Steiner loops satisfying the statement of Moufang's theorem

Maria de Lourdes Merlini Giuliani, Giliard Souza dos Anjos and Charles J. Colbourn

Abstract. Andrew Rajah posed at the Loops'11 Conference in Trest, Czech Republic, the following conjecture: *Is every variety of loops that satisfies Moufang's theorem contained in the variety of Moufang loops?* This paper is motivated by that problem. We give a partial answer to this question and present two types of Steiner loops, one that satisfies Moufang's theorem and another that does not, and neither is Moufang loop.

1. Introduction

A nonempty set L with a binary operation is a *loop* if there exists an identity element 1 with $1x = x = x1$ for every $x \in L$ and both left and right multiplication by any fixed element of L permutes every element of L.

A loop L has the *inverse property* (and is an *IP loop*), if and only if there is a bijection $L \longrightarrow L : x \mapsto x^{-1}$ such whenever $x, y \in L$, $x^{-1}(xy) = y = (yx)x^{-1}$. It can be seen that *IP* loops also satisfy $(xy)^{-1} = y^{-1}x^{-1}$. A *Steiner loop* is an IP loop of exponent 2. A loop M is a *Moufang loop* if it satisfies any of the following equivalent identities:

$$x(y \cdot xz) = (xy \cdot x)z,$$
$$y(x \cdot zx) = (yx \cdot z)x,$$
$$xy \cdot zx = x(yz \cdot x).$$

Such loops were introduced by Moufang [3] in 1934. The *associator* of elements $a, b, c \in L$ is the unique element (a, b, c) of L satisfying the equation: $ab \cdot c = (a \cdot bc)(a, b, c)$.

Theorem 1.1. [Moufang's Theorem [4]] *Let M be a Moufang loop. If $a, b, c \in M$ such that $(a, b, c) = 1$, then a, b, c generate a subgroup of M.*

In view of Theorem 1.1, every Moufang loop is *diassociative*, that is, any two of its elements generate a group. However, Theorem 1.1 was formulated for Moufang

2010 Mathematics Subject Classification: 20N05
Keywords: Steiner loop; Moufang loop; Moufang theorem.
The second author was partially supported by FAPESP, Proc. 2012/21323-0

loops. We consider its statement for another class of loops, namely, for the variety of Steiner loops.

Our motivation arises from the question posed by Andrew Rajah at the Loops'11 Conference concerning the relationship between Moufang loops and loops that satisfy Moufang's theorem. The results in this paper were first presented at the Third Mile High Conference on Nonassociative Mathematics in Denver, 2013. Later, Stuhl [7] explored solutions based on Steiner Oriented Hall Loops, and a combinatorial characterization of Steiner loops satisfying Moufang's theorem in terms of configurations has been established [1]. Despite the combinatorial characterization in [1], the algebraic treatment here remains useful for two reasons. First, these results provide the foundational work for [1]; and second, they provide an algebraic framework to understand such loops, which complements the combinatorial framework.

2. Steiner loops and Moufang's theorem

Definition 2.1. A loop L *satisfies Moufang's Property*, $\mathcal{MP}$, if L is not Moufang loop, but it satisfies the statement of Moufang's theorem, i.e., if $a, b, c \in L$ such that $(a, b, c) = 1$, then a, b, c generate a subgroup of L.

It is known that there exists only one Steiner loop S of order 10. We prove that this Steiner loop S satisfies Moufang's Property $\mathcal{MP}$. Its Cayley table can be found, for example, using the GAP Library [9], as seen below:

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	1	4	3	8	10	9	5	7	6
3	3	4	1	2	10	9	8	7	6	5
4	4	3	2	1	9	8	10	6	5	7
5	5	8	10	9	1	7	6	2	4	3
6	6	10	9	8	7	1	5	4	3	2
7	7	9	8	10	6	5	1	3	2	4
8	8	5	7	6	2	4	3	1	10	9
9	9	7	6	5	4	3	2	10	1	8
10	10	6	5	7	3	2	4	9	8	1

For any $x, y, z \in S$, such that $x \neq y$; $y \neq z$; $z \neq x$, $x \neq 1, y \neq 1, z \neq 1$, $x \cdot yz = xy \cdot z$ implies that $z = xy$. So $< x, y, z > = < x, y >$, and hence x, y, z generate a group.

A *Steiner triple system* $(Q, \mathcal{B})$, or $STS(n)$, is a non-empty set Q with n elements and a set $\mathcal{B}$ of unordered triples $\{a, b, c\}$ such that

(i) a, b, c are distinct elements of Q;

(ii) when $a, b \in Q$ and $a \neq b$, there exists a unique triple $\{a, b, c\} \in \mathcal{B}$.

