ON THE SMALLEST SIMPLE, UNIPOTENT BOL LOOP

K. W. JOHNSON[1] AND J. D. H. SMITH[2]

Abstract. Finite simple, unipotent Bol loops have recently been identified and constructed using group theory. However, the purely group-theoretical constructions of the actual loops are indirect, somewhat arbitrary in places, and rely on computer calculations to a certain extent. In the spirit of revisionism, this paper is intended to give a more explicit combinatorial specification of the smallest simple, unipotent Bol loop, making use of concepts from projective geometry and quasigroup theory along with the group-theoretical background. The loop has dual permutation representations on the projective line of order 5, with doubly stochastic action matrices.

1. Introduction

1.1. **Simple Bol loops.** The classification of the finite simple groups was readily applied and extended in quasigroup theory to yield a full classification of the finite simple Moufang loops [8, 12]. On the other hand, it transpires that almost all finite quasigroups are simple, being of rank 2 [5][16, §6.8]. Once the finite simple Moufang loops were classified, attention turned to the search for finite simple Bol loops. Using guidelines laid down by group theory [1, 2], they have now been found in such abundance that they do not appear to be amenable to a general classification [3, 11, 14, 15], despite the apparent intention of [1]. In fact, the known non-Moufang examples that have been studied so far all turn out to have rank 2. This leads to the *Rank* 2 *Problem*: Does the multiplication group of a finite, simple, non-Moufang Bol loop necessarily have a doubly transitive action on the loop?

Against this background, it nevertheless appears that the smallest simple, unipotent Bol loop N (whose order is 96) does warrant special attention. It owes its existence to the exceptional isomorphism between the groups $\mathrm{PGL}(2,5)$ and S_5. The loop N was previously constructed using the general methods of group theory, working mainly with the

2000 *Mathematics Subject Classification.* 20N05, 14N05.

Key words and phrases. Bol loop, projective line, permutation representation, revisionism, nonassociative geometry, Bruck loop.

symmetric group [3, 15]. However, the group-theoretical construction of the actual loop is indirect, and rather arbitrary in places. (Contrast §5.1 with the comments preceding Lemma 3.1 of [15]). The current paper aims to give a more explicit and combinatorial analysis of the loop, by using projective geometry and the theory of quasigroups. From this perspective, the loop N emerges as a nonassociative version of the projective line of order 5, much as noncommutative geometry leads to a deeper view of classical objects [6].

The Main Theorem of [1] admits the possibility of finite simple, unipotent Bol loops associated to each prime power of the form $q = 2^n + 1$ with $q \geq 5$. The primes of the form $2^n + 1$ are the *Fermat primes* $F_m = 2^{2^m} + 1$ [9, §2.5]. The only examples known are for $0 \leq m \leq 4$, but the possibility of further examples is currently open. Catalan's conjecture, now Mihăilescu's Theorem [13], implies that the only composite prime power of the form $q = 2^n + 1$ is $9 = 2^3 + 1$. In this context, it is worth noting that although there is an exceptional isomorphism $\mathrm{PSL}(2, 9) \cong A_6$, there is no corresponding isomorphism $\mathrm{PGL}(2, 9) \cong S_6$ [7, p.4],[10, Aufg. II.6]. The existence of finite simple, unipotent Bol loops over prime powers of the form $q = 2^n+1$ with $q > 5$ is an open question. If the answer were to turn out positive, it would not be inconceivable that the constraints imposed by the existence of the Bol loops could limit the number of possible Fermat primes.

1.2. **Plan of the paper.** The paper begins with background sections on quasigroup theory and projective geometry, approaching the exceptional isomorphism between $\mathrm{PGL}(2, 5)$ and S_5 from the projective geometry side. Section 4 describes the *nub* N_∞, the Boolean part of the loop N. Section 5 reprises the known group theory construction of the full loop N. Projective geometry gives a natural specification of the groups involved, and a detailed identification of each element of N. Section 6 (Table 2) provides a direct description of the maximal subloops of N (compare [3]). Section 7 exhibits the doubly-stochastic actions of N on the projective line of order 5, and uses them to obtain the maximality of the subloops from Section 6. This is one of the first structural applications of the new theory of quasigroup permutation representations.

Readers are referred to [16, 17] for concepts and conventions that are not otherwise explained explicitly.

