MINIMALLY NONASSOCIATIVE NILPOTENT MOUFANG LOOPS

ORIN CHEIN AND EDGAR G. GOODAIRE

Abstract. This paper considers the following question: "Which varieties of Moufang loops have the property that the minimally nonassociative loops in the variety are precisely those which are indecomposable and which can be generated by three elements?" It was shown previously [CGta] that the variety of commutative Moufang loops has this property. Here we investigate the variety of centrally nilpotent Moufang loops. We find that while this variety as a whole does not have the property in question, the subvariety consisting of Moufang loops which are centrally nilpotent of class 2 does. We also find some other families of loops which have this property, and consider a number of examples.

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 [CGta]. 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), minimal 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 if $L = G \times H$ with G and H proper subloops then G and H must be associative, and hence so must L.

In [CGta], 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 family of Moufang loops has *Property 3I* if nonassociative loops in the family are MNA if and only if they are indecomposable and can be generated by three elements.

1991 *Mathematics Subject Classification.* Primary 20N05.

Research for this paper was completed while the first author was a visitor in the Department of Mathematics and Statistics at Memorial University, whose faculty and staff he wishes to thank for their hospitality.

The research of the first author was supported by a study leave and a grant-in-aid of research from Temple University and that of the second author was supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. OGP0009087. March 6, 2002.

It is natural to ask whether the variety 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 varieties of Moufang loops other than CML's have Property 3I. We will identify several other such varieties 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 variety of centrally nilpotent Moufang loops. Although this variety is seen not to have Property 3I in general, the subvariety of Moufang loops of nilpotence class 2 does. We investigate some important subfamilies such as the small Frattini Moufang loops and the RA loops. We also consider the family of Moufang loops with a unique nontrivial commutator and the loops of type $M(G, *, g_0)$.

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 $g^\alpha h^\beta s^\gamma$, where $s = (g, h)$ and where $0 \le \gamma \le 1$,*
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 $g^\alpha h^\beta s^\gamma$. Since $s^2 = 1$, we can assume that $0 \le \gamma \le 1$.

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 $0 \le \alpha, \beta, \pi, \rho \le 1$. 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 $(gh, h) = (g, h)((g, h), h)(h, h) = (g, h) = s$. Thus, s is the unique nontrivial commutator.

4) Let $z = (g^\alpha h^\beta)s^\gamma \in Z(G)$. Then, since g^2, h^2 and s are central, there is no loss of generality in assuming that $0 \le \alpha, \beta \le 1$. 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 α and β must both be 0, and so $z \in \langle g^2, h^2, s\rangle$. □

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

1) *$L/Z \cong C_2 \times C_2 \times C_2$,*
2) *every element in L may be expressed in the form $[(a^\alpha b^\beta)c^\gamma]s^\delta$,*
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 [CR72, Corollary 2] and s is the unique nontrivial associator, also by Lemma 3 of [CG90].

1) Since $L = \langle a, b, c\rangle$ and squares are central, $L/Z = \langle aZ, bZ, cZ\rangle \subseteq C_2 \times C_2 \times C_2$. If L/Z were a proper subgroup, it could be generated by fewer than three elements, say xZ and yZ, then $L = \langle x, y, Z\rangle = \langle x, y\rangle Z$ 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, using the Moufang identity $[(xy)z]y = x[y(zy)]$ and the centrality of s,

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

Since $(c^\gamma, a^\pi b^\rho)$, $(a^\alpha b^\beta, a^\pi b^\rho, c^{\sigma+2\gamma})$ and (b^β, a^π) are all in $\langle s\rangle$, this becomes first $(a^\alpha b^\beta)[(a^\pi b^\rho)c^{\sigma+2\gamma}]s^\phi$, then $[(a^\alpha b^\beta)(a^\pi b^\rho)]c^{\sigma+2\gamma}]s^\psi$, and finally $[(a^{\alpha+\pi}b^{\beta+\rho})c^{\sigma+2\gamma}]s^\mu$, where ϕ, ψ and μ depend on $\delta + \tau$ and the commutators and associator mentioned in the previous sentence. Therefore, $d = [(a^{\alpha+\pi}b^{\beta+\rho})c^{\gamma+\sigma}]s^\mu$.

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 $0 \le \alpha, \beta, \gamma \le 1$. 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 α, β, and γ must all be 0. Therefore, $z \in \langle a^2, b^2, c^2, s\rangle$. □

Lemma 2.3. *Let L be a nonassociative Moufang p-loop which can be generated by three elements, say $L = \langle a, b, c\rangle$. Suppose that L has a central element s such that $L/\langle s\rangle$ is an elementary abelian p-group. Then*

1) $L/\langle s\rangle \cong C_p \times C_p \times C_p$,
2) *every element in L may be expressed in the form* $[(a^\alpha b^\beta)c^\gamma]s^\delta$,
3) $Z(L) = \langle s\rangle$.

