Sylow’s theorem for Moufang loops

ALEXANDER N. GRISHKOV\textsuperscript{1}, ANDREI V. ZAVARNITSINE\textsuperscript{2}

Abstract

For finite Moufang loops, we prove an analog of the first Sylow theorem giving a criterion of the existence of a \( p \)-Sylow subloop. We also find the maximal order of \( p \)-subloops in the Moufang loops that do not possess \( p \)-Sylow subloops.

Keywords: Moufang loop, Sylow’s theorem, group with triality

MSC2000: 08A05, 20N05, 17D05

1 Introduction

After a positive solution to the Lagrange problem for finite Moufang loops was given [8], proving an analog of Sylow’s theorems has become an important problem in the theory of finite Moufang loops [7]. We should mention right away that an obvious obstruction to the precise analog of the first Sylow theorem about the existence of a \( p \)-Sylow subloop has been known for a long time: if \( M(q) \) is a finite simple Paige loop over a finite field \( F \), then the orders of elements of \( M(q) \) divide \( q(q^2 - 1) \), whereas the order of \( M(q) \) is

\[ \frac{1}{d} q^3(q^4 - 1), \]

where \( d = \gcd(2, q - 1) \). Hence, for a prime \( p \) dividing \( \frac{1}{d}(q^2 + 1) \), a \( p \)-Sylow subloop of \( M(q) \) does not exist; consequently, nor does it exist in any finite Moufang loop having a composition factor isomorphic to \( M(q) \).

The main result of the present paper asserts that this obstruction to the existence of a \( p \)-Sylow subloop is in fact the only one. Namely, if a composition series of a Moufang loop \( M \) contains no simple factors \( M(q) \) such that \( p \mid \frac{1}{d}(q^2 + 1) \), then \( M \) has a \( p \)-Sylow subloop. In this case, we call \( p \) a \textit{Sylow prime} for \( M \). In particular, every prime is Sylow for all solvable finite Moufang loops, i. e., a \( p \)-Sylow subloop exists in this case for every \( p \).

We note that this result for Moufang loops of odd order (in fact, a stronger result on the existence of Hall \( \pi \)-subloops) was proved in [5].

Many major results about finite Moufang loops were proved based on the correspondence between Moufang loops and groups with triality [4]. This

\textsuperscript{1}Departamento de Matemática, USP, São Paulo, Brazil.
\textsuperscript{2}Sobolev Institute of Mathematics, Novosibirsk, Russia
paper is not an exception. Clearly, the existence of a $p$-Sylow subloop is related to the existence of an $S$-invariant subgroup in a corresponding group $G$ with triality $S$. Unfortunately, even when the above obstruction to the existence of a $p$-Sylow subloop in $M$ is absent (which is always the case, for example, when $p = 2$ or $3$), one cannot guarantee existence in $G$ of an $S$-invariant $p$-Sylow subgroup. We therefore prove only that $G$ possesses a sufficiently large $S$-invariant $p$-subgroup whose corresponding $p$-subloop in $M$ is $p$-Sylow.

A Moufang loop $M$ may still have nontrivial $p$-subloops even when $p$ is not a Sylow prime for $M$. The order of such a $p$-subloop is obviously bounded by the product of the orders of $p$-Sylow subloops of the composition factor of $M$ for which $p$ is Sylow. In the last section, we show that this bound is actually achieved for all finite Moufang loops $M$. We call such $p$-subloops of maximal order quasi-$p$-Sylow. In this way, Sylow’s theorem can be reformulated as follows:

**Theorem A** Every finite Moufang loop has a quasi-$p$-Sylow subloop for all primes $p$.

The proof of this result uses the following important structural theorem (see Theorem 3 in section 5) for Moufang loops:

**Theorem B** Every finite Moufang loop $M$ contains uniquely determined normal subloops $Gr(M)$ and $M_0$ such that $Gr(M) \leq M_0$, $M/M_0$ is an elementary abelian 2-group, $M_0/Gr(M)$ is the direct product of simple Paige loops $M(q)$ (where $q$ may vary), the composition factors of $Gr(M)$ are groups, and $Gr(M/Gr(M)) = 1$.

Another interesting auxiliary fact we obtain is that a nonassociative minimal normal subloop of a finite Moufang loop must necessarily be simple (see (i) of Theorem 3). This extends the well-known group-theoretic assertion that a minimal normal subgroup of a finite group is the direct product of isomorphic simple groups.

It is natural to conjecture that the analogs of other two Sylow theorems, namely the embedding of $p$-subloops of $M$ into a quasi-$p$-Sylow subloop and the conjugacy of quasi-$p$-Sylow subloops by (inner) automorphisms of $M$, are true for finite Moufang loops as well. As far as determining the number of quasi-$p$-Sylow subloops, at present we do not have a formulation of the corresponding conjecture for lack of sufficient experimental data.
2 Preliminaries

All loops we consider are finite. If $x, y$ are elements of a group $G$ then $x^y = y^{-1}xy$, $x^{-y} = (x^{-1})^y$, $[x, y] = x^{-1}x^y$. $Z(G)$ is the center of $G$. If $\varphi \in \text{Aut}(G)$ then $x^\varphi$ is the image of $x$ under $\varphi$. If $n$ is an integer and $p$ is a prime then the notation $p^k \parallel n$ for $k \geq 0$ means that $p^k \mid n$ and $p^{k+1} \nmid n$. For natural numbers $m, n$, we write $(m, n)$ for $\gcd(m, n)$.

A loop $M$ is called a Moufang loop if $xy \cdot zx = (x \cdot yz)x$ for all $x, y, z \in M$. For $x, y, z \in M$ define the commutator $[x, y]$ by $xy = yx \cdot [x, y]$. The nucleus $\text{Nuc}(M)$ of a Moufang loop $M$ is the set $\{a \in M \mid a \cdot xy = ax \cdot y \ \forall x, y \in M\}$. For basic properties of Moufang loops, see [1].

To arbitrary elements $x, y$ of a Moufang loop $M$, there are associated bijections $L_x, R_x, T_x, L_{x,y}, R_{x,y}$ of $M$ defined as follows:

$$yL_x = xy, \quad yR_x = yx, \quad \text{for all } y \in M;$$

$$T_x = L_x^{-1}R_x, \quad L_{x,y} = L_xL_yL_{yx}^{-1}, \quad R_{x,y} = R_xR_yR_{xy}^{-1}. \quad (1)$$

The multiplication group $\text{Mlt}(M)$ of $M$ is the group of permutations of $M$ generated by $L_x$ and $R_x$ for all $x \in M$, and the inner mapping group $\mathcal{I}(M)$ is the subgroup of $\text{Mlt}(M)$ generated by $T_x$ and $R_{x,y}$ for all $x, y \in M$.

A pseudoautomorphism of a Moufang loop $M$ is a bijection $A : M \to M$ with the property that there exists an element $a \in M$ such that

$$xA(yA \cdot a) = (x \cdot y)A \cdot a \quad \text{for all } x, y \in M.$$  

Such an element $a$ is called a right companion of $A$. Denote by $\text{PsAut}(M)$ the group formed by all pairs $(A, a)$, where $A$ is a pseudoautomorphism of $M$ with right companion $a$, with respect to the operation $(A, a)(B, b) = (AB, aB \cdot b)$. Denote by $\text{PsInn}(M)$ the subgroup of $\text{PsAut}(M)$ generated by the elements $(T_x, x^{-3})$ and $(R_{x,y}, [x, y])$ for all $x, y \in M$ (such elements are in $\text{PsAut}(M)$ by Lemma VII.2.2 in [1]).

