Bol loops of odd prime exponent

Tuval Foguel

Department of Mathematics and Computer Science
Stillwell 426
Western Carolina University
Cullowhee, NC 28723 USA
tsfoguel@wcu.edu

Michael Kinyon

Department of Mathematics
2360 S Gaylord St
University of Denver
Denver CO 80208 USA
mkinyon@math.du.edu

Although any finite Bol loop of odd prime exponent is solvable, we show there exist such Bol loops with trivial center. We also construct finitely generated, infinite, simple Bruck loops of odd prime exponent for sufficiently large primes. This shows that the Burnside problem for Bruck loops has a negative answer.

Keywords: Bol loop, Bruck loop, Moufang loop, p-loop, central nilpotence, Bruck-Tarski monster.

2000 Mathematics Subject Classification: 20N05

1. Introduction

A *loop* $(Q, \cdot)$ consists of a set Q with a binary operation $\cdot : Q \times Q \to Q$ such that (i) for all $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$, and (ii) there exists $1 \in Q$ such that $1x = x1 = x$ for all $x \in Q$. A loop Q is said to be a (right) *Bol loop* if it satisfies the identity

$$[(xy)z]y = x[(yz)y] \tag{Bol}$$

for all $x, y, z \in Q$. For $x \in Q$, define the *right* and *left translations* by x by, respectively, $yR_x = yx$ and $yL_x = xy$ for all $y \in Q$. Then the Bol identity is equivalent to

$$R_x R_y R_x = R_{(xy)x}$$

1

for all $x, y \in Q$. Much of the literature on Bol loops (*e.g.*, [15]) works with the dual notion of *left* Bol loop defined by the identity $x[y(xz)] = [x(yx)]z$. Results for left Bol loops dualize trivially to results about right Bol loops. For background in loop theory, we refer the reader to [5,25]. Basic information about Bol loops, especially facts not explicitly cited below, can be found in [26].

Let Q be a loop. For $x \in Q$ and $n \in \mathbb{Z}$, set $x^n = 1R_x^n$. If Q is a Bol loop, then Q is *power-associative*, that is, $x^m x^n = x^{m+n}$ for all $x \in Q$, $m, n \in \mathbb{Z}$, and Q is also *right power-alternative*, that is, $R_x^n = R_{x^n}$ for all $x \in Q$, $n \in \mathbb{Z}$. Finite Bol loops satisfy the *elementwise Lagrange property*, that is, the order of any element divides the order of the loop. (It is still an open whether or not Bol loops satisfy the full Lagrange property: does the order of a subloop of a finite Bol loop divide the order of the loop?) A Bol loop is said to be *uniquely 2-divisible* if the squaring map $x \mapsto x^2$ is a bijection. If Q is a finite Bol loop, unique 2-divisibility is equivalent to every element of Q having finite odd order, and also to Q itself having odd order [8]. Bol loops of odd order satisfy the *Cauchy property*, that is, for each prime p, there exists an element of order p [8].

For p a prime, a power-associative loop is called a *p-loop* if every element has finite order which is some power of p, that is, for each x, there exists $n > 0$ such that $x^{p^n} = 1$. If Q is a finite Bol loop, then by the elementwise Lagrange and Cauchy properties, being a p-loop is equivalent to Q itself having order some power of p.

Two important subclasses of Bol loops are *Moufang loops* and *Bruck loops*. The former can be defined in various ways, for instance, as those Bol loops satisfying the antiautomorphic inverse property $(xy)^{-1} = y^{-1}x^{-1}$. Bruck loops are Bol loops satisfying the automorphic inverse property $(xy)^{-1} = x^{-1}y^{-1}$. The intersection of these two classes is the class of *commutative Moufang loops*.

The *multiplication group* of a loop Q is the group $\mathrm{Mlt}(Q) = \langle R_x, L_x | x \in Q \rangle$. The *inner mapping group* $\mathrm{Inn}(Q)$ is the stabilizer of the identity element $1 \in Q$. A subloop which is invariant under the action of $\mathrm{Inn}(Q)$ is said to be *normal*. An important fact about normal subloops we will use later is that they are *permutable*, that is, if H, K are subloops of a loop Q and if K is normal, then HK and KH are subloops of Q. A loop with no nontrivial normal subloops is *simple*.

