# BRUCK LOOPS WITH ABELIAN INNER MAPPING GROUPS

J. D. PHILLIPS AND DAVID STANOVSKÝ

Abstract. Bruck loops with abelian inner mapping groups are centrally nilpotent of class at most 2.

## 1. The theorem

A *loop* $(Q, \cdot)$ is a set $Q$ with a binary operation $\cdot$ such that (i) for each $x \in Q$, the *left translation* $L(x) : Q \to Q; y \mapsto xy$ and the *right translation* $R(x) : Q \to Q; y \mapsto yx$ are bijections, and (ii) there exists $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$. The left and right translations generate the *multiplication group* $\mathrm{Mlt}(Q) = \langle L(x), R(x) \mid x \in Q \rangle$. The *inner mapping group* $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1$ is the stabilizer of $1 \in Q$. Standard references for the theory of loops are [2, 4, 25].

The *left nucleus* of a loop $Q$ is given by $\mathrm{N}_\lambda(Q) = \{a : a \cdot xy = ax \cdot y, \forall x, y \in Q\}$. The *middle nucleus*, $\mathrm{N}_\mu(Q)$, and the *right nucleus*, $\mathrm{N}_\rho(Q)$, are defined analogously. The *nucleus*, then, is given by $\mathrm{N}(Q) = \mathrm{N}_\lambda(Q) \cap \mathrm{N}_\mu(Q) \cap \mathrm{N}_\rho(Q)$. The *commutant* of $Q$ is given by $\mathrm{C}(Q) = \{c : \forall x \in Q, cx = xc\}$. The *center* is the normal subloop given by $\mathrm{Z}(Q) = \mathrm{N}(Q) \cap \mathrm{C}(Q)$. Now, define $\mathrm{Z}_0(Q) = \{1\}$, and $\mathrm{Z}_{i+1}(Q)$, $i \geq 0$, as the preimage of $\mathrm{Z}(Q/\mathrm{Z}_i(Q))$ under the canonical projection. The loop $Q$ is *(centrally) nilpotent of class* $n$, written $\mathrm{c}\ell(Q) = n$, if $\mathrm{Z}_{n-1}(Q) < \mathrm{Z}_n(Q) = Q$.

Recall that if $Q$ is a group, then $Q/\mathrm{Z}(Q)$ is isomorphic to $\mathrm{Inn}(Q)$. Thus $\mathrm{Inn}(Q)$ is nilpotent of class at most $n$ if and only if $Q$ is nilpotent of class at most $n+1$. For loops, however, the situation is much more complicated. In the positive direction, Bruck [3] showed that if $Q$ is nilpotent with $\mathrm{c}\ell(Q) \leq 2$, then $\mathrm{Inn}(Q)$ is abelian. However, A. Vesanen found a nilpotent loop $Q$ of order 18 with $\mathrm{c}\ell(Q) = 3$ such that $\mathrm{Inn}(Q)$ is not even nilpotent [17]. In the converse direction, Niemenmaa recently showed that if $Q$ is finite and $\mathrm{Inn}(Q)$ is nilpotent, then $Q$ is nilpotent [23].

It was long believed that the converse of Bruck's result was true; that is, it was believed that if $Q$ is a (finite) loop with abelian inner mapping loop, then $\mathrm{c}\ell(Q) \leq 2$. Much work in loop theory was devoted to attempting to prove this [9, 16, 24]. However, in 2004, Csörgő [7] constructed a loop $Q$ of order 128, with abelian inner mapping group, and with $\mathrm{c}\ell(Q) = 3$. Loops $Q$ with abelian inner mapping group and with $\mathrm{c}\ell(Q) > 2$ have come to be called *loops of Csörgő type*. Additional constructions of loops of Csörgő type followed in rapid succession [10, 11, 22].

In the positive direction, there are at least a few classes of loops for which it has been shown that all loops in the class with abelian inner mapping groups must

2000 *Mathematics Subject Classification.* 20N05.