Proof. Let $A = \langle s\rangle$. Since L/A is an abelian group, all commutators and all associators in L are contained in A.

1) Since $L = \langle a, b, c\rangle$, then, L/A can be generated by three elements. That is, $L/A = \langle aA, bA, cA\rangle \subseteq C_p \times C_p \times C_p$. If L/A were a proper subgroup, it could be generated by fewer than three elements, say xA and yA. But then $L = \langle x, y, A\rangle = \langle x, y\rangle A$ would be associative, by diassociativity, contrary to assumption. Therefore $L/A \cong C_p \times C_p \times C_p$.

2) This is exactly the same as the proof of part 2) of Lemma 2.2.

3) Since $A \subseteq Z(L)$, $L/Z(L)$ is a homomorphic image of L/A. Therefore, by part 1), $L/Z(L) \subseteq C_p \times C_p \times C_p$, since any homomorphic image of $C_p \times C_p \times C_p$ is isomorphic to a subgroup of $C_p \times C_p \times C_p$. If $L/Z(L)$ were a proper subgroup, it could be generated by two or fewer elements, say $L/Z(L) = \langle xZ, yZ\rangle$. But then, as above, $L = \langle x, y, Z\rangle$ would be associative by diassociativity, contrary to assumption. Hence $L/Z(L) \cong C_p \times C_p \times C_p \cong L/A$ and $Z(L) = A = \langle s\rangle$, since $A \subseteq Z(L)$. □

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

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^*)u \\ (gu)(hu) &= h^* g g_0. \end{aligned} \tag{3.1}$$

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

Remark 3.1. For $g \in G$, $(gu)^{-1} = (g^{*-1}{g_0}^{-1})u$.

Remark 3.2. Note that $gg^* = g^*g$, since $(g^*g)g = g(g^*g) = (gg^*)g$. Also, for g and h in G, $(gh)(gh)^* = ghh^*g^* = g(hh^*)g^* = (gg^*)(hh^*)$, and, by induction, this generalizes to any number of elements of G.

Remark 3.3. 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 Gu,

$m = (k^{-1}g)(ku) = (k^{-1}g)v \in Gv$. Furthermore,

$$\begin{aligned} g(hv) &= g[h(ku)] = g[(kh)u] = (khg)u = (hg)(ku) = (hg)v \\ (gv)h &= [g(ku)]h = [(kg)u]h = (kgh^*)u = (gh^*)(ku) = (gh^*)v \\ (gv)(hv) &= [g(ku)][h(ku)] = [(kg)u][(kh)u] = (kh)^*(kg)g_0 = h^*gkk^*g_0. \end{aligned} \tag{3.2}$$

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

$$\begin{aligned} g(hu) &= (hg)u \\ (gu)h &= (gh^{-1})u \\ (gu)(hu) &= h^{-1}g. \end{aligned} \tag{3.3}$$

Remark 3.4. 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

$$\begin{aligned} g(hv) &= (hg)v \\ (gv)h &= (gh^{-1})v \\ (gv)(hv) &= h^{-1}g. \end{aligned} \tag{3.4}$$

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

Lemma 3.5. *If $L = M(G, *, g_0)$, then $A(L)$, the subloop generated by the associators in L, is just G', the commutator subgroup of G.*

Proof. First observe that, for $g, h \in G$, $g(hu) = (hg)u = [gh(h, g)]u = [(gh)u](h, g)^*$, so that $(g, h, u) = [(h, g)^*]^{-1} = (h^{*-1}, g^{*-1})$. Since g^{*-1} and h^{*-1} run through G as g and h do, every commutator in G is an associator. Therefore $G' \subseteq A(L)$.

For subsets A, B and C of L, we will use the notation (A, B, C) to denote the subloop generated by all associators of the form (a, b, c), where a, b and c run through A, B and C respectively. Thus, in particular, $A(L) = (L, L, L)$.

Let $x, y, z \in L$. We wish to show that $(x, y, z) \in G'$. Since G is associative and since the product of two elements of Gu is in G, it follows from equations (5.17), (5.18) and (5.19) on page 124 of [Bru58] that there is no loss of generality if we assume that two of the elements are in G and the third is in Gu. In fact, since $(gu, hu, ku) = (gu, (hu)(ku), ku) = (gu, (hu)(ku), (ku)(gu)) \in (Gu, G, G)$, $(gu, hu, k) = ((gu)(hu), k, hu)^{-1} \in (G, G, Gu)$, $(gu, h, ku) = (gu, h, (ku)(gu)) \in (Gu, G, G)$, and $(g, hu, ku) = (g, (hu)(ku), ku) \in (G, G, Gu)$, we need only consider (x, y, z) where $x = gu, y = h, z = k$ or $x = g, y = h, z = ku$. In the first case, $[(gu)h]k = (gh^*k^*)u$ and $(gu)(hk) = (gk^*h^*)u$, so, using Remark 3.1,

$$\begin{aligned} (gu, h, k) &= [(gk^*h^*)u]^{-1}[(gh^*k^*)u] = \{[(hkg^*)^{-1}{g_0}^{-1}]u\}[(gh^*k^*)u] \\ &= g^{*-1}k^{-1}h^{-1}khg^* = g^{*-1}(k, h)g^* \in G'. \end{aligned}$$