By [13], the only finite simple nonassociative Moufang loops are the Paige loops $M(q)$ which exist for every finite field $F_q$. The order of $M(q)$ is $\frac{1}{2}q^3(q^4 - 1)$, where $d = (2, q - 1)$, and is the product of two coprime numbers $q^3(q^2 - 1)$ and $\frac{1}{d}(q^2 + 1)$.

Let $M$ be a Moufang loop and let $p$ be a prime. $M$ is a $p$-loop if the order of every element of $M$ is a power of $p$ (for Moufang loops, this is equivalent to the condition that $|M|$ be a power of $p$). A $p$-Sylow subloop of $M$ is a subloop of order $p^k$, where $p^k \parallel |M|$, $k \geq 0$. We denote by $\text{Syl}_p(M)$ the
set of all $p$-Sylow subloops of $M$. The fact that $Syl_p(M)$ can be empty for $p$ dividing $|M|$ was observed long ago. For example, the simple Paige loop $M(2)$ of order 120 does not have elements of order 5. The classification [9] of maximal subloops of $M(q)$ implies the following assertion:

**Lemma 1** If $p \nmid \frac{1}{d}(q^2 + 1)$ then $Syl_p(M(q)) \neq \emptyset$. If $p \mid \frac{1}{d}(q^2 + 1)$ then $M(q)$ does not have elements of order $p$; in particular, $Syl_p(M(q)) = \emptyset$ in this case.

**Proof.** First, suppose that $q$ is a power of $p$. Consider a maximal subloop of $M(q)$ of shape $q^2 : PSL_2(q)$ (i.e. a split extension of a normal elementary abelian subgroup order $q^2$ by the simple group $PSL_2(q)$). This subloop obviously contains a subloop of order $q^3$ which is therefore $p$-Sylow in $M(q)$.

If $p \mid q^2 - 1$ then consider a maximal subloop of type $M(PSL_2(q), 2)$ (i.e. a loop with a normal subgroup $PSL_2(q)$ of index 2 constructed by the Chein duplication process as in Theorem 1 of [2]). Then obviously $Syl_p(PSL_2(q)) \subseteq Syl_p(M(q))$ whenever $p$ is odd, and $M(S, 2) \in Syl_2(M(q))$ for every $S \in Syl_2(PSL_2(q))$.

If $p \mid \frac{1}{d}(q^2 + 1)$ then it can be easily seen by induction that every maximal subloop of $M(q)$ either has order coprime with $p$ or contains no elements of order $p$. ▲

Note that we will give another proof (see Corollary 2 below) of the existence of a $p$-Sylow subloop in $M(q)$ which does not use the classification [9]. However, the explicit structure of the Sylow subloops of $M(q)$ is best seen from the proof of Lemma 1 above.

Lemma 1 also shows that there is an obstruction to the existence of a $p$-Sylow subloop in an arbitrary finite Moufang loop $M$ having a composition factor $M(q)$ with $\frac{1}{d}(q^2 + 1)$ divisible by $p$.

**Definition.** Let $M$ be a Moufang loop. A prime $p$ is called a Sylow prime for $M$ if, for every composition factor of $M$ that is isomorphic to $M(q)$ for some $q$, we have $p \nmid \frac{q^2 + 1}{(2q-1)}$.

Obviously, $p$ is a Sylow prime for $M$ if and only if it is such for all composition factors of $M$. We can now state the main theorem.

**Theorem 1 (Sylow’s theorem)** Let $M$ be a finite Moufang loop and let $p$ be a prime. Then $M$ contains a $p$-Sylow subloop if and only if $p$ is a Sylow prime for $M$. 
Before proving this theorem, we will require some facts about groups with triality which are introduced in the next section. As an important corollary to Sylow’s theorem, we obtain the following assertion:

**Corollary 1**  
(i) Every Moufang loop has a 2-Sylow and a 3-Sylow subloop.  
(ii) If all composition factors of a Moufang loop $M$ are groups then $M$ has a $p$-Sylow subloop for all primes $p$.

**Proof.**  
(i) The primes 2 and 3 are Sylow for every loop, since $\frac{q^2 + 1}{(2, q-1)}$ is coprime with 6 for all prime powers $q$.  
(ii) If $M$ is as stated then all primes are Sylow for $M$ by definition. ▲

### 3 Groups with triality

A group $G$ possessing automorphisms $\rho$ and $\sigma$ that satisfy $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ is called a *group with triality* $\langle \rho, \sigma \rangle$ if

$$[x, \sigma][x, \sigma]^\rho[x, \sigma]^\rho^2 = 1$$

for every $x$ in $G$, where $[x, \sigma] = x^{-1}x^\sigma$. We henceforth denote $S = \langle \sigma, \rho \rangle$. Obviously, $S$ is a homomorphic image of the symmetric group $S_3$ of degree 3. (Strictly speaking, we have fixed a homomorphism $\gamma : S_3 \rightarrow Aut(G)$ and then identified the generators $\rho$ and $\sigma$ of $S_3$ with their images under $\gamma$ to simplify the notation. We thus implicitly consider $G$ as a *group with operators* $S_3$ in the sense of §15 of [12].) It should be noted that the identity (2) does not depend on a particular choice of the generators $\rho$ and $\sigma$ [4].

Let $G$ be a group with triality $S$. Put $M = \{[x, \sigma] \mid x \in G\}$ and $H = C_G(\sigma)$. Then $M$ endowed with the multiplication

$$m.n = m^{-\rho}nm^{-\rho^2} \text{ for all } m, n \in M$$

becomes a Moufang loop $(M, \cdot)$ of order $|G : H|$. We denote this loop by $\mathcal{M}(G)$. Every Moufang loop can be obtained in this way from a suitable group with triality. Moreover, for every subloop $M_0 \leq \mathcal{M}(G)$, there exists an $S$-invariant subgroup $G_0$ of $G$ (in brief, $S$-*subgroup*) such that $M_0 = \mathcal{M}(G_0)$. Any element of $\mathcal{M}(G)$ has the same order whether viewed as a group or loop element. For more details on this, see [8, 10]. We observe that

$$m^\sigma = m^{-1} \in M \text{ for all } m \in M.$$
A homomorphism \( \varphi : G_1 \to G_2 \) of groups \( G_1 \) and \( G_2 \) with triality \( S \) is called an \( S \)-homomorphism if \( \alpha \varphi = \varphi \alpha \) for all \( \alpha \in S \). (Again, strictly speaking, we have fixed homomorphisms \( \gamma_i : S_3 \to Aut(G_i) \), \( i = 1, 2 \), and then required \( (\alpha \gamma_1) \varphi = \varphi (\alpha \gamma_2) \) for all \( \alpha \in S_3 \) thus making \( \varphi \) an operator homomorphism from \( G_1 \) to \( G_2 \). This is clearly a morphism in the category of groups with triality.) Denote by \( Z_S(G) \) the \( S \)-center of \( G \), which is by definition the maximal normal \( S \)-subgroup of \( G \) on which \( S \) acts trivially.

**Lemma 2** Let \( G \) be a group with triality \( S = \langle \sigma, \rho \rangle \) and let \( M = M(G) \). Then

(i) \( [[G, S], S] = [G, S] \),
(ii) \( Z_S(G/Z_S(G)) = 1 \) and \( Z_S(G) = C_G([G, S]S) \),
(iii) \( [G, S] \) is generated by \( M \cup M^\rho \),
(iv) the elements \( m, m^\rho, m^{\rho^2} \) of \( G \) pairwise commute for all \( m \in M \),
(v) \( m^{-\rho}nm^{-\rho^2} = n^{-\rho^2}mn^{-\rho} \) for all \( m, n \in M \).

**Proof.** See Lemmas 1 and 2 in [10]. ▲

**Lemma 3** Let \( G \) be a group with triality \( S = \langle \sigma, \rho \rangle \) and let \( M = M(G) \). Then the semidirect product \( G_0 = G \rtimes \langle \rho \rangle \) is a group with triality \( S \) if and only if \( M \) has exponent 3.

