This is to certify that the
dissertation entitled

Subloops of the unit octonions

presented by

Stephen M. Gagola III

has been accepted towards fulfillment
of the requirements for the

Ph.D. degree in Mathematics

Jonathan D. Hall
Major Professor's Signature

June 21, 2005
Date

SUBLOOPS OF THE UNIT OCTONIONS

By

Stephen M. Gagola III

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

2005

Abstract

Subloops of the unit octonions

By

Stephen M. Gagola III

The class of Moufang loops is defined by the identities $x(y(xz)) = ((xy)x)z$, $z(x(yx)) = ((zx)y)x$, and $(xy)(zx) = (x(yz))x$; Non-associative finite simple Moufang loops form the central topic of this work. The emphasis will be on their connections with composition algebras. A composition algebra over some field, not necessarily finite, is either $F1$ with $charF = 2$ or an algebra with a non-degenerate quadratic form, q, that admits composition. If its dimension over the field is eight then we have what we call an octonion algebra. Here we categorize all the subloops of the unit octonions and in particular describe all the finite maximal subloops by using the reflection groups of these Moufang loops. Furthermore, Lagrange's Theorem for Moufang loops then follows as a corollary.

Contents

Tables

1 Introduction and Main Results

In this section, we explain the necessary material and introduce the needed notation. After presenting the basic notions, let us briefly summarize the results of this work.

Let F be an arbitrary field and A a vector space over F. A is said to be an *algebra* over F if there is a bilinear multiplication on A satisfying :

1. $x(y+z) = xy + xz$

2. $(x+y)z = xz + yz$

3. $(ax)y = a(xy) = x(ay)$

for all $x, y, z \in A$ and $a \in F$. Notice that an algebra is not necessarily associative, meaning $x(yz) = (xy)z$ for all $x, y, z \in A$. Also, an algebra is not always assumed to contain an identity element. A *subalgebra* of A is a subspace, B, of A that forms an algebra with respect to this multiplication. We will denote this by $B \leq A$. A *bilinear form* on A is a map $(\cdot|\cdot) : A \times A \longrightarrow F$ such that

1. $(x+y|z) = (x|z) + (y|z)$,

2. $(z|x+y) = (z|x) + (z|y)$, and

3. $(ax|y) = a(x|y) = (x|ay)$,

for any $x, y, z \in A$ and $a \in F$. If $B \leq A$ then $B^{\perp} = \{x \in A | (x|y) = 0 \text{ for all } y \in B\}$. A map $q : A \longrightarrow F$ is a *quadratic form* on A if

1. $q(ax) = a^2q(x)$ for all $x \in A$ and $a \in F$

2. and the map from $A \times A$ to F given by $(x|y) = q(x+y) - q(x) - q(y)$ is a (symmetric) bilinear form.

We say that the quadratic form q is non-degenerate if $\{x \in A|(x|y) = 0$ for all $y \in A\} = 0$.

An algebra A over a field F is a *composition algebra* if it has a multiplicative norm, that is, a quadratic form, $q : A \longrightarrow F$, with $q(ab) = q(a)q(b)$ for all $a, b \in A$, is nonzero for $F1$, and in general is non-degenerate. A composition algebra does not have to contain an identity element but is closely related to one that does contain an identity. Such a connection is an *isotopy* and every composition algebra is isotopic to an algebra with an identity, see Jacobson [13, p. 418]. The following theorem, dealing with the dimension of composition algebras, was proven by Hurwitz [12]. A proof is given in section three below.

Theorem 1.1. *Suppose A is a composition algebra over a field F. Then it is of dimension one, two, four, or eight.*

A composition algebra of dimension four is usually called a *quaternion algebra,* and such an algebra of dimension eight is usually called an *octonian algebra.* A quaternion algebra is associative. However, unlike the quaternions, the octonions are nonassociative but do satisfy the *Moufang identity*, $z(x(yx)) = ((zx)y)x$ (see proposition 3.9). One can show that such an identity, $z(x(yx)) = ((zx)y)x$, is actually equivalent to:

1. $x(y(xz)) = ((xy)x)z$

and

2. $(xy)(zx) = (x(yz))x$ (see Lemma 3.1 of [4]).