The *right nucleus* of a loop Q is the set $N_r(Q) = \{a \in Q \mid (ax)y = a(xy) \; \forall x, y \in Q\}$, the *left nucleus* is $N_l(Q) = \{a \in Q \mid (xy)a = x(ya) \; \forall x, y \in Q\}$, the *middle nucleus* is $N_m(Q) = \{a \in Q \mid (xa)y = x(ay) \; \forall x, y \in Q\}$, and the *nucleus* is $N(Q) = N_r(Q) \cap N_m(Q) \cap N_l(Q)$. These are all subloops. In a Bol loop Q, $N_r(Q) = N_m(Q)$ is a normal subloop [8], but $N_l(Q)$ is not necessarily normal.

For a subset S of a loop Q, we borrow terminology from semigroup theory and define the *commutant of S in Q* to be the set $C_Q(S) = \{a \in Q \mid ax = xa \; \forall x \in S\}$. As usual, if $S = \{x\}$ is a singleton, we write $C_Q(x)$ instead of $C_Q(\{x\})$. The *commutant* of Q itself is $C(Q) = C_Q(Q)$. (This latter set is also known as the centrum or semicenter or commutative center.) Note that $C(Q) = \bigcap_{x \in Q} C_Q(x)$. The commutant of a Moufang loop is a subloop [25], but this is not generally true

in Bol loops or even Bruck loops [18]. It is, however, true that in a uniquely 2-divisible Bol loop, the commutant is a subloop [17]. Even in Moufang loops, the normality of the commutant remains an open problem. In §3, we show that *in a uniquely* 2-*divisible Bruck loop, the commutant is a normal subloop.*

The *center* of a loop Q is $Z(Q) = N(Q) \cap C(Q)$. This is exactly the fixed point subset of $\text{Inn}(Q)$. The notion of *upper central series* is defined in the same way as in group theory, and a loop is *centrally nilpotent* if it has a finitely terminating upper central series. As in group theory, a loop is *solvable* if it has a normal series with factors which are abelian groups. Centrally nilpotent loops are necessarily solvable.

Much has been learned about Bol loops in the last few years, especially thanks to work of Nagy. For about three decades, the existence of finite, simple, non-Moufang Bol loops was the main open problem in loop theory. Firstly, Nagy gave a very general construction of a large class of such loops [19]. The construction showed that not only are there many such loops (more than will likely allow for a classification any time soon), but there are also surprising examples. For instance, Nagy showed that there exist finite, simple, non-Moufang Bol loops of odd order [19]. This answered negatively a question of [8], and is in sharp contrast to the more specialized cases: every finite Bruck loop of odd order is solvable [10] and every finite Moufang loop of odd order is solvable [11].

Turning now to p-loops, we consider first $p = 2$. Finite Moufang 2-loops are centrally nilpotent [12]. There exist finite Bruck loops of exponent 2 with trivial center [16]; the smallest order at which this occurs is 16. More recently, building on earlier work of Aschbacher [4], Nagy constructed a finite simple Bol loop of exponent 2 and order 96 [21].

What of Bol p-loops for p an odd prime? Thanks to seminal work of Glauberman, it is known that every finite Bruck p-loop has nontrivial center [10], and every finite Moufang p-loop has nontrivial center [11]. It follows immediately by induction that such loops in either class are centrally nilpotent.

In the general case, the best positive result for a finite Bol p-loop is again due to Nagy: such a loop is solvable [20]. However, until recently, the following problem was considered to be open:

Does every finite Bol p-loop have nontrivial center?

In §2 we present examples for $p = 3$ showing that the answer to this question is no. As it turns out, our examples are related to a loop which has been in the literature since 1963, and which, suitably interpreted, would have already answered the question.

Finitely generated commutative Moufang loops are finite [5], and so it follows from Glauberman's results that for each odd prime p, a finitely generated commutative Moufang p-loop of finite exponent is centrally nilpotent. (This can, in fact, be shown directly for commutative Moufang loops [5].) One might then ask the following:

Is every finitely generated Bruck p-loop of finite exponent centrally nilpotent?

In §5, we answer this question negatively by constructing a family of Bruck loops we call *Bruck-Tarski monsters*, which are finitely generated, infinite and simple.

2. Finite Bol 3-loops with trivial center

While searching for particular types of projective planes, Keedwell gave an example of a normalized latin square of order 27 with certain properties. He published the example in two papers [13,14] in 1963 and 1965, respectively. Dénes and Keedwell later included the example in their well-known book on latin squares ([7], p. 50).

A normalized latin square is the Cayley table for a loop. It is obvious by inspection that the loop from Keedwell's latin square has exponent 3, but no other properties are immediately apparent. Perhaps because the example appeared in the latin square literature, the loop theory community seems to have been unaware of it.

