# Lagrange's Theorem for Moufang loops

S.M. Gagola III
J.I. Hall
Department of Mathematics
Michigan State University
East Lansing, Michigan 48824, U.S.A.

Submitted: 12 October 2004
Revised: 31 January 2005

**Abstract**

All finite Moufang loops have the Lagrange property.

## 1 Introduction

A finite loop $L$ is said to have the *Lagrange property* if, for every subloop $K$ of $L$, the order of $K$, written $|K|$, is a divisor of $|L|$, the order of $L$. Lagrange's Theorem states that all finite groups have the Lagrange property. Here we resolve, in the positive, the long-standing conjecture that, more generally, all finite Moufang loops have the Lagrange property:

**(1.1)** THEOREM. *Let $K$ be a subloop of the finite Moufang loop $L$. Then $|K|$ divides $|L|$.*

It is well-known that the Lagrange property is valid for all Moufang loops if and only if it is valid for finite simple Moufang loops [4, Lemma V.2.1]. Of course, Lagrange's Theorem holds if the simple loop is a group; so only nonassociative, finite, simple Moufang loops need be considered. These were classified by Liebeck [15], the only examples being the loops $P(q)$ first studied by Paige [19]. The Paige loop $P(q)$ is the central quotient of the loop of norm 1 units in $Oct(q)$, the split octonians over the finite field $\mathbb{F}_q$. Liebeck's proof used Doro's observation [7] that Moufang loops correspond to groups with triality. The corresponding triality group for $P(q)$ is $P\Omega_8^+(q){:}Sym(3)$.

In our proof we show that it is enough to check divisibility for $K$ maximal in $L = P(q)$ and that these subloops correspond to maximal triality subgroups

*Primary subject:* 20N05, *Secondary subject:* 20D06; *Keywords:* Moufang loop, Lagrange's Theorem, group with triality

of $P\Omega_8^+(q){:}Sym(3)$. All maximal subgroups of $P\Omega_8^+(q){:}Sym(3)$ have been catalogued by Kleidman [14], and we show that each corresponding subloop conforms to the Lagrange property.

Earlier work on the Lagrange property for Moufang loops can be found in [5, 16, 24].

This paper was first submitted for publication in June 2004. We quickly learned that the paper [11] with the same result (and title!) had been written by A.N. Grishkov and A.V. Zavarnitsine and submitted in late 2003. The same authors have a second preprint [12] which finds the maximal subloops of the finite Paige loops (from which the Lagrange property follows, as mentioned above). More recently, we learned that Eric Moorhouse [17] has also independently classified the maximal subloops of the finite Paige loops and thereby verified the Lagrange property. The work of [11, 12, 17] depends, as does ours, on Kleidman's classification [14] of the maximal subgroups of $P\Omega_8^+(q){:}Sym(3)$. The details of the several proofs are, however, different; and we have been encouraged by Doctors Grishkov and Zavarnitsine and by others to continue with publication of our version.

The first author's thesis [9], prepared without prior knowledge of [11, 12, 17], improves upon the work of this paper and those in two ways. All finite subloops of arbitrary (possibly infinite) Paige loops are described, the classification of maximal subloops of the finite loops and the Lagrange property thus being corollaries. Since the containing loop need not be finite, Kleidman's results [14] are not directly applicable. Furthermore Kleidman's proof makes broad use of the classification of finite simple groups, and it is desirable to minimize reliance upon that major result. The results of [9] (which will appear elsewhere) are almost entirely elementary in proof, with only a few specific results from the classification used.

For general reference on loop theory, see [4, 20]. For group theory see [1], and for geometry see [21]. If $s$ is an element of $GL_K(V)$, then, for the vector $v$ in $V$, the commutator $[v, s]$ is defined to be $v(s-1) = -v + v.s$. Similarly, for a subspace $U$ of $V$ and a subset $S$ of $GL_K(V)$, the commutator subspace $[U, S]$ is the $K$-span of the various $[u, s]$ with $u \in U$ and $s \in S$.

## 2 Loops, designs, and triality

We introduce Moufang loops, Latin square designs, and groups with triality. These are linked in Theorem 2.2 (from [13]), which is fundamental to this paper. We also present some general results about groups with triality, especially those coming from subloops of Moufang loops.

A *loop* is a set $L$ equipped with a binary product that possesses an identity element 1 and such that the equations $ax = c$ and $yb = c$ have unique solutions $x$ and $y$ for all $a, b, c \in L$. Thus a loop can be thought of as a group that might not be associative. A *Moufang loop* satisfies the weak associative law

$$((ab)a)c = a(b(ac)),$$

for all $a, b, c \in L$. Such loops were first studied by Moufang [18] in the context of alternative algebras. Clearly every group is a Moufang loop.

A *Latin square design* $\mathcal{D}$ is a pair $\mathcal{D} = (P, A)$ of points $P = P(\mathcal{D})$ and lines $A = A(\mathcal{D})$ (subsets of $P$) with the properties:

> $(i)$ $P$ is the disjoint union of three parts $R$, $C$, $E$.
>
> $(ii)$ every line $l \in A$ contains exactly three points, meeting each of $R$, $C$, $E$ exactly once.
>
> $(iii)$ any pair of points from different parts belong to exactly one line.

We have $|R| = |C| = |E| = n$, say. The $n^2$ lines of the Latin square design with $|P| = 3n$ correspond to the $n^2$ cells of a Latin square with side $n$. The line $\{a_R, b_C, c_E\}$ asserts that in row $a$, column $b$ of the Latin square one finds the entry $c$.

Let $\mathcal{D} = (P, A)$ be a Latin square design. Choose a line $l_0 \in A$ and a set $L$ that we use to label $R$ (one-to-one) in such a way that the point $l_0 \cap R$ is labelled by the element 1 (or sometimes, for clarity, $1_R$). We also will label $C$ and $E$ by $L$ and, in doing so, define a multiplication on $L$ with identity element 1. We call $L$ the *Thomsen loop* of $\mathcal{D}$, $L = \mathcal{L}(\mathcal{D})$. For a line $l$ of $A$, we write $[\,a, b, c\,]$ in place of $\{a_R, b_C, c_E\}$.

The loop and labeling are given as follows:

> 1. *Label* $l_0$ *as* $[\,1, 1, 1\,]$*, and label the points of* $R \setminus 1_R$ *with* $L \setminus 1$.
>
> 2. *Label* $E$ *with the set* $L^{-1}$ *of right inverses of members of* $L$ *via* $[\,a, 1, a^{-1}\,] \in A$.
>
> 3. *Label* $C$ *with the members of* $L$ *via* $[\,1, a, a^{-1}\,] \in A$.
>
> 4. *The right inverse map is determined by* $[\,a, a^{-1}, 1\,] = [\,a, b, 1\,] \in A$*; so* $E$*, previously only labelled by* $L^{-1}$*, is now also labelled by* $L$.
>
> 5. *Define* $ab = c$ *in* $L$ *by* $[\,a, b, c^{-1}\,] \in A$*. (That is,* $[\,d, e, f\,] \in A$ *if and only if* $(de)f = 1$ *in* $L$*.)*

Choice of a different identity line $l_0$ and of a different identification of $L$ with $R$ correspond to loop isotopy for $L$ [4, 20].

Conversely, if $L$ is a loop, then the *Thomsen design* of $L$, $\mathcal{D} = \mathcal{T}(L)$, has point set $P(L) = L_R \cup L_C \cup L_E$ of size $3|L|$ and line set $A(L)$ consisting of those triples $\{a_R, b_C, c_E\} = [\,a, b, c\,]$ with $(ab)c = 1$ in $L$. (Thomsen [23] seems to have been the first to associate discrete incidence systems with arbitrary loops. Most of the earlier work on webs concentrated on Euclidean geometry.)

The two constructions are easily seen to be inverses of each other in the sense that $\mathcal{T}(\mathcal{L}(\mathcal{D}))$ is isomorphic to $\mathcal{D}$ and $\mathcal{L}(\mathcal{T}(L))$ is isotopic to $L$.

