Moufang loops of odd order pq^4

Wing Loon Chee*and Andrew Rajah
School of Mathematical Sciences, Universiti Sains Malaysia,
11800 USM, Penang, Malaysia.
wlchee@ymail.com, andy@cs.usm.my

Abstract

The paper continues on the characterisation of positive integers n for which all Moufang loops of order n are associative. We study the case $n = pq^4$ where p and q are distinct odd primes, and show that all Moufang loops of order pq^4 are associative if and only if $q \neq 3$ and $q \not\equiv 1 \pmod{p}$.

Keywords: Moufang loop, order, nonassociative, nucleus, associator

MSC 2010: 20N05

1 Introduction

A Moufang loop is a loop that satisfies the Moufang identity $(xy)(zx) = [x(yz)]x$. Moufang loops are closely related to groups as they share many common properties, e.g., Moufang loops have the inverse property, and satisfy Lagrange's theorem [8], Sylow's theorems (with exception to conjugacy) [6, 9], and Hall's theorem [5]. Another evidence of Moufang loops being "almost" groups, can be found in Moufang's theorem: (1) Any associative triplets in a Moufang loop generate a group; and (2) Moufang loops are diassociative.

Since groups are associative, they satisfy the Moufang identity. Hence, all groups are Moufang loops. However, the converse is not true. The smallest nonassociative Moufang loop is of order 12, constructed by Chein and Pflugfelder [3]. The existence of nonassociative Moufang loops of order 3^4 and p^5 for any prime $p > 3$, has also been proved by Bol [1] and Wright [18] respectively. The most recent class of finite nonassociative Moufang loops was constructed by the second author [14] where he showed that for odd primes p and q, there exists a nonassociative Moufang loop of order pq^3 if and only if $q \equiv 1 \pmod{p}$.

Following the path of these researchers, our interest is to construct new classes of nonassociative Moufang loops. In particular, we study the question:

*Current affiliation: Department of Applied Mathematics, Faculty of Engineering, The University of Nottingham Malaysia Campus, Broga Road, 43500 Semenyih, Selangor, Malaysia. Email: wingloon.chee@nottingham.edu.my

"For what positive integer n does there exist a nonassociative Moufang loop of order n?". To achieve this objective, however, we need to eliminate those cases where all Moufang loops of a particular order are associative. Hence, our research can be divided into two directions: (1) Prove that all Moufang loops of order n are associative, for some positive integer n; or (2) Prove that a nonassociative Moufang loop of order n exists, by giving precisely the product rule of any pair of elements in that loop.

The latest result that is of significance to our research can be found in [15]: If L is a Moufang loop of order $p_1 \cdots p_m q^3 r_1 \cdots r_n$ where $p_1 < \cdots < p_m < q < r_1 < \cdots < r_n$ are odd primes with $q \not\equiv 1 \pmod{p_i}$ for all $i \in \{1, \ldots, m\}$, then L is a group. In this paper, we study the next open case, that is, Moufang loops of order pq^4 where $p < q$ are odd primes. We obtain the necessary and sufficient conditions for the existence of nonassociative Moufang loops of odd order pq^4.

2 Definitions and Notations

Below are some basic definitions and notations that are used throughout this article. We refer the reader to [2] and [13] for a comprehensive description of loop theory.

Definition 2.1. A binary system L is called a *loop* if

(a) L has an identity element;

(b) for any $x, y \in L$, there exist unique elements $a, b \in L$ such that $xa = y$ and $bx = y$.

Definition 2.2. A loop L is a *Moufang loop* if it satisfies any one of the following (equivalent) Moufang identities:

$$(xy)(zx) = [x(yz)]x,$$
$$x[y(xz)] = [(xy)x]z,$$
$$[(zx)y]x = z[x(yx)].$$

From now on, we define L as a Moufang loop.

Definition 2.3. Define

$$z\mathcal{T}(x) = x^{-1}(zx),$$
$$z\mathcal{L}(x, y) = (yx)^{-1}[y(xz)],$$
$$z\mathcal{R}(x, y) = [(zx)y](xy)^{-1}.$$

$\mathcal{I}(L) = \langle \mathcal{T}(x), \mathcal{L}(x, y), \mathcal{R}(x, y) \mid x, y \in L \rangle$ is called the *inner mapping group* of L.

Definition 2.4. The *associator* of three elements x, y, z in L is the unique element $(x, y, z) \in L$ such that $(xy)z = [x(yz)](x, y, z)$. The *associator subloop* of L, denoted by L_a, is the subloop generated by all the associators in L.

Definition 2.5. The *commutator* of two elements x, y in L is the unique element $[x, y] \in L$ such that $xy = (yx)[x, y]$. The *commutator subloop* of L, denoted by L_c, is the subloop generated by all the commutators in L.

Definition 2.6. The *nucleus* of L, denoted by $N(L)$, is the subloop consisting of all $n \in L$ such that $(n, x, y) = (x, n, y) = (x, y, n) = 1$ for all $x, y \in L$.

Definition 2.7. Let K be a subset of L. The *centraliser* of K in L, denoted by $C_L(K)$, is the set consisting of all $\ell \in L$ such that $\ell k = k\ell$ for all $k \in K$.

Definition 2.8. L is *minimally nonassociative* if L is not associative but all proper subloops and proper quotient loops of L are associative.

3 Known Results

Throughout this section, L is defined as a Moufang loop.

Lemma 3.1. *Let $x, y, z \in L$.*

(a) $x\mathcal{L}(z, y) = x(x, y, z)^{-1}$ [2, p.124, Lemma 5.4 (5.16)];

(b) $(x, y, z) = (x, y, zy)$ [2, p.124, Lemma 5.4 (5.17)];

(c) $(x, y, z) = (xy, z, y)^{-1}$ [2, p.124, Lemma 5.4 (5.18)];

(d) $(x, y, z) = (x, y, zx)$ [2, p.124, Lemma 5.4 (5.19)];

(e) $(xn, y, z) = (x, yn, z) = (x, y, zn) = (x, y, z)$ *for any* $n \in N(L)$ [10, p. 267, Lemma 1];

(f) $(x, y, z) = (z, y, x)^{-1} = (y, z, x)$ *if* $L_a \subseteq N(L)$ [14, p. 71, Lemma 2].