Similarly, in the second case, $(gh)(ku) = (kgh)u$ and $g[h(ku)] = (khg)u$, so

$$\begin{aligned}(g, h, ku) &= [(khg)u]^{-1}[(kgh)u] = \{[(khg)^{*-1}{g_0}^{-1}]u\}[(kgh)u] \\ &= k^{*-1}h^{*-1}g^{*-1}h^*g^*k^* = k^{*-1}(h^*, g^*)k^* \in G'.\end{aligned}$$

□

Lemma 3.6. *If $L = M(G, *, g_0)$, then the centre, $Z(L) = \{z \in Z(G) \mid z^* = z\}$. In the special case that $L = M(G, 2)$, $Z(L) = \{z \in Z(G) \mid z^2 = 1\}$.*

Proof. First note that the second statement follows immediately from the first, since,in $M(G, 2)$, $z^* = z^{-1}$. For the first statement, first note that if $v \in Gu$ is in $Z(L)$, then $gv = vg = g^*v$, by Remark 3.3, and so $g^* = g$ for all $g \in G$. But then, $gh = (gh)^* = h^*g^* = hg$, for all $g, h \in G$, and so G is abelian and L is a group. Therefore, $Z(L) \subseteq G$. If $z \in Z(L)$, then, clearly, z commutes with every element of G, and so $Z(L) \subseteq Z(G)$. For $g \in G$, $ug = g^*u$, so if z commutes with u, then $z^* = z$. Thus $Z(L) \subseteq \{z \in Z(G) \mid z^* = z\}$. Conversely, if $z \in Z(G)$ and $z^* = z$, then, for any element $g \in G$, $zg = gz$ and $z(gu) = (gz)u = (gz^*)u = (gu)z$, so z commutes with every element of L. Furthermore, $(zg)(hu) = (hzg)u = (hgz)u = z[(hg)u] = z[g(hu)]$, so $(z, g, hu) = 1$; and, similarly, $[z(gu)](hu) = [(gz)u][hu] = gzh^*g_0 = zgh^*g_0 = z[(gu)(hu)]$, so $(z, gu, hu) = 1$. Therefore $z \in Z(L)$, and so $\{z \in Z(G) \mid z^2 = 1\} \subseteq Z(L)$. □

Remark 3.7. It is worth noting that, for any $g \in G$, not only do we have $gg^* \in Z(G)$, 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 3.8. *A nonassociative Moufang loop of the form $L = G \cup Gu = M(G, *, g_0)$ can be generated by three elements if and only if there exist elements $g, h, k \in G$, with $(g, h) \neq 1$, such that $G = \langle g, h, gg^*, hh^*, kk^*g_0\rangle$. 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 $\langle a, b, c\rangle = \langle ab, b, c\rangle = \langle a, bc, c\rangle = \langle ac, bc, c\rangle$, 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),

$$\begin{aligned}g(hv) &= (hg)v \\ (gv)h &= (gh^*)v = (gh^{-1}hh^*)v \\ (gv)(hv) &= h^*gkk^*g_0 = h^*hh^{-1}gkk^*g_0 = h^{-1}ghh^*kk^*g_0,\end{aligned} \tag{3.5}$$

the last equation following from Remark 3.2 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 $G = \langle g, h\rangle$.

Conversely, if $G = \langle g, h, gg^*, hh^*, kk^*g_0\rangle$ for some $g, h, k \in G$, let $v = ku$ and let $H = \langle g, h, v\rangle$. Then $kk^*g_0 = v^2 \in H$. Also $vg = (ku)g = (kg^*)u = g^*(ku) = g^*v$, so $g^* = (vg)v^{-1} \in H$, and, similarly $h^* \in H$. But then $G \subseteq H$. Since $v \notin G$, $G \neq H$. But G is of index 2 in L, so $H = L$ and $L = H = \langle g, h, v\rangle$ can be generated by three elements. □

