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 $M(q) = PSL(\mathbf{O}(q))$, where $\mathbf{O}(q)$ 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

[**8**] of maximal subgroups in the automorphism groups of $P\Omega_8^+(q)$ to find the possible candidates for G_0 and then determine the order of the corresponding subloops of $M(q)$. 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 V be a vector space of dimension 2 over the field $\boldsymbol{F}_3$ of three elements and let $e \notin V$ be a symbol. Define on the set $L = V \cup \{e\}$ the structure of a diassociative loop as follows. Put $e \cdot x = x \cdot e = x$ for every $x \in L$, $v^2 = e$ for every $v \in V$, and $v \cdot w = u$ whenever $v, w \in V$, $v \neq w$, and $\{v, w, u\}$ is an affine line in V. Clearly, $|L| = 10$ and, for distinct elements v and w of V, the set $\{e, v, w, v \cdot w\}$ is a subgroup of L of order 4. This is an example of a Steiner loop (see p. 23 in [**5**]).

A loop M is called a *right Bol* loop if the identity $(xy \cdot z)y = x(yz \cdot y)$ holds for all $x, y, z \in M$. The class of Moufang loops is exactly the intersection of the classes of diassociative and right Bol loops. We mention here that a counterexample to Lagrange's theorem among the right Bol loops is not known to the authors.

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

$$[x, \sigma] \cdot [x, \sigma]^{\rho} \cdot [x, \sigma]^{\rho^2} = 1, \tag{2·1}$$

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 ρ and σ of S (see [**4**]) and we will thus speak of a group with triality S. This fact, together with Lemma $3 \cdot 2$ in [**10**], implies

Lemma 1. *The condition (2·1) is equivalent to* $[x\rho, \sigma]^3 = 1$ *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 $P \leqslant Q$ ($P \trianglelefteq Q$). 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

$$\xi(g) = g^{-1}g^{\sigma} = [g, \sigma], \qquad \phi(g) = g^{-\rho}g^{\rho^2}, \qquad \eta(g) = gg^{-\rho\sigma}g^{\rho^2} = g[g, \sigma]^{-\rho^2}.$$

Also, put $M = \xi(G)$ and $H = C_G(\sigma)$. Observe that

$$m^\sigma = m^{-1} \in M \quad \text{for all} \quad m \in M. \tag{2·2}$$

LEMMA 2. *In the above notation, we have:*
(i) $n^{-\rho^2}mn^{-\rho} = m^{-\rho}nm^{-\rho^2} \in M \quad \forall\, m, n \in M$,
(ii) $[m, m^\rho] = [m, m^{\rho^2}] = [m^\rho, m^{\rho^2}] = 1 \quad \forall\, m \in M$,
(iii) $[m^\rho, n^{-\rho^2}] = [m^{-\rho^2}, n^\rho] \in H \quad \forall\, m, n \in M$,
(iv) $\eta(g) \in H \quad \forall\, g \in G$,
(v) $\phi(H) \subseteq M$, $\phi(M) \subseteq H$.

Proof. (i) By (2·1) and (2·2), we have $\xi(m^{\rho^2}n^{\rho^2}) = n^{-\rho^2}m^{-\rho^2}m^{\sigma\rho}n^{\sigma\rho} = n^{-\rho^2}m^{-\rho^2}m^{-\rho}n^{-\rho} = n^{-\rho^2}mn^{-\rho} \in M$ for all $m, n \in M$. Moreover, (2·1) also implies $n^{-\rho^2}mn^{-\rho}(n^{-\rho^2}mn^{-\rho})^\rho(n^{-\rho^2}mn^{-\rho})^{\rho^2} = n^{-\rho^2}mn^{\rho^2}m^\rho nm^{\rho^2}n^{-1} = 1$.
Conjugating this equality by n, we obtain $n^{-1}n^{-\rho^2}mn^{\rho^2}m^\rho nm^{\rho^2} = n^\rho mn^{\rho^2}m^\rho nm^{\rho^2} = 1$ for all $m, n \in M$. Replacing m by m^{-1}, we have $n^{-\rho^2}mn^{-\rho} = m^{-\rho}nm^{-\rho^2}$.

(ii) For every $m \in M$, we have $mm^\rho m^{\rho^2} = 1$ by (2·1). Using (2·2), we obtain $1 = m^\sigma m^{\rho\sigma}m^{\rho^2\sigma} = m^{-1}m^{-\rho^2}m^{-\rho}$. Replacing m by m^{-1}, we have $mm^{\rho^2}m^\rho = mm^\rho m^{\rho^2}$; therefore, $[m^\rho, m^{\rho^2}] = 1$.

(iii) Let $m, n \in M$. Then, by item (i), we have $n^{-\rho^2}m^{-1}n^{-\rho} = m^\rho nm^{\rho^2}$. Applying ρ^2 to this equality, we have $n^{-\rho}m^{-\rho^2}n^{-1} = mn^{\rho^2}m^\rho$. This, together with (2·1), implies $n^{-\rho}m^{-\rho^2}n^\rho n^{\rho^2} = m^{-\rho^2}m^{-\rho}n^{\rho^2}m^\rho$; hence, $m^{\rho^2}n^{-\rho}m^{-\rho^2}n^\rho = m^{-\rho}n^{\rho^2}m^\rho n^{-\rho^2}$, i.e., $[m^{-\rho^2}, n^\rho] = [m^\rho, n^{-\rho^2}]$. We also have by (2·2) $[m^\rho, n^{-\rho^2}]^\sigma = [m^{\rho\sigma}, n^{-\rho^2\sigma}] = [m^{-\rho^2}, n^\rho] = [m^\rho, n^{-\rho^2}]$. Therefore, $[m^\rho, n^{-\rho^2}] \in H$.

(iv) $\eta(g)^\sigma = g^\sigma g^{-\rho}g^{\sigma\rho} = g(g^{-1}g^\sigma)(g^{-1}g^\sigma)^\rho = g(g^{-1}g^\sigma)^{-\rho^2} = gg^{-\rho\sigma}g^{\rho^2} = \eta(g)$.