2. Quasigroup theory

2.1. **Quasigroups.** A *quasigroup* $(Q, \cdot)$ is a set Q with a multiplication $Q \times Q \to Q; (p, q) \mapsto x \cdot y$ such that both the *right multiplications*

$R(q) : Q \to Q; x \mapsto x \cdot q$ and *left multiplications* $L(q) : Q \to Q; x \mapsto q \cdot x$ are permutations of Q for each q in Q. When there is no danger of confusion, multiplication may also be denoted by juxtaposition, which is taken to bind more strongly than multiplications written explicitly. Thus $xy \cdot z$ means $(x \cdot y) \cdot z$, for example. The *multiplication group* $\operatorname{Mlt} Q$ of a quasigroup Q is the subgroup of the permutation group $Q!$ generated by $\{R(q), L(q) \mid q \in Q\}$. The quasigroup Q is said to have *rank* 2 if $\operatorname{Mlt} Q$ acts doubly transitively on Q. In this case, Q is simple.

2.2. **Loops.** A *loop* $(L, \cdot, e)$ is a quasigroup $(L, \cdot)$ containing an *identity element* e such that $R(e) = L(e) = 1_L$, the identity map on L. A quasigroup $(Q, \cdot)$ is *idempotent* if $x \cdot x = x$ for x in Q. A loop $(L, +, e)$ is *unipotent* if $x + x = e$ for x in L. An idempotent quasigroup Q yields a unipotent loop $(Q', +, e)$ on the disjoint union $Q' = Q + \{e\}$ of the set Q with a singleton $\{e\}$. The loop multiplication $+$ is specified by setting $e + x = x = x + e$, $x + x = e$, and $x + y = x \cdot y$ for x and y distinct. Conversely, a unipotent loop $(L, +, e)$ yields an idempotent quasigroup $(L^*, \cdot)$ on the set $L^* = L \setminus \{e\}$ with $x \cdot x = x$ and $x \cdot y = x + y$ for distinct elements x, y of L^*. Then $L^{*\prime} \cong L$. Similarly, $Q'^* \cong Q$ for an idempotent quasigroup Q [16, §1.5].

2.3. **Bol loops.** A *right Bol loop* is a loop $(Q, \cdot, e)$ satisfying

$$R(x)R(y)R(x) = R(xy \cdot x)\,. \tag{2.1}$$

Setting $y = e$ in (2.1) shows that a right Bol loop $(Q, \cdot, e)$ is unipotent if and only if $R(x)^2 = 1$ for all x in Q. Thus unipotent Bol loops are sometimes described as having "exponent 2" [1, 15]. (Compare [16, §11.2] for exponents in quasigroup theory.)

2.4. **Loop transversals.** Let $T = \{e\} + T^*$ be a transversal to a subgroup H of a group $(G, \cdot, e)$. Define a multiplication $\circ$ on T by

$$tu \in H(t \circ u)\,. \tag{2.2}$$

The transversal T is said to be a *loop transversal* if $(T, \circ, e)$ is a loop. In this case, the loop $(T, \circ, e)$ is unipotent if T^* consists of involutions. The loop transversal T is a *Bol loop transversal* if $(T, \circ, e)$ is a right Bol loop.

2.5. **Right and left homogeneous spaces.** Suppose that P is a subquasigroup of a quasigroup $(Q, \cdot)$. The *relative left multiplication group* $\operatorname{LMlt}_Q P$ of P in Q is the subgroup of the permutation group $Q!$ generated by the set $\{L(p) \mid p \in P\}$ of left multiplications by ekements of P. The (*right*) *homogeneous space* $P\backslash Q$ is the set of orbits of $\operatorname{LMlt}_Q P$ on Q. For a group Q, these orbits are the right cosets of P.

If Q is finite, each element q of Q has a $|P\backslash Q| \times |P\backslash Q|$ row-stochastic (*right*) *action matrix* $R_{P\backslash Q}(q)$ with XY-entry

$$[R_{P\backslash Q}(q)]_{XY} = \frac{|X \cap R(q)^{-1}(Y)|}{|X|}$$

for elements X, Y of $P\backslash Q$ [16]. If Q is a group, then $R_{P\backslash Q}(q)$ is the usual permutation matrix of the action of q on $P\backslash Q$.

Dually, the *relative right multiplication group* $\mathrm{RMlt}_Q P$ of P in Q is the subgroup of $Q!$ generated by the set $\{R(p) \mid p \in P\}$ of right multiplications by ekements of P. The (*left*) *homogeneous space* Q/P is the set of orbits of $\mathrm{RMlt}_Q P$ on Q. If Q is finite, each element q of Q has a $|Q/P| \times |Q/P|$ column-stochastic (*left*) *action matrix* $L_{Q/P}(q)$ with YX-entry

$$[L_{Q/P}(q)]_{YX} = \frac{|L(q)^{-1}(Y) \cap X|}{|X|}$$

for elements Y, X of Q/P.

