THREE-GENERATOR MOUFLANG LOOPS

ORIN CHEIN AND EDGAR G. GOODAIRE

ABSTRACT. This paper considers the following question: “Which classes of Moufang loops have the property that the minimally nonassociative loops in the class are precisely those which are indecomposable and which can be generated by three elements?” It was shown previously [CGa] that the class of commutative Moufang loops has this property. Here we investigate several other classes of Moufang loops and find some which do have this property as well as some which do not.

1. Introduction

Motivated by a paper of Miller and Moreno [MM03], in which they investigate nonabelian groups in which every proper subgroup is abelian, we began our study of minimally nonassociative Moufang loops in [CGa]. In the current paper, we call a group of the type studied by Miller and Moreno an MM group, and we call a Moufang loop an MNA loop if it is minimally nonassociative - that is, if it is not associative but all its proper subloops are associative.

Since Moufang loops are diassociative (that is, any two elements generate an associative subloop), nonassociativity for a Moufang loop \( L \) is equivalent to the statement that \( L \) is generated by any three elements which do not associate. Note also that an MNA loop must be indecomposable because \( L = G \times H \) with \( G \) and \( H \) proper subloops implies that \( L \) is associative.

In [CGa], we proved that for commutative Moufang loops (CML’s), these two necessary conditions are sufficient for minimal nonassociativity. That is, a CML is MNA if and only if it is indecomposable and can be generated by three elements.

We say that a class of Moufang loops has Property 3I if loops in the class are MNA if and only if they are indecomposable and can be generated by three elements.

It is natural to ask whether the class of all Moufang loops is characterized by these two properties.

That the answer is no can be seen by the following example.

Example 1.1. Consider the smallest simple Moufang loop, of order 120 [Pai56]. This is clearly indecomposable, and it can be generated by three elements [Voj]. But it
is not minimally nonassociative since it contains nonassociative subloops of orders 12 and 24 [MG].

This then raises the question of whether any classes of Moufang loops other than CML’s have Property 3I. We will identify other such classes below. In Section 2, we present some preliminary results which will be used throughout the paper. Section 3 considers when Moufang loops of type $M(G, *, g_0)$ can be generated by three elements and investigates the connection between when loops of this type are MNA and when the group $G$ is MM. Section 4 considers the class of nilpotent nonassociative Moufang loops. Although this class of loops is seen not to have Property 3I, we identify some subclasses which do have the property in question. These subclasses include small Frattini Moufang loops, Moufang loops with a unique nontrivial commutator (which includes the class of RA loops) and loops of type $M(G, *, g_0)$ which are nilpotent of class two. Finally, in Section 5 we identify precisely which RA loops can be generated by three elements.

2. Preliminaries

Although some of the results of this paper carry over to infinite loops, we will assume in the remainder of this paper that all loops under consideration are finite Moufang loops. We refer the reader to [Pfl90] or [Bru58] for the basic definitions and properties of Moufang loops.

For most Moufang loops considered in this paper, the centre $Z(L)$ will be of some interest. Except when there is the possibility of confusion, we will simply denote this centre by $Z$ throughout the paper.

**Lemma 2.1.** Let $G$ be a nonabelian group which can be generated by two elements, say $G = \langle g, h \rangle$, and suppose that squares are central in $G$. Then

1) $G/Z(G) \cong C_2 \times C_2$,

2) every element of $G$ can be expressed in the form $g^{a}h^{b}s^{\gamma}$, where $s = (g, h)$ and where $0 \leq \gamma \leq 1$,

3) $s$ is the unique nontrivial commutator of $G$,

4) $Z(G) = \langle g^2, h^2, s \rangle$.

**Proof.** 1) Since squares are central in $G$, $G/Z(G)$ is an elementary abelian 2-group. But $G = \langle g, h \rangle$, so $G/Z(G) = \langle gZ(G), hZ(G) \rangle$ can be generated by two elements. Therefore $G/Z \subseteq C_2 \times C_2$. If $G/Z(G)$ were a proper subgroup, it would be cyclic, forcing $G$ to be abelian, contrary to assumption. Therefore $G/Z(G) \cong C_2 \times C_2$.

2) The commutator $s = (g, h)$ is central since $(g, h) = g^{-1}h^{-1}gh = g^{-2}(gh^{-1})^2h^2 \in Z(G)$. Therefore, using the centrality of $g^2$ and the standard commutator identities [Hal59, p. 150], $1 = (g^2, h) = (g, h)((g, h), g)(g, h) = (g, h)^2$, so $s^2 = 1$, and $(h, g) = (g, h)^{-1} = s^{-1} = s$. But then, $hg = gh(h, g) = ghs$, so any element in $G = \langle g, h \rangle$ can be expressed in the form $g^a h^b s^\gamma$. Since $s^2 = 1$, we can assume that $0 \leq \gamma \leq 1$.

3) Consider $x = (g^\alpha h^\beta s^\gamma, g^\pi h^\rho s^\sigma)$. Since $s$ and squares are central and can therefore be removed from commutators, there is no loss of generality in assuming that $x = (g^\alpha h^\beta, g^\pi h^\rho)$, where $0 \leq \alpha, \beta, \pi, \rho \leq 1$. Since $(g, g) = (h, h) = (gh, gh) = 1$, and
since \((g, gh) = (gh, g)^{-1}\) and \((h, gh) = (gh, h)^{-1}\), we need only consider \((gh, g)\) and \((gh, h)\). By the standard commutator identities, \((gh, g) = (g, g)((g, g), h)(h, g) = (h, g) = s^{-1} = s\), and \((gh, h) = (g, h)((g, h), h)(h, h) = (h, h) = s\). Thus, \(s\) is the unique nontrivial commutator.