Lemma 3.2. *Let $x, y, u, v \in L$ and $\theta \in \mathcal{I}(L)$.*

(a) $(xy)\theta \cdot c = (x\theta) \cdot (y\theta \cdot c)$ *where* $c = [u^{-1}, v^{-1}]$ *if* $\theta = \mathcal{L}(u, v)$, *and* $c = u^{-3}$ *if* $\theta = \mathcal{T}(u)$ [2, p. 112, Lemma 2.1; p. 113, Lemma 2.2; and p. 117, Lemma 3.2];

(b) $(x^n)\theta = (x\theta)^n$ *for any integer* n [2, p. 117, Lemma 3.2; and p. 120, (4.1)].

Lemma 3.3. *Suppose $K \trianglelefteq L$. Then L/K is associative $\Rightarrow L_a \subseteq K$* [11, p. 563, Lemma 1].

Lemma 3.4. *Let L be finite. Suppose $K \leq C_L(L_a)$ and $(|K|, |L_a|) = 1$. Then $K \subseteq N(L)$* [12, Lemma 5, p. 480].

Lemma 3.5. *Let $|L|$ be odd. Then L contains a Hall π-subloop where π is any set of odd primes* [7, p. 409, Theorem 12].

Lemma 3.6. *Suppose L has an odd order and contains a normal Hall subloop $H = \langle x \rangle L_a$ for some $x \in H - L_a$. Then $L_a \subseteq N(L) \Rightarrow H \subseteq N(L)$* [15, p. 373, Lemma 3.17].

Lemma 3.7. *Let $|L| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ where $p_1 < p_2 < \cdots < p_n$ are odd primes and $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}^+$.*

(a) *Suppose $\alpha_i \leq 2$ for all i. Then for every $i \in \{1, 2, \ldots, n\}$, there exists a normal subloop $H_i \trianglelefteq L$ where $|H_i| = p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n}$* [16, p. 970, Lemma 4.1(a)].

(b) *Suppose there exists some $\alpha_k \geq 3$ such that $\alpha_i \leq 2$ for all $i < k$. Then for every $i \in \{1, 2, \ldots, k\}$, there exists a normal subloop $H_i \trianglelefteq L$ where $|H_i| = p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n}$* [16, p. 970, Lemma 4.1(b)].

(c) *Suppose $\alpha_n = 1$ and $p_n \not\equiv 1 \pmod{p_i}$ for all $i < n$. Then there exists a normal subloop of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{n-1}^{\alpha_{n-1}}$ in L* [17, p. 1362, Lemma 4.1].

Lemma 3.8. *Suppose L is not associative.*

(a) *Let $K \leq L$. If $L = \langle x, y \rangle K$ for some $x, y \in L$, then $K \nsubseteq N(L)$* [4, p. 144, Theorem 4.1].

(b) *If L is finite, then $|L|/|N(L)| \neq 1, p$ or pq where p and q are (not necessarily distinct) primes* [4, p. 145, Corollary 4.2].

Lemma 3.9. *Suppose L is minimally nonassociative with an odd order, and contains a maximal normal subloop M.*

(a) *L_a is the unique minimal normal subloop of L, and an elementary abelian group. Moreover, $(L_a, L_a, L) = \{1\}$* [4, p. 140, Theorem 3.3(b)].

(b) *$(k_1k_2, \ell_1, \ell_2) = (k_1, \ell_1, \ell_2)(k_2, \ell_1, \ell_2)$ for any $k_i \in L_a$ and $\ell_i \in L$* [4, p. 141, Proposition 3.4].

(c) *L_a and L_c lie in M, and $L = M\langle x \rangle$ for any $x \in L - M$* [12, p. 478, Lemma 1(b)].

(d) *If H is a Hall subloop of L, then $H \trianglelefteq L_aH \Rightarrow (|L_a|, |H|) \neq 1$* [4, p. 143, Theorem 3.10].

(e) *$(k, w, \ell) = (\ell, k, w^{-1})^{-1}$ for any $k \in L_a$, $w \in M$ and $\ell \in L$* [11, p. 565, Lemma 6(a)].

(f) *$((L_a, M, L)[L_a, M], M, L) = \{1\}$* [11, p. 565, Lemma 6(c)].

(g) *For any $w \in M$ and $\ell \in L$, there exists some $k_0 \in L_a - \{1\}$ such that $(k_0, w, \ell) = (u^{-1}k_0u, w, \ell) = 1$ for all $u \in M$* [4, p. 141, Theorem 3.7; and 15, p. 373, Lemma 3.18].

(h) *If $(k, w, \ell) \neq 1$ for some (fixed) elements $k \in L_a$, $w \in M$ and $\ell \in L$, then L_a contains a proper nontrivial subloop which is normal in M* [4, p. 142, Theorem 3.8].

(i) *If $L_a \subseteq N(L)$, then $[M, (L - M, M, M)] = \{1\}$* [17, p. 1363, Lemma 4.4].

(j) *If* $L_a \subseteq N(L)$*, then for every* $x \in L - M$*, there exist some* $g, h \in M - L_a$ *such that* $(x, g, h) \neq 1$ [17, p. 1362, Lemma 4.2].

(k) $L_a \trianglelefteq N(L)$ *if and only if* $(L_a, M, L) = \{1\}$ [4, p. 146, Theorem 4.7].

