SYLOW THEORY FOR QUASIGROUPS II: SECTIONAL ACTION

MICHAEL K. KINYON[1], JONATHAN D. H. SMITH[2],
AND PETR VOJTĚCHOVSKÝ[3]

Abstract. The first paper in this series initiated a study of Sylow theory for quasigroups and Latin squares, based on orbits of the left multiplication group. The current paper is based on so-called pseudo-orbits, which are formed by the images of a subset under the set of left translations. The two approaches agree for groups, but differ in the general case. Subsets are described as sectional if the pseudo-orbit that they generate actually partitions the quasigroup. Sectional subsets are especially well-behaved in the newly identified class of conflatable quasigroups, which provides a unified treatment of Moufang, Bol, and conjugacy-closure properties. Relationships between sectional and Lagrangean properties of subquasigroups are established. Structural implications of sectional properties in loops are investigated, and divisors of the order of a finite quasigroup are classified according to the behavior of sectional subsets and pseudo-orbits. An upper bound is given on the size of a pseudo-orbit. Various interactions of the Sylow theory with design theory are discussed. In particular, it is shown how Sylow theory yields readily computable isomorphism invariants with the resolving power to distinguish each of the 80 Steiner triple systems of order 15.

1. Introduction

This paper is part of a research program to extend Sylow theory from finite groups to finite quasigroups and Latin squares. General approaches to the extension have been both top-down and bottom-up. The top-down approach works with the Burnside order, a labeled

2010 *Mathematics Subject Classification.* 20N05, 05B07.

Key words and phrases. Latin square, quasigroup, Sylow theorem, Moufang loop, loop coset, Steiner triple system.

Work on this paper was begun while the second author enjoyed the hospitality of the Department of Mathematics, University of Denver, partially supported by the Simons Foundation under the auspices of Collaboration Grant 210176 to P. Vojtěchovský.

order structure on the set of isomorphism classes of irreducible permutation representations of a quasigroup [19, §§10–13]. The bottom-up approach, which is modeled on Wielandt's treatment of the Sylow theory for groups [22], studies the combinatorial or geometric structure of systems of subsets of a quasigroup. In a predecessor paper, the systems studied were the orbits of a given subset under the full left multiplication group of the quasigroup [19, §§5–9]. In the current paper, which again works solely with the bottom-up approach, the systems studied are the images of a subset under the set of left multiplications by elements of the quasigroup. For groups, these two versions of the bottom-up approach coincide, but they separate for general quasigroups.

If S is a subset of a quasigroup Q, then the *pseudo-orbit* generated by S is the system $\{SL(q) \mid q \in Q\}$ of images of S under the left multiplications $L(q)$ by elements q of Q (see Example 2.2). The left multiplications are the permutations represented by the rows of the Latin square forming the body of the bordered multiplication table. The images under the left multiplications are the *cosets* that appeared in [13], but here they are described as *left translates*.

A subset S is said to be *sectional* if the pseudo-orbit it generates forms a partition of Q. Note that in the finite case, a nonempty subset S is sectional if and only if the columns indexed by S in the multiplication table of Q can be partitioned into $|Q|/|S|$ pairwise disjoint Latin subsquares of order $|S|$.

In Wielandt's approach to the Sylow theory for groups, p-subgroups of a finite group Q (for a prime p) appear in the pseudo-orbits of sectional subsets of p-power order. The basic properties of pseudo-orbits and sectional subsets are studied in Section 2.

One of the primary motivations for the extension of Sylow theory to quasigroups is the insight that the extension provides into various aspects of quasigroup theory, and the way that it leads to a unification of these diverse aspects. This effect is seen clearly in Section 3, which investigates when each element of the orbit of a subset under the full left multiplication group is actually sectional. Theorem 3.7 shows that this happens within the class of (*left*) *conflatable* quasigroups Q, satisfying the property

$$\forall\, x \in Q\,,\ \exists\, \alpha_x \in Q!\,.\ \forall\, y \in Q\,,\ L(x)L(y)\alpha_x \in L(Q)$$

— compare (3.1). Conflatable quasigroups form the framework for a unified treatment of various classes of quasigroups and loops that have appeared in the literature, such as Moufang loops, Bol quasigroups, conjugacy-closed loops, and distributive quasigroups.

Section 4 investigates the relationships between the sectional and Lagrangean properties for subquasigroups. The concepts coincide for loops, but differ for general quasigroups. Sufficient conditions for sectionality are also given. Section 5 provides a classification of the divisors d of the order of a finite quasigroup, based on the behavior of the pseudo-orbits of subsets of size d. This classification is correlated with the classification from [19], which was based on the behavior of orbits under the full left multiplication group.

Theorem 6.5 provides an upper bound for the size of the pseudo-orbit of a (non-sectional) subgroup of a quasigroup, in terms of the semilattice of subgroups containing the given subgroup. This bound is sharp, for example, when applied to Klein 4-subgroups of the smallest simple, non-associative Moufang loop, the *Paige loop* $\mathsf{PSL}_{1,3}(2)$ of order 120 [17].

The concluding Sections 7 and 8 offer applications and illustrations of the current Sylow theory in design theory and loop theory respectively. In particular, §7.1 shows how Sylow theory produces readily computed invariants that are powerful enough to distinguish each of the 80 Steiner triple systems of order 15 (compare Table 4 and [6, Table II.1.28]).

Readers are referred to [18] and [20] for quasigroup-theoretic and general algebraic concepts and conventions that are not otherwise explicitly clarified here.

2. Pseudo-orbits and sectional subsets

A *quasigroup* Q is a set with a binary operation $\cdot$ such that the equation $x \cdot y = z$ has a unique solution in Q whenever two of the three elements x, y, z of Q are specified. This is equivalent to saying that the *left multiplications* $L(q)\colon Q \to Q; x \mapsto qx$ and the *right multiplications* $R(q)\colon Q \to Q; x \mapsto xq$ by each element q of Q are bijections of Q. In particular, unlabeled multiplication tables of finite quasigroups (which we will employ throughout the paper and whose rows and columns we tacitly label $1, \ldots, |Q|$) are precisely Latin squares. We also set $y\backslash x = xL(y)^{-1}$, and $x/y = xR(y)^{-1}$ for elements x, y of a quasigroup Q. Finally, a *loop* is defined as a quasigroup Q with an *identity* element $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$.

2.1. **Pseudo-orbits.**

Definition 2.1. Let S be a subset of a quasigroup Q. Then

$$\{SL(q) \mid q \in Q\}$$

is called the (*left*) *pseudo-orbit generated* by S in Q. Its elements are described as (*left*) *translates* of S in Q.

Example 2.2. Consider the quasigroup with multiplication table

1	2	3	4	5	6
2	1	4	5	6	3
3	4	5	6	1	2
4	6	2	1	3	5
5	3	6	2	4	1
6	5	1	3	2	4

The set $\big\{\{1,3\},\ \{1,6\},\ \{2,4\},\ \{3,5\},\ \{5,6\}\big\}$ is the pseudo-orbit of $\{1,3\}$.

We begin with an elementary observation.

Lemma 2.3. *Let S be a non-empty subset of a quasigroup Q. Then the pseudo-orbit generated by S is a cover of Q.*

Proof. Let s be an element of S, and let x be an element of Q. Then $x = (x/s)s$ lies in the translate $SL(x/s)$ of S. □

Note that common membership in a pseudo-orbit is not a transitive relation. More specifically, define a relation $\sim$ on subsets of a quasigroup Q by

$$S_1 \sim S_2 \quad \Leftrightarrow \quad \exists\, S \subseteq Q\,.\,\exists\, q_1, q_2 \in Q\,.\, S_1 = q_1 S \ \text{ and } \ S_2 = q_2 S\,.$$

Certainly, $\sim$ is symmetric.

Lemma 2.4. *Let Q be a quasigroup. Then the relation $\sim$ is reflexive.*

Proof. If Q is empty, the result is immediate. Otherwise, let S_1 be a subset of Q. For an element q of Q, consider $S = S_1 L(q)^{-1}$. Then $S_1 = SL(q)$, so $S_1 \sim S_1$. □

In general, $\sim$ is not a transitive relation. For instance, in the quasigroup of Example 2.2, we have $\{1,2,3\} \sim \{1,2,4\} \sim \{1,2,5\}$, but $\{1,2,3\} \nsim \{1,2,5\}$.

Recall that for a quasigroup Q, the *left multiplication group* $\mathrm{LMlt}\, Q$ of Q is the permutation group $\langle L(q) \mid q \in Q\rangle_{Q!}$ of the underlying set Q generated by the full set $\{L(q) \mid q \in Q\}$ of left multiplications by elements of Q.

Proposition 2.5. *If two subsets of a quasigroup Q are related by the transitive closure of $\sim$, then they lie in the same orbit under the left multiplication group* $\mathrm{LMlt}\, Q$.

Proof. Suppose that S and S' lie in the transitive closure of $\sim$, and are thus related by a chain of the form

$$S = S_0 \sim S_1 \sim \cdots \sim S_r = S' . \tag{2.1}$$

It will be shown by induction on r that S' lies in the $\operatorname{LMlt} Q$-orbit of S. If $r = 0$, the result is trivial. Now suppose that $S_{r-1} = S\lambda$, for some element λ of $\operatorname{LMlt} Q$. Suppose $S_{r-1} = S^*L(q_1)$ and $S_r = S^*L(q_2)$ for $q_1, q_2 \in Q$ and some subset S^* of Q. Then

$$S' = S^*L(q_2) = S_{r-1}L(q_1)^{-1}L(q_2) = S\lambda L(q_1)^{-1}L(q_2) \in S \operatorname{LMlt} Q$$

as required. □

Theorem 2.6. *Two subsets of a finite loop Q are related by the transitive closure of $\sim$ if and only if they lie in the same orbit under the left multiplication group* $\operatorname{LMlt} Q$.

