Lagrange’s theorem for Moufang Loops

BY ALEXANDER N. GRISHKOV
Departamento de Matemática, Universidade de São Paulo,
Caixa Postal 66281, São Paulo-SP, 05311-970, Brasil,
and Omsk State University, pr. Mira 55-a, 644077, Russia
E-mail: grishkov@ime.usp.br

AND ANDREI V. ZAVARNITSINE
Sobolev Institute of Mathematics,
pr. Koptyuga 4, Novosibirsk, 630090, Russia
and Departamento de Matemática, Universidade de São Paulo,
Caixa Postal 66281, São Paulo-SP, 05311-970, Brasil
E-mail: zavarn@ime.usp.br

(Received 24 March 2003; revised 2 January 2004)

Abstract
We prove that the order of any subloop of a finite Moufang loop is a factor of the order
of the loop, thus obtaining an analog of Lagrange’s theorem for finite Moufang loops.

1. Introduction
The remarkable connection between Moufang loops and groups with triality, which was
first discovered by G. Glauberman [7] and then developed by S. Doro [4] and P. Mikheev
[11], proved to be very useful in the study of loops. Thus, M. Liebeck used this connection
in his classification [10] of finite simple Moufang loops. He proved that the unique simple
finite non-associative Moufang loops are the Paige loops $M(q) = PSL(O(q))$, where
$O(q)$ is a simple alternative 8-dimensional Cayley-Dickson algebra over the finite field of
$q$ elements (see [13]).

In the first part of this paper, we describe the correspondence between the maximal
subloops of a given Moufang loop and some subgroups of the corresponding group with
triality. In the second part, we apply this correspondence to solve a longstanding problem
in the theory of Moufang loops which asserts that the order of an arbitrary subloop $M_0$
of a finite Moufang loop $M$ divides the order of $M$. In view of Lemma 2.1 on the page
93 in [1], this problem can be reduced to the case when $M$ is a simple loop and, due to
M. Liebeck’s classification [10], to the case when $M = M(q)$. It is also clear that the
subloop $M_0$ can be assumed to be maximal in $M$.

It is known that the triality group corresponding to the loop $M(q)$ is the finite simple
orthogonal group $P\Omega_8^+(q)$. Under the above correspondence, a maximal subloop $M_0$
of $M(q)$ is linked to a certain subgroup $G_0$ of $P\Omega_8^+(q)$. We use P. Kleidman’s description

† supported by FAPESP and CNPq, Brazil
‡ supported by FAPESP, Brazil, and RAS, Russia
A. N. Grishkov and A. V. Zavarnitsine

The condition \( L \) theorem among the right Bol loops is not known to the authors. It turns out that all such orders divide the order of \( M(q) \), which proves

Lagrange’s Theorem. The order of any subloop of a finite Moufang loop \( M \) divides the order of \( M \).

The authors of [3] have concluded that a solution to Lagrange’s problem may be achieved for any variety of loops, in which there exists a classification of (finite) simple loops, by establishing that all simple loops in this variety satisfy the Lagrange property. We do this for the variety of Moufang loops. In particular, our proof is dependent on the classification of finite simple groups.

Every Moufang loop \( M \) is diassociative, i.e., any subloop of \( M \) generated by two elements is a group. We note that, in general, for diassociative loops Lagrange’s theorem is not true. For example, let \( M \) be a group. We note that, in general, for diassociative loops Lagrange’s theorem is not true. For example, let \( M \) be a group. We note that, in general, for diassociative loops Lagrange’s theorem is not true. For example, let \( M \) be a group.

2. Moufang loops and groups with triality

A loop \( M \) is called a Moufang loop if

\[ xy \cdot zx = (x \cdot yz)x \quad \text{for all} \quad x, y, z \in M. \]

A group \( G \) possessing automorphisms \( \rho \) and \( \sigma \) such that \( \rho^3 = \sigma^2 = (\rho \sigma)^2 = 1 \) is called a group with triality (relative to \( \rho \) and \( \sigma \)) if the following relation holds for every \( x \) in \( G \):

\[ [x, \sigma] \cdot [x, \sigma]^\rho \cdot [x, \sigma]^\sigma = 1, \quad (2.1) \]

where \( [x, \sigma] = x^{-1}x^\sigma \). We denote \( S = \langle \rho, \sigma \rangle \). The triality is called non-trivial if \( S \neq 1 \). The most interesting situation is when \( S \) is isomorphic to the symmetric group \( S_3 \) in which case the relation (2.1) does not depend on the particular choice of the generators \( \rho \) and \( \sigma \) of \( S \) (see [4]) and we will thus speak of a group with triality \( S \). This fact, together with Lemma 3.2 in [10], implies

**Lemma 1.** The condition (2.1) is equivalent to \( [x \rho, \sigma] = 1 \) for every \( x \) in \( G \).

The expression \([x \rho, \sigma] \) here is to be regarded in the semidirect product \( GS \).

Introduce some notation: \( C_p(Q) \) is the centralizer of \( Q \) in \( P \). If \( P \) is a (normal) subgroup of \( Q \) then we write \( P \trianglelefteq Q \) \( (P \trianglelefteq Q) \). Put \( [x, y] = x^{-1}y^{-1}xy \), \( g^h = h^{-1}gh \), \( g^{-h} = (g^{-1})^h \).

If \( G \) is a group with triality \( S \) then, for \( g \in G \), define

\[ \xi(g) = g^{-1}y^\sigma = [g, \sigma], \quad \phi(g) = g^{-\rho}y^\sigma, \quad \eta(g) = gg^{-\rho \sigma}y^\sigma = g[g, \sigma]^{-\rho \sigma}. \]
Also, put $M = \xi(G)$ and $H = C_G(\sigma)$. Observe that
\[ m^\sigma = m^{-1} \in M \quad \text{for all} \quad m \in M. \quad (2.2) \]

**Lemma 2.** In the above notation, we have:

(i) $m_n = m_n^m \in M$ for all $m, n \in M$,

(ii) $[m, m^\sigma] = [m, m^\sigma] = [m, m^\sigma] = 1$ for all $m \in M$,

(iii) $[m^\sigma, n^\sigma] = [m^\sigma, n^\sigma] \in H$ for all $m, n \in M$,

(iv) $\phi(g) \in H \quad \forall g \in G$,

(v) $\phi(H) \subseteq M$, $\phi(M) \subseteq H$.

**Proof.** (i) By (2.1) and (2.2), we have $\xi(m^\sigma n^\sigma) = n^{-\sigma} m^{-\sigma} m^\sigma n^\sigma = n^{-\sigma} m^{-\sigma} m^\sigma n^{-\sigma} = n^{-\sigma} m^{-\sigma} m^\sigma n^{-\sigma} \in M$ for all $m, n \in M$. Moreover, (2.1) also implies $n^{-\sigma} m_n^{-\sigma} = n^{-\sigma} m_n^{-\sigma} m^\sigma n^{-\sigma} = n^{-\sigma} m_n^{-\sigma} m^\sigma n^{-\sigma} n^{-1} = 1$.

Conjugating this equality by $n$, we obtain $n^{-1} m^{-1} m^\sigma n = m^{-1} m^\sigma m = m^{-1} m^\sigma m$. Applying $\rho^2$ to this equality, we have $n^{-\sigma} m^{-\sigma} n^{-1} = m^\sigma m^\sigma$. This, together with (2.1), implies $n^{-\sigma} m^{-\sigma} n^{-1} = m^{-\sigma} m^\sigma n^{-1} = m^{-\sigma} m^\sigma$; hence,

$m^{-\sigma} m^\sigma n^{-1} = m^{-\sigma} m^\sigma m^\sigma m^{-1} = m^{-\sigma} m^\sigma m^\sigma$.

(iv) $\eta(g)^{\rho} = g^\sigma g^{-\sigma} g^{\rho} = g(g^{-1})^\sigma g^\sigma = g(g^{-1})^\sigma = g^{-\sigma} g = \eta(g)$.