Remark 3.9. It is noteworthy that while the minimal number of generators for a loop of type $M(G, 2)$ is always at least as big as 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 3.10. Let $G = Q_8 \times C_2 \times C_2 \times C_2$, where Q_8 denotes the quaternions. Then

$$\begin{aligned} G = \langle x, y, z, v, w \mid x^4 = z^2 = v^2 = w^2 = (x, z) = (x, v) = (x, w) = (y, z) = (y, v) \\ = (y, w) = (z, v) = (z, w) = (v, w) = 1, y^2 = (x, y) = x^2\rangle, \end{aligned}$$

and G cannot be generated by fewer than five elements, because $G/\langle x^2\rangle \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2$ requires five generators. Furthermore, every element $g \in G$ may be expressed in the form $g = x^\alpha y^\beta z^\gamma v^\delta w^\epsilon$, where $0 \le \alpha \le 3$ and $0 \le \beta, \gamma, \delta, \epsilon \le 1$. If $h = x^\pi y^\rho z^\sigma v^\tau w^\phi$, then $gh = x^{\alpha+\pi+2\beta\pi} y^{\beta+\rho} z^{\gamma+\sigma} v^{\delta+\tau} w^{\epsilon+\phi}$.

Define $*$ on G by $g^* = (x^\alpha y^\beta z^\gamma v^\delta w^\epsilon)^* = x^{\alpha+2\alpha\beta} y^\beta z^\gamma v^{\alpha+\delta} w^{\beta+\epsilon}$. 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,

$$\begin{aligned} (gh)^* &= x^{\alpha+\pi+2\beta\pi+2(\alpha+\pi+2\beta\pi)(\beta+\rho)} y^{\beta+\rho} z^{\gamma+\sigma} v^{\alpha+\pi+2\beta\pi+\delta+\tau} w^{\beta+\rho+\epsilon+\phi} \\ &= x^{\alpha+\pi+2(\alpha\beta+\alpha\rho+\pi\rho)} y^{\beta+\rho} z^{\gamma+\sigma} v^{\alpha+\delta+\pi+\tau} w^{\beta+\epsilon+\rho+\phi}, \end{aligned}$$

whereas

$$\begin{aligned} h^*g^* &= (x^{\pi+2\pi\rho} y^\rho z^\sigma v^{\pi+\tau} w^{\rho+\phi})(x^{\alpha+2\alpha\beta} y^\beta z^\gamma v^{\alpha+\delta} w^{\beta+\epsilon}) \\ &= x^{\pi+2\pi\rho+\alpha+2\alpha\beta+2\rho(\alpha+2\alpha\beta)} y^{\rho+\beta} z^{\sigma+\gamma} v^{\pi+\tau+\alpha+\delta} w^{\rho+\phi+\beta+\epsilon} \\ &= x^{\alpha+\pi+2\alpha\beta+2\pi\rho+2\alpha\rho} y^{\beta+\rho} z^{\gamma+\sigma} v^{\alpha+\delta+\pi+\tau} w^{\beta+\epsilon+\rho+\phi} = (gh)^*. \end{aligned}$$

Thus $*$ is an involution on G. Note that $x^* = xv$ 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 $v = x^{-1}(ux)u^{-1} \in \langle x, u\rangle$. 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.

Since $Z(G) = \langle x^2, z, v, w\rangle$ and since each of these elements is fixed by $*$, $Z(L) = Z(G) = \langle x^2, z, v, w\rangle$. Also, since all squares in L are central, $L/Z(L)$ is an elementary abelian 2-group. Thus L is centrally 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 3.11. *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 $wv^{-1} = (bu)(au)^{-1} = (bu)((a^{-1})^* u)g_0{}^{-1} = a^{-1}b \in G$, so $wv^{-1} \in K \cap G = H$, and $w \in Hv$. Thus, $K = H \cup Hv$. Let $h_0 = v^2 = (au)^2 = a^* a g_0 \in G$. 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. □

Theorem 3.12. *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 [CGp, Corollary 1.4].)

Theorem 3.13. *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. □

Remark 3.14. 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, as we now show, provides a counterexample to the converse of Theorem 3.12.

We first observe 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 $a \in G$, $aa^* \in \langle x^2, v, w \rangle$. Therefore, $h_0 = mz$ for some $m \in \langle x^2, v, w \rangle$.

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, $(xt_1)^2 = x^2 \in H$. 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 $(xt_1)^* = xvt_1 \in H$, and so $v = (xt_1)^{-1}(xt_1)^* \in H$. Similarly, $w = (xt_2)^{-1}(xt_2)^* \in H$. Therefore, $z = m^{-1}h_0 \in H$, since $m \in \langle x^2, v, w\rangle \subseteq H$. Finally, $t_1, t_2 \in \langle x^2, z, v, w\rangle \subseteq H$ 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 Theorem 3.12 does not hold.

4. Nilpotent loops

The natural generalization of CML's is the variety of centrally nilpotent Moufang loops. We will show shortly that this variety of loops does not have Property 3I but that the subvariety consisting of loops of nilpotence class 2 does. However, before we do so, we recall some facts about this variety 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 variety 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 Theorem 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 variety of centrally 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 ≤ 8 are associative), but every Moufang loop of order 16 has a nontrivial centre by Lemma 4.1(2). (See also [Che74] or [GMR99]). This forces 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 variety of centrally nilpotent Moufang loops does not have Property 3I.