In Theorem 2.2 below, we will see that Moufang loops correspond to Latin square designs admitting certain types of automorphisms. Here the automorphism group $\mathrm{Aut}(\mathcal{D})$ of the Latin square design $\mathcal{D} = (P, A)$ consists of all permutations $g$ of the point set $P$ that take lines to lines; that is, $\{a,b,c\} \in A$ if and only if $\{ag,bg,cg\} \in A$.

For $x \in P$, say $x \in R$, consider the partial permutation $\tau_x$ that exchanges the sets $C$ and $E$ via

$$\tau_x(y) = z,\ \tau_x(z) = y \quad \text{if and only if} \quad [\,x,y,z\,] \in A\,.$$

The question is whether $\tau_x$ can be extended to a permutation on all $P$ (by defining it on $R$) so that $\tau_x$ is in $\mathrm{Aut}(\mathcal{D})$.

If $\tau_x$ has two extensions $\alpha$ and $\beta$ to $\mathrm{Aut}(\mathcal{D})$, then $\alpha\beta$ and $\alpha\beta^{-1}$ are trivial on $C \cup E$ and so on $\mathcal{D}$. That is, $\alpha = \beta^{-1} = \beta$. Therefore, $\tau_x$ has at most one such extension, and if it exists then it has order 2. Thus we may, without confusion, call this extension $\tau_x$ as well. It is a *central automorphism* of $\mathcal{D}$ with *center* $x$.

Completely similar remarks are valid for central automorphisms $\tau_y$ and $\tau_z$ with centers $y \in C$ and $z \in E$. If we want to emphasize the part of $P$ from which the center comes, then we may write $\tau_x = \rho_x$, $\tau_y = \kappa_y$, and $\tau_z = \epsilon_z$.

**(2.1)** Proposition. ([13, Prop. 2.3]) *For an arbitrary Latin square design* $\mathcal{D} = (P,A)$,

$$\{\tau_p \,|\, p \in P,\ \tau_p \in \mathrm{Aut}(\mathcal{D})\}$$

*is a normal set of elements of order* 2 *in* $\mathrm{Aut}(\mathcal{D})$*. For* $g, \tau_p \in \mathrm{Aut}(\mathcal{D})$*, we have* $\tau_p^g = \tau_{pg}$.

*If* $\tau_p, \tau_q \in \mathrm{Aut}(\mathcal{D})$ *with $p$ and $q$ belonging to different parts of $P$, then* $\tau_p\tau_q$ *has order* 3*. In this case* $\{\tau_p \,|\, p \in P,\ \tau_p \in \mathrm{Aut}(\mathcal{D})\}$ *is a single conjugacy class of* $\mathrm{Aut}(\mathcal{D})$*.*

The case where $\tau_p \in \mathrm{Aut}(\mathcal{D})$, for every point $p$ of $P$, will lead to Moufang loops. The proposition suggests an abstract setting for such groups.

Let $D = D^G$ be a normal set of elements of order 2 in the group $G = \langle D \rangle$. Then $(G, D, \pi)$, or just $G$, is said to be a *group with triality* (or *triality group*) with respect to the set $D$ of *triality reflections* (or just *reflections*) and *projection* $\pi$ provided:

> $\pi$ is a homomorphism from $G$ onto $Sym(3)$, and $|de| = 3$ whenever $d, e \in D$ with $\pi(d) \neq \pi(e)$.

That is, if $d, e \in D$ with $\pi(d) \neq \pi(e)$ then $\langle d, e \rangle \simeq Sym(3)$. In particular $d$ and $e$ are conjugate in the group they generate, so the normal set $D$ is actually a single conjugacy class of $G$. It is often (but not always) the case that the class $D$ and projection map $\pi$ are uniquely determined within the group $G$ with triality.

The group $\ker(\pi)$ is called the *rotation subgroup* of $(G, D, \pi)$.

Proposition 2.1 allows the construction of groups with triality from Latin square designs that admit the central automorphism $\tau_p$ for each point $p$. In this case we write $D(\mathcal{D}) = \{\,\tau_p \,|\, p \in P\,\}$ and $G(\mathcal{D}) = \langle D(\mathcal{D}) \rangle$. By Proposition 2.1, the group $G(\mathcal{D})$ is a group with triality whose reflection class is $D(\mathcal{D})$. The projection map $\pi\colon G(\mathcal{D}) \longrightarrow Sym(\rho,\kappa,\epsilon)$ is then given by

$$\rho_p \mapsto (\rho)(\kappa,\epsilon)\,,\ \kappa_p \mapsto (\kappa)(\rho,\epsilon)\,,\ \epsilon_p \mapsto (\epsilon)(\rho,\kappa)\,,$$

for $p \in P$. If $L$ is a loop with $\mathcal{D} = \mathcal{T}(L)$, then we write $G(L)$ for $G(\mathcal{D})$ and $D(L)$ for $D(\mathcal{D})$. Given $a \in L$, we also write $\rho_a$ for $\tau_{a_R}$, $\kappa_a$ for $\tau_{a_C}$, and $\epsilon_a$ for $\tau_{a_E}$.

Conversely, given a group $(G, D, \pi)$ with triality, we can define a Latin square design $\mathcal{T}((G, D, \pi))$ with point set $P = D$. For each $d, e \in D$ with $\pi(d) \neq \pi(e)$, we have $\langle d, e\rangle \simeq Sym(3)$; so we take the line of $\mathcal{T}((G, D, \pi))$ on $d, e$ to be $\{d, e, ded = ede\}$. We thus also refer to the subgroup $\langle d, e\rangle \simeq Sym(3)$ as a *line* of the group $(G, D, \pi)$ with triality.

Usually we can write $\mathcal{T}(G)$ for $\mathcal{T}((G, D, \pi))$ without ambiguity. If $L$ is a loop with $\mathcal{T}((G, D, \pi)) = \mathcal{T}(L)$, then we also write $L = \mathcal{L}((G, D, \pi)) = \mathcal{L}(G)$. This is an abuse, since $L$ is only determined up to isotopy by $(G, D, \pi)$.

The fundamental connection between arbitrary Moufang loops and abstract groups with triality was observed and studied by Doro [7], motivated by the work of Glauberman [10]. Doro's definition of triality is different but equivalent to the one given here. In Doro's treatment the rotation subgroup $\ker(\pi)$, rather than the larger group $G$, is called a group with triality.

Bol [3] gave a geometric characterization of 3-nets or 3-webs (dual to Latin square designs—see [4, I.4] or [20, II.1]) that are coordinatized by Moufang loops. Tits [22] showed that Bol's 3-nets admit reflections as automorphisms. (See also Bruck [4, p.120].) Tits also noted and discussed the connection with triality for orthogonal groups and the octonians. Our treatment follows that of [13], which was in part motivated by the work of Funk and Nagy [8].

**(2.2)** Theorem. ([13, Theorem 3.6]) *The following are equivalent:*

(1) *$L$ is a Moufang loop;*

(2) *$\mathcal{D} = (P, A)$ is a Latin square design admitting a central automorphism at each point;*

(3) *$(G, D, \pi)$ is a group with triality and $Z(G) = 1$.*

*Indeed:*

*given $L$ as in (1), we have $\mathcal{D} = \mathcal{T}(L)$, $G = G(L)$, and $D = D(L)$;*

*given $\mathcal{D}$ as in (2), we have $L = \mathcal{L}(\mathcal{D})$, $G = G(\mathcal{D})$, and $D = D(\mathcal{D})$;*

*given $G$ as in (3), we have $L = \mathcal{L}(G)$ and $\mathcal{D} = \mathcal{T}(G)$.*

*Under (1), the map $\pi = \pi_L$ is determined by projection onto $\langle \rho_1, \kappa_1, \epsilon_1\rangle \simeq Sym(3)$. That is, $\rho_a \mapsto \rho_1$, $\kappa_a \mapsto \kappa_1$, and $\epsilon_a \mapsto \epsilon_1$, for $a \in L$. Similarly, under (2), a suitable map $\pi = \pi_{\mathcal{D}}$ can be determined by projection onto any line.*

In this correspondence, we have

$$3|L| = |P| = |D|\,.$$

These equalities are crucial for our study of the Lagrange property.