A Steiner triple system $(Q, \mathcal{B})$ with $|Q| = n$ elements exists if and only if $n \geqslant 1$ and $n \equiv 1$ *or* $3 \pmod 6$ [8]. Because there is a one-to-one correspondence between the variety of Steiner triple systems and the variety of all Steiner Loops [2], Steiner loops have order $m \equiv 2$ *or* $4 \pmod 6$. This underlies the study of Steiner triple systems from an algebraic point of view as in [4], [5] and [6].

We use the following standard construction of Steiner triple systems [8], sometimes called the *Bose construction*. Let $n = 2t + 1$ and define $Q := \mathbb{Z}_n \times \mathbb{Z}_3$. A Steiner triple system $(Q, \mathcal{B})$ can be formed with $\mathcal{B}$ consisting of the following triples

$$\begin{array}{ll} \{(x,0),(x,1),(x,2)\} & \text{where} \quad x \in \mathbb{Z}_n, \text{ and} \\ \{(x,i),(y,i),(\frac{x+y}{2}, i+1)\} & \text{where} \quad x \neq y; x, y \in \mathbb{Z}_n, i \in \mathbb{Z}_3 \end{array}$$

The corresponding Steiner loops can be defined directly. Let $S = Q \cup \{1\}$. Define a binary operation $*$ with identity element 1 as follows:

$$\begin{aligned} (x,i) * (x,j) &= (x,k) && i \neq j,\ i \neq k,\ j \neq k, \\ (x,i) * (y,i) &= (\tfrac{x+y}{2}, i+1) && x \neq y, \\ (x,i) * (y,i+1) &= (2y - x, i) && x \neq y, \\ (x,i) * (y,i-1) &= (2x - y, i-1) && x \neq y, \\ (x,i) * (x,i) &= 1 \end{aligned}$$

Then $(S,*)$ is commutative loop. However, $(S,*)$ is not a Moufang loop. If we take the elements $x = (0,0)$ $y = (1,0)$ and $z = (0,1)$ then $(xy)(zx) = (-1/2, 1)$. On the other hand, $x((yz)x) = (-1,0)$, so $(S,*)$ does not satisfy one of the Moufang identities.

Analyzing Steiner loops from the Bose construction, there are two types: one that satisfies $\mathcal{MP}$, and another that does not. Using computer calculations and the `Loops` package in GAP [9], first we studied the Steiner loops of order k with $k \in M_1$ where

$$M_1 = \{16, 28, 34, 40, 46, 52, 58, 79, 76, 82, 88, 94, 100, 112, 118, 124, 130, 136, 142, 154\}$$

from the Bose construction. Each of these Steiner loops satisfies $\mathcal{MP}$. However, none of the Steiner loops of order $k \in \{22, 64, 106, 148\}$ from the Bose construction satisfies $\mathcal{MP}$. The explanation for this follows.

Theorem 2.2. *Let S be a Steiner loop from the Bose construction. Then S has the property $\mathcal{MP}$ if and only if 7 is an invertible element in $\mathbb{Z}_n$.*

Proof. Suppose S has property $\mathcal{MP}$. If 7 is not invertible in $\mathbb{Z}_n$, then exists an element $a \in \mathbb{Z}_n$, $a \neq 0$ such that $7a = 0$. Hence $8a = a$. Because n is odd, $2a = a/4$. The associator $((0,1),(0,0),(a,0)) = 1$ while $((0,1),(a,0),(0,0)) \neq 1$, thus the elements $(0,1),(0,0),(a,0)$ associate in some order, but not in every order, a contradiction.

Now, suppose that 7 is invertible in $\mathbb{Z}_n$. We consider all possible triples of elements of S. Our strategy is to show that if the associator $(a, b, c) = 1$, then a, b, c are in the same triple. There are 25 generic triple elements of S; here $x, y, z \in \mathbb{Z}_n$ are distinct and $i, j, k \in \mathbb{Z}_3$ are distinct:

$\{(x,i),(x,i),(x,i)\}$, $\{(x,i),(x,i),(x,j)\}$, $\{(x,i),(x,i),(y,i)\}$, $\{(x,i),(x,i),(y,j)\}$, $\{(x,i),(x,j),(x,i)\}$, $\{(x,i),(x,j),(x,j)\}$, $\{(x,i),(x,j),(y,i)\}$, $\{(x,i),(x,j),(y,j)\}$, $\{(x,i),(x,j),(x,k)\}$, $\{(x,i),(x,j),(y,k)\}$, $\{(x,i),(y,i),(x,i)\}$, $\{(x,i),(y,i),(x,j)\}$, $\{(x,i),(y,i),(y,i)\}$, $\{(x,i),(y,i),(y,j)\}$, $\{(x,i),(y,i),(z,i)\}$, $\{(x,i),(y,i),(z,j)\}$, $\{(x,i),(y,j),(x,i)\}$, $\{(x,i),(y,j),(x,j)\}$, $\{(x,i),(y,j),(y,i)\}$, $\{(x,i),(y,j),(y,j)\}$, $\{(x,i),(y,j),(z,i)\}$, $\{(x,i),(y,j),(z,j)\}$, $\{(x,i),(y,j),(x,k)\}$, $\{(x,i),(y,j),(y,k)\}$, $\{(x,i),(y,j),(z,k)\}$.