Let $h$ and $m$ be elements of $H$ and $M$, respectively. Then (2.2) and (ii) imply $\phi(m)^2 = m^\sigma m^\sigma = m^\sigma m^\sigma = \phi(m) \in H$. $\xi(\phi(h)^{\rho}) = \xi(h^\sigma h = h^{-\sigma} h = h^\sigma h^\sigma = \phi(h) \in M$. □

By item (iv) of this lemma, every $g \in G$ admits the decomposition $g = \eta(g)\xi(g)^{\rho}$ with $\eta(g) \in H$ and $\xi(g) \in M$. In particular, for all $m, n \in M$, we have by item (i)

\[ m_n^\sigma = \eta(m_n^\sigma n^\rho) \xi(m_n^\sigma n^\rho)^{\rho} = [m_n^\sigma, n^\rho] = [m_n^\sigma, n^\rho]. \quad (2.3) \]

Let $G$ be an arbitrary group with triality. It was shown in Lemma 1 of [4] that the set $M^\sigma$ is a right transversal of $H$ in $G$. For $g \in G$, we define $\pi(g)$ to be the unique element of $M^\sigma$ such that $\pi(g)g^{-1} \in H$. Then the composition $m_1 \cdot m_2 = \pi(m_1 m_2)$ endows $M^\sigma$ with the structure of a Moufang loop (see Theorem 1 in [4]). By (2.3), the mapping $m \mapsto m^\sigma$ for $m \in M$ is an isomorphism of loops $(M, \cdot) \cong (M^\sigma, \cdot)$, where, by definition,

\[ m \cdot n = m^\sigma n n^{-\sigma} \quad \text{for all} \quad m, n \in M. \quad (2.4) \]

We denote the loop $(M, \cdot)$ by $M(G)$ and note that $\|M(G)\| = [G : H]$. The relation (2.4) implies that the identity of $M(G)$ coincides with the identity of $G$ and, for every $m \in M(G)$, taking the inverse $m^{-1}$ or any power $m^t$ is the same whether considered in $M(G)$ or in $G$.

Suppose that $G_0$ is an S-invariant subgroup of $G$ (shortly, $S$-subgroup). Then $G_0$ is a group with triality $S$ and $M(G_0)$ is a subgroup of $M = M(G)$. In the following Theorem 1, we prove that all subloops of $M$ may be constructed in this way. Note that the relation $G_1 < G_2$ for $S$-subgroups $G_1$ and $G_2$ of $G$ implies the relation $M(G_1) \leq M(G_2)$ for the
Let \( m, n, k \in M \) then

(i) \( m^{-1}.n.m = h^{-1}n, \) where \( h = \phi(m) \in H. \)

(ii) \((k,m).n, (m.n)^{-1} = h^{-1}kh, \) where \( h = [m^\rho, n^{-\rho}] \in H \)

(iii) \( m^{-1}.n^{-1}.m.n = \phi([m^\rho, n^{-\rho}]) \in M. \)

Proof. (i) By Lemma 2, \( h = \phi(m) \in H. \) Note that (i) of Lemma 2 implies the following alternative expression for the multiplication in \( M: \)

\[
x.y = y^{-\rho}x y^{-\rho} \quad \text{for all} \quad x, y \in M.
\]

Using it, we have \( m^{-1}.n.m = m^{-1}((m^{-\rho}km^{-\rho}).n).mn^{-\rho}m^\rho = m^\rho m^{-\rho}m^{-\rho}m^\rho \) for all \( n \in M. \)

We also have \( h^{-1}nh = m^{-\rho}m^{-\rho}m^{-\rho}m^\rho. \) The claim follows, since \( m^\rho m^{-\rho} = m^{-\rho}m^\rho \) by (ii) of Lemma (2).

(ii) For \( m, n, k \in M, \) we have by (2-5)

\[
((k.m).n)(m.n)^{-1} = ((m^{-\rho}km^{-\rho}).n).n^{-\rho}mn^{-\rho} = (n^{-\rho}km^{-\rho}.n^{-\rho}).n^{-\rho}mn^{-\rho} = (n^{-\rho}m^{-\rho}(n^{-\rho}m^{-1}n^\rho))^\rho = n^{-\rho}m^{-\rho}(n^{-\rho}m^{-1}n^\rho)^\rho = (n^{-\rho}m^{-\rho}n^{-\rho}m^{-\rho}n^{-1}m^{-1}n^\rho)m^{-\rho}n = [n^{-\rho}, m^{-\rho}]n = [m^\rho, n^{-\rho}]^{-\rho}[m^{-\rho}, n^{-\rho}]^{-\rho} = [m^\rho, n^{-\rho}]^{-\rho} = \phi([m^\rho, n^{-\rho}]).
\]

However, Lemma 2 (iv) implies \([n^\rho, m^{-\rho}] = [n^{-\rho}, m^\rho].\)

(iii) Using (2-5), (2-1) and (ii),(iii) of Lemma 2, we have

\[
m^{-1}.n^{-1}.m.n = (m^{-1}.n^{-1}).(m.n) = (n^{-\rho}m^{-1}n^\rho)(n^{-\rho}mn^{-\rho}) = (n^{-\rho}m^{-\rho}n^{-\rho}m^{-1}n^\rho)(n^{-\rho}mn^{-\rho}) = [n^{-\rho}, m^{-\rho}]n = [m^\rho, n^{-\rho}]^{-\rho} = \phi([m^\rho, n^{-\rho}]). \]

Theorem 1. Let \( G \) be a group with triality \( S = \langle \rho, \sigma \rangle, \) \( G = HM^\rho, \) where \( H = C_G(\sigma) \) and \( M = \{[g, \sigma] \mid g \in G\}, \) and let \( M(G) = \langle M, \rangle \) be the corresponding Moufang loop. Then, for every subloop \( P \subseteq \mathcal{M}(G), \) there exists an \( S \)-subgroup \( Q \subseteq G \) such that \( M(Q) = P. \) Moreover,

(i) if \( G_0 \) is the \( S \)-subgroup generated by \( M \) then \( G_0 \subseteq G, \)

(ii) if \( G_1 \subseteq G_0 \) is an \( S \)-subgroup such that \( M(G_1) = \mathcal{M}(G_0), \) then \( G_1 = G_0. \)

Proof. Let \( P \subseteq M \) be a subloop, which means that \( P \subseteq M \) and, for \( m, n \in P, \)

\[
m.n = m^\rho m^{-\rho} \in P. \]

We denote by \( Q \) the subgroup of \( G \) generated by \( P \cup P^\rho \cup P^{\rho\sigma}. \)

It is clear that \( Q \) is \( \rho \)-invariant. Also, (2-2) implies

\[
P^\rho = P, \quad (P^\rho)^\sigma = P^\rho, \quad (P^\rho^\sigma)^\rho = P^\rho.
\]

Hence, \( Q \) is \( S \)-invariant. We wish to prove that \( \mathcal{M}(Q) = P. \)

Let \( H_0 \) be the subgroup of \( Q \) generated by the set \( T = \{m^\rho m^{-\rho}, [m^\rho, n^{-\rho}] \mid m, n \in P\}. \)

By (iii) and (v) of Lemma 2, \( H_0 \subseteq H. \) Denote \( Q_0 = H_0^{P^\rho} \) and prove that \( Q = Q_0. \)

This will imply that

\[
\mathcal{M}(Q) = \mathcal{M}(Q_0) = \{\xi(h^{P^\rho}) \mid h \in H_0, p \in P\}.
\]
However, $\xi(hp^2) = p^{-\rho}h^{-1}h^p = p^{-\rho}h^{-1}h^p = p^{-\rho}p^{-\rho} = p$ by (2.1). Therefore, we will have $M(Q) = P$ as is required.

Clearly, $Q_0 \subseteq Q$. On the other hand, observe that $P \subseteq Q_0$. Indeed, if $m \in P$ then, by (2.1) and (ii) of Lemma 2, we have

$$m = m^{-\rho}m^{-\rho} = m^{-\rho}m^{-\rho}(m^{-\rho})^2 = (m^{-\rho}m^{-\rho})(m^{-\rho})^2 \in Q_0.$$  

Now, for $m \in P$, we also have $m^\rho = (m^\rho m^{-\rho})m^\rho \in Q_0$ and $m^\rho \in Q_0$ by definition. Therefore, $P \cup P^\rho \cup P^\rho \subseteq Q_0$. Hence, for the equality $Q = Q_0$ to hold, it suffices to show that $Q_0$ is a subgroup.

By (i) and (ii) of Lemma 3, we have $P^h = P$ for all $h \in T$. Thus,

$$P^h = P \quad \text{for all} \quad h \in H_0. \quad (2.6)$$

First, show that

$$\phi(H_0) \subseteq P. \quad (2.7)$$

Let $a, b \in H_0$ and suppose that $\phi(a), \phi(b) \in P$. Then

$$\phi(ab) = (ab)^{-\rho}(ab)^{\rho} = b^{-\rho}(a^{-\rho}a^\rho)b^\rho = (b^{-\rho}b^{-1})^{-\rho} \phi(a)b(b^{-1}b^\rho) = (b^{-\rho}b^{-1})^{-\rho} \phi(b) \in P \quad \text{by (2.6)}.$$  

Hence, it suffices to prove that $\phi(m^{-\rho}m^\rho) \in P$ and $\phi([m^\rho, n^{-\rho}]) \in P$. We have

$$\phi(m^{-\rho}m^\rho) = m^{-1}m^\rho \in P,$$

and

$$\phi([m^\rho, n^{-\rho}]) = m^{-1}n^{-1}m^{\rho}n^{\rho} \in P \quad \text{by (ii) of Lemma 3}.$$  

