Minimally nonassociative Moufang loops with a unique nonidentity commutator are ring alternative

Orin Chein, Edgar G. Goodaire

Abstract. We investigate finite Moufang loops with a unique nonidentity commutator which are not associative, but all of whose proper subloops are associative. Curiously, perhaps, such loops turn out to be "ring alternative", in the sense that their loop rings are alternative rings.

Keywords: Moufang loops, RA loops, alternative rings, minimal nonassociativity

Classification: Primary 20N05

1. Introduction

A *Moufang* loop is a loop which satisfies any of the following three (equivalent) identities:

$$(xy \cdot x)z = x(y \cdot xz) \qquad \text{the left Moufang identity,}$$
$$(xy \cdot z)y = x(y \cdot zy) \qquad \text{the right Moufang identity,}$$

and

$$(xy)(zx) = (x \cdot yz)x \qquad \text{the middle Moufang identity.}$$

The most important property of a Moufang loop was found by R. Moufang herself [Pfl90, Section IV.2]: the subloop generated by any three elements which associate (in some order) is always associative. Since $(xx)z = x(xz)$ in a Moufang loop (put $y = 1$ in the left Moufang identity), the subloop generated by any two elements x and z is associative. That is, Moufang loops are *diassociative*. Traditionally, the standard western reference for the theory of loops was the monograph by R.H. Bruck [Bru58]. Two other more recent sources of information, both written

Research of the first author was supported by a Summer Research grant from Temple University.

Research of the second author was supported in part by the Natural Sciences and Engineering Research Council of Canada, Grant No. OGP0009087.

in a more leisurely style, are a textbook by Hala Pflugfelder [Pfl90] and Chapter II of a monograph by the second author, E. Jespers and C.P. Milies [GJM96].

In this paper, we call a Moufang loop *minimally nonassociative* if it is not associative but all its proper subloops are associative. Evidently, this condition is equivalent to the statement that L is generated by any three elements which do not associate. A minimally nonassociative loop must be indecomposable because $L = G \times H$ with G and H proper subloops implies that L is associative.

If x, y and z are elements of a loop L, we denote by (x, y) the commutator of x and y and, by (x, y, z), the associator of x, y and z. These elements are defined by the equations

$$xy = (yx)(x, y) \quad \text{and} \quad (xy)z = (x \cdot yz)(x, y, z).$$

We begin with two lemmas, the first due to R.H. Bruck [Bru58, Lemma 5.5, p. 125] and the second to the authors [CG90b, Lemma 3].

Lemma 1.1. *Let L be a Moufang loop in which $(x, y, (y, z)) = 1$ is an identity. Then $(x^n, y, z) = (x, y, z)^n$ for all $x, y, z \in L$ and all integers n. Moreover, the associator (x, y, z) lies in the centre of the subloop generated by x, y and z.*

Lemma 1.2. *Let L be a Moufang loop with a unique nonidentity commutator s. Then s is central of order 2, $(x^2, y) = 1$ for all $x, y \in L$ and, for any $x, y, z \in L$, $(x, y, z)^3$ is either 1 or s. Moreover, L is an extra loop (see Section 2 for the definition) if and only if s is also a unique nonidentity associator in L.*

Our interest in minimally nonassociative Moufang loops derives from a 1903 paper by G.A. Miller and H.C. Moreno, who studied nonabelian groups, all of whose proper subgroups are abelian ([MM03]). Such groups, together with a construction of the first author ([Che74, Theorem 1]), lead quickly to a family of minimally nonassociative Moufang loops. Let G be a group, u an element not in G and $L = G \cup Gu$ the disjoint union of G and $Gu = \{gu \mid g \in G\}$. Extending the multiplication from G to L by the rules

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^{-1})u \\ (gu)(hu) &= h^{-1}g \end{aligned} \tag{1.1}$$

produces a Moufang loop, denoted $M(G, 2)$, which is not associative if and only if G is not abelian ([Che74]). Clearly, if $M(G, 2)$ is minimally nonassociative, then G must be one of the groups arising in the work of Miller and Moreno, and the converse is also true because of the lemma which follows.