Proof. Suppose that $S' = S\lambda$ for $S, S' \subseteq Q$ and $\lambda \in \operatorname{LMlt} Q$. It will be shown, by induction on the length of λ as a word over the alphabet $\{L(q) \mid q \in Q\}$, that there is a chain of the form (2.1). This is certainly true if $\lambda = 1$. For the induction step, suppose that $S'' = S\lambda L(q)$, with $S' = S\lambda$ and a chain (2.1) given by the induction hypothesis. Then $S'' = S'L(q)$ and $S' = S'L(1)$, so $S' \sim S''$, and the chain (2.1) is extended to $S \sim \cdots \sim S' \sim S''$. □

2.2. **Sectional and poly-sectional subsets.** Within a quasigroup Q, the following recursive definition specifies disjointness properties of various pseudo-orbits. Right-handed versions of the concepts in the definition may also be formulated.

Definition 2.7. Let S be a subset of a quasigroup Q.

(a) The subset S is said to be a (*left*) *sectional* or 1-*sectional* subset if the left pseudo-orbit it generates is a partition of Q. In this case, the pseudo-orbit itself is described as *partitional*.
(b) Let p be a positive integer. Then S is (*left*) $(p+1)$-*sectional* if it is sectional, and if each element of the pseudo-orbit it generates is itself p-sectional.
(c) The subset S is (*left*) *poly-sectional* if it is left p-sectional for each positive integer p.
(d) If S is left poly-sectional in Q, define the (*left*) *sectional degree* of S in Q to be infinite. Otherwise, set the left sectional degree to be the largest nonnegative integer p such that S is p-sectional in Q but not $(p+1)$-sectional. (By default, each subset of Q is 0-sectional.)

(e) The subset S is (*left*) *multi-sectional* if each element of the orbit of S under the left multiplication group $\mathrm{LMlt}\, Q$ is itself sectional.

Lemma 2.8. *Let S be a subset of a quasigroup Q. If S is multi-sectional, then it is poly-sectional.*

Proof. Let T be an element of the orbit of S under $\mathrm{LMlt}\, Q$. Then the pseudo-orbit generated by T is contained in the orbit of S under $\mathrm{LMlt}\, Q$. □

Note that singleton subsets are always multi-sectional. In finite quasigroups, the concepts of poly-sectionality and multi-sectionality coincide, and may thus be used interchangeably:

Proposition 2.9. *Let S be a subset of a finite quasigroup Q. Then S is multi-sectional if and only if it is poly-sectional.*

Proof. Lemma 2.8 provides the "only if" direction. Conversely, let S be a poly-sectional subset of a finite quasigroup Q. The finiteness of Q implies the finiteness of $\mathrm{LMlt}\, Q$. An element of the orbit of S under $\mathrm{LMlt}\, Q$ then takes the form $SL(q_1)\dots L(q_p)$ for some natural number p. Since S is poly-sectional, it follows that $SL(q_1)\dots L(q_p)$ is sectional. □

Problem 2.10. Is there a (necessarily infinite) quasigroup Q containing a poly-sectional subset that is not multi-sectional?

2.3. **Sectional degrees and Steiner loops.** We exhibit sectional sets with sectional degree 1 or 2.

First consider the quasigroup of Example 2.2. Its subset $\{1,4\}$, with pseudo-orbit $\big\{\{1,4\},\{2,5\},\{3,6\}\big\}$, is the unique sectional subset of size two. For example, $\big\{\{2,5\},\{1,4\},\{1,6\},\{3,4\},\{3,6\}\big\}$ is the pseudo-orbit of $\{2,5\}$.

Consider a quasigroup $(Q,\circ)$. Define the *ternary multiplication table* to be $T(Q)$ or

$$T(Q,\circ) = \{(q_1,q_2,q_3) \in Q^3 \mid q_1 \circ q_2 = q_3\}\,. \tag{2.2}$$

The quasigroup $(Q,\circ)$ is described as being *totally symmetric* if $T(Q)$ is invariant under the action of the symmetric group S_3 permuting the coordinates of its entries. An idempotent, totally symmetric quasigroup $(Q,\circ)$ is described as a *Steiner quasigroup*, since the underlying sets of the asymmetric triples lying in $T(Q)$ then form the blocks of a Steiner triple system on Q. Conversely, each Steiner triple system $(Q,\mathcal{B})$ yields a Steiner quasigroup with blocks of the form $\{q_1,q_2,q_1\circ q_2\}$ for $q_1 \neq q_2 \in Q$. Given a Steiner quasigroup $(Q,\circ)$, a *Steiner loop*

$(Q \dot\cup \{e\}, +)$ is obtained by adjoining an identity element e to the underlying set Q, imposing the unipotent law $q + q = e$ for each element q of Q, and $q_1 + q_2 = q_1 \circ q_2$ for distinct elements q_1, q_2 of Q [7, p.65], [18, §1.5–6]. Note that for $i = 1, 2$, Steiner triple systems $(Q_i, \mathcal{B}_i)$ are isomorphic if and only if the corresponding Steiner quasigroups $(Q_i, \circ)$ or Steiner loops $(Q_i \dot\cup \{e\}, +)$ are isomorphic.

Consider the 80 Steiner triple systems of order 15 [6, Table II.1.28]. Four of the Steiner triple systems are actually Kirkman triple systems. The corresponding 15-element Steiner quasigroups themselves are analyzed later in §7.1. For now, it suffices to remark that within all of the Steiner quasigroups of order 15, there are no proper, non-trivial sectional subsets whatsoever.

Among the 80 Steiner loops of order 16, there are loops Q (Kirkman or non-Kirkman as desired) that contain a 2-element subset S with sectional degree 2. For instance, consider the Steiner loop whose (unlabeled) multiplication table is given by the Latin square of Table 1. The underlying Steiner triple system is identified as number 4 in [6, Table II.1.28]. In the `LOOPS` package [15] for `GAP` [10], the corresponding unipotent loop is identified as `SteinerLoop(16,4)`. Then the subset $\{5, 7\}$ is 2-sectional, but not 3-sectional. More general problems are as follows.

Problem 2.11. For each integer $p > 2$, construct a finite quasigroup Q with a subset S such that the left sectional degree of S in Q is p.

Problem 2.12. For given extended natural numbers $p, q \in \mathbb{N} \cup \{\infty\}$, when is it possible to find a subset S of a finite quasigroup Q such that the left sectional degree of S in Q is p and the right sectional degree of S in Q is q?

2.4. **Right nuclear subsets.** Recall that the (possibly empty) subset

$$\{s \in Q \mid \forall\ x, y \in Q\,,\ x(ys) = (xy)s\}$$

of a quasigroup Q is known as the *right nucleus* of Q.

Proposition 2.13. *Let S be a left sectional subset of a finite quasigroup Q. Suppose that S is a subset of the right nucleus of Q. Then S is left multi-sectional.*

Proof. Induction on n yields

$$sL(q_1)L(q_2)\dots L(q_n) = sL\big(q_1 L(q_2)\dots L(q_n)\big) \tag{2.3}$$

for every $q_1, \dots, q_n \in Q$ and $s \in S$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	4	1	2	7	8	5	6	11	12	9	10	15	16	13	14
4	3	2	1	8	7	6	5	12	11	10	9	16	15	14	13
5	6	7	8	1	2	3	4	13	14	15	16	9	10	11	12
6	5	8	7	2	1	4	3	15	13	16	14	10	12	9	11
7	8	5	6	3	4	1	2	16	15	14	13	12	11	10	9
8	7	6	5	4	3	2	1	14	16	13	15	11	9	12	10
9	10	11	12	13	15	16	14	1	2	3	4	5	8	6	7
10	9	12	11	14	13	15	16	2	1	4	3	6	5	7	8
11	12	9	10	15	16	14	13	3	4	1	2	8	7	5	6
12	11	10	9	16	14	13	15	4	3	2	1	7	6	8	5
13	14	15	16	9	10	12	11	5	6	8	7	1	2	3	4
14	13	16	15	10	12	11	9	8	5	7	6	2	1	4	3
15	16	13	14	11	9	10	12	6	7	5	8	3	4	1	2
16	15	14	13	12	11	9	10	7	8	6	5	4	3	2	1

TABLE 1. Multiplication table of `SteinerLoop(16,4)`

Consider an element $\lambda = L(q_1)L(q_2)\dots L(q_n)$ of $\operatorname{LMlt} Q$, and the corresponding element $S\lambda$ of the orbit of S under $\operatorname{LMlt} Q$. Suppose that there are elements x and y of Q such that $x(S\lambda)$ and $y(S\lambda)$ intersect non-trivially, say $x(s_1\lambda) = y(s_2\lambda)$ for certain elements s_1 and s_2 of S.

Set $u = q_1L(q_2)\dots L(q_n)L(x)$ and $v = q_1L(q_2)\dots L(q_n)L(y)$. For each element s of S, the equation (2.3) yields

$$\begin{aligned} sL(u) &= sL\big(q_1L(q_2)\dots L(q_n)L(x)\big) \\ &= sL(q_1)L(q_2)\dots L(q_n)L(x) = x(s\lambda)\,, \end{aligned}$$

and similarly $sL(v) = y(s\lambda)$. In particular, $x(S\lambda) = uS$ and $y(S\lambda) = vS$, along with $s_1L(u) = x(s_1\lambda) = y(s_2\lambda) = s_2L(v)$. By the latter equation, uS and vS intersect. Since S is sectional, $uS = vS$. Thus $x(S\lambda) = y(S\lambda)$. It follows that $S\lambda$ is itself sectional, as required. □

Proposition 2.14. *Let S be a left sectional subset of a loop Q. Suppose that S is a subset of the right nucleus of Q. Then S is left multi-sectional.*

Proof. For x, $y \in Q$ and $s \in S$, we have

$$x\backslash(ys) = (x\backslash y)s \quad \text{and in particular} \quad x\backslash s = (x\backslash 1)s \tag{2.4}$$

since $x[x\backslash(ys)] = ys = [x(x\backslash y)]s = x[(x\backslash y)s]$. Using (2.3) and (2.4), induction on n shows that

$$sL(q_1)^{\varepsilon_1} \dots L(q_n)^{\varepsilon_n} = sL\big(1L(q_1)^{\varepsilon_1} \dots L(q_n)^{\varepsilon_n}\big) \tag{2.5}$$

for all $q_1, \dots, q_n \in Q$, $s \in S$ and $\varepsilon \in \{1, -1\}$.