This shows that (2.7) holds. Now we can prove that $Q_0 = H_0P^\rho$ is a subgroup. Let $m^\rho, n^\rho \in P^\rho$. Then, by (2.3),

$$m^\rho n^\rho = [m^\rho, n^{-\rho}][(m, n)^{\rho}]. \quad (2.8)$$

Hence, $m^\rho n^\rho \in Q_0$. Let $h \in H_0$, $m \in P$. Then we have

$$m^\rho h = \eta(m^\rho h)\xi(m^\rho h)^{\rho} = h_1 m_1^{\rho},$$

where

$$m_1 = \xi(m^\rho h) = h^{-1}m^{-\rho}m^\rho = m^h \in P \quad \text{by (2.6)}, \quad$$

and

$$h_1 = \eta(m^\rho h) = m^\rho h^{-1}m^{-\rho}m^\rho = m^\rho h^{-1}m^{-\rho}m^\rho = m^\rho h^{-1}m^{-\rho}m^\rho = m^\rho h(m^h)^{-\rho} = h(h^{-1}h^\rho)(h^{-1}m^\rho h^\rho)(h^{-1}h^\rho)(m^h)^{-\rho} = h[h^{-1}h^\rho, (m^h)^{-\rho}] = h_1[h_1^\rho, (m^h)^{-\rho}] \in H_0 \quad \text{by (2.6) and (2.7).}$$

Now we have for $m, n \in P$ and $h, k \in H_0$

$$(gm^\rho)^{(hn)^\rho} = gh_1 m_1^{\rho} = gh_1k(m_1, n)^{\rho} \in Q_0,$$  

where $m^\rho h = h_1 m_1^{\rho}$ as above and

$$m_1^{\rho} = m(k, n)^{\rho} \in Q_0 \quad \text{as in (2.8) for} \quad k \in H_0.$$  

These remarks show that $Q_0$ is a subgroup.

Let $G_0$ be the $S$-subgroup of $G$ generated by $M$. Show that $G_0 \leq G$. By (2.1), $G_0$ is generated by $X = \{M \cup M^\rho\}$. Since $G = H M^\rho$, it suffices to show that $X^H \subseteq G_0$.

We have $M^h = M$ for $h \in H$. Prove that $h^{-1}m^\rho h \in G_0$ for $h \in H$, $m \in M$. Since $G_0$ is $S$-invariant, we show $h^{-\rho}m^{\rho}h^{-\rho} \in G_0$. We have $h^{-\rho}m^{\rho}h^{-\rho} = (h^{-\rho}h)h^{-1}h^{-1}h^{-1}$. However, $h^{-\rho}h = \phi(h)^\rho \in M^\rho$ and $m^\rho \in M$. Thus $G_0$ is a normal subgroup of $G$.

The last assertion of the theorem is obvious. Indeed, if $M(G_1) = M(G_0)$, then $M \subseteq G_1$ and $G_0 \subseteq G_1 = G_0$. $$\square$$

An $S$-subgroup of $G$ that is maximal among the $S$-subgroups is called $S$-maximal.

**Corollary 1.** Let $G$ be a group with triality $S = \langle \rho, \sigma \rangle$ and let $M = M(G)$ be the corresponding Moufang loop. Suppose that $G$ coincides with its $S$-subgroup generated by $M$. Then, for any maximal subloop $M_0 \leq M$, there exists an $S$-maximal subloop $G_0 \leq G$ such that $M(G_0) = M_0$. Moreover, the order of the subloop $M_0$ is given by $|M_0| = |G_0 : C_{G_0}(\sigma)|$. 

**LaGrange’s theorem for Moufang Loops**
Let \( M \) be a Sylow 2-subgroup of \( G \). If both \( M \) and \( M' \) are maximal subloops of \( \Omega_q \) and \( M \neq M' \), then \( M \) and \( M' \) are conjugate in \( Aut(G) \). For our purposes, it is more convenient to look at \( M \) instead of \( \Omega_q \). Now suppose that \( M \) is a non-degenerate quadratic form \( \langle \cdot, \cdot \rangle \) of \( V \) such that \( \langle v, w \rangle = 0 \) for all \( v, w \in V \). A reflection \( r_v \) in a non-singular vector \( v \) is a linear transformation of \( V \) given by

\[
r_v(x) = x - \frac{(x, v)}{Q(v)} v.
\]

Clearly, the reflections \( r_v \) are involutions in \( GO_k^+q \). By Lemma 4, we may assume that \( G = D_4(q) \) and \( S \) is conjugate in \( Aut(G) \) to the group of graph automorphisms of \( D_4(q) \).

**Proof.** Let \( X = \{ P \leq G \mid P \) is S-invariant and \( M(P) = M_0 \} \). By Theorem 1, the set \( X \) is non-empty. Choose some maximal element \( P \in X \). If \( P \) is not \( S \)-maximal there exists a \( S \)-subgroup \( P_1 \) such that \( P < P_1 \). Hence, \( P_1 \notin X \) and \( M_1 = M(P_1) > M_0 \). But \( M_0 \) is a maximal subloop of \( M \); hence, \( M(P_1) = M \). Then, by item (ii) of Theorem 1, \( P_1 = G \), since \( G \) coincides with the \( S \)-subgroup generated by \( M \). We have a contradiction. \( \square \)

**Lemma 4.** If \( G \) is a finite non-abelian simple group with non-trivial triality \( S = \langle \rho, \sigma \rangle \) then \( G = D_4(q) \) and \( S \) is conjugate in \( Aut(G) \) to the group of graph automorphisms of \( G \) which is isomorphic to \( S_3 \). If this is the case then \( M(G) \) is isomorphic to \( M(q) \).

**Proof.** If both \( \rho \) and \( \sigma \) are outer automorphisms, the result follows by [10]. Hence, we may assume that \( \rho \) is inner. Then Lemma 1 implies that \( [g, \sigma]^3 = 1 \) for all \( g \in G \). Let \( T \) be a Sylow 2-subgroup of \( G(\sigma) \) containing \( \sigma \). Since \( [g, \sigma] = \sigma^g \sigma \), we have \( \sigma^G \cap T = \{ \sigma \} \), i.e., \( \sigma \) is an isolated involution in \( T \). By Glauberman’s \( Z^{*-}\)-theorem, \( Z^*(G(\sigma)) \neq 1 \), which contradicts simplicity of \( G \) and non-triviality of \( S \). \( \square \)

Now suppose that \( M = M(q) \) is a non-associative simple Moufang loop. One of the groups with triality corresponding to \( M \) is \( G = D_4(q) \). By Lemma 4, we may assume that \( S \) is the group of graph automorphisms of \( D_4(q) \) and, by Corollary 1, the orders of maximal subloops of \( M \) lie in the set of indices \( |G_0 : C_{G_0}(\sigma)| \) as \( G_0 \) runs through all \( S \)-maximal subgroups of \( D_4(q) \).

3. **\( S \)-maximal subgroups of \( P\Omega_k^+q \)**

For our purposes, it is more convenient to look at \( D_4(q) \) as the orthogonal simple group \( P\Omega_k^+q \). First, give some definitions. A quadratic form \( Q \) on a vector space \( V \) is called non-degenerate if

\[
\{ v \in V \mid (v, w) = 0 \quad \text{for all} \quad w \in V \} \cap \{ v \in V \mid Q(v) = 0 \}
\]

contains only the zero vector of \( V \), where \( (\ , \ ) \) is the bilinear form associated with \( Q \), i.e., \((v, w) = Q(v + w) - Q(v) - Q(w)\). For \( v \in V \), we call \( Q(v) \) the norm of \( v \) and say that \( v \) is (non-)singular if it has a (non-)zero norm. A subspace \( W \leq V \) is called non-degenerate if \( Q|_W \) is a non-degenerate quadratic form on \( W \) and totally singular (t.s.) if \( Q \) vanishes on \( W \). By definition, \( W^{\perp} = \{ v \in V \mid (v, w) = 0 \quad \text{for all} \quad w \in W \} \). A non-degenerate orthogonal space \( (V, Q) \) of even dimension \( 2m \) is said to have type ‘+’ or ‘−’ if all maximal t.s. subspaces of \( V \) have dimension \( m \) or \( m - 1 \), respectively.

Now let \( V \) be an \( 8 \)-dimensional vector space over \( F = GF(q) \), \( q = p^n \), equipped with a non-degenerate quadratic form \( Q : V \rightarrow F \) of type ‘+’. We choose a standard basis \( (e_1, \ldots, e_4, f_1, \ldots, f_4) \) of \( V \) such that

\[
(e_i, f_i) = 1, \quad Q(e_i) = Q(f_i) = (e_i, f_j) = (e_i, e_j) = (f_i, f_j) = 0 \quad \text{for} \quad i \neq j.
\]

A reflection \( r_v \) in a non-singular vector \( v \) is a linear transformation of \( V \) given by

\[
r_v(x) = x - \frac{(x, v)}{Q(v)} v.
\]

Clearly, the reflections \( r_v \) are involutions in \( GO_k^+q \). By \( r_\mu \) we denote the reflection in a vector whose norm is a square in \( F^* \). If \( q \) is odd then \( \mu \) denotes a non-square in \( F^* \). The image of the natural homomorphism \( GO_k^+q \rightarrow PGO_k^+q \) is denoted by an overline.
“—” and the full preimage by an overhat “ˆ—”. By \( Z_n \) we mean a cyclic group of order \( n \) and by \( D_{2n} \) a dihedral group of order \( 2n \). Denote \( d = (2, q - 1) \).

