

LOOPS AND THE LAGRANGE PROPERTY

ORIN CHEIN, MICHAEL K. KINYON,
ANDREW RAJAH, AND PETR VOJTĚCHOVSKÝ

ABSTRACT. Let \mathcal{F} be a family of finite loops closed under subloops and factor loops. Then every loop in \mathcal{F} has the strong Lagrange property if and only if every simple loop in \mathcal{F} has the weak Lagrange property. We exhibit several such families, and indicate how the Lagrange property enters into the problem of existence of finite simple loops.

The two most important open problems in loop theory, namely the existence of a finite simple Bol loop and the Lagrange property for Moufang loops, have been around for more than 40 years. While we certainly have not solved these problems, we show that they are closely related. Some of the ideas developed here have been present in the loop-theoretical community, however, in a rather vague form. We thus felt the need to express them more precisely and in a more definite way.

We assume only basic familiarity with loops (not reaching beyond the introductory chapters of [17]), and with universal algebraic concepts (e.g. variety [10]). All loops mentioned below are finite.

We begin with the crucial notion: the Lagrange property. A loop L is said to have the *weak Lagrange property* if, for each subloop K of L , $|K|$ divides $|L|$. It has the *strong Lagrange property* if every subloop K of L has the weak Lagrange property.

A loop may have the weak Lagrange property but not the strong Lagrange property. Four of the six nonisomorphic loops of order 5 have elements of order 2 and hence fail to satisfy the weak Lagrange property. Let K be one of these loops. As noted in [17, p. 13], if L is a loop of order 10 having K as a subloop and satisfying the property that every proper subloop of L is contained in K , then L will have the weak but not the strong Lagrange property. It is not difficult to construct a multiplication table for such a loop.

Our main result depends on the following lemma, which is a restatement of [1, Lemma V.2.1].

Lemma 1. *Let L be a loop with a normal subloop N such that*

- (i) *N has the weak (resp. strong) Lagrange property, and*
- (ii) *L/N has the weak (resp. strong) Lagrange property.*

Then L has the weak (resp. strong) Lagrange property.

1991 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Lagrange property, Moufang loop, Bol loop, A-loop.

There are some classes of loops studied in the literature to which the lemma applies directly. For each of these, the normal subloop in question is associative. For instance, an easy induction shows that any solvable loop satisfies the strong Lagrange property. In particular, any (centrally) nilpotent loop satisfies this property as well.

Before we turn to more specific examples, we recall a few definitions. Let L be a loop and $x \in L$. When x has a two-sided inverse, we denote it by x^{-1} . A loop L has the *automorphic inverse property* if $x^{-1}y^{-1} = (xy)^{-1}$ holds for every $x, y \in L$. A loop L is (*right*) *Bol* (resp. *left Bol*), if $((xy)z)y = x((yz)y)$ (resp. $(x(yx))z = x(y(xz))$) holds for every $x, y, z \in L$. *Moufang loops* are loops that are both right Bol and left Bol. Since the concepts of right Bol loop and left Bol loop are anti-isomorphic to each other, right Bol and left Bol loops share the same algebraic properties. Thus, in what follows, when we refer to Bol loops, the reader may think of left Bol or right Bol as he or she sees fit. A Bol loop which has the automorphic inverse property is called a *Bruck loop*. Bruck loops of odd order are called *B-loops*[6, p. 376]. An *A-loop* is a loop all of whose inner mappings are automorphisms [2]. Finally, an M_k loop is a Moufang loop L for which $L/\text{Nuc}(L)$ has exponent $k - 1$ and no smaller exponent, where $\text{Nuc}(L)$ is the nucleus of L [16, 4].

Example 1. Let L be a Moufang loop with an associative normal subloop K such that L/K satisfies the strong Lagrange property. By the lemma, L has the strong Lagrange property.

As an example, if L is an M_k loop where $k = 2^m + 1$ and if $K = \text{Nuc}(L)$, then L/K is a Moufang 2-loop which, by [8] is centrally nilpotent (cf. [3]).

As another example of this type, let L be a Moufang loop with an associative normal subloop K such that $|L/K|$ is odd. In this case L/K has the strong Lagrange property by [7, Thm. 2]. For instance, if L is an M_k loop with k even, then $K = \text{Nuc}(L)$ is an associative normal subloop such that L/K is of odd exponent, $k - 1$, and so L/K must have odd order (cf. [3]).

Since every Moufang *A-loop* is an M_4 loop [11, Cor. 2], and every commutative Moufang loop is a Moufang *A-loop* [2], it follows that every Moufang *A-loop*, and in particular, every commutative Moufang loop has the strong Lagrange property.