Using the LOOPS package [22] for GAP [9], we analyzed Keedwell's loop and found that it was, in fact, a *left* Bol loop with trivial center. The loop has a normal associative subloop of order 9. Using tools from the LOOPS package, we took the transpose of the Cayley table to get a *right* Bol loop, and then constructed an isomorphic copy in which the normal subloop of order 9 is in the upper left corner.

Two loop structures $(Q, \cdot)$ and $(Q, \circ)$ on the same underlying set Q are said to be (principally) *isotopic* if there exist $a, b \in Q$ such that $x \circ y = xR_a^{-1} \cdot yL_b^{-1}$ where the translations are taken in $(Q, \cdot)$. Every isotope of a Bol loop is itself a Bol loop. Further, every loop isotopic to a Bol loop $(Q, \cdot)$ is isomorphic to an isotope of a particular form, namely one given by $x \circ y = xR_a \cdot yL_a^{-1}$ for $a \in Q$ [26].

We computed all principal isotopes of our modified version of Keedwell's loop, a task made easier since it is enough to consider isotopes of the form $x \circ y = xR_a \cdot yL_a^{-1}$. It turns out that there are exactly two isotopy classes. We present here a representative from each class in Tables 1 and 2.

We computed various structures attached to these loops. Besides the multiplication groups and inner mappings groups, we also computed the following. The *right* and *left multiplication groups* of a loop Q are $\mathrm{RMlt}(Q) = \langle R_x \mid x \in Q \rangle$ and $\mathrm{LMlt}(Q) = \langle L_x \mid x \in Q \rangle$, and their respective stabilizers of the identity element are the *right* and *left inner mapping groups* $\mathrm{LInn}(Q)$ and $\mathrm{RInn}(Q)$. Isotopic loops have isomorphic multiplication groups (both full and one-sided). The *associator subloop* $A(Q)$ is the smallest normal subloop of Q such that $Q/A(Q)$ is a group. The *derived subloop* Q' (sometimes called the commutator-associator subloop) is the smallest normal subloop of Q such that Q/Q' is an abelian group.

In the discussion that follows, Q refers to either of the two loops.

- $G := \mathrm{Mlt}(Q) = \mathrm{LMlt}(Q)$ is a solvable group of order $2^6 3^7$ and derived length 3. The derived subgroup G' has order $2^6 3^6$, while G'' is elementary abelian of order 3^5. G itself is a semidirect product of C_3 with G' and is

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
2	3	1	5	6	4	8	9	7	15	13	14	18	16	17	12	10	11	22	23	24	25	26	27	19	20	21
3	1	2	6	4	5	9	7	8	17	18	16	11	12	10	14	15	13	25	26	27	19	20	21	22	23	24
4	5	6	7	8	9	1	2	3	14	15	13	17	18	16	11	12	10	26	27	25	20	21	19	23	24	22
5	6	4	8	9	7	2	3	1	16	17	18	10	11	12	13	14	15	20	21	19	23	24	22	26	27	25
6	4	5	9	7	8	3	1	2	12	10	11	15	13	14	18	16	17	23	24	22	26	27	25	20	21	19
7	8	9	1	2	3	4	5	6	18	16	17	12	10	11	15	13	14	24	22	23	27	25	26	21	19	20
8	9	7	2	3	1	5	6	4	11	12	10	14	15	13	17	18	16	27	25	26	21	19	20	24	22	23
9	7	8	3	1	2	6	4	5	13	14	15	16	17	18	10	11	12	21	19	20	24	22	23	27	25	26
10	11	12	13	14	15	16	17	18	19	21	20	25	27	26	22	24	23	1	3	2	7	9	8	4	6	5
11	12	10	14	15	13	17	18	16	27	26	25	24	23	22	21	20	19	8	7	9	5	4	6	2	1	3
12	10	11	15	13	14	18	16	17	23	22	24	20	19	21	26	25	27	6	5	4	3	2	1	9	8	7
13	14	15	16	17	18	10	11	12	21	20	19	27	26	25	24	23	22	9	8	7	6	5	4	3	2	1
14	15	13	17	18	16	11	12	10	26	25	27	23	22	24	20	19	21	4	6	5	1	3	2	7	9	8
15	13	14	18	16	17	12	10	11	22	24	23	19	21	20	25	27	26	2	1	3	8	7	9	5	4	6
16	17	18	10	11	12	13	14	15	20	19	21	26	25	27	23	22	24	5	4	6	2	1	3	8	7	9
17	18	16	11	12	10	14	15	13	25	27	26	22	24	23	19	21	20	3	2	1	9	8	7	6	5	4
18	16	17	12	10	11	15	13	14	24	23	22	21	20	19	27	26	25	7	9	8	4	6	5	1	3	2
19	20	21	22	23	24	25	26	27	1	7	4	6	3	9	8	5	2	10	18	14	12	17	13	11	16	15
20	21	19	23	24	22	26	27	25	5	2	8	7	4	1	3	9	6	16	15	11	18	14	10	17	13	12
21	19	20	24	22	23	27	25	26	9	6	3	2	8	5	4	1	7	13	12	17	15	11	16	14	10	18
22	23	24	25	26	27	19	20	21	2	8	5	4	1	7	9	6	3	15	11	16	14	10	18	13	12	17
23	24	22	26	27	25	20	21	19	6	3	9	8	5	2	1	7	4	12	17	13	11	16	15	10	18	14
24	22	23	27	25	26	21	19	20	7	4	1	3	9	6	5	2	8	18	14	10	17	13	12	16	15	11
25	26	27	19	20	21	22	23	24	3	9	6	5	2	8	7	4	1	17	13	12	16	15	11	18	14	10
26	27	25	20	21	19	23	24	22	4	1	7	9	6	3	2	8	5	14	10	18	13	12	17	15	11	16
27	25	26	21	19	20	24	22	23	8	5	2	1	7	4	6	3	9	11	16	15	10	18	14	12	17	13