3. Projective geometry

3.1. **The projective line.** For a prime power q, the *projective line* $\mathrm{PG}(1, \mathrm{q})$ of order q is taken to be the disjoint union $\{\infty\} + \mathrm{GF}(q)$. The image of the group homomorphism

$$\mathrm{GL}(2,q) \to \mathrm{PG}(1,\mathrm{q})!\,; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \Big(x \mapsto \frac{ax+c}{bx+d}\Big) \tag{3.1}$$

is the *projective group* $\mathrm{PGL}(2,q)$ of order $(q+1)q(q-1)$. The projective group $\mathrm{PGL}(2,5)$ is generated by the *shift* $\lambda : x \mapsto x+1$, the *doubler* $\mu : x \mapsto 2x$, and the *negated inversion*

$$\nu : x \mapsto -x^{-1}\,. \tag{3.2}$$

The group $\mathrm{PGL}(2,5)$ has order 120, the order of the symmetric group S_5. The exceptional isomorphism $\mathrm{PGL}(2,5) \cong S_5$ will be apparent from §3.5 below.

The doubler is an automorphism of the additive group $\big(\mathrm{GF}(5), +\big)$, so the shift and multiplier generate the split extension

$$\big(\mathrm{GF}(5), +\big) \rtimes \mathrm{GF}(5)^* \tag{3.3}$$

of order 20, the stabilizer of ∞ in $\mathrm{PGL}(2,5)$. The stabilizer of the ordered pair $(\infty, 0)$ is $\langle\mu\rangle = \mathrm{GF}(5)^*$, which acts regularly on $\mathrm{GF}(5)^*$. Thus $\mathrm{PGL}(2,5)$ is sharply triply transitive on $\mathrm{PG}(1,5)$.

3.2. **The cross-ratio.** Let $\big((x_1, x_2), (x_3, x_4)\big)$ be an ordered pair of ordered pairs of points of the projective line, with $|\{x_1, x_2, x_3, x_4\}| > 2$. The *cross-ratio* is the element

$$X\big((x_1, x_2), (x_3, x_4)\big) = \frac{(x_1 - x_3)(x_2 - x_4)}{(x_1 - x_4)(x_2 - x_3)}$$

of $\{\infty\} + \mathrm{GF}(q)$ [18, §2.7]. An unordered pair $\big\{\{x_1, x_2\}, \{x_3, x_4\}\big\}$ of unordered pairs of distinct points is said to be *harmonically conjugate* if the well-defined relation $X\big((x_1, x_2), (x_3, x_4)\big) = -1$ holds [18, 2.7.5(ii)].

3.3. **The extended Lee metric.** The inhomogeneous coordinates for $\mathrm{PG}(1, 5)$ admit a metric structure. The set $\mathrm{GF}(5)$ of finite points carries the *Lee metric* $|x - y|$ of coding theory, given by

$$\{|x - y|\} = \{\pm(x - y)\} \cap \{0, 1, 2\}$$

[4, §8.2]. This metric is extended by setting $|x - \infty| = \infty$ for finite x. Note that λ preserves the extended Lee metric. Now μ interchanges the distances 1 and 2, while the negation μ^2 also preserves the extended Lee metric. Indeed, the subgroup $\langle \lambda, \mu^2 \rangle$ of $\mathrm{PGL}(2, 5)$ preserves the metric.

3.4. **Harmonically conjugate pairs.** The unordered pairs of points of the projective line $\mathrm{PG}(1, 5)$ of order 5 break up naturally into 5 triples a, b, c, d, e of pairs that are mutually harmonically conjugate. These triples are given in the columns of Table 1. The column labels identify the triples. Each triple contains a unique pair of each of the three possible distances ∞, 1, 2 in the extended Lee metric. Since $\mathrm{PGL}(2, 5)$ preserves cross-ratios, it permutes the set $\{a, b, c, d, e\}$.

	a	b	c	d	e
∞	$\infty 0$	$\infty 1$	$\infty 2$	$\infty 3$	$\infty 4$
1	23	34	40	01	12
2	14	20	31	42	03

TABLE 1. Harmonically conjugate pairs.