Remark 4.3. It is worth noting that the nilpotence class of $M(D_8, 2)$ is 3.

On the other hand, there are some subvarieties of centrally nilpotent loops which do have Property 3I, for example Moufang loops which are nilpotent of class at most 2.

Theorem 4.4. *If L is an indecomposable nonassociative Moufang loop which can be generated by three elements, and if L is centrally nilpotent of class 2, then L is an MNA loop.*

Proof. By Lemma 4.1(1), since L is centrally nilpotent, it is a direct product of p-loops. Since L is indecomposable, it is a p-loop.

Let L^* denote the normal closure of the subloop of L generated by all associators. Since L/Z is an abelian group, all associators are central and hence are fixed by any inner mapping of L. Therefore, in this case, L^* is simply the subloop of L generated by all associators. By [Hsu00, Theorem 3.3], if $x_1, \ldots, x_n$ generate L, then L^* is generated by $\{(x_i, x_j, x_k) \mid 1 \leq i < j < k \leq n\}$. In particular, if $L = \langle a, b, c \rangle$, then $L^* = \langle (a, b, c) \rangle$ is cyclic. That is, $L^* = \langle s \rangle$, where $s = (a, b, c)$. By [Hsu00, Theorem 3.8], L/L^* is an abelian group of exponent dividing six. In particular, L^* is central and, since L is not a group, $L^* \neq L$ and L/L^* is not trivial. But since L is a p-loop, so is L/L^*, and so it is either of exponent 2 or of exponent 3. That is, L/L^* is either an elementary abelian 2-group or an elementary abelian 3-group. Thus, by Lemma 2.3, $L/L^* \cong C_p \times C_p \times C_p$, and every element in L may be expressed in the form $[(a^\alpha b^\beta)c^\gamma]s^\delta$.

Let K be any proper subloop of L, and let $\overline{K}$ be the image of K in L/L^*. If $\overline{K}$ is a proper subgroup of $L/L^* \cong C_p \times C_p \times C_p$, then $\overline{K}$ can be generated by two or fewer elements, say xL^* and yL^*. But then, $K \subseteq \langle x, y, L^* \rangle$, which is associative, by diassociativity and the centrality of L^*. On the other hand, if $\overline{K}$ is not proper, then $\overline{K} = L/L^*$ and so $L = KL^*$. Since $a, b, c \in L$, $a = xs^\pi$, $b = ys^\rho$ and $c = zs^\sigma$, for some $x, y, z \in K$ and some integers π, ρ and σ. Then $x = as^{-\pi}, y = bs^{-\rho}, z = cs^{-\sigma} \in K$. But, since s is central, $(x, y, z) = (a, b, c) = s \in K$. Thus, $a, b, c \in K$, and so $K = L$ and K is not proper, contrary to assumption. Therefore, every proper subloop of L is associative, and so L is MNA. ☐

Corollary 4.5. *The variety of Moufang loops which are centrally nilpotent of class 2 has Property 3I.*

As a consequence of this corollary, we can resolve the MNA question for several families which have appeared in the literature.

Definition 4.6. 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 [Hsu00].

Clearly, SFML's are centrally nilpotent of class 2, so we obtain the following corollary:

Corollary 4.7. *The family of SFML's has property 3I.*

Another family of Moufang loops which are centrally nilpotent of class 2 and which therefore have Property 3I are the RA loops.

Definition 4.8. A loop L is said to be *ring alternative* or *RA* for short, if the loop ring RL is alternative over any ring R of characteristic different from 2.

These loops was originally studied in [Goo83] and fully characterized in [CG86]. Every such loop is centrally nilpotent of class 2 since squares are central and $L/Z \cong C_2 \times C_2 \times C_2$.

Corollary 4.9. *The family of RA loops has Property 3I.*

Remark 4.10. It is also worth noting that every RA loop has a unique nontrivial commutator, s, and is of type $M(G, *, g_0)$, where the mapping $*$ is defined by

$$g^* = \begin{cases} g & \text{if } g \in Z(G) \\ gs & \text{otherwise,} \end{cases} \tag{4.1}$$

[GJM96, Theorem IV.3.1].

The family of Moufang loops with a unique nontrivial commutator is another family of centrally nilpotent Moufang loops (not necessarily of class 2) which can be shown to have Property 3I.