**Proof.** For all \( g \in G \), we have \((g\rho)^{-1}(g\rho)^\sigma = \rho^2g^{-1}g^\sigma \rho^2 \) and \((g\rho^2)^{-1}(g\rho^2)^\sigma = \rho g^{-1}g^\sigma \rho \). Put \( m = g^{-1}g^\sigma \). Then

\[
(\rho m\rho)(\rho m\rho)^\rho(\rho m\rho)^{\rho^2} = m^{\rho^2}m^\rho m = 1,
\]

\[
(\rho^2m\rho^2)(\rho^2m\rho^2)^\rho(\rho^2m\rho^2)^{\rho^2} = (m^\rho)^3.
\]

Hence, \( G_0 \) is a group with triality iff \( m^3 = 1 \) for all \( m \in M(G) \). ▲

Note that if \( M(G) \) has exponent 3 then \( G \rtimes S \) is also a group with triality \( S \) (where \( S \) acts by inner automorphisms). However, in this case \( M(GS) = M(G, \rho) \).

Given a Moufang loop \( M \), there exists a universal group with triality \( D(M) \) introduced by Doro [4] which satisfies \( M(D(M)) \cong M \), \( [D(M), S] = D(M) \) and, if \( G \) is any group with triality such that \( M(G) \cong M \) and \( G = [G, S] \), then there is an \( S \)-epimorphism \( \tau : D(M) \to G \). Denote \( E(M) \cong D(M)/Z_S(D(M)) \). Then \( M(E(M)) \cong M \).

A group \( G \) (with triality) is called \( S \)-simple if it has no proper \( S \)-homomorphic images or, equivalently, contains no normal \( S \)-subgroups.
Lemma 4 Every finite $S$-simple group is $S$-isomorphic to one of the following $S$-simple groups:

(i) A finite simple group $G$ with trivial $S$-action. In this case, $M(G)$ is the trivial loop;

(ii) $G = \langle a \mid a^3 = 1 \rangle \cong \mathbb{Z}_3$, $a^\rho = a$, $a^\sigma = a^{-1}$. In this case, $M(G) \cong \mathbb{Z}_3$;

(iii) $G = \langle a, b \mid a^p = b^3 = [a, b] = 1 \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$, $p \neq 3$ is a prime, $a^\rho = b$, $b^\rho = a^{-1}b^{-1}$, $a^\sigma = b$, $b^\sigma = a$. In this case, $M(G) \cong \mathbb{Z}_p$;

(iv) $G = V_1 \times V_2 \times V_3$, $\alpha_i : V \to V_i$, $i = 1, 2, 3$, are isomorphisms, $V$ is a finite nonabelian simple group, $(v_1, v_2, v_3)^\sigma = (v_2, v_1, v_3)$, $(v_1, v_2, v_3)^\rho = (v_3, v_1, v_2)$. In this case, $M(G) \cong V$;

(v) $G \cong P\Omega^+_8(q)$, $S$ is the group of graph automorphisms of $G$. In this case, $M(G) \cong M(q)$ is the simple Paige loop.

Proof. See [4, 14]. ▲

Let $F$ be a field. An $FS$-module $V$ is called a triality module if $V$ is a group with triality $S$. The representations $\varphi_i^{(\chi)}$ of $S$ corresponding to the indecomposable $FS$-modules $V_i^{(\chi)}$ are shown in Table 1. They depend on whether the characteristic $\chi$ of $F$ is 2, 3, or otherwise. We may assume $F$ to be a prime field, since the decomposition field of $S$ is prime in any characteristic [3]. The fact whether a module is a triality module is indicated by ‘✓’ in the last column.

Lemma 5 Table 1 holds.

Proof. The indecomposable $FS$-modules are well-known and can be readily determined (for example, using §64 in [3]). Namely, if $\chi \neq 2, 3$ then every indecomposable $FS$-module is irreducible by Maschke’s theorem. If $\chi = 3$ then there are exactly 6 indecomposable $FS$-modules by Theorem (64.6) of [3] and the ones shown in Table 1 are easily seen to be indecomposable and pairwise nonisomorphic. If $\chi = 2$ then by the same theorem there are two non-faithful indecomposable modules: the trivial one and the reducible (projective) one. The irreducible 2-dimensional module is projective and is the only indecomposable faithful $FS$-module in characteristic 2, which follows from the fact that this module is the only faithful component of the induced modules of the 2-Sylow subgroup of $S$ (Theorem (63.8) of [3]).

The triality of a module $V$ is equivalent to the condition that the element $(\sigma - 1)(1 + \rho + \rho^2)$ of $FS$ annihilates $V$, which is directly verified in each case. ▲
Table 1: Indecomposable $S_3$-modules

| $\chi$ | $V$  | dim $V$ | $\varphi$ | $(12)\varphi$ | $(123)\varphi$ | Triality |
|--------|------|---------|-----------|----------------|----------------|-----------|
| $\neq 2, 3$ | $V^{(0)}_1$ | 1 | $\varphi^{(0)}_1$ | 1 | 1 | ✓ |
|          | $V^{(0)}_2$ | 1 | $\varphi^{(0)}_2$ | -1 | 1 | — |
|          | $V^{(0)}_3$ | 2 | $\varphi^{(0)}_3$ | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ | ✓ |
| 2       | $V^{(2)}_1$ | 1 | $\varphi^{(2)}_1$ | 1 | 1 | ✓ |
|          | $V^{(2)}_2$ | 2 | $\varphi^{(2)}_2$ | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ | ✓ |
|          | $V^{(2)}_3$ | 2 | $\varphi^{(2)}_3$ | $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | — |
| 3       | $V^{(3)}_1$ | 1 | $\varphi^{(3)}_1$ | 1 | 1 | ✓ |
|          | $V^{(3)}_2$ | 1 | $\varphi^{(3)}_2$ | -1 | 1 | ✓ |
|          | $V^{(3)}_3$ | 2 | $\varphi^{(3)}_3$ | $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | ✓ |
|          | $V^{(3)}_4$ | 2 | $\varphi^{(3)}_4$ | $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | ✓ |
|          | $V^{(3)}_5$ | 3 | $\varphi^{(3)}_5$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ | ✓ |
|          | $V^{(3)}_6$ | 3 | $\varphi^{(3)}_6$ | $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ | — |

**Lemma 6** Let $G$ be an $S$-simple group with triality. Let $p$ be a Sylow prime for $M(G)$. Then $G$ has a $p$-Sylow $S$-subgroup.

**Proof.** We analyze the cases (i)–(v) of Lemma 4. If $G$ is as in cases (i)–(iii), the claim readily follows. Let case (iv) hold. Then, for any $P \in Syl_p(V)$, the group $P_1 \times P_2 \times P_3$ is the required $p$-Sylow $S$-subgroup of $G$, where $P_i =$
\( \alpha_i(P), \ i = 1, 2, 3. \) Suppose that \( G \cong PO^+_3(q) \) as in case (v) and \( S \) is the group of graph automorphisms of \( G. \) We will use the structure of some \( S \)-subgroups of \( G \) (for details, see [11]). We have \( |G| = \frac{1}{d}q^{12}(q^6 - 1)(q^4 - 1)^2(q^2 - 1) = n_1n_2n_3, \) where the integers

\[
\begin{align*}
n_1 &= \frac{3}{(3,q)}q^{12}(q^2 - 1)^4, \\
n_2 &= \frac{(3,q)(q^2+q+1)(q^2-q+1)}{3}, \\
n_3 &= \left( \frac{q^2+1}{d} \right)^2
\end{align*}
\]

are pairwise coprime. By hypothesis, \( p|n_1n_2. \) If \( p|n_2 \) then \( Syl_p(C_G(S)) \subseteq Syl_p(G), \) since \( C_G(S) \cong G_2(q) \) and \( n_2 \) divides \( |G_2(q)| = q^6(q^6 - 1)(q^2 - 1). \) Hence, any subgroup in \( Syl_p(C_G(S)) \) is the required one.