Lemma 3.10. *Suppose* L *is minimally nonassociative with order* $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ *where* $p_1, p_2, \ldots, p_n$ *are distinct odd primes and* $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}^+$*. Then*

(a) $|L_a| = p_i^{\beta_i}$ *for some* i *satisfying* $\alpha_i \geq 2$*; and some* β_i *satisfying* $0 < \beta_i < \alpha_i$*;*

(b) $p_i^{\alpha_i} \nmid |N(L)|$ *for all* i*.*

[4, p. 145, Theorem 4.5]

Lemma 3.11. *Suppose* $|L| = p_1 \cdots p_m q^\alpha r_1 \cdots r_n$ *where* $p_1 < \cdots < p_m < q < r_1 < \cdots < r_n$ *are odd primes. Then* L *is a group if any of the following two conditions hold:*

(a) $\alpha = 3$ *and* $q \not\equiv 1 \pmod{p_i}$ *for all* $i \in \{1, 2, \ldots, m\}$ [15, p. 374, Theorem]*; or*

(b) $m = 0$*,* $p > 3$ *and* $\alpha \leq 4$ [11, p. 567, Theorem].

Lemma 3.12. *Let* p *and* q *be distinct odd primes. There exists a nonassociative Moufang loop of order* pq^3 *if and only if* $q \equiv 1 \pmod{p}$ [14, p. 78, Theorem 1; and p. 86, Theorem 2].

4 New Results

Lemma 4.1. *Let* L *be a Moufang loop and* $x, y, z \in L$*. Suppose* $L_a \subseteq N(L)$*,* $[y, (y, z, x)] = 1$ *and* $x^{-1}yx = y^\alpha k$ *for some* $k \in N(L)$ *and* $\alpha \in \mathbb{Z}^+$*. Then* $(x^{-1}, y, z) = (x, y, z)^{-\alpha}$*.*

Proof. First, we show the equation $(y^\alpha, z, x) = (y, z, x)^\alpha$, which is needed in the proof of this lemma.

By Lemma 3.2(b), $y^\alpha \mathcal{L}(x, z) = [y\mathcal{L}(x, z)]^\alpha$. So

$$\begin{aligned} y^\alpha (y^\alpha, z, x)^{-1} &= [y(y, z, x)^{-1}]^\alpha && \text{by Lemma 3.1(a)} \\ &= y^\alpha (y, z, x)^{-\alpha} && \text{as } [y, (y, z, x)] = 1. \end{aligned}$$

Hence,

$$(y^\alpha, z, x) = (y, z, x)^\alpha \tag{4.1}$$

by cancellation. Now

$$\begin{aligned}
(x^{-1},y,z) &= (x^{-1}y,z,y)^{-1} && \text{by Lemma 3.1(c)}\\
&= (x^{-1}y,z,xx^{-1}y)^{-1} && \text{by diassociativity}\\
&= (x^{-1}y,z,x)^{-1} && \text{by Lemma 3.1(d)}\\
&= (y^{\alpha}kx^{-1},z,x)^{-1} && \text{by the hypothesis } x^{-1}yx=y^{\alpha}k\\
&= (y^{\alpha}k,z,x)^{-1} && \text{by Lemmas 3.1(d) and 3.1(f)}\\
&= (y^{\alpha},z,x)^{-1} && \text{by Lemma 3.1(e)}\\
&= (y,z,x)^{-\alpha} && \text{by (4.1)}\\
&= (x,y,z)^{-\alpha} && \text{by Lemma 3.1(f).}
\end{aligned}$$

□

Lemma 4.2. *Let L be a nonassociative Moufang loop of odd order and $x \in L$. Suppose $|L_a| = p^2$ for some prime p and $(|x|, p-1) = 1$. If there exists some $k_0 \in L_a - \{1\}$ such that $[k_0, x] = 1$, then $[L_a, x] \subseteq \langle k_0 \rangle$.*

Proof. Since $|L_a| = p^2$ and L_a is elementary abelian, there exists $k_1 \in L_a - \langle k_0 \rangle$ such that $L_a = \langle k_0 \rangle \times \langle k_1 \rangle$. As $L_a \trianglelefteq L$, it follows that $x^{-1}k_1x \in L_a$. Hence, we can write $x^{-1}k_1x = k_0^{\alpha}k_1^{\beta}$ for some $\alpha, \beta \in \mathbb{Z}^+$. By induction, $x^{-|x|}k_1x^{|x|} = k_0^{\alpha(1+\beta+\cdots+\beta^{|x|-1})}k_1^{\beta^{|x|}}$. Then $k_0^{-\alpha(1+\beta+\cdots+\beta^{|x|-1})} = k_1^{\beta^{|x|}-1} = 1$. Since $|k_1| = p$, the second equation gives $\beta^{|x|} \equiv 1 \pmod p$. So, β has $(|x|, p-1) = 1$ solution. Hence, $\beta = 1$. Thus, $x^{-1}k_1x = k_0^{\alpha}k_1$. Therefore, $k_1^{-1}x^{-1}k_1x = [k_1, x] = k_0^{\alpha} \in \langle k_0 \rangle$. Since $[k_0, x] = 1 \in \langle k_0 \rangle$, we can easily show that $[k, x] \in \langle k_0 \rangle$ for all $k \in L_a$ by writing $k = k_0^{\gamma}k_1^{\delta}$ for some $\gamma, \delta \in \mathbb{Z}^+$. □

Corollary 4.3. *Let L be a nonassociative Moufang loop of odd order and $x \in L$. Suppose $|L_a| = p^2$ for some prime p and $(|x|, p) = (|x|, p-1) = 1$. If there exists some $k_0 \in L_a - \{1\}$ such that $[k_0, x] = 1$, then $[L_a, x] = \{1\}$.*

Proof. Let $k_1 \in L_a - \langle k_0 \rangle$ such that $L_a = \langle k_0 \rangle \times \langle k_1 \rangle$. Write $x^{-1}k_1x = k_0^{\alpha}k_1^{\beta}$ for some $\alpha, \beta \in \mathbb{Z}^+$. From the proof of Lemma 4.2, $k_0^{\alpha(1+\beta+\cdots+\beta^{|x|-1})} = 1$ where $\beta = 1$. Hence, $k_0^{\alpha|x|} = 1$ and p divides $\alpha|x|$. Since $(|x|, p) = 1$, it follows that $p \mid \alpha$. Hence, $x^{-1}k_1x = k_1$, i.e., $[k_1, x] = 1$. As x commutes with both generators of L_a, we have $[k, x] = 1$ for all $k \in L_a$. □