(v) Let h and m be elements of H and M, respectively. Then (2·2) and (ii) imply $\phi(m)^\sigma = m^{-\rho\sigma}m^{\rho^2\sigma} = m^{\rho^2}m^{-\rho} = m^{-\rho}m^{\rho^2} = \phi(m) \in H$.
$\xi(\phi(h)^{\rho^2}) = \xi(h^{-1}h^\rho) = h^{-\rho}hh^{-\sigma}h^{\sigma\rho^2} = h^{-\rho}h^{\rho^2} = \phi(h) \in M$. □

By item (iv) of this lemma, every $g \in G$ admits the decomposition $g = \eta(g)\xi(g)^{\rho^2}$ with $\eta(g) \in H$ and $\xi(g) \in M$. In particular, for all $m, n \in M$, we have by item (i)

$$m^{\rho^2}n^{\rho^2} = \eta(m^{\rho^2}n^{\rho^2})\xi(m^{\rho^2}n^{\rho^2})^{\rho^2} = [m^{-\rho^2}, n^\rho](m^{-\rho}nm^{-\rho^2})^{\rho^2}. \tag{2·3}$$

Let G be an arbitrary group with triality. It was shown in Lemma 1 of [**4**] that the set M^{ρ^2} is a right transversal of H in G. For $g \in G$, we define $\pi(g)$ to be the unique element of M^{ρ^2} such that $\pi(g)g^{-1} \in H$. Then the composition $m_1 \cdot m_2 = \pi(m_1m_2)$ endows M^{ρ^2} with the structure of a Moufang loop (see Theorem 1 in [**4**]). By (2·3), the mapping $m \mapsto m^{\rho^2}$ for $m \in M$ is an isomorphism of loops $(M, .\,) \cong (M^{\rho^2}, \cdot\,)$, where, by definition,

$$m.n = m^{-\rho}nm^{-\rho^2} \quad \text{for all} \quad n, m \in M. \tag{2·4}$$

We denote the loop (M, .) by $\mathcal{M}(G)$ and note that $|\mathcal{M}(G)| = |G : H|$. The relation (2·4) implies that the identity of $\mathcal{M}(G)$ coincides with the identity of G and, for every $m \in \mathcal{M}(G)$, taking the inverse m^{-1} or any power m^t is the same whether considered in $\mathcal{M}(G)$ 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 $\mathcal{M}(G_0)$ is a subloop of $M = \mathcal{M}(G)$. 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 $\mathcal{M}(G_1) \leqslant \mathcal{M}(G_2)$ for the corresponding loops. It is possible however that two distinct S-subgroups of G give rise to the same subloop of M.

Lemma 3. *Let* $m, n, k \in M$ *then*
(i) $m^{-1}.n.m = h^{-1}nh$, *where* $h = \phi(m) \in H$,
(ii) $((k.m).n).(m.n)^{-1} = h^{-1}kh$, *where* $h = [m^\rho, n^{-\rho^2}] \in H$
(iii) $m^{-1}.n^{-1}.m.n = \phi([m^\rho, n^{-\rho^2}]) \in M$.

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:

$$x.y = y^{-\rho^2}xy^{-\rho} \quad \text{for all} \quad x, y \in M. \tag{2·5}$$

Using it, we have $m^{-1}.n.m = m^{-1}.(m^{-\rho^2}nm^{-\rho}) = m^\rho m^{-\rho^2}nm^{-\rho}m^{\rho^2}$ for all $n \in M$. We also have $h^{-1}nh = m^{-\rho^2}m^\rho nm^{-\rho}m^{\rho^2}$. The claim follows, since $m^\rho m^{-\rho^2} = m^{-\rho^2}m^\rho$ by (ii) of Lemma (2).

(ii) For $m, n, k \in M$, we have by (2·5)
$((k.m).n)(m.n)^{-1} = ((m^{-\rho^2}km^{-\rho}).n).(n^{-\rho^2}mn^{-\rho})^{-1} =$
$(n^{-\rho^2}m^{-\rho^2}km^{-\rho}n^{-\rho}).(n^\rho m^{-1}n^{\rho^2}) =$
$(n^\rho m^{-1}n^{\rho^2})^{-\rho^2}n^{-\rho^2}m^{-\rho^2}km^{-\rho}n^{-\rho}(n^\rho m^{-1}n^{\rho^2})^{-\rho} =$
$n^{-\rho}m^{\rho^2}(n^{-1}n^{-\rho^2})m^{-\rho^2}km^{-\rho}(n^{-\rho}n^{-1})m^\rho n^{-\rho^2} =$
$n^{-\rho}m^{\rho^2}n^\rho m^{-\rho^2}km^{-\rho}n^{\rho^2}m^\rho n^{-\rho^2} = [n^\rho, m^{-\rho^2}]k[m^\rho, n^{-\rho^2}]$.
On the other hand, $h^{-1}kh = [n^{-\rho^2}, m^\rho]k[m^\rho, n^{-\rho^2}]$.
However, Lemma 2 (iv) implies $[n^\rho, m^{-\rho^2}] = [n^{-\rho^2}, m^\rho]$.

(iii) Using (2·5), (2·1) and (ii),(iii) of Lemma 2, we have
$m^{-1}.n^{-1}.m.n = (m^{-1}.n^{-1}).(m.n) = (n^{\rho^2}m^{-1}n^\rho).(n^{-\rho^2}mn^{-\rho}) =$
$(n^{-\rho^2}mn^{-\rho})^{-\rho^2}(n^{\rho^2}m^{-1}n^\rho)(n^{-\rho^2}mn^{-\rho})^{-\rho} = nm^{-\rho^2}(n^\rho n^{\rho^2})m^{-1}(n^\rho n^{\rho^2})m^{-\rho}n =$
$nm^{-\rho^2}n^{-1}m^{-1}n^{-1}m^{-\rho}n = nm^{-\rho^2}n^{-1}m^{\rho^2}(m^{-\rho^2}m^{-1}m^{-\rho})m^\rho n^{-1}m^{-\rho}n =$
$[n^{-1}, m^{\rho^2}][m^{-\rho}, n] = [m^\rho, n^{-\rho^2}]^{-\rho}[m^{-\rho^2}, n^\rho]^{\rho^2} =$
$[m^\rho, n^{-\rho^2}]^{-\rho}[m^\rho, n^{-\rho^2}]^{\rho^2} = \phi([m^\rho, n^{-\rho^2}])$. □