*Key words and phrases.* Bruck loop, inner mapping group, centrally nilpotent.

This work is a part of the research project MSM 0021620839 financed by MŠMT ČR. The second author was partly supported by the GAČR grant #201/08/P056.

have nilpotency class no greater than 2, e.g. automorphic loops [20], left conjugacy closed loops [8], and 2-divisible Moufang loops [19]. It is the purpose of this paper to lengthen this list. Here is our main result:

**Theorem 1.** *Let $Q$ be a Bruck loop with abelian inner mapping group. Then $Q$ is nilpotent and $\mathrm{c}\ell(Q) \leq 2$.*

We now give all pertinent definitions. A *left Bol loop* is a loop satisfying the identity $x(y \cdot xz) = (x \cdot yx)z$; *right Bol loops* satisfy the mirror identity. A left Bol loop that is also a right Bol loop is a *Moufang loop*. We refer to left Bol loops simply as *Bol loops* for the balance of the paper. In Bol loops, each element has a unique two-sided inverse element, denoted by $x^{-1}$, satisfying $x \cdot x^{-1} = x^{-1} \cdot x = 1$. The *automorphic inverse property*, denoted by AIP, is given by $(xy)^{-1} = x^{-1}y^{-1}$. The *antiautomorphic inverse property*, denoted by AAIP, is given by: $(xy)^{-1} = y^{-1}x^{-1}$. The *left inverse property*, denoted by LIP, is given by $x^{-1} \cdot xy = y$. The *right inverse property*, denoted by RIP, is defined analogously. Moufang loops satisfy both the LIP and the RIP. (Left) Bol loops satisfy the LIP, but need not satisfy the RIP (a left Bol loop that satisfies the RIP is, in fact, a Moufang loop). Moufang loops satisfy the AAIP. Moufang loops can be characterized as Bol loops that satisfy the AAIP. Bol loops that satisfy the AIP are called *Bruck loops*. Bruck loops can thus be thought of as dual to Moufang loops in the variety of Bol loops. Much is known about both Moufang loops [6, 25] and Bruck loops [1, 12, 13, 14, 18]; they are two of the most important and widely investigated classes of loops.

## 2. The proof

Let $Q$ be a loop. Then $\mathrm{Inn}(Q)$, is generated by the following three families of mappings [4]:

$$\begin{aligned} T(x) &= L(x)^{-1}R(x) \\ R(x,y) &= R(x)R(y)R(xy)^{-1} \\ L(x,y) &= L(x)L(y)L(yx)^{-1}. \end{aligned}$$

The condition "$\mathrm{Inn}(Q)$ is abelian" can thus be expressed equationally as:

$$\begin{aligned} R(w,x)R(y,z) &= R(y,z)R(w,x) \\ L(w,x)L(y,z) &= L(y,z)L(w,x) \\ R(w,x)L(y,z) &= L(y,z)R(w,x) \\ R(x,y)T(z) &= T(z)R(x,y) \\ L(x,y)T(z) &= T(z)L(x,y) \\ T(y)T(z) &= T(z)T(y) \end{aligned}$$

We define the *associator*, $(x,y,z)$ of $x$, $y$, and $z$, as follows: $xy \cdot z = (x \cdot yz)(x,y,z)$. We define the *commutator*, $[x,y]$ of $x$ and $y$, as follows: $xy = yx \cdot [x,y]$. With this notation in place, it's easy to state the definition of "centrally nilpotent of class 2" in equational form.

**Lemma 2.** *A loop, $Q$, has $\mathrm{c}\ell(Q) \leq 2$ if the following ten terms vanish:* $[[x,y],z]$, $[x,[y,z]]$, $[(w,x,y),z]$, $[w,(x,y,z)]$, $([w,x],y,z)$, $(w,[x,y],z)$, $(w,x,[y,z])$, $((v,w,x),y,z)$, $(v,(w,x,y),z)$, *and* $(v,w,(x,y,z))$.