3.5. **The symmetric transpositions.** The projective group $\mathrm{PGL}(2, 5)$ contains the elements

$$0_1 = (cd) = \mu\nu = (\infty\ 0)(1\ 2)(3\ 4) : x \mapsto 2x^{-1} \tag{3.4}$$

and

$$0_2 = (be) = \nu\mu = (\infty\ 0)(1\ 3)(2\ 4) : x \mapsto 3x^{-1} \tag{3.5}$$

along with their successive conjugates by the shift $\lambda : x \mapsto x + 1$ or $(c\ d\ e\ a\ b)$. Note that $0_1^\nu = 0_2$. The 10 conjugate elements

$$0_1, 0_2, 1_1, 1_2, 2_1, 2_2, 3_1, 3_2, 4_1, 4_2$$

are known as *symmetric transpositions*. In (3.4) and (3.5), the first term identifies the image of ∞. The suffix indicates the Lee distance between the mutual images of the remaining finite points. These conventions extend to each symmetric transposition, so that 3_2 for example may be identified immediately as $(\infty 3)(0\ 2)(1\ 4)$. The second term in (3.4) and (3.5) describes the mapping as a transposition on the set $\{a, b, c, d, e\}$ of harmonically conjugate triples. Since the group $\mathrm{PGL}(2, 5)$ contains $\mu\nu = (c\ d)$ and the shift $\lambda = (c\ d\ e\ a\ b)$, it is directly seen to be isomorphic to the permutation group $\{a, b, c, d, e\}! = S_5$.

3.6. **Presentations.** With the generating set $\{\lambda, \mu, \nu\}$, the projective group $\mathrm{PGL}(2, 5)$ is presented by the relations

$$\lambda^5 = \mu^4 = \nu^2 = (\mu\nu)^2 = (\lambda\nu)^3 = \lambda^{-2}\lambda^\mu = 1\,. \tag{3.6}$$

The subgroup $\mathrm{PGL}(2, 5)_\infty$ or

$$\langle \lambda, \mu \mid \lambda^5 = \mu^4 = \lambda^{-2}\lambda^\mu = 1 \rangle \tag{3.7}$$

is the split extension (3.3), or the normalizer of a Sylow 5-subgroup of $\mathrm{PGL}(2, 5) \cong S_5$. The subgroup

$$\langle \mu, \nu \mid \mu^4 = \nu^2 = (\mu\nu)^2 = 1 \rangle \tag{3.8}$$

is the dihedral group D_4, the stabilizer in $\mathrm{PGL}(2, 5)$ of the doubleton $\{\infty, 0\}$.

4. The nub

4.1. **Sets of projective points.** Under the operation of symmetric difference, the power set $\mathcal{P}\big(\mathrm{PG}(1, 5)\big)$ of the projective line forms an abelian, unipotent loop or group of order 2^6. Singleton sets will be stripped of their braces, and the symmetric difference will be written simply by juxtaposition. The projective group $\mathrm{PGL}(2, 5)$ acts as a group of automorphisms of the unipotent loop, by an extension of its natural action on the projective line.

The power set $\mathcal{P}\big(\mathrm{PG}(1, 5)\big)$ decomposes as a disjoint union

$$\mathcal{P}\big(\mathrm{PG}(1, 5)\big) = \mathcal{P}\big(\mathrm{PG}(1, 5)\big)_0 + \mathcal{P}\big(\mathrm{PG}(1, 5)\big)_1 \tag{4.1}$$

of two subsets. The first summand $\mathcal{P}\big(\mathrm{PG}(1, 5)\big)_0$ consists of the subsets of even cardinality, while $\mathcal{P}\big(\mathrm{PG}(1, 5)\big)_1$ comprises the subsets of odd cardinality. The summands are invariant under the action of $\mathrm{PGL}(2, 5)$.

4.2. **The nub.** The full projective line $\mathrm{PG}(1,5)$ generates a 2-element subloop of $\mathcal{P}\big(\mathrm{PG}(1,5)\big)$, invariant under the action of $\mathrm{PGL}(2,5)$. Set

$$J = \mathcal{P}\big(\mathrm{PG}(1,5)\big) \Big/ \langle \mathrm{PG}(1,5) \rangle$$

for the quotient. The quotient inherits the unipotence of $\mathcal{P}\big(\mathrm{PG}(1,5)\big)$ and the automorphism group $\mathrm{PGL}(2,5)$. Since $|\mathrm{PG}(1,5)|$ is even, the quotient also admits a disjoint union decomposition $J = J_0 + J_1$ corresponding to (4.1). Elements of J_0 are called *even*, while elements of J_1 are *odd*. In the quotient, elements are denoted simply by their representatives, for example the even element $\infty 2 = 0134$. Within J, the set J_0 of even elements forms a 16-element subloop N_∞, known as the *nub*. The group $\mathrm{PGL}(2,5)$ acts as a transitive group of automorphisms on the corresponding 15-element idempotent quasigroup N_∞^*.