Theorem 1. *Let* G *be a group with triality* $S = \langle \rho, \sigma \rangle$, $G = HM^{\rho^2}$, *where* $H = C_G(\sigma)$ *and* $M = \{[g, \sigma] \mid g \in G\}$, *and let* $\mathcal{M}(G) = (M, .)$ *be the corresponding Moufang loop. Then, for every subloop* $P \leqslant \mathcal{M}(G)$, *there exists an* S-*subgroup* $Q \leqslant G$ *such that* $\mathcal{M}(Q) = P$. *Moreover,*
(i) *if* G_0 *is the* S-*subgroup generated by* M *then* $G_0 \trianglelefteq G$,
(ii) *if* $G_1 \leqslant G_0$ *is an* S-*subgroup such that* $\mathcal{M}(G_1) = \mathcal{M}(G_0)$, *then* $G_1 = G_0$.

Proof. Let $P \leqslant M$ be a subloop, which means that $P \subseteq M$ and, for $m, n \in P$, $m.n = m^{-\rho}nm^{-\rho^2} \in P$. We denote by Q the subgroup of G generated by $P \cup P^\rho \cup P^{\rho^2}$. It is clear that Q is ρ-invariant. Also, (2·2) implies

$$P^\sigma = P, \quad (P^\rho)^\sigma = P^{\rho^2}, \quad (P^{\rho^2})^\sigma = P^\rho.$$

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 $T = \{m^{-\rho}m^{\rho^2}, [m^\rho, n^{-\rho^2}] \mid m, n \in P\}$. By (iii) and (v) of Lemma 2, $H_0 \subseteq H$. Denote $Q_0 = H_0P^{\rho^2}$ and prove that $Q = Q_0$. This will imply that

$$\mathcal{M}(Q) = \mathcal{M}(Q_0) = \xi(Q_0) = \{\, \xi(hp^{\rho^2}) \mid h \in H_0, p \in P \,\}.$$

However, $\xi(hp^{\rho^2}) = p^{-\rho^2}h^{-1}h^{\sigma}p^{\rho^2\sigma} = p^{-\rho^2}h^{-1}hp^{\sigma\rho} = p^{-\rho^2}p^{-\rho} = p$ by (2·1). Therefore, we will have $\mathcal{M}(Q) = P$ 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

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

Now, for $m \in P$, we also have $m^{\rho} = (m^{\rho}m^{-\rho^2})m^{\rho^2} \in Q_0$ and $m^{\rho^2} \in Q_0$ by definition. Therefore, $P \cup P^{\rho} \cup P^{\rho^2} \subseteq Q_0$. 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,

$$P^h = P \quad \text{for all} \quad h \in H_0. \tag{2·6}$$

First, show that

$$\phi(H_0) \subseteq P. \tag{2·7}$$

Let $a, b \in H_0$ and suppose that $\phi(a), \phi(b) \in P$. Then
$\phi(ab) = (ab)^{-\rho}(ab)^{\rho^2} = b^{-\rho}(a^{-\rho}a^{\rho^2})b^{\rho^2} = (b^{-\rho}b)b^{-1}\phi(a)b(b^{-1}b^{\rho^2}) =$
$(b^{-\rho}b^{\rho^2})^{-\rho^2}\phi(a)^b(b^{-\rho}b^{\rho^2})^{-\rho} = \phi(a)^b.\phi(b) \in P$ by (2·6).
Hence, it suffices to prove that $\phi(m^{-\rho}m^{\rho^2}) \in P$ and $\phi([m^{\rho}, n^{-\rho^2}]) \in P$. We have
$\phi(m^{-\rho}m^{\rho^2}) = m^{-1}m^{\rho^2}m^{-1}m^{\rho} = m^{-3} \in P$, and
$\phi([m^{\rho}, n^{-\rho^2}]) = m^{-1}.n^{-1}.m.n \in P$ by (iii) of Lemma 3. This shows that (2·7) holds.
Now we can prove that $Q_0 = H_0P^{\rho^2}$ is a subgroup. Let $m^{\rho^2}, n^{\rho^2} \in P^{\rho^2}$. Then, by (2·3),

$$m^{\rho^2}n^{\rho^2} = [m^{\rho}, n^{-\rho^2}](m.n)^{\rho^2}. \tag{2·8}$$

Hence, $m^{\rho^2}n^{\rho^2} \in Q_0$. Let $h \in H_0$, $m \in P$. Then we have
$m^{\rho^2}h = \eta(m^{\rho^2}h)\xi(m^{\rho^2}h)^{\rho^2} = h_1m_1^{\rho^2}$, where
$m_1 = \xi(m^{\rho^2}h) = h^{-1}m^{-\rho^2}m^{-\rho}h^{\sigma} = m^h \in P$ by (2·6), and
$h_1 = \eta(m^{\rho^2}h) = m^{\rho^2}hh^{-\rho\sigma}m^{-\sigma}m^{\rho}h^{\rho^2} = m^{\rho^2}hh^{-\rho^2}m^{-\rho^2}h^{\rho^2} = m^{\rho^2}h(m^h)^{-\rho^2} =$
$h(h^{-1}h^{\rho^2})(h^{-\rho^2}m^{\rho^2}h^{\rho^2})(h^{-\rho^2}h)(m^h)^{-\rho^2} = h[h^{-\rho^2}h, (m^h)^{-\rho^2}] =$
$h[\phi(h)^{\rho}, (m^h)^{-\rho^2}] \in H_0$ by (2·6) and (2·7).
Now we have for $m, n \in P$ and $g, h \in H_0$
$(gm^{\rho^2})(hn^{\rho^2}) = gh_1m_1^{\rho^2}n^{\rho^2} = gh_1k(m_1.n)^{\rho^2} \in Q_0$, where $m^{\rho^2}h = h_1m_1^{\rho^2}$ as above and $m_1^{\rho^2}n^{\rho^2} = k(m_1.n)^{\rho^2}$ as in (2·8) for $k \in H_0$.
These remarks show that Q_0 is a subgroup.