Henceforth, we put \( G = P\Omega^+_s(q) \), \( \Omega = \Omega^+_s(q) \), and \( M = M(q) \). It is known that
\[
|G| = \frac{1}{d^2} q^{12} (q^6 - 1)(q^4 - 1)^2(q^2 - 1), \quad |M| = \frac{1}{d^2} q^{12} (q^4 - 1).
\]

If \( H \) is a subgroup of \( G \) then \([H]\) denotes the \( G\)-conjugacy class of \( H \).

We will be using the following lemma.

**Lemma 5.** Given a reflection of form \( r_3 \) in \( GO^+_m(q) \), where \( \varepsilon = \pm 1 \) and \( m = 2t \), we have \( |GO^+_m(q) : C_{GO^+_m(q)}(r_3)| = \frac{1}{d} q^{t-1}(q^t - \varepsilon) \).

**Proof.** See Proposition 3 and Lemma 5 in [12]. \( \square \)

Let \( S = \langle \rho, \sigma \rangle \cong S_3 \) be a subgroup of \( \text{Aut}(G) \) such that \( G \) is a group with triality \( S \). Although, by Lemma 4, \( S \) can be chosen arbitrarily up to \( \text{Aut}(G)\)-conjugacy, we choose it so that \( \sigma \) be equal to \( \underline{r}_3 \) for some fixed reflection \( r_3 \) (see discussion on p. 182 in [8]). Denote \( G_1 = G(\sigma) \).

A subgroup in \( GS \) that is \( \text{Aut}(G)\)-conjugate to \( S \) is called a triality \( S_3\)-complement. An involution in \( GS \) is called a triality involution if it lies in a triality \( S_3\)-complement. We remark that, in view of the structure of \( \text{Aut}(G) \) (see, e.g., section 1.4 in [8]), all triality \( S_3\)-complements in \( GS \) are in fact conjugate in \( GS \) and all triality involutions in \( G_1 \) are conjugate in \( G_1 \). It follows that the triality involutions in \( G_1 \) are precisely the involutions \( \underline{r}_3 \) for all reflections \( r_3 \) in \( GO^+_2(q) \).

**Lemma 6.** The number of triality involutions in \( G_1 \) is \( |M| \), and the number of triality \( S_3\)-complements in \( GS \) is \( |M|^2 \).

**Proof.** The assertion follows from the above remarks about conjugacy, Lemma 5, and the fact that \( |N_G(S)| = |G_2(q)| \) (see Proposition 3.1.1 in [8]). \( \square \)

Now let \( G_0 \) be an \( S\)-maximal subgroup of \( G \). Then \( N_{GS}(G_0) \) is a maximal subgroup of \( GS \). We make use of the main result of [8] which, in particular, classifies all maximal subgroups of \( GS \). Table 1 contains the list of representatives \( G_0 \) of the \( G\)-conjugacy classes \([G_0]\) of subgroups of \( G \) such that \( N_{GS}(G_0) \) is a maximal subgroup in \( GS \). The notation is mostly borrowed from [8]. Column II indicates for which values of \( q \) (with “—” meaning “for all \( q \)”) the corresponding subgroup \( G_0 \) is defined and the normalizer \( N_{GS}(G_0) \) is maximal in \( GS \). Column III shows “✓” (“—”) if \( G_0 \) is always (never) maximal in \( G \), or indicates specific values of \( q \) for which it is maximal. Column IV gives the size of \( G_0 \). Column V gives the order of the corresponding subloop \( M(G_0) \) which happens not to depend on the choice of an \( S\)-maximal representative in \([G_0]\) (for details, see Theorem 2 below).

Note that all subgroups \( G_0 \) from Table 1 satisfy \( N_G(G_0) = G_0 \). We wish to determine which subgroups \( P \) in \([G_0]\) are \( S\)-maximal and, if so, what the order of the corresponding subloop \( M(P) \) is. Since all subgroups in \([G_0]\) are conjugate to \( G_0 \), this problem is equivalent to the study of triality \( S_3\)-complements in \( GS \) of \( G_0 \) of a fixed representative \( G_0 \).

For proving the main theorem, we will need some more auxiliary lemmas.

**Lemma 7.** If \( H \) is a subgroup of \( G \) such that \( GN_{GS}(H) = GS \) then \( N_{GS}(H) \) contains a triality \( S_3\)-complement if and only if it contains a triality involution.
It suffices to prove that any two triality involutions that belong to different cosets $G\sigma \rho$ contains exactly $2$ cosets $G\sigma \rho$. Denote by $\epsilon$ the number of $-1$-subspaces of $\mathbb{F}_q$. For $\epsilon$ is an orthogonal geometry of sign $\pm$. By definition, an involution is totally singular then $w$ is a non-singular vector. The claim readily follows.

**Proof.** It suffices to prove that any two triality involutions that belong to different cosets in $G_S : G \in G\sigma \rho$. By Lemma 6, we see that each triality involution in $G = G(\sigma)$ lies in $|M|$ triality $S_3$-complements each of which intersects the two cosets $G\sigma \rho$ and $G\sigma \rho$ by a triality involution. However, each of these two cosets contains exactly $|M|$ triality involutions and the claim follows. □

**Lemma 8.** Suppose that a reflection $r_v$ normalizes a subspace $W \subseteq V$. We have

(i) either $v \in W$ or $v \in W^\perp$,

(ii) if $W$ is totally singular then $v \in W^\perp$.

**Proof.** The fact that $r_v$ normalizes $W$ is equivalent to the condition that $(w, v)v \in W$ for all $w \in W$, since $v$ is a non-singular vector. The claim readily follows. □

By definition, an $m$-subspace of $V$ is a subspace of dimension $m$. If $m$ is even then an $\varepsilon m$-subspace of $W$ where $\varepsilon = \pm 1$, is a non-degenerate $m$-subspace such that $(W, Q|_W)$ is an orthogonal geometry of sign $\varepsilon$. For $q$ odd, a $+1$-subspace (a $-1$-subspace) is a $1$-subspace spanned by a non-singular vector whose norm is a square (non-square). For $q$ even, a $+1$-subspace is an arbitrary non-degenerate $1$-subspace.

**Lemma 9.** Suppose that $q$ is odd and $Q_0$ is a quadratic form defined on a vector space $W$ over $\mathbb{F}$. If $\dim W = \dim \ker Q_0$ is even then the number of $+1$-subspaces of $W$ is equal to the number of $-1$-subspaces of $W$.

**Proof.** Denote by $n^\varepsilon(W_{Q_0})$ the number of $\varepsilon 1$-subspaces in $W$ with respect to $Q_0$, $\varepsilon = \pm 1$. Clearly, we may assume that $\ker Q_0 = 0$ and thus $\dim W$ is even. Consider

<table>
<thead>
<tr>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_0$</td>
<td>restrictions on $q$</td>
<td>maximality in $G$</td>
<td>$</td>
<td>G_0</td>
</tr>
<tr>
<td>1.</td>
<td>$P_2$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>2.</td>
<td>$R_{42}$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>3.</td>
<td>$N_1$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>4.</td>
<td>$N_2$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>5.</td>
<td>$N_3$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>6.</td>
<td>$N_4$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>7.</td>
<td>$I_{12}$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>8.</td>
<td>$I_{22}$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>9.</td>
<td>$I_{33}$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>10.</td>
<td>$G_2$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>11.</td>
<td>$P\Omega^+_8(2)$</td>
<td>$q \neq 3$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>12.</td>
<td>$P\Omega^+_8(q_0)$</td>
<td>$q = q_0^k$, $k$ prime, $(d, k) = 1$</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>13.</td>
<td>$P\Omega^+_8(q_0).2$</td>
<td>$q = q_0^2$ odd</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
<tr>
<td>14.</td>
<td>$P\Omega^+_8(q)$</td>
<td>$q = q_0^2$ odd</td>
<td>$\frac{1}{192}q^4(q^8 - 1)(q^2 - 1)$</td>
<td>120</td>
</tr>
</tbody>
</table>
the quadratic form $Q_1 = \mu Q_0$. It is known that $Q_1$ is equivalent to $Q_0$. We thus have $n^+(W_{Q_0}) = n^+(W_{Q_1}) = n^-(W_{Q_0})$. □

**Lemma 10.** Suppose that $q$ is even, $W$ is a non-degenerate orthogonal $+2m$-space over $F$, and $T$ is a t.s. $m$-subspace in $W$. Then, for $g \in GO^+_{2m}(W)$, $m - \dim(T \cap Ty)$ is even if and only if $g \in \Omega^+_{2m}(W)$.