We call a composition algebra a *division algebra* if it contains no zero-divisors. Otherwise it is said to be *split.*

A *quasigroup* is a non-empty set S with a closed binary operation, $(x, y) \mapsto x \cdot y$, such that

1. $a \cdot x = b$ determines a unique element $x \in S$ given $a, b \in S$ and

2. $b = y \cdot a$ determines a unique element $y \in S$ given $a, b \in S$.

A *loop* is a quasigroup, L, with an identity element and a *subloop* of L is a subset of L which, under the binary operation, is a loop. A finite loop L is said to have the *Lagrange property* if for any subloop K of L the order of K, $|K|$, divides the order of L, $|L|$. Lagrange's Theorem says that finite groups have the Lagrange property, but in general, a finite loop does not satisfy the Lagrange property. For instance, one can easily construct a loop of five elements all of which are of order one or two as one can see in Table 1.

	1	a	b	c	d
1	1	a	b	c	d
a	a	1	d	b	c
b	b	c	1	d	a
c	c	d	a	1	b
d	d	b	c	a	1

Table 1: A multiplication table for a loop of order five

The reason for this is because without associativity, the coset decomposition breaks down.

Definition 1.2. *A Moufang loop is a loop, L, that satisfies the Moufang identities.*

The main results of this thesis are the following four theorems. The first is a version of the Aschbacher-O'Nan-Scott Theorem [2] and is valid for subloops of octonion algebras.

Theorem 1.3. *Let L be a subloop of an octonion algebra, C, over the field F. Consider the reflection subgroup $R = R(L) = \langle \rho_x \mid x \in L \rangle$ where $V = F^8$. Then there are three possibilities:*

1. *$V > [V, R]$ with one of the following*
   (a) *$L \leq S^{\perp}$ for some hexagon line S;*
   (b) *$L \leq Q$ for some nonsplit quaternion subalgebra Q;*
   (c) *$L \leq [V, R]$, where L is totally isotropic and F is a nonperfect field of characteristic two;*
2. *$V = [V, R]$ is reducible and there is a quaternion subalgebra Q with $L \leq Q \cup Q^{\perp}$;*
3. *R is irreducible on V.*

Here, $[V, R] = span(\{-v + v^r \mid r \in R, v \in V\})$. By a reflection, ρ_x, of V we are referring to the map $\rho_x : V \longrightarrow V$ sending v to $v - \frac{(x|v)}{q(x)}x$. We will let $O(V, q)$ be the orthogonal group with respect to q consisting of all the linear transformations that

preserve q. Note that we always have $\rho_x \in O(V,q)$ (see [25]). By irreducible, we mean that there does not exist a proper subspace of V that is left invariant under R. Also, for a hexagon line we mean a totally singular 2-space that is contained in $1^\perp$ such that the multiplication is zero.

In the split case, the subalgebras $S^\perp$ and Q are uniquely determined up to the action of $Aut(C)$. See Proposition 5.4 and Theorem 5.6 below.

The loops that can occur under Theorem 1.3.1 and 1.3.2 are relatively elementary in structure. The loop $(S^\perp)^*$ is described in detail in Section 5 and is a loop extension of the abelian group F^2 by the group $GL_2(F)$. The loops under Theorem 1.3.2 contain subloops of index at most 2 that are contained in the quaternion subalgebra Q. Since quaternion algebras are associative, their subloops are groups.

We will only describe the finite subloops that occur in Theorem 1.3.3.

Theorem 1.4. *Let L be a finite subloop of an octonion algebra C over the field F. Let $R = \langle \rho_x \mid x \in L \rangle \leq O(C,q)$. If R is irreducible on C then R is one of the following and unique up to conjugacy in $O(C,q)$:*

1. *$R = {}^+\Omega_8^+(F_o)$ for some finite subfield F_o of F of odd characteristic. We have C split and $SLL(F_o) \leq L \leq F^* \cdot GLL(F_o)$.*

2. *$R = O_8^+(F_o)$ for some finite subfield F_o of F of characteristic 2. We have C split and $SLL(F_o) \leq L \leq F^* \cdot GLL(F_o)$.*