4) Let \(z = (g^2 h b)^s \in Z(G)\). Then, since \(g^2, h^2\) and \(s\) are central, there is no loss of generality in assuming that \(0 \leq \alpha, \beta, \gamma \leq 1\). But since \(G = \langle g, h \rangle = \langle g, gh \rangle\) is not abelian, none of the elements \(g, h\) or \(gh\) can be central. Therefore \(\alpha\) and \(\beta\) must both be 0, and so \(z \in \langle g^2, h^2, s \rangle\).

\[\text{Lemma 2.2. Let } L \text{ be a nonassociative Moufang loop which can be generated by three elements, say } L = \langle a, b, c \rangle. \text{ Suppose that } L \text{ has a unique nontrivial commutator, } s, \text{ and that squares are central in } L. \text{ Then} \]

1) \(L/Z \cong C_2 \times C_2 \times C_2\),

2) every element in \(L\) may be expressed in the form \((a^\alpha b^\beta c^\gamma s^\delta, s^\delta)\),

3) \(Z = \langle a^2, b^2, c^2, s \rangle\).

**Proof.** Since \(s\) is the unique nontrivial commutator, it follows from [CG90, Lemma 3] that \(s^2 = 1\) and \(s \in Z\). Also, since squares are central, they are nuclear, and so \(L\) is an extra loop [CRT2, Corollary 2] and \(s\) is the unique nontrivial associator, also by Lemma 3 of [CG90].

1) Since \(L = \langle a, b, c \rangle\), then, since squares are central, \(L/Z = \langle aZ, bZ, cZ \rangle \subset C_2 \times C_2 \times C_2\). If \(L/Z\) were a proper subgroup, it could be generated by fewer than three elements, say \(xZ\) and \(yZ\), then \(L = \langle x, y \rangle Z = \langle x, y \rangle Z\) would be associative, by diassociativity, contrary to assumption. Therefore \(L/Z = C_2 \times C_2 \times C_2\).

2) Since the generators \(a\), \(b\), and \(c\) can all be expressed in the form \([(a^\alpha b^\beta c^\gamma)]s^\delta\), in order to see that every element of \(L\) can be expressed in this form, it is enough to see that the product of two elements in this form can again be expressed in this form.

Let \(d = \{(a^\alpha b^\beta c^\gamma)s^\delta \} \{(a^\pi b^\rho c^\sigma)s^\tau \}\). Then, by the centrality of \(s\) and the Moufang identities,

\[
dc^\tau = \{(a^\alpha b^\beta c^\gamma)s^\delta \} \{(a^\pi b^\rho c^\sigma)s^\tau \}c^\gamma = (a^\alpha b^\beta c^\pi b^\rho c^\sigma + \gamma)s^{\delta + \tau}
\]

\[
= (a^\alpha b^\beta)(a^\pi b^\rho)c^{\sigma + 2\gamma}s^\phi = [(a^\alpha b^\beta)(a^\pi b^\rho)]c^{\sigma + 2\gamma}s^\psi = [(a^{\alpha + \pi} b^{\beta + \rho})c^{\sigma + 2\gamma}]s^\mu,
\]

for some \(\phi, \psi, \mu\). Therefore, \(d = [(a^{\alpha + \pi} b^{\beta + \rho})c^{\sigma + 2\gamma}]s^\mu\).

3) Let \(z = [(a^\alpha b^\beta c^\gamma)]s^\delta \in Z\). Since \(a^2, b^2, c^2\) and \(s\) are central, there is no loss of generality if we assume that \(0 \leq \alpha, \beta, \gamma \leq 1\). But since \(L = \langle a, b, c \rangle = \langle ac, bc, c \rangle = \langle a, ab, (ab)c \rangle\) is not associative, none of the elements \(a, b, c, ab, ac, bc, (ab)c\) can be central. Therefore \(\alpha, \beta, \gamma\) must all be 0. Therefore, \(z \in \langle a^2, b^2, c^2, s \rangle\). \[\square\]

### 3. Loops of Type \(M(G, *, g_0)\)

We begin this section by recalling a construction first introduced in [Che78, Theorem 2'], (See also [GJM96, §II.5.2]),

Let \(G\) be a group 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 \(g_0 \in G\) which is fixed by * 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

$$g(hu) = (hg)u$$

(3.1)

$$(gu)h = (gh^*)u$$

$$(gu)(hu) = h^*gg_0.$$  

Then $L$ is a Moufang loop, denoted $M(G, +, g_0)$, which is associative if and only if $G$ is abelian.

**Remark 3.1.** Note that $gg^* = g^*g$, since $(g^*g)g = g(g^*g) = (gg^*)g$. Also, for $g$ and $h$ in $G$, $(gh)(gh)^* = ghh^*g^* = g(gh^*)g = (gg^*)(hh^*)$, and, by induction, this generalizes to any number of elements of $G$.

**Remark 3.2.** It is also worth noting that if $v = ku$, where $k$ is any element of $G$, then we can use $v$ in place of $u$ in describing $L$. That is, for any $m = gu$ in $G$, $m = (k^{-1}g)(ku) = (k^{-1}g)v \in Gv$. Furthermore,

$$g(hv) = g[h(ku)] = g[(kh)u] = (khg)u = (hg)(ku) = (hg)v$$

(3.2)

$$(gv)h = [g(ku)]h = [(kg)u]h = (gh^*)u = (gh^*)(ku) = (gh^*)v$$

Thus, using $v$ in place of $u$, $L = G \cup Gv = M(G, +, kk^*g_0)$. Note that $*$ does not change and that $g_0$ is replaced by $kk^*g_0$.

As a special case of this construction (although, historically it preceded it [Che74, Theorem 1]), taking $*$ to be the inverse mapping and $g_0 = 1$, we obtain the loop $M(G, 2)$. In this case, (3.1) becomes

$$g(hu) = (hg)u$$

(3.3)

$$(gu)h = (gh^{-1})u$$

$$(gu)(hu) = h^{-1}g.$$  

**Remark 3.3.** If $L = G \cup Gu = M(G, 2)$, then replacing $u$ by $v = ku$ for $k \in G$ gives $L = G \cup Gv = M(G, 2)$, where (3.2) becomes

$$g(hv) = (hg)v$$

(3.4)

$$(gv)h = (gh^{-1})v$$

$$(gv)(hv) = h^{-1}g.$$  

Note that $v^2 = u^2 = g_0 = 1$.