Let G_0 be the S-subgroup of G generated by M. Show that $G_0 \trianglelefteq G$. By (2·1), G_0 is generated by $X = \{M \cup M^{\rho}\}$. Since $G = HM^{\rho^2}$, 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 $h^{-\rho^2}mh^{\rho^2} \in G_0$. We have $h^{-\rho^2}mh^{\rho^2} = (h^{-\rho^2}h)m^h(h^{-\rho^2}h)^{-1}$. However, $h^{-\rho^2}h = \phi(h)^{\rho} \in M^{\rho}$ and $m^h \in M$. Thus G_0 is a normal subgroup of G.

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

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 $M = \mathcal{M}(G)$ be the corresponding Moufang loop. Suppose that G coincides with its S-subgroup generated by M. Then, for any maximal subloop $M_0 \leqslant M$, there exists an S-maximal subgroup $G_0 \leqslant G$ such that $\mathcal{M}(G_0) = M_0$. Moreover, the order of the subloop M_0 is given by $|M_0| = |G_0 : C_{G_0}(\sigma)|$.*

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

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 $\mathcal{M}(G)$ is isomorphic to $M(q)$.*

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

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 $P\Omega_8^+(q)$*

For our purposes, it is more convenient to look at $D_4(q)$ as the orthogonal simple group $P\Omega_8^+(q)$. First, give some definitions. A quadratic form Q on a vector space V is called *non-degenerate* if

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

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 $W \leqslant V$ 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, $W^\perp = \{v \in V \mid (v, w) = 0 \text{ for all } w \in W\}$. 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 $\boldsymbol{F} = GF(q)$, $q = p^n$, equipped with a non-degenerate quadratic form $Q : V \to \boldsymbol{F}$ of type $'+'$. We choose a standard basis $(e_1, \dots, e_4, f_1, \dots, f_4)$ 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 $GO_8^+(q)$. By $r_\square$ we denote the reflection in a vector whose norm is a square in $\boldsymbol{F}^*$. If q is odd then μ denotes a non-square in $\boldsymbol{F}^*$. The image of the natural homomorphism $GO_8^+(q) \to PGO_8^+(q)$ is denoted by an overline

"$\overline{}$" and the full preimage by an overhat "$\widehat{}$". 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 $G = P\Omega_8^+(q)$, $\Omega = \Omega_8^+(q)$, and $M = M(q)$. It is known that

$$|G| = \frac{1}{d^2} q^{12}(q^6-1)(q^4-1)^2(q^2-1), \qquad |M| = \frac{1}{d} q^3(q^4-1).$$

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 $r_\square$ in $GO_m^\varepsilon(q)$, where $\varepsilon = \pm 1$ and $m = 2t$, we have $|GO_m^\varepsilon(q) : C_{GO_m^\varepsilon(q)}(r_\square)| = \frac{1}{d} q^{t-1}(q^t - \varepsilon)$.*

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

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

A subgroup in GS that is $\mathrm{Aut}(G)$-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 $\mathrm{Aut}(G)$ (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 $\overline{r_\square}$ for all reflections $r_\square$ in $GO_8^+(q)$.

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 $\mathcal{M}(G_0)$ 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 $\mathcal{M}(P)$ 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 the normalizer $N_{GS}(G_0)$ 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.*

Table 1. *S-maximal subgroups of* $P\Omega_8^+(q)$

	I	II	III	IV	V
	G_0	restrictions on q	maximality in G	$\|G_0\|$	$\|\mathcal{M}(G_0)\|$
1.	P_2	—	—	$\frac{1}{d^2}q^{12}(q-1)^4(q+1)$	$\frac{1}{d}q^3(q-1)$
2.	R_{s2}	—	✓	$\frac{1}{d^2}q^{12}(q-1)^4(q+1)^3$	$\frac{1}{d}q^3(q^2-1)$
3.	N_1	—	—	$\frac{2}{d^2}q^3(q^3+1)(q+1)^3(q-1)$	$\frac{1}{d}(q+1)$
4.	N_2	$q \geqslant 4$	—	$\frac{2}{d^2}q^3(q^3-1)(q-1)^3(q+1)$	$\frac{1}{d}(q-1)$
5.	N_3	$q \neq 3$	—	$\frac{16}{d^2}(q^2+1)^2$	—
6.	N_4^4	$q = p \geqslant 3$	—	$2^{12}\cdot 3\cdot 7$	8
7.	I_{+2}	$q \geqslant 7$	$q \geqslant 7$	$\frac{192}{d^2}(q-1)^4$	$\frac{4}{d}(q-1)$
8.	I_{-2}	$q \neq 3$	$q \neq 3$	$\frac{192}{d^2}(q+1)^4$	$\frac{4}{d}(q+1)$
9.	I_{+4}	$q \geqslant 3$	$q \geqslant 3$	$\frac{4}{d^2}q^4(q^2-1)^4$	$\frac{2}{d}q(q^2-1)$
10.	G_2^1	—	—	$q^6(q^6-1)(q^2-1)$	1
11.	$P\Omega_8^+(2)$	$q = p \geqslant 3$	✓	$2^{12}\cdot 3^5\cdot 5^2\cdot 7$	120
12.	$P\Omega_8^+(q_0)$	$q = q_0^k, k$ prime, $(d,k)=1$	✓	$\frac{1}{d^2}q_0^{12}(q_0^2-1)(q_0^4-1)^2(q_0^6-1)$	$\frac{1}{d}q_0^3(q_0^4-1)$
13.	$P\Omega_8^+(q_0).2^2$	$q = q_0^2$ odd	✓	$q^6(q-1)(q^2-1)^2(q^3-1)$	$q_0^3(q_0^4-1)$
14.	$PGL_3^\varepsilon(q)$	$2 < q \equiv \varepsilon(3)$, $\varepsilon \pm 1$	✓	$q^3(q^3-\varepsilon)(q^2-1)$	—