3. *$R = W(E_8) \cong 2O_8^+(2)$ and $2GLL(2) \leq L \leq F^* \cdot 2GLL(2)$ when $charF$ is not 2.*

Notice that the previous two results give a precise description of all finite subloops of octonian algebras. We have already discussed the structure of such subloops under 1.3.1 and 1.3.2 in general. Since a quaternion algebra always has a quadratic extension that is split, the finite subgroups that may occur are to be found on Dickson's list [24, Theorem 6.17] of finite subgroups of the matrix algebra $M_2(F)$. These two theorems can be thought of as providing an analogue of Dickson's theorem for octonian algebras.

In particular, we find all the maximal subloops of finite octonian algebras.

Theorem 1.5. *Let C be a finite octonion algebra over a field F and let L be a maximal subloop of B where $SLL(F) \leq B \leq GLL(F)$. Then L is one of the following:*

1. $L = \left(S^{\perp}\right)^{*} \cap B$ *for some hexagon line S;*
2. $L = \left(Q \cup Q^{\perp}\right)^{*} \cap B$ *for some quaternion subalgebra Q;*
3. $L = F^{*} \cdot GLL(F_o) \cap B$ *for some maximal subfield F_o of F;*
4. $L = \{x \in B | q(x) \in G\}$ *for some maximal subgroup, G, of $\{q(x) | x \in B\}$;*
5. $L = F^{*} \cdot 2GLL(2) \cap B$ *where $F = F_p$ for some odd prime p.*

As a corollary to Theorem 1.5, we get the following theorem which has been a conjecture for over forty years.

Theorem 1.6. *All finite Moufang loops have the Lagrange property.*

There have been several recent proofs of the Lagrange property for finite Moufang loops. The author of this thesis and his supervisor give a proof in [8]. There is also an independent and earlier proof by A. Grishkov and A. Zavarnitsine [9] and a third proof by E. Moorhouse [18]. All of these proofs make use of the classification of finite simple groups in two ways. First, they use a result of Liebeck [17] to reduce to the case of finite Paige loops $P(q)$. Secondly, they use Kleidman's list [16] of the maximal subgroups of the triality group $P\Omega_8^+(q) : S_3$ to treat the finite Paige loops $P(q)$. Zavarnitsine has a second paper [27] in which he classifies the maximal subloops of finite octonian algebras, as in Theorem 1.5. Again, he appeals to Kleidman's list.

The proofs of Theorems 1.5 and 1.6 given here are fundamentally different from these others. In particular, Theorem 1.5 is independent of the classification of finite simple groups and Theorem 1.6 is only dependent on Liebeck's work. Indeed, other than from using Liebeck's result once, the only place where nonelementary finite group theory is used in this thesis is in the case of characteristic 2 in Theorem 7.2. Also, as noted there, this part of the argument can probably be simplified as well.

In this thesis, as well as these other references, the crucial starting point is Doro's observation [6] that Moufang loops correspond to certain groups with triality. The treatment of groups with triality used here is that of [8] and [10].

The standard reference for general loop theory is Bruck [4] and for octonian algebras Springer and Veldkamp [22]. For group theory see [24], and for geometry see [25].

2 Notation and Terminology

For a field F consider the algebra, C, consisting of all the matrices

$$\begin{pmatrix} a & v \\ u & b \end{pmatrix}$$

where $a, b \in F$ and $v, u \in F^3$. Here, addition is defined by

$$\begin{pmatrix} a & v \\ u & b \end{pmatrix} + \begin{pmatrix} c & \alpha \\ \beta & d \end{pmatrix} = \begin{pmatrix} a+c & v+\alpha \\ u+\beta & b+d \end{pmatrix}$$

and multiplication is defined by

$$\begin{pmatrix} a & v \\ u & b \end{pmatrix}\begin{pmatrix} c & \alpha \\ \beta & d \end{pmatrix} = \begin{pmatrix} ac+v\cdot\beta & a\alpha+dv-u\times\beta \\ b\beta+cu+v\times\alpha & bd+u\cdot\alpha \end{pmatrix}$$

where $v \cdot u$ and $v \times u$ are the standard dot product and cross product. One can obtain an octonion algebra by letting $ab - v \cdot u = det \begin{pmatrix} a & v \\ u & b \end{pmatrix}$ be its norm, q. A straightforward calculation shows that q is a quadratic form and is multiplicative.