**Remark 3.4.** If $L = M(G, +, g_0)$, then the centre, $Z(L) = \{z \in Z(G) \mid z^* = z\}$ [Che78, Corollary 5]. In the special case that $L = M(G, 2)$, $Z(L) = \{z \in Z(G) \mid z^2 = 1\}$ (since $z^* = z^{-1}$).

It is worth noting that, for any $g \in G$, not only is $gg^* \in Z(G)$, but, in fact, $gg^* \in Z(L)$, since $(gg^*)^* = g^*g^* = gg^*$. Similarly, $g_0 \in Z(L)$, since $g_0 \in Z(G)$ and $g_0$ is fixed by $*$. 


Lemma 3.5. If \( L = G \cup Gu = M(G, *, g_0) \) is a nonassociative Moufang loop which can be generated by three elements, then there exist elements \( g, h \in G \), \( v \in Gu \), with \( (g, h) \neq 1 \), such that \( L = \langle g, h, v \rangle \) and \( G = \langle g, gg^*, hh^*, kk^*g_0 \rangle \). In particular, if \( L = M(G, 2) \), then \( G = \langle g, h \rangle \).

Proof. Suppose that \( L = \langle a, b, c \rangle \). Since not all three of these elements can be in \( G \), there is no loss of generality if we assume that \( c = ku \), for some \( k \in G \). Also, since \( \langle a, b, c \rangle = \langle ab, b, c \rangle = \langle a, bc, c \rangle \), and since the product of two elements which lie outside \( G \) must lie in \( G \), there is also no loss in generality in assuming that \( a \in G \) and \( b \in G \). (I.e., if \( a \notin G \), then replace \( a \) by \( ac \), etc.) Let \( g = a \), \( h = b \) and \( v = c = ku \). Thus \( L = \langle g, h, v \rangle \). By (3.2),

\[
(ghv) = (g(hv))v = (ghhh')v = (ghhh')v = (ghhh')v = (ghhh')v
\]

the last equation following from Remark 3.6 and the centrality of \( hh^* \).

For any element \( m \in G \), \( mv \in L = \langle g, h, v \rangle \), so \( mv \) can be expressed as a word in \( g, h \) and \( v \). Using (3.5), we can bring any \( v \)'s to the right, obtaining \( mv = nv \), where \( n \in \langle g, h, gg^*, hh^*, kk^*g_0 \rangle \). Therefore, \( m = n \in \langle g, h, gg^*, hh^*, kk^*g_0 \rangle \), and, since \( m \) was an arbitrary element of \( G \), \( G = \langle g, h, gg^*, hh^*, kk^*g_0 \rangle \). Since \( G \) is not abelian, and since \( gg^*, hh^* \) and \( kk^*g_0 \) are central in \( G \), we must have \( (g, h) \neq 1 \).

In the case that \( L = M(G, 2) \), \( t^* = t^{-1} \) for any \( t \in G \), and \( g_0 = 1 \), so \( G = \langle g, h \rangle \). □

Remark 3.6. It is noteworthy that while the minimal number of generators for a loop of type \( M(G, 2) \) is always one more than the minimal number of generators for \( G \), Lemma 3.8 suggests that if \( L = M(G, *, g_0) \), then the minimal size of a generating set for \( L \) might actually be smaller than the minimal size of a set of generators for \( G \). That this may actually occur may be seen in the following example.

Example 3.7. Let \( G = Q_8 \times C_2 \times C_2 \times C_2 \), where \( Q_8 \) denotes the quaternions. Then

\[
G = \langle x, y, z, v, w \mid x^4 = z^2 = v^2 = w^2 = (x, z) = (x, v) = (x, w) = (y, z) = (y, v)
\]

\[
= (y, w) = (z, v) = (z, w) = (v, w) = 1, y^2 = (x, y)^2 = x^2 \rangle.
\]

Then \( G \) cannot be generated by fewer than five generators. To see this, note that \( G/\langle x^2 \rangle \cong C_2 \times C_2 \times C_2 \times C_2 \). Furthermore, every element \( g \in G \) may be expressed in the form \( g = x^\alpha y^\beta z^\gamma v^\delta w^\epsilon \), where \( 0 \leq \alpha \leq 3 \) and \( 0 \leq \beta, \gamma, \delta, \epsilon \leq 1 \). If \( h = x^\rho y^\sigma z^\tau v^\nu w^\phi \), then \( gh = x^{\alpha + \rho} y^{\beta + \sigma} z^{\gamma + \tau} v^{\delta + \nu} w^{\epsilon + \phi} \).

Define \( * \) on \( G \) by \( g^* = (x^\alpha y^\beta z^\gamma v^\delta w^\epsilon)^* = x^{\alpha + 2\alpha \beta} y^{\beta + 2\beta \gamma} z^{\gamma + 2\gamma \delta} v^{\delta + 2\delta \epsilon} w^{\epsilon + 2\epsilon \phi} \). Then, since \( x^4 = v^2 = w^2 = 1 \), \( (g^*)^* = g \). Furthermore, since \( z^2 = 1 \) and \( y^2 = x^2 \), \( gg^* \in \langle x^2, v, w \rangle \subseteq Z(G) = \langle x^2, z, v, w \rangle \). Finally,

\[
(gh)^* = x^{\alpha + \pi + 2\beta\pi + 2(\alpha + \pi + 2\beta\pi)(\beta + \rho)} y^{\beta + \rho \gamma + \sigma \epsilon + v + \alpha + 2\beta \pi + \delta + \tau} w^{\beta + \rho + \epsilon + \phi} = x^{\alpha + \pi + 2(\alpha \beta + \alpha \rho + \pi \rho)} y^{\beta + \rho \gamma + \sigma \epsilon + \delta + \pi + \tau} w^{\beta + \rho + \epsilon + \phi},
\]
Let $w \in G$, $H$ minimal nonassociativity of $G$, and then $H \subseteq K$.

Lemma 3.8. Thus $x^* = xv$ and $y^* = yw$. Let $g_0 = z$. Then $(g_0)^* = z^* = z$.