Proof. It suffices to prove that any two triality involutions that belong to different cosets in $GS : G$ generate a triality S_3-complement. By lemma 6, we see that each triality involution in $G_1 = G\langle\sigma\rangle$ lies in $|M|$ triality S_3-complements each of which intersects the two cosets $G\sigma\rho$ and $G\rho\sigma$ 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 $W \leqslant V$. 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 *εm-subspace* W of V, where $\varepsilon = \pm 1$, is a non-degenerate m-subspace such that $(W, Q|_W)$ is an orthogonal geometry of sign ε. For q odd, a *+1-subspace* (*–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 $\boldsymbol{F}$. 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 the quadratic form $Q_1 = \mu Q_0$. It is known that Q_1 is equivalent to Q_0. We thus have $n^+(W_{Q_0}) = n^+(W_{Q_1}) = n^-(W_{Q_0})$. $\square$

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

Proof. See Description 4 on p.30 in [**9**]. $\square$

LEMMA 11. *Let λ 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 $L_2(q^2) \cong P\Omega^-_4(q)$ 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 λ act on the basis $\mathfrak{u} = (u_1 \otimes u_1,\ u_1 \otimes u_2,\ u_2 \otimes u_1,\ u_2 \otimes u_2)$ as the linear mapping with matrix

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

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 $\mathfrak{u}$ 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 $\boldsymbol{F}_q$-subspace W spanned by the vectors $w_1 = u_1 \otimes u_1$, $w_2 = u_2 \otimes u_2$, $w_3 = u_1 \otimes u_2 + u_2 \otimes u_1$, $w_4 = \theta u_1 \otimes u_2 + \theta^\lambda u_2 \otimes u_1$, where θ lies in $\boldsymbol{F}_{q^2} \backslash \boldsymbol{F}_q$ and $\theta^2 \in \boldsymbol{F}_q$ for q odd. We thus have an embedding $SL_2(q^2)\langle\lambda\rangle \leqslant GL_4(q) = GL(W)$. Moreover, $K(w) \in \boldsymbol{F}_q$ 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, $SL_2(q^2)\langle\lambda\rangle \leqslant GO^-_4(q)$. It remains to notice that the element λ acts on W as the reflection r_{w_4} for q odd and r_{w_3} for q even. $\square$

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 $W_2 \leqslant 1$.*

Proof. Choose a basis $\mathfrak{w} = (w_1, \ldots, w_k)$ of W_1, where $k = \dim W_1$. Then $\mathfrak{w}^{r_v} = (w_1 r_v, \ldots, w_k r_v)$ is a basis of W_2 and $\mathfrak{w} \cup \mathfrak{w}^{r_v}$ can be extended to a basis $\mathfrak{v}$ of V. By considering the matrix of r_v in $\mathfrak{v}$, 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, $k \leqslant 1$, since r_v is a reflection. $\square$

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_3-subgroup or a $PGL^\varepsilon_3(q)$-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 $\overline{r_\square}$. To prove that the order $|\mathcal{M}(P)|$ is independent of the choice of an S-maximal representative

P in $[G_0]$, we show that all triality involutions in $G_0\langle\overline{r_\square}\rangle$ are G_0-conjugate. This is equivalent to proving that all reflections $r_\square$ that normalize $\widehat{G_0}$ are $\widehat{G_0}$-conjugate.

We proceed with a case-by-case analysis of the subgroups from Table 1. For a more detailed description of their structure, see [**8**].

1. G_0 is a P_2-subgroup. The parabolic subgroup P_2 is the normalizer in G of three totally singular subspaces U, R, T of V, where $U \leqslant R\cap T$, $\dim U = 1$, $\dim R = \dim T = 4$, and $\dim R\cap T = 3$. Since each totally singular 3-space is contained in exactly 2 totally singular 4-spaces which are interchanged by a reflection of form $r_\square$, it follows that G_0 is normalized by the triality involution $\overline{r_\square}$. By Lemma 8, a reflection r_v normalizes $\widehat{G_0} = N_\Omega(U, R\cap T)$ 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 $r_\square$ 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

$$v = u + \alpha e_4 + \beta f_4, \qquad (3\cdot1)$$

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 $\frac{1}{d}q^3(q-1)$. It remains to show that all reflections $r_\square$ normalizing $\widehat{G_0}$ are $\widehat{G_0}$-conjugate. This holds if and only if $\widehat{G_0}$ 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 $g \in \widehat{G_0}$ to any vector v of form (3·1) with $u = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3$ and $\beta = \alpha^{-1}$. Put

$$\begin{aligned}
e_1 g &= e_1, & f_1 g &= -\alpha\alpha_1 e_4 + f_1,\\
e_2 g &= e_2, & f_2 g &= -\alpha\alpha_2 e_4 + f_2,\\
e_3 g &= e_3, & f_3 g &= -\alpha\alpha_3 e_4 + f_3,\\
e_4 g &= \alpha e_4, & f_4 g &= \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha^{-1} f_4,
\end{aligned}$$

and extend the action of g to all of V by linearity. It can be seen that $wg = v$ and $Q(xg) = Q(x)$ for all x in V, i.e., $g \in GO_8^+(q)$. It is clear that in fact $g \in SO_8^+(q)$. Since $g|_{R\cap T}$ is the identity mapping, we have $g \in N_{SO_8^+(q)}(U, R\cap T)$. If q is even then $g \in \widehat{G_0}$ by Lemma 10. Suppose that q is odd and $g \in SO_8^+(q)\backslash\Omega$. Consider the linear mapping $g_1 = r_{e_1+f_1} r_{e_1+\mu f_1}$. Clearly, $g_1 \in N_{SO_8^+(q)}(U, R\cap T)\backslash\Omega$ and g_1 centralizes w. Then $g_1 g \in \widehat{G_0}$ is the required element.