Lemma 4.4. *Let L be a minimally nonassociative Moufang loop of odd order and M a maximal normal subloop of L.*

(a) *Suppose there exist some $k \in L_a$, $w \in M$ and $\ell \in L$ such that $(k, w, \ell) = 1$. Then $(k, L_a\langle w \rangle, \ell) = \{1\}$.*

(b) *Suppose there exist some $k \in L_a$ and $w \in M$ such that $[k, w] = 1$. Then $[k, L_a\langle w \rangle] = \{1\}$.*

Proof. Suppose

$$(k, w, \ell) = 1 \text{ for some } k \in L_a,\ w \in M \text{ and } \ell \in L.$$

Let $c = [k^{-1}, \ell^{-1}]$. Take any $u \in L_a\langle w\rangle$. Write $u = k_1 w^\alpha$ for some $k_1 \in L_a$ and $\alpha \in \mathbb{Z}^+$. Now

$$\begin{aligned}
& u\mathcal{L}(k,\ell)\cdot c = k_1\mathcal{L}(k,\ell)\cdot[w^\alpha\mathcal{L}(k,\ell)\cdot c] && \text{by Lemma 3.2(a)}\\
\Rightarrow\ & u(u,\ell,k)^{-1}\cdot c \\
& = k_1(k_1,\ell,k)^{-1}\cdot[w^\alpha(w^\alpha,\ell,k)^{-1}\cdot c] && \text{by Lemma 3.1(a)}\\
& = k_1\cdot w^\alpha c && \text{by Lemma 3.9(a) and hypothesis}\\
& = k_1 w^\alpha\cdot c && \text{by Lemma 3.9(c)}\\
& = uc.
\end{aligned}$$

After cancellation, we get $(u,\ell,k)^{-1} = 1$. By Moufang's theorem, $(k,u,\ell) = 1$. This proves (a).

Suppose

$$[k,w] = 1 \text{ for some } k \in L_a \text{ and } w \in M.$$

For any $u \in L_a\langle w\rangle$, write $u = k_2 w^\beta$ for some $k_2 \in L_a$ and $\beta \in \mathbb{Z}^+$. Then

$$\begin{aligned}
[k,u] &= k^{-1}u^{-1}ku && \text{by definition of commutator}\\
&= k^{-1}(w^{-\beta}k_2^{-1})k(k_2w^\beta) && \text{by antiautomorphic inverse property}\\
&= k^{-1}w^{-\beta}k_2^{-1}kk_2w^\beta && \text{by Lemma 3.9(c)}\\
&= k^{-1}w^{-\beta}kw^\beta && \text{as } L_a \text{ is abelian by Lemma 3.9(a)}\\
&= 1 && \text{by hypothesis and diassociativity.}
\end{aligned}$$

This completes the proof of this lemma. □

Lemma 4.5. *Let L be a minimally nonassociative Moufang loop of odd order and M a maximal normal subloop of L. Suppose there exist some $k \in L_a - \{1\}$ and $x \in L - M$ such that $(k, M, x) = [k, M] = \{1\}$. Then $L_a \trianglelefteq N(L)$.*

Proof. Since M is a maximal normal subloop of L, we can write $L = M\langle x\rangle$ by Lemma 3.9(c). Take any $\ell \in L$. Then $\ell = u_1 x^\alpha$ where $u_1 \in M$ and $\alpha \in \mathbb{Z}^+$.

Let u be any element in M. Write $c = [k^{-1}, u^{-1}]$. By Lemma 3.2(a), $\ell\mathcal{L}(k,u)\cdot c = u_1\mathcal{L}(k,u)\cdot[x^\alpha\mathcal{L}(k,u)\cdot c]$. Since $[k,u] = 1$, we have

$$\ell(\ell,u,k)^{-1} = u_1(u_1,u,k)^{-1}\cdot[x^\alpha(x^\alpha,u,k)^{-1}] \tag{4.2}$$

by Lemma 3.1(a).

Since $L_a \subseteq M$ by Lemma 3.9(c), $k, u, u_1 \in M$. As L is minimally nonassociative, it follows that M is a group and $(u_1, u, k) = 1$. By our hypothesis and Moufang's theorem, $(x^\alpha, u, k) = 1$. By cancellation from (4.2) and Moufang's theorem, we get

$$(k,u,\ell) = 1 \text{ for all } u \in M \text{ and } \ell \in L. \tag{4.3}$$

Take any $h \in L$. We wish to show that $(k,h,\ell) = 1$. If $h \in M$, then we are through. Now if $h \notin M$, then by Lemma 3.9(c), $L = M\langle h\rangle$. Hence for any

$\ell \in L$, we can write $\ell = u_2 h^\beta$ for some $u_2 \in M$ and $\beta \in \mathbb{Z}^+$. Next,

$$\begin{aligned}(k,h,\ell) &= (k,h,u_2h^\beta) \\ &= (k,h,u_2) && \text{by Lemma 3.1(b)} \\ &= 1 && \text{by (4.3) and Moufang's theorem.}\end{aligned}$$

Hence, $k \in N(L)$. Now $N(L)$ is a nontrivial normal subloop of L. Thus $L/N(L)$ is a proper quotient loop of L. By the minimally nonassociative property of L, $L/N(L)$ is associative and by Lemmas 3.3 and 3.9(a), $L_a \trianglelefteq N(L)$. $\square$