4.3. **Decomposing the nub.** For each element x of $\mathrm{GF}(5)$, the nub decomposes as a disjoint union $N_\infty = \infty_x + \overline{\infty}_x$. The summand $\overline{\infty}_x$ consists of those 8 doubletons which contain just one of the projective points x and ∞ from $\mathrm{PG}(1,5)$. The complementary summand ∞_x forms a subloop of N_∞. Then ∞_x^* forms a 7-element subquasigroup of N_∞^*, corresponding to a projective plane in $\mathrm{PG}(3,2)$. Among the 15 projective planes in the $\mathrm{PG}(3,2)$, the 5 different ∞_x^* are recognized as the planes containing six points corresponding to 2-element subsets of $\mathrm{GF}(5)$.

4.4. **Satellites of symmetric transpositions.** For each of the 10 symmetric transpositions x_d, with $x \in \mathrm{GF}(5)$ and $d = 1, 2$, certain elements of J are fixed by $x_d R(\infty x)$. These elements are known as the *satellites* of x_d. Write $S_{x,d} = \{k \in J \mid k x_d = k \infty x\}$ for the set of satellites of x_d. The satellites of $0_1 = (\infty 0)(1\ 2)(3\ 4)$ are

$$\infty,\ 0,\ \infty 12 = 034,\ \infty 34 = 012,\ 13,\ 14,\ 23,\ 24\,, \tag{4.2}$$

while the satellites of $0_2 = (\infty 0)(1\ 3)(2\ 4)$ are

$$\infty,\ 0,\ \infty 13 = 024,\ \infty 24 = 013,\ 12,\ 14,\ 32,\ 34\,. \tag{4.3}$$

These lists of 8 satellites are easily composed from the fourth terms of (3.4) and (3.5). For example, the doubleton satellites consist of an element from each of the two finite transpositions that make up the symmetric transposition. The corresponding lists for the remaining symmetric transpositions are compiled in similar fashion, or otherwise by applying successive powers of the shift λ to (4.2) and (4.3). For an alternative method, see §4.5 below.

4.5. **From satellites to the nub.** Let x be an element of GF(5). For each of the proper Lee distances $d = 1, 2$, there is a bijection $\eta_{x,d} : S_{x,d} \to \infty_x; k \mapsto k'$ known as *evening out*. For the 4 even satellites k of x_d, one sets $k' = k$, while $k' = \infty k$ for each of the 4 odd satellites k. In particular, $\infty' = e$.

For a symmetric transposition $x_d = (\infty\ x)(x_1\ x_2)(x_3\ x_4)$, the inverse map $\eta_{x,d}^{-1} : \infty_x \to S_{x,d}$ acts as the identity on the even satellites x_1x_3, x_1x_4, x_2x_3 and x_2x_4. It maps by

$$e \mapsto \infty\,,\ \infty x \mapsto x\,,\ x_1x_2 \mapsto \infty x_1x_2\,,\ x_3x_4 \mapsto \infty x_3x_4$$

to the odd satellites. Knowledge of $\eta_{x,d}^{-1}$ provides an alternative way to identify the satellites of the given symmetric transposition x_d.

5. Building the loop

5.1. **The group.** A group G is specified to fill the exact sequence

$$1 \longrightarrow \langle \mathrm{PG}(1,5) \rangle \longrightarrow \mathcal{P}\big(\mathrm{PG}(1,5)\big) \longrightarrow G \xrightarrow{\pi} \mathrm{PGL}(2,5) \longrightarrow 1 \tag{5.1}$$

of groups, so that $|G| = |J| \cdot |\mathrm{PGL}(2,5)| = 2^8 \cdot 3 \cdot 5$. The group G is generated by J and elements $\widetilde{\lambda}$, $\widetilde{\mu}$, $\widetilde{\nu}$. The homomorphism π from G to $\mathrm{PGL}(2,5)$ takes $\widetilde{\lambda}$ to λ, $\widetilde{\mu}$ to μ, $\widetilde{\nu}$ to ν, and J to $\{1\}$. The relations for G are given by the multiplication table of J, the conjugations

$$s^{\widetilde{\lambda}} = s\lambda\,,\ s^{\widetilde{\mu}} = s\mu\,,\ s^{\widetilde{\nu}} = s\nu$$

for s in J, and the inflated version

$$\widetilde{\lambda}^5 = \infty\widetilde{\mu}^4 = 124\widetilde{\nu}^2 = \infty 0(\widetilde{\mu}\widetilde{\nu})^2 = (\widetilde{\lambda}\widetilde{\nu})^3 = \widetilde{\lambda}^{-2}\widetilde{\lambda}^{\widetilde{\mu}} = 1$$

of (3.6).