Let C be this algebra over the field F with the quadratic form, $q : x \mapsto det(x)$. We will denote the associated bilinear form as $(x|y) = q(x + y) - q(x) - q(y)$ where $x, y \in C$. For every element, v, in C we will define the *conjugate* of v as $\bar{v} = -v + (v|1)1$. Notice that an element $x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in C$ is invertible if and only if $det(x) \neq 0$ and that its inverse is $\frac{1}{det(x)} \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}$.

Clearly $det \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 0$, so C is a split octonion algebra. Indeed, as we will see in Proposition 5.4, any split octonion algebra over F is uniquely determined and

is therefore isomorphic to C. Indeed if F is finite, then there are always nonzero singular elements. So any octonion algebra over a finite field, F, is split and isomorphic to C.

By Proposition 3.9, C satisfies the Moufang identities. In particular, the set of all the invertible elements of C, $GLL(F)$, is a Moufang loop. Let $SLL(F)$ be the set of all the elements in $GLL(F)$ that are of norm one. The center of $SLL(F)$, the set of all elements that commute and associate with the other elements of $SLL(F)$, is $Z(SLL(F)) = \{\pm I\}$. Similarly, $Z(GLL(F)) = F^* \cdot I$.

Using the natural definition of homomorphisms for loops (see Bruck [4, Chapter IV]) gives rise to what we mean by "normal subloops" and "simple loops". The subloop N of L is a normal subloop if there exists a homomorphism $\varphi : L \longrightarrow L_1$ such that $N = ker(\varphi)$. If the only normal subloops of L are L and $\{1\}$ then we say that L is simple. It was proven by Paige [20] that if F is a finite field then $PSLL(F) = SLL(F)/\{\pm I\}$ is a simple Moufang loop and usually denoted by $P(F)$ or $P(q)$ where $q = |F|$.

When F is finite, since $dim_F(V)$ is even, there are (up to equivalence) two nondegenerate quadratic forms on V, distinguished by the sign, ϵ. For the corresponding orthogonal group we will write $O_8^\epsilon(F)$. Furthermore, ${}^+\Omega_8^\epsilon(F)$ will be used to denote the subgroup of index 2 in $O_8^\epsilon(F)$ that is generated by the reflections, ρ_x, with center, x, of square norm. Also, we will use ${}^-\Omega_8^\epsilon(F)$ to denote the subgroup of index 2 in $O_8^\epsilon(F)$ which is generated by the reflections, ρ_y, with center, y, of nonsquare norm. In addition, we will let $W(E_8)$ represent the Weyl group of the Lie algebra E_8.

3 General Composition Algebras

We start off with some observations about the composition algebras. Here we will let A be any composition algebra that contains an identity element, 1. By definition, all subalgebras contain the identity element. Using the definition of $\bar{v}$ one can see, from section 1.3 of F. Veldkamp and T. A. Springer [22], that:

1. $\bar{v} = -\rho_1(v)$ for all $v \in A$,

2. $\bar{v} = -v$ for all $v \in 1^{\perp}$,

3. $\bar{\bar{v}} = v$ for any element $v \in A$, and

4. $\overline{v+u} = \bar{v} + \bar{u}$ for any elements $v, u \in A$.

Lemma 3.1. *For any elements $x, v, u \in A$, the following properties hold:*

1. $(vx|ux) = (v|u)q(x)$,

2. $(1|u)(x|v) = (v|ux) + (x|uv)$, *and*

3. $(xu|v) = (u|\bar{x}v)$ *and* $(ux|v) = (u|v\bar{x})$.

Proof. By definition of the bilinear form

$$\begin{aligned}(vx|ux) &= q(vx+ux) - q(vx) - q(ux) \\ &= q((v+u)x) - q(v)q(x) - q(u)q(x) \\ &= q(v+u)q(x) - q(v