Lemma 4.6. *Let L be a minimally nonassociative Moufang loop of odd order and M a maximal normal subloop of L. Suppose $(k_0, w_0, \ell_0) \neq 1$ for some (fixed) $k_0 \in L_a$, $w_0 \in M$ and $\ell_0 \in L$. Then for any $x \in L - M$, there exist some $k \in L_a$ and $w \in M$ such that $(k, w, x) \neq 1$.*

Proof. Suppose not. Then there exists some $x_0 \in L - M$ such that

$$(k, w, x_0) = 1 \text{ for all } k \in L_a \text{ and all } w \in M. \tag{4.4}$$

By Lemma 3.9(c), $L = M\langle x_0 \rangle$. Hence $\ell_0 = w_1 x_0^\alpha$ where $w_1 \in M$ and $\alpha \in \mathbb{Z}^+$. Write $c = [k_0^{-1}, w_0^{-1}]$. Now $L_a \trianglelefteq L$ by Lemma 3.9(a). Thus, $c = k_0 \cdot w_0 k_0^{-1} w_0^{-1} \in L_a$ by diassociativity. Then by Lemmas 3.2(a) and 3.1(a),

$$\begin{aligned} & \ell_0 \mathcal{L}(k_0, w_0) \cdot c = w_1 \mathcal{L}(k_0, w_0) \cdot [x_0^\alpha \mathcal{L}(k_0, w_0) \cdot c] \\ \Rightarrow\quad & \ell_0 (\ell_0, w_0, k_0)^{-1} \cdot c = w_1 (w_1, w_0, k_0)^{-1} \cdot [x_0^\alpha (x_0^\alpha, w_0, k_0)^{-1} \cdot c]. \end{aligned}$$

Now $k_0 \in L_a \subseteq M$ by Lemma 3.9(c). Since L is minimally nonassociative and M is a proper subloop of L, it follows that M is a group. Hence $(w_1, w_0, k_0) = 1$. Our assumption in (4.4) and Moufang's theorem give $(x_0^\alpha, w_0, k_0) = 1$. Thus,

$$\begin{aligned}\ell_0(\ell_0, w_0, k_0)^{-1} \cdot c &= w_1 \cdot x_0^\alpha c \\ &= w_1 x_0^\alpha \cdot c && \text{as } c \in L_a \text{ and } (c, w_1, x_0) = 1 \text{ by (4.4)} \\ &= \ell_0 c.\end{aligned}$$

By cancellation and Moufang's theorem, we have $(k_0, w_0, \ell_0) = 1$ which contradicts our hypothesis. The result now follows. $\square$

Lemma 4.7. *Let L be a nonassociative Moufang loop of order pq^4 where $p < q$ are odd primes with $q \not\equiv 1 \pmod p$; and Q a maximal normal subloop of order q^4 in L. Suppose $|L_a| = q^2$.*

(a) *$(L_a, Q, L) = \{1\}$.*

(b) *If $L_a \subseteq N(L)$, then $x^{-1}Qx \subseteq \langle w \rangle L_a$ for all $x \in L - Q$.*

Proof. (a) Assume not. Then $(k', w', \ell') \neq 1$ for some $k' \in L_a$, $w' \in Q$ and $\ell' \in L$. By Lemma 3.5, there exists a subloop P of order p in L. As P is cyclic, we can write $P = \langle x \rangle$. Clearly $x \in L - Q$. Then by Lemma 4.6,

$$(k, w, x) \neq 1 \text{ for some } k \in L_a \text{ and } w \in Q. \tag{4.5}$$

Now by Lemma 3.9(g), there exists $k_0 \in L_a - \{1\}$ such that

$$(k_0, w, x) = 1. \tag{4.6}$$

Then by Lemma 3.9(h), there exists $S = \langle u^{-1}k_0u \mid u \in Q \rangle$, a proper nontrivial subloop of L_a which is normal in Q. Since $|L_a| = q^2$, it follows that $|S| = q$. As $1 \neq k_0 \in S$, we can write $S = \langle k_0 \rangle$. Hence, $u^{-1}k_0u \in \langle k_0 \rangle$ for all $u \in Q$ as $S \trianglelefteq Q$. Thus, $[k_0, u] = 1$ for all $u \in Q$ by result from group theory.

Since $(k, w, x) \neq 1$, we have $k \notin \langle k_0 \rangle$. Hence, $L_a = \langle k_0 \rangle \times \langle k \rangle$. Then by Lemma 4.2, $[k, w] \in \langle k_0 \rangle$ as $(|w|, q - 1) = 1$. Now

$$\begin{aligned}
& ((k, w, x)[k, w], w, x) = 1 && \text{by Lemma 3.9(f)} \\
\Rightarrow\quad & ((k, w, x), w, x)([k, w], w, x) = 1 && \text{by Lemma 3.9(b)} \\
\Rightarrow\quad & ((k, w, x), w, x)(k_0^{\alpha}, w, x) = 1 && \text{for some } \alpha \in \mathbb{Z}^+ \\
\Rightarrow\quad & ((k, w, x), w, x) = 1 && \text{since } (k_0, w, x) = 1 \text{ by (4.6).}
\end{aligned}$$

Write $k_1 = (k, w, x)$. Then

$$(k_1, w, x) = 1. \tag{4.7}$$

Suppose $k_1 \notin \langle k_0 \rangle$. Then $L_a = \langle k_0 \rangle \times \langle k_1 \rangle$. Hence

$$\begin{aligned}
(k, w, x) &= (k_0^{\beta} k_1^{\gamma}, w, x) && \text{for some } \beta, \gamma \in \mathbb{Z}^+ \\
&= (k_0^{\beta}, w, x)(k_1^{\gamma}, w, x) && \text{by Lemma 3.9(b)} \\
&= 1 && \text{by (4.6) and (4.7).}
\end{aligned}$$