When we consider $j \neq i,\ j \neq k,\ k \neq i$, we assume that $j = i+1$ and $k = i-1$ or $j = i-1$ and $k = i+1$. We identify 59 different sets of triples of elements and calculate the associators of each set. We found that in the first 37 triples the associator is different from 1, as listed below:

$\{(x,i),(x,i+1),(y,i)\}$, $\{(x,i),(x,i-1),(y,i)\}$, $\{(x,i),(x,i+1),(y,i+1)\}$,
$\{(x,i),(y,i),(x,i+1)\}$, $\{(x,i),(y,i),(x,i-1)\}$, $\{(x,i),(y,i),(y,i-1)\}$,
$\{(x,i),(y,i),(z,i)$, where $z \neq \frac{x+y}{2}$ and $x \neq \frac{y+z}{2}\}$,
$\{(x,i),(y,i),(z,i)$, where $z \neq \frac{x+y}{2}$ and $x = \frac{y+z}{2}\}$,
$\{(x,i),(y,i),(z,i)$, where $z = \frac{x+y}{2}$ and $x \neq \frac{y+z}{2}\}$,
$\{(x,i),(y,i),(z,i)$, where $z = \frac{x+y}{2}$ and $x = \frac{y+z}{2}\}$,
$\{(x,i),(y,i),(z,i+1)$, where $z \neq \frac{x+y}{2}\}$, $\{(x,i),(y,i+1),(x,i+1)\}$,
$\{(x,i),(y,i),(z,i-1)$, where $z \neq \frac{x+y}{2}$ and $x \neq 2y-z\}$,
$\{(x,i),(y,i),(z,i-1)$, where $z = \frac{x+y}{2}$ and $x \neq 2y-z\}$,
$\{(x,i),(y,i),(z,i-1)$, where $z = \frac{x+y}{2}$ and $x = 2y-z\}$,
$\{(x,i),(y,i-1),(x,i-1)\}$, $\{(x,i),(y,i+1),(y,i)\}$, $\{(x,i),(y,i-1),(y,i)\}$,
$\{(x,i),(y,i+1),(z,i)$, where $z \neq 2y-x\}$,
$\{(x,i),(y,i-1),(z,i)$, where $z \neq 2x-y$ and $x \neq 2z-y\}$,
$\{(x,i),(y,i-1),(z,i)$, where $z \neq 2x-y$ and $x = 2z-y\}$,
$\{(x,i),(y,i-1),(z,i)$, where $z = 2x-y$ and $x \neq 2z-y\}$,
$\{(x,i),(y,i-1),(z,i)$, where $z = 2x-y$ and $x = 2z-y\}$,
$\{(x,i),(y,i+1),(z,i+1)$, where $z \neq 2y-x$ and $x \neq \frac{y+z}{2}\}$,
$\{(x,i),(y,i+1),(z,i+1)$, where $z \neq 2y-x$ and $x = \frac{y+z}{2}\}$,
$\{(x,i),(y,i+1),(z,i+1)$, where $z = 2y-x$ and $x = \frac{y+z}{2}\}$,
$\{(x,i),(y,i-1),(z,i-1)$, where $z \neq 2x-y\}$, $\{(x,i),(y,i+1),(x,i-1)\}$,
$\{(x,i),(y,i-1),(x,i+1)\}$, $\{(x,i),(y,i+1),(y,i-1)\}$,
$\{(x,i),(y,i+1),(z,i-1)$, where $z \neq 2y-x$ and $x \neq 2z-y\}$,
$\{(x,i),(y,i+1),(z,i-1)$, where $z = 2y-x$ and $x \neq 2z-y\}$,
$\{(x,i),(y,i+1),(z,i-1)$, where $z = 2y-x$ and $x = 2z-y\}$,
$\{(x,i),(y,i-1),(z,i+1)$, where $z \neq 2x-y$ and $x \neq 2y-z\}$,
$\{(x,i),(y,i-1),(z,i+1)$, where $z \neq 2x-y$ and $x = 2y-z\}$,

$\{(x,i),(y,i-1),(z,i+1)$, where $z=2x-y$ and $x=2y-z\}$,
$\{(x,i),(x,i-1),(y,i+1)\}$.