We can now mimic the proof of Proposition 2.13. Consider $\lambda = L(q_1)^{\varepsilon_1} \dots L(q_n)^{\varepsilon_n} \in \operatorname{LMlt} Q$, and suppose that $x(s_1\lambda) = y(s_2\lambda)$ for some x, $y \in Q$ and s_1, $s_2 \in S$. Set $u = 1L(q_1)^{\varepsilon_1} \dots L(q_n)^{\varepsilon_n} L(x)$ and $v = 1L(q_1)^{\varepsilon_1} \dots L(q_n)^{\varepsilon_n} L(y)$. For each $s \in S$, (2.5) yields

$$\begin{aligned} sL(u) &= sL\big(1L(q_1)^{\varepsilon_1} \dots L(q_n)^{\varepsilon_n} L(x)\big) \\ &= sL(q_1)^{\varepsilon_1} \dots L(q_n)^{\varepsilon_n} L(x) = x(s\lambda)\,, \end{aligned}$$

and similarly $sL(v) = y(s\lambda)$. The remainder of the proof follows as for Proposition 2.13. □

Problem 2.15. Does Proposition 2.13 extend to infinite quasigroups?

2.5. **Non-overlapping orbits.** This brief paragraph relates the topics of the current section with the concepts of overlapping and non-overlapping orbits introduced earlier [19, §5]. Recall that in a finite quasigroup Q, the orbit of a subset S under the left multiplication group $\operatorname{LMlt} Q$ is said to be *overlapping* if it contains distinct elements that are not disjoint, and otherwise is described as *non-overlapping*.

Lemma 2.16. *Let Q be a finite quasigroup. Suppose that S is a subset of Q which lies in a non-overlapping orbit. Then S is a multi-sectional subset of Q.*

Proof. Let T be an element of the orbit of S under $\operatorname{LMlt} Q$. The pseudo-orbit $\{TL(q) \mid q \in Q\}$ of T is a subset of the $\operatorname{LMlt} Q$-orbit of S. If this orbit contains no distinct elements that are not disjoint, then neither will the pseudo-orbit. By Lemma 2.3, it follows that the pseudo-orbit partitions Q. Thus S is multi-sectional. □

Corollary 2.17. *Let S be a congruence class on a finite, non-empty quasigroup Q. Then S is multi-sectional.*

Proof. By [19, Proposition 5.2], S lies in a non-overlapping orbit. □

3. Conflatable quasigroups

This section introduces a new class of quasigroups, which comprises many well-known examples such as Bol loops and conjugacy-closed loops. In a finite member of this class, each sectional subset is polysectional.

3.1. **Definitions and examples.**

Definition 3.1. Let Q be a quasigroup.

(a) The quasigroup Q is said to be (*left*) *conflatable* if the condition (3.1)

$$\forall\, x \in Q\,,\ \exists\, \alpha_x \in Q!\,.\ \forall\, y \in Q\,,\ \exists\, v_{x,y} \in Q\,.\ L(x)L(y)\alpha_x = L(v_{x,y})$$

is satisfied.

(b) The quasigroup Q is said to be *right conflatable* if its opposite Q^{op} is left conflatable.

The Latin verb *conflāre* has the sense of "blow on" or "melt down". In (3.1), α_x is "blown on" $L(x)L(y)$, and "melts it down" to $L(v_{x,y})$.

For quasigroups $(Q,\cdot)$ and $(Q',\circ)$, recall that a *homotopy* is a triple (f,g,h) of functions from Q to Q' such that $x^f \circ y^g = (x\cdot y)^h$ for all x,y in Q. A homotopy is an *isotopy* if it consists of bijections. An isotopy is an *autotopy* if its domain $(Q,\cdot)$ and codomain $(Q',\circ)$ coincide.

Remark 3.2. (a) If Q is a left conflatable loop, then application of the equation from (3.1) to the identity element yields $(yx)^{\alpha_x} = v_{x,y}$. Thus for each element x of Q, the self-map $Q \to Q; y \mapsto v_{x,y} = yR(x)\alpha_x$ is bijective. The condition (3.1) may then be reformulated as saying that for each x in Q, there is an autotopy $\big(R(x)\alpha_x, L(x)^{-1}, \alpha_x\big)$ of Q.

(b) If Q is a quasigroup, applying the conclusion of (3.1) to $x\backslash x$ yields $v_{x,y}\cdot(x\backslash x) = yR(x)\alpha_x$. The autotopy $\big(R(x)\alpha_x R(x\backslash x)^{-1}, L(x)^{-1}, \alpha_x\big)$ is obtained in this case.

Example 3.3. (a) A group is conflatable, with $\alpha_x = 1$ and $v_{x,y} = yx$ in (3.1).

(b) More generally, a left Bol loop is left conflatable, with $\alpha_x = L(x)$ and $v_{x,y} = x\cdot yx$. It is worth noting that groups are conflatable in various ways, e.g. as in (a), or as here.

(c) Even more generally, a left Bol quasigroup [8] is left conflatable, with $\alpha_x = L(x)$ and $v_{x,y} = (x\cdot yx)/(x\backslash x)$.

(d) A left conjugacy-closed loop [16] is left conflatable, with $\alpha_x = L(x)^{-1}$ and $v_{x,y} = x\backslash(yx)$.

(e) More generally, define a *left conjugacy-closed quasigroup* to be a quasigroup satisfying the identity

$$x\backslash(y \cdot xz) = \big[(x\backslash(yx))/(x\backslash x)\big]z\,. \tag{3.2}$$

(This identity does not seem to have appeared in the literature.) Left conjugacy-closed quasigroups are left conflatable, with $\alpha_x = L(x)^{-1}$ and $v_{x,y} = (x\backslash(yx))/(x\backslash x)$.

Remark 3.4. The "conjugacy-closed quasigroups" considered in [12] are required to satisfy the condition

$$\big[(xy)/x\big]z = x\big[y(x\backslash z)\big]\,. \tag{3.3}$$

Now although the quasigroup of integers modulo 3 under the multiplication operation $x \cdot y = y - x$ does satisfy the quasigroup left conjugacy closure identity (3.2), it does not satisfy (3.3), since $[(0 \cdot 1)/0] \cdot 0 \neq 0 \cdot [1 \cdot (0\backslash 0)]$.

3.2. **Conflatability and isotopy.** Recall that a *principal isotopy* is an isotopy whose third component is an identity function. Finite quasigroups are principally isotopic if and only if they have the same Latin square in the body of their bordered multiplication tables, where the two respective tables differ at most by the orders in which the Latin square entries appear down the left borders or across the top borders.

Proposition 3.5. *Let*

$$(f, g, 1_Q)\colon (Q, \cdot) \to (Q, \circ) \tag{3.4}$$

be a principal isotopy from a left conflatable quasigroup $(Q, \cdot)$*. Suppose that the second component* g *of* (3.4) *is an automorphism of* $(Q, \circ)$*. Then* $(Q, \circ)$ *is left conflatable.*

Proof. Let q be an element of Q. Write $L(q)$ for left multiplication by q in $(Q, \cdot)$, and $L_\circ(q)$ for left multiplication by q in $(Q, \circ)$. The principal isotopy implies that

$$L(q) = gL_\circ(q^f)$$

for each element q of Q. On the other hand, the automorphic property of g implies that

$$L_\circ(q^g) = g^{-1}L_\circ(q)g$$

for each element q of Q. The conclusion

$$L(x)L(y)\alpha_x = L(v_{x,y})$$

of the conflatability condition (3.1) for $(Q,\cdot)$ may then be written, after left multiplication by g^{-2} and right multiplication by g, in the form

$$\begin{aligned} L_\circ(x^{fg})L_\circ(y^f)\big[\alpha_x g\big] &= g^{-2}\big[gL_\circ(x^f)gL_\circ(y^f)\alpha_x\big]g \\ &= g^{-2}\big[gL_\circ\big(v^f_{x,y}\big)\big]g = L_\circ\big(v^{fg}_{x,y}\big)\,. \end{aligned}$$

Thus

$$\forall\ x\in Q\,,\ \exists\ \alpha_{(xg^{-1}f^{-1})}g\in Q!\,.\ \forall\ y\in Q\,,\ \exists\ v^{fg}_{xg^{-1}f^{-1},yf^{-1}}\in Q\,.$$
$$L_\circ(x)L_\circ(y)\big[\alpha_{(xg^{-1}f^{-1})}g\big] = L_\circ\big(v^{fg}_{xg^{-1}f^{-1},yf^{-1}}\big)\,,$$

establishing the left conflatability of $(Q,\circ)$. □

The chiral dual follows:

Corollary 3.6. *Let*

$$(f,g,1_Q)\colon (Q,\cdot)\to(Q,\circ) \tag{3.5}$$

be a principal isotopy whose domain is a right conflatable quasigroup $(Q,\cdot)$. Suppose that the first component f of (3.5) *is an automorphism of $(Q,\circ)$. Then $(Q,\circ)$ is right conflatable.*

3.3. **Conflatability and sectionality.**

Theorem 3.7. *Let S be a sectional subset of a conflatable finite quasigroup Q. Then S is multi-sectional.*

Proof. Since Q is finite, each element λ of the left multiplication group of Q may be written as a monoid word in the elements of the generating set $\{L(q)\mid q\in Q\}$. It will be shown, by induction on the length of such a word λ, that each element $S\lambda$ of $S\mathrm{LMlt}\,Q$ is sectional. Since S is sectional, the claim is true for the image of S under the unique word of length 0.