Lemma 1.3. *Let G be a nonabelian group and let K be a subloop of the Moufang loop $L = M(G, 2)$. Then either K is a subgroup of G or $K = M(H, 2)$ where H is some subgroup of G.*

Proof: If $K \subseteq G$ there is nothing to prove, so assume there is an element of the form $v = au$ in K. We prove that $K = K_1 \cup K_1 v = M(K_1, 2)$, with $K_1 = K \cap G$. Clearly, $K_1 \subseteq K$ and $K_1 v \subseteq K$, by closure, so it suffices to show $K \subseteq K_1 \cup K_1 v$. Let $x \in K$. Then $x \in K_1$ or else $x = gu$ for some $g \in G$. In the latter case, $x = gu = (a^{-1}g)(au) = (a^{-1}g)v \in K_1 v$ since $a^{-1}g$ is clearly in G and $a^{-1}g = (gu)(au) \in K_1$. This establishes $K \subseteq K_1 \cup K_1 v$ and so $K = K_1 \cup K_1 v$. It remains to show that multiplication in K is in accordance with the rules given in (1.1). This is the case since, for $g, h \in G$,

$$g(hv) = g[h(au)] = g(ah \cdot u) = (ahg)u = (hg)(au) = (hg)v$$
$$(gv)h = (g \cdot au)h = (ag \cdot u)h = (agh^{-1})u = (gh^{-1})(au) = (gh^{-1})v$$

and

$$(gv)(hv) = [(ag)u][(ah)u] = (ah)^{-1}(ag) = h^{-1}g.$$

□

Corollary 1.4. *Let G be a nonabelian group. The Moufang loop $M(G, 2)$ is minimally nonassociative if and only if G has the "Miller-Moreno property": every proper subgroup of G is abelian.*

Many of the loops which appear in this paper are of the form $M(G, *, g_0)$, a type more general than $M(G, 2)$. These too were originally identified by the first author ([Che78, Theorem 2′]). Within a decade, they came into prominence when it was discovered that if a loop ring RL is an alternative ring, where the coefficient ring R has characteristic different from 2, then $L = M(G, *, g_0)$ ([GP87], [GJM96, Theorem IV.3.1]).

To construct the loop $M(G, *, g_0)$, one starts with a nonabelian group G which possesses an *involution* $g \mapsto g^*$ (that is, an antiautomorphism of period two) such that gg^* is in the centre of G for all $g \in G$. Take a central element $g_0 \in G$ and an element u not in G and form the set $L = G \cup Gu$. Define multiplication in L by extending multiplication from G with the rules

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^*)u \\ (gu)(hu) &= g_0 h^* g. \end{aligned} \tag{1.2}$$

Then L is a Moufang loop, denoted $M(G, *, g_0)$ ([GJM96, § II.5.2]), which is not associative. As noted, certain loops of this kind are *ring alternative*, RA for short; that is, they have alternative loop rings in characteristic different from 2, and hence in any characteristic ([CG90a, Corollary 2.4]). Curiously, the loops which arise in this paper are ring alternative.

2. Main results

The *centrum* of a loop L is the set

$$\mathcal{C}(L) = \{a \in L \mid (a, x) = 1 \text{ for all } x \in L\},$$

the *nucleus* is the subloop

$$\mathcal{N}(L) = \{a \in L \mid (a, x, y) = (x, a, y) = (x, y, a) \text{ for all } x, y \in L\}$$

and the *centre* is the (normal) subloop

$$\mathcal{Z}(L) = \{a \in \mathcal{N}(L) \mid (a, x) = 1 \text{ for all } x \in L\}.$$

A loop is *extra* if it satisfies the identity

$$(xy \cdot z)x = x(y \cdot zx).$$

Extra loops were investigated by F. Fenyves, who showed that they are Moufang ([Fen68]). Later, D.A. Robinson and the first author showed that extra loops are precisely those Moufang loops in which all squares of elements are in the nucleus ([CR72]).

Theorem 2.1. *Let L be a minimally nonassociative finite Moufang loop with a unique nonidentity commutator, s. Then s is also a unique nonidentity associator and L is an RA loop; that is, for any (commutative, associative) coefficient ring R, the loop ring RL is alternative.*