If $Q$ is a Bol loop, then $\mathrm{N}_\lambda(Q) = \mathrm{N}_\mu(Q)$. Using this fact, the next lemma is clear.

**Lemma 3.** *A Bol loop, $Q$, has $\mathrm{c}\ell(Q) \leq 2$ if the following six terms vanish:* $[[x,y],z]$, $[(w,x,y),z]$, $([w,x],y,z)$, $(w,x,[y,z])$, $((v,w,x),y,z)$, *and* $(v,w,(x,y,z))$.

If $Q$ is a Bruck loop, this can be strengthened considerably.

**Lemma 4.** *A Bruck loop, $Q$, with abelian inner mapping group, has $\mathrm{c}\ell(Q) \leq 2$ if $((v,w,x),y,z)$ vanishes.*

*Proof.* We will make use of the following fact, which is easy to check, and which holds in any Bruck loop:

$$[y,x] = (x^{-1}, y^{-1}, yx) \tag{$*$}$$

By $(*)$ we have $([w,x],y,z) = ((x^{-1},w^{-1},wx),y,z)$, which vanishes, by assumption. Next, we note that it is easy to check that in a Bruck loop in which $((v,w,x),y,z)$ vanishes, we have:

$$[x^{-1},y^{-1}] = [y,x] \tag{$**$}$$

Now, using first $(**)$ and then $(*)$ we have $[[x,y],z] = [z^{-1},[x,y]^{-1}] = ([x,y],z,z^{-1}[x,y]^{-1})$, which vanishes, as established in the previous paragraph.

Next, combine $(*)$ and $(**)$ to obtain $[x,y] = (x,y,y^{-1}x^{-1})$. Thus, we have $[(w,x,y),z] = ((w,x,y),z,z^{-1}(w,x,y)^{-1})$, which vanishes by assumption.

Next, since clearly $[x,y]^{-1} = [x^{-1},y^{-1}]$ in Bruck loops, by $(**)$ we have $[x,y]^{-1} = [y,x]$. Thus, we also have $[y,x]\cdot[x,y]z = [x,y]^{-1}\cdot[x,y]z = z = (z[x,y])/[x,y] = ([x,y]z)/[x,y]$. Since $z$ is arbitrary, we get $[y,x]w = w/[x,y]$. Now, use this, the (left) Bol law, the LIP and the fact that $[x,y]$ is in both the commutant and left nucleus to get $w\cdot x[y,z] = w\cdot[y,z]x = ([y,z]\cdot[y,z]^{-1}w)\cdot[y,z]x = [y,z]([y,z]^{-1}w\cdot[y,z]x) = [y,z]([z,y]w\cdot[y,z]x) = [y,z]((w/[y,z])\cdot[y,z]x) = [y,z]\cdot((w/[y,z])[y,z])x = [y,z]w\cdot x = [y,z]\cdot wx = wx\cdot[y,z]$. In other words, $(w,x,[y,z])$ vanishes.

Next, using the LIP and the easy to establish fact that $(xy)/(x[x,y]) = y$, we obtain $w/(x,y,z) = (x,y,z)^{-1}w$. Finally, use this, the (left) Bol law, the LIP and the fact that $(x,y,z)$ is in both the commutant and left nucleus to get $v\cdot w(x,y,z) = v\cdot(x,y,z)w = ((x,y,z)\cdot(x,y,z)^{-1}v)\cdot(x,y,z)w = (x,y,z)((x,y,z)^{-1}v\cdot(x,y,z)w) = (x,y,z)(v/(x,y,z)\cdot(x,y,z)w) = (x,y,z)\cdot((v/(x,y,z))(x,y,z))w = (x,y,z)v\cdot w = (x,y,z)\cdot vw = vw\cdot(x,y,z)$. In other words, $(v,w,(x,y,z))$ vanishes.

