Theorem 1.3 *A Steiner loop is a Moufang loop if and only if it is a boolean loop.*

In the vernacular of Steiner triple systems, a Steiner loop is a Moufang loop if and only if in its associated Steiner triple system every triangle appears in a Pasch configuration, or equivalently every triangle generates a sub-STS(7). That is, it is projective [6, 22].

We examine when Steiner loops satisfy Moufang's theorem, and prove:

Theorem 1.4 *A Steiner loop satisfies Moufang's theorem if and only if its corresponding Steiner triple system has the property that every Pasch configuration generates a sub-STS(7).*

As a consequence, we determine existence spectra for various classes of Steiner loops:

Theorem 1.5 *There is a Steiner loop of order v that*

1. *is a Moufang loop if and only if $v = 2^n$ and $n \geq 0$;*
2. *is ruthless if and only if $v \equiv 2, 4 \pmod 6$, $v \geq 10$, and $v \neq 14$;*
3. *does not satisfy Moufang's theorem if and only if $v \equiv 2, 4 \pmod 6$ and $v \geq 14$.*

An STS(v) is *ruthless* when its loop is ruthless. In [8], ruthless loops of order $3n + 1$ are given when n is odd and $n \not\equiv 0 \pmod 7$. Theorem 1.4 subsumes this result as follows. Bose [1] gives a construction for STS($3n$) when n is odd; Brouwer [2] and Doyen [11] establish that this system is anti-Pasch precisely when $n \not\equiv 0 \pmod 7$. Many explicit constructions for anti-Pasch STS(v)s are known [7], and each yields a class of ruthless loops (by Theorem 1.4). Of particular interest, the Hall triple systems first defined in [14] provide examples of anti-Pasch STSs with many subsystems, because every three distinct elements generate a subsystem of order 3 or 9; see also [5, 21]. The multiplication groups of the corresponding *Hall loops* are determined in [23].

Naturally no anti-Pasch STS can have a projective subsystem. However, in Section 4 we establish that ruthless STS(v)s exist that have nontrivial projective subsystems; to do this, we prove that three recursive constructions for ruthless STS(v)s either preserve or introduce nontrivial projective subsystems.

In the sequel, we write the binary operation as juxtaposition rather than writing $\oplus$.

2 Steiner loops that satisfy Moufang's theorem

We prove two easy lemmas to begin.

Lemma 2.1 *Let $(V, \mathcal{B})$ be an STS(v), and let e be the identity element of its Steiner loop. For every $S \subseteq V \cup \{e\}$, the following statements are equivalent:*

1. *S generates a subgroup of order 1, 2, or 4 in the Steiner loop.*

2. *There exists a* $B \in \mathcal{B}$ *for which* $S \setminus \{e\} \subseteq B$.

Proof When $S \setminus \{e\} \subseteq B = \{x, y, z\} \in \mathcal{B}$, $\{x, y, z, e\}$ generates a boolean subloop of order 4, in which every subloop is a group. In the other direction, if there is no block $B \in \mathcal{B}$ with $S \setminus \{e\} \subseteq B$, then choose $\{x, y, z\} \subseteq S$ so that $\{x, y, z\}$ is not a block (i.e., they are not collinear). The subloop generated contains (at least) the five elements $\{e, x, y, z, xy\}$, which are distinct. So the subloop generated has order greater than 4. ■

Lemma 2.2 *Let* $(V, \mathcal{B})$ *be an STS*(v)*, and let* e *be the identity element of its Steiner loop. For every* $x, y, c \in V$ *that are not collinear, the following statements are equivalent:*

1. x, y, c *satisfy the associativity* $x(yc) = (xy)c$.

2. x, y, c *form a Pasch configuration in the STS in which* $\{x, y\}$ *and* $\{y, c\}$ *appear in blocks but* $\{x, c\}$ *does not.*

Proof Suppose that $x(yc) = (xy)c$. Write $yc = z$, $xy = a$, and $xz = ac = b$. Then the blocks $\{x, y, a\}$, $\{x, z, b\}$, $\{y, z, c\}$, and $\{a, b, c\}$ form a Pasch configuration with no block containing $\{x, c\}$. The converse is immediate. ■