Proof: By Lemma 1.2, s is central of order 2 and $x^2 \in \mathcal{C}(L)$ for any x. Let x and y be elements of L which do not commute. Using diassociativity, we have

$$\begin{aligned}
(xy)^2 &= xyxy = sx^2y^2 \\
(xy)^3 &= sx^2y^2xy = sx^3y^3 && \text{since } y^2 \in \mathcal{C}(L) \\
(xy)^4 &= sx^3y^3xy \\
&= sx^3y^2yxy \\
&= s^2x^3y^2xy^2 = x^4y^4 && \text{since } s^2 = 1
\end{aligned}$$

and, in general,

$$(xy)^n = \begin{cases} x^n y^n & n \equiv 0 \text{ or } 1 \pmod 4 \\ sx^n y^n & n \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Thus

$$(xy)^{2^t} = x^{2^t} y^{2^t}$$

for any $t \geq 0$, an equation which holds also in the case that x and y commute. It follows that the set L_0 of elements in L which have 2-power order is a subloop of L_0 and a normal subloop since inner maps in a Moufang loop preserve order. (See [GJM96, § 1.9 and Theorem 3.3].) Now let x be an element of odd order $2k+1$. Then $x = (x^{-k})^2$ shows that $x \in \mathcal{C}(L)$. We conclude that the subset A of L consisting of elements of odd order is also a normal subloop of L. An elementary argument shows that $L = L_0 A$ and hence $L \cong L_0 \times A$. Since a minimally nonassociative loop is indecomposable, it follows that $L = L_0$ is a 2-loop.

Next, we note that centrality of s implies the identity $(x, y, (y, z)) = 1$, so, by Lemma 1.1, the associator (x, y, z) lies in the centre of the subloop generated by x, y, z. Since L is minimally nonassociative (and hence generated by any three elements which do not associate), this subloop is either trivial or the entire loop L. It follows that associators in L are central and that $L/\mathcal{Z}(L)$ is an abelian group.

Let $x, y, z \in L$. Lemma 1.2 implies that $(x, y, z)^6 = 1$ and so, since L is a 2-loop, $(x, y, z)^2 = 1$. By Lemma 1.1, $(x^2, y, z) = (x, y, z)^2 = 1$. Thus, $x^2 \in \mathcal{N}(L)$ for any $x \in L$, so L is an extra loop by [CR72] and Lemma 1.2 tells us that s is a unique nonidentity associator. Since also $x^2 \in \mathcal{C}(L)$, we have in fact that $x^2 \in \mathcal{Z}(L)$ for any x. Thus $L/\mathcal{Z}(L)$ is an abelian group of exponent 2. Since L can be generated by 3 elements, the same is true for $L/\mathcal{Z}(L)$, so $L/\mathcal{Z}(L) \cong C_2 \times C_2 \times C_2$. (Note that if there were some collapsing and $L/\mathcal{Z}(L)$ could be generated by two elements, then L would be associative, contrary to assumption.)

It is easily seen that $L = \langle \mathcal{Z}(L), a, b, u \rangle$ is generated by its centre and three elements a, b, u. Since L is not commutative, we may pick these elements so that $ab \neq ba$. Let $G = \langle \mathcal{Z}(L), a, b \rangle$ be the subloop of L generated by a, b and $\mathcal{Z}(L)$. By diassociativity and the definition of centre, G is a group. Since it contains a and b, it is not abelian and it contains s.

Since $g_0 = u^2 \in \mathcal{Z}(L) \subseteq G$ and $\theta\colon g \mapsto u^{-1}gu$ maps G to G — after all, $u^{-1}gu$ is either g or sg — we may apply Theorem 1 of [Che78] and conclude that $L = G \cup Gu$ with multiplication given by the rules

$$\begin{aligned} g(hu) &= [(g\theta)(h\theta)]\theta^{-1}u \\ (gu)h &= [g(h\theta^{-1})]u \\ (gu)(hu) &= [(g\theta)h]\theta^{-1}g_0, \end{aligned}$$

where $g, h \in G$. We claim that θ is an antihomomorphism, in which case these rules are precisely those of (1.2) with $* = \theta$. Since, $gg^* = gu^{-1}gu = g^2$ or sg^2 is central, it would follow immediately that $L = M(G, *, g_0)$.