**Proof.** See Description 4 on p.30 in [9]. □

**Lemma 11.** Let $\lambda$ be the field automorphism of $L_2(q^2)$ of order 2. Then the isomorphism $L_2(q^2)/\langle \lambda \rangle \cong PGO^+_4(q)$ holds.

**Proof.** Note that the isomorphism $L_2(q^2) \cong PGO^+_4(q)$ is well-known. Let $U$ be the natural 2-dimensional $SL_2(q^2)$-module with basis $(u_1, u_2)$. Since $SL_2(q^2) \cong Sp_2(q^2)$, there exists a non-degenerate symplectic form $k$ on $U$ that is invariant under $SL_2(q^2)$. The $SL_2(q^2)$-module $U \otimes U^\lambda$ is extended to an $SL_2(q^2)/\langle \lambda \rangle$-module if we make $\lambda$ act on the basis $u = (u_1 \oplus u_1, u_1 \oplus u_2, u_2 \oplus u_1, u_2 \oplus u_2)$ as the linear mapping with matrix

$$
\begin{pmatrix}
1 & 1 & & \\
& 1 & & \\
& & 1 & \\
& & & 1
\end{pmatrix}.
$$

Introduce a bilinear form $k^*$ on $U \otimes U^\lambda$ by putting

$$k^*(u_i \otimes u_j, u_s \otimes u_t) = k(u_i, u_s)k(u_j, u_t)$$

for all basis vectors in $u$ and extending it to $U \otimes U^\lambda$ by linearity. If $q$ is odd, there exists a unique quadratic form $K$, associated with $k^*$. For $q$ even, define, additionally, $K(u_i \otimes u_j) = 0$, $i, j = 1, 2$. Note that $U \otimes U^\lambda$ possesses an $SL_2(q^2)/\langle \lambda \rangle$-invariant $F_q$-subspace $W$ spanned by the vectors $w_1 = u_1 \otimes u_1$, $w_2 = u_2 \otimes u_2$, $w_3 = u_1 \otimes u_2 + u_2 \otimes u_1$, $w_4 = \theta u_1 \otimes u_2 + \theta^2 u_2 \otimes u_1$, where $\theta$ lies in $F_q^\ast$, $F_q$ and $\theta^2 \in F_q$, for $q$ odd. We thus have an embedding $SL_2(q^2)/\langle \lambda \rangle \leq GL_4(q) = GL(W)$. Moreover, $K(w) \in F_q$ for all $w \in W$ and $K$ is a non-degenerate quadratic form on $W$ of sign $-1$ which is preserved by $SL_2(q^2)/\langle \lambda \rangle$; thus, $SL_2(q^2)/\langle \lambda \rangle \leq G_2(q^2)$. It remains to notice that the element $\lambda$ acts on $W$ as the reflection $r_{w_1}$ for $q$ odd and $r_{w_2}$ for $q$ even. □

**Lemma 12.** If a reflection $r_v$ permutes two subspaces $W_1$ and $W_2$ of $V$ such that $W_1 \cap W_2 = 0$ then $\dim W_1 = \dim W_2 \leq 1$.

**Proof.** Choose a basis $w = (w_1, \ldots, w_k)$ of $W_1$, where $k = \dim W_1$. Then $w^v = (w_1r_v, \ldots, w_kr_v)$ is a basis of $W_2$ and $w \cup w^v$ can be extended to a basis $v$ of $V$. By considering the matrix of $r_v$ in $v$, it is clear that, in odd characteristic, the number of eigenvalues of $r_v$ distinct from 1 is at least $k$ and, in even characteristic, the number of non-trivial Jordan blocks of $r_v$ is at least $k$. Thus, $k \leq 1$, since $r_v$ is a reflection. □

We are now ready to prove the main theorem of this section.

**Theorem 2.** If $G_0$ is a group from Table 1 then the class $[G_0]$ contains $S$-maximal subgroups unless $G_0$ is an $N_2$-subgroup or a $PGL_2(q)$-subgroup. The order of the subloop $\mathcal{M}(P)$ is the same for all $S$-maximal members $P$ of $[G_0]$ and is given in column $V$ of Table 1.

**Proof.** By Lemma 7, we have to check whether $G_0$ is normalized by an involution $r_v$. To prove that the order $|\mathcal{M}(P)|$ is independent of the choice of an $S$-maximal representative...
Then $g \in G_0$. Since $Q$ is totally singular 4-spaces which are interchanged by a reflection of form $R$, where $g \in G_0$ is normalized by the triality involution $\hat{\tau}$. By Lemma 8, a reflection $r_v$ normalizes $G_0 = \mathcal{N}_G(U, R \cap T)$ if and only if $v \in U^\perp \cap (R \cap T)^\perp = (R \cap T)^\perp$. Thus, the number of such reflections of form $r_v$ is equal to the number of $+1$-subspaces in $(R \cap T)^\perp$. Without loss of generality we may assume that $R = \langle e_1, e_2, e_3, e_4 \rangle$ and $T = \langle e_1, e_2, e_3, f_4 \rangle$. Then $(R \cap T)^\perp = \langle e_1, e_2, e_3, e_4, f_4 \rangle$. Let $v \in (R \cap T)^\perp$. Write

$$v = u + \alpha e_4 + \beta f_4,$$

(3.1)

where $u \in \langle e_1, e_2, e_3 \rangle$. Then $Q(v) = \alpha \beta \neq 0$ if and only if $\alpha \neq 0$ and $\beta \neq 0$. Consequently, the number of non-singular vectors in $(R \cap T)^\perp$ is $q^3(q - 1)^2$ and thus, by Lemma 9, the number of $+1$-subspaces in $(R \cap T)^\perp$ is $\frac{1}{3}q^3(q - 1)$. It remains to show that all reflections $r_v$ normalizing $G_0$ are $G_0$-conjugate. This holds if and only if $G_0$ acts transitively on all $+1$-subspaces in $(R \cap T)^\perp$ or, equivalently, on all vectors $v$ with $Q(v) = 1$. Such vectors have form (3.1) with $\alpha \beta = 1$. We show that the vector $w = e_4 + f_4$ is moved by some $g \in G_0$ to any vector $v$ of form (3.1) with $u = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3$ and $\beta = \alpha^{-1}$. Let

$$e_1 g = e_1, \quad f_1 g = -\alpha \alpha_1 e_4 + f_1,$$

$$e_2 g = e_2, \quad f_2 g = -\alpha \alpha_2 e_4 + f_2,$$

$$e_3 g = e_3, \quad f_3 g = -\alpha \alpha_3 e_4 + f_3,$$

$$e_4 g = \alpha \alpha_4, \quad f_4 g = \alpha \alpha_1 e_1 + \alpha \alpha_2 e_2 + \alpha \alpha_3 e_3 + \alpha^{-1} f_4,$$

and extend the action of $g$ to all of $V$ by linearity. It can be seen that $w g = v$ and $Q(x g) = Q(x)$ for all $x \in V$, i.e., $g \in GO^+_U(q)$. It is clear that in fact $g \in SO^+_U(q)$. Since $g |_{R \cap T}$ is the identity mapping, we have $g \in N_{SO^+_U(q)}(U, R \cap T)$. If $q$ is even then $g \in G_0$ by Lemma 10. Suppose that $q$ is odd and $g \in SO^+_U(q) \setminus \Omega$. Consider the linear mapping $g_1 = r_{e_1 + f_1} r_{e_1 + f_1}$. Clearly, $g_1 \in N_{SO^+_U(q)}(U, R \cap T) \setminus \Omega$ and $g_1$ centralizes $w$. Then $g_1 g \in G_0$ is the required element.