Proof of Theorem 1.4. For the necessity, consider a Steiner loop for Steiner triple system $(V, \mathcal{B})$ that satisfies Moufang's theorem. Select elements $\{x, y, c\} \subseteq V \cup \{e\}$ for which $x(yc) = (xy)c$ with x, y, c non-collinear. Consider the subgroup generated by $\{x, y, c\}$, and suppose it has element set W. Using Lemma 2.2, because the Pasch configuration with triples $\{x, y, a\}$, $\{x, z, b\}$, $\{y, z, c\}$, and $\{a, b, c\}$ is present, $\{e, x, y, z, a, b, c\} \subseteq W$. Then because the subloop on W forms a group, $x(yz) = xc = d = az = (xy)z$ so $\{x, c, d\}$ and $\{z, a, d\}$ are triples. By the same token, $x(zy) = xc = d = by = (xz)y$ so $\{y, b, d\}$ is a triple. These seven triples form a sub-STS(7).

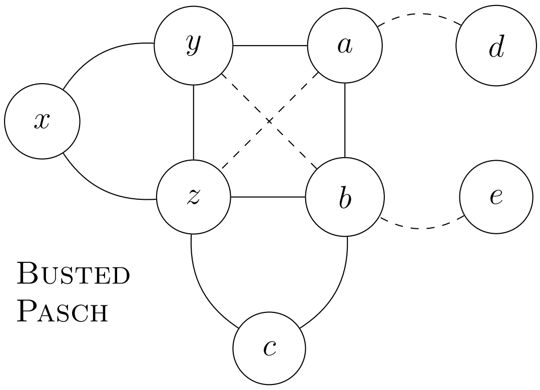
For sufficiency, suppose that every Pasch configuration generates a sub-STS(7). Consider elements $\{x, y, c\} \subseteq V \cup \{e\}$. By Lemma 2.1 the conclusion holds when they are collinear. By Lemma 2.2, if $\{x, y, c\}$ are non-collinear and do not appear in a Pasch configuration, they do not associate in the loop. When Pasch configurations are present, each generates a sub-STS(7), corresponding to a boolean subloop (a subgroup) of order 8. ■

3 Steiner loops: Moufang, ruthless, and neither

Proof of Theorem 1.5. The first statement follows from Theorem 1.3 and the definition of projective triple systems.

Now we treat the second statement. When $v \equiv 2, 4 \pmod 6$, $v \geq 10$, and $v \neq 14$, apply Theorems 1.3, 1.4, and 1.2. That $v \neq 8$ follows from the observation that the unique STS(7) is projective, so its loop is Moufang. That $v \neq 14$ follows from the fact that both STS(13)s contain Pasch configurations but do not contain a sub-STS(7).

Finally we treat the third statement. When $v \leq 8$, the only Steiner triple systems are projective. The unique STS(9) has a loop that satisfies Moufang's theorem. The two nonisomorphic STS(13)s contain Pasch configurations but no subsystem of order 7, so their loops do not satisfy Moufang's theorem. Now consider the 6-line 8-element configuration



BUSTED PASCH

The Pasch configuration in solid lines cannot generate an STS(7) if the two dashed lines of the configuration are also present. Applying known embedding results for partial Steiner triple systems [4], there exists an STS($v-1$) for every $v-1 \geq 19$ that contains this configuration, and hence the STS does not satisfy Moufang's theorem. It remains to treat $v = 16$. Among the 80 STS(15)s, 23 have sub-STS(7)s and only one is anti-Pasch [7], so the remaining ones all provide Steiner loops of order 16 that do not satisfy Moufang's theorem. ■

4 Systems with Pasch configurations

The proof of Theorem 1.5(2) as it stands leaves an important question unanswered: Can ruthless STSs contain Pasch configurations? According to Theorem 1.4, a loop is ruthless exactly when every Pasch configuration in its associated STS generates a sub-STS(7). This permits a ruthless STS to contain subsystems that are projective, those that are not, or indeed a combination of the two.

The *(special)* $v \to 2v+1$ *construction*, essentially due to Kirkman [17], is as follows. Let $(V, \mathcal{B})$ be an STS(v). Form an STS($2v+1$), $(W = (V \times \{0,1\}) \cup \{\infty\}, \mathcal{D})$, where $\mathcal{D}$ consists of the triples

- $\{\{(x,i),(y,j),(z,k)\} : \{x,y,z\} \in \mathcal{B}, i,j,k \in \{0,1\}, i+j+k \equiv 0 \bmod 2\}$, and
- $\{\{\infty,(x,0),(x,1)\} : x \in V\}$.

When $(V, \mathcal{B})$ is projective, $(W, \mathcal{D})$ is also projective.