To prove that θ is an antihomomorphism, we must prove that

$$u^{-1}(xy)u = (u^{-1}yu)(u^{-1}xu) \tag{2.1}$$

for all $x, y \in G$. Since a^2 and b^2 are central, the quotient group $G/\mathcal{Z}(G) \cong C_2 \times C_2$. Thus $G = \mathcal{Z} \cup \mathcal{Z}a \cup \mathcal{Z}b \cup \mathcal{Z}ab$. If x is central, both sides of (2.1) are $xu^{-1}yu$. If x and y come from the same one of the three cosets $\mathcal{Z}a$, $\mathcal{Z}b$, $\mathcal{Z}ab$, then $xy \in \mathcal{Z}$ (note that $abab = sa^2b^2$), so $y = zx$ for some $z \in \mathcal{Z}$, and each side of (2.1) is $zu^{-1}x^2u$, by diassociativity. Suppose x and y are in different cosets (and neither is central). Then $(x, y) \neq 1$. Also, x, y and u do not associate because a, b and u do not associate. Thus x, y and u^{-1} do not associate, so $(x, y) = s = (x, y, u^{-1})$. Let $t = (u^{-1}yu)(u^{-1}xu)$. By the right Moufang identity, diassociativity and the centrality of u^2,

$$tu = (u^{-1}y)[u(u^{-1}xu)u] = (u^{-1}y)(xu^2) = (u^{-1}y \cdot x)u^2.$$

Since commutators and associators in L are central,

$$\begin{aligned} t &= (u^{-1}y \cdot x)u \\ &= (u^{-1} \cdot yx)u(u^{-1}, y, x) \\ &= u^{-1}(yx)u(u^{-1}, y, x) \\ &= [u^{-1}(xy)u](x, y)(u^{-1}, y, x) = u^{-1}(xy)u, \end{aligned}$$

the last equality following from $(x, y) = s = (u^{-1}, y, x)$. We have established that θ is indeed an antihomomorphism, so $L = M(G, *, g_0)$ with $* = \theta$.

Since $G/\mathcal{Z}(G) \cong C_2 \times C_2$, G has the so-called "LC property" ([CG86, pp. 305–306], [GJM96, Proposition III.3.6]). Thus L is an RA loop by [GJM96, Corollary III.3.4].

$\square$

3. Loops of the form $M(G, *, g_0)$

This paper has brought to the fore once again loops of the form $M(G, *, g_0)$. In this final section, we determine when such loops are minimally nonassociative and, in particular, which RA loops are minimally nonassociative. Corollary 1.4 gave the answer when $g^* = g^{-1}$ and $g_0 = 1$.

Theorem 3.1. *Let $L = M(G, *, g_0)$ for some nonabelian group G, involution $g \mapsto g^*$ of G and $g_0 \in \mathcal{Z}(G)$. If L is minimally nonassociative and $H^* \subseteq H$ for every nonabelian subgroup H of G, then $G = \langle a, b, g_0\rangle$ for any noncommuting elements $a, b \in G$. Conversely, if G is a 2-group such that $G = \langle a, b, g_0\rangle$ whenever $a, b \in G$ do not commute (for example, if G is a 2-group with the Miller-Moreno property), then L is minimally nonassociative.*

Proof: Suppose L is minimally nonassociative and $a, b \in G$ do not commute. Then $H = \langle a, b, g_0\rangle$ is a nonabelian group and $L_1 = M(H, *, g_0)$ is a subloop of L which is not associative. Thus $L_1 = L$, so $H = G$. Conversely, let G be a 2-group and suppose $G = \langle a, b, g_0 \rangle$ for any noncommuting elements $a, b \in G$. Let x, y and z be any three elements of L which do not associate. We prove that $\langle x, y, z \rangle = L$. There are apparently eight cases to explore, according as x, y, z are of the form g or gu, $g \in G$. In fact, observations such as $\langle g, hu, ku \rangle = \langle g, (hu)(ku), ku \rangle$ and $(hu)(ku) \in G$, show that it is sufficient simply to examine the case $x = g$, $y = h$, $z = ku$, with $g, h, k \in G$.

Let $a = (g, h, ku)$ be the associator of g, h and ku. Since

$$(gh)(ku) = (kgh)u \quad \text{and} \quad g(h \cdot ku) = g(kh \cdot u) = (khg)u,$$

we must have $(kgh)u = [(khg)u]a$. It follows that $a \in G$ and $kgh = khga^*$ so that $a^* = g^{-1}h^{-1}gh = (g, h)$. Since $(x, y, z) \neq 1$, it follows that $(g, h) \neq 1$ so, by hypothesis, $G = \langle g, h, g_0 \rangle$. Write $k = wg_0^\gamma$ with w a word in g and h. We have