Table 1. Right Bol loop 1 of order 27 and exponent 3 with trivial center.

6   *Tuval Foguel and Michael Kinyon*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
2	3	1	5	6	4	8	9	7	11	12	10	14	15	13	17	18	16	20	21	19	23	24	22	26	27	25
3	1	2	6	4	5	9	7	8	12	10	11	15	13	14	18	16	17	21	19	20	24	22	23	27	25	26
4	6	5	1	3	2	8	9	7	18	17	16	11	10	12	15	14	13	27	26	25	20	19	21	24	23	22
5	4	6	2	1	3	9	7	8	16	18	17	12	11	10	13	15	14	25	27	26	21	20	19	22	24	23
6	5	4	3	2	1	7	8	9	17	16	18	10	12	11	14	13	15	26	25	27	19	21	20	23	22	24
7	8	9	8	9	7	1	3	2	27	26	25	20	19	21	24	23	22	4	6	5	16	18	17	14	13	15
8	9	7	9	7	8	2	1	3	25	27	26	21	20	19	22	24	23	6	5	4	17	16	18	15	14	13
9	7	8	7	8	9	3	2	1	26	25	27	19	21	20	23	22	24	5	4	6	18	17	16	13	15	14
10	14	18	16	17	13	24	25	26	1	6	5	8	7	9	2	4	3	21	20	19	27	23	22	11	12	15
11	13	17	18	15	16	25	27	24	3	1	6	9	8	7	4	2	5	19	22	23	21	26	20	12	10	18
12	15	16	17	13	18	27	24	25	2	3	1	7	9	8	5	6	4	20	23	22	26	21	27	10	11	16
13	16	12	14	18	15	20	21	19	8	9	7	6	5	4	3	1	2	26	27	24	11	10	12	17	18	10
14	18	13	15	16	17	22	20	21	7	8	9	4	6	5	1	3	2	24	25	26	10	12	11	11	14	13
15	17	14	18	15	16	24	22	23	9	7	8	5	4	6	2	1	3	25	26	27	12	11	10	14	15	18
16	10	15	13	14	12	26	23	24	4	5	3	1	2	6	9	7	8	22	19	20	14	13	15	16	10	11
17	12	11	15	16	13	27	25	26	6	4	5	2	3	1	7	8	9	23	20	21	15	14	13	18	17	14
18	11	10	14	18	17	23	24	22	5	6	4	3	1	2	8	9	7	21	18	19	13	15	14	10	16	17
19	23	27	26	25	24	4	6	5	21	19	20	26	27	25	22	23	21	1	3	2	8	9	7	18	14	13
20	21	22	27	26	25	6	5	4	20	22	23	25	27	26	19	20	18	3	1	2	9	7	8	12	17	16
21	22	26	25	27	23	5	4	6	19	23	22	27	25	26	20	21	19	2	3	1	7	8	9	15	11	10
22	24	21	20	19	27	16	17	18	27	21	26	11	10	12	14	15	13	8	9	7	3	1	2	5	6	4
23	25	20	19	21	22	18	16	17	23	26	21	10	12	11	13	14	15	9	7	8	1	3	2	6	4	5
24	22	23	21	20	26	17	18	16	22	20	27	12	11	10	15	13	14	7	8	9	2	1	3	4	9	6
25	26	27	24	22	23	14	15	13	11	12	10	17	18	16	10	13	18	27	24	25	5	6	4	1	2	3
26	25	27	23	24	22	13	14	15	12	10	11	18	16	17	11	18	12	24	20	21	6	4	5	2	3	1
27	26	25	24	23	22	15	13	14	15	18	16	10	17	18	16	14	17	23	21	20	4	5	6	3	1	2