2. G_0 is an R_{s2}-subgroup. The parabolic subgroup R_{s2} is the normalizer in G of a totally singular 2-subspace $U \leqslant V$. We may assume that $U = \langle e_1, e_2\rangle$. Note that the triality involution $\overline{r_{e_3+f_3}}$ 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 $\widehat{G_0}$ is the reflection in a non-singular vector $v \in U^\perp$. Write

$$v = u + \alpha e_3 + \beta f_3 + \gamma e_4 + \delta f_4, \qquad (3\cdot2)$$

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 $\frac{1}{d}q^3(q^2-1)$. As above, it remains to show that $\widehat{G_0} = N_\Omega(U)$ 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 $g \in \widehat{G_0}$. First, find an $h \in \Omega_4^+(q) = \Omega(\langle e_3, f_3, e_4, f_4\rangle)$ 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

$$\begin{aligned} e_1 g &= e_1, & f_1 g &= -\alpha_1 e_3 h + f_1, \\ e_2 g &= e_2, & f_2 g &= -\alpha_2 e_3 h + f_2, \\ e_3 g &= e_3 h, & f_3 g &= \alpha_1 e_1 + \alpha_2 e_2 + f_3 h, \\ e_4 g &= e_4 h, & f_4 g &= f_4 h, \end{aligned}$$

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, $g \in SO_8^+(q)$. If q 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 $g \in \widehat{G_0}$ by Lemma 10. Suppose that q is odd and $g \in SO_8^+(q) \backslash \Omega$. Consider the element $g_1 = r_{e_1+f_1} r_{e_1+\mu f_1}$. Clearly, $g_1 \in N_{SO_8^+(q)}(U) \backslash \Omega$ and g_1 centralizes w. Then $g_1 g \in \widehat{G_0}$ 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 $F \leqslant G$ such that $\widehat{F}$ is the normalizer of an irreducible subgroup of Ω isomorphic to $SU_4(q)$. 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 $N \leqslant G$ 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 $\boldsymbol{F}_{q^2}$ 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 $W_0 = W_1^{\perp} = \langle w_2, w_3, w_4 \rangle$. The space W can be regarded as an 8-space W^* over $\boldsymbol{F}$ 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 $\varphi : GU_4(q) \hookrightarrow GO_8^+(q)$.

Let N be the image under φ 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

$$\begin{aligned} A &\cong GU_1(q) \leqslant GO_2^-(q) = GO(W_1^*), \\ B &\cong GU_3(q) \leqslant GO_6^-(q) = GO(W_0^*). \end{aligned}$$

Note that $A \cong Z_{q+1}$. Denote by η_1 the unique subgroup of $\overline{A}$ of order r, where r is the largest prime divisor of $(q+1)/d$. Now, define $\widehat{N_1}$ to be the subgroup of Ω 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 $\widehat{N_1}$ 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 $R = N_G(W_1^*)$ of the –2-subspace W_1^*, which is an R_{-2}-subgroup of G, and $\eta(R) = \eta_1$. Moreover, N_1 lies in the F_2-subgroup $F = \overline{N_\Omega(SU_4(q)\varphi)}$ and $\eta_2 = \eta(F)$ is the cyclic subgroup of order r in $\overline{Z\varphi}$, 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 Ω, and centralizes δ; it follows that the triality involution $\overline{r_{w_1}}$ normalizes G_0. We have $|\widehat{G_0} : C_{\widehat{G_0}}(r_{w_1})| = |N : C_N(r_{w_1})| = |A : C_A(r_{w_1})|$ and, since $\langle A, r_{w_1} \rangle \cong D_{2(q+1)}$, this index is equal to $(q+1)/d$.

We now show $\widehat{G_0}$-conjugacy of all reflections $r_\square$ that normalize $\widehat{G_0}$. Since any such reflection normalizes N, it suffices to show that all $r_\square$'s normalizing N lie in $\langle A, r_{w_1}\rangle$. Suppose that $r_v = r_\square$ 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 $v \in W_1^*$ then $r_v \in \langle A, r_{w_1}\rangle$. 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 $B \cong GU_3(q) \leqslant GO_6^-(q) = GO(W_0^*)$.

Suppose, by way of contradiction, that r_v is such a reflection. The group $GO_6^-(q)$ is naturally embedded into the group $GO_6^+(q^2)$ of orthogonal transformations of the vector space $U = W_0^* \otimes \boldsymbol{F}_{q^2}$ 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

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

with respect to this decomposition, where $b^{\#}$ is the image of b under the matrix Frobenius map, corresponding to the map $[x \to x^q]$ of $\boldsymbol{F}_{q^2}$. 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_{s4}-*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_{s4}-subgroups are isomorphic. If K is either an R_{+2} subgroup or an I_{s4}-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 $N \leqslant G$ is an N_2-*subgroup* if $N = R \cap I$, with R an R_{+2} subgroup, I an I_{s4}-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

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

where c^{-T} denotes the inverse-transpose of c. Clearly, this is an element of $GO_8^+(q)$ and thus we have an embedding $\varphi : GL_4(q) \hookrightarrow GO_8^+(q)$.

Let N be the image under φ of a subgroup in $GL_4(q)$ isomorphic to $GL_1(q) \times GL_3(q)$ such that, in a suitable basis of V, N has the block diagonal form

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

where

$$A \cong GL_1(q) \leqslant GO_2^+(q) = GO(V_1),$$
$$B \cong GL_3(q) \leqslant GO_6^+(q) = GO(V_0),$$

with $V_1 = \langle e_1, f_1\rangle$ and $V_0 = V_1^{\perp}$. Note that $A \cong Z_{q-1}$. Denote by η_1 the unique subgroup of $\overline{A}$ of order r, where r is the largest prime divisor of $(q-1)/d$. Now, define $\widehat{N_2}$ to be the subgroup of Ω generated by $N\cap\Omega$ and $\delta = r_{w_1}r_{w_2}r_{w_3}r_{w_4}$, where $w_i = e_i+f_i$, $i = 1,\ldots,4$. Let N_2 be the image of $\widehat{N_2}$ 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 $\overline{r_{w_1}}$ normalizes G_0 and that $|\widehat{G_0} : C_{\widehat{G_0}}(r_{w_1})| = |A : C_A(r_{w_1})| = (q-1)/d$. The conjugacy of the triality involutions in $G_0\langle\overline{r_{w_1}}\rangle$ 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 $B \cong GL_3(q) \leqslant GO_6^+(q) = GO(V_0)$. 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 $\overline{r_v}$ is such an involution. Then r_v normalizes a Sylow r-subgroup R in Ω. 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 $R \leqslant N_{GO_8^+(q)}(\{V_1, V_2\}) \cong (GO_4^-(q) \times GO_4^-(q)).2$. This implies that r_v normalizes the set $\{V_1, V_2\}$. By Lemmas 12 and 8, $v \in V_i$, with $i = 1$ or $i = 2$. In particular, r_v normalizes a Sylow r-subgroup $R_i \leqslant \Omega_4^-(V_i) \cong \Omega_4^-(q)$. Since $\Omega_4^-(q)\langle r_v\rangle \cong PGO_4^-(q)$, we may assume by lemma 11 that, in the group $L_2(q^2)\langle\lambda\rangle$, λ normalizes a Sylow r-subgroup or, equivalently, the field automorphism λ of $SL_2(q^2)$ 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 θ and θ^{-1} be the characteristic roots of x. Note that $\theta^{q^2-1} \neq 1$, since otherwise $\theta^{q^2-1} = 1$ and $\theta^{q^2+1} = 1$ would imply that $x^2 = 1$ contrary to the fact that r is odd. Since the characteristic roots of x^λ are θ^q and θ^{-q}, we have $\{\theta^q, \theta^{-q}\} = \{\theta, \theta^{-1}\}$, which implies $\theta^q = \theta$ or $\theta^q = \theta^{-1}$. In either case, $\theta^{q^2-1} = 1$, a contradiction.