Lemma 4.11. *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. □

Theorem 4.12. *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 $3m+2^r n = 1$. Therefore, $(x, y, z) = (x, y, z)^{3m+2^r n} = (x, y, z)^{3m} = [(x, y, z)^3]^m \in \langle s\rangle$. That is, $(x, y, z) = s$, for any x, y and z which do not associate. Thus L has a unique nontrivial central associator. 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 $[(a^\alpha b^\beta)c^\gamma]s^\delta$, 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 $c = zz_3$, for some $x, y, z \in K$, and $z_1, z_2, z_3 \in Z$. Then $x = az_1{}^{-1} = [(a^{2\alpha+1}b^{2\beta})c^{2\gamma}]s^\delta \in K$. Since L is a 2-loop, $|a| = 2^t$ for some t. By the Division Algorithm, there exist integers m and n such that $m(2\alpha+1)+n2^t = 1$. Thus $a = a^{m(2\alpha+1)}$, and so, since a^2, b^2, c^2 and s are central, $x' = x^m = (ab^{2m\beta})c^{2m\gamma}s^{m\delta} \in K$. In a similar manner, starting with $y = b{z_2}^{-1}$ and $z = c{z_3}^{-1}$, we find elements $y' = (a^{2\pi}b)c^{2\rho}s^{\nu_1} \in K$ and $z' = (a^{2\sigma}b^{2\tau})cs^{\phi_1} \in K$. But then $y'' = (x')^{-2\pi}y' = b^{1-4m\pi\beta}c^{2\rho-4m\pi\gamma}s^{\nu_2} \in K$ and, again using the Division Algorithm, $y''' = bc^{2r}s^{\nu_3} \in K$. By a similar argument, we find $z''' = b^{2j}cs^{\phi_3} \in K$, and then $z'''' = ((y''')^{-2j}z''')^i = cs^{\phi_4} \in K$. Using z'''', we can then kill the c term from y''', getting y'''' of the form $bs^{\nu_4} \in K$. Using first z'''' and then y'''', we can kill off first the c and then the b terms from x', getting x'' of the form as^{μ_2} in K. Finally, $(x'', y'''') = (a, b) = s$, so $s \in K$ and then a, b and c are in K. But a, b and c generate L, so $K = L$ is not a proper subloop. Therefore, every proper subloop of L is associative, and so L is MNA. □

Corollary 4.13. *The family of Moufang loops with at most one nontrivial commutator has Property 3I.*

We also have the following theorem.

Theorem 4.14. *If $L = M(G, *, g_0)$ is a Moufang loop which can be generated by three elements and which is centrally nilpotent of class 2, then L is an RA loop.*

Proof. Since L is centrally nilpotent of class 2, $L/Z(L)$ is an abelian group. Therefore, for all $x, y \in L$, $(x, y) \in Z(L)$. Since $Z(L) \subseteq G$ by Lemma 3.6, $G/Z(L)$ is well defined. 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 (if it were abelian, then $L = M(G, *, g_0)$ would be associative). Let $g, h \in G$. Since $g, h \in L$, $(g, h) \in Z(L) = \{z \in Z(G) \mid z^* = z\}$, by Lemma 3.6. Since * is an involution, $(g^{-1})^* = (g^*)^{-1}$, 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 $L = \langle g, h, v\rangle$ and $G = \langle g, h, gg^*, hh^*, kk^*g_0\rangle$. Let $H = \langle g, h\rangle$. 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 $G = \langle g, h, gg^*, hh^*, kk^*g_0\rangle \subseteq HZ(G) \subseteq G$, $G = HZ(G)$, and it follows that $G/Z(G) \cong H/(H \cap Z(G)) \cong H/Z(H)$ is also $C_2 \times C_2$. By [GJM96, Proposition III.3.6], the group G has a unique nonidentity commutator and a certain "lack of commutativity" property, so, by [GJM96, Corollary III.3.4], L is an RA loop. □

Corollary 4.15. *The family of loops of the form $M(G, *, g_0)$ which are centrally nilpotent of class 2 has Property 3I.*

Remark 4.16. 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 centrally nilpotent of class 3, but is not MNA.

So far, all of the MNA loops considered in this paper are centrally nilpotent of class ≤ 2. This raises several questions: Must every MNA loop be centrally nilpotent? If an MNA loop is centrally nilpotent, must its nilpotence class be ≤ 2? The answer to both of these questions is "no".

Example 4.17. The loop $L = M(B_3, 2)$ is MNA but not centrally nilpotent, where B_3 denotes the Burnside group of order 27 and exponent 3. That L is MNA follows from Theorem 3.12, since B_3 is clearly MM. That it is not centrally nilpotent follows from Lemma 3.6, since the fact that B_3 contains no elements of order 2 means that $Z(L)$ is trivial.