Therefore, we may assume that \( p|n_1. \) If \( p|q \) then consider an \( S \)-invariant parabolic subgroup \( R_{s_2} \) of \( G \) (in the notation of [11]) of order \( \frac{1}{d}q^{12}(q-1)^4(q + 1)^3. \) It has the following \( S \)-invariant structure \( R_{s_2} = q^9 \times (SL_2(q) \circ SL_2(q) \circ SL_2(q)), q - 1 \) with \( S \) naturally permuting the three factors \( SL_2(q), \) where \( \circ \) denotes the central product. The group \( SL_2(q) \circ SL_2(q) \circ SL_2(q) \) has an obvious \( p \)-Sylow \( S \)-subgroup whose preimage in \( R_{s_2} \) is the required subgroup.

If \( p \nmid q \) then consider an \( S \)-subgroup \( I_{+4} \) of order \( \frac{1}{d}q^4(q^2 - 1)^4. \) It has the structure \( (SL_2(q) \circ SL_2(q) \circ SL_2(q)) \circ K, \) where \( K = \mathbb{Z}_2 \times \mathbb{Z}_2 \) and \( K \times S \cong S_4 \) naturally permutes the four factors \( SL_2(q). \) It is easy to see that this group contains a \( p \)-Sylow \( S \)-subgroup.

Finally, if \( p \nmid q \) and \( p = 3 \) then let \( q \equiv \varepsilon(3), \ \varepsilon = \pm 1. \) The required \( 3 \)-Sylow subgroup is inside an \( S \)-subgroup \( I_{s_2} \) of order \( \frac{192}{d^2}(q - \varepsilon)^4. \) To see this, consider an \( \varepsilon \)-2-decomposition of the Cayley algebra \( \Omega(q) = V_1 \oplus \ldots \oplus V_4 \) which is also a \( \mathbb{Z}_2 \times \mathbb{Z}_2 \)-grading with \( 1 \in V_1 \) (see Section 4 in [9]). Let \( R \) be the centralizer of this decomposition in \( \Omega_+(q) \) extended by the 4-group \( ((12)(34), (13)(24)) \) of permutations of the subspaces \( \{V_i\}, \ i = 1, \ldots, 4. \) This group has the following structure \( R = (\mathbb{Z}_2(q-1))^4.d^2.2^3.2^2. \) In particular, the \( 3 \)-Sylow subgroup of \( R \) is characteristic. Take the group \( T = \langle (23), (34) \rangle \cong S_3 \) of permutations of \( \{V_i\}, \ i = 2, 3, 4 \) which acts identically on \( V_1 \) and induces automorphisms of \( \Omega(q). \) Then the group \( I_{s_2} = R \times T \) is the image in \( PO_3^+(q) \) of \( R \times T \subseteq \Omega_3^+(q). \) It is \( S \)-invariant with \( S \) centralizing \( T \) (because \( T \) is a group of automorphisms of \( \Omega(q) \)). It is now clear that the \( 3 \)-Sylow subgroup \( O_3(R) \times \langle (2,3,4) \rangle \) of \( I_{s_2} \) is \( S \)-invariant. \( \blacklozenge \)

**Lemma 7** Let \( G \) be a group with triality \( S = \langle \rho, \sigma \rangle \) and let \( \mathcal{M}(G) = \{[g, \sigma] | g \in G \} = (M, .) \) be the corresponding Moufang loop. Then, for every subloop
\(P \leq \mathcal{M}(G),\) the group \(Q = \langle P \cup P^\rho \rangle\) is an \(S\)-subgroup of \(G\) such that \(\mathcal{M}(Q) = P\) and \([Q, S] = Q\).

Proof. By Theorem 1 in [8], \(Q\) is an \(S\)-subgroup and \(\mathcal{M}(Q) = P\). By Lemma 2, \([Q, S]\) is the \(S\)-subgroup of \(G\) generated by \(P\). Hence, we have \(Q \subseteq [Q, S]\). ▲

Lemma 8 Let \(M\) be a finite Moufang \(p\)-loop. Then

(i) \(PsInn(M)\) is a \(p\)-group;

(ii) Any group with triality \(G\) such that \(\mathcal{M}(G) \cong M\) and \([G, S] = G\) is a \(p\)-group.

Proof. (i) The kernel of the natural epimorphism \(\lambda : PsInn(M) \to \mathcal{I}(M)\) which acts by \(\lambda : (A, a) \mapsto A\) is a subgroup of \(\text{Nuc}(M)\) hence is a \(p\)-group. The group \(\mathcal{I}(M)\) is a subgroup of \(\text{Mlt}(M)\) which is a \(p\)-group by Lemma VI.2.2 in [1] and Theorem 4 in [5].

(ii) Let \(G\) be as stated. Then \(G\) is finite, since it is a quotient of the finite group \(\mathcal{D}(M)\) (see Corollary 3 in [4]). We have \(G/Z_S(G) \cong \mathcal{E}(M)\) and \(|\mathcal{E}(M)| = |PsInn(M)| \cdot |M|\) (see [10]) is a power of \(p\) by (i). Hence, it remains to prove that \(K = Z_S(G)\) is a \(p\)-group. Let \(P \in Syl_p(G)\). We have \(G = O_{p'}(K) \times P\), since \(K\) is a central subgroup of \(G\). The condition \([G, S] = G\) now implies \(O_{p'}(K) = 1\). ▲

In the following lemma, for an integer \(n\) and a prime \(p\), we denote by \(n_p\) the maximal power of \(p\) dividing \(n\).

Lemma 9 Let \(G\) be a group with triality \(S = \langle \rho, \sigma \rangle\), let \(M = \mathcal{M}(G)\), and let \(p\) be a prime.

(i) If \(N \leq G\) is an \(S\)-subgroup containing a \(p\)-Sylow subgroup of \(G\) then \(|\mathcal{M}(N)|_p = |M|_p\).

(ii) If \(P \in Syl_p(G)\) is \(S\)-invariant then \(\mathcal{M}(P) \in Syl_p(M)\).

Proof. (i) Let \(H = C_G(\sigma)\). We have \(|\mathcal{M}(N)| = |N|/|N \cap H|\), and \(|M| = |G|/|H|\). By Lagrange’s theorem [8], \(|M|/|\mathcal{M}(N)| = |G|/|NH|\) is an integer. However, \(|G|_p = |N|_p\) divides \(|N|\) which, in turn, divides \(|NH|\). Hence \(|M : \mathcal{M}(N)|\) is coprime with \(p\).

(ii) Since \(\mathcal{M}(P)\) is a \(p\)-loop and \(|M : \mathcal{M}(P)|\) is coprime with \(p\) by (i), it follows that \(\mathcal{M}(P) \in Syl_p(M)\). ▲

As a consequence, we have an alternative proof independent of the classification [9] of the following assertion (cf. Lemma 1 above):
Corollary 2 If $p$ is a Sylow prime for $M(q)$ then $\text{Syl}_p(M(q))$ is nonempty.

Proof. We have $M(q) = M(G)$, where $G = P\Omega^+_8(q)$ is $S$-simple. By Lemma 6, $G$ contains a $p$-Sylow $S$-subgroup. The claim follows by (ii) of Lemma 9. ▲

Lemma 10 Let $G = VP$ be a group with triality $S$ such that $P$ is a $p$-group, $V \triangleleft G$, $p \nmid |V|$. Suppose that $M(V)$ is generated by at most 2 elements, where $\overline{P} = G/P$ satisfies $[\overline{P}, S] = \overline{P}$. Then $G$ has a $p$-Sylow $S$-subgroup.