That every commutative Moufang loop has the strong Lagrange property is, in fact, a well-known folk result, and follows from the central nilpotence of these loops and the lemma.

Example 2. Let L be a Bruck loop with an associative normal subloop K such that $|L/K|$ is odd. Since L/K is a B-loop, it follows from [6, Cor. 4] that L/K has the strong Lagrange property. By the lemma, so does L . For instance, since a commutative Moufang loop of odd order is obviously a B-loop, this gives an alternative proof that every such loop has the strong Lagrange property.

Example 3. The lemma also applies directly to those loops L for which the derived subloop L' (i.e., the smallest subloop L' such that L/L' is an abelian group) has the strong Lagrange property. For instance, let L be a “central” Bol loop in the terminology of Kreuzer [12], i.e., a Bol loop L such that L' is contained in the center. These are just centrally nilpotent Bol loops of nilpotence class 2, and thus these loops have the strong Lagrange property. As another example, Bruck and Paige [2] showed that an A-loop L has the property that all of its loop isotopes are A-loops if and only if $L/\text{Nuc}(L)$ is a group, in other words, if and only if L is nuclearly nilpotent of class 2. By the lemma, such an L has the strong Lagrange property.

We now come to our main result—the connection between simple loops and loops satisfying the Lagrange property.

Theorem 1. *Let \mathcal{F} be a nonempty family of finite loops such that*

- (1) *If $L \in \mathcal{F}$ and $N \triangleleft L$, then $N \in \mathcal{F}$;*
- (2) *If $L \in \mathcal{F}$ and $N \triangleleft L$, then $L/N \in \mathcal{F}$;*
- (3) *Every simple loop in \mathcal{F} has the weak Lagrange property.*

Then every loop in \mathcal{F} has the weak Lagrange property.

Proof. We proceed by induction on the order of loops in \mathcal{F} . Note that (1) implies that \mathcal{F} contains the trivial loop $\langle 1 \rangle$, for which the desired conclusion is trivial. Now fix $L \in \mathcal{F}$ and assume that the result holds for all loops in \mathcal{F} of order less than $|L|$. If L is simple, we are finished by (3). Thus assume that L is not simple, so that L has a nontrivial proper normal subloop N . Since $|N| < |L|$, (1) and the induction hypothesis imply that N has the weak Lagrange property. Since $|L/N| < |L|$, (2) and the induction hypothesis imply that L/N has the weak Lagrange property. By Lemma 1, L has the weak Lagrange property. \square

Corollary 1. *Let \mathcal{F} be a nonempty family of finite loops such that*

- (1') *If $L \in \mathcal{F}$ and $K \leq L$, then $K \in \mathcal{F}$;*
- (2) *If $L \in \mathcal{F}$ and $N \triangleleft L$, then $L/N \in \mathcal{F}$;*
- (3) *Every simple loop in \mathcal{F} has the weak Lagrange property.*

Then every loop in \mathcal{F} has the strong Lagrange property.

Proof. Since (1') implies (1), Theorem 1 implies that every loop in \mathcal{F} has the weak Lagrange property. But then (1') yields the desired result. \square

Corollary 2. *Let \mathcal{V} be a variety of loops such that every simple loop in \mathcal{V} has the weak Lagrange property. Then every loop in \mathcal{V} has the strong Lagrange property.*

Corollary 2 is of particular interest for those varieties of loops for which there exists a classification of all simple loops. A prominent example is the variety of Moufang loops, where it is known that every simple nonassociative Moufang loop is isomorphic to a Paige loop (cf. [15], [13]). It follows from Corollary 2 that if the weak Lagrange property can be established for each of the Paige loops, then every Moufang loop will have the strong Lagrange property.

There is one Paige loop for every finite field $GF(q)$; its order is $q^3(q^4 - 1)$ when q is even, and $q^3(q^4 - 1)/2$ when q is odd [15]. The weak Lagrange property for the smallest 120-element Paige loop has been established in [9] and [18]. The next smallest Paige loop has order 1080. Thus based on published literature, we can state this result.

Corollary 3. *Every Moufang loop of order less than 1080 has the strong Lagrange property.*

Proof. A simple Moufang loop of order less than 1080 is a group or the smallest Paige loop. The result follows from Corollary 1. \square

Incidentally, since no Paige loop is commutative, it follows from Corollary 2 that, once again, every commutative Moufang loop has the strong Lagrange property.

The authors have been informed by G. E. Moorehouse [14] that by a computer search, he has found that the Paige loop of order 1080 satisfies the weak Lagrange property. If we assume this to be correct, then we may state the following.