6. G_0 is an N_4^4-subgroup. Suppose that $q = p$ is an odd prime. Choose a basis $\mathfrak{v} = (v_1,\ldots,v_8)$ of V such that $(v_i, v_j) = 0$, $i \neq j$, and $Q(v_i) = 1$ for $i = 1,\ldots,8$. An N_4^4-subgroup is conjugate in G to the normalizer $N_G(P)$ of the subgroup P of order 8 generated by the involutions $\overline{x}$, $\overline{y}$, $\overline{z}$, where

$$\begin{aligned} x &= \mathrm{diag}_{\mathfrak{v}}(1,1,1,1,-1,-1,-1,-1),\\ y &= \mathrm{diag}_{\mathfrak{v}}(1,1,-1,-1,1,1,-1,-1),\\ z &= \mathrm{diag}_{\mathfrak{v}}(1,-1,1,-1,1,-1,1,-1) \end{aligned}$$

are elements of Ω. We assume that $G_0 = N_G(P)$. Notice that $\widehat{P} = \langle -1, x, y, z\rangle$, where –1 is the central involution of Ω, and that $N_{GO_8^+(q)}(\widehat{P})$ consists of monomial matrices. We prove that the only reflections $r_\square$ that normalize $\widehat{P}$ are r_{v_i}, $i = 1,\ldots,8$. Since these reflections are $\widehat{G_0}$-conjugate (which follows from the fact that $\widehat{G_0}$ acts transitively on the vectors v_i's), this will imply that $|\mathcal{M}(G_0)| = 8$.

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

(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 $(g_{55}, g_{66}, g_{77}, g_{88})$,

(ii) $(g_{11}, g_{22}, g_{33}, g_{44}) = \pm(g_{55}, g_{66}, g_{77}, g_{88})$.

By (i), it follows that either $1 \leqslant i < j \leqslant 4$ or $5 \leqslant i < j \leqslant 6$, since otherwise $x^{r_v} \notin \widehat{P}$. Without loss assume that $1 \leqslant i < j \leqslant 4$. Clearly, there is a $g \in \widehat{P}$ with $g_{ii} \neq g_{jj}$. But then the matrices g and g^{r_v} 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 $\widehat{P}$ are uniquely determined by the lower four entries and one arbitrary upper diagonal one.

7-8. G_0 is an $I_{\varepsilon 2}$-subgroup, $\varepsilon = \pm 1$. An *$I_{\varepsilon 2}$-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 $\varepsilon 2$-subspaces V_i, $i = 1, \ldots, 4$. A reflections $r_v = r_\square$ normalizes $\widehat{G_0}$ 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 $\frac{1}{d}(q - \varepsilon)$. Thus there are $\frac{4}{d}(q - \varepsilon)$ reflections of form $r_\square$ that normalize $\{V_1, \ldots, V_4\}$. They are all $\widehat{G_0}$-conjugate since $\widehat{G_0}$ permutes transitively the subspaces V_i's and the $+1$-subspaces inside each V_i (see [**9**], Proposition 4.2.11).

9. G_0 is an I_{+4}-subgroup. An *I_{+4}-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 $r_v = r_\square$ normalizes $\widehat{G_0}$ 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 $\frac{1}{d}q(q^2 - 1)$. Thus there are $\frac{2}{d}q(q^2 - 1)$ reflections of form $r_\square$ that normalize $\{V_1, V_2\}$. They are all $\widehat{G_0}$-conjugate for the same reasons as in the case above.

10. G_0 is a G_2^1-subgroup. A *G_2^1-subgroup* is a subgroup G_0 of G isomorphic to $G_2(q)$ and such that $GN_{GS}(G_0) = GS$. 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.

11. G_0 is a $P\Omega_8^+(2)$-subgroup. Consider a rational 8-dimensional vector space W with a basis $\mathfrak{w} = \{w_1, \ldots, w_8\}$ orthonormal with respect to some non-degenerate quadratic form $K : W \to \mathbb{Q}$. It can be proven (e.g., using GAP [**6**]) that the linear mappings of W that have matrices

$$A = \begin{pmatrix} . & -1 & . & . & . & . & . & . \\ -1 & . & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . \\ . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & . & 1 \end{pmatrix}, \qquad B = \frac{1}{2}\begin{pmatrix} 1 & . & . & . & . & 1 & 1 & 1 \\ 1 & . & . & . & . & -1 & 1 & -1 \\ 1 & . & . & . & . & 1 & -1 & -1 \\ 1 & . & . & . & . & -1 & -1 & 1 \\ . & -1 & 1 & -1 & 1 & . & . & . \\ . & 1 & 1 & 1 & 1 & . & . & . \\ . & -1 & -1 & 1 & 1 & . & . & . \\ . & 1 & -1 & -1 & 1 & . & . & . \end{pmatrix},$$

in the basis $\mathfrak{w}$ generate a subgroup of $GL(W, \mathbb{Q})$ isomorphic to the bicyclic extension $2.P\Omega_8^+(2).2$. 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 $\{v_1, \ldots, v_8\}$ of V which is orthonormal, i.e. such that $(v_i, v_j) = 0$, $i \neq j$, and $(v_i, v_i) = 1$ for $i = 1, \ldots, 8$. Then $r_{v_1+v_2}$ 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 $r_{v_1+v_2}$. Denote $\widehat{G_0} = \langle A_p, B_p \rangle' \cong 2.P\Omega_8^+(2)$. It is clear that $\widehat{G_0}$ lies in Ω and its image G_0 in G is an $P\Omega_8^+(2)$-subgroup normalized by the triality involution $\overline{r_{v_1+v_2}}$. By Lemma 7, assume that G_0 is S-invariant. Lemma 4 now implies that there is a unique subloop of