Remark: The group G is described in [3, 15]. The set J_0 of even elements of J satisfies $J_0 = [G, J]$, in agreement with the notation of [15, Lemma 3.4].

5.2. **Lifting the symmetric transpositions.** For x in GF(5), define $\widetilde{x}_1 = \widetilde{\lambda}^{-x}(\widetilde{\mu}\widetilde{\nu})\widetilde{\lambda}^x$ and $\widetilde{x}_2 = \widetilde{\lambda}^{-x}(\widetilde{\nu}\widetilde{\mu})\widetilde{\lambda}^x$ by analogy with §3.5. Note that $\widetilde{x}_d$ maps under π to the symmetric transposition x_d for $d = 1, 2$. Now

$$\big(\infty \cdot \widetilde{0}_1\big)^2 = \infty(\infty\mu\nu)(\widetilde{\mu}\widetilde{\nu})^2 = \infty 0 \infty 0 = e\,.$$

The conjugacy class $\big(\infty \cdot \widetilde{0}_1\big)^G$ consists of the 80 involutions of the form

$$k \cdot \widetilde{x}_d \tag{5.2}$$

with $x \in \mathrm{GF}(5)$ and $d = 1, 2$, where k is a satellite of x_d. There are conjugation actions $\infty \cdot \widetilde{0}_1 \overset{\widetilde{\mu}^2}{\mapsto} 24 \cdot \widetilde{0}_1 \overset{23}{\mapsto} 13 \cdot \widetilde{0}_1$ and $24 \cdot \widetilde{0}_1 \overset{\infty 1}{\mapsto} 23 \cdot \widetilde{0}_1 \overset{14}{\mapsto} 14 \cdot \widetilde{0}_1$ as well as $\infty \cdot \widetilde{0}_1 \overset{23}{\mapsto} 0 \cdot \widetilde{0}_1$, $\infty \cdot \widetilde{0}_1 \overset{\infty 1}{\mapsto} \infty 34 \cdot \widetilde{0}_1$, and $\infty \cdot \widetilde{0}_1 \overset{\infty 3}{\mapsto} \infty 12 \cdot \widetilde{0}_1$.

Then $\widetilde{\nu}^{-1}$ conjugates $S_{0,1}\widetilde{0}_1$ to $S_{0,2}\widetilde{0}_2$. The remaining elements of the conjugacy class $\big(\infty\cdot\widetilde{0}_1\big)^G$ are obtained on conjugating $S_{0,1}\widetilde{0}_1$ and $S_{0,2}\widetilde{0}_2$ by successive powers of the lifted shift $\widetilde{\lambda}$.

5.3. **The loop transversal.** Consider the subgroup $H = \langle\widetilde{\lambda}, \widetilde{\mu}\rangle$ of G, which fills the exact sequence

$$1 \longrightarrow \langle\infty\rangle \longrightarrow H \xrightarrow{\pi} \langle\lambda, \mu\rangle \longrightarrow 1$$

of groups. In particular, (3.7) shows that $|H| = 2^3 \cdot 5$. Define the disjoint union $T = \{e\} + N_\infty^* + \big(\infty \cdot \widetilde{0}_1\big)^G$. Thus $|T| = 1 + 15 + 80 = 2^5 \cdot 3 = |G|/|H|$. By methods similar to those of [15], which will not be repeated here, T is shown to be a Bol loop transversal to H in G. In the notation of §4.5, one has $H\big(k \cdot \widetilde{x}_d\big) = H\big(k\eta_{x,d} \cdot \widetilde{x}_d\big)$ for $x \in \mathrm{GF}(5)$, $d = 1, 2$, and $k \in S_{x,d}$.

5.4. **The loop.** For x in $\mathrm{GF}(5)$ and $d = 1, 2$, define the formal coset $N_{x,d} = \infty_x \cdot x_d$ and the disjoint union $N_x = N_{x,1} + N_{x,2}$. The underlying set of the loop N is taken as the disjoint union

$$N = N_\infty + N_0 + N_1 + N_2 + N_3 + N_4 .$$

A projection

$$\pi : N \to \mathrm{PG}(1, 5) \tag{5.3}$$

is defined as the sum of the maps $N_y \to \{y\}$ over all projective points y. A bijection $\beta : T \to N$ is given by the sum of the identity map on the nub N_∞ and the maps $S_{x,d} \cdot \widetilde{x}_d \to N_{x,d}; k \cdot \widetilde{x}_d \mapsto k\eta_{x,d} \cdot x_d$ for $x \in \mathrm{GF}(5)$ and $d = 1, 2$, using (5.2) to identify arguments of these latter maps. The unipotent, right Bol loop structure $(N, \circ, e)$ on N is defined by requiring $\beta : T \to N$ to be a loop isomorphism, in which the domain loop structure $(T, \circ, e)$ is given by (2.2). It will often be convenient to abuse language slightly, assuming that β identifies T with N.