Example 4.18. There are five MNA loops of order 32 which are centrally nilpotent of class greater than 2. In the notation of [Che78], these are $M_{32}(16\Gamma_2 d, 2)$, $M_{32}(1,3,7,2,4,6)$, $M_{32}(3,3,5,4,4,0)$, $M_{32}(3,3,5,4,4,2)$ and $M_{32}(5,7,7,2,4,2)$. These are clearly centrally nilpotent, as they are 2-loops. To see that these are MNA and not nilpotent of class 2, it is simplest to check [GMR99], where they are denoted by 32/6, 32/26, 32/29, 32/30 and 32/36. In each case, the subloops of index 2 are all associative (assuring that they are MNA) and the commutator subloop properly contains the center (assuring nilpotence class greater than 2) which happens to coincide with the associator subloop. Here, we will consider only the first of these loops, $L = M(G, 2)$, where $G = 16\Gamma_2 d = \langle x, y \mid x^8 = (xy)^2 = 1, y^2 = x^2\rangle$. Since squares are clearly central in G, it is easily seen that G is MM, and so L is MNA by Theorem 3.12. On the other hand, $Z(G) = \langle x^2\rangle$, so $Z(L) = \langle x^4\rangle$, by Lemma 3.6. In L, $ux = x^{-1}u = x^7u$, so in $L/Z(L)$, $uZxZ = x^7ZuZ = x^3ZuZ \neq xZuZ$. Thus, $L/Z(L)$ is not commutative. Therefore, L is not nilpotent of class 2. (It is not hard to describe $L/Z(L)$. Observe that $G/Z(L) = \langle x, y \mid x^4 = (xy)^2 = 1, y^2 = x^2\rangle \cong D_4$, which is abelian since $xyxy = 1$, $x^4 = 1$ and $y^2 = x^2$ imply that $yx = x^{-1}y^{-1} = x^3y^{-1} = xy$. Let $z = xy$. Then, $G/Z(L) = \langle x, z\rangle \cong C_4 \times C_2$. Since the inverse map is still an involution on $G/Z(L)$, $L/Z(L) = M(G/Z(L), 2)$, which is associative, since $G/Z(L)$ is abelian. In fact, $L/Z(L) = \langle x, z, u \mid x^4 = z^2 = u^2 = (x, z) = (u, z) = 1, ux = x^{-1}u\rangle \cong D_4 \times C_2$. This is nilpotent of class 2, so that L is nilpotent of class 3. In fact, the other four loops listed above are nilpotent of class 3 as well.)

Example 4.18 raises a new question: Do there exist nonassociative Moufang loops of arbitrary nilpotence class which are MNA? The answer yes, as the following lemma shows.

Lemma 4.19. *For any positive integer n, let G_n be the group $G_n = \langle x, y \mid x^{2^n} = 1, y^2 = x^2, (x, y) = x^{2^{n-1}}\rangle$. Then $L_n = M(G_n, 2)$ is an MNA Moufang loop which is centrally nilpotent of class n.*

Proof. To prove that L_n is centrally nilpotent of class n, we proceed by induction on n.

For $n = 1$, $G_1 = \langle x, y \mid x^2 = y^2 = 1, (x, y) = x\rangle$. Since $x^2 = 1$ and $(x, y) = x$, we have $x = 1$, $G_1 \cong C_2$, and $L_1 \cong C_2 \times C_2$, which is an abelian group.

Suppose that L_k is centrally nilpotent of class k. $G_{k+1} = \langle x, y \mid x^{2^{k+1}} = 1, y^2 = x^2, (x, y) = x^{2^k}\rangle$. Since $y^2 = x^2$, $x^{-1}yxy^{-1} = x^{-1}y^{-1}xy = (x, y) = x^{2^k}$ and so

$yx = x^{2^k+1}y$. Thus, every element of G_{k+1} can be expressed in the form $x^r y^s$, and, since $y^2 = x^2$, we can assume that $0 \le s \le 1$. Also, since $y^2 = x^2$, $x^2y = y^2y = yy^2 = yx^2$, so x^2 is central. On the other hand, since $(x, y) \ne 1$, neither x nor y is central, and neither is xy, since $(xy, x) = (y, x) \ne 1$. Thus $Z(G_{k+1}) = \langle x^2\rangle$. By Lemma 3.6, $Z = Z(L_{k+1}) = \langle z \in Z(G_{k+1}) \mid z^2 = 1\rangle = \langle x^{2^k}\rangle$.

Let $a = xZ$, $b = yZ$ and $v = uZ$ be the images of x, y and u in L_{k+1}/Z. Then $a^{2^k} = x^{2^k}Z = 1Z$, $b^2 = y^2Z = x^2Z = a^2$, and $(a, b) = (xZ, yZ) = (x, y)Z = x^{2^k}Z = a^{2^k}$, so that $\langle a, b\rangle \cong G_k$. (Note that $a^r \ne 1Z$ for $r < k+1$, since $x^r \notin Z$ for such r.)