Thus we can form $L = G \cup Gu = M(G, *, g_0)$. Surely $\{x, y, z, v, w, u\}$ generates $L$. But $ux = x^*u = (xv)u$, so $v = x^{-1}uxu^{-1} \in \langle x, u \rangle$. Similarly, $w = y^{-1}(uy)u^{-1} \in \langle y, u \rangle$. Finally, $u^2 = g_0 = z$, so $z \in \langle u \rangle$. Putting these together, $z, v, w \in \langle x, y, u \rangle$, so $L = \langle x, y, u \rangle$. Thus, $L$ can be generated by three elements.

Note that since $Z(G) = \langle x^2, z, v, w \rangle$ and since each of these elements is fixed by *, $Z(L) = Z(G) = \langle x^2, z, v, w \rangle$.

Note also that all squares in $L$ are central, so that $L/Z(L)$ is an elementary abelian 2-group. Thus $L$ is nilpotent of class 2.

There is a connection between when a loop of type $M(G, *, g_0)$ is MNA and when $G$ is MM. To investigate this connection, we first need the following lemma.

**Lemma 3.8.** If $L = G \cup Gu = M(G, *, g_0)$ and if $K$ is a subloop of $L$ which is not contained in $G$, then there exists a subgroup $H$ of $G$ and an element $h_0$ in the centre of $H$ such that $K = M(H, *, h_0)$.

**Proof.** Let $H = K \cap G$, and let $v$ be any element of $K$ which is not in $H$. Then $v$ is not in $G$, so $v = au$ for some $a \in G$. Since $K$ is a subloop, $Hv \subseteq K$, so $H \cup Hv \subseteq K$.

We wish to prove equality. If $w \in K$, then either $w \in H$ or else $w = bu$ for some $b \in G$. But then $wv^{-1} = (bu)(au)^{-1} = (bu)((a^{-1})^*w)g_0^{-1} = a^{-1}b \in G$, so $wv^{-1} \in K \cap G = H$, and $w \in Hv$. Thus, $K = H \cup Hv$. Let $h_0 = v^2 = (au)^2 = a^*ag_0 \in G$.

But $v \in K$ and $K$ is closed, so $h_0 = v^2 \in K$. Thus $h_0 \in K \cap G = H$. That the required multiplication holds follows from (3.2). In particular, for $h \in H$, $vh = h^*v$, so $h^* = vhv^{-1} \in K \cap G = H$. Thus $H$ is closed under *, $M(H, *, h_0)$ is a loop, and $M(H, *, h_0) = K$, completing the proof. 

**Corollary 3.9.** Suppose that $L = M(G, *, g_0)$ for some $G$, * and $g_0$. If $G$ is an MM group then $L$ is MNA.

**Proof.** Since $G$ is MM, every proper subgroup, $H$, of $G$ is abelian, so, for any choice of $h_0 \in Z(H)$, $M(H, *, h_0)$ is associative. By Lemma 3.11, every proper subloop of $L$ is either a subgroup of $G$ or it is of the form $M(H, *, h_0)$ for some proper subgroup $H$ of $G$. In either case, $K$ is associative. 

In the case that $L = M(G, 2)$, the converse of this Corollary holds as well. (See [CGb, Corollary 1.4].)

**Corollary 3.10.** If $L = M(G, 2)$ is MNA, then $G$ is MM.

**Proof.** If $G$ were not MM, then it would contain a proper nonabelian subgroup $H$, and then $M(H, 2)$ would be a proper nonassociative subloop of $L$, contradicting the minimal nonassociativity of $L$. 

The difficulty in generalizing this argument to $L = M(G, *, g_0)$ is that if $H$ is a subgroup of $G$, then $H$ may not be closed under $*$, and so $M(H, *, h_0)$ may not be well defined. Closing it, by considering $\langle H, H^* \rangle$ may give all of $G$. This is what happens in Example 3.10, which in fact provides a counterexample to the converse of Corollary 3.12.

We first note that $L$ is MNA. If $K$ is a nonassociative subloop of $L$, then, by Lemma 3.11, there would have to be a nonabelian subgroup $H$ of $G$ and an element $h_0 \in Z(H)$ such that $K = M(H, *, h_0)$. (If $H$ were abelian, $K$ would be associative.) From the proof of Lemma 3.11, we can assert that $h_0 = aa^*g_0 = aa^*z$, for some $a \in G$. But, for any $a \in G$, $aa^* \in (x^2)$. Therefore, $h_0 = z$ or $x^2z$.

Since $x^2, z, v, w \in Z(G)$, the only noncentral elements of $G$ are of the form $xt$, $yt$ or $(xy)t$, where $t \in Z(G)$. Since $\langle xt_1, (xy)t_2 \rangle$ contains an element of the form $yt_3$, and since $\langle yt_1, (xy)t_2 \rangle$ contains an element of the form $xt_3$, there is no loss of generality in assuming that $xt_1, yt_2 \in H$.

Since central elements of $G$ are of order 2, $(xt_1)^2 = x^2 \in H$, and so $z \in H$, since $z = h_0$ or $z = x^{-2}h_0$. Also, since $K = M(H, *, h_0)$, $*$ is an involution on $H$. But $x^2, z, v$ and $w$ are fixed by $*$, and so any central element $t$ is fixed as well. Thus $(xt_1)^* = xt_1 \in H$, and so $v = (xt_1)^{-1}(xt_1)^* \in H$. Similarly, $w = (xt_2)^{-1}(xt_2)^* \in H$. Therefore, $t_1, t_2 \in H$ and so $x, y \in H$. But then $H = G$ and $K = L$. Thus $L$ is MNA.

On the other hand, $G$ is not MM, since $\langle x, y \rangle \cong Q_8$ is a proper nonabelian subgroup of $G$. Thus the converse of Corollary 3.12 does not hold.

4. Nilpotent loops

The natural generalization of CML’s is the class of centrally nilpotent Moufang loops. We will show shortly that this class of loops does not have Property 3I. However, before we do so, we recall some facts about this class of loops.

**Lemma 4.1.** 1) If $L$ is a centrally nilpotent Moufang loop then $L$ is a direct product of $p$-loops [Gla68, Theorem 5], [GW68, Corollary 1].