$$\langle g, h, ku \rangle = \langle g, h, g_0^\gamma u \rangle = \langle g, h, u^{2\gamma+1} \rangle$$

since $g_0 = u^2$. Since G is 2-group, $u^n = 1$ for some n, a power of 2. Writing $in + j(2\gamma + 1) = 1$ for integers i and j, we have $u = u^{in+j(2\gamma+1)} = (u^{2\gamma+1})^j$ and so $\langle g, h, ku \rangle = \langle g, h, u \rangle$. But $g_0 = u^2$, so $G = \langle g, h, g_0 \rangle \subseteq \langle g, h, u \rangle$. Thus $L = G \cup Gu \subseteq \langle g, h, u \rangle$, which implies equality and the desired result. □

Corollary 3.2. *An RA loop L in which every element has finite order is minimally nonassociative if and only if it is indecomposable and of the form $L = M(G, *, g_0)$ for some nonabelian group which satisfies $G = \langle a, b, g_0 \rangle$ for any noncommuting elements $a, b \in G$.*

Proof: Suppose the RA loop L is minimally nonassociative. We remarked in the introduction that L must be indecomposable. It is known that L is of the form $L = M(G, *, g_0)$ and that L has a unique nonidentity commutator s such that $g^* = g$ or $g^* = sg$ for $g \in G$ ([GJM96, Theorem IV.3.1]). It follows readily that $H^* \subseteq H$ for any nonabelian subgroup H of G, so $G = \langle a, b, g_0 \rangle$ for any noncommuting elements $a, b \in G$ by the theorem.

The converse follows directly from Theorem 3.1 because if every element of an RA loop $L = M(G, *, g_0)$ has finite order and L is indecomposable, then G is a 2-group ([CG86, Theorem 6], [GJM96, Corollary V.1.4]. □

Remark 3.3. Finite indecomposable RA loops fall into seven categories which have been denoted $\mathcal{L}_1, \dots, \mathcal{L}_7$ ([JLM95], [GJM96, § V.3]). Direct application of Corollary 3.2 shows that all loops in classes $\mathcal{L}_2$, $\mathcal{L}_4$ and $\mathcal{L}_6$ are minimally nonassociative.

References

[Bru58] Bruck R.H., *A survey of binary systems*, Ergeb. Math. Grenzgeb., vol. 20, Springer-Verlag, 1958.

[CG86] Chein O., Goodaire E.G., *Loops whose loop rings are alternative*, Comm. Algebra **14** (1986), no. 2, 293–310.

[CG90a] Chein O., Goodaire E.G., *Loops whose loop rings in characteristic* 2 *are alternative*, Comm. Algebra **18** (1990), no. 3, 659–688.

[CG90b] Chein O., Goodaire E.G., *Moufang loops with a unique nonidentity commutator* (*associator, square*), J. Algebra **130** (1990), no. 2, 369–384.

[Che74] Chein O., *Moufang loops of small order I*, Trans. Amer. Math. Soc. **188** (1974), 31–51.

[Che78] Chein O., *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. 197, 1–131.

[CR72] Chein O., Robinson D.A., *An "extra" law for characterizing Moufang loops*, Proc. Amer. Math. Soc. **33** (1972), 29–32.

[Fen68] Fenyves F., *Extra loops I*, Publ. Math. Debrecen **15** (1968), 235–238.

[GJM96] Goodaire E.G., Jespers E., Polcino Milies C., *Alternative loop rings*, North-Holland Math. Studies, vol. 184, Elsevier, Amsterdam, 1996.

[GP87] Goodaire E.G., Parmenter M.M., *Semi-simplicity of alternative loop rings*, Acta Math. Hungar. **50** (1987), no. 3–4, 241–247.

[JLM95] Jespers E., Leal G., Polcino Milies C., *Classifying indecomposable RA loops*, J. Algebra **176** (1995), 5057–5076.

[MM03] Miller G.A., Moreno H.C., *Nonabelian groups in which every subgroup is abelian*, Trans. Amer. Math. Soc. **4** (1903), 398–404.

[Pfl90] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.

Department of Mathematics, Temple University, Philadelphia, PA 19122, U.S.A.

E-mail: orin@math.temple.edu

Memorial University of Newfoundland, St. John's, Newfoundland A1C 5S7, Canada

E-mail: edgar@math.mun.ca

(*Received* April 19, 2001, *revised* May 7, 2001)