Table 2. Right Bol loop 2 of order 27 and exponent 3 with trivial center.

also a semidirect product of a subgroup of order $2^6 3$ (the group $[192,3]$, according to GAP [9]) with G''.

(Note that if the order of G were a power of 3, then by a theorem of A. A. Albert, the centers of the two loops would be nontrivial [2].)

- $H := \mathrm{Inn}(Q) = \mathrm{LInn}(Q)$ is a solvable group of order $2^6 3^4$ and derived length 2. H' is elementary abelian of order 3^4 and H itself factors as a semidirect product of an abelian subgroup of order 2^6 with H'.
- $K := \mathrm{RMlt}(Q)$ is a nilpotent group of order 3^5 and nilpotency class 2. GAP [9] identifies it as group $[243, 37]$, a group with rank 3. $K' = Z(K)$ is elementary abelian of order 9 and $K/Z(K)$ is also elementary abelian.
- $\mathrm{RInn}(Q)$ is an elementary abelian group of order 9.
- $N_r(Q) = N_m(Q) = 1$.
- $C(Q) = 1$.
- $N_l(Q) = A(Q) = Q'$ is an elementary abelian group of order 9 (the upper left corner of both tables). This is the unique nontrivial normal subloop.

3. Commutants of uniquely 2-divisible Bruck loops

As mentioned in the introduction, in a uniquely 2-divisible Bol loop Q, the commutant $C(Q)$ is a subloop. In this section we address the normality of this subloop in uniquely 2-divisible Bruck loops.

A subloop is normal if it is invariant under the action of $\mathrm{Inn}(Q)$. The group $\mathrm{Inn}(Q)$ is generated by the following permutations:

$$R_{x,y} = R_x R_y R_{xy}^{-1} \qquad T_x = R_x L_x^{-1} \qquad L_{x,y} = L_x L_y L_{yx}^{-1}$$

for all $x, y \in Q$. In a Bruck loop, the right inner mappings $R_{x,y}$ play a special role. The following result can be found in various sources; see, *e.g.*, [15] (translating between left and right Bruck loops).

Proposition 3.1. *In a Bruck loop, each $R_{x,y}$ is an automorphism.*

Theorem 3.1. *Let Q be a uniquely 2-divisible Bol loop such that each $R_{x,y}$ is an automorphism. Then $C(Q)$ is a normal subloop.*

Proof. The commutant $C(Q)$ is fixed by each T_x, $x \in Q$. It is clear from the definition of $C(Q)$ that it is invariant under the action of automorphisms, and so it follows that $cR_{x,y} \in C(Q)$ for all $x, y \in Q$, $c \in C(Q)$. It is thus enough to check that for all $c \in C(Q)$, $x, y \in Q$, we have $cL_{x,y} \in C(Q)$. Now for fixed $x, y \in Q$, set $z = cL_{x,y}$, and let $u = y^{1/2}$. We compute

$$(xy)z = x(yc) = x(cy) = x[(cu)u] = x[(uc)u][(xu)c]u = [c(xu)]u$$

using the right alternative property in the third equality and (BOL) in the fifth equality. Thus

$$[(xy)z](xy)^{-1} = \{[c(xu)]u\}(xy)^{-1} = \{[c(xu)]u\}(xu^2)^{-1} = cR_{xu,u} \,.$$

Therefore $[(xy)z](xy)^{-1} \in C(Q)$. But then $(xy)z = \{[(xy)z](xy)^{-1}\}(xy) = (xy)\{[(xy)z](xy)^{-1}\}$. Canceling, we have $z = [(xy)z](xy)^{-1}$, and so $z \in C(Q)$, as claimed. □

Corollary 3.1. *If Q is a uniquely 2-divisible Bruck loop, then $C(Q)$ is a normal subloop.*

4. Twisted subgroups and uniquely 2-divisible Bruck loops

In this section, we briefly review some facts about twisted subgroups, and a standard construction of Bruck loops.