2) If $L$ is a $p$-loop, then $L$ is centrally nilpotent. In particular, $L$ has a nontrivial centre [Gla68, Theorem 4], [GW68].

3) If $L$ is a $p$-loop, Lagrange’s Theorem holds for $L$ [Gla68, Theorem 2], [GW68, p. 415].

We are now ready to show that the class of centrally nilpotent Moufang loops does not have Property 3I.

**Example 4.2.** Consider the dihedral group $D_8 = \langle a, b \mid a^8 = b^2 = (ab)^2 = 1 \rangle$. This group is not MM, since $\langle a^2, b \rangle$ is a proper nonabelian subgroup. Therefore, by Corollary 3.13, $L = M(D_8, 2)$ is not minimally nonassociative. On the other hand, $L$ is a 2-loop and so, by Lemma 4.1(2), it is centrally nilpotent. Since $D_8$ can be generated by two elements $L$ can be generated by three elements.

Thus, to show that the class of nilpotent Moufang loops does not have Property 3I, it is enough to show that $L$ is indecomposable. To see this, note that the centre of $L$ is $\{z \in D_8 \mid z^2 = 1\} = \langle a^4 \rangle$, which is of order two. On the other hand, if $L$
were decomposable, it would have to be a direct product of $C_2$ and a nonassociative Moufang loop of order 16 (since Moufang loops of order $\leq 8$ are associative), but every Moufang loop of order 16 has a nontrivial centre by Lemma 4.1(2). (See also [Che74] or [GMR99]), forcing the centre of the direct product to be of order exceeding two.

Thus $M(D_8, 2)$ is an indecomposable centrally nilpotent Moufang loop which can be generated by three elements but which is not minimally nonassociative, and so the class of centrally nilpotent nonassociative Moufang loops does not have Property 3I. It is worth noting that the nilpotence class of $M(D_8, 2)$ is 3.

On the other hand, there are some subclasses of nilpotent loops which do have Property 3I. One such subclass is the class of small Frattini Moufang loops first described by Hsu in [Hsu00].

Definition 4.3. A Moufang loop $L$ is called a small Frattini Moufang Loop (SFML) if $L$ is a $p$-loop, $p$ prime, which contains a central subloop $A$ of order $p$ such that $L/A$ is an elementary abelian $p$-group.

Theorem 4.4. If $L$ is a nonassociative SFML which can be generated by three elements, then $|L| = p^4$ for some prime $p$, $|Z| = p$, and $L$ is indecomposable.

Proof. Suppose $L = \langle a, b, c \rangle$, and let $A$ be as in Definition 4.6. Then $\{aA, bA, cA\}$ is a set of generators for $L/A$. If $L/A$ could be generated by two elements, say $xA$ and $yA$, then $L = \langle x, y, A \rangle$ is associative, by diassociativity and the centrality of $A$. But $L/A$ is an elementary abelian $p$-group, so $L/A \cong C_p \times C_p \times C_p$, and so $|L/A| = p^3$. Thus $|L| = |L/A| \cdot |A| = p^4$. If $|Z| > p$, then $|L/Z| = p^r$, for some $r \leq 2$. But then $L/Z$ can be generated by two or fewer elements, forcing $L$ to be associative, as above. Thus $|Z| = p$. If $L \cong M \times N$, then $Z \cong Z(M) \times Z(N)$, forcing $Z(M)$ or $Z(N)$ to be trivial. But $M$ and $N$ are $p$-loops and hence have nontrivial centres by Lemma 4.1(2), giving a contradiction. □

Theorem 4.5. If $L$ is a nonassociative SFML which can be generated by three elements, then $L$ is MNA.

Proof. Since $L$ is a $p$-loop, Lemma 4.1(3) tells us that Lagrange’s Theorem holds for $L$. Thus, if $K$ is any proper subloop of $L$, then $|K| = p^r$, with $r \leq 3$. But then $K$ is associative by [Che74, Proposition 1]. □

Corollary 4.6. The class of SFML’s has property 3I.

Remark 4.7. It should be noted that this result is quite limited in its scope. Hsu showed that, for $p > 3$, SFML’s are associative, so that nonassociative SFML’s exist only for $p = 2$ (these are just the code loops of Greiss [Gri86], see also [CG90]), or for $p = 3$.

Another special class of nilpotent Moufang loops is the class of Moufang loops with a unique nontrivial commutator.

Lemma 4.8. If $L$ is a nonassociative Moufang loop with a unique nontrivial commutator, then $L$ is centrally nilpotent.
Proof. If $L$ has a unique commutator, say $s$, then $s \in Z$ [CG90]. Therefore, $L/Z$ is a CML. By the Bruck-Slaby Theorem [Bru58], finitely generated CML’s are centrally nilpotent. Since both $Z$ and $L/Z$ are centrally nilpotent, so is $L$. \hfill $\Box$

**Theorem 4.9.** If $L$ is an indecomposable nonassociative Moufang loop with a unique nontrivial commutator, and if $L$ can be generated by three elements, then $L$ is an MNA loop which is centrally nilpotent of class 2.

**Proof.** Suppose $L = \langle a, b, c \rangle$, and let $s$ be the unique nontrivial commutator in $L$. Since $L$ is centrally nilpotent, Lemma 4.1(1) tells us it is a direct product of p-loops. Since it is indecomposable, it is a p-loop. By [CG90, Lemma 3], $s^2 = 1$, $s \in Z$ and, for any $x, y, z$ in $L$, $(x, y, z)^3 \in \langle s \rangle$. Since $s$ is of order 2 and $L$ is a p-loop, $p$ must be 2, and so the order of $(x, y, z)$ must be $2^r$ for some $r$. By the Division Algorithm, there exist integers $m$ and $n$ such that $3m + 2^n = 1$. Therefore, $(x, y, z) = (x, y, z)^{3m+2^n} = (x, y, z)^{3m} = [(x, y, z)^3]^m \in \langle s \rangle$. That is, $(x, y, z) = s$, for any $x, y$ and $z$ which do not associate. Thus $L$ has a unique nontrivial associator, $s \in Z$. Therefore $L/Z$ is an abelian group, and so $L$ is centrally nilpotent of class 2. Furthermore, since $L$ has a unique nontrivial associator, Lemma 3 of [CG90] also tells us that squares are central in $L$, and so $L/Z$ is an elementary abelian 2-group.