2. $G_0$ is an $R_{e_2}$-subgroup. The parabolic subgroup $R_{e_2}$ is the normalizer in $G$ of a totally singular 2-subspace $U \subseteq V$. We may assume that $U = \langle e_1, e_2 \rangle$. Note that the triality involution $r_{e_1 + f_1}$ normalizes $G_0$. As is the case above, we show that $\mathcal{M}(G_0)$ is equal to the number of $+1$-subspaces in $U^\perp$. By Lemma 8, an arbitrary reflection that normalizes $G_0$ is the reflection in a non-singular vector $v \in U^\perp$. Write

$$v = u + \alpha e_3 + \beta f_3 + \gamma e_4 + \delta f_4,$$

(3.2)

where $u \in \langle e_1, e_2 \rangle$. Then $Q(v) = \alpha \beta + \gamma \delta$. Thus there are $q^3(q - 1)^2(q + 1)$ vectors in $U^\perp$ with $Q(v) \neq 0$ and, by Lemma 9, the number of $+1$-subspaces is $\frac{1}{3}q^3(q^2 - 1)$. As above, it remains to show that $G_0 = \mathcal{N}_G(U)$ acts transitively on the vectors (3.2), where $u = \alpha_1 e_1 + \alpha_2 e_2$ and $\alpha \beta + \gamma \delta = 1$. We show that any such vector is the image of $w = e_3 + f_3$ under some element $g \in G_0$. First, find an $h \in \Omega^+_4(q) = \mathcal{O}(e_3, f_3, e_3, f_4)$ such that $(e_3 + f_3) h = \alpha e_3 + \beta f_3 + \gamma e_4 + \delta f_4$. Such an $h$ exists inasmuch as $\Omega^+_4(q)$ acts
transitively on the set of vectors \( v \) with \( Q(v) = 1 \) (see [9], Lemma 2.10.5). Now put

\[
e_1 g = e_1, \quad f_1 g = -\alpha_1 e_3 h + f_1, \\
e_2 g = e_2, \quad f_2 g = -\alpha_2 e_3 h + f_2, \\
e_3 g = e_3 h, \quad f_3 g = \alpha_1 e_1 + \alpha_2 e_2 + f_3 h, \\
e_4 g = e_4 h, \quad f_4 g = f_4 h,
\]

and extend the action of \( g \) to all of \( V \). Clearly, \( g \) stabilizes \( U \), and \( \det g = 1 \). It can be seen that \( Q(xg) = Q(x) \) for all \( x \in V \); thus, \( g \in SO^+_4(q) \). If \( g \) is even then denoting \( T = \langle e_1, e_2, e_3, e_4 \rangle \) and \( T_0 = \langle e_3, e_4 \rangle \) we see that \( \dim (T \cap Tg) = 2 + \dim (T_0 \cap T_0 h) \) is even and thus \( g \in \overline{G_0} \) by Lemma 10. Suppose that \( g \) is odd and \( g \in SO^+_4(q)\). Consider the element \( g_1 = r_{e_1+f_1} r_{e_1+\mu f_1} \). Clearly, \( g_1 \in N_{SO^+_4(q)}(U)\). Consequently, we have an embedding \( \eta : G \to SO^+_4(q) \). Consider the element \( g_1 = r_{e_1+f_1} r_{e_1+\mu f_1} \). Clearly, \( g_1 \in N_{SO^+_4(q)}(U) \) and \( g_1 \) centralizes \( w \). Then \( g_1 g \in \overline{G_0} \) is an element that sends \( w \) to \( v \).

3. \( G_0 \) is an \( N_1 \)-subgroup. By definition, an \( R_{-2} \)-subgroup of \( G \) is the normalizer \( N_G(W) \) of a \(-2\)-subspace \( W \) of \( V \), and an \( F_2 \)-subgroup is a subgroup \( F \subseteq G \) such that \( F \) is the normalizer of an irreducible \( G \)-orbit of \( \Omega \) isomorphic to \( SU_q(q) \). It is known that \( R_{-2} \) and \( F_2 \)-subgroups are isomorphic. If \( K \) is either an \( R_{-2} \)-subgroup or an \( F_2 \)-subgroup then \( \eta(K) \) denotes the unique cyclic normal subgroup of \( K \) of order \( r \), where \( r \) is the largest prime divisor of \((q + 1)/d \). By definition, a subgroup \( N \subseteq G \) is an \( N_1 \)-subgroup if \( N = R \cap F \), with \( R \) an \( R_{-2} \)-subgroup, \( F \) an \( F_2 \)-subgroup, and \( \eta(R), \eta(F) = 1 \).

Suppose that \( W \) is a \( 4 \)-space over \( F_q^2 \) with a non-degenerate unitary form \( k \). Then \( W \) has a basis \( \{w_1, w_2, w_3, w_4\} \) orthonormal with respect to \( k \). Denote \( W_i = \langle w_i \rangle \), \( i = 1, \ldots, 4 \), and \( W_0 = W_1^2 = \langle w_2, w_3, w_4 \rangle \). The space \( W \) can be regarded as an \( 8 \)-space \( W^* \) over \( F \) with quadratic form \( Q^* \) defined by the rule \( Q^*(w) = k(w, w) \) for every \( w \in W^* \). It is known (see [9], Proposition 4.3.18) that \( (W^*, Q^*) \) and \( (V, Q) \) are isometric and thus can be identified. Consequently, we have an embedding \( \varphi : GU_4(q) \rightarrow GO_8^+(q) \).

Let \( N \) be the image under \( \varphi \) of a subgroup in \( GU_4(q) \) isomorphic to \( GU_1(q) \times GU_3(q) \) such that, in a suitable basis of \( V \), \( N \) has the block diagonal form

\[
\begin{pmatrix}
A & \\
& B
\end{pmatrix},
\]

where

\[
A \cong GU_1(q) \leq GO_2^+(q) = GO(W_1^*), \\
B \cong GU_3(q) \leq GO_6^+(q) = GO(W_0^*).
\]

Note that \( A \cong Z_{q+1} \). Denote by \( \eta_1 \) the unique subgroup of \( A \) of order \( r \), where \( r \) is the largest prime divisor of \((q + 1)/d \). Now, define \( N_1 \) to be the subgroup of \( G \) generated by \( N \cap \Omega \) and \( \delta = r_{w_1} r_{w_2} r_{w_3} r_{w_4} \). Let \( N_1 \) be the image of \( N_1 \) in \( G \). We show that \( N_1 \) is an \( N_1 \)-subgroup of \( G \) in the sense of the definition given above.

Clearly, \( N_1 \) lies in the normalizer \( N_G(W_1^*) \) of the \(-2\)-subspace \( W_1^* \), which is an \( R_{-2} \)-subgroup of \( G \), and \( \eta(R) = 1 \). Moreover, \( N_1 \) lies in the \( F_2 \)-subgroup \( F = N_G(SU_4(q)v) \) and \( \eta_2 = \eta(F) \) is the cyclic subgroup of order \( r \) in \( \mathbb{Z}^* \), where \( Z = Z(GU_4(q)) \). It can be seen that \( |\eta_1, \eta_2| = 1 \) which implies that \( N_1 \) is contained in the \( N_1 \)-subgroup \( R \cap F \). The equality follows from the coincidence of the orders of these subgroups. We thus may assume that \( G_0 \) is the subgroup \( N_1 \) constructed above.

Since the reflection \( r_{w_1} \) normalizes \( N \) and \( \Omega \), and centralizes \( \delta \); it follows that the triality involution \( \overline{r_{w_1}} \) normalizes \( G_0 \). We have \( [\overline{G_0} : C_{\overline{G_0}}(r_{w_1})] = [N : C_N(r_{w_1})] = [A : C_A(r_{w_1})] \) and, since \( [A, r_{w_1}] \cong D_{2(q+1)} \), this index is equal to \((q + 1)/d \).
We now show $\widetilde{G}_0$-conjugacy of all reflections $r_v$ that normalize $\widetilde{G}_0$. Since any such reflection normalizes $N$, it suffices to show that all $r_v$'s normalizing $N$ lie in $\langle A, r_w \rangle$.

Suppose that $r_v = r_w$ normalizes $N$. Note that $W^*_0$ and $W^*_1$ are the unique $N$-invariant 6- and 2-subspaces of $V$, respectively. Since the subspace $W^*_i r_v$, $i = 0, 1$, is $N$-invariant, we have $W^*_i r_v = W^*_i$. Lemma 8 now implies that $v \in W^*_i$ for $i = 0$ or $i = 1$. If $v \in W^*_i$ then $r_v \in \langle A, r_w \rangle$. It remains to show that there exists no $v \in W^*_0$ such that $r_v$ would normalize $N$ or, equivalently, there is no $r_v$ in $GO(W^*_0)$ that would normalize $B \cong GU_3(q) \leq GO^+_6(q) = GO(W^*_0)$.

Suppose, by way of contradiction, that $r_v$ is such a reflection. The group $GO^+_6(q)$ is naturally embedded into the group $GO^+_0(q^2)$ of orthogonal transformations of the vector space $U = W^*_0 \otimes F_{q^2}$ with quadratic form $K$ such that $K|_{W^*_0} = Q^*$. (We regard $W^*_0$ as a subset of $U$. See the remarks after Proposition 2.8.1 in [9].) Note that $r_v$ can be extended to a reflection of $U$. There exists a decomposition $U = U_1 + U_2$ of $U$ into the direct sum of two totally singular 3-subspaces such that every element of $B$ has the block diagonal form

$$\begin{pmatrix} b & \cdot \\ \cdot & b^\# \end{pmatrix}$$

with respect to this decomposition, where $b^\#$ is the image of $b$ under the matrix Frobenius map, corresponding to the map $[x \rightarrow x^q]$ of $F_{q^2}$. The $B$-submodules $U_1$ and $U_2$ of $U$ are irreducible and non-isomorphic. Since $U_i r_v$ is a $B$-submodule of $U$ isomorphic to $U_i$, it follows that $r_v$ normalizes $U_i$, $i = 1, 2$. By Lemma 8, $v \in U_1$ or $v \in U_2$. This contradicts the fact that $U_1$ and $U_2$ are totally singular.