This contradicts (4.5). So $k_1 \in \langle k_0 \rangle$, i.e., $\langle k_0 \rangle = \langle k_1 \rangle = C_q$. By using Lemma 3.2(b), we get

$$\begin{aligned}
& x^{-1}\mathcal{L}(w^{-1}, k) = [x\mathcal{L}(w^{-1}, k)]^{-1} \\
\Rightarrow\quad & x^{-1}(x^{-1}, k, w^{-1})^{-1} = [x(x, k, w^{-1})^{-1}]^{-1} && \text{by Lemma 3.1(a)} \\
& \qquad = (x, k, w^{-1})x^{-1} \\
\Rightarrow\quad & x(x, k, w^{-1})x^{-1} = (x^{-1}, k, w^{-1})^{-1} \\
\Rightarrow\quad & x(x, k, w^{-1})^{-1}x^{-1} = (x^{-1}, k, w^{-1}) \\
\Rightarrow\quad & x(k, w, x)x^{-1} = (x^{-1}, k, w^{-1}) && \text{by Lemma 3.9(e)} \\
\Rightarrow\quad & xk_1x^{-1} = (x^{-1}, k, w^{-1}).
\end{aligned}$$

Suppose $(x^{-1}, k, w^{-1}) \in \langle k_1 \rangle$. Then, $xk_1x^{-1} \in \langle k_1 \rangle$. Hence, $[k_1, x] = 1$ by diassociativity and the fact that $(|x|, |k_1| - 1) = (p, q - 1) = 1$. Also $(|x|, q) = (p, q) = 1$ as p and q are distinct primes. Thus, by Corollary 4.3, $[k, x] = 1$ for all $k \in L_a$. So, $x \in C_L(L_a)$ and $\langle x \rangle \leq C_L(L_a)$. Therefore, by Lemma 3.4, we have $\langle x \rangle \subseteq N(L)$, contrary to (4.5). So, $(x^{-1}, k, w^{-1}) \notin \langle k_1 \rangle$. By Lemma 3.9(e), $(x^{-1}, k, w^{-1}) = (k, w, x^{-1})^{-1}$.

Now write $k_2 = (k, w, x^{-1})^{-1}$. Then $L_a = \langle k_1 \rangle \times \langle k_2 \rangle$. Next

$$\begin{array}{lll} & ((k,w,x^{-1})[k,w],w,x^{-1}) = 1 & \text{by Lemma 3.9(f)} \\ \Rightarrow & ((k,w,x^{-1}),w,x^{-1})([k,w],w,x^{-1}) = 1 & \text{by Lemma 3.9(b)} \\ \Rightarrow & ((k,w,x^{-1}),w,x^{-1})(k_0^{\alpha},w,x^{-1}) = 1 & \text{for some } \alpha \in \mathbb{Z}^+ \\ \Rightarrow & ((k,w,x^{-1}),w,x^{-1}) = 1 & \text{as } (k_0,w,x) = 1 \text{ by (4.6)} \\ \Rightarrow & ((k,w,x^{-1})^{-1},w,x) = 1 & \text{by Moufang's theorem.} \end{array}$$

Hence,

$$(k_2, w, x) = 1. \tag{4.8}$$

Then

$$\begin{aligned} (k,w,x) &= (k_1^{\delta}k_2^{\varepsilon},w,x) && \text{for some } \delta,\varepsilon \in \mathbb{Z}^+ \\ &= (k_1^{\delta},w,x)(k_2^{\varepsilon},w,x) && \text{by Lemma 3.9(b)} \\ &= 1 && \text{by (4.7) and (4.8).} \end{aligned}$$

This contradicts (4.5). The result now follows.

(b) By Lemma 3.9(c), $L_a \subseteq Q$. Take any $x \in L - Q$ and $w \in Q$.

Suppose $w \in L_a$. Then $x^{-1}wx \in L_a = \langle w \rangle L_a$ as $L_a \trianglelefteq L$.

Now suppose $w \in Q - L_a$. Since Q is a q-loop, it follows that q divides $|w|$. It is also clear that p divides $|x|$. Now we form a subloop $H = \langle x, w \rangle$ in L.

Case 1. $|H| = pq$.

By Lemma 3.7(a), $\langle w \rangle \trianglelefteq H$. Then $x^{-1}wx \in \langle w \rangle \subseteq \langle w \rangle L_a$.

Case 2. $|H| = pq^2$.

We know that $|L_aH| = \frac{|L_a||H|}{|L_a \cap H|} = \frac{q^2 \cdot pq^2}{|L_a \cap H|} \leq pq^4$. Since $|L_a| = q^2$, we have $|L_a \cap H| = 1, q$ or q^2.

Suppose $|L_a \cap H| = 1$. Then $|L_aH| = pq^4 = |L|$. Hence, $L = \langle x, w \rangle L_a$. By Lemma 3.8(a), $L_a \nsubseteq N(L)$, contradicting our hypothesis.

Suppose $|L_a \cap H| = q^2$. Then $L_a \subseteq H$. By Lemma 3.7(a), there exists a normal subloop Q_0 of order q^2 in H. Now $|L_aQ_0| = \frac{|L_a||Q_0|}{|L_a \cap Q_0|} = \frac{q^2 \cdot q^2}{|L_a \cap Q_0|} \leq |H| = pq^2$. Hence, $|L_a \cap Q_0| = q^2$ and $L_a = Q_0$. This is a contradiction as $w \in Q_0 - L_a$.

So, $|L_a \cap H| = q$. Then there exists some $k_1 \in L_a - H$. By forming a subloop $\langle H, k_1 \rangle$ in L, we have $|\langle H, k_1 \rangle| = pq^3$ or pq^4. If $|\langle H, k_1 \rangle| = pq^4$, then $L = \langle H, k_1 \rangle = \langle x, w, k_1 \rangle$. Since $k_1 \in L_a \subseteq N(L)$, it follows that $(x, w, k_1) = 1$. Thus L is a group by Moufang's theorem. This is a contradiction.