By Lemma 2.2, $L/Z \cong C_2 \times C_2 \times C_2$, every element in $L$ may be expressed in the form $(a^m b^n c^p)^s$, and $Z = \langle a^2, b^2, c^2, s \rangle$.

Let $K$ be any proper subloop of $L$, and let $\overline{K}$ be the image of $K$ in $L/Z$. If $\overline{K}$ is a proper subgroup of $L/Z \cong C_2 \times C_2 \times C_2$, then $\overline{K}$ can be generated by two or fewer elements, say $xZ$ and $yZ$. But then, $K \subseteq \langle x, y, Z \rangle$, which is associative, as above. On the other hand, if $\overline{K}$ is not proper, then $\overline{K}' = L/Z$ and so $L = KZ$. Since $a, b, c \in L$, $a = xz_1$, $b = yz_2$ and $c = z_3$, for some $x, y, z \in K$, and $z_1, z_2, z_3 \in Z$. Then $x = az_1^{-1} = [(a^{2m+1} b^{2^n} c^{2^n})]^{s^6} \in K$. Since $L$ is a 2-loop, $|a| = 2^r$ for some $r$. By the Division Algorithm, there exist integers $m$ and $n$ such that $m(2a+1)+n2^r = 1$. Thus $a = a^{m(2a+1)}$, and so, since $a^2, b^2, c^2$ and $s$ are central, \[ x' = x^m = (a^{b^{2m+1}} c^{2m})^{s^6} \in K. \] In a similar manner, starting with $y = b_{2z-1}$ and $z = c_{2z-1}$, we find elements $y' = (a^{2n} b^{2^n} c^{2^n})^{s^6} \in K$ and $z' = (a^{2n} b^{2^r} c^{2^r})^{s^6} \in K$. But then $y'' = (x')^{-2r} y' = b^{1-4m} b^{2r} c^{2r} s^{2r} \in K$ and, for any using the Division Algorithm, $y''' = b^{2r} s^{2r} \in K$. By a similar argument, we find $z''' = b^{2r} c^{2r} s^{2r} \in K$, and then $z''' = (y'''^{-2} z'''')^{-1} = c^{2r} s^{2r} \in K$. Using $z'''$, we can then kill the $c$ term from $y'''$, getting $y'''$ of the form $a^{2r} b^{2r} c^{2r} s^{2r} \in K$. Finally, $(x''', y''') = (a, b, c) = s$, so $s \in K$ and then $a, b$ and $c$ are in $K$. But $a, b$ and $c$ generate $L$, so $K = L$, and so $L$ is a proper subloop. Therefore, every proper subloop of $L$ is associative, and so $L$ is MNA. \hfill $\Box$

**Corollary 4.10.** The class of nonassociative Moufang loops with a unique nontrivial commutator has Property 3I.

Another family of nonassociative Moufang loops which are nilpotent of class 2 and which have Property 3I are the RA loops. A loop $L$ is said to be ring alternative or RA for short, if the loop ring $RL$ is alternative, where $R$ is any ring of characteristic
different from 2. This class of loops was originally studied in [Goo83] and fully characterized in [CG86]. Every such loop has a unique nontrivial commutator, $s$, and is of type $M(G, *, g_0)$, where the mapping $*$ is defined by

\[
g^* = \begin{cases} 
g & \text{if } g \in Z(G) \\
gs & \text{otherwise}, \end{cases}
\]

[GJM96, Theorem IV.3.1].

Remark 4.11. It is also worth noting that, in each of these loops, squares are central and that $L/Z(L) \cong C_2 \times C_2 \times C_2$. Since $L/Z(L)$ is an abelian group, $L$ is nilpotent of class 2.

Since RA loops have a unique nontrivial commutator, the following corollary follows from Corollary 4.13.

Corollary 4.12. The class of RA loops has Property 3I.

We also have the following theorem.

Theorem 4.13. If $L = M(G, *, g_0)$ is a Moufang loop which can be generated by three elements and which is nilpotent of class 2, then $L$ is an RA loop.

Proof. Since $L$ is nilpotent of class 2, $L/Z(L)$ is an abelian group. Therefore, for all $x, y \in L$, $(x, y) \in Z(L)$. Since $Z(L) \subseteq G$, $G/Z(L)$ is well defined, and since $G/Z(L) \subseteq L/Z(L)$, $G/Z(L)$ is also an abelian group. Therefore, $G/Z(G) \cong (G/Z(L))/(Z(G)/Z(L))$ is an abelian group as well. Thus, $G$ is also nilpotent of class 2 (it cannot be abelian since $L$ is not associative). Let $g, h \in G$. Since $g, h \in L$, $(g, h) \in Z(L) = \{z \in Z(G) \mid z^* = z\}$, by Remark 3.6. Since $*$ is an involution, 

\[
(g^{-1})^* = (g^*)^{-1}, \quad \text{so } (g, h)^* = (g^{-1}h^{-1}gh)^* = h^*g^*(h^*)^{-1}(g^*)^{-1} = ((h^*)^{-1}, (g^*)^{-1}).
\]

Now $gg^*$ and $hh^*$ are central in $G$, so $((h^*)^{-1}, (g^*)^{-1}) = (hh^*(h^*)^{-1}, gg^*(g^*)^{-1}) = (h, g) = (g, h)^{-1}$. Thus, $(g, h) = (g, h)^* = (g, h)^{-1}$, so $(g, h)^2 = 1$. Using standard commutator identities [Hal59, p. 150], $(g^2, h) = (g, h)((g, h), g)(g, h) = (g, h)^2 = 1$, the second equation holding since $(g, h)$ is central in $G$. Thus $g^2 \in Z(G)$. Since this holds for any $g \in G$, $G/Z(G)$ is an elementary abelian 2-group.