Corollary 4. *Every Moufang loop of order less than 16320 has the strong Lagrange property.*

Altogether, we have demonstrated that a loop has the strong Lagrange property whenever it belongs to one of the following classes: Moufang loops with an associative normal subloop of odd index, Bruck loops with an associative normal subloop of odd index, loops whose derived subloops have the strong Lagrange property, and Moufang loops of order less than 1080.

We conclude this paper with a couple of remarks on a potential application for Corollary 2 to the existence of finite simple non-Moufang Bol loops. This can be split into two problems: the existence of a finite simple Bruck loop and the existence of a finite simple proper (non-Moufang, non-Bruck) Bol loop.

First, to establish the existence of a finite simple Bruck loop, it would be sufficient to find a Bruck loop which violates the weak Lagrange property, for then Corollary 2 would imply the existence of a simple Bruck loop which is not a cyclic group.

On the other hand, Corollary 2 might apply to the problem of the existence of finite simple proper Bol loops if the weak Lagrange property is established for all Paige loops. It would then be sufficient to find a Bol loop which violated the weak Lagrange property, for by Corollary 2, there

would exist a simple Bol loop which violated that property. If all simple Moufang loops have the weak Lagrange property, then the simple Bol loop in question will not be Moufang.

REFERENCES

- [1] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1958; third printing, 1971.
- [2] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math. (2)* **63** (1956) 308-323.
- [3] O. Chein, Lagrange's theorem for M_k -loops, *Arch. Math. (Basel)* **24** (1973), 121-122.
- [4] O. Chein and H. O. Pflugfelder, On maps $x \rightarrow x^n$ and the isotopy-isomorphy property of Moufang loops, *Aequationes Math.* 6 (1971) 157-161.
- [5] O. Chein, H. O. Pflugfelder, and J. D. H. Smith, *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Math. **9**, Heldermann Verlag, 1990.
- [6] G. Glauberman, On loops of odd order I. *J. Algebra* **1** (1964) 374-396.
- [7] G. Glauberman, On loops of odd order II. *J. Algebra* **8** (1968) 393-414.
- [8] G. Glauberman and C. R. B. Wright, Nilpotence of finite Moufang 2-loops, *J. Algebra* **8** (1968) 415-417.
- [9] M. L. Merlini Guiliani, César Polcino Milies, On the structure of the simple Moufang loop $GLL(F_2)$, in *Nonassociative algebra and its applications*, the Fourth International Conference, Lecture Notes in Pure and Applied Mathematics **211**, ed. R. Costa, A. Grishkov, H. Guzzo, Jr., L. A. Peresi. Marcel Dekker, New York, 2000.
- [10] George A. Grätzer, *Universal Algebra*, Princeton, Van Nostrand, 1968.
- [11] M. Kinyon, K. Kunen, and J. D. Phillips, Every diassociative A-loop is Moufang, *Proc. Amer. Math. Soc.* **130** (2002) 619-624.
- [12] A. Kreuzer, Central Bol loops, in *Nearrings, nearfields and K-loops* (Hamburg, 1995), 301-310, Math. Appl. **426**, Kluwer Acad. Publ., Dordrecht, 1997.
- [13] M. W. Liebeck, The classification of finite simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* **102** (1987) 33-47.
- [14] G. E. Moorehouse, private communication.
- [15] L. J. Paige, A Class of Simple Moufang Loops, *Proc. Amer. Math. Soc.* **7** (1956) 471-482.
- [16] H. Orlik-Pflugfelder, A special class of Moufang loops, *Proc. Amer. Math. Soc.* **26** (1970) 583-586
- [17] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.
- [18] P. Vojtěchovský, *Finite simple Moufang loops*, Ph.D. Dissertation, Iowa State University, 2001. Available online at www.vojtechovsky.com.

DEPARTMENT OF MATHEMATICS, TEMPLE UNIVERSITY, 1805 N. BROAD ST., PHILADELPHIA, PA 19122 USA
E-mail address: orin@math.temple.edu
URL: <http://math.temple.edu/~orin>

DEPARTMENT OF MATHEMATICS, WESTERN MICHIGAN UNIVERSITY, KALAMAZOO, MI 49008-5248 USA
E-mail address: mkinyon@wmich.edu
URL: <http://unix.cc.wmich.edu/~mkinyon>

SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITI SAINS MALAYSIA, 11800 USM PENANG, MALAYSIA
E-mail address: andy@cs.usm.my
URL: <http://www.mat.usm.my/math/staff2.htm#AR>

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IA 50011 USA
E-mail address: petr@iastate.edu, petr@math.iastate.edu
URL: <http://www.vojtechovsky.com>

Eingegangen am 16. Mai 2002.