Therefore, $|\langle H, k_1 \rangle| = pq^3$. By Lemma 3.7(b), there exists a normal subloop Q_1 of order q^3 in $\langle H, k_1 \rangle$. Now since $L_a \subseteq \langle H, k_1 \rangle$, it follows easily that $L_a \subseteq Q_1$. As $w \notin L_a$, we can write $Q_1 = \langle w \rangle L_a$. Hence, $x^{-1}wx \in Q_1 = \langle w \rangle L_a$.

Case 3. $|H| = pq^3$.

Suppose $L_a \nsubseteq H$. Then there exists some $k_2 \in L_a - H$. Hence, $|\langle H, k_2\rangle| = pq^4 = |L|$. Thus, $L = \langle H, k_2\rangle = \langle x, w, k_2\rangle$. Similar to the previous case, $(x, w, k_2) = 1$ as $k_2 \in L_a \subseteq N(L)$. Then by Moufang's theorem, L is a group which is a contradiction.

So, $L_a \subseteq H$. By Lemma 3.7(b), there exists a normal subloop Q_2 of order q^3 in H. Clearly $L_a \subseteq Q_2$. Since $w \notin L_a$, we can write $Q_2 = \langle w\rangle L_a$. Hence, $x^{-1}wx \in Q_2 = \langle w\rangle L_a$.

Case 4. $|H| = pq^4$.

Then $L = H = \langle x, w\rangle$. Hence, L is a group by diassociativity. This is a contradiction.

The result now follows. □

Theorem 4.8. *Let L be a Moufang loop of order pq^4 where $p < q$ are odd primes and $q \not\equiv 1 \pmod p$. Then L is a group.*

Proof. Suppose L is not associative. By Lagrange's theorem, the order of any subloop of L divides the order of L. Hence, by Lemma 3.11, every proper subloop of L is a group. The same applies to every proper quotient loop of L. Thus L is minimally nonassociative.

Now by Lemma 3.9(a), L_a is a minimal normal subloop of L and is an elementary abelian group. So $|L_a| = q, q^2$ or q^3 by Lemma 3.10(a).

From Lemma 3.5, there exists a subloop P of order p in L. Since P is cyclic, we can write $P = \langle x\rangle$. By Lemma 3.7(b), there exists a normal subloop Q of order q^4 in L. Clearly Q is a maximal normal subloop of L. Hence, $L = Q\langle x\rangle$ by Lemma 3.9(c).

Case 1. $|L_a| = q$.

Since $L_a \trianglelefteq L$, L_aP is a subloop of order pq in L. By Lemma 3.7(c), $P \trianglelefteq L_aP$. Now $(|L_a|, |P|) = (q, p) = 1$, contrary to Lemma 3.9(d).

Case 2. $|L_a| = q^2$.

From Lemma 4.7(a), we have $(k, w, \ell) = 1$ for all $k \in L_a$, $w \in Q$, $\ell \in L$. By Lemma 3.9(k), $L_a \trianglelefteq N(L)$. Hence, q^2 divides $|N(L)|$. Now p and q^4 cannot divide $|N(L)|$ by Lemma 3.10(b). Thus, $|N(L)| = q^2$ or q^3.

Suppose $|N(L)| = q^3$. Then $|L|/|N(L)| = pq$. This contradicts Lemma 3.8(b). So, $|N(L)| = q^2$ and $L_a = N(L)$.

By Lemma 3.9(j), there exist some $g, h \in Q$ such that $(x, g, h) \neq 1$. Now by Lemmas 3.2(b) and 3.1(a), we get first $x^{-1}\mathcal{L}(h, g) = [x\mathcal{L}(h, g)]^{-1}$, then $x^{-1}(x^{-1}, g, h)^{-1} = (x, g, h)x^{-1}$, and finally

$$x(x, g, h)x^{-1} = (x^{-1}, g, h)^{-1}. \tag{4.9}$$

By Lemma 4.7(b), we have $x^{-1}gx = g^\alpha k$ for some $k \in L_a$ and $\alpha \in \mathbb{Z}^+$. By Lemma 3.9(i), $[g, (x, g, h)] = 1$. Then we use Lemma 4.1 to obtain $(x^{-1}, g, h)^{-1} = (x, g, h)^\alpha \in \langle (x, g, h)\rangle$.

Now from equation (4.9), $x(x,g,h)x^{-1} = (x,g,h)^{\alpha}$. Then, by diassociativity, $\langle x,(x,g,h)\rangle$ is a group and hence, $[x,(x,g,h)] = 1$ by group theory. We observe that since $|x| = p$, it follows that $(|x|,q) = (|x|,q-1) = 1$. So by using Corollary 4.3, we have $[x,k] = 1$ for all $k \in L_a$. Hence, $x \in C_L(L_a)$ and $\langle x\rangle \le C_L(L_a)$. It is also clear that $(|\langle x\rangle|,|L_a|) = (p,q^2) = 1$. Thus by Lemma 3.4, we have $\langle x\rangle \subseteq N(L)$, a contradiction as $|N(L)| = q^2$.

Case 3. $|L_a| = q^3$.

Recall that Q is a maximal normal subloop of L. Since $|Q| = q^4$ and $|L_a| = q^3$, we can write $Q = L_a\langle u\rangle$ for any $u \in Q - L_a$.

Subcase 3.1. $(k,w,\ell) = 1$ for all $k \in L_a$, $w \in Q$, $\ell \in L$.

By Lemma 3.9(k), $L_a \trianglelefteq N(L)$. Then by Lemma 3.6, $Q \subseteq N(L)$. This contradicts Lemma 3.10(b).

Subcase 3.2. $(k,w,\ell) \neq 1$ for some $k \in L_a$, $w \in Q$, $\ell \in L$.

Suppose $w \in L_a$. Then $(k,w,\ell) = 1$ as $(L_a,L_a,L) = \{1\}$ by Lemma 3.9(a). Hence, $w \notin L_a$. Thus, we can write $Q = L_a\langle w\rangle$. By Lemma 3.9(g), there exists some $k_0 \in L_a - \{1\}$ such that $(k_0,w,\ell) = 1$. So, $(k_0,u,\ell) = 1$ for all $u \in Q$, by Lemma 4.4(a).