Now suppose, by induction, that all the images of S under words of length less than n are sectional. Suppose that λ has length n, say $\lambda = L(q_1)\dots L(q_n)$ for $q_1,\dots,q_n\in Q$, and that there are elements x,y of Q such that $S\lambda L(x)$ intersects non-trivially with $S\lambda L(y)$. In other words, there are elements s and t of S such that $s\lambda L(x) = t\lambda L(y)$, or

$$sL(q_1)\dots L(q_{n-1})L(q_n)L(x) = tL(q_1)\dots L(q_{n-1})L(q_n)L(y)\,. \tag{3.6}$$

Since Q is conflatable, $L(q_n)L(x)\alpha_{q_n} = L(v_{q_n,x})$ and $L(q_n)L(y)\alpha_{q_n} = L(v_{q_n,y})$. Then (3.6) implies

$$sL(q_1)\dots L(q_{n-1})L(q_n)L(x)\alpha_{q_n} = tL(q_1)\dots L(q_{n-1})L(q_n)L(y)\alpha_{q_n}\,,$$

whence

$$sL(q_1)\dots L(q_{n-1})L(v_{q_n,x}) = tL(q_1)\dots L(q_{n-1})L(v_{q_n,y})\,.$$

By the induction hypothesis, which implies that $SL(q_1)\dots L(q_{n-1})$ is sectional, it follows that

$$SL(q_1)\dots L(q_{n-1})L(v_{q_n,x}) = SL(q_1)\dots L(q_{n-1})L(v_{q_n,y})$$

or

$$SL(q_1)\dots L(q_{n-1})L(q_n)L(x)\alpha_{q_n} = SL(q_1)\dots L(q_{n-1})L(q_n)L(y)\alpha_{q_n}\,.$$

Applying the inverse of α_{q_n} to both sides yields

$$SL(q_1)\dots L(q_{n-1})L(q_n)L(x) = SL(q_1)\dots L(q_{n-1})L(q_n)L(y)\,,$$

showing that $S\lambda$ is sectional. □

4. Sectional subquasigroups

4.1. **Sectional versus Lagrangean.** In general, a left sectional subquasigroup of a finite quasigroup need not be left Lagrangean. Recall that a subquasigroup P of a finite quasigroup Q is *left Lagrangean* if the relative right multiplication group $\mathrm{RMlt}_Q P = \langle R(p) \mid p \in P\rangle_{Q!}$ of P in Q acts semitransitively, so that its orbits all have the same size $|P|$ [18, §4.5] [19, §4].

Example 4.1. Consider the opposite Q of the quasigroup of integers modulo 3 under subtraction, with $S = \{0\}$. The subquasigroup S is left sectional. However, $1R_Q(0) = 1 -^{\mathsf{op}} 0 = 0 - 1 = 2$, so $\{1, 2\}$ is an orbit of $\mathrm{RMlt}_Q S$, and S is not left Lagrangean.

The following result summarizes the main connections between the subquasigroup properties of being sectional and being Lagrangean.

Theorem 4.2. *Let S be a non-empty subquasigroup of a finite quasigroup Q.*

(a) *If S is left Lagrangean, then it is left sectional.*
(b) *If S is left sectional, and contains a right identity for Q, then it is left Lagrangean.*

Proof. (a) If S is left Lagrangean, the relative right multiplication group $\mathrm{RMlt}_Q S$ of S in Q acts semitransitively on Q. This means that each orbit $q\mathrm{RMlt}_Q S$ of $\mathrm{RMlt}_Q S$ on Q has the same length $|S|$ as the orbit S. Now the left translate qS of an element q of Q is contained in its orbit $q\mathrm{RMlt}_Q S$. Since $|S| = |qS| \leq |q\mathrm{RMlt}_Q S| = |S|$, it follows that $qS = q\mathrm{RMlt}_Q S$: the translates and orbits coincide. Since the orbits partition Q, one may say that the left translates qS partition Q, and S is left sectional.

(b) Suppose that S is left sectional, and contains an element e with $R_Q(e) = 1$ (i.e., a right identity for Q). Since Q is finite, the relative

right multiplication group $\mathrm{RMlt}_Q S$ of S in Q consists of monoid words in the alphabet $\{R(s) \mid s \in S\}$. Let x be an element of Q. It will be shown, by induction on the length n of such a word $R(s_1) \dots R(s_n)$, with $s_i \in S$, that $xR(s_1) \dots R(s_n)$ lies in the translate xS. The result is true for $n = 0$, since $x1 = x = xe \in xS$. Now suppose $x\alpha \in xS$ for words α of length less than n. Then $xR(s_1) \dots R(s_n) = x\beta R(s_n)$ with $\beta = R(s_1) \dots R(s_{n-1})$, and $x\beta = xs$ with some $s \in S$, by induction. Thus $xR(s_1) \dots R(s_n) = (xs)s_n \in (xs)S$. However, $(xs)S \ni (xs)e = xs \in xS$. Since S is left sectional, this implies $(xs)S = xS$, and therefore $xR(s_1) \dots R(s_n) \in xS$, as required. □

Corollary 4.3. *Let S be a subloop of a finite loop. Then S is left Lagrangean if and only if it is left sectional.*

Corollary 4.4. *Let S be a cyclic subgroup of a finite loop L. Then S is left sectional in each of the following cases:*

(a) *L is a right Bol loop;*
(b) *L is a di-associative loop.*

Proof. In [19, §11], it was shown that cyclic subloops of finite right Bol (including Moufang) and di-associative loops are left Lagrangean. The result then follows by Corollary 4.3. □

4.2. **Paige loops.** The results of this paragraph were obtained using a GAP computation with the LOOPS package. However, the first statement of Proposition 4.5 is a consequence of Corollary 4.4.

Proposition 4.5. *In the Paige loop $\mathsf{PSL}_{1,3}(2)$, subloops of order 2 and 3 are sectional (cf. §4.1), while subloops of orders 4 (cf. §8.1), 6, 8, 12 and 24 are not. This list comprises all the proper, non-trivial subloops of $\mathsf{PSL}_{1,3}(2)$.*

Although the subloops of order 2 and 3 lie in overlapping orbits (of $\mathrm{LMlt}\,\mathsf{PSL}_{1,3}(2)$), each element of these two orbits is a sectional subset of $\mathsf{PSL}_{1,3}(2)$. Furthermore, there are no other sectional subsets of sizes 2 or 3.

Additional information, beyond that incorporated in Proposition 4.5, is listed in Table 2. The term "orbit length" refers to orbits of the left multiplication group $\mathrm{LMlt}\,\mathsf{PSL}_{1,3}(2)$, as studied in [19]. The subloops were classified in [21]. See §8.1 below for a description of the two types of Klein 4-subgroup $V_4^{\pm}$. Note that $G \sqcup 2$ denotes the Chein double of a group G, also often written as $M_{2|G|}(G, 2)$ [5, 9].

Subloop type	Size	Pseudo-orbit length	Orbit length
C_2	2	60	3780
C_3	3	40	1120
V_4^+	4	102	9450
V_4^-	4	114	113400
S_3	6	110	67200
C_2^3	8	71	2025
A_4	12	98	3150
$S_3 \sqsupset 2$	12	109	11200
$A_4 \sqsupset 2$	24	49	1575

TABLE 2. Subloops of the Paige loop $\mathsf{PSL}_{1,3}(2)$

4.3. **Group extensions.**

Lemma 4.6. *Let q and q' be elements of a quasigroup Q. Suppose that V is a congruence on Q. Then $q' \cdot q^V = (q'q)^V$.*

Proof. The equivalence classes $q' \cdot q^V$ and $(q'q)^V$ both contain $q'q$, so they coincide. □

Theorem 4.7. *Let Q be a finite quasigroup, with congruence V, such that Q^V is a group with identity element e^V. If a subquasigroup P of Q contains e^V, then P is a sectional subquasigroup of Q.*

Proof. Suppose $x \in q_1P \cap q_2P$ for $q_1, q_2 \in Q$. Then $x^V \in q_1^V P^V \cap q_2^V P^V$. In the group Q^V, intersecting cosets of the subgroup P^V coincide, so $q_1^V P^V = q_2^V P^V$. Thus for each element p_1 of P, one has

$$q_1p_1 \in q_1^V p_1^V \subseteq q_1^V P^V = q_2^V P^V = \{(q_2p)^V \mid p \in P\}.$$

In other words,

$$\exists\, p_2 \in P \,.\, q_1p_1 \in (q_2p_2)^V = q_2 \cdot p_2^V,$$

the equality holding by Lemma 4.6. Since P^V contains the congruence class e^V, it is a union of V-classes. Thus there is an element p_2' of P (in p_2^V) such that $q_1p_1 = q_2p_2'$. It follows that $q_1p_1 \in q_2P$, and so $q_1P = q_2P$, as required. □

Corollary 4.8. *Let L be a finite loop, with normal subloop N, such that L/N is a group. If a subloop P of L contains N, then P is a sectional subloop of L.*

5. Classifying divisors

In the part of Sylow theory presented in [19, §8], non-overlapping orbits provided the basis for a classification of the divisors of the order of a non-trivial finite quasigroup. Here, the partitional pseudo-orbits play a comparable role. A parallel classification is established (§5.1–5.2), and compared with the previous classification (§5.3).

5.1. **The classification.**

Definition 5.1. Let d be a positive integer, and let Q be a quasigroup whose (finite) order is a multiple of d. For the quasigroup Q, the integer d is said to have ...

- ... *type J** if a sectional subset of size d exists;
- ... *type I** if there is a pseudo-orbit, generated by a sectional subset of size d, which contains a subquasigroup of Q;
- ... *type H** if each pseudo-orbit generated by a sectional subset of size d contains a subquasigroup of Q;
- ... *type G** if it has type H*, and if each subquasigroup in a pseudo-orbit generated by a (left) sectional subset of size d is (right) Lagrangean.

5.2. **Separating the classes.**

We provide a sequence of examples of 6-element loops that separate the classes of Definition 5.1.

Example 5.2. In the loop whose (unlabeled) multiplication table is the Latin square

1	2	3	4	5	6
2	1	4	3	6	5
3	4	5	6	1	2
4	5	6	1	2	3
5	6	1	2	3	4
6	3	2	5	4	1

the divisor 2 is not of type J*: no doubleton is sectional.

Example 5.3. In the loop whose (unlabeled) multiplication table is the Latin square

1	2	3	4	5	6
2	1	4	3	6	5
3	5	1	6	4	2
4	6	5	2	3	1
5	4	6	1	2	3
6	3	2	5	1	4

the divisor 2 is of type J*, but not I*. Note that the doubleton $\{3,4\}$ is sectional, although the pseudo-orbit $\big\{\{1,6\},\{2,5\},\{3,4\}\big\}$ it generates contains no subquasigroup.