6. The maximal subloops

6.1. **Five maximal subloops.** For each x in $\mathrm{GF}(5)$, the 32-element disjoint union $M_x = N_\infty + N_x$ forms a subloop of N, which will emerge as a maximal proper subloop of N (§7.4). Conjugation by the lifted shift $\widetilde{\lambda}$ in G provides a series

$$M_0 \xrightarrow{\widetilde{\lambda}} M_1 \xrightarrow{\widetilde{\lambda}} M_2 \xrightarrow{\widetilde{\lambda}} M_3 \xrightarrow{\widetilde{\lambda}} M_4 \xrightarrow{\widetilde{\lambda}} M_0$$

of isomorphisms that permute these maximal subloops M_x cyclically, their respective subloops N_∞ remaining invariant. To describe the maximal subloops, it suffices to specify M_0.

M_0	$q \in \infty_0$	$s \in \overline{\infty}_0$	$q \cdot 0_1 \in \infty_0 \cdot 0_1$	$q \cdot 0_2 \in \infty_0 \cdot 0_2$
$p \in \infty_0$	pq	ps	$pq \cdot 0_1$	$pq \cdot 0_2$
$r \in \overline{\infty}_0$	rq	rs	$\infty 1(-rq) \cdot 0_2$	$\infty 4(-rq) \cdot 0_1$
$p \cdot 0_1$	$pq^{\mu\nu} \cdot 0_1$	$\infty 1(-p)s^{\nu\mu} \cdot 0_2$	pq	$\infty 1(-p)q$
$p \cdot 0_2$	$pq^{\nu\mu} \cdot 0_2$	$\infty 4(-p)s^{\mu\nu} \cdot 0_1$	$\infty 4(-p)q$	pq

TABLE 2. The multiplication table of M_0.

6.2. **The multiplication table of a maximal subloop.** Table 2 presents the multiplication table of the maximal subloop M_0. The multiplication in the nub $N_\infty = \infty_0 + \overline{\infty}_0$, denoted by juxtaposition, is taken to bind more strongly than the negation $x \mapsto -x$ acting on the nub. Recall that both ∞_0 and $\overline{\infty}_0$ are invariant under the action of the group (3.8), namely $\mathrm{PGL}(2,5)_{\{\infty,0\}}$. In the table, p and q denote elements of ∞_0, while r and s denote elements of $\overline{\infty}_0$. From the table, it is apparent that M_0 has the composition series $\{e\} < N_\infty < M_0$ with abelian quotients N_∞ and $\{N_\infty, N_0\}$. Thus M_0 is solvable.

7. Permutation representations

7.1. **The projective line of order 5 as a homogeneous space.** The description of the maximal subloops given in Section 6 shows that the right and left homogeneous spaces of the nub take the form

$$N_\infty \backslash N = N / N_\infty = \{N_\infty, N_0, N_1, N_2, N_3, N_4\},$$

which is readily identified with the projective line $\mathrm{PG}(1,5)$ of order 5 by means of the mapping (5.3). It follows that the loop N has right and left permutation actions on the projective line. Note that the nub is both right and left Lagrangean in N (i.e., $\mathrm{LMlt}_N N_\infty$ and $\mathrm{RMlt}_N N_\infty$ act semitransitively on N [16, §4.5]). This implies that the action matrices of N on the projective line are doubly stochastic [11, Th. 6.1].

7.2. **Right action on the projective line.** In the right action of N on the projective line $\mathrm{PG}(1,5)$, the doubly stochastic action matrices are actually permutation matrices. First, note that the elements of the nub act trivially. Now suppose that for $a \neq x$ in $\mathrm{GF}(5)$, one has

$$H\big(a' \cdot \widetilde{a}_e \cdot k \cdot \widetilde{x}_d\big) = H\big(b' \cdot \widetilde{b}_f\big) \tag{7.1}$$

for b in $\mathrm{GF}(5)$, $e, d, f = 1, 2$, and respective satellites a', k, b' of a_e, x_d, and b_f. Applying the homomorphism π to (7.1) yields

$$\infty H^\pi \big(a' \cdot \widetilde{a}_e \cdot k \cdot \widetilde{x}_d\big)^\pi = \infty H^\pi \big(b' \cdot \widetilde{b}_f\big)^\pi$$

or $ax_d = \infty a_e x_d = \infty b_f = b$, which will be written symbolically as

$$a \circ x_d = b\,. \tag{7.2}$$

Thus for x in GF(5) and $d = 1, 2$, each element $p \cdot x_d$ of $N_{x,d}$ (with p in ∞_x) acts on PG$(1, 5)$ as the permutation x_d.