Proof. Denote $M = M(G)$. Let $\{m_i\}_{i \in I}$ generate $M$ modulo $W = M(V)$. By hypothesis, we may assume $|I| \leq 2$. In particular, $N = \langle \{m_i\}_{i \in I} \rangle$ is a group (since Moufang loops are diassociative) and $M = WN$. Hence, any $R \in \text{Syl}_p(N)$ is in $\text{Syl}_p(M)$. By Lemma 7, $Q = \langle R \cup R^p \rangle$ is an $S$-subgroup of $G$ such that $M(Q) = R$ and $[Q, S] = Q$. Hence $QV/V = \overline{P}$ in view of $[\overline{P}, S] = \overline{P}$. By Lemma 8, $Q$ is the required $p$-Sylow $S$-subgroup. ▲

4 Proof of the theorem

We are going to prove the following extended form of Theorem 1:

Theorem 2 Let $M$ be a finite Moufang loop and let $p$ be a prime. Let $G$ be a group with triality such that $M(G) = M$. Then the following conditions are equivalent:

(i) $M$ has a $p$-Sylow subloop,

(ii) $p$ is a Sylow prime for $M$,

(iii) $G$ has an $S$-invariant $p$-subgroup $Q$ such that $M(Q) \in \text{Syl}_p(M)$.

Proof. Let $k \geq 0$ be such that $p^k || |M|$.

(i) $\Rightarrow$ (ii). Suppose that $M$ possesses a $p$-Sylow subloop $P$. We prove by induction on the length of a composition series of $M$ that $p$ is a Sylow prime for $M$. If $M$ is simple, this follows from Lemma 1. Let $N$ be a proper normal subloop of $M$. It suffices to show that $p$ is a Sylow prime for both $N$ and $\overline{M} = M/N$. Note that $P \cap N$ is a $p$-subloop of $N$ and $\overline{P} = \langle P, N \rangle/N$ is a $p$-subloop of $\overline{M}$ by

$$\frac{\langle P, N \rangle}{N} \cong \frac{P}{P \cap N}.$$  \hfill (5)

11
such that $M_N/P$. In both cases we can use induction for $a$.

It is sufficient to show that $Z$ then the condition (see Theorem IV.1.5 in [1]). By Lagrange’s theorem [8], $|P|$ divides $|\langle P, N \rangle|$ which in turn divides $|M|$. Hence (5) also implies that the integers

$$\frac{|N|}{|P \cap N|} = \frac{|\langle P, N \rangle|}{|P|}, \quad \frac{|M|}{|\bar{P}|} = \frac{|M|}{|\langle P, N \rangle|}$$

are coprime with $p$. It follows that $P \cap N \in Syl_p(N)$ and $\bar{P} \in Syl_p(M)$. By induction, $p$ is a Sylow prime for both $N$ and $\bar{M}$.

(ii) $\Rightarrow$ (iii). We now suppose that $p$ is a Sylow prime for $M = M(G)$. Proceed by induction on $|M|$.

If $Z_S(G) \neq 1$ then consider $G_0 = G/Z_S(G)$. This group satisfies $Z_S(G_0) = 1$ and $M(G_0) = M$. If we show that $P_0$ is an $S$-invariant $p$-subgroup of $G_0$ such that $M(P_0) \in Syl_p(M)$ then the preimage $P$ of $P_0$ in $G$ also satisfies $M(P) \in Syl_p(M)$. If $P$ is not a $p$-group then we take $[P, S]$ which is a $p$-group by (ii) of Lemma 8 and $M([P, S]) = M(P)$.

Hence, we may assume that $Z_S(G) = 1$. Clearly, we may also assume that $[G, S] = G$. Take a minimal normal $S$-subgroup $V$ of $G$. Then $V$ is characteristically simple (see Theorem 1.5 in Chap. 2 of [6]). Two cases are possible:

(1) $p \mid |V|$. Then we may assume that $V$ is nonabelian (otherwise $V$ is a $p$-group and we apply induction for $G/V$, which is possible, since $p$ is a Sylow prime for $M(G/V)$ and $|M(G/V)| < |M|$). We have $V = V_1 \times \ldots \times V_s$ is the product of isomorphic nonabelian simple groups $V_i$’s. Since $p$ is Sylow for $M(V)$ and $V$ is a direct product of $S$-simple groups, it follows by Lemma 6 that $V$ has a $p$-Sylow $S$-subgroup $W$.

By assumption $W \neq 1$. We have $G = VN$, where $N = N_G(W)$ is $S$-invariant. Observe that $N$ contains a $p$-Sylow subgroup of $G$. Moreover $N < G$, since $W \not\trianglelefteq V$; and $M(N) < M$, since $[G, S] = G$. Also note that $p$ is Sylow for $M(N)$, since $W \trianglelefteq N \cap V \trianglelefteq N$ is an $S$-invariant series for $N$ and $W$ is a $p$-group, $(N \cap V)/W$ is a $p'$-group, and $N/(N \cap V) \cong G/V$. By induction, there exists a $p$-subgroup $P$ in $N$ such that $M(P) \in Syl_p(M(N))$. By (i) of Lemma 9, $M(P) \in Syl_p(M)$.

(2) $p \nmid |V|$. By induction, we may assume that $\bar{P} = G/V$ is a $p$-group. It is sufficient to show that $G$ has a nontrivial $S$-invariant $p$-subgroup $P_0$ such that $\bar{P}_0 = P_0V/V$ is normal in $\bar{P}$. Indeed, if such a subgroup exists then the condition $Z_S(G) = 1$ implies that either $M(P_0) \neq 1$ or $P_0 \not\trianglelefteq G$.

In both cases we can use induction for $N/P_0$, where $N = N_G(P_0)$. This is because $|M(N/P_0)| < |M|$ and $p$ is Sylow for $M(N/P_0)$, since $N/P_0$ is an.
extension of the $p'$-group $C_V(P_0)$ by the $p$-group $\overline{P}/P_0$. By induction, $N/P_0$ contains an $S$-invariant $p$-subgroup $\overline{P}_1$ such that $M(\overline{P}_1) \in Syl_p(M(N/P_0))$. Then the full preimage $P_1$ of $\overline{P}_1$ in $N$ in the required $S$-subgroup, since $M(U_1) \in Syl_p(M(N)) \subseteq Syl_p(M)$.

Let $\mathcal{Z} = Z(\overline{P})$ and suppose that $M(\mathcal{Z}) \neq 1$. The existence of $P_0$ is this case is easy. Take $z \in M(G)$ such that $1 \neq z \in M(\mathcal{Z})$, where $\mathcal{Z} = Vz$. The group $G_0 = \langle V, z, z^p \rangle$ satisfies the conditions of Lemma 10. We take $P_0$ to be a $p$-Sylow $S$-subgroup of $G_0$. Then $\overline{P}_0 \trianglelefteq \overline{P}$ as a central subgroup of $\overline{P}$.

Suppose that $M(\mathcal{Z}) = 1$. Then $M(\overline{P}_1) \neq 1$, where $\overline{P}_1/\mathcal{Z} = Z(\overline{P}/\mathcal{Z})$, since otherwise we would have $\overline{Z}_1 \leq Z_S(\overline{P}) \leq \mathcal{Z}$ (the latter inclusion follows from $[\overline{P}, S] = \overline{P}$ and (ii) of Lemma 2). Take $a \in M(G)$ such that $1 \neq a \in M(\overline{P}_1)$ and put $A = \langle a, a^p \rangle$. Then $A$ is an $S$-subgroup of $G$ not contained in $\mathcal{Z}$, where $\mathcal{Z}$ is the full preimage of $\mathcal{Z}$ in $G$.