If $(G, D, \pi)$ is a group with triality and $Q$ is a normal subgroup of $G$ that is contained in $\ker(\pi)$, then $G/Q$ is also a group with triality. Subgroups of $G$ also give rise to new groups with triality. We say that the subgroup $H$ of $G$ *admits the triality* if $(\langle D \cap H\rangle, D \cap H, \pi|_{\langle D\cap H\rangle})$ is itself a group with triality. The following is elementary:

**(2.3)** Lemma. *Let $(G, D, \pi)$ be a group with triality, and let $H$ be a subgroup of $G$. Then the following are equivalent:*

(1) *$H$ admits the triality;*

(2) *$H$ contains a line;*

(3) *$G = \ker(\pi).H$ and $H \cap D$ is nonempty.*

Certain properties of groups with triality, particularly those regarding cardinality, can be discussed in terms of quotients and subgroups.

**(2.4)** Lemma. *Let $(G, D, \pi)$ be a group with triality. Set $M = \ker(\pi)$, the rotation subgroup.*

(1) *Assume that the subgroup $H$ of $G$ admits the triality, and let $M_0$ be the rotation subgroup of $H_0 = \langle D \cap H \rangle$. The set $D \cap H = D \cap H_0$ is a single conjugacy class of $H_0$. For $r \in D \cap H$, we have*

$$|D \cap H| = 3|D \cap rM_0| \quad \text{and} \quad D \cap rM_0 = r^{M_0} = r^{M \cap H}\,.$$

(2) *Assume $Q$ is a normal subgroup of $G$ that is contained in $M$, and set $\bar{G} = G/Q$. Let $I$ be a line of $G$ with $r \in D \cap I$. Then $Q.I$ admits the triality and $(\bar{G}, \bar{D}, \bar{\pi})$ is a group with triality. Furthermore*

$$|D| = |\bar{D}| \cdot |D \cap rQ| = 3|\bar{r}^{\bar{M}}| \cdot |r^Q|\,.$$

Proof. (1) By definition and Lemma 2.3, $H_0$ is a group with triality. As already seen in Proposition 2.1 and the remarks that follow it, $D \cap H = D \cap H_0$ is a single class of $H_0$. These involutions are uniformly distributed among the cosets corresponding to the involutions of $\pi(H_0) \simeq Sym(3)$, so $|D \cap H| = |D \cap H_0| = 3|D \cap rM_0|$.

Clearly $D \cap rM_0 \supseteq r^{M \cap H} \supseteq r^{M_0}$. In $H_0/M_0 \simeq Sym(3)$, we find $\langle r \rangle M_0 = N_{H_0}(rM_0)$. Therefore

$$D \cap rM_0 = r^{H_0} \cap rM_0 = r^{\langle r \rangle M_0} = r^{M_0}\,,$$

completing (1).

(2) This is immediate except for the last line. There $|\bar{D}| = 3|\bar{D} \cap \bar{r}\bar{M}| = 3|\bar{r}^{\bar{M}}|$ and $D \cap rQ = r^Q$, both by (1).

**(2.5)** Proposition. *Let $\mathcal{D} = (P, A)$ be a Latin square design. Consider the group $Univ(\mathcal{D})$ with generators $\tilde{d}$, one for each $d \in P$, and relations $\tilde{d}^2 = 1$ and $\tilde{d}\tilde{e}\tilde{d} = \tilde{f} = \tilde{e}\tilde{d}\tilde{e}$, for all $d \in P$ and $[\,d, e, f\,] \in A$. Then $Univ(\mathcal{D})$ is a triality group with reflection class $\tilde{D} = \{\, \tilde{d} \,|\, d \in P \,\}$ whose projection map $\tilde{\pi}$ with image $Sym(\rho, \kappa, \epsilon)$ is given by*

$$\tilde{r} \mapsto (\rho)(\kappa, \epsilon)\,,\ \tilde{c} \mapsto (\kappa)(\rho, \epsilon)\,,\ \tilde{e} \mapsto (\epsilon)(\rho, \kappa)\,,$$

*for all $r \in R$, $c \in C$, and $e \in E$.*

*Assume additionally that the Latin square design $\mathcal{D} = (P, A)$ admits a central automorphism at each point. Then we have $\mathcal{T}(Univ(\mathcal{D})) \simeq \mathcal{D}$ and $Univ(\mathcal{D})/Z(Univ(\mathcal{D})) \simeq G(\mathcal{D})$ with $\tilde{D}$ mapped bijectively to $D(\mathcal{D})$. Indeed any group with triality whose associated Latin square design is isomorphic to $\mathcal{D}$ is a central quotient of $Univ(\mathcal{D})$.*

Proof. By construction, for an arbitrary Latin square design $\mathcal{D}$, $\tilde{D}$ is a conjugacy class of elements of order 2 in $\tilde{G} = Univ(\mathcal{D})$ and $\tilde{\pi}$ is a homomorphism onto $Sym(\rho, \kappa, \epsilon)$. Furthermore, if $x, y \in \tilde{D}$ with $\tilde{\pi}(x) \neq \tilde{\pi}(y)$ then $|xy| = 3$; so $Univ(\mathcal{D})$ is a group with triality as described.

For most Latin square designs, $Univ(\mathcal{D})$ will itself be symmetric of degree 3. If, however, $\mathcal{D}$ admits a central automorphism at each point, then $\tilde{d} \mapsto \tau_d$, for all $d \in P$, is a bijection of $\tilde{D}$ and $D(\mathcal{D})$; and it describes a homomorphism of $Univ(\mathcal{D})$ onto $G(\mathcal{D})$ since all relations are determined by $\mathcal{D}$. If $Z$ is the kernel of this homomorphism, then $\tilde{d} = \tilde{D} \cap \tilde{d}Z$, for all $d \in P$. Therefore $\tilde{d}^Z = \tilde{d}$, and $Z$ is central in $Univ(\mathcal{D})$. As $G(\mathcal{D})$ has trivial center, in fact $Z = Z(Univ(\mathcal{D}))$.

Indeed, if $(G, D, \pi)$ is a group with triality and $\mathcal{T}((G, D, \pi)) \simeq \mathcal{D}$, then the argument of the previous paragraph remains valid except we no longer know that $G$ has trivial center. Still we find that $G$ is isomorphic to $Univ(\mathcal{D})/Z_0$ for some $Z_0 \leq Z(Univ(\mathcal{D}))$.

The group $Univ(\mathcal{D})$ is called the *universal triality group* of $\mathcal{D}$, and we also write $Univ(L) = Univ(\mathcal{D})$ for any Moufang loop $L$ with $\mathcal{D} = \mathcal{T}(L)$. The proposition should be compared with Doro's [7, Theorem 2], which provides a presentation for the rotation group $\ker(\tilde{\pi})$ of $Univ(L)$.

Let $L$ be a Moufang loop. If $K$ is a subloop of $L$, then we set $D_L(K) = \{\, \rho_a, \kappa_a, \epsilon_a \,|\, a \in K \,\}$ of size $3|K|$ and $G_L(K) = \langle D_L(K) \rangle$. Thus $G(L) = G_L(L)$ and $D(L) = D_L(L)$. Always $G_L(K)$ contains the identity line $I(L) = \langle \rho_1, \kappa_1, \epsilon_1 \rangle \simeq Sym(3)$ and so admits the triality.

**(2.6)** Proposition. *Let $L$ be a Moufang loop. Set $G = G(L)$, $D = D(L)$, and $\pi = \pi_L$.*

(1) *Let $K$ be a subloop of $L$. Then $H = G_L(K)$ is a triality subgroup of $G$ with reflection class $D_L(K) = D \cap H = D \cap N_G(H)$ and projection map equal to the restriction $\pi|_H$. We have $|D \cap H| = 3|K|$, and $H$ is a central quotient of $Univ(K)$ as group with triality.*

(2) *If $I(L) \leq N \leq G$, then there is a subloop $K$ of $L$ with $D_L(K) = D \cap N$ and $G_L(K) = \langle D \cap N \rangle$.*

(3) *If $K$ is a maximal subloop of $L$, then $N_G(G_L(K))$ is a maximal subgroup of $G$ with $G = \ker(\pi).N_G(G_L(K))$.*

Proof. (1) As $G_L(K)$ contains $I(L)$, it admits the triality by Lemma 2.3. By Proposition 2.5, $G_L(K)$ is a central quotient of $Univ(K)$ and $|D \cap H| = |D_L(K)| = 3|K|$. By Lemma 2.4.1 applied to $N_G(H)$, the set $D \cap N_G(H)$ is a single conjugacy class of $N_G(H)$ and so must be the class $D \cap H$.