We were assisted in this proof by the automated reasoning tool Prover9 [21]. □

Thus, to prove Theorem 1 it suffices to show that if $Q$ is a Bruck loop with abelian inner mapping group, then $((v,w,x),y,z)$ vanishes. This statement is expressible equationally, as we have seen, and is thus amenable to attack by automated reasoning. It is, though, an extremely difficult problem for automated theorem provers,

as we discovered. Eventually, though, we succeeded with Waldmeister [15], with the following input file:

```
NAME            Bruck

MODE            PROOF

SORTS           ANY

SIGNATURE       a: -> ANY
                asoc: ANY ANY ANY -> ANY
                b: -> ANY
                c: -> ANY
                d: -> ANY
                e: -> ANY
                i: ANY -> ANY
                mult: ANY ANY -> ANY
                op_l: ANY ANY ANY -> ANY
                op_r: ANY ANY ANY -> ANY
                op_t: ANY ANY -> ANY
                rd: ANY ANY -> ANY
                unit: -> ANY

ORDERING        KBO
                i=1, mult=1, op_t=1, rd=1, asoc=1, op_l=1, op_r=1, unit=1, e=1, d=1, c=1, b=1, a=1
                i > rd > mult > op_t > asoc > op_l > op_r > unit > e > d > c > b > a

VARIABLES       E,D,C,B,A: ANY

EQUATIONS       mult(unit, A) = A
                mult(A, unit) = A
                mult(A, i(A)) = unit
                mult(i(A), A) = unit
                i(mult(A, B)) = mult(i(A), i(B))
                mult(i(A), mult(A, B)) = B
                rd(mult(A, B), B) = A
                mult(rd(A, B), B) = A
                mult(mult(A, mult(B, A)), C) = mult(A, mult(B, mult(A, C)))
                mult(mult(A, B), C) = mult(mult(A, mult(B, C)), asoc(A, B, C))
                op_l(A, B, C) = mult(i(mult(C, B)), mult(C, mult(B, A)))
                op_r(A, B, C) = rd(mult(mult(A, B), C), mult(B, C))
                op_t(A, B) = mult(i(B), mult(A, B))
                op_r(op_r(A, B, C), D, E) = op_r(op_r(A, D, E), B, C)
                op_l(op_r(A, B, C), D, E) = op_r(op_l(A, D, E), B, C)
                op_l(op_l(A, B, C), D, E) = op_l(op_l(A, D, E), B, C)
                op_t(op_r(A, B, C), D) = op_r(op_t(A, D), B, C)
                op_t(op_l(A, B, C), D) = op_l(op_t(A, D), B, C)
                op_t(op_t(A, B), C) = op_t(op_t(A, C), B)

CONCLUSION      asoc(asoc(a, b, c), d, e) = unit
```

The Waldmeister output file, i.e., the proof of Theorem 1, is titanic, over 16,000 lines of raw ouput, or over 1000 pages of structured equational reasoning (the running time was about 15 hours). The output file and its automatic transformation into a "readable" equational proof may be found at either of the following sites:

http://www.karlin.mff.cuni.cz/~stanovsk/math/bruck.htm

http://euclid.nmu.edu/~jophilli/paper-supplements.html

The proof is far too long to translate into a "human friendly" form.

**Problem 5.** *Find a "human friendly" proof of Theorem 1.*

*Remark* 6. In [22] Nagy and Vojtěchovský constructed a Moufang loop of order $2^{14}$, of nilpotency class 3, and with abelian inner mapping group. Thus, since Moufang loops are also Bol loops, our Theorem 1 does not generalize to Bol loops. Moufang loops with abelian inner mapping group are nilpotent of class at most 3 [19], and 2-divisible Moufang loops with abelian inner mapping group are nilpotent of class at most 2 [19]. It is unknown whether either of these two results can be generalized to Bol loops.