Suppose $[k_0,w] = 1$. By Lemma 4.4(b), $[k_0,u] = 1$ for all $u \in Q$ as $Q = L_a\langle w\rangle$. So by Lemma 4.5, $L_a \trianglelefteq N(L)$. Hence, q^3 divides $|N(L)|$. Thus, $|L|/|N(L)| = 1, p$ or pq. This contradicts Lemma 3.8(b). Therefore, $[k_0,w] \neq 1$.

By Lemma 3.9(h), there exists $S = \langle u^{-1}k_0u \mid u \in Q\rangle$, a proper nontrivial subloop of L_a which is normal in Q. Since $|L_a| = q^3$, it follows that $|S| = q$ or q^2.

Suppose $|S| = q$. Since $1 \neq k_0 \in S$, we can write $S = \langle k_0\rangle$. Hence, $w^{-1}k_0w \in \langle k_0\rangle$ as $S \trianglelefteq Q$. Thus, by result from group theory, we get $[k_0,w] = 1$, a contradiction.

So, $|S| = q^2$. Since Q is a finite q-group and $S \trianglelefteq Q$, we have $S \cap Z(Q) \neq \{1\}$ by result from group theory. As $[k_0,w] \neq 1$, it follows that $k_0 \notin Z(Q)$. Hence, $|S \cap Z(Q)| = q$. Then there exists some $s \in S$ such that $[s,u] = 1$ for all $u \in Q$. Since $(k_0,w,\ell) = 1$, it follows from Lemma 3.9(g) that $(s,w,\ell) = 1$. Thus, $(s,u,\ell) = 1$ for all $u \in Q$ by Lemma 4.4(a). Now by Lemma 4.5, $L_a \trianglelefteq N(L)$. This is a contradiction as $(k,w,\ell) \neq 1$.

Therefore, nevertheless, L is a group. □

Corollary 4.9. *Let p and q be distinct odd primes. All Moufang loops of order pq^4 are associative if and only if $q \neq 3$ and $q \not\equiv 1 \pmod{p}$.*

Proof. Suppose $q = 3$. Then there exists a nonassociative Moufang loop of order $q^4 = 3^4$. Hence, by using the direct product of this nonassociative Moufang loop and any group of order p, we can construct a nonassociative Moufang loop of order $p \cdot 3^4$.

Suppose, on the other hand, that $q \equiv 1 \pmod{p}$. By Lemma 3.12, there exists a nonassociative Moufang loop of order pq^3. Again by using the direct product of this nonassociative Moufang loop and any group of order q, we can construct a nonassociative Moufang loop of order pq^4.

Now suppose L is a Moufang loop of order pq^4 with $q \not\equiv 1 \pmod p$ and $q \neq 3$. If $q < p$, then by Lemma 3.11(b), L is associative. However if $p < q$, then L is associative by Theorem 4.8. □

5 Open Questions

Let p_1, p_2 and q be odd primes with $p_i < q$ and $q \not\equiv 1 \pmod{p_i}$ for all i. Are all Moufang loops of order $p_1 p_2 q^4$ associative if

(a) $p_1 = p_2$?

(b) $p_1 \neq p_2$?

Acknowledgments

The research of the first author was supported by the USM Fellowship Scheme. The research of the second author was supported by grant no. 203/PMATHS/6711231 of the Fundamental Research Grant Scheme.We also thank the referees for their careful reading and useful comments.

References

[1] G. Bol, Gewebe und gruppen, *Math. Ann.* **114** (1937), 414–431.

[2] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, New York, 1971.

[3] O. Chein and H. O. Pflugfelder, The smallest Moufang loop, *Arch. Math.* **22** (1971), 573–576.

[4] W. L. Chee and A. Rajah, Moufang loops that are almost groups, *J. Group Theory* **15** (2012), 137–149.

[5] S. M. Gagola III, Hall's theorem for Moufang loops, *J. Algebra* **323** (2010), 3252–3262.

[6] S. M. Gagola III, The number of Sylow p-subloops in finite Moufang loops, *Comm. Algebra* **38** (2010), 1436–1448.

[7] G. Glauberman, On loops of odd order II, *J. Algebra* **8** (1968), 393–414.

[8] A. N. Grishkov and A. V. Zavarnitsine, Lagrange's theorem for Moufang loops, *Math. Proc. Camb. Phil. Soc.* **139** (2005), 41–57.

[9] A. N. Grishkov and A. V. Zavarnitsine, Sylow's theorem for Moufang loops, *J. Algebra* **321** (2009), 1813–1825.

[10] F. Leong and A. Rajah, On Moufang loops of odd order pq^2, *J. Algebra* **176** (1995), 265–270.

[11] F. Leong and A. Rajah, Moufang loops of odd order $p^4q_1\cdots q_n$, *J. Algebra* **184** (1996), 561–569.

[12] F. Leong and A. Rajah, Moufang loops of odd order $p^\alpha q_1^2\cdots q_n^2 r_1\cdots r_m$, *J. Algebra* **190** (1997), 474–486.

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

[14] A. Rajah, Moufang loops of odd order pq^3, *J. Algebra* **235** (2001), 66–93.

[15] A. Rajah and W. L. Chee, Moufang loops of odd order $p_1p_2\cdots p_nq^3$, *Bull. Malays. Math. Sci. Soc. (2)* **34** (2) (2011), 369–377.

[16] A. Rajah and W. L. Chee, Moufang loops of odd order $p_1^2p_2^2\cdots p_n^2q^3$, *Int. J. Algebra* **5** (20) (2011), 965–975.

[17] A. Rajah and W. L. Chee, Moufang loops of odd order p^3q^3, *Internat. J. Algebra Comput.* **21** (8) (2011), 1357–1367.

[18] C. R. B. Wright, Nilpotency conditions for finite loops, *Illinois J. Math.* **9** (1965), 399–409.