M corresponding to $P\Omega_8^+(2)$-subgroups of G whose order is $|M(2)|$. We remark that a computer-free proof of the embedding $P\Omega_8^+(2) \hookrightarrow P\Omega_8^+(p)$ can be obtained using the fact that the group $2.P\Omega_8^+(2).2$ is isomorphic to the Weyl group of the root system of type E_8.

12-13. G_0 is a $P\Omega_8^+(q_0)$- or a $P\Omega_8^+(q_0).2^2$-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 $P\Omega_8^+(q_0)$ which is S-invariant. Clearly, $\mathcal{M}(G_0) \cong M(q_0)$. Now let $d = k = 2$; in particular, q is odd. Then $\lambda = \mu^2$ is a non-square in $\boldsymbol{F}_{q_0}$. Let H be a natural copy of $\Omega_8^+(q_0)$ in Ω that acts on the $\boldsymbol{F}_{q_0}$-subspace V_0 of V spanned by the standard basis $\mathfrak{v} = (e_1, \dots, f_4)$ and respects the quadratic form $Q_0 = Q|_{V_0}$. Define

$$b = \mathrm{diag}_{\mathfrak{v}}(\mu, \mu, \mu, \mu, \mu^{-1}, \mu^{-1}, \mu^{-1}, \mu^{-1}),$$
$$c = \mathrm{diag}_{\mathfrak{v}}(\lambda^{-1}, 1, 1, 1, \lambda, 1, 1, 1).$$

Note that $b, c \in \Omega$ and $c = r_{e_1+f_1} r_{e_1+\lambda f_1}$. We assume that $G_0 = N_G(\overline{H}) = \langle \overline{H}, \overline{b}, \overline{c}\rangle \cong \mathrm{InnDiag}(P\Omega_8^+(q_0))$, i.e. the group of inner-diagonal automorphisms of $P\Omega_8^+(q_0)$ (see [**8**], Proposition 2.2.9). The group G_0 is normalized by the triality involution $\overline{r_v}$, where $v = e_1 + f_1$. Moreover, since $H^{r_v} = H$, $c^{r_v} = c^{-1}$, and $b^{r_v} = bc$, it follows that $C_{G_0}(\overline{r_v}) \leqslant \langle \overline{H}, \overline{c}\rangle$. Note that the coset $\overline{H}\overline{c}$ contains an element $\overline{a}$ that commutes with $\overline{r_v}$ (put, for instance, $a = r_{e_2+f_2} r_{e_2+\lambda f_2}$). Therefore, $|G_0 : C_{G_0}(\overline{r_v})| = 2|\overline{H} : C_{\overline{H}}(\overline{r_v})| = 2|M(q_0)|$. The conjugacy of triality S_3-complements in $G_0 S$ follows from Lemma 4.

14. G_0 is a $PGL_3^{\varepsilon}(q)$-subgroup. Suppose that $q \equiv \varepsilon (\mathrm{mod}\ 3)$, $\varepsilon = \pm 1$. Then G contains a maximal subgroup G_0 isomorphic to $PGL_3^{\varepsilon}(q)$. If G_0 were S-invariant then, by Lemma 4, the subgroup of G_0 isomorphic to $L_3^{\varepsilon}(q)$ would have trivial triality relative to S. But then G_0 would be a subgroup of $C_G(\rho) \cong G_2(q)$, 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 $P\Omega_8^+(q)$ being simple satisfies the conditions of Corollary 1. Hence, all maximal subloops of $M(q) = \mathcal{M}(P\Omega_8^+(q))$ have form $\mathcal{M}(G_0)$ for certain S-maximal subgroups G_0 of $P\Omega_8^+(q)$. By Theorem 2, the orders $|\mathcal{M}(G_0)|$ 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

[**1**] R. H. Bruck, A survey of binary systems (Springer-Verlag, 1958).
[**2**] R. H. Bruck, Some theorems on Moufang loops, *Math. Z.*, **73**, (1960), 59–78.
[**3**] O. Chein, M. K. Kinyon, A. Rajah, P. Vojtěchovský, Loops and the Lagrange property, *Result. Math.*, **43**, N 1–2 (2003) 74–78.
[**4**] S. Doro, Simple Moufang loops, *Math. Proc. Camb. Phil. Soc.*, **83**, (1978), 377-392.
[**5**] T. Evans, Varieties of loops and quasigroups. Quasigroups and loops: theory and applications, Sigma Ser. Pure Math. 8, 1-26 (1990).
[**6**] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews, 2002, (http://www.gap-system.org)
[**7**] G. Glauberman, On loops of odd order II, *J. Algebra*, **8**, (1968), 393-414.
[**8**] 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.
[**9**] P. Kleidman, M. Liebeck, The subgroup structure of the finite classical groups. London

Mathematical Society Lecture Note Series, 129. Cambridge etc.: Cambridge University Press. (1990).

[**10**] M. W. Liebeck, The classification of finite simple Moufang loops, *Math. Proc. Camb. Phil. Soc.*, **102**, (1987), 33-47.

[**11**] P. O. Mikheev, Enveloping groups of Moufang loops, *Russ. Math. Surv.*, **48**, N 2 (1993), 195-196.

[**12**] V. A. Vasil'ev, V. D. Mazurov, Minimal permutation representations of finite simple orthogonal groups. *Algebra and Logic*,**33**, N 6 (1994), 337-350; translation from *Algebra i Logika*, **33**, N 6 (1994), 603-627.

[**13**] K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, A. I. Shirshov, Rings that are nearly associative, Pure and Applied Mathematics, 104. Academic Press, New York-London, 1982.