Furthermore, for $c, d \in \langle a, b\rangle$, $c = gZ$ and $d = hZ$ for some $g, h \in \langle x, y\rangle$. Therefore, $c(dv) = g(hu)Z = (hg)uZ = (dc)v$; $(cv)d = (gu)hZ = (gh^{-1})uZ = (cd^{-1})v$; and $(cv)(dv) = (gu)(hu)Z = h^{-1}gZ = d^{-1}c$. Thus, $L_{k+1}/Z(L_{k+1}) \cong M(G_k, 2)$, which, by the induction hypothesis, is centrally nilpotent of class k. Thus L_{k+1} is centrally nilpotent of class $k + 1$, completing the induction.

To see that $L = L_n$ is MNA, it is enough by Theorem 3.12 to see that $G = G_n$ is MM. But every element $g \in G$ can be expressed in the form $g = x^r y^s$, so $g^2 = x^{2r}y^{2s}(x, y)^{rs} \in \langle x^2\rangle = Z(G)$. Thus, squares are central and $G/Z(G) \cong C_2 \times C_2$. In addition, the order of g divides the order of x which is 2^n, so G is a 2-group.

If H is any subgroup of G, let $\overline{H}$ be the image of H in G/Z. If $\overline{H}$ is a proper subgroup, then it is cyclic and H is abelian. On the other hand, if $\overline{H} = G/Z$, then $G = HZ$ and so $x = hz$, for some $h \in H$, $z \in Z = \langle x^2\rangle$. Therefore, $h = xz^{-1} = x^{2t+1} \in H$. But H is a 2-group since G is, and so, again using the Division Algorithm as above, $x \in H$. A similar argument shows that $y \in H$, so that $H = G$ is not proper. Thus every proper subgroup of G is abelian, and so G is MM and L is MNA. □

We conclude with the following result which suggests a possible approach toward finding all centrally nilpotent MNA Moufang loops of a given class provided that one knows all those of smaller class.

Theorem 4.20. *If L is an MNA Moufang loop with center Z, then L/Z is either associative or MNA.*

Proof. Let $\overline{K}$ be a proper subloop of L/Z, and let K be the full preimage of $\overline{K}$ in L. Then K is a proper subloop of L and so, since L is MNA, K and hence $\overline{K}$ are associative. Thus every proper subloop of L/Z is associative, and so L/Z is either associative itself or it is MNA. □

References

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

[CGta] Orin Chein and Edgar G. Goodaire, *Minimally nonassociative commutative Moufang loops*, Resultate der Mathematik, to appear.

[CGp] Orin Chein and Edgar G. Goodaire, *Minimally nonassociative Moufang loops with a unique nonidentity commutator are ring alternative*, preprint.

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

[CG90] Orin Chein and Edgar G. Goodaire, *Moufang loops with a unique nonidentity commutator (associator, square)*, J. Algebra **130** (1990), no. 2, 369–384.
[Che74] Orin Chein, *Moufang loops of small order I*, Trans. Amer. Math. Soc. **188** (1974), 31–51.
[Che78] Orin Chein, *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. 197, 1–131.
[CR72] Orin Chein and D. A. Robinson, *An "extra" law for characterizing Moufang loops*, Proc. Amer. Math. Soc. **33** (1972), 29–32.
[GJM96] E. G. Goodaire, E. Jespers, and C. Polcino Milies, *Alternative loop rings*, North-Holland Math. Studies, vol. 184, Elsevier, Amsterdam, 1996.
[Gla68] George Glauberman, *On loops of odd order II*, J. Algebra **8** (1968), 393–414.
[GMR99] Edgar G. Goodaire, Sean May, and Maitreyi Raman, *The Moufang loops of order less than* 64, Nova Science Publishers, Inc., Commack, New York, 1999.
[Goo83] Edgar G. Goodaire, *Alternative loop rings*, Publ. Math. Debrecen **30** (1983), 31–38.
[GW68] G. Glauberman and C. R. B. Wright, *Nilpotence of finite Moufang* 2*-loops*, J. Algebra **8** (1968), 415–417.
[Hal59] M. Hall, Jr., *The theory of groups*, MacMillan, New York, 1959.
[Hsu00] Tim Hsu, *Moufang loops of class* 2 *and cubic forms*, Math. Proc. Cambridge Philos. Soc. **128** (2000), 197–222.
[MG] C. Polcino Milies and M. L. Merlini Giuliani, *The smallest Moufang loop*, preprint.
[MM03] G. A. Miller and H. C. Moreno, *Nonabelian groups in which every subgroup is abelian*, Trans. Amer. Math. Soc. **4** (1903), 398–404.
[Pai56] Lowell J. Paige, *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471–482.
[Pfl90] H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Heldermann Verlag, Berlin, 1990.
[Voj] Petr Vojtěchovský, *Generators of nonassociative simple Moufang loops over finite prime fields*, J. Algebra, to appear.

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