Example 5.4. In the loop whose (unlabeled) multiplication table is the Latin square

1	2	3	4	5	6
2	1	4	3	6	5
3	5	1	6	2	4
4	6	2	5	1	3
5	3	6	2	4	1
6	4	5	1	3	2

the divisor 2 is of type I*, but not H*. Note that the subloop $\{1,2\}$ generates the partitional pseudo-orbit $\big\{\{1,2\},\{3,5\},\{4,6\}\big\}$. On the other hand, the pseudo-orbit $\big\{\{1,6\},\{2,5\},\{3,4\}\big\}$ generated by $\{2,5\}$ contains no subquasigroup.

Remark 5.5. Example 5.11 below shows that in the Paige loop $\mathsf{PSL}_{1,3}(2)$ of order 120, the divisors 2 and 3 have type I*, but not H*.

Example 5.6. In the loop whose (unlabeled) multiplication table is the Latin square

1	2	3	4	5	6
2	1	4	3	6	5
3	5	1	6	2	4
4	6	2	5	1	3
5	4	6	1	3	2
6	3	5	2	4	1

the divisor 2 is of type H*, but not G*. For instance, the subloop $\{1,6\}$ generates the partitional pseudo-orbit $\big\{\{1,6\},\{2,5\},\{3,4\}\big\}$, but the relative left multiplication group of $\{1,6\}$ has $\{2,3,5,4\}$ as an orbit.

Example 5.7. In the non-associative loop whose (unlabeled) multiplication table is the Latin square

1	2	3	4	5	6
2	1	4	3	6	5
3	4	5	6	1	2
4	3	6	5	2	1
5	6	1	2	4	3
6	5	2	1	3	4

the divisor 2 is of type G*.

5.3. **Comparing classifications.** In this paragraph, comparisons are made between the two parallel classifications of divisors of the order of a finite quasigroup: the classification of [19, §8] based on non-overlapping orbits, and the classification of §5.1 based on sectional subsets and pseudo-orbits. For convenience, we recall the former classification:

Definition 5.8. [19] Let d be a positive integer, and let Q be a quasigroup whose (finite) order is a multiple of d. Consider the action of $\mathrm{LMlt}\, Q$ on the set $\binom{Q}{d}$ of subsets of Q of size d. For the quasigroup Q, the integer d is said to have ...

- ... *type J* if at least one non-overlapping orbit exists;
- ... *type I* if the action has at least one non-overlapping orbit which contains a subquasigroup of Q;
- ... *type H* if the action has non-overlapping orbits, each of which contains a subquasigroup of Q;
- ... *type G* if it has type H, and if each subquasigroup in a non-overlapping orbit is (right) Lagrangean.

The first result is a consequence of Lemmas 6.1(b) and 2.16.

Lemma 5.9. *Let d be a positive integer, and let Q be a quasigroup whose (finite) order is a multiple of d.*

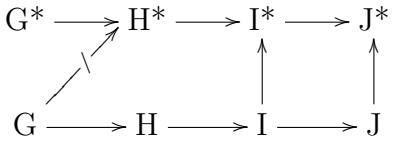
(a) *If d has type J, then it has type J*.*
(b) *If d has type I, then it has type I*.*

Example 5.10. Consider the loop Q of Example 5.4. The orbit of the subloop $\{1,2\}$ under $\mathrm{LMlt}\, Q$ coincides with its partitional pseudo-orbit $\big\{\{1,2\},\{3,5\},\{4,6\}\big\}$, while all the remaining two-element subsets lie in a single $\mathrm{LMlt}\, Q$-orbit. Thus $\big\{\{1,2\},\{3,5\},\{4,6\}\big\}$ is the unique non-overlapping orbit on $\binom{Q}{2}$. Furthermore, $\{1,2\}$ is right and left Lagrangean (e.g., by Corollary 4.3). Thus 2 has type G, even though it does not have type H*.

Along with Lemma 5.9(b), the following example shows that type I is properly contained in type I*, and that type J is properly contained in type J*.

Example 5.11. Consider the Paige loop $\mathsf{PSL}_{1,3}(2)$, of order 120. By Proposition 4.5, it follows that both 2 and 3 are of type I*, but not of type H* or I. In particular, 2 has type J*. However, 2 does not have type J, since there are just two orbits of the full left multiplication group on the set of two-element subsets, having respective lengths 3360 and 3780 (as determined by the `LOOPS` package for `GAP`).

The relationships between the divisor classes are summarized in the diagram



where plain arrows indicate proper containments, and the slashed arrow indicates non-containment.

6. Pseudo-orbit lengths

If a subset S of a finite quasigroup Q is sectional, Lemma 2.3 ensures that the length of its pseudo-orbit is $|Q|/|S|$. On the other hand, the same lemma shows that a subset S which is not sectional generates a longer pseudo-orbit. If the length of a pseudo-orbit is l, the *co-length* $\text{co-l}_Q(S)$ of the pseudo-orbit is defined as $|Q| - l$. These co-lengths provide powerful isomorphism invariants, as illustrated below in §7.1.

6.1. **The coset function.** Let S be a subset of a finite quasigroup Q. Define the *coset function*

$$c_S \colon Q \to 2^Q; q \mapsto qS\,.$$

The relation kernel $\ker c_S$ of the coset function, defined by relating elements q, q' of Q if and only if $qS = q'S$, is an equivalence relation on Q. By the First Isomorphism Theorem for sets, there is a bijection

$$b \colon Q^{\ker c_S} \to \{qS \mid q \in Q\}; q^{\ker c_S} \mapsto qS \tag{6.1}$$

to the image of the coset function, namely the pseudo-orbit generated by S, from the set $Q^{\ker c_S}$ of equivalence classes. One obtains the formula

$$\text{co-l}_Q(S) = |Q| - \left|Q^{\ker c_S}\right| = \sum_{K \in Q^{\ker c_S}} (|K| - 1) \tag{6.2}$$

for the co-length of the pseudo-orbit generated by S. In this context, it is sometimes convenient to refer to the quantity $|K| - 1$ as the *excess* of a $(\ker c_S)$-class K, and to describe such a class as *excessive* if $|K| > 1$.

Lemma 6.1. *Suppose that S is a non-empty subquasigroup of a finite quasigroup Q.*

(a) *S is a $(\ker c_S)$-class.*
(b) *S is a member of the pseudo-orbit it generates.*

Proof. For an element q of Q, one has $qS = S$ iff $q \in S$. □

Example 6.2. Consider the opposite Q of the quasigroup of integers modulo 3 under subtraction, with $S = \{0\}$. In this case, the bijection (6.1) maps $\{0\} \mapsto \{0\}$, $\{1\} \mapsto \{2\}$, and $\{2\} \mapsto \{1\}$, so for $q \in Q \setminus S$, the equivalence class $q^{\ker c_S}$ may differ from its corresponding image qS, even when S is a subquasigroup.

From (6.2), one obtains the following.

Corollary 6.3. *The co-length of the pseudo-orbit generated by a non-empty subquasigroup S is at least $|S| - 1$.*

6.2. **A lower bound on certain co-lengths.**

Lemma 6.4. *Let S be a subgroup of a subgroup G of a quasigroup Q. Then each element of G lies in a $(\ker c_S)$-class of size $|S|$.*

Proof. Suppose $x \in G$ and $y \in Q$. If $xS = yS$, then $x = x1_S \in xS = yS$ implies $x = ys$ for some element s of S, so $y = x/s \in G$. Thus the two elements x and y are related by $\ker c_S$ if and only if they lie in the same group (left) coset in G. It follows that the $(\ker c_S)$-class of each element x of G has size $|S|$. □

Theorem 6.5. *Let S be a subgroup of a quasigroup Q. Let $\mathcal{M}$ be the meet semilattice (under set-theoretical inclusion) of all subgroups of Q that contain S. Let $\mu_{\mathcal{M}}$ be the Möbius function in $\mathcal{M}$. Then*

$$\sum_{G \in \mathcal{M}} \sum_{H \in \mathcal{M}} \mu_{\mathcal{M}}(H, G)\,(|H|/|S|)\,(|S| - 1) \tag{6.3}$$

is a lower bound on the co-length of the pseudo-orbit generated by S.

Proof. Extend the meet semilattice order $\mathcal{M}$ to a linear order $\mathcal{L}$ (cf. [3], [20, O, Prop. 3.5.4(a)]). Recall that the Möbius function values $\mu_{\mathcal{M}}(H, G)$ appearing in (6.3) are the entries of the matrix inverse to the upper triangular incidence matrix of the order relation $\mathcal{M}$ with respect to a basis ordered by $\mathcal{L}$.

The subgroup S is the first element in the linear order $\mathcal{L}$. By Lemma 6.1 and Corollary 6.3, the elements of S contribute

$$|S| - 1 = \mu_{\mathcal{M}}(S, S)\,(|S|/|S|)\,(|S| - 1)$$

to the sum form (6.2) for $\text{co-l}_Q(S)$.

Now consider progressively building up the sum (6.3) by taking the general elements G of $\mathcal{M}$ in the order that is determined by $\mathcal{L}$. By Lemma 6.4, the elements of G make a total contribution of

$$(|G|/|S|)\,(|S| - 1)$$

to the sum (6.2). However, the only "new" contributions, that have not already arisen from elements of a subgroup H of G (which necessarily shows up earlier in $\mathcal{L}$), are counted by the summand

$$\sum_{H \in \mathcal{M}} \mu_{\mathcal{M}}(H, G)\,(|H|/|S|)\,(|S| - 1)$$

of (6.3). □

Remark 6.6. Section 8.1 provides examples where the lower bound given in Theorem 6.5 is sharp. On the other hand, there are many cases where the lower bound is not sharp, especially for sectional subgroups. Remark 8.5 provides an example of a non-sectional subgroup for which the bound is not sharp.