Since $L$ can be generated by three elements, we can apply Lemma 3.8. Thus there exist elements $g, h \in G$, $(g, h) \neq 1$, and $v = ku \in Gu$ such that $L = (g, h, v)$ and $G = \langle g, h, gg^*, hh^*, kk^*g_0 \rangle$. Let $H = (g, h)$. Since squares are central in $G$, they are central in $H$. Therefore, by Lemma 2.1, $H/Z(H) \cong C_2 \times C_2$. Since $G = HZ(G)$, it follows that $G/Z(G) \cong H/(H \cap Z(G)) = H/Z(H)$ is nilpotent of class 2 with a unique nonidentity commutator and a certain “lack of commutativity” property, so, by [GJM96, Corollary III.3.4], $L$ is an RA loop.

\[\Box\]

Corollary 4.14. The class of nonassociative loops which are nilpotent of class 2 and of the form $M(G, *, g_0)$ has Property 3I.

Remark 4.15. Example 4.2 shows that the assumption that the nilpotence class is 2 is critical. The loop $M(D_8, 2)$ can be generated by three elements, is indecomposable and nilpotent of class 3, but is not MNA.
Remark 4.16. Corollaries 4.7, 4.13, 4.9 and 4.15 suggest that three-generator, indecomposable Moufang loops which are nilpotent of class 2 might always be MNA. A check, using the tables found in [GMR99], shows that this is true for all Moufang loops of orders 16 or 32. However, at the moment, this is still an open question in general.

5. RA loops

Corollary 4.9 tells us that every indecomposable nonassociative RA loop which can be generated by three elements is MNA. Expanding on the final remark in [CGb], we determine which RA loops can be generated by three elements.

Lemma 5.1. If $L = M(G, *, g_0)$ is an RA loop, then $L$ can be generated by three elements if and only if there exist elements $g, h, k$ in $G$ such that $(g, h) \neq 1$ and $G = \langle g, h, k^2g_0 \rangle$.

Proof. Suppose that $L$ can be generated by three elements. Then, by Lemma 3.8, there exist elements $g, h, k$ in $G$, with $(g, h) \neq 1$, such that $G = \langle g, h, gg^*, hh^*, kk^*g_0 \rangle$. Since $(g, h) \neq 1$, $(g, h) = s$, the unique commutator. Thus, $s \in \langle g, h \rangle$. Also, since $g^* = g$ or $gs$ by (4.1), $gg^* \in \langle g, h \rangle$. The same is true for $hh^*$. Thus, $G = \langle g, h, kk^*g_0 \rangle$.

Finally, $kk^* = k^2$ or $k^2s$, so $G = \langle g, h, k^2g_0 \rangle$, as required.

Conversely, if $G = \langle g, h, k^2g_0 \rangle$ with $(g, h) = s$, then $G \subseteq \langle g, h, ku \rangle$ since $(ku)^2 = kk^*g_0 = k^2g_0$ or $sk^2g_0$. Since $k \in G$, $u \in \langle g, h, ku \rangle$, so $L = G \cup Gu \supseteq \langle g, h, ku \rangle$, hence $L = \langle g, h, ku \rangle$.

Our goal is to identify those RA loops which can be generated by three elements in terms the classification of RA loops first presented in [JLM95]. (See also [GJM96, Chapter V].)

To present this classification, we must first describe five classes of groups which depend on positive integer parameters $m_1$, $m_2$ and $m_3$:

\begin{align*}
D_1 &= \langle x, y, t_1 | x^2 = y^2 = t_1^{2m_1} = 1 \rangle \\
D_2 &= \langle x, y, t_1 | x^2 = y^2 = t_1^{2m_1} = 1 \rangle \\
D_3 &= \langle x, y, t_1, t_2 | x^2 = t_1^{2m_1} = t_2^{2m_2} = 1, y^2 = t_2 \rangle \\
D_4 &= \langle x, y, t_1, t_2 | x^2 = t_1, y^2 = t_2, t_1^{2m_1} = t_2^{2m_2} = 1 \rangle \\
D_5 &= \langle x, y, t_1, t_2, t_3 | x^2 = t_2, y^2 = t_3, t_1^{2m_1} = t_2^{2m_2} = t_3^{2m_3} = 1 \rangle
\end{align*}

where, in each case, $(x, y) = s = t_1^{2m_1}$ is the unique nontrivial commutator, and where the centre is the direct product of the cyclic groups generated by any $t_i$'s which appear.

Remark 5.2. Note that, in each case, $G = \langle x, y, t_1 \rangle$.

Remark 5.3. Since squares are central in groups of type $D_i$, $i = 1, 2, \ldots, 5$, the only pairs of noncommuting elements in these loops are of one of the following three forms: $xy$ and $yz$; $xy$ and $(xy)z$; or $yu$ and $(xy)z$, where $v$ and $z$ are central elements of $G$. 

\[ \text{THREE-GENERATOR MOUFANG LOOPS} \]
The indecomposable RA loops fall into seven categories. In each category, $L = M(G, *, g_0)$, where $G$ and $g_0$ are as indicated in the following table:

<table>
<thead>
<tr>
<th>Loop type</th>
<th>Group type</th>
<th>$g_0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_1$</td>
<td>$D_1$</td>
<td>1</td>
</tr>
<tr>
<td>$L_2$</td>
<td>$D_2$</td>
<td>$t_1$</td>
</tr>
<tr>
<td>$L_3$</td>
<td>$D_3$</td>
<td>1</td>
</tr>
<tr>
<td>$L_4$</td>
<td>$D_4$</td>
<td>$t_1$</td>
</tr>
<tr>
<td>$L_5$</td>
<td>$D_5$</td>
<td>1</td>
</tr>
<tr>
<td>$L_6$</td>
<td>$D_5$</td>
<td>$t_1$</td>
</tr>
<tr>
<td>$L_7$</td>
<td>$D_5 \times \langle w \rangle$</td>
<td>$w$</td>
</tr>
</tbody>
</table>

Note that in each category there are many loops, depending on the positive integer parameters $m_1$, $m_2$ and $m_3$, as reflected in the $D$'s.

**Lemma 5.4.** If $G$ is a group of type $D_1$, $D_3$, or $D_5$, then $G = \langle g, h, k^2 \rangle$ for some elements $g$, $h$ and $k$ in $G$ if and only if $m_1 = 1$.