Theorem 4.1 *When $(V, \mathcal{B})$ is a ruthless STS(v), and $(W, \mathcal{D})$ is the STS($2v+1$) obtained by the special $v \to 2v+1$ construction, $(W, \mathcal{D})$ is ruthless.*

Proof Any Pasch configuration in $(W, \mathcal{D})$ that contains ∞ must contain two triples $\{\infty, (x, 0), (x, 1)\}$, $\{\infty, (y, 0), (y, 1)\}$ for some $x, y \in V$. The remaining two triples must be of the form $\{(x, i), (y, j), (z, i + j \bmod 2)\}$ and $\{(x, 1 - i), (y, 1 - j), (z, i + j \bmod 2)\}$, so that $B = \{x, y, z\} \in \mathcal{B}$. Then $(B \times \{0, 1\}) \cup \{\infty\}$ supports a sub-STS(7) by construction.

So consider a Pasch configuration in $(W, \mathcal{D})$ that does not contain ∞. Suppose that its elements are $\{(x_j, i_j) : 1 \leq j \leq 6\}$, and its triples are

$$\{\{(x_1, i_1), (x_3, i_3), (x_5, i_5)\}, \{(x_1, i_1), (x_4, i_4), (x_6, i_6)\},$$
$$\{(x_2, i_2), (x_3, i_3), (x_6, i_6)\}, \{(x_2, i_2), (x_4, i_4), (x_5, i_5)\}\}.$$

Because ∞ is not one of the points, $\{x_1, x_2\}$, $\{x_3, x_4\}$, and $\{x_5, x_6\}$ are disjoint sets. If it is not the case that all six are distinct, without loss of generality $x_1 = x_2$. Then the structure of the triples requires that $x_3 = x_4$ and $x_5 = x_6$, and that $B = \{x_1, x_3, x_5\} \in \mathcal{B}$. Then $(B \times \{0, 1\}) \cup \{\infty\}$ supports a sub-STS(7) by construction.

If elements $\{x_j : 1 \leq j \leq 6\}$ are all distinct, then they form a Pasch configuration in $(V, \mathcal{B})$. Because this generates a (projective) sub-STS(7) $(V', \mathcal{B}')$ of $(V, \mathcal{B})$, the elements of the Pasch chosen all lie in a projective sub-STS(15) of $(W, \mathcal{D})$ on $(V' \times \{0, 1\}) \cup \{\infty\}$; hence the Pasch generates a sub-STS(7). ■

When the STS(v) contains a sub-STS(w), the STS($2v + 1$) contains a sub-STS($2w+1$). Thus the STS($2v+1$) always contains a sub-STS(7). Iterating Theorem 4.1 n times starting with a ruthless STS(v), one obtains a ruthless STS($2^n(v+1)-1$) that contains a sub-STS($2^{n+2} - 1$). The subsystem is projective here, but the system is not.

We also develop a tripling construction.

Theorem 4.2 *If an STS(v) that satisfies Moufang's theorem exists, then a ruthless STS($3v$) exists. The STS($3v$) contains a Pasch configuration exactly when an STS(v) that satisfies Moufang's theorem does.*

Proof For $i \in \{0, 1, 2\}$, let $(V, \mathcal{B}_i)$ be an STS(v) that satisfies Moufang's theorem (it is ruthless or projective). Let L be a $v \times v$ Latin square having no 2×2 subsquare, which exists by [15]. Index its rows, columns, and symbols by the elements of V. Form an STS($3v$) on $V \times \{0, 1, 2\}$ by including the *inside* triples $\{\{x_i, y_i, z_i\} : \{x, y, z\} \in \mathcal{B}_i, i \in \{0, 1, 2\}\}$ and the *transverse* triples $\{\{a_0, b_1, c_2\} : a, b \in V, L(a, b) = c\}$. Consider a Pasch configuration in the STS($3v$). Either it consists of four inside triples or of four transverse triples. In the latter case, a Pasch configuration arises only when the four triples correspond to a 2×2 subsquare in L, which does not occur. In the former, because each STS(v) is ruthless or projective, the Pasch configuration generates a sub-STS(7) as required. The STS($3v$) is always ruthless, never projective. ■

A more involved "$3v - 2$" construction also applies.