*Remark* 7. This is the first problem in loop theory that was solved with the assistance of the automated theorem prover Waldmeister. We made several attempts with different provers (Gandalf, E, Prover9, Vampire) and formalizations of the problem; they all failed. Also, as far as we know, to date this is the most complicated proof in algebra obtained by an automated theorem prover. Its simplification seems to be a challenge. For a detailed account of using automated reasoning in algebra, see [26].

## References


[1] M. Aschbacher, M.K. Kinyon, and J.D. Phillips, *Finite Bruck loops*, Transactions of the American Mathematical Society, **358** (2006), 3061–3075.

[2] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Izdat. Nauka, Moscow, 1967 (Russian).

[3] R. H. Bruck, Contributions to the theory of loops, *Trans. Amer. Math. Soc.* **60** (1946), 245–354.

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

[5] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) **63** (1956), 308–323.

[6] O. Chein, *Moufang loops of small order*, Memoirs of the American Mathematical Society, Volume 13, Issue 1, Number 197 (1978).

[7] P. Csörgő, Abelian inner mappings and nilpotency class greater than two, *European J. Combin.* **28** (2007), 858–867.

[8] P. Csörgő and A. Drápal, Left conjugacy closed loops of nilpotency class two, *Results Math.* 47 (2005), 242–265.

[9] P. Csörgő and T. Kepka, On loops whose inner permutations commute, *Comment. Math. Univ. Carolin.* **45** (2004), 213–221.

[10] A. Drápal and M. K. Kinyon, Buchsteiner loops: associators and constructions, submitted.

[11] A. Drápal and P. Vojtěchovský, Explicit constructions of loops with commuting inner mappings, *European J. Combin.* **29** (2008), 1662–1681.

[12] T. Foguel, M.K. Kinyon and J.D. Phillips, On twisted subgroups and Bol loops of odd order, *Rocky Mountain J. of Math.* **36** 1 (2006), 183–212.

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

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

[15] T. Hillenbrand, http://www.waldmeister.org

[16] T. Kepka, On the abelian inner permutation groups of loops, *Comm. Algebra* **26** (1998), 857–861.
[17] T. Kepka and J.D. Phillips, Connected transversals to subnormal subgroups, *Comment. Math. Univ. Carolin.* **38** (1997), 223–230.
[18] H. Kiechle, *Theory of K-loops*, Lecture Notes in Mathematics, 1778, Springer-Verlag, 2002.
[19] M. K. Kinyon, J.D. Phillips, Robert Veroff, and P. Vojtěchovský, Moufang loops with abelian inner mapping groups, in preperation.
[20] M. K. Kinyon and P. Vojtěchovský, Autmorphic loops with abelian inner mapping groups, in preperation.
[21] W. W. McCune, *Prover9*, automated reasoning software, and *Mace4*, finite model builder, Argonne National Laboratory, 2005.
`http://www.prover9.org`
[22] G. P. Nagy and P. Vojtěchovský, Moufang loops with commuting inner mappings, to appear in Journal of Pure and Applied Algebra.
[23] M. Niemenmaa, Finite loops with nilpotent inner mapping groups are centrally nilpotent, *Bull. Australian Math. Soc.* 79/1 (2009), 109-114.
[24] M. Niemenmaa and T. Kepka, On connected transversals to abelian subgroups in finite groups, *Bull. London Math. Soc.* **24** (1992), 343–346.
[25] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.
[26] J. D. Phillips, D. Stanovský, *Automated theorem proving in quasigroup and loop theory*, to appear in AI Communications.

(Stanovský) Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 18675 Prague, Czech Republic
*E-mail address*: `stanovsk@karlin.mff.cuni.cz`
*URL*: `http://www.karlin.mff.cuni.cz/~stanovsk/`

(Phillips) Department of Mathematics & Computer Science, Northern Michigan University, Marquette, MI 49855 USA
*E-mail address*: `jophilli@nmu.edu`
*URL*: `http://euclid.nmu.edu/~jophilli/`