Recall that a subset T of a group G is a *twisted subgroup* of G if (i) $1 \in T$, (ii) $T^{-1} = T$, and (iii) $xTx \subseteq T$ for all $x \in T$ [3,8].

Let G be a group and suppose $\tau \in \mathrm{Aut}(G)$ has order 2. A typical example of a twisted subgroup which is not a subgroup is the set $K(\tau) = \{g \in G \mid g^\tau = g^{-1}\}$.

If T is a twisted subgroup, the *Aschbacher radical* of T is the set $T' = \{x_1 \cdots x_n \mid x_1^{-1} \cdots x_n^{-1} = 1, x_i \in T\}$. This is a normal subgroup of G [3], and it also measures whether or not T arises as a set of inverted elements of an involutory automorphism in the case where T generates G.

Proposition 4.1 ([3], Thm. 2.2; [8], Prop. 3.9). *Let G be a group, $T \subseteq G$ a twisted subgroup and assume $\langle T \rangle = G$. There exists $\tau \in \mathrm{Aut}(G)$ with $\tau^2 = 1$ such that $T \subseteq K(\tau)$ if and only if $T' = 1$.*

A twisted subgroup T of a group G is said to be *uniquely 2-divisible* if each $x \in T$ has a unique square root in T, that is, a unique element $x^{1/2} \in T$ such that $(x^{1/2})^2 = x$. On such a twisted subgroup, we may define a new binary operation $\odot : T \times T \to T$ by

$$x \odot y := (yx^2y)^{1/2}$$

for $x, y \in T$. Following Glauberman [10], we denote the magma $(T, \odot)$ by $T(1/2)$. The following properties are straightforward to verify [10,8]. (Note that in [10,8], the operation is $x \odot y = (xy^2x)^{1/2}$, which gives a *left* Bruck loop.)

- $T(1/2)$ is a uniquely 2-divisible Bruck loop.
- Integer powers of elements in T formed in G agree with those in $T(1/2)$. Thus an element has finite order in T if and only if it has the same order in $T(1/2)$.
- If $K \subseteq T$ is a subloop of $T(1/2)$, then K is a twisted subgroup of G.

5. Bruck-Tarski Monsters

A *Tarski monster* $\mathcal{T}$ is an infinite group in which every nontrivial proper subgroup is cyclic of order a fixed prime p. A Tarski monster is a simple group. Such groups were constructed by Ol'shanskii [23] for every $p > 10^{75}$. For more detail about these groups, see [24].

One can clearly make sense of the notion of a Tarski monster for any class of power-associative loops. Here we consider the following.

Definition 5.1. A *Bruck-Tarski monster* is an infinite Bruck loop in which every nontrivial proper subloop is cyclic of prime order p.

An immediate consequence of this definition is that *a Bruck-Tarski monster is a two-generated loop of exponent p.*

Theorem 5.1. *A Bruck-Tarski monster $\mathcal{BT}$ is a simple loop.*

Proof. Let $\mathcal{K}, \mathcal{H}$ be distinct proper subloops of $\mathcal{BT}$ which are cyclic groups of prime order p. If $\mathcal{K}$ is a normal subloop, then $\mathcal{K}$ is permutable, and so $\mathcal{HK}$ is a subloop. But $p < |\mathcal{HK}| < \infty$, a contradiction. Therefore the only normal subloops of $\mathcal{BT}$ are trivial, and so $\mathcal{BT}$ is a simple loop. □

Corollary 5.1. *If $\mathcal{BT}$ is a Bruck-Tarski monster, then $N_r(\mathcal{BT}) = N_m(\mathcal{BT}) = C(\mathcal{BT}) = 1$.*

Proof. The right and middle nuclei coincide in any Bol loop and are normal. The triviality of the commutant follows from Corollary 3.1. □

Now we will show that Bruck-Tarski monsters exist. Firstly, we need the following.

Lemma 5.1. *If $\mathcal{T}$ is a Tarski monster group, then $\mathrm{Aut}(\mathcal{T})$ contains no involutions.*

Proof. Suppose $\iota \in \mathrm{Aut}(\mathcal{T})$ is an involution. Let $G = \mathcal{T}\langle i \rangle$ be the semidirect product of $\mathcal{T}$ by $\langle i \rangle$. Then by ([28], 14.3.8), either $Z(G)$ contains an involution or G has a proper infinite subgroup with nontrivial center. In either case, we have a contradiction. □

Theorem 5.2. *If $\mathcal{T}$ is a Tarski monster, then $\mathcal{T}(1/2)$ is a Bruck-Tarski monster.*