Theorem 4.3 *If an STS(v) that satisfies Moufang's theorem exists and $v \notin \{3, 9\}$, then a ruthless STS($3v - 2$) exists. The STS($3v - 2$) always contains a Pasch configuration.*

Proof Let $n = (v-1)/2$ and H be a latin square with no 2×2 subsquare and with rows, columns, and symbols indexed by an n-set X, which exists because $n \notin \{1, 2, 4\}$ [15]. Let L be a $(v-1)\times(v-1)$ latin square with rows, columns, and symbols indexed by $X \times \{0, 1\}$ so that $L((x, i), (y, j)) = (H(x, y), i + j \bmod 2)$ whenever $x, y \in X$ and $i, j \in \{0, 1\}$. Let $V = (X \times \{0, 1\}) \cup \{\infty\}$ and $(V, \mathcal{B})$ be an STS(v) satisfying Moufang's theorem that contains $\{\{\infty, (x, 0), (x, 1)\} : x \in X\}$ as blocks.

Form an STS($3v-2$) on $\{\infty\} \cup (X \times \{0, 1\} \times \{0, 1, 2\})$ by including

1. $\{\{(x, i, \sigma), (y, j, \sigma), (z, \ell, \sigma)\} : \{(x, i), (y, j), (z, \ell)\} \in \mathcal{B}, \{x, y, z\} \subseteq X, \sigma \in \{0, 1, 2\}\}$ (*inside* triples),
2. $\{\{\infty, (x, 0, \sigma), (x, 1, \sigma)\} : x \in X, \sigma \in \{0, 1, 2\}\}$ (*infinite* triples), and
3. $\{\{(x, i, 0), (y, j, 1), (z, \ell, 2)\} : x, y \in X, i, j \in \{0, 1\}, L((x, i), (y, j)) = (z, \ell)\}$ (*transverse* triples).

Consider a Pasch configuration P in the STS($3v-2$). If P contains two triples from one of the sub-STS(v)s, then P lies inside a sub-STS(v) and hence generates a sub-STS(7). Other Pasch configurations must contain a transverse triple. So suppose that $\{(x, i, 0), (y, j, 1), (z, \ell, 2)\}$ is a triple of P. Exactly one other triple B of P contains $(x, i, 0)$.

B **is inside:** Without loss of generality, $B = \{(x, i, 0), (w, a, 0), (u, b, 0)\}$. Then the remaining triples of P either cover the pairs $\{(w, a, 0), (y, j, 1)\}$ and $\{(u, b, 0), (z, \ell, 2)\}$, or the pairs $\{(w, a, 0), (z, \ell, 2)\}$ and $\{(u, b, 0), (y, j, 1)\}$. Then the two triples containing these are both transverse. However, the third points in these triples must have different third coordinates, and hence P is not a Pasch configuration. Indeed by symmetry no Pasch configuration can contain both a transverse and an inside triple.

B **is infinite:** Then $B = \{\infty, (x, i, 0), (x, 1-i, 0)\}$. The remaining two triples of P either cover the pairs $\{\infty, (y, j, 1)\}$ and $\{(x, 1-i, 0), (z, \ell, 2)\}$ or the pairs $\{\infty, (z, \ell, 2)\}$ and $\{(x, 1-i, 0), (y, j, 1)\}$. For the first, the two remaining triples are $\{\infty, (y, j, 1), (y, 1-j, 1)\}$ and $\{(x, 1-i, 0), (y, 1-j, 1), (z, \ell, 2)\}$. By construction, $\{(x, 1-i, 0), (y, j, 1), (z, 1-\ell, 2)\}$ and $\{(x, i, 0), (y, 1-j, 1), (z, 1-\ell, 2)\}$ are triples of the STS($3v-2$). The triple $\{\infty, (z, \ell, 2), (z, 1-\ell, 2)\}$, which is also present, completes a sub-STS(7). The second situation is similar. Indeed by symmetry every Pasch configuration that contains a transverse and an infinite triple generates a sub-STS(7).

B **is transverse:** We may suppose that no triple of P is inside or infinite; all are transverse. If B covers pair $\{(x, i, 0), (y, 1-j, 1)\}$ or $\{(x, i, 0), (z, 1-\ell, 2)\}$, then $B = \{(x, i, 0), (y, 1-j, 1), (z, 1-\ell, 2)\}$, and P contains the two further triples $\{(x, 1-i, 0), (y, j, 1), (z, 1-\ell, 2)\}$ and $\{(x, 1-i, 0), (y, 1-j, 1), (z, \ell, 2)\}$; a sub-STS(7) is generated by P that includes three infinite triples. It remains to treat the case when $B = \{(x, i, 0), (w, a, 1), (u, b, 2)\}$ with $w \neq y$ and $u \neq z$; this requires that $H(x, y) = z$ and $H(x, w) = u$. For the remaining two transverse triples to form a Pasch configuration, suppose that the first coordinate of the final element of P is f. Then $H(f, y) = u$, and $H(f, w) = z$. This cannot happen because $u \neq z$ and H has no 2×2 subsquare.