7. Connections with design theory

This section presents some connections between design theory and the current Sylow theory for quasigroups. In §7.1, it is shown how the Sylow theory provides easily computed isomorphism invariants, indeed complete invariants, to distinguish among the 80 Steiner triple systems of order 15 [6, Table II.1.28]. Within §7.2, certain aspects of Hall triple systems are examined from the standpoint of Sylow theory. Finally, §7.3 presents a small example where successive translates of a sectional subloop of a loop may be used to produce regular graphs.

7.1. **Steiner quasigroups of order** 15**.** Let X be a set. Suppose that $(V, E, c : E \to X)$ is an edge-labeled graph. We say that two edge-labeled graphs $(V_i, E_i, c_i : E_i \to X)$ are *isomorphic* if there is a bijection $\varphi : V_1 \to V_2$ that induces a bijection $\psi : E_1 \to E_2$ such that $ec_1 = e\psi c_2$ for every $e \in E_1$.

For a quasigroup Q, let $\Gamma(Q)$ be the complete graph with vertex set Q, where each edge $\{x, y\}$ is labeled by the colength $\text{co-l}_Q\big(\{x, y\}\big)$ of the subset $\{x, y\}$ in Q. It is clear that two quasigroups Q_1, Q_2 are non-isomorphic if the corresponding edge-labeled graphs $\Gamma(Q_1)$, $\Gamma(Q_2)$ are non-isomorphic.

The following (computational) result shows that the colength graph $\Gamma(Q)$ provides a complete isomorphism invariant for the 80 Steiner triple systems of order 15 tabulated in [6, Table II.1.28].

Theorem 7.1. *Up to isomorphism, the* 80 *Steiner triple systems of order* 15 *are distinguished by means of the colengths of two-element subsets. More precisely, let* $Q_1, \ldots, Q_{80}$ *be a full set of representatives for the* 80 *isomorphism classes of Steiner quasigroups of order* 15*. Then no two edge-labeled graphs* $\Gamma(Q_i)$, $\Gamma(Q_j)$ *with* $i \neq j$ *are isomorphic.*

Further powerful isomorphism invariants are obtained from Sylow theory as follows. For a linearly ordered quasigroup Q of finite order n, and for each $1 \leq i \leq n$, consider the lexicographically ordered sequence

$$s_i(Q) = (S_1, \ldots, S_{b_i})$$

of all i-element chains $S_k = \{q_{j_1} < q_{j_2} < \cdots < q_{j_i}\}$ in Q, with $b_i = \binom{n}{i}$ and $1 \leq k \leq b_i$. Define the i-th *colength sequence*

$$c_i(Q) = \left(\text{co-l}_Q(S_1), \ldots, \text{co-l}_Q(S_{b_i})\right).$$

The second colength sequences $c_2(Q)$ turn out to be pairwise distinct for the 80 Steiner quasigroups of order 15 as they are implemented in the `LOOPS` package. Nevertheless, since the colength sequences $c_i(Q)$ for $i > 1$ depend on the ordering of the underlying elements of Q, they are not invariants of quasigroup isomorphism.

However, if $c_i^*(Q)$ is the sorted version of the i-th colength sequence $c_i(Q)$, then $c_i^*(Q)$ is a quasigroup isomorphism invariant. Represent these i-th *sorted colength sequences* as multisets, where $x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}$ means that the colength x_1 occurs i_1 times, the colength x_2 occurs i_2 times, and so on, with $x_1 < \ldots < x_m$.

It transpires that the 80 Steiner quasigroups of order 15 fall into 49 different classes according to $c_2^*(Q)$, with no class containing more than 5 quasigroups. See Table 3 for more information. Combining $c_2^*(Q)$, $c_3^*(Q)$ and $c_4^*(Q)$ suffices to distinguish all but two Steiner quasigroups of order 15, the exceptions being the quasigroups associated with items 62 and 63 from [6, Table II.1.28].

Most strikingly, the invariant $c_6^*(Q)$ is complete. Details may be found in Table 4.

Theorem 7.2. *The sixth sorted colength sequence $c_6^*(Q)$ suffices to separate all the* 80 *Steiner quasigroups of order* 15*.*

Remark 7.3. Consider a quasigroup Q of order n that is specified by its multiplication table. For a fixed constant $1 < i \leq \lfloor n/2 \rfloor$, the complexity of the computation of the i-th sorted colength $c_i^*(Q)$ is polynomial in n. Similarly, the complexity of the computation of the full collection of all i-th sorted colengths $c_i^*(Q)$ for every $1 < i \leq \lfloor n/2 \rfloor$ is also polynomial in n.

7.2. **Hall triple systems.** Hall triple systems are designs that may be characterized readily in terms of certain quasigroups.

Definition 7.4. Let $(Q, \circ)$ be a quasigroup.

80 0^{105}	77 $0^{99}2^{6}$	57 $0^{92}2^{12}6^{1}$	37 $0^{91}2^{12}6^{2}$	67, 69, 71, 72 $0^{90}2^{15}$	50 $0^{89}2^{15}6^{1}$	66, 68, 73, 78, 79 $0^{87}2^{18}$
46, 49, 60 $0^{86}2^{18}6^{1}$	62, 63, 65, 75 $0^{84}2^{21}$	42, 44, 48, 56, 58 $0^{83}2^{21}6^{1}$	38, 51 $0^{82}2^{21}6^{2}$	74 $0^{81}2^{24}$	43 $0^{81}2^{21}6^{3}$	45, 52, 55 $0^{80}2^{24}6^{1}$
36, 53 $0^{79}2^{24}6^{2}$	70 $0^{78}2^{27}$	47 $0^{77}2^{27}6^{1}$	41 $0^{77}2^{24}6^{4}$	54 $0^{76}2^{27}6^{2}$	35 $0^{76}2^{24}6^{5}$	64, 76 $0^{75}2^{30}$
40 $0^{74}2^{27}6^{4}$	34, 39 $0^{73}2^{30}6^{2}$	17 $0^{72}2^{12}6^{21}$	33 $0^{71}2^{33}6^{1}$	27, 30 $0^{69}2^{33}6^{3}$	32, 59 $0^{68}2^{36}6^{1}$	28 $0^{66}2^{36}6^{3}$
61 $0^{63}2^{42}$	25 $0^{63}2^{33}6^{9}$	29 $0^{62}2^{36}6^{7}$	19, 22 $0^{60}2^{42}6^{3}$	23, 31 $0^{59}2^{42}6^{4}$	26 $0^{58}2^{36}6^{11}$	24 $0^{56}2^{45}6^{4}$
16 $0^{56}6^{49}$	21 $0^{55}2^{45}6^{5}$	20 $0^{53}2^{48}6^{4}$	15, 18 $0^{52}2^{42}6^{11}$	7, 13 $0^{48}2^{36}6^{21}$	11 $0^{46}2^{54}6^{5}$	8, 14 $0^{44}2^{36}6^{25}$
9, 10 $0^{38}2^{54}6^{13}$	12 $0^{35}2^{57}6^{13}$	3 $0^{32}2^{24}6^{49}$	6 $0^{24}2^{66}6^{15}$	4, 5 $0^{16}2^{60}6^{29}$	2 $2^{48}6^{57}$	1 6^{105}

TABLE 3. The 80 Steiner quasigroups Q of order 15 from [6, Table II.1.28], classified into 49 classes according to the sorted colength sequences $c_2^*(Q)$. The entries are ordered lexicographically by their colength sequences.

(a) $(Q, \circ)$ is *left distributive* if each left multiplication

$$L_\circ(q)\colon Q \to Q; x \mapsto q \circ x$$

by an element q of Q is an automorphism of $(Q, \circ)$.

(b) $(Q, \circ)$ is *right distributive* if each right multiplication

$$R_\circ(q)\colon Q \to Q; x \mapsto x \circ q$$

by an element q of Q is an automorphism of $(Q, \circ)$.

(c) $(Q, \circ)$ is *distributive* if it is both left and right distributive.

(d) $(Q, \circ)$ is said to be a *TSDQ* if it is totally symmetric and distributive.

Distributive quasigroups are conflatable.

Proposition 7.5. *Let $(Q, \circ)$ be a distributive quasigroup.*

(a) *Each element e of Q is idempotent in $(Q, \circ)$.*

(b) *For a given element e of Q, define*

$$x \cdot y = xR_\circ(e)^{-1} \circ yL_\circ(e)^{-1}. \tag{7.1}$$

Then $(Q, \cdot, e)$ is a commutative Moufang loop.

(c) *The quasigroup $(Q, \circ)$ is conflatable.*

Proof. (a) Note $e \circ (e \circ e) = (e \circ e) \circ (e \circ e)$ by Definition 7.4(a), and cancel $e \circ e$.

(b) This is Belousov's Theorem [1, Teorema 1], [2, Teorema 8.1].