(2) Let $M = \ker(\pi)$. We know that $\rho_1$ acts on $C = D \cap \kappa_1 M$ and $E = D \cap \epsilon_1 M$ via

$$a_C{\cdot}\rho_1 = (a^{-1})_E \quad \text{and} \quad a_E{\cdot}\rho_1 = (a^{-1})_C\,,$$

for all $a \in L$. To describe its action on $R = D \cap \rho_1 M$, consider $l = [\,a, a^{-1}, 1\,] = \{a_R, (a^{-1})_C, 1_E\}$, a line of $A(L)$. Thus

$$l.\rho_1 = \{a_R{\cdot}\rho_1, (a^{-1})_C{\cdot}\rho_1, 1_E{\cdot}\rho_1\} = \{a_R{\cdot}\rho_1, a_E, 1_C\} = [\,a.\rho_1, 1, a\,]$$

is also in $A(L)$. The unique line of shape $[\,*, 1, a\,]$ is $[\,a^{-1}, 1, a\,]$, so we conclude that $a_R.\rho_1 = (a^{-1})_R$. Similar statements hold for $\kappa_1$ and $\epsilon_1$, giving

$$a_R.\rho_1 = (a^{-1})_R\,, \quad a_C.\kappa_1 = (a^{-1})_C\,, \quad a_E.\epsilon_1 = (a^{-1})_E\,,$$

for all $a \in L$. This in turn allows us to calculate the action of $t = \kappa_1\rho_1$ on $D$, and we find $t = (R, C, E)$ ; that is,

$$a_R.t = a_C\,, \quad a_C.t = a_E\,, \quad a_E.t = a_R\,,$$

for all $a \in L$.

Let $K = \{\, a \in L \,|\, \rho_a \in N\,\}$. As $t \in I(L) \leq N$, we have also $K = \{\, a \in L \,|\, \kappa_a \in N\,\} = \{\, a \in L \,|\, \epsilon_a \in N\,\}$. As $\rho_1 \in I(L) \leq N$, the subset $K$ of $L$ contains 1 and is closed under inverses. If $a, b \in K$ then $\rho_a, \kappa_b \in N$ and $\rho_a\kappa_b\rho_a = \epsilon_c \in N$, thus $c = (ab)^{-1} \in K$ and $ab \in K$. Therefore $K$ is a subloop of $L$; so we have verified $D \cap N = D_L(K)$ and $\langle D \cap N\rangle = G_L(K)$, as claimed.

(3) As $N = N_G(G_L(K)) = N_G(D_L(K))$ (by (1)) contains the line $I(L)$, we have $G = \ker(\pi).N$. Suppose $N$ is not maximal in $G$, and choose $n \in G\backslash N$ with $N^* = \langle n, N\rangle$ proper in $G$. As $n \notin N$, we have $(D{\cap}N)^n \neq D{\cap}N = D_L(K)$. Thus $D \supset D{\cap}N^* \supset D{\cap}N$. By (2), there is a subloop $K^*$ of $L$ with $D(K^*) = D \cap N^*$ and $L > K^* > K$. Therefore $K$ is not maximal in $L$.

# 3 Paige loops and their groups

The fundamental group theoretic result in the classification of finite, nonassociative, simple Moufang loops was the following:

**(3.1)** THEOREM. (DORO [7], LIEBECK [15]) *Let $(G, D, \pi)$ be a finite group with triality, and let $I$ be a line of $G$. Let $M$ be a semisimple, $I$-invariant subgroup of $G$, and let $E$ be a nonabelian simple direct factor of $M$. Then we have one of:*

(1) $[E, I] = 1$*;*

(2) $\langle E, I\rangle \simeq E^3{:}I$*, a wreathed product;*

(3) $\langle E, I\rangle = E{:}I \simeq P\Omega_8^+(q){:}Sym(3)$*, for some $q$, and $I$ is uniquely determined within $E{:}I$ up to conjugacy.*

PROOF. The transitive $I$-space $\Omega = \{E^I\}$ has size dividing 6. As $\langle\Omega\rangle.I$ admits the triality, $|\Omega|$ is not 2 or 6 by [7, Prop. 1]. In the same place, Doro showed that $|\Omega| = 3$ gives the wreathed case (2).

If $|\Omega| = 1$, then either $[I, E] = 1$ or $I$ induces outer automorphisms on $E$ by [7, Cor. 4, p.382]. In the latter case, Liebeck [15] showed we must have (3).

Doro [7] also showed that, under Theorem 3.1.2, the loop $\mathcal{L}(\langle E, I\rangle)$ is isomorphic to the group $E$. Therefore our verification of the Lagrange property involves a careful study of the group and associated loop occuring under Theorem 3.1.3.

Over the finite field $\mathbb{F}_q$ a nondegenerate 8-dimensional composition algebra is uniquely determined up to isomorphism as the $\mathbb{F}_q$-algebra of split octonians $Oct(q)$ ([19, §2]). These can be conveniently written as Zorn's vector matrices

$$m = \begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix}$$

with $a, d \in \mathbb{F}_q$ and $\vec{b}, \vec{c} \in \mathbb{F}_q^3$. Multiplication is given by

$$\begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix} \begin{bmatrix} x & \vec{y} \\ \vec{z} & w \end{bmatrix} = \begin{bmatrix} ax + \vec{b} \cdot \vec{z} & a\vec{y} + w\vec{b} - \vec{c} \times \vec{z} \\ x\vec{c} + d\vec{z} + \vec{b} \times \vec{y} & \vec{c} \cdot \vec{y} + dw \end{bmatrix}$$

using the standard dot and cross products of 3-vectors. The associated quadratic form, which admits composition, is the norm (or determinant) $\Delta(m) = ad - \vec{b} \cdot \vec{c}$. (See [15] for a different rendering of $Oct(q)$.)

In $Oct(q)$ an element $m$ is invertible if and only if $\Delta(m) \neq 0$, and the loop of units $GLL(q)$ is a Moufang loop. This possesses a normal subloop $SLL(q)$ consisting of all units with norm 1. The scalars of $SLL(q)$ form a normal subloop $\{\pm I\}$ of order $d = \gcd(q-1, 2)$, and the Paige loop is the quotient $P(q) = PSLL(q) = SLL(q)/\{\pm I\}$. (See [19] for all of this.) The Zorn construction of the split octonian algebra $Oct(F)$ and its Moufang loop of units $GLL(F)$ can be made over arbitrary fields $F$. Also of interest is the quotient of the full unit loop by scalars: $PGLL(F) = GLL(F)/\{\, \alpha I \mid \alpha \in F\,\}$. The Paige loop $P(q)$ has index $d$ in $PGLL(q)$ as the squares of $\mathbb{F}_q^*$ have index $d$ in $\mathbb{F}_q^*$.

**(3.2)** Theorem. (Paige [19]) *The loop $P(q)$ is a simple, nonassociative, Moufang loop. We have $|P(q)| = q^3(q^4-1)/d$, where $d = \gcd(q-1, 2)$.*

**(3.3)** Lemma. *For prime power $q$, set $d = \gcd(q-1, 2)$ and $\ell(q) = q^3(q^4-1)/d$.*

(1) *If $q_0$ divides $q$, then $\ell(q_0)$ divides $\ell(q)$.*

(2) *If odd $q_0^2 = q$, then $2\ell(q_0)$ divides $\ell(q)$.*

(3) *$\ell(2) = 120$ divides $\ell(q)$, for all $q$.*

Proof. This is elementary.