The elementary abelian group $\overline{P}/\Phi(\overline{P})$ is the direct product $U_1 \times \ldots \times U_t$ of indecomposable triality $F_pS$-modules $U_i$'s. The condition $[\overline{P}, S] = \overline{P}$ implies that the $U_i$'s are at most 2-dimensional and, depending on $p$, are isomorphic to one of the modules $V_3(0), V_2(2), V_2(3), V_4(3)$ from Table 1. Moreover, we have $M(U_i) = \langle u_i \rangle$ is cyclic of order $p$ and $U_i = \langle u_i, u_i^p \rangle$ (observe that $u_i^p = u_i$ if $U_i \cong V_2(3)$). Let $w_i$ be corresponding preimages of $u_i$ in $M(G)$. Then $G$ is generated modulo $V$ by the $S$-subgroups $W_i = \langle w_i, w_i^p \rangle$. Since $Z_1 \geq A \nsubseteq \mathcal{Z}$, where $Z_1$ is the full preimage of $\mathcal{Z}_1$ in $G$, it follows that there exists $i_0$ such that $W = [A, W_{i_0}] \nsubseteq V$. On the other hand, $W \subseteq Z$, since $A \subseteq Z_1$. Denote $G_0 = \langle V, A, W_{i_0} \rangle$ and $\overline{G}_0 = G_0/V$. Then the $S$-subgroup $\overline{G}_0$ satisfies the conditions of Lemma 10, since the images of $a$ and $w_{i_0}$ in $\overline{G}_0$ generate $M(\overline{G}_0)$ as a loop and $\overline{G}_0$ as an $S$-group (whence the condition $[\overline{G}_0, S] = \overline{G}_0$). Let $P_1$ be a $p$-Sylow $S$-subgroup of $\overline{G}_0$. Put $P_0 = P_1 \cap Z$. It remains to observe that $P_0 \neq 1$, since $P_0 \cap WV = P_1 \cap WV \neq 1$ in view of $W \nsubseteq V$.

(iii) $\Rightarrow$ (i). Obvious. ▲

We note that it is not true in general that if $G$ is a group with triality and $p$ is Sylow for $M(G)$ then $G$ contains a $p$-Sylow $S$-subgroup. For example, let $G = S$ on which $S$ acts by inner automorphisms. Then 2 is a Sylow prime for $M(G) \cong \mathbb{Z}_3$, but $G$ does not have a 2-Sylow $S$-subgroup.

5 The group-type radical of Moufang loops

A finite Moufang loop $M$ is said to be a loop of group type if all composition factors of $M$ are groups. For example, all solvable Moufang loops are loops
of group type. It is clear that the normal subloop of $M$ generated by two normal subloops of group type is again a loop of group type. Hence we have

**Proposition 1** Every finite Moufang loop has a unique maximal normal subloop of group type.

We denote this maximal normal subloop of group type by $Gr(M)$. It is obvious that $Gr(M/Gr(M)) = 1$, hence we call $Gr(M)$ the group-type radical of $M$.

For $q$ odd, the simple Paige loop $M(q)$ has a two-fold extension isomorphic to the loop $PGL(\mathbb{O}(q))$, where $\mathbb{O}(q)$ is the Cayley algebra over $F_q$ (see Section 4 in [9]). We denote this extension by $M(q).2$. Also define

$$\widehat{M(q)} = \begin{cases} M(q).2, & \text{if } q \text{ is odd} \\ M(q), & \text{if } q \text{ is even} \end{cases}$$

It can be seen that the group $\text{InnDiag}(P\mathbb{O}_8^+(q))$ of inner-diagonal automorphisms of $P\mathbb{O}_8^+(q)$ is a group with triality $S$ corresponding to $\widehat{M(q)}$, where $S$ is the group of graph automorphisms of $P\mathbb{O}_8^+(q)$. It is known that the factor group

$$\text{InnDiag}(P\mathbb{O}_8^+(q))/P\mathbb{O}_8^+(q)$$

is trivial for $q$ even and isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ for $q$ odd. Moreover, in the latter case, $S$ acts nontrivially on $\mathbb{Z}_2 \times \mathbb{Z}_2$ so that $\mathbb{M}(\mathbb{Z}_2 \times \mathbb{Z}_2) = \mathbb{Z}_2$, whence $|\widehat{M(q)}| = 2|M(q)|$.

The following assertion is the main result of this section (cf. Theorem B in the introduction):

**Theorem 3** Let $M$ be a finite Moufang loop and let $N$ be a minimal normal subloop of $M$. Then we have

(i) $N$ is the direct product of isomorphic simple loops. Furthermore, if $N$ is nonassociative then it is simple.

(ii) Suppose, additionally, that $M$ satisfies $Gr(M) = 1$. Then by (i) every minimal normal subloop of $M$ is a simple Paige loop $M(q)$ for some $q$. Denote $\text{Soc}(M) = \prod M(q)$ and $\widehat{\text{Soc}}(M) = \prod \widehat{M(q)}$, where both products are taken over all minimal normal subloops of $M$. Then

$$\text{Soc}(M) \trianglelefteq M \trianglelefteq \widehat{\text{Soc}}(M).$$

In particular, $M/\text{Soc}(M)$ is an elementary abelian 2-group.
Proof. Suppose that \( M \) and \( N \) are as stated.

(i) Let \( G \) be a group with triality \( S = \langle \rho, \sigma \rangle \) such that \( M(G) = M = \{ x^{-1}x^\sigma \mid x \in G \} \), \( [G, S] = G \), and let \( Q_0 \) be a minimal normal \( S \)-subgroup of \( G \) corresponding to \( N \). Since \( Q_0 \) is characteristically simple, we have \( Q_0 = Q_1 \times \ldots \times Q_n \), where \( Q_i, 1 \leq i \leq n \), are isomorphic simple groups. Note that we also have the decomposition \( Q_0 = R_1 \times \ldots \times R_k \), where \( R_j, 1 \leq j \leq k \), are \( S \)-simple groups if \( Q_0 \) is nonabelian or indecomposable \( S \)-modules if \( Q_0 \) is abelian; moreover, \( N = M(Q_0) = M(R_1) \times \ldots \times M(R_k) \).

If \( Q_1 \neq P\Omega^+_8(q) \) for any \( q \) then Lemmas 5 and 4 imply that all \( M(R_j)'s \) are either trivial or isomorphic simple groups. Hence, we may assume that \( Q_1 \equiv P\Omega^+_8(q) \), with \( q = p^m \), \( p \) a prime. We denote \( I = \{ i \mid Q_i^S = Q_i \} \).

If either \( I = \emptyset \) or \( [Q_i, S] = 1 \) for all \( i \in I \) then each \( R_j \) is either an \( S \)-group from item (iv) of Lemma 4 with \( V_t = P\Omega^+_8(q) \), \( t = 1, 2, 3 \), or is isomorphic to \( P\Omega^+_8(q) \) with trivial \( S \)-action. Hence, in this case, \( N = \text{the direct product of several} \ P\Omega^+_8(q)'s \) and the claim holds. Consequently, we may assume that \( 1 \in I \) and \( M(Q_1) = M(q) \neq 1 \). We prove that \( n = 1 \) in this case. Assume the contrary. Denote \( K = N_G(Q_1) \). Observe that \( K \) is \( S \)-invariant. We have \( K \neq G \), since otherwise \( Q_1 \) would be a normal \( S \)-subgroup contrary to the choice of \( Q_0 \). Note that we cannot have the inclusion \( M \subseteq K \), since \( G \) is \( S \)-generated by \( M \) (i.e., \( G = \langle \cup_{x \in S} M^x \rangle \), which follows from \( [G, S] = G \) by (iii) of Lemma 2).