Proof. Suppose that $\mathcal{K} \neq 1$ is a subloop of $\mathcal{T}(1/2)$ which is not a cyclic group of prime order p. Then $\mathcal{K}$ is a twisted subgroup of $\mathcal{T}$ and $\mathcal{T} = \langle \mathcal{K} \rangle$. Since $\mathrm{Aut}(\mathcal{T})$ contains no involutions (Lemma 5.1), it follows from Proposition 4.1 that $\mathcal{K}' > 1$. But $\mathcal{T}$ is a simple group, so $\mathcal{T} = \mathcal{K}' \subseteq \mathcal{K}$. Thus as a loop, $\mathcal{K} = \mathcal{T}(1/2)$. □

In 1902, Burnside introduced what is now known as the Burnside Problem [6]: Is a finitely generated periodic group of bounded exponent necessarily finite? Of course, one can formulate the problem more generally for power-associative loops as follows:

Given a class $\mathcal{P}$ of power-associative loops, is a loop from $\mathcal{P}$ which is finitely generated, periodic and of bounded exponent necessarily finite?

For the class $\mathcal{P}$ of all groups, the question was answered negatively in 1968 by Adian and Novikov [1], and is now also seen to be negative by the existence of Tarski monsters. On the other hand, the answer is affirmative when $\mathcal{P}$ is the class of solvable groups ([28], 5.4.11) or when $\mathcal{P}$ is the class of commutative Moufang loops ([5], Thm. 11.3). We now have an answer for the class of Bruck loops.

Corollary 5.2. *The Burnside problem for Bruck loops has a negative answer.*

Proof. A Bruck-Tarski monster is a finitely generated, but infinite periodic Bruck loop of bounded exponent. $\qquad\square$

We conclude with a few properties of Bruck-Tarski monsters constructed from Tarski monster groups. Given a group G and $x, y \in G$, we use the usual notation $x^y = y^{-1}xy$ and $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$.

Theorem 5.3. *Let $\mathcal{T}$ is a Tarski monster. If $1 \neq x \in \mathcal{T}$, then $C_{\mathcal{T}(1/2)}(x) = \langle x \rangle$.*

Proof. Clearly $\langle x \rangle \subseteq C_{\mathcal{T}(1/2)}(x)$. For the converse, suppose that $x, y \in \mathcal{T}(1/2)$ lie in distinct cyclic subloops, and assume that $y \in C_{\mathcal{T}(1/2)}(x)$. Then $x \odot y = y \odot x$ iff $(yx^2y)^{1/2} = (xy^2x)^{1/2}$ iff $yx^2y = xy^2x$ iff $[x, y] = [x^{-1}, y^{-1}]$. Thus $[x, y]xy = [x^{-1}, y^{-1}]xy = xy[x, y]$, that is, $xy \in C_{\mathcal{T}}([x, y]) = \langle [x, y] \rangle$. Thus xy generates $\langle [x, y] \rangle$. Now $(xy)^x = (xy)^{y^{-1}} = yx = xy[y, x] = xy[x, y]^{-1} \in \langle [x, y] \rangle$. Since x and y generate $\mathcal{T}$, this shows $\langle [x, y] \rangle$ is normal in $\mathcal{T}$. Since $\mathcal{T}$ is simple, either $\langle [x, y] \rangle = 1$ or $\langle [x, y] \rangle = \mathcal{T}$, which in either case is a contradiction. $\qquad\square$

Theorem 5.4. *If $\mathcal{T}$ is a Tarski monster, then $N_l(\mathcal{T}(1/2)) = 1$.*

Proof. Assume that $1 \neq a \in N_l(\mathcal{T}(1/2))$. Then for all $x, y \in \mathcal{T}(1/2)$, we have $a \odot (x \odot y) = (a \odot x) \odot y$, that is, $((yx^2y)^{1/2}a^2(yx^2y)^{1/2})^{1/2} = (yxa^2xy)^{1/2}$. Squaring both sides, we get $(yx^2y)^{1/2}a^2(yx^2y)^{1/2} = yxa^2xy$, or equivalently,