We have $G(P(q)) = P\Omega_8^+(q){:}Sym(3)$ as in Theorem 3.1.3. This is well-known [7, 15] and a consequence of Theorems 3.1 and 3.2. An elementary proof, using only the Cartan-Dieudonné Theorem [21, Theorem 11.39], that $G(P(F)) = P\Omega_8^+(F){:}Sym(3)$, for all fields $F$, can easily be extracted from [2, Theorem 1]. Also evident from [2] is that a triality reflection of $P\Omega_8^+(F){:}Sym(3)$ induces a reflection on $PO_8^+(F)$ (discussed further below) and that $\ker(\pi)$ is the corresponding rotation subgroup $P\Omega_8^+(F)$ (hence the terminology). The normal subgroup of $\mathrm{Aut}(P\Omega_8^+(q))$ generated by this reflection class is $P\Omega_8^+(q){:}Sym(3)$ when $q$ is even but is $P\Omega_8^+(q){:}Sym(4)$ when $q$ is odd. For odd $q$, within $\mathrm{Aut}(P\Omega_8^+(q))$ there are four triality subgroups $P\Omega_8^+(q){:}Sym(3)$, permuted faithfully by $P\Omega_8^+(q){:}Sym(4)/P\Omega_8^+(q) \simeq Sym(4)$. See also [14, §1.4]. (More generally [2], the normal subgroup $G^*$ of $\mathrm{Aut}(P\Omega_8^+(F))$ generated by the reflection class has $G^*/P\Omega_8^+(F) \simeq Q^2{:}Sym(3)$, where $Q$ is the multiplicative group of the field $F$ modulo its squares. Indeed $G^* = G(PGLL(F))$, the triality group associated with the octonian loop of units modulo scalars.)

The related group $O_8^+(q)$ acts as the full isometry group of the 8-dimensional orthogonal space $(V, \Delta)$, where $V = \mathbb{F}_q^8$ is the vector space carrying $Oct(q)$. This orthogonal space has $+$-*type*; that is, it is the perpendicular direct sum of nondegenerate 2-spaces, each of which contains singular vectors. A vector $v$ is *singular* if $\Delta(v) = 0$, in which case the subspace spanned by $v$ is also *singular.* A nonsingular 1-space is of $+$-*type* if all its $\Delta$ values are squares and otherwise is of $-$-*type.* (Thus a 1-space is of $+$-type if and only if it contains a vector $v$ with $\Delta(v) = 1$.) A nondegenerate subspace is of $-$-*type* if it is not of $+$-type, and a subspace is *totally singular* if all its vectors are singular.

The intersection of $PO_8^+(q)$ with $P\Omega_8^+(q){:}Sym(3)$ is $P\Omega_8^+(q)\langle r\rangle$ where $r$ represents a $+$-reflection $\hat{r}$ of $O_8^+(q)$. In saying that $\hat{r}$ is a $+$-*reflection* we mean that, for its action on $V$, the *center* $[V, \hat{r}] = V(\hat{r} - 1)$ is a nonsingular 1-space of $+$-type (so in characteristic 2, the $+$-reflections are actually transvections).

Recall that a subspace $W$ of $V$ is invariant under the $+$-reflection $s$ if and only if either $W$ contains the center $[V, s]$ or $W$ is perpendicular to the center: $W \le [V, s]^\perp = C_V(s)$.

In odd characteristic $\mathrm{Aut}(P\Omega_8^+(q))$ does not act on $\Omega_8^+(q)$ but instead on its double cover $Spin_8^+(q)$. Nevertheless, we occasionally abuse terminology by discussing the action of elements and subgroups $H$ of $P\Omega_8^+(q){:}Sym(3)$ on the underlying vector space $V$, for instance, blurring the distinction between a $+$-reflection $\hat{r}$ of $O_8^+(q)$ and the element $r$ of $PO_8^+(q)$ representing it. For $H \le PO_8^+(q)$ we should more properly lift $H$ to a subgroup $\hat{H} \le O_8^+(q)$, so that $H \simeq \hat{H}/\hat{Z}$ with $\hat{Z} = Z(O_8^+(q))$ of order $\gcd(q-1, 2)$. Further care is required when $H$ is not conjugate into $PO_8^+(q)$ (that is, when 3 divides $|\pi(H)|$). In that case, we must confine our discussion to the way $H$ acts on the set of subspaces of the associated $D_4$ geometry—the set $S^1$ of totally singular 1-spaces, the set $S^2$ of totally singular 2-spaces, and the two classes $S_1^4$ and $S_2^4$ of totally singular 4-spaces of $V$. (Two totally singular 4-spaces $W_1$ and $W_2$ belong to the same class if and only if $W_1 \cap W_2$ has even dimension.) The group $P\Omega_8^+(q){:}Sym(3)$ leaves $S^2$ invariant and permutes the members of $S^1 \cup S_1^4 \cup S_2^4$, inducing $Sym(3)$ on $\{S^1, S_1^4, S_2^4\}$. See [2, §§2-3].

We make extensive use of Kleidman's work [14] on maximal subgroups of groups $G$ for $P\Omega_8^+(q) \le G \le \mathrm{Aut}(P\Omega_8^+(q))$. In particular, we use his notation for such maximal subgroups.

**(3.4)** Theorem. *Let $N$ be a maximal subgroup of $G = P\Omega_8^+(q){:}Sym(3)$ with $G = P\Omega_8^+(q).N$. Then $N_0 = N \cap P\Omega_8^+(q)$ has one of the types:*

$$G_2, K_3, S_a, S_2, K_5, N_1, N_2, N_3, N_4, P_2, R_{s2}, I_{+2}, I_{-2}, I_{+4}\,.$$

*Conversely, for each of these types, there is a unique $P\Omega_8^+(q)$-conjugacy class of subgroups $N_0$ with $G = N_G(N_0)P\Omega_8^+(q)$.*

Proof. By Kleidman's results [14, Prop. 4.2.1, Table III], all such $N_0$ must have one of these types or $K_4$ or $K_6$. But subgroups $N_0$ of those two types have $P\Omega_8^+(q)N_G(N_0)$ proper in $G$; see [14, 2.3.4,2.3.9].

Uniqueness follows immediately from [14, Table I], except when $q$ is odd and $N_0$ has type $K_3$, $S_2$, $K_5$, or $N_4$. In the exceptional cases $P\Omega_8^+(q)$ has four conjugacy classes of subgroups $N_0$, and these are permuted by $\mathrm{Aut}(P\Omega_8^+(q))$ and $P\Omega_8^+(q){:}Sym(4)$ with induced action $Sym(4)$. Therefore exactly one of the classes satisfies $G = P\Omega_8^+(q)N_G(N_0)$.

In Table K below, we have extracted what is most important for us from Kleidman's Tables I [14, pp.186–191] and III [14, p.238]. Table K lists the conjugacy classes of subgroups $N_0$ of $P\Omega_8^+(q)$ for which $N = N_G(N_0)$ is maximal in $G = P\Omega_8^+(q){:}Sym(3)$ and has $P\Omega_8^+(q).N = G$. We call such an $N$ a maximal complementing subgroup of $P\Omega_8^+(q){:}Sym(3)$. A complementing $N$ might not contain reflections and so not admit the triality. (In fact only in the cases $K_3$ and $N_3$ does complementing $N$ fail to admit the triality [9].)

The first column of the table lists Kleidman's names for the cases. (We have surpressed Kleidman's additional superscripts, since he must consider more than one class while we only have one.) The second column gives the isomorphism type of $N_0$. Here the symbol $\downarrow$ indicates that the subgroup described is actually the preimage in $\Omega_8^+(q)$, so a central subgroup of order $d = \gcd(q-1, 2)$ must be factored out. The third column provides restrictions on the field $\mathbb{F}_q$ and characteristic $p$ without which the corresponding $N$ is not maximal. The notation $\frac{1}{d}A$ indicates a subgroup of index $d$ in $A$. The group $A^a$ is the direct product of $a$ copies of $A$; especially $p^a$ is elementary abelian of that order. A group $[q^a]$ has order $q^a$ but undescribed isomorphism type.