Although the STS(v) may or may not contain sub-STS(7)s, the STS($3v - 2$) surely does. Indeed it has $((v - 1)/2)^2$ sub-STS(7)s obtained by selecting an infinite triple from two of the sub-STS(v)s. Nevertheless the STS($3v - 2$) is not projective. ■

It may be of interest to determine for which orders an STS(v) can be ruthless but have non-trivial projective subsystems (or, in other words, ruthless STSs containing Pasch configurations). It appears plausible that this occurs whenever $v \equiv 1, 3 \pmod 6$ and $v \geq 19$.

5 Loop Direct Product

We now employ a direct product of loops, which can be seen as a generalization of the special $v \to 2v + 1$ construction. Let $L_1 = (X, \oplus)$ and $L_2 = (Y, \otimes)$ be loops. The *direct product* $L_1 \times L_2$ has elements $X \times Y$ and binary operation $\times$ defined by $(x_1, y_1) \times (x_2, y_2) = (x_1 \oplus x_2, y_1 \otimes y_2)$.

Theorem 5.1 *Let $L_1 = (X, \oplus)$ and $L_2 = (Y, \otimes)$ be finite loops. Then $L_1 \times L_2$ satisfies Moufang's theorem if and only if both L_1 and L_2 satisfy Moufang's theorem.*

Proof If L_1 does not satisfy Moufang's theorem, it has three associating elements a_1, a_2, a_3 that generate a subloop S_1 that is not a group. Denoting by e_2 the identity element of L_2, $\{a_1, a_2, a_3\} \times \{e_2\}$ associate in $L_1 \times L_2$ and generate $S_1 \times \{e_2\}$, a subloop which is not a group. Hence $L_1 \times L_2$ does not satisfy Moufang's theorem. Symmetrically, if L_2 does not satisfy Moufang's theorem, neither does $L_1 \times L_2$.

Now suppose that L_1 and L_2 both satisfy Moufang's theorem. Consider three elements $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ in $L_1 \times L_2$ that associate as

$$((a_1, b_1) \times (a_2, b_2)) \times (a_3, b_3) = (a_1, b_1) \times ((a_2, b_2) \times (a_3, b_3)).$$

Then $(a_1 \oplus a_2) \oplus a_3 = a_1 \oplus (a_2 \oplus a_3)$ so the elements associate in L_1; similarly they associate in L_2. Now let S_1 be the subloop of L_1 generated by $\{a_1, a_2, a_3\}$, and let S_2 be the subloop of L_2 generated by $\{b_1, b_2, b_3\}$. The subloop of $L_1 \times L_2$ generated by $\{(a_1, b_1), (a_2, b_2), (a_3, b_3)\}$ is a subloop of $S_1 \times S_2$. Because S_1 and S_2 are groups, every subloop of $S_1 \times S_2$ is a group. So whenever three elements associate in $L_1 \times L_2$, they generate a subgroup. ■

Theorem 5.1 gives further examples of ruthless Steiner triple systems that contain projective subsystems. Perhaps more importantly, if we take L_1 to be a ruthless loop and L_2 to be a non-commutative group or Moufang loop, the direct product is not a Moufang loop, is not commutative (and hence not a Steiner loop), but nonetheless satisfies Moufang's theorem.

It may be important to observe that direct product of Steiner loops is *not* the same as direct product of Steiner triple systems. For the STS(3) with triple $\{0, 1, 2\}$ and the STS(7) with triples $\{\{i, i+1, i+3\} : i \in \mathbb{Z}_7\}$ the STS direct product (an STS(21)) contains a Pasch configuration on $\{(0, 0), (5, 0), (1, 1), (2, 1), (3, 2), (6, 2)\}$ because the STS(7) contains the triples $\{0, 1, 3\}$, $\{0, 2, 6\}$, $\{2, 3, 5\}$, and $\{1, 5, 6\}$. This Pasch configuration generates the additional elements $\{(4, 0), (4, 1), (4, 2)\}$ and hence generates a subsystem that is not projective. Hence the STS(21) is neither projective nor ruthless. Consequently any STS($3v$) obtained by the (STS) direct product of a ruthless STS(v) with a sub-STS(7) and an STS(3) cannot itself be ruthless.