1 $0^{4480}4^{525}$	2 $0^{4456}1^{160}2^{144}3^{96}4^{149}$	3 $0^{4444}1^{272}2^{72}3^{144}4^{73}$	4 $0^{4504}1^{284}2^{124}3^{52}4^{41}$
5 $0^{4512}1^{304}2^{76}3^{56}4^{57}$	6 $0^{4580}1^{312}2^{72}3^{8}4^{33}$	7 $0^{4600}1^{288}2^{36}3^{24}4^{57}$	8 $0^{4526}1^{322}2^{80}3^{58}4^{19}$
9 $0^{4600}1^{306}2^{62}3^{26}4^{11}$	10 $0^{4602}1^{304}2^{60}3^{28}4^{11}$	11 $0^{4638}1^{320}2^{32}3^{8}4^{7}$	12 $0^{4551}1^{355}2^{71}3^{21}4^{7}$
13 $0^{4554}1^{322}2^{68}3^{42}4^{19}$	14 $0^{4522}1^{320}2^{96}3^{48}4^{19}$	15 $0^{4626}1^{304}2^{48}3^{16}4^{11}$	16 $0^{4438}1^{280}2^{84}3^{168}4^{35}$
17 $0^{4570}1^{326}2^{60}3^{30}4^{19}$	18 $0^{4622}1^{310}2^{48}3^{14}4^{11}$	19 $0^{4692}1^{274}2^{26}3^{6}4^{7}$	20 $0^{4647}1^{322}2^{29}4^{7}$
21 $0^{4605}1^{370}2^{23}4^{7}$	22 $0^{4650}1^{328}2^{20}4^{7}$	23 $0^{4663}1^{307}2^{22}3^{13}$	24 $0^{4643}1^{326}2^{24}3^{12}$
25 $0^{4614}1^{330}2^{45}3^{16}$	26 $0^{4586}1^{347}2^{53}3^{19}$	27 $0^{4671}1^{308}2^{18}3^{8}$	28 $0^{4652}1^{325}2^{21}3^{7}$
29 $0^{4632}1^{323}2^{35}3^{15}$	30 $0^{4662}1^{319}2^{17}3^{7}$	31 $0^{4679}1^{292}2^{20}3^{14}$	32 $0^{4663}1^{323}2^{12}3^{7}$
33 $0^{4671}1^{317}2^{14}3^{3}$	34 $0^{4648}1^{336}2^{17}3^{4}$	35 $0^{4611}1^{368}2^{20}3^{6}$	36 $0^{4697}1^{290}2^{18}$
37 $0^{4645}1^{354}2^{6}$	38 $0^{4635}1^{356}2^{10}3^{4}$	39 $0^{4646}1^{338}2^{17}3^{4}$	40 $0^{4648}1^{327}2^{27}3^{3}$
41 $0^{4640}1^{342}2^{19}3^{4}$	42 $0^{4596}1^{397}2^{11}3^{1}$	43 $0^{4668}1^{321}2^{15}3^{1}$	44 $0^{4684}1^{309}2^{11}3^{1}$
45 $0^{4650}1^{342}2^{11}3^{2}$	46 $0^{4645}1^{349}2^{10}3^{1}$	47 $0^{4668}1^{325}2^{9}3^{3}$	48 $0^{4672}1^{320}2^{13}$
49 $0^{4661}1^{332}2^{12}$	50 $0^{4668}1^{327}2^{7}3^{3}$	51 $0^{4622}1^{365}2^{17}3^{1}$	52 $0^{4653}1^{337}2^{14}3^{1}$
53 $0^{4664}1^{324}2^{13}3^{4}$	54 $0^{4631}1^{355}2^{16}3^{3}$	55 $0^{4630}1^{361}2^{13}3^{1}$	56 $0^{4660}1^{329}2^{15}3^{1}$
57 $0^{4678}1^{318}2^{9}$	58 $0^{4700}1^{291}2^{11}3^{3}$	59 $0^{4608}1^{377}2^{17}3^{3}$	60 $0^{4624}1^{365}2^{15}3^{1}$
61 $0^{4704}1^{280}2^{14}4^{7}$	62 $0^{4710}1^{287}2^{5}3^{3}$	63 $0^{4713}1^{284}2^{2}3^{6}$	64 $0^{4680}1^{311}2^{11}3^{3}$
65 $0^{4658}1^{335}2^{11}3^{1}$	66 $0^{4661}1^{336}2^{6}3^{2}$	67 $0^{4650}1^{348}2^{5}3^{2}$	68 $0^{4682}1^{315}2^{7}3^{1}$
69 $0^{4670}1^{326}2^{7}3^{2}$	70 $0^{4664}1^{327}2^{13}3^{1}$	71 $0^{4689}1^{307}2^{8}3^{1}$	72 $0^{4654}1^{341}2^{9}3^{1}$
73 $0^{4611}1^{384}2^{8}3^{2}$	74 $0^{4703}1^{290}2^{12}$	75 $0^{4652}1^{342}2^{11}$	76 $0^{4705}1^{290}2^{10}$
77 $0^{4669}1^{333}2^{2}3^{1}$	78 $0^{4675}1^{320}2^{8}3^{2}$	79 $0^{4699}1^{300}3^{6}$	80 $0^{4675}1^{330}$

TABLE 4. Distinguishing the 80 Steiner quasigroups Q of order 15 using the sorted colength sequences $c_6^*(Q)$. The table is ordered by the index r of the corresponding Steiner triple systems in [6, Table II.1.28].

(c) If $(Q, \circ)$ is empty, the result is immediate. Otherwise, choose an element e of Q. By (b), there then exists a principal isotopy

$$\big(R_\circ(e), L_\circ(e), 1_Q\big) \colon (Q, \cdot) \to (Q, \circ) \tag{7.2}$$

from a commutative Moufang loop structure $(Q, \cdot, e)$ on the set Q. By (a), the automorphism $L_\circ(e)$ of $(Q, \circ)$ fixes e. Thus in the principal isotopy (7.2), the second component is an automorphism of the domain multiplication (7.1). As noted in Example 3.3(b), the left Bol loop $(Q, \cdot, e)$ is conflatable. Proposition 3.5 then implies that the codomain $(Q, \circ)$ of (7.2) is left conflatable. A chirally dual argument shows that $(Q, \circ)$ is right conflatable. □

Three approaches to Hall triple systems are collected in the following result. In the present context, the condition of Proposition 7.6(a) is the most appropriate.

Proposition 7.6. [23] *Let $(Q, \mathcal{B})$ be a Steiner triple system. Then the following conditions are equivalent:*

(a) *The corresponding Steiner quasigroup $(Q, \circ)$ is a TSDQ;*
(b) *For each block B in $\mathcal{B}$, and for each element q of Q, the translate $q \circ B$ is again a block of Q;*
(c) *For each element q of Q, there is an involutory automorphism of $(Q, \mathcal{B})$ with q as its unique fixed point.*

Definition 7.7. (a) A Steiner triple system is a *Hall triple system* if it satisfies the equivalent conditions of Proposition 7.6.

(b) A Hall triple system is a *Hall matroid* if it does not constitute the set of lines in an affine geometry over $\mathsf{GF}(3)$.

Remark 7.8. (a) Hall triple systems are also known as "affine triple systems" [23].

(b) The terminology of Definition 7.7(b) was introduced in [23], in reference to the unique Hall matroid of order 81 constructed in [11].

Proposition 7.9. *Let B be a block of a finite Hall triple system $(Q, \mathcal{B})$. Then B is a multi-sectional subset of the corresponding TSDQ $(Q, \circ)$.*

Proof. Suppose that $B = \{e, p, e \circ p\}$. Now within the corresponding commutative Moufang loop $(Q, \cdot, e)$, the set B is the cyclic subgroup $\{e, p, p^{-1}\}$. By Corollary 4.4, B is (left) sectional in $(Q, \cdot, e)$. Consider the left translate $q \circ B$ of B in $(Q, \circ)$ by an element q of Q. Then by (7.1), one has $q \circ B = qR_\circ(e) \cdot BL_\circ(e) = qR_\circ(e) \cdot B$, a left translate of B in $(Q, \cdot, e)$. Since these left translates partition Q, it follows that B is sectional in $(Q, \circ)$. By Proposition 7.5(c), $(Q, \circ)$ is conflatable. Theorem 3.7 then shows that B is multi-sectional in $(Q, \circ)$. □

Proposition 7.10. *Consider the Hall matroid $(Q, \mathcal{B})$ of order 81. There is a block B in $\mathcal{B}$, along with elements q_1, q_2 of Q, such that the double translate $q_1 \circ (q_2 \circ B)$ does not appear as the single translate $q \circ B$ for any element q of Q.*

Proof. Build the Hall matroid on the free commutative Moufang loop $(Q, \cdot, e)$ of exponent 3 on the 3-element set $\{x, y, z\}$. Consider the block $B = \{e, x, x^{-1}\}$. For each element q of Q, the subloop of $(Q, \cdot, e)$ generated by $(q \circ B) \cup B$ has order at most 9, as the associative subloop generated by $\{q, x\}$.

Now take $q_2 = y$, so that $q_2 \circ B = \{y^{-1}, y^{-1}x^{-1}, y^{-1}x\}$. Then take $q_1 = z^{-1}$, so that $q_1 \circ (q_2 \circ B) = \{zy, z(yx), z(yx^{-1})\}$. In terms of the associator (x, y, z), the double translate may be rewritten as

$$q_1 \circ (q_2 \circ B) = \{zy, (zy)x(x, y, z), (zy)x^{-1}(x, y, z)^{-1}\}$$

(compare [4, Ch. 8]). The subloop of $(Q, \cdot, e)$ generated by the union of $q_1 \circ (q_2 \circ B)$ and B then contains the elements zy, x, and (x, y, z). As such, it has order 27. Thus $q_1 \circ (q_2 \circ B)$ is not of the form $q \circ B$ for any element q of Q. □

7.3. **Regular graphs in a Chein double.** Let $Q = S_3 \supset 2 = M(S_3, 2)$ be the Chein double of the symmetric group S_3. Having order 12, it is the smallest non-associative Moufang loop. Here is the multiplication table of Q:

1	2	3	4	5	6	7	8	9	10	11	12
2	1	4	3	6	5	8	7	12	11	10	9
3	6	5	2	1	4	9	10	11	12	7	8
4	5	6	1	2	3	10	9	8	7	12	11
5	4	1	6	3	2	11	12	7	8	9	10
6	3	2	5	4	1	12	11	10	9	8	7
7	8	11	10	9	12	1	2	5	4	3	6
8	7	12	9	10	11	2	1	4	5	6	3
9	12	7	8	11	10	3	4	1	6	5	2
10	11	8	7	12	9	4	3	6	1	2	5
11	10	9	12	7	8	5	6	3	2	1	4
12	9	10	11	8	7	6	5	2	3	4	1

Out of the $\binom{12}{2} = 66$ two-element subsets of Q, 54 have sectional degree ∞ and 12 have sectional degree 0.

Consider $S_1 = \{1, 2\}$. The left pseudo-orbit $S_1L(Q)$ of S_1 is

$$\{\{1, 2\}, \{3, 6\}, \{4, 5\}, \{7, 8\}, \{9, 12\}, \{10, 11\}\},$$

the union of all the pseudo-orbits of elements of $S_1L(Q)$ is $S_1L(Q)L(Q) = S_1L(Q) \cup \{\{3,4\},\{5,6\},\{7,10\},\{7,12\},\{8,9\},\{8,11\},\{9,10\},\{11,12\}\}$, and the union of all the pseudo-orbits of elements of $S_1L(Q)L(Q)$ is

$$S_1L(Q)L(Q)L(Q) = S_1L(Q)L(Q) \cup \{\{1,4\},\{1,6\},\{2,3\},\{2,5\}\},$$

a 1-$(12,2,3)$ design D_1, i.e., a 3-regular graph on 12 vertices. In fact, D_1 consists of two connected components, each isomorphic to the complete bipartite graph $K_{3,3}$.