**Table K.** Maximal complementing subgroups of $P\Omega_8^+(q){:}Sym(3)$

| Name | Isomorphism type of $N_0$ | Restrictions |
|---|---|---|
| $G_2$ | $G_2(q)$ | – |
| $K_3$ | $PGL_3^\epsilon(q)$ | $\epsilon = \pm,\ 2 < q \equiv \epsilon 1 \pmod 3$ |
| $S_a$ | $P\Omega_8^+(q_0)$ | $q = q_0^a$, $a$ prime |
| $S_2$ | $P\Omega_8^+(q_0).2^2$ | $q = q_0^2$, odd |
| $K_5$ | $P\Omega_8^+(2)$ | $q = p \geq 3$ |
| $N_1$ | $\downarrow\left(\frac{1}{d}Z_{q+1} \times \frac{1}{d}GU_3(q)\right).2^d$ | – |
| $N_2$ | $\downarrow\left(\frac{1}{d}Z_{q-1} \times \frac{1}{d}GL_3(q)\right).2^d$ | $q \geq 4$ |
| $N_3$ | $\left(D_{(2/d)(q^2+1)} \times D_{(2/d)(q^2+1)}\right).2^2$ | $q \neq 3$ |
| $N_4$ | $[2^9]{:}GL_3(2)$ | $q = p \geq 3$ |
| $P_2$ | $\downarrow[q^{11}]\left(\frac{1}{d}Z_{q-1}\right)^2{:}\frac{1}{d}GL_2(q).d^2$ | – |
| $R_{s2}$ | $\downarrow[q^9]{:}\left(\frac{1}{d}GL_2(q) \times \Omega_4^+(q)\right).d$ | – |
| $I_{+2}$ | $\downarrow\left(\frac{1}{d}Z_{q-1}\right)^4.d^3.2^3.Sym(4)$ | $q \geq 7$ |
| $I_{-2}$ | $\downarrow\left(\frac{1}{d}Z_{q+1}\right)^4.d^3.2^3.Sym(4)$ | $q \neq 3$ |
| $I_{+4}$ | $\left(\Omega_4^+(q) \circ \Omega_4^+(q)\right).2.2^d$ | $q \geq 3$ |

# 4 Maximal triality subgroups of $P\Omega_8^+(q){:}Sym(3)$

**(4.1)** Theorem. *Let $G = P\Omega_8^+(q){:}Sym(3)$ with $D$ its class of triality reflections. If $N$ is a maximal subgroup of $G$ with $G = P\Omega_8^+(q).\langle D \cap N\rangle$, then $|D\cap N|$ divides $|D|$.*

Given this theorem, we have

Proof of Theorem 1.1:

Let $L$ be a finite Moufang loop and $K$ a subloop. The proof is by induction on $|L|$, the result being clear for $|L| = 1$.

By [4, Lemma V.2.1] and induction, $L$ is simple. (Lemma 2.4.2 could also be used in place of the reference.) As Lagrange's Theorem holds in groups, we may assume that $L$ is nonassociative. Therefore by Liebeck's theorem [15], $L$ is $P(q)$ for some prime power $q$.

The result is evident if $L = K$, so we may assume that $K$ is proper in $L$ and let $K_1$ be a maximal subloop of $L$ containing $K$. By induction $|K|$ divides $|K_1|$, so we are reduced to the case in which $K_1 = K$ is a maximal subloop of $L$.

Let $N$ be the normalizer of $G_L(K)$ in $G = G(L) = P\Omega_8^+(q){:}Sym(3)$. By Proposition 2.6.3, $N$ is a maximal subgroup of $G$ with $G = P\Omega_8^+(q).N$. By Proposition 2.6.1 and Theorem 4.1, $3|K| = |D\cap N|$ divides $|D| = 3|L|$. Therefore $|K|$ divides $|L|$, as desired.

It remains to prove Theorem 4.1. Let $G = P\Omega_8^+(q){:}Sym(3)$ with $D$ its class of triality reflections. By Theorem 3.1.3, the class $D$ is uniquely determined as is the line class $I^G$. The projection $\pi$ is also unique, given by $\pi{:}\, G \longrightarrow G/G'' \simeq Sym(3)$. We let $M$ be the rotation subgroup $\ker(\pi) = G'' = P\Omega_8^+(q)$. Fix a line $I$, and let $O_3(I) = \langle t\rangle$ and $r = D \cap I \cap PO_8^+(q)$. Set $d = \gcd(q-1, 2)$. By Proposition 2.6 and Theorem 3.2 we have $|D| = 3|P(q)| = 3\ell(q) = 3q^3(q^4-1)/d$.

Let $N$ be maximal in $G$ as in Theorem 4.1. Therefore $N$ is a maximal complementing subgroup in $G$, and the group $N_0 = N \cap M$ has one of the types on Kleidman's list as given in Theorem 3.4 and Table K. We treat the various cases in a sequence of propositions. By Theorem 3.1.3 we may assume $I \leq N$, so $N = N_0{:}I$.

The involution $r$ of $I$ is a $+$-reflection of $PO_8^+(q)$. It is important that, by Lemma 2.4.1, the set $D\cap rN_0 = r^{N_0}$ consists of all the $+$-reflections of $PO_8^+(q)$ that are contained in $N$. Therefore when $N$ and $N_0$ have natural geometric descriptions in terms of $V = \mathbb{F}_q^8$, the number $|D \cap N| = 3|D \cap rN_0|$ can be calculated by counting $+$-reflections or their associated centers.

**(4.2)** Lemma. *Let $H_0$ be a normal subgroup of $N_0$ with $C_{N_0}(H_0) = 1$. Then either $[H_0, I] \neq 1$ or $[N_0, I] = 1$.*

Proof. If $[H_0, I] = 1$, then $I = C_N(H_0)$ is normal in $N = N_0{:}I$. Therefore $[N_0, I] \leq N_0 \cap I = 1$.

**(4.3)** Proposition. (1) *The group $N_0$ has type $G_2$ if and only if $N = N_0 \times I$. In this case $N = N_G(\langle t\rangle) = N_G(I) \simeq G_2(q) \times Sym(3)$ and $|D \cap N| = 3$.*

(2) *The group $N_0$ does not have type $K_3$.*

Proof. For $N_0$ of type $G_2$ or $K_3$, the derived group $H_0 = N_0'$ is a simple group not isomorphic to any $P\Omega_8^+(q_0)$ and has trivial centralizer in $N_0$.

The subgroup $H_0.I$ admits the triality, so by Theorem 3.1 we must have $[H_0, I] = 1$. By Lemma 4.2, we have $[N_0, I] = 1$. (Here and elsewhere we use Theorem 3.1 in the form: if $I$ normalizes $B \leq M$ and $I$ does not centralize a nonsolvable $B$-composition factor, then the isomorphism type of that factor either is $P\Omega_8^+(q_0)$, for some $q_0$, or appears as an $B$-composition factor with multiplicity at least three.)

In (1), $N_0 \simeq G_2(q)$ is indeed centralized by $I$ and is also the centralizer in $M$ of the 3-element $t$. (See [14, Prop. 3.1.1].)

In (2), $N_0$ is $PGL_3(q)\,(= PGL_3^+(q))$ or $PGU_3(q)\,(= PGL_3^-(q))$. We have $N = N_0.I < N_G(I)$ of type $G_2$, against maximality.

In view of Proposition 4.3 we may now assume that $N_0$ is not contained in $C_G(I) = C_M(t) = N_M(\langle t\rangle) = N_M(I)$. Indeed, we may assume that $I$ centralizes no appropriate $H_0$ as in Lemma 4.2.

**(4.4)** Proposition. *If $N_0$ has type $S_a$, $S_2$, or $K_5$, then $|D \cap N|$ is, respectively, $3\ell(q_0)$ (for $q = q_0^a$), $6\ell(q_0)$ (for $q = q_0^2$), or $3\ell(2)$ and divides $|D| = 3\ell(q)$.*

Proof. For $S_a$ and $K_5$, the subgroup $N_0$ is $P\Omega_8^+(q_0)$ with, respectively, $q = q_0^a$ and $q_0 = 2$. As $I$ acts nontrivially on $N_0$, by Theorem 3.1 we have $\langle D \cap N\rangle = P\Omega_8^+(q_0){:}Sym(3)$. In this case $|D \cap N| = 3\ell(q_0)$ by Theorems 3.1.3 and 3.2. Therefore $|D \cap N|$ divides $|D| = 3\ell(q)$ by Theorem 3.2 and Lemma 3.3.