4. $G_0$ is an $N_2$-subgroup. In this case, assume $q \geq 4$.

By definition, an $R_{+2}$-subgroup of $G$ is the normalizer $N_G(W)$ of a +2-subspace $W$ of $V$, and an $I_{+4}$-subgroup is the stabilizer of a decomposition of $V$ into the direct sum of two totally singular 4-subspaces. It is known that $R_{+2}$- and $I_{+4}$-subgroups are isomorphic. If $K$ is either an $R_{+2}$-subgroup or an $I_{+4}$-subgroup then $\eta(K)$ denotes the unique cyclic normal subgroup of $K$ of order $r$, where $r$ is the largest prime divisor of $(q - 1)/d$. By definition, a subgroup $N \leq G$ is an $N_2$-subgroup if $N = R \cap I$, with $R$ an $R_{+2}$ subgroup, $I$ an $I_{+4}$-subgroup, and $[\eta(R), \eta(I)] = 1$.

Take a matrix $c \in GL_4(q)$ and consider the linear transformation of $V$ that, in the standard basis $(e_1, \ldots, e_4, f_1 \ldots f_4)$, has the matrix

$$\begin{pmatrix} c & c^{-T} \\ \cdot & \cdot \end{pmatrix},$$

where $c^{-T}$ denotes the inverse-transpose of $c$. Clearly, this is an element of $GO^+_4(q)$ and thus we have an embedding $\varphi : GL_4(q) \hookrightarrow GO^+_4(q)$.

Let $N$ be the image under $\varphi$ of a subgroup in $GL_4(q)$ isomorphic to $GL_3(q) \times GL_4(q)$ such that, in a suitable basis of $V$, $N$ has the block diagonal form

$$\begin{pmatrix} A & \cdot \\ \cdot & B \end{pmatrix},$$

where

$$A \cong GL_3(q) \leq GO^+_2(q) = GO(V_1),$$

$$B \cong GL_3(q) \leq GO^+_6(q) = GO(V_0),$$
with $V_1 = \langle e_1, f_1 \rangle$ and $V_0 = V_1^\perp$. Note that $A \cong Z_{q-1}$. Denote by $n_1$ the unique subgroup of $\Omega$ of order $r$, where $r$ is the largest prime divisor of $(q-1)/d$. Now, define $N_2$ to be the subgroup of $\Omega$ generated by $N \cap \Omega$ and $\delta = r_1, r_2, r_3, r_4$, where $w_i = e_i + f_i$, $i = 1, \ldots, 4$.

Let $N_2$ be the image of $N_2$ in $G$. It is not difficult to show that $N_2$ is an $N_2$-subgroup of $G$ in the sense of the above definition. We thus may assume that $G_0$ is the subgroup $N_2$ constructed above. As in the previous case, it can be shown that the triality involution $r_{w_i}$ normalizes $G_0$ and that $[G_0 : C_{G_0}(r_{w_i})] = |A : C_A(r_{w_i})| = (q-1)/d$. The conjugacy of the triality involutions in $G_0(\langle r_{w_i} \rangle)$ is also verified in a similar way. Namely, we only need to show that there exists no $r_v$ in $GO(V_0)$ that would normalize $B \cong GL_3(q) \leq GO^+_6(q) = GO(V_0)$. This, however, also follows from the fact that $V_0$ decomposes into the direct sum $V_0 = U_1 + U_2$ of two totally singular 3-subspaces $U_1 = \langle e_2, e_3, e_4 \rangle$ and $U_2 = \langle f_2, f_3, f_4 \rangle$ which are non-isomorphic irreducible $B$-submodules of $V_0$.

5. $G_0$ is an $N_3$-subgroup. By definition, an $N_3$-subgroup of $G$ is the normalizer of a Sylow $r$-subgroup of $G$, where $r$ is an odd prime divisor of $q^2 - 1$. We show that no triality involution normalizes $G_0$. Suppose, by way of contradiction, that $\pi_G$ is such an involution. Then $r_v$ normalizes a Sylow $r$-subgroup $R_v$ in $\Omega$. There exists a decomposition $V = V_1 + V_2$, where $V_1$ and $V_2 = V_1^\perp$ are $-4$-subspaces of $V$, such that $R_v \subseteq N \cap \Omega = \Omega_v$. By Lemma 12 and 8, $v \in V_i$, with $i = 1$ or $i = 2$. In particular, $r_v$ normalizes a Sylow $r$-subgroup $R_v \subseteq \Omega_v$ of order 8. Since $\Omega_v \cong PGL_2(q)$, we may assume by Lemma 11 that, in the group $L_2(q^2) / \langle \lambda \rangle$, $\lambda$ normalizes a Sylow $r$-subgroup or, equivalently, the field automorphism $\lambda$ of order 2 normalizes a Sylow $r$-subgroup $X = \langle x \rangle$, with $|x| = r$. This implies that $x^\lambda = x$ or $x^\lambda = x^{-1}$. Let $\theta$ and $\theta^{-1}$ be the characteristic roots of $x$. Note that $\theta^{q - 1} \neq 1$, since otherwise $\theta^{q - 1} = 1$ and $\theta^{q + 1} = 1$ would imply that $x^2 = 1$, contrary to the fact that $r$ is odd. Since the characteristic roots of $x^\lambda$ are $\theta$ and $\theta^{-q}$, we have $\{\theta, \theta^{-q}\}$ is a non-trivial subgroup of $\Omega$, which implies $\theta^q = \theta$ and $\theta^{q + 1} = 1$. In either case, $\theta^{q + 1} = 1$, a contradiction.

6. $G_0$ is an $N_2$-subgroup. Suppose that $q = p$ is an odd prime. Choose a basis $v = (v_1, \ldots, v_8)$ of $V$ such that $(v_i, v_j) = 0$, $i \neq j$, and $Q(v_i) = 1$ for $i = 1, \ldots, 8$. An $N_2$-subgroup is conjugate in $G$ to the normalizer $N_G(P)$ of the subgroup $P$ of order 8 generated by the involutions $\pi, \pi, \pi$, where

$$
x = \text{diag}_q(1, 1, 1, 1, -1, -1, -1, -1),
y = \text{diag}_q(1, 1, -1, -1, 1, 1, -1, -1),
z = \text{diag}_q(1, -1, -1, -1, 1, 1, 1, 1)
$$

are elements of $\Omega$. We assume that $G_0 = N_G(P)$. Notice that $\hat{P} = \langle -1, x, y, z \rangle$, where $-1$ is the central involution of $\Omega$, and that $\hat{N}_G(P)$ consists of monomial matrices.

We prove that the only reflections $r_{v_i}$ that normalize $\hat{P}$ are $r_{v_i}$, $i = 1, \ldots, 8$. Since these reflections are $G_0$-conjugate (which follows from the fact that $G_0$ acts transitively on the vectors $v_i$), this will imply that $|M(G_0)| = 8$.

Let $r_v = r_{v_i}$ normalize $\hat{P}$. Then $r_v$ either normalizes each $+1$-subspace $(v_i)$, $i = 1, \ldots, 8$, or permutes two of them while centralizing the others. In the former case, Lemma 8 implies that $v = v_i$ for some $i$ and we show that the latter case is impossible. Suppose, to the contrary, that $1 \leq i < j \leq 8$ are such that $(v_i) r_v = (v_j)$. We make two observations about every matrix $g \in \hat{P}$:

(i) the number of $-1$'s in $(g_{11}, g_{22}, g_{33}, g_{44})$ is even and so is the number of $-1$'s in $(g_{55}, g_{66}, g_{77}, g_{88})$. 

Lagrange's theorem for Moufang Loops
(ii) \((g_{11}, g_{22}, g_{33}, g_{44}) = \pm (g_{55}, g_{66}, g_{77}, g_{88})\).

By (i), it follows that either \(1 \leq i < j \leq 4\) or \(5 \leq i < j \leq 6\), since otherwise \(x^{i}x^{j} \not\in \tilde{P}\).

Without loss assume that \(1 \leq i < j \leq 4\). Clearly, there is a \(g \in \tilde{P}\) with \(g_{ii} \neq g_{jj}\). But then the matrices \(g\) and \(g^{r}\) have all entries equal except for those at positions \((i,i)\) and \((j,j)\). This, however, contradicts (ii) which says that the upper four diagonal entries of every element in \(\tilde{P}\) are uniquely determined by the lower four entries and one arbitrary upper diagonal one.