$$x^{-1}y^{-1}(yx^2y)^{1/2}a^2(yx^2y)^{1/2}y^{-1}x^{-1} = a^2 \,.$$

But $x^{-1}y^{-1}(yx^2y)^{1/2}(yx^2y)^{1/2}y^{-1}x^{-1} = 1$, and therefore $x^{-1}y^{-1}(yx^2y)^{1/2} \in C_{\mathcal{T}}(a^2) = \langle a \rangle$ for all $x, y \in \mathcal{T}$. Suppose that for some $x, y \in \mathcal{T}$, $x^{-1}y^{-1}(yx^2y)^{1/2}$ generates $\langle a \rangle$. For every $z \in \mathcal{T}$, $(x^{-1}y^{-1}(yx^2y)^{1/2})^z = (x^z)^{-1}(y^z)^{-1}(y^z(x^z)^2y^z)^{1/2} \in \langle a \rangle$, and so $\langle a \rangle$ is a normal subgroup, a contradiction. Thus for all $x, y \in \mathcal{T}$, $x^{-1}y^{-1}(yx^2y)^{1/2} = 1$, or $yx^2y = (yx)^2$ or $xy = yx$, another contradiction. Therefore $N_l(\mathcal{T}(1/2)) = 1$. $\qquad\square$

References

[1] S. I. Adian and P. S. Novikov, Infinite periodic groups I, II, III, *Izv. Akad. Nauk SSSR Ser. matem.* **32** No. 1, 2, 3 (1968), 212-244, 251-524, 709–731.

[2] A.A. Albert, Quasigroups I, *Trans. Amer. Math. Soc.* **54** (1943) 507–520.

[3] M. Aschbacher, Near subgroups of finite groups, *J. Group Theory* **1** (1998) 113–129.

[4] M. Aschbacher, Bol loops of exponent 2, *J. Algebra* **288** (2005), 99–136.

[5] R. H. Bruck, *A Survey of Binary Systems* Springer-Verlag, Berlin, 1971

[6] W. Burnside, An unsettled question in the theory of discontinuous groups, *Quart. J. Pure and Appl. Math.* **33** (1902), 2330-238.

[7] J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Academic Press, New York-London, 1974.

[8] T. Foguel, M. K. Kinyon and J. D. Phillips, On twisted subgroups and Bol loops of odd order, *Rocky Mountain Math. J.* **36**, no.1 (2006) 183-212.

[9] The GAP Group, GAP – *Groups, Algorithms, and Programming*, Version 4.4.12, 2008, http://www.gap-system.org

[10] G. Glauberman, On loops of odd order I, *J. Algebra* **1** (1964), 374–396.

[11] G. Glauberman, On loops of odd order II, *J. Algebra* **8** (1968), 393–414.

[12] G. Glauberman and C. R. B Wright, Nilpotence of finite Moufang 2-loops, *J. Algebra* **8** (1968), 415–417.

[13] A. D. Keedwell, On the order of projective planes with characteristic, *Rend. Mat. e Appl.* (5) **22** (1963), 498–530.

[14] A. D. Keedwell, A search for projective planes of a special type with the aid of a digital computer, *Math. Comp.* **19** (1965), 317–322

[15] H. Kiechle, *Theory of K-loops*, Lecture Notes in Mathematics **1778**, Springer-Verlag, Berlin, 2002.

[16] H. Kiechle and G. P. Nagy, On the extension of involutorial Bol loops, *Abh. Math. Sem. Univ. Hamburg* **72** (2002), 235–250.

[17] M. K. Kinyon and J. D. Phillips, Commutants of Bol loops of odd order, *Proc. Amer. Math. Soc.* **132** (2004), 617–619.

[18] M. K. Kinyon, J. D. Phillips and P. Vojtěchovský, When is the commutant of a Bol loop a subloop? *Trans. Amer. Math. Soc.* **360** (2008), 2393–2408.

[19] G. P. Nagy, A class of simple proper Bol loops, *Manuscripta Math.* **127** (2008), 81–88.

[20] G. P. Nagy, Some remarks on simple Bol loops, *Comment. Math. Univ. Carolin.* **49** (2008), 259–270.

[21] G. P. Nagy, A class of finite simple Bol loops of exponent 2, *Trans. Amer. Math. Soc.* **361** (2009), 5331–5343.

[22] G. P. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops*, version 2.1.0, package for GAP, http://www.math.du.edu/loops.

[23] A. Yu. Ol'sanskii, An infinite group with subgroups of prime order, *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980), 309-321.

[24] A. Yu. Ol'sanskii, *Geometry of Defining Relations in Groups*, Kluwer, Dordrecht, 1991.

[25] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990.

[26] D. A. Robinson, Bol loops, *Trans. Amer. Math. Soc.* **123** (1966), 341–354.

[27] D. A. Robinson, Some open questions on Bol loops, mimeographed notes, *Oberwolfach Conference on Bol and Moufang Loops*, 1976.

[28] D. J. S. Robinson, *A course in the theory of groups*, Springer-Verlag, New York, 1996.