For $S_2$, $N_0$ is $P\Omega_8^+(q_0).2^2$ with $q = q_0^2$, odd. By Lemma 4.2, $I$ acts nontrivially on $N_0' = P\Omega_8^+(q)$, hence by Theorem 3.1 we have $N_0'.I = P\Omega_8^+(q_0){:}Sym(3)$. Therefore $N_0.I = N \simeq P\Omega_8^+(q_0){:}Sym(4) \leq \mathrm{Aut}(P\Omega_8^+(q_0))$. Hence $|D \cap N| = 6\ell(q_0)$, a divisor of $|D| = 3\ell(q_0^2)$ by Theorem 3.2 and Lemma 3.3.2.

Remark. Indeed $G$ does contain subgroups with triality of each of these types [9].

For $N_0$ of type $S_a$, we have $P\Omega_8^+(q_0){:}Sym(3)$ with $q_0^a = q$, corresponding to the subfield subloop $P(q_0)$ of $P(q)$. For $N_0$ of type $S_2$, we have $G_L(K) = P\Omega_8^+(q_0){:}Sym(4)$, corresponding within $P(q_0^2)$ to the subloop $K = PGLL(q_0)$ of all unit octonians over $\mathbb{F}_{q_0}$ (not just those of norm 1) modulo scalars, since the nonsquares of $\mathbb{F}_{q_0}$ are squares in $\mathbb{F}_{q_0^2}$.

The unit integral octonians span (modulo $\{\pm I\}$) a subloop $P(2)$ [6]. Therefore all Paige loops $P(F)$ contain $P(2)$, as in $K_5$.

**(4.5)** Proposition. *If $N_0$ has type $N_1$ or $N_2$, then $|D \cap N|$ is, respectively, $3(q+1)/d$ or $3(q-1)/d$ and so divides $|D|$.*

Proof. By Lemma 2.4, $|D\cap N| = 3|D\cap rN_0|$. Here $D\cap rN_0 = r^{N_0}$ consists of those $+$-reflections of $PO_8^+(q)$ that are in $N$.

See [14, Prop. 3.2.2-3]. Set $N_- = N_1$ and $N_+ = N_2$. Then $N_0$ of type $N_\epsilon$ leaves invariant a decomposition $V = U_\epsilon \perp W_\epsilon$, where $U_\epsilon$ is a nondegenerate 2-space of $\epsilon$-type. On $U_\epsilon$ the group $N_0$ induces at least $\Omega_2^\epsilon(q) \simeq Z_{q-\epsilon 1}$, transitive on the nonsingular 1-spaces of $+$-type in $U_\epsilon$. If $(q,\epsilon) = (2,-)$, set $E = N_0'$ and otherwise set $E = N_0''$. Then the nondegenerate 6-space $W_\epsilon = [V,E]$ of $\epsilon$-type admits the characteristic subgroup $E \simeq SL_3^\epsilon(q)$ of $N_0$ acting irreducibly. (Here $SL_3^+(q) = SL_3(q)$ and $SL_3^-(q) = SU_3(q)$.) Elements of $rN_0$ must therefore respect the decomposition.

If $(q,\epsilon) \neq (2,-)$ then $E$ is quasisimple, and $[I,E] = 1$ by Theorem 3.1.3. When $(q,\epsilon) = (2,-)$, the characteristic subgroup $Z(E) \simeq Z_3$ is fixed-point-free on $W_-$; so the $+$-reflection $r$ does not invert $Z(E)$ and instead must centralize it. Therefore in all cases no $+$-reflection of $r^{N_0}$ has its center in $W_\epsilon$.

A $+$-reflection $s$ of $r^{N_0}$ must leave $W_\epsilon$ invariant, so by the previous paragraph its center belongs to $W_\epsilon^\perp = U_\epsilon$. Conversely, the $+$-reflection $r$ has its center in $U_\epsilon$, so $r^{N_0}$ contains all $+$-reflections with center in $U_\epsilon$. Thus we have $|D\cap N| = 3|D\cap rN_0| = 3(q-\epsilon 1)/d$, always a divisor of $3\ell(q) = 3q^3(q^4-1)/d$.

Remark. Here we find subloops of order $(q-\epsilon 1)/d$ that are cyclic subgroups of $P(q)$ [9]. Especially they are not maximal, since Moufang proved that all 2-generated Moufang loops are groups ([4, §7.4],[20, IV.2.1]).

**(4.6)** Proposition. *$N_0$ does not have type $N_3$.*

Proof. A subgroup $N_0$ of type $N_3$ is the normalizer of a Sylow $l$-subgroup, for any odd prime divisor $l$ of $q^2+1$. (See [14, Prop. 3.3.1] for properties of subgroups of type $N_3$.) $N_0$ leaves invariant a direct sum decomposition into 4-spaces, $V = W_0 \perp W_1$. It contains a characteristic subgroup $Z \simeq Z_l \times Z_l$ that acts on each $W_i$ irreducibly without fixed points, the two representations not being isomorphic. An element $g \in O_8^+(q)$ of order 2 that switches $W_0$ and $W_1$ has $[V,g]$ of dimension 4 and so is not a reflection. A $+$-reflection $s$ of $N$ would therefore fix each $W_i$, acting on $Z$ and the induced $Z_l$. But then, for $1 \neq z \in Z$, the dihedral group $S = \langle s, s^z\rangle$ of order $2l$ would be irreducible on $[W_i, S] = W_i$, a 4-space, for one of the values of $i$. This is impossible since $S$ is generated by two reflections.

**(4.7)** Proposition. *If $N_0$ has type $N_4$, then $|D\cap N|$ divides 24 and so divides $|D|$.*

Proof. Here $N_0 \simeq [2^9]{:}GL_3(2)$, where $S = O_2(N_0)$ of order $2^9$ has $S' = Z(S) \simeq 2^3$ with $GL_3(2)$ acting naturally. (In [14] see 3.4.2 and the proof of 4.1.10.)

By Theorem 3.1.3 we have $[I, N_0] \leq S$. Let $H \leq N_0$ with $H \simeq GL_3(2)$. The 3-element $t$ of $I$ must have a fixed point in its action on the $N$-space $\{H^{N_0}\} = \{H^S\}$ of size a power of 2. Therefore we may assume $t \in N_G(H)$. But then $[t,H] \leq H\cap S = 1$, so $H \leq C_M(t) = C_M(I)$ by Proposition 4.3.1.

The group $I \times H$ acts on $Z(S)$ with $H$ irreducible, so $[I, Z(S)] = 1$. With $\bar{N} = N/Z(S)$, we then have by the previous paragraph and Lemma 2.4

$$|D \cap N| = |D \cap IS| = |\bar{D} \cap \overline{IS}| = 3|\bar{D} \cap \bar{r}^{\bar{S}}|\,.$$

As $\bar{S}$ is abelian of order $2^6$, we find that $|D \cap N|$ divides $3.2^3$. By Lemma 3.3.3, this divides $|D|$.

Remark. Maximal subgroups of type $N_4$ only occur when $q$ is an odd prime. In that case $D \cap N$ has size exactly $3.2^3 = 24$; see [9]. The $+$-reflections of $rN_0$ are those with centers from an orthonormal basis for $V$, eigenvectors for $Z(S)$. The corresponding subloop is an elementary abelian group of order 8.

**(4.8)** Proposition. *If $N_0$ has type $P_2$ or $R_{s2}$, then $|D \cap N|$ is, respectively, $3q^3(q-1)/d$ or $3q^3(q^2-1)/d$ and so divides $|D|$.*

Proof. Let $N_0$ have type $R_{s2}$. There is a totally singular 2-space $T$ of $V$ with $N_0$ its stabilizer in $M$ and $N$ its stabilizer in $G$. (See [14, p.194].) As $T$ is totally singular, the $+$-reflection $a$ fixes $T$ if and only if its center $Z = [V, a]$ is perpendicular to $T$. The subspace $T^\perp$ is equal to $T \oplus Y$, where $Y$ is a nondegenerate 4-space of $+$-type. The subspace $Y$ contains $q(q^2-1)/d$ nonsingular 1-spaces of $+$-type, so $T^\perp$ contains $q^2 \cdot q(q^2-1)/d$ such 1-spaces. Therefore $|D \cap N| = 3q^3(q^2-1)/d$, a divisor of $|D| = 3\ell(q) = 3q^3(q^4-1)/d$, as desired.