Hence, there exists \( x \in M \setminus K \) such that \( x^l \in K \) for a prime \( l \). Let \( y = x^l \). Then we have

\[
x^\rho = x^{-1}, \quad y^\rho = x^{-1}y^{-1}, \quad y^\sigma = xy, \quad [x, y] = 1 \tag{6}
\]

in view of (4) and (iv) of Lemma 2. Denote \( Q_{(i,j)} = Q_1^{x^iy^j}, i, j \in \mathbb{Z}/l\mathbb{Z}, Q = Q_{(0,0)} = Q_1 \). Suppose that \( x^ay^b \in K \), then by (6) we have \( (x^ay^b)^\sigma = x^{b^{-a}}y^b \in K \) and \( (x^ay^b)^\rho = x^{-b}y^{a-b} \in K \). Hence \( 3a \equiv 3b \equiv 0 \pmod{l} \).

I. \( l > 3 \). Then \( a \equiv b \equiv 0 \pmod{l} \) and all groups \( Q_{(i,j)} \) are different. By (6) we obtain

\[
Q_{(i,j)}^\sigma = Q_{(-i,-j)}, \quad Q_{(i,j)}^\rho = Q_{(-j,-i)} \tag{7}
\]

Since \( Q_0 \) is a group with triality, the orbits of \( S \) on the set \( \{Q_1, \ldots, Q_n\} \) are all of size 1 or 3. Hence by (7) the set

\[
\{(i, j), (j - i, j), (-j, i - j), (i, i - j), (-j, -i), (j - i, -i)\}
\]

has 3 elements or less for all \( i, j \in \mathbb{Z}/l\mathbb{Z} \). However, this is possible only in the case \( l = 2 \).
II. $l = 3$. Since $x^3, y^3 \in K$ we have by (6)

$$(Q^{xy^{-1}}) = Q^{xy} = (Q^3)^{xy^{-1}} = Q^{xy^{-1}},$$
$$(Q^{xy^{-1}})^p = Q^{x^{-2}y^{-1}} = (Q^{x^{-3}})^{xy^{-1}} = Q^{xy^{-1}}.$$

Similarly, we can prove that the set $X = \{Q^x, Q^{xy}, Q^{xy}, Q^{xy^2}, Q^{xy^2} \}$ is an $S$-orbit. Since $|X| > 1$ and $Q$ is a simple group, we have $|X| = 3$. If $Q^x = Q^{xy^2}$, an application of $\rho$ gives $Q^y = Q^{xy}$, which implies $Q^x = Q$ in contradiction with the choice of $x$. The cases $Q^x = Q^{xy}$ or $Q^x = Q^{xy^2}$ are treated similarly. In the other cases: $Q^x = Q^y$, $Q^x = Q^{xy^2}$ we have $|X| = 2$, a contradiction.

III. $l = 2$. Then the subgroup $Q \times Q^x \times Q^y \times Q^{xy}$ is $S$-invariant and

$$(Q^x)^\sigma = Q^x, \quad (Q^y)^\sigma = Q^y, \quad (Q^x)^\rho = Q^y, \quad (Q^y)^\rho = Q^{xy}, \quad (Q^{xy})^\rho = Q^x.$$

Let $a \in Q$. We apply the identity of triality (2) to $g = ax$. We have

$$r = r^{-1} = x^{-1}(a^{-1}a)^{-1} \quad \text{and} \quad r = r^a = x^{-2}(a^{-1}a)^{-1}xy = x^{-2}(a^{-1}a)^{-1}x^{-2}(a^{-1}a)^{-1}x^{-2}y = x^{-2}(a^{-1}a)^{-1}x^{-2}(a^{-1}a)^{-1}x^{-2}y.$$
\[ [G, S] = G \text{ forces } G \text{ to be an } S\text{-subgroup of } \prod_j D_j \rtimes \Gamma_j \leq \text{Aut}(T), \]

where \( D_j = \text{InnDiag}(P\Omega^+_8(q_j)) \) and \( \Gamma_j \) is the group of graph automorphisms of \( P\Omega^+_8(q_j) \). Since the \( j \)th projection \( G \to D_j \rtimes \Gamma_j \) commutes with the action of \( S \), its image \( G_j \) must be a subgroup with triality in \( D_j \rtimes \Gamma_j \). However \( M(G_j) \), containing \( M(q) \) as a subloop, does not have exponent 3. By Lemma 3, we must have \( G_j \leq D_j \). Hence, \( G_j \) is either \( P\Omega^+_8(q_j) \) or \( \text{InnDiag}(P\Omega^+_8(q_j)) \), and \( M(G_j) \) is either \( M(q) \) or \( \hat{M}(q) \), accordingly. ▲

Observe that part III of the proof of item (i) implies, in particular, the following useful fact:

**Proposition 2** Let the symmetric group \( S_4 \) act on the direct product of isomorphic groups \( G = G_1 \times G_2 \times G_3 \times G_4 \) in such a way that \( (G_i)^\tau = G_i^\tau \) for all \( i = 1, \ldots, 4 \) and \( \tau \in S \). Let \( S_4 = S \times N \), where \( S = \langle \sigma = (12), \rho = (123) \rangle \) and \( N = \langle (12)(34), (13)(24) \rangle \). If the semidirect product \( N \rtimes G \) is a group with triality \( S \) then \( G_4 \leq C_G(S) \).

The following lemma will be used in the next section:

**Lemma 11** Let \( M \) and \( N \) be Moufang loops.

(i) If \( \varphi : M \to N \) is a homomorphism then \( \text{Gr}(M)^\varphi \leq \text{Gr}(M^\varphi) \), where the inclusion can be proper;

(ii) If \( \text{Gr}(M) = 1 \) and \( N \trianglelefteq M \) then \( \text{Gr}(N) = 1 \).

**Proof.** The inclusion in (i) readily follows from the definition. If we take \( M = \hat{M}(3) \) and \( N = \mathbb{Z}_2 \) then \( N \) is a homomorphic image of \( M \); however, \( \text{Gr}(M) = 1 \) and \( \text{Gr}(N) = N \). To show (ii), define \( \pi_i \) to be the projection of \( \text{Soc}(M) \) to its \( i \)th direct factor isomorphic to \( \hat{M}(q) \) (see item (ii) of Theorem 3). Then \( \pi_i \) maps \( N \) to a normal subgroup of \( \pi_i(M) \) which is either \( M(q) \) or \( \hat{M}(q) \). In any case, \( \text{Gr}(N^{\pi_i}) = 1 \). By (i), this implies \( \text{Gr}(N)^{\pi_i} = 1 \) for all \( i \) and the claim follows. ▲

### 6 \( p \)-Subloops for non-Sylow primes \( p \)

The main theorem about the existence of \( p \)-Sylow subloops suggests the following natural question: How large can a \( p \)-subloop of a Moufang loop \( M \) be if \( p \) is not a Sylow prime for \( M \)? In this section, we show that it can
be as large as possible. To give a more precise statement, we need another
definition.
Suppose that $M$ is a finite Moufang loop and $M_i$, $1 \leq i \leq l$, are the
composition factors of $M$. Let $p$ be any prime. Take $P_i \in \text{Syl}_p(M_i)$ if $p$
is a Sylow prime for $M_i$ and put $P_i = 1$, otherwise. Then a quasi-$p$-Sylow
subloop of $M$ is a subloop of order $\prod_{1 \leq i \leq l} |P_i|$. By Lemma 1, a quasi-$p$-Sylow
subloop, if exists, must be a maximal $p$-subloop of $M$ and its order must be
the maximal order of all $p$-subloops of $M$. Denote by $Q$-$\text{Syl}_p(M)$ the set
of all quasi-$p$-Sylow subloops of $M$. Clearly, if $p$ is a Sylow prime for
$M_i$ then $Q$-$\text{Syl}_p(M_i) = \text{Syl}_p(M_i)$. Our main result of this section is the following
assertion (cf. Theorem A in the introduction):