Next, there are 14 triples for which the associator is 1 and they are in the same triple of the STS; consequently, they are in a Klein group (and so generate a subgroup).

$\{(x,i),(x,i),(x,i)\}$, $\{(x,i),(x,i),(x,j)\}$, $\{(x,i),(x,i),(y,i)\}$, $\{(x,i),(x,i),(y,j)\}$,
$\{(x,i),(x,j),(x,i)\}$, $\{(x,i),(x,j),(x,j)\}$, $\{(x,i),(y,i),(x,i)\}$, $\{(x,i),(y,i),(y,i)\}$,
$\{(x,i),(y,i),(z,i+1)$, where $z=\frac{x+y}{2}\}$, $\{(x,i),(y,j),(x,i)\}$, $\{(x,i),(y,j),(y,j)\}$,
$\{(x,i),(y,i+1),(z,i)$, where $z=2y-x\}$,
$\{(x,i),(y,i-1),(z,i-1)$, where $z=2x-y\}$, $\{(x,i),(x,j),(x,k)\}$

There remain 8 cases to consider:

$\{(x,i),(x,i-1),(y,i-1)\}$, $\{(x,i),(y,i),(y,i+1)\}$,
$\{(x,i),(y,i-1),(y,i+1)\}$, $\{(x,i),(x,i+1),(y,i-1)\}$,
$\{(x,i),(y,i),(z,i-1)$, where $x=2y-z, z\neq\frac{x+y}{2}\}$,
$\{(x,i),(y,i+1),(z,i+1)$ where $z=2y-x, x\neq\frac{y+z}{2}\}$,
$\{(x,i),(y,i+1),(z,i-1)$ where $z\neq 2y-x, x=2z-y\}$,
$\{(x,i),(y,i-1),(z,i+1)$ where $z=2x-y, x\neq 2y-z\}$

Each has associator different from 1 because 7 is invertible in $\mathbb{Z}_n$. Take for instance the triple $\{(x,i),(x,i+1),(y,i-1)\}$ with $x\neq y$ of the STS. Now $(x,i)*((x,i+1)*(y,i-1))=(4y-3x,i)$ and $((x,i)*(x,i+1))*(y,i-1)=(\frac{x+y}{2},i)$. The associator $((x,i),(x,i+1),(y,i-1))$ is 1 if and only if $7x=7y$. Because 7 is invertible in $\mathbb{Z}_n$, we obtain $x=y$, a contradiction. □

3. Beyond Steiner loops

We have seen that certain Steiner loops from the Bose construction provide examples of loops satisfying $\mathcal{MP}$. Further examples can be obtained by the direct product of loops, the proof of which is straightforward:

Lemma 3.1. *Let S and M be loops that satisfy Moufang's theorem. Then $S\times M$ satisfies Moufang's theorem, and $S\times M$ satisfies $\mathcal{MP}$ if one or both of S and M satisfy $\mathcal{MP}$.*

Taking S to satisfy $\mathcal{MP}$ and M to be a group or a Moufang loop provides numerous examples of loops that satisfy $\mathcal{MP}$ but are neither Steiner nor Moufang loops. A characterization of loops that satisfy Moufang's theorem must therefore consider loops beyond the varieties examined here.

References

[1] **C.J. Colbourn, M.L. Merlini Giuliani, A. Rosa, and I. Stuhl**, *Steiner loops satisfying Moufang's theorem*, Australasian J. Combinatorics **63** (2015), 170–181.

[2] **B. Ganter and U. Pfüller**, *A remark on commutative di-associative loops*, Algebra Univ. **21** (1985), 310-311.

[3] **R. Moufang**, *Zur Struktur von Alternativkörpern*, Math. Ann. **110** (1935), 416-430.

[4] **H.O. Pflugfelder**, *Quasigroups and Loops: Introduction*, Heldermann Verlag, 1990.

[5] **K. Strambach and I. Stuhl**, *Translation group of Steiner loops*, Discrete Math. **309** (2009), 4225-4227.

[6] **K. Strambach and I. Stuhl**, *Oriented Steiner loops*, Beitr Algebra Geom. bf 54 (2013), 131-145.

[7] **I. Stuhl**, *Moufang's theorem for non-Moufang loops*, Aequationes Math. **90** (2016), $329 - 333$.

[8] **J.H. Van Lint and R.M. Wilson**, *A course in combinatorics*, Camb. Uni. Press, 2001.

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

Received March 26, 2015
Revised January 10, 2016

M.L. Merlini Giuliani and G.S. Anjos
Universidade Federal do ABC, Santo André (SP), 09210-180 Brazil
E-mail: maria.giuliani@ufabc.edu.br

C.J. Colbourn
School of CIDSE, Arizona State University, Tempe, AZ 85287, U.S.A
E-mail: giliard.anjos@ufabc.edu.br