REMARK: The right action of N on PGL$(1, 5)$ may be viewed as a quasigroup-theoretical implementation, for the case $q = 5$, of the object (G^*, H^*, K^*) that appears in the Main Theorem of [1].

7.3. **Left action on the projective line.** In the left action of N on the projective line PG$(1, 5)$, elements of the nub again act trivially. For p in ∞_0 and $d = 1, 2$, one has

$$L_{N/N_\infty}(p \cdot 0_d) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 1/2 & 0 \end{bmatrix}\,. \tag{7.3}$$

The remaining doubly stochastic action matrices are obtained using conjugation by powers of the shift.

Table 2 determines the form for the top left-hand corner of the matrix in (7.3). Double stochasticity then fixes the remaining entries of the first two columns and rows. For each element x of GF$(5)^*$, the column $[L_{N/N_\infty}(p \cdot 0_d)]_{*x}$ of (7.3) indexed by x is given by

$$\frac{1}{2}\left[R_{N_\infty \backslash N}(p \cdot x_1) + R_{N_\infty \backslash N}(p \cdot x_2)\right]_{*0}\,,$$

the average of the columns indexed by 0 in the two respective right action matrices. Using an extension of the symbolic notation of (7.2), $0 \circ x_1 = a$ and $0 \circ x_2 = b$ imply $0 \circ x = \frac{1}{2}(a + b)$.

7.4. **Maximality of the 32-element subloops.** Consider a subloop P of N containing M_0 and an element of a single coset $N_{x,d}$ with x in GF$(5)^*$. Since P contains N_∞, the shift of Table 2 by $\widetilde{\lambda}^x$ shows that P contains N_x. Applying the cube

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3/8 & 3/8 & 1/8 & 1/8 \\ 0 & 0 & 1/8 & 3/8 & 1/8 & 3/8 \\ 0 & 0 & 3/8 & 1/8 & 3/8 & 1/8 \\ 0 & 0 & 1/8 & 1/8 & 3/8 & 3/8 \end{bmatrix}$$

of (7.3) shows that P contains an element of the subset N_y for each y in $\mathrm{GF}(5)^*$. For each such y, the shift of Table 2 by $\widetilde{\lambda}^y$ then shows that P contains N_y Thus $P = N$.

References

[1] M. Aschbacher, *On Bol loops of exponent* 2, J. Alg. **288** (2005), 99–136.
[2] M. Aschbacher, M.K. Kinyon and J.D. Phillips, *Finite Bruck loops*, Trans. Amer. Math. Soc. **358** (2005), 3061–3075.
[3] B. Baumeister and A. Stein, *Self-invariant* 1*-factorizations of complete graphs and finite Bol loops of exponent* 2, Beiträge Algebra Geom. **51** (2010), 117-135.
[4] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, NY, 1968.
[5] P.J. Cameron, *Almost all quasigroups have rank* 2, Discr. Math. **106/107** (1992), 111–115.
[6] A. Connes, *Noncommutative Geometry*, Academic Press, San Diego, CA, 1994.
[7] J.H. Conway *et al.*, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
[8] S. Doro, *Simple Moufang loops*, Math. Proc. Camb. Phil. Soc. **83** (1978), 377–392.
[9] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers* (4th ed.), Oxford University Press, Oxford, 1960.
[10] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
[11] K.W. Johnson and J.D.H. Smith, *Matched pairs, permutation representations, and the Bol property*, Comm. Alg. **38** (2010), 2903–2914.
[12] M.W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Camb. Phil. Soc. **102** (1987), 33–47.
[13] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.
[14] G.P. Nagy, *A class of simple proper Bol loops*, Manuscripta Math. **127** (2008), 81-88.
[15] G. P. Nagy, *A class of finite simple Bol loops of exponent* 2, Trans. Amer. Math. Soc. **361** (2009), 5331-5343.
[16] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.
[17] J.D.H. Smith and A. B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.
[18] J.A. Todd, *Projective and Analytical Geometry*, Pitman, London, 1954.

[1] Department of Mathematics, Pennsylvania State University Abington, 1600 Woodland Avenue, Abington, PA19001, U.S.A.

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

E-mail address: [1]kwj1@psu.edu, [2]jdhsmith@iastate.edu
URL: http://www.orion.math.iastate.edu/jdhsmith/