Similarly, with $S_2 = \{1,7\}$ and $S_3 = \{1,8\}$ we obtain 3-regular graphs D_2, D_3, respectively. The three graphs D_1, D_2, D_3 are isomorphic and pairwise edge-disjoint, so $D = D_1 \cup D_2 \cup D_3$ is a 9-regular graph on 12 vertices. The complement of D in the complete graph K_{12} consists of four disjoint 3-cycles, and each of these 3-cycles corresponds to a translate of the normal subloop $S = \{1,3,5\}$ of Q.

8. Structural implications

This section applies the current Sylow theory to structural questions in certain loops: the smallest simple nonassociative Moufang loop in §8.1, commutative Moufang loops of exponent 3 in §8.2, and a Bol loop in §8.3.

8.1. **Klein 4-subgroups of the smallest Paige loop.** The automorphism group of the simple Moufang loop $\mathsf{PSL}_{1,3}(2)$ has two disjoint orbits (of respective lengths 63 and 252) on the set of Klein 4-subgroups [21, §5.2.6]. Members of the two orbits are identified as respectively having *positive type* and *negative type*. Hitherto, they have only been distinguished by the number of elementary abelian subgroups of order 8 in $\mathsf{PSL}_{1,3}(2)$ within which they are contained, namely 3 for the positive type and 1 for the negative type. The following result (paraphrasing part of the content of Table 2) shows how the types are distinguished within the current theory.

Proposition 8.1. *In the simple Moufang loop* $\mathsf{PSL}_{1,3}(2)$ *of order* 120*, the pseudo-orbit generated by a Klein* 4*-subgroup of positive type has co-length* 18*, while the pseudo-orbit generated by a Klein* 4*-subgroup of negative type has co-length* 6*.*

Remark 8.2. Proposition 8.1 provides examples where the lower bound given in Theorem 6.5 is sharp.

(a) For each Klein 4-subgroup V_4^- of negative type, the co-length of $6 = 2 \cdot (4-1)$ is explained entirely in terms of the two excessive classes constituted by elements of the unique elementary abelian subgroup of

order 8 that contains V_4^-. Indeed, V_4^- is not contained in any other subgroups ([21, Figure 5.1, p.59]).

(b) Each Klein 4-subgroup V_4^+ of positive type is contained in 3 subgroups of order 8 and 1 (alternating) subgroup of order 12 ([21, Figure 5.1, p.59]). The co-length of order $18 = (1 + 3 + 2) \cdot (4 - 1)$ is then accounted for by the excessive class V_4^+ itself, its unique complementary coset in each of the 3 elementary abelian subgroups of order 8 that contain it, and its two complementary cosets in the subgroup of order 12.

8.2. **Subgroups of commutative Moufang loops.** Suppose that L is a commutative Moufang loop of exponent 3. If S is a subgroup of order 3, Corollary 4.4 shows that S is sectional. The following result identifies when subgroups of order 9 are sectional.

Theorem 8.3. *Let L be a commutative Moufang loop of exponent 3. Then a subgroup S of L of order 9 is sectional if and only if it intersects the center non-trivially.*

Proof. First, suppose that S intersects the center non-trivially. Then S is of the form $\langle y \rangle \oplus \langle z \rangle$ with a non-trivial central element z. Consider two intersecting translates xS and $x'S$ of S in L, say with $xs_1 = x's_2$ for $s_1, s_2 \in S$. Then $x' = (xs_1)s_2^{-1} \in \langle x, y, z \rangle$. Since the associator $(x, y, z) = 1$, Moufang's Theorem implies that $G = \langle x, y, z \rangle$ is a subgroup of L. Then xS and $x'S$, as intersecting cosets of S inside the group G, actually coincide. It follows that S is sectional.

Now suppose that S has trivial intersection with the center. Then S is generated by two elements u, v such that the inner mapping $R(v, u) = R(v)R(u)R(vu)^{-1}$ is non-trivial. Suppose that w is an element of L which is not fixed by $R(v, u)$, i.e., which does not associate with u and v. This means that $\{w, v, u\}$ freely generates a free commutative Moufang loop of exponent 3, so the associator (w, v, u) does not lie in the subgroup S.

Consider the translates wS and $(wv)S$ of S. The translates overlap, since $wS \ni w1 = w = (wv)v^{-1} \in (wv)S$. Now suppose that $wS = (wv)S$. Since $vu \in S$, there is then an element s of S such that $w(vu) = (wv)s$. However, $w(vu) = (wv)[u(w, v, u)^{-1}]$, since

$$wR(v)R(u)R(vu)^{-1} = wR(v, u) = w(w, v, u)\,.$$

This implies that $u(w, v, u)^{-1} = s \in S$, leading to the contradiction $(w, v, u) \in S$. Thus the intersecting translates wS and $(wv)S$ are distinct, implying that S is not sectional. □

8.3. **Subloops of order** 4 **in a Bol loop of order** 16. Let B be a Bol loop with the following properties:

(a) $|B| = 16$;
(b) The center $Z(B)$ is trivial;
(c) B has exponent 4;
(d) The right nucleus $N_R(B)$ has order 8;
(e) B contains 7 involutions; and
(f) $|\mathrm{LMlt}\, B| = 128$.

In fact, B is known to be unique (up to isomorphism). In Moorhouse's nomenclature [14], it is the loop `16.7.2.443`. In the `LOOPS` package for `GAP`, it is identified as `LeftBolLoop(16,1)`. The following result was obtained using that package. Note that B contains elements of exponent 4.

Proposition 8.4. *In the Bol loop B, a subloop of order* 4 *is sectional if and only if it is isomorphic to the Klein* 4*-group. Indeed, cyclic subgroups of order* 4 *generate pseudo-orbits of length* 8*.*

Remark 8.5. The cyclic subgroups of order 4 are maximal subloops of B, so the co-length bound given by Theorem 6.5 is not sharp in this case.

Acknowledgement

We are grateful to anonymous referees for their extremely valuable comments on earlier versions of this paper. In particular, the notion of p-sectional subsets, and Proposition 2.14, were suggested by a referee.

References

[1] V.D. Belousov, "On the structure of distributive quasigroups" (Russian), *Mat. Sbornik* 50 (1960), 267–298.
[2] V.D. Belousov, *Foundations of the Theory of Quasigroups and Loops* (Russian), Nauka, Moscow, 1967.
[3] G. Bińczak, A.B. Romanowska, and J.D.H. Smith "Poset extensions, convex sets, and semilattice presentations," *Discrete Math.* **307** (2007), 1-11.
[4] R.H. Bruck, *A Survey of Binary Systems*, Springer, Berlin, 1971.
[5] O. Chein, "Moufang Loops of Small Order," *Memoirs of the Amer. Math. Soc.* No. 197, Amer. Math. Soc., Providence, RI, 1978.
[6] C.J. Colbourn and J.H. Dinitz (eds.), *Handbook of Combinatorial Designs*, 2nd. ed., Chapman & Hall/CRC, Boca Raton, FL, 2007.
[7] C.J. Colbourn and A. Rosa, *Triple Systems*, Clarendon Press, Oxford, 1999.
[8] I.A. Florja, "Bol quasigroups" (Russian), *Studies in General Algebra (Sem.)* (Russian), pp. 136–154, Akad. Nauk Moldav. SSR, Kishinev, 1965.
[9] S.M. Gagola III, "Conjugacy of Sylow 2-subloops of the Chein loops $M_{2n}(G, 2)$," *Comm. Algebra* **37** (2009), 2804–2810.

[10] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008, http://www.gap-system.org.
[11] M. Hall, "Automorphisms of Steiner triple systems," *IBM J. Res. Develop.* **4** (1960), 460–472.
[12] A.D. Keedwell, "The existence of Buchsteiner and conjugacy-closed quasigroups," *European J. Combin.* **30** (2009), 1382–1385.
[13] M.K. Kinyon, K. Pula and P. Vojtěchovský, "Incidence properties of cosets in loops," *J. Comb. Designs* **20** (2012), 179–197.
[14] E. Moorhouse, "Bol loops of small order," http://www.uwyo.edu/moorhouse/pub/bol/bol16.html
[15] G.P. Nagy and P. Vojtěchovský, LOOPS, version 2.2.0, package for GAP, http://www.math.du.edu/loops
[16] P.T. Nagy and K. Strambach, "Loops as invariant sections in groups, and their geometry," *Canad. J. Math.* **46** (1994), 1027–1056.
[17] L.J. Paige, "A class of simple Moufang loops," *Proc. Amer. Math. Soc.* **7** (1956), 471–482.
[18] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.
[19] J.D.H. Smith, "Sylow theory for quasigroups," *J. Comb. Designs* **23** (2015), 115–133.
[20] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.
[21] P. Vojtěchovský, *Finite simple Moufang loops*, Ph.D. thesis, Iowa State University, 2001. Available online at http://www.math.du.edu/~petr/data/papers/finite_simple_Moufang_loops.pdf
[22] H. Wielandt, "Ein Beweis für die Existenz von Sylowgruppen," *Arch. Math.* **10** (1959), 401–402.
[23] H.P. Young, "Affine triple systems and matroid designs," *Math. Z.* **132** (1973), 343–359.

[1,3]Department of Mathematics, University of Denver, Denver, Colorado 80208, U.S.A.

[2]Department of Mathematics, Iowa State University, Ames, Iowa 50011, U.S.A.

E-mail address: [1]mkinyon@math.du.edu
E-mail address: [2]jdhsmith@iastate.edu
E-mail address: [3]petr@math.du.edu
URL: [1]http://www.math.du.edu/~mkinyon/
URL: [2]http://www.math.iastate.edu/jdhsmith/
URL: [3]http://www.math.du.edu/~petr/