Suppose $N_0$ has type $P_2$. Thus $N_0$ is the stabilizer of a singular 1-space $U$ and two totally singular 4-spaces, $W_1$ and $W_2$, with $U$ contained in the subspace $W_1 \cap W_2$ of dimension 3. (See [14, p.192].) In the action of $G = P\Omega_8^+(q){:}Sym(3)$ on its $D_4$ geometry, the subgroup $N$ is the global stabilizer of the set $\{U, W_1, W_2\}$, permuting these as $Sym(3)$.

Consider a $+$-reflection $a$ of $rN_0$. The element $a$ fixes $U$ and switches $W_1$ and $W_2$. The center $Z = [V, a]$ is nonsingular of $+$-type. The reflection $a$ fixes the 5-space $W = W_1 + W_2$. As $W \geq W^\perp = W_1 \cap W_2$, we must have $Z \leq W$. Conversely, for any $+$-reflection $b$ with $[V, b] \leq W$, we have $b$ switching $W_1$ and $W_2$, the only two maximal totally singular subspaces of $W$. Also $b$ fixes $U$, since $U$ is in $b$-invariant $W_1 \cap W_2$, a totally singular subspace of $[V, b]^\perp = C_V(b)$. Therefore $b \in rN_0$.

Thus $|D \cap rN_0|$ equals the number of 1-spaces in $W$ of $+$-type. Here $W$ is the perpendicular direct sum of the totally singular 3-space $W_1 \cap W_2$ and a nondegenerate 2-space $X$ of $+$-type. The subspace $X$ contains $(q-1)/d$ nonsingular 1-spaces of $+$-type, so $W$ contains $q^3 \cdot (q-1)/d$ such 1-spaces.

Therefore $|D \cap N| = 3q^3(q-1)/d$ also divides $3\ell(q)$, as desired.

Remark. Corresponding loops of cardinality $q^3(q^e-1)/d$, with $e = 1, 2$, do exist [9]. In fact, a loop for type $P_2$ is a subloop of a loop for type $R_{s2}$.

**(4.9)** Proposition. *If $N_0$ has type $I_{+2}$, $I_{-2}$, or $I_{+4}$, then $|D \cap N|$ is, respectively, $12(q-1)/d$, $12(q+1)/d$, or $6q(q^2-1)/d$ and so divides $|D|$.*

PROOF. For type $I_{\epsilon e}$ with $\epsilon = \pm$ and $e = 2, 4$, the group $N_0$ is maximal in $PO_8^+(q)$ (for appropriate $q$) and leaves invariant a unique decomposition of $V$ as the perpendicular direct sum of $8/e$ component $e$-spaces, each nondegenerate of $\epsilon$-type. (See [14, p.177 and 194].)

The reflections of $rN_0$ must respect this decomposition. An element that switches two of the components has commutator dimension at least 2 and so is not a reflection. On the other hand, any +-reflection whose center belongs to one of the components leaves the decomposition invariant and so belongs to $rN_0$. For $e = 2$, this gives $|D \cap rN_0| = 4 \cdot (q - \epsilon 1)/d$; and, for $e = 4$ and $\epsilon = +$, this gives $|D \cap rN_0| = 2 \cdot q(q^2 - 1)/d$. In all cases, we have $|D \cap N|$ a divisor of $3\ell(q) = 3q^3(q^2 - 1)(q^2 + 1)/d$, as desired.

REMARK. The loops corresponding to the cases $I_{\epsilon 2}$ are in fact subloops of loops coming from the case $I_{+4}$; see [9].

Theorem 4.1 now follows from Theorem 3.4 and Propositions 4.3-4.9.

REMARK. As the remarks of this section indicate, the present arguments come close to, but fall short of, a classification of the maximal subloops of the finite Paige loops. We have given the order of the reflection class in each case. This determines the order of the corresponding subloops, but there could be isotopic, nonisomorphic loops (necessarily of the same order) corresponding to the same class. (In fact, this does not happen.) It is also the case that the various loops may not be maximal. Indeed, the only maximal subloops come under types $S_a$, $S_2$, $K_5$, $R_{s2}$, and $I_{+4}$. (When $q = 2$, a subgroup of type $I_{+4}$ is contained properly in one of type $I_{-2}$, but the two subgroups correspond to the same maximal subloop of order 12.) See [9, 12, 17] for full discussion and resolution of these questions.

ACKNOWLEDGEMENTS. We thank Michael Kinyon and Gábor Nagy for bringing the results of [11] to our attention, and we thank Doctors Grishkov and Zavarnitsine for their understanding and encouragement.

# References

[1] M. Aschbacher, “Finite Group Theory,” Second edition, Cambridge Studies in Advanced Mathematics, **10**, Cambridge University Press, Cambridge, 2000.

[2] F. van der Blij and T.A. Springer, Octaves and triality, Nieuw Arch. Wisk., **8** (1960), 158–169.

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

[4] R.H. Bruck, “A Survey of Binary Systems,” Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[5] O. Chein, M.K. Kinyon, A. Rajah, P. Vojtěchovský, Loops and the Lagrange property, Results Math., **43** (2003), 74–78.

[6] H.S.M. Coxeter, Integral Cayley numbers, Duke Math. J., **13** (1946), 561–578.

[7] S. Doro, Simple Moufang loops, Math. Proc. Cambridge Philos. Soc., **83** (1978), 377–392.

[8] M. Funk and P.T. Nagy, On collineation groups generated by Bol reflections, J. Geom., **48** (1993), 63–78.

[9] S.M. Gagola III, Ph.D. thesis, Michigan State University, 2005.

[10] G. Glauberman, On loops of odd order, I, J. Algebra, **1** (1964), 374–396, II, J. Algebra, **8** (1968), 393–414.

[11] A.N. Grishkov and A.V. Zavarnitsine, Lagrange's theorem for Moufang loops, Math. Proc. Cambridge Philos. Soc., to appear.

[12] A.N. Grishkov and A.V. Zavarnitsine, Maximal subloops of simple Moufang loops, preprint 2004, 43 pages.

[13] J.I. Hall and G.P. Nagy, On Moufang 3-nets and groups with triality, Acta Sci. Math. (Szeged), **67** (2001), 675–685.

[14] 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** (1987), 173–242.

[15] M.W. Liebeck, The classification of finite simple Moufang loops, Math. Proc. Cambridge Philos. Soc., **102** (1987), 33–47.

[16] M.L. Merlini Giuliani and C. Polcino Milies, On the structure of the simple Moufang loop GLL($\mathbf{F}_2$), in “Nonassociative Algebra and its Applications (Säo Paulo, 1998),” Lecture Notes in Pure and Appl. Math., **211**, Dekker, New York, 2000, 313–319.

[17] E. Moorhouse, personal communication, Aug. 2004.

[18] R. Moufang, Zur Struktur von Alternativkörpern, Math. Ann., **110** (1935), 416–430.

[19] L.J. Paige, A class of simple Moufang loops, Proc. Amer. Math. Soc., **7** (1956), 471–482.

[20] H.O. Pflugfelder, “Quasigroups and Loops: Introduction,” Sigma Series in Pure Mathematics, **7**, Heldermann Verlag, Berlin, 1990.

[21] D.E. Taylor, "The Geometry of the Classical Groups," Sigma Series in Pure Mathematics, **9**, Heldermann Verlag, Berlin, 1992.

[22] J. Tits, Sur la trialité et les algèbres d'octaves, Acad. Roy. Belg. Bull. Cl. Sci., **44** (1958), 332–350.

[23] G. Thomsen, Topologische Fragen der Differentialgeometrie XII, Schnittpunktssätze in ebenen Geweben, Abh. Math. Semin. Univ. Hambg., **7** (1929), 99–106.

[24] P. Vojtěchovský, Finite simple Moufang loops, Ph.D. Thesis, Iowa State University, 2001.