**Theorem 4** Let $p$ be a prime and $M$ a finite Moufang loop. Then $M$ con-
tains a quasi-$p$-Sylow subloop.

**Proof.** We may assume that $p$ is non-Sylow for $M$, since otherwise the result
follows from Theorem 2. This implies that $p > 3$. We proceed by induction
on the composition length $l$ of $M$. If $l = 1$ then the claim holds by definition.
Assume that $l > 1$. Let $N$ be a minimal normal subloop of $M$. By induction,
there exists $\overline{P} \in Q$-$\text{Syl}_p(M)$, where $\overline{M} = M/N$. Let $P$ be the full preimage
of $\overline{P}$ in $M$. If $p$ is a Sylow prime for $N$ then it is such for $P$ as well. In
this case, $P$ contains a $p$-Sylow subloop by Theorem 2 which is obviously
quasi-$p$-Sylow for $M$. Hence, we may assume that $p$ is non-Sylow for $N$. But
then $N$ must be nonassociative and, by Theorem 3, $N$ is simple. Note that a
quasi-$p$-Sylow subloop of $P$, if exists, must have order $|\overline{P}|$. Let $R = \text{Gr}(P)$.
Since $p$ is odd, it is easy to conclude by (ii) of Theorem 2 that $P/R \cong N$ and
$|R| = |\overline{P}|$. Hence, $R \in Q$-$\text{Syl}_p(P) \subseteq Q$-$\text{Syl}_p(N)$. ▲

A corresponding fact about groups with triality can be stated as follows:

**Corollary 3** Let $p$ be a prime and let $G$ be a group with triality $S$. Then $G$
possesses an $S$-invariant $p$-subgroup $P$ such that $\mathcal{M}(P) \in Q$-$\text{Syl}_p(\mathcal{M}(G))$.

**Proof.** This assertion is a generalization of the implication $(i) \Rightarrow (iii)$ of
Theorem 2 and can be proved as follows. Denote $M = \mathcal{M}(G)$. We identify
$M$ with the subset $\{ [x, \sigma] \mid x \in G \} \subseteq G$. Let $N \in Q$-$\text{Syl}_p(M)$, which exists
by Theorem 4. By Lemma 7, $P = \langle N \cup N^p \rangle$ is an $S$-subgroup of $G$ such
that $\mathcal{M}(P) = N$ and $[P, S] = P$. By (ii) of Lemma 8, $P$ is the required
$p$-subgroup. ▲
Let $M$ be a Moufang loop and let $p$ be a prime. Denote by $Gr_p(M)$ the product of all normal subloops of $M$ for which $p$ is a Sylow prime. The properties of $Gr_p(M)$ are as follows:

**Proposition 3**

(i) $Gr_p(M) \trianglelefteq M$ and $p$ is a Sylow prime for $Gr_p(M)$;
(ii) The factor loop $M/Gr_p(M)$ contains no elements of order $p$;
(iii) All $p$-subloops of $M$ are contained in $Gr_p(M)$;
(iv) $Syl_p(Gr_p(M)) = Q\cdot Syl_p(M)$;
(v) $Gr(M) = Gr(Gr_p(M)) = \bigcap_p Gr_p(M)$.

**Proof.** Item (i) follows directly from the definition. We may henceforth assume that $p$ is non-Sylow for $M$, since otherwise $Gr_p(M) = M$ and the claim trivially holds. In particular, we have $p > 3$. Observe that $Gr(M) \trianglelefteq Gr_p(M)$. Hence, $M/Gr_p(M) \cong \overline{M}/Gr_p(M)$, where $\overline{M} = M/Gr(M)$, and it is easy to conclude by Theorem 3 that $Soc(M/Gr_p(M))$ must be the product of $M(q)$ for which $p$ is non-Sylow. Hence, $M/Gr_p(M)$ does not contain elements of order $p$ by Lemma 1 and (ii) follows. If $P$ is a $p$-subloop of $M$ then $PGr_p(M)/Gr_p(M)$ is a $p$-subloop of $M/Gr_p(M)$ and hence must be trivial by (ii), which implies (iii). The inclusion $Syl_p(Gr_p(M)) \subseteq Q\cdot Syl_p(M)$ holds by the definition of a quasi-$p$-Sylow subloop, since the composition factors of $M/Gr_p(M)$ are $M(q)$ for which $p$ is non-Sylow and, possibly, cyclic groups of order 2, as we just explained in proving (ii). The reverse inclusion holds by (iii) and the fact that quasi-$p$-Sylow subloops are $p$-subloops of maximal order. Finally, we show that (v) holds. The inclusions $Gr(M) \trianglelefteq Gr(Gr_p(M))$ and $Gr(M) \trianglelefteq \bigcap_p Gr_p(M)$ are obvious from $Gr(M) \trianglelefteq Gr_p(M)$. Since $Gr_p(M)/Gr(M)$ is a normal subloop of $M/Gr(M)$, its group-type radical must be trivial by Lemma 11. It follows easily that $Gr(Gr_p(M)) \trianglelefteq Gr(M)$. Now denote by $R$ the image of $\bigcap_p Gr_p(M)$ in $M/Gr(M)$. Since $R$ is a normal subloop, it follows by (ii) of Lemma 11 that every minimal normal subloop of $R$ is $M(q)$ for some $q$. However, for every $M(q)$, there is a non-Sylow prime. Hence $R$ has no nontrivial normal subloops and thus must be trivial.

This proposition shows that $Gr_p(M)$ can be viewed as a $p$-analog of the group-type radical $Gr(M)$. In particular, the study of embeddings of $p$-subloops into each other and determining the number of quasi-$p$-Sylow subloops of $M$ can be reduced to the case when $p$ is a Sylow prime for $M$. 

19
References

[1] R. H. Bruck, A survey of binary systems (Springer-Verlag, 1958).

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

[3] C. W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras. Pure and Applied Mathematics, Vol. XI Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[4] S. Doro, Simple Moufang loops, *Math. Proc. Camb. Phil. Soc.*, **83**, (1978), 377–392.

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

[6] D. Gorenstein, Finite groups. Harper & Row, Publishers, New York-London 1968.

[7] A. N. Grishkov, A. V. Zavarnitsine, Sylow’s theorem for Moufang loops I, Preprint RT-MAT 2005-17, IME-USP, São Paulo (2005), 14p.

[8] A. N. Grishkov, A. V. Zavarnitsine, Lagrange’s theorem for Moufang loops, *Math. Proc. Camb. Phil. Soc.*, **139**, N 1 (2005), 41–57.

[9] A. N. Grishkov, A. V. Zavarnitsine, Maximal subloops of finite simple Moufang loops, *J. Algebra*, **302**, N 2 (2006), 646–677.

[10] A. N. Grishkov, A. V. Zavarnitsine, Groups with triality, *J. Algebra Appl.*, **5**, N 4 (2006), 441–463.

[11] P. B. Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega^+_8(q)$ and of their automorphism groups, *J. Algebra*, **110**, N 1 (1987), 173–242.

[12] A. G. Kurosh, The theory of groups, Chelsea Publishing Co., New York 1960, Vol. 1: 272 pp.

[13] M. W. Liebeck, The classification of finite simple Moufang loops, *Math. Proc. Camb. Phil. Soc.*, **102**, (1987), 33–47.
[14] G. P. Nagy, P. Vojtěchovský, Octonions, simple Moufang loops and triality, *Quasigroups and Related Systems*, 10, (2003), 65–94.

[15] H. O. Pflugfelder, Quasigroups and loops: introduction, *Sigma Series in Pure Mathematics*, 7. Berlin: Heldermann Verlag. (1990).