\textbf{7-8.} \(G_{0}\) is an \(I_{22}\)-subgroup, \(\varepsilon = \pm 1\). An \(I_{22}\)-subgroup \(G_{0}\) is the normalizer in \(G\) of a decomposition \(V = V_{1} + \ldots + V_{4}\) of \(V\) into the direct sum of pairwise orthogonal \(\varepsilon\)-subspaces \(V_{i}, i = 1, \ldots, 4\). A reflections \(r_{v} = r_{\square}\) normalizes \(\tilde{G}_{0}\) if and only if it normalizes the set \(\{V_{1}, \ldots, V_{4}\}\). By Lemma 12, \(r_{v}\) centralizes this set. By Lemma 8, \(v \in V_{i}\) for some \(i\). By Lemma 5, the number of +1-subspaces of \(V_{i}\) is \(\frac{1}{2}(q - \varepsilon)\). Thus there are \(\frac{1}{2}(q - \varepsilon)\) reflections of form \(r_{\square}\) that normalize \(\{V_{1}, \ldots, V_{4}\}\). They are all \(\tilde{G}_{0}\)-conjugate since \(\tilde{G}_{0}\) permutes transitively the subspaces \(V_{i}\)’s and the +1-subspaces inside each \(V_{i}\) (see [9], Proposition 4.2.11).

\textbf{9.} \(G_{0}\) is an \(I_{44}\)-subgroup. An \(I_{44}\)-subgroup \(G_{0}\) is the normalizer in \(G\) of a decomposition \(V = V_{1} + V_{2}\) of \(V\) into the orthogonal sum of two +4-subspaces. As above, a reflections \(r_{v} = r_{\hat{v}}\) normalizes \(\tilde{G}_{0}\) if and only if \(v \in V_{i}\) for \(i = 1\) or \(i = 2\). By Lemma 5, the number of +1-subspaces of \(V_{i}\) is \(\frac{1}{2}(q - \varepsilon)\). Thus there are \(\frac{1}{2}(q - \varepsilon)\) reflections of form \(r_{\square}\) that normalize \(\{V_{1}, V_{2}\}\). They are all \(\tilde{G}_{0}\)-conjugate for the same reasons as in the case above.

\textbf{10.} \(G_{0}\) is a \(G_{2,2}\)-subgroup. A \(G_{2,2}\)-subgroup is a subgroup \(G_{0}\) of \(G\) isomorphic to \(G_{2}(q)\) and such that \(G_{N_{GS}}(G_{0}) = GS\). By Proposition 3.1.1 in [8], we may assume that \(G_{0} = C_{G}(S)\); thus, \(G_{0}\) is a group with trivial triality relative to \(S\). The fact that \(G_{0}S\) contains no other triality \(S_{3}\)-complements follows from Lemma 4. Therefore, the Moufang loop \(\mathcal{M}(G_{0})\) is trivial.

\textbf{11.} \(G_{0}\) is a \(PO_{8}^{+}(2)\)-subgroup. Consider a rational 8-dimensional vector space \(W\) with a basis \(w = \{w_{1}, \ldots, w_{8}\}\) orthonormal with respect to some non-degenerate quadratic form \(K: W \rightarrow \Omega\). It can be proven (e.g., using \textsc{GAP} [6]) that the linear mappings of \(W\) that have matrices

\[
A = \begin{pmatrix}
-1 & & & & & & & \\
& 1 & & & & & & \\
& & 1 & & & & & \\
& & & 1 & & & & \\
& & & & 1 & & & \\
& & & & & 1 & & \\
& & & & & & 1 & \\
& & & & & & & 1
\end{pmatrix}, \quad B = \frac{1}{2} \begin{pmatrix}
1 & & & & & & & \\
& -1 & & & & & & \\
& & 1 & & & & & \\
& & & 1 & & & & \\
& & & & -1 & & & \\
& & & & & -1 & & \\
& & & & & & -1 & \\
& & & & & & & 1
\end{pmatrix},
\]

in the basis \(w\) generate a subgroup of \(GL(W, \Omega)\) isomorphic to the bicyclic extension \(2 \cdot PO_{8}^{+}(2)\cdot 2\). Note that \(A\) is the matrix of the reflection \(r_{w_{1}+w_{2}}\) of \(W\). Moreover, \(AA^{T} = BB^{T} = E\), i.e., these mappings respect the above quadratic form \(K\). Now suppose that \(q = p\) is an odd prime. Choose a basis \(\{u_{1}, \ldots, u_{8}\}\) of \(V\) which is orthonormal, i.e., such that \((u_{i}, u_{j}) = 0, i \neq j\), and \((u_{i}, u_{i}) = 1\) for \(i = 1, \ldots, 8\). Then \(r_{u_{1}+u_{2}}\) has form \(r_{\square}\), the \(p\)-reduced matrices \(A_{p}\) and \(B_{p}\) lie in \(GO_{8}^{+}(p)\), and \(A_{p}\) is the matrix of \(r_{u_{1}+u_{2}}\). Denote \(\tilde{G}_{0} = \langle A_{p}, B_{p} \rangle \cong 2 \cdot PO_{8}^{+}(2)\). It is clear that \(\tilde{G}_{0}\) lies in \(\Omega\) and its image \(G_{0}\) in \(G\) is an \(PO_{8}^{+}(2)\)-subgroup normalized by the triality involution \(r_{w_{1}+w_{2}}\). By Lemma 7, assume that \(G_{0}\) is \(S\)-invariant. Lemma 4 now implies that there is a unique subloop of
M corresponding to $PΩ^+_8(2)$-subgroups of $G$ whose order is $|M(2)|$. We remark that a computer-free proof of the embedding $PΩ^+_8(2) → PΩ^+_8(p)$ can be obtained using the fact that the group $2.PΩ^+_8(2).2$ is isomorphic to the Weyl group of the root system of type $E_8$.

12-13. $G_0$ is a $PΩ^+_8(q_0)$- or a $PΩ^+_8(q_0).2$-subgroup. Suppose that $q = q_0^k$, with $k$ prime. First, let $(d, k) = 1$. In $G$, there exists a maximal subgroup $G_0$ isomorphic to $PΩ^+_8(q_0)$ which is $S$-invariant. Clearly, $M(G_0) ∼= M(q_0)$. Now let $d = k = 2$; in particular, $q$ is odd. Then $λ = μ^2$ is a non-square in $F_{q_0}$. Let $H$ be a natural copy of $Ω^+_8(q_0)$ in $Ω$ that acts on the $F_{q_0}$-subspace $V_0$ of $V$ spanned by the standard basis $v = (e_1, \ldots, f_4)$ and respects the quadratic form $Q_0 = Q|_{V_0}$. Define

$$b = \text{diag}_{θ}(μ, μ, μ, μ, μ^{-1}, μ^{-1}, μ^{-1}, μ^{-1}),$$

$$c = \text{diag}_{θ}(λ^{-1}, 1, 1, 1, λ, 1, 1, 1).$$

Note that $b, c ∈ Ω$ and $c = r_{e_1+f_1}r_{e_1+λf_1}$. We assume that $G_0 = N_G(HT) = \langle HT, t, r \rangle ∼= \text{InnDiag}(PΩ^+_8(q_0))$, i.e. the group of inner-diagonal automorphisms of $PΩ^+_8(q_0)$ (see [8], Proposition 2.2.9). The group $G_0$ is normalized by the triality involution $τ_v$, where $v = e_1 + f_1$. Moreover, since $H^{τ_v} = H$, $e^{τ_v} = e^{-1}$, and $b^{τ_v} = bc$, it follows that $C_{G_0}(τ_v) ≤ ⟨HT, r⟩$. Note that the coset $HT$ contains an element $τ$ that commutes with $τ_v$ (put, for instance, $a = r_{e_2+f_2}r_{e_2+λf_2}$). Therefore, $|G_0 : C_{G_0}(τ_v)| = |HT : C_{HT}(τ)| = 2|M(q_0)|$. The conjugacy of triality $S_3$-complements in $G_0S$ follows from Lemma 4.

14. $G_0$ is a $\text{PGL}_3(q)$-subgroup. Suppose that $q ∼= ε(\text{mod } 3)$, $ε = ±1$. Then $G$ contains a maximal subgroup $G_0$ isomorphic to $\text{PGL}_3(q)$. If $G_0$ were $S$-invariant then, by Lemma 4, the subgroup of $G_0$ isomorphic to $L_3(q)$ would have trivial triality relative to $S$. But then $G_0$ would be a subgroup of $C_G(ρ) ∼= G_2(q)$, which contradicts maximality of $G_0$.

We can now make the concluding remarks. As was explained in the introduction, we only need to check whether the orders of maximal subloops of $M(q)$ divide $|M(q)|$. The group $PΩ^+_8(q)$ being simple satisfies the conditions of Corollary 1. Hence, all maximal subloops of $M(q) = M(PΩ^+_8(q))$ have form $M(G_0)$ for certain $S$-maximal subgroups $G_0$ of $PΩ^+_8(q)$. By Theorem 2, the orders $|M(G_0)|$ for all $S$-maximal subgroups $G_0$ are listed in column $V$ of Table 1. Since they all divide $|M(q)|$, Lagrange’s theorem holds.

Acknowledgements. The authors are thankful to professor V. D. Mazurov for the discussion of the content of this paper and to the reviewer for many useful remarks that allowed us to improve the exposition.

REFERENCES