**Proof.** Since $\langle g, h, k^2 \rangle = \langle g, gh, k^2 \rangle$, it follows from Remark 5.3 that there is no loss in generality in assuming that $g = xv$ and $h = yz$, for some central elements $v$ and $z$ in $G$.

If $m_1 = 1$, then $t_1 = t_1^{2m_1 - 1} = s = (x, y)$, so $G = \langle x, y \rangle = \langle g, h, k^2 \rangle$, where $g = x$, $h = y$ and $k = 1$.

On the other hand, if $m_1 > 1$, then we claim that $t_1 \notin \langle g, h \rangle$ and, in fact, $t_1 \notin \langle g, h, G^2 \rangle$, where $G^2$ denotes the subgroup of $G$ generated by the squares.

To see this, first note that every element of $G$ may be represented in the form $g^\alpha h^\beta z$, where $0 \leq \alpha, \beta \leq 1$ and $z \in Z(G)$. In particular, since squares are central in $G$, every element of $\langle g, h, G^2 \rangle$ may be represented in the form $g^\alpha h^\beta z$, where $0 \leq \alpha, \beta \leq 1$ and $z \in \langle G^2, s \rangle = G^2$. [Since $m_1 > 1$, $s = t_1^{2m_1 - 1} \in G^2$.] If $t_1$ were in $\langle g, h, G^2 \rangle$, then $t_1 = g^\alpha h^\beta z$, as above, and, since $t_1$ is central but $g$ and $gh$ are not, we must have $\alpha = \beta = 0$. Thus $t_1 = z \in G^2$. That is, $t_1 = (g^\alpha h^\beta z')^2 = x^{2\pi} y^{2\rho} s^{\pi \rho} z'^{2\pi}$, where $z', z'' \in Z(G)$.

We now consider three cases.

If $G$ is of type $D_1$, then $Z(G) = \langle t_1 \rangle$, and so $t_1 = x^{2\pi} y^{2\rho} s^{\pi \rho} t_1^{2\sigma} = t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho}$, for some integer $k$.

If $G$ is of type $D_3$, then $Z(G) = \langle t_1 \rangle \times \langle t_2 \rangle$, and so $t_1 = x^{2\pi} y^{2\rho} s^{\pi \rho} t_1^{2\sigma} t_2^{2\sigma} = t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho}$, for some integer $k$.

If $G$ is of type $D_5$, then $Z(G) = \langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle$, and so $t_1 = x^{2\pi} y^{2\rho} s^{\pi \rho} t_1^{2\sigma} t_2^{2\sigma} t_3^{2\sigma} = t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho} + t_1^{2m_1 - 1} x^{2\pi} y^{2\rho} s^{\pi \rho}$, for some integer $k$.

In each case, $t_1^{2k-1} = 1$, contradicting the fact that $|t_1| = 2m_1$. Thus $t_1 \notin \langle g, h, G^2 \rangle$, and so $\langle g, h, G^2 \rangle \neq G$.

**Corollary 5.5.** If $L$ is an RA loop of type $L_1$, $L_3$, $L_5$ or $L_7$, then $L$ can be generated by three elements if and only if $m_1 = 1$. 


If $L$ is of type $\mathcal{L}_1$, $\mathcal{L}_3$ or $\mathcal{L}_5$, then $g_0 = 1$ and so, by Lemma 5.1, $L$ can be generated by three elements if and only if there exist elements $g$, $h$, $k$ in $G$ with $(g, h) = s$ and $G = \langle g, h, k^2 \rangle$. But if $L$ is of type $\mathcal{L}_1$, $\mathcal{L}_3$ or $\mathcal{L}_5$, then $G$ is of type $\mathcal{D}_1$, $\mathcal{D}_3$, or $\mathcal{D}_5$, and so, by Lemma 5.4, there exist such $g$, $h$ and $k$ if and only if $m_1 = 1$.

If $L$ is of type $\mathcal{L}_7$, then $G$ is a direct product of a group of type $\mathcal{D}_5$ with a cyclic group $\langle w \rangle$. Here, $g_0 = w$. In a manner similar to the $\mathcal{D}_5$ case in the proof of Lemma 5.4, $t_1 \in \langle g, h, k^2 w \rangle$ if and only if $m_1 = 1$. [If $m_1 > 1$, any $w$’s which appear in any word in $g$, $h$ and $k^2 w$ may be extracted (and hence are irrelevant) since $G$ is a direct product and $t_1 \notin \langle g, h, k^2 \rangle$. On the other hand, if $m_1 = 1$, then $t_1 = s = \langle x, y \rangle$, and so $G = \langle x, y, w \rangle = \langle x, y, g_0 \rangle$.] □

**Lemma 5.6.** If $L$ is an RA loop of type $\mathcal{L}_2$, $\mathcal{L}_4$ or $\mathcal{L}_6$, then $L$ can be generated by three elements.

**Proof.** In all three cases, $u^2 = g_0 = t_1$ and $\langle x, y, t_1 \rangle = G$, so $\langle x, y, u \rangle = L$. □

Combining Corollary 4.9 with the results of this section, we can determine exactly which RA loops are MNA.

**Theorem 5.7.** An indecomposable RA loop $L$ is MNA if and only if $L$ is of type $\mathcal{L}_2$, $\mathcal{L}_4$ or $\mathcal{L}_6$, or of type $\mathcal{L}_1$, $\mathcal{L}_3$, $\mathcal{L}_5$ or $\mathcal{L}_7$, with $m_1 = 1$.

**References**


[CGb] Orin Chein and Edgar G. Goodaire, _Minimally nonassociative Moufang loops with a unique nonidentity commutator are ring alternative_, preprint.


TEMPLE UNIVERSITY, PHILADELPHIA, PA 19122 U.S.A.

*E-mail address*: orin@math.temple.edu

MEMORIAL UNIVERSITY OF NEWFOUNDLAND, ST. JOHN’S, NEWFOUNDLAND, CANADA A1C 5S7

*E-mail address*: edgar@math.mun.ca