6 Conclusion

Certain configurations in Steiner triple systems underlie when the corresponding Steiner loop satisfies Moufang's theorem. Indeed a rich class of Steiner loops satisfying Moufang's theorem arises from the anti-Pasch Steiner triple systems, whose existence has been studied extensively. Nevertheless, we have shown that while all Steiner loops from anti-Pasch Steiner triple systems satisfy Moufang's theorem, and hence provided one for each possible order, these classes do not coincide. Indeed ruthless Steiner triple systems can exhibit a rich structure of subsystems, both projective and non-projective.

Acknowledgments

The research of the third author was supported by NSERC Grant No. A7268. The fourth author has been supported by FAPESP Grant — process No 11/51845-5, and expresses her gratitude to IMS, University of São Paulo, Brazil, for the warm hospitality.

References

[1] R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* 9 (1939), 353–399.

[2] A. E. Brouwer, *Steiner triple systems without forbidden subconfigurations*, Mathematisch Centrum, Amsterdam, 1977. Afdeling Zuivere Wiskunde, No. ZW 104/77. [Department of Pure Mathematics, No. ZW 104/77].

[3] R. H. Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie. Springer Verlag, Berlin, 1958.

[4] D. Bryant and D. Horsley, A proof of Lindner's conjecture on embeddings of partial Steiner triple systems, *J. Combin. Des.* 17(1) (2009), 63–89.

[5] F. Buekenhout, Une caractérisation des espaces affins basée sur la notion de droite, *Math. Z.* 111 (1969), 367–371.

[6] P. J. Cameron, *Parallelisms of complete designs*, Cambridge University Press, Cambridge, 1976. London Mathematical Society Lecture Note Series, No. 23.

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

[8] M. De Lourdes Merlini Giuliani and G. Souza Dos Anjos, Steiner loops satisfying Moufang's theorem, (2013) (submitted).

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

[10] J. Doyen, Sur la structure de certains systèmes triples de Steiner, *Math. Z.* 111 (1969), 289–300.

[11] J. Doyen, Linear spaces and Steiner systems, In *Geometries and groups (Berlin, 1981)*, vol. 893 of *Lecture Notes in Math.*, pp. 30–42. Springer, Berlin, 1981.

[12] A. Drápal, A simplified proof of Moufang's theorem, *Proc. Amer. Math. Soc.* 139(1) (2011), 93–98.

[13] M. J. Grannell, T. S. Griggs and C. A. Whitehead, The resolution of the anti-Pasch conjecture, *J. Combin. Des.* 8(4) (2000), 300–309.

[14] M. Hall, Jr., Automorphisms of Steiner triple systems, *IBM J. Res. Develop.* 4 (1960), 460–472.

[15] K. Heinrich, Latin squares with and without subsquares of prescribed type, In *Latin Squares: New Developments in the Theory and Applications*, pp. 101–148. North-Holland, Amsterdam, 1991. Ann. Discrete Math. 46.

[16] M. K. Kinyon, K. Kunen and J. D. Phillips, A generalization of Moufang and Steiner loops, *Algebra Universalis* 48(1) (2002), 81–101.

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

[18] A. C. H. Ling, C. J. Colbourn, M. J. Grannell and T. S. Griggs, Construction techniques for anti-Pasch Steiner triple systems, *J. London Math. Soc. (2)* 61(3) (2000), 641–657.

[19] R. Moufang, Zur Struktur von Alternativkörpern, *Math. Ann.* 110(1) (1935), 416–430.

[20] H. O. Pflugfelder, *Quasigroups and loops: introduction*, vol. 7 of *Sigma Series in Pure Mathematics*, Heldermann Verlag, Berlin, 1990.

[21] R. Roth and D. K. Ray-Chaudhuri, Hall triple systems and commutative Moufang exponent 3 loops: the case of nilpotence class 2, *J. Combin. Theory Ser. A* 36(2) (1984), 129–162.

[22] D. R. Stinson and Y. J. Wei, Some results on quadrilaterals in Steiner triple systems, *Discrete Math.* 105(1-3) (1992), 207–219.

[23] K. Strambach and I. Stuhl, Translation groups of Steiner loops, *Discrete Math.* 309(13) (2009), 4225–4227.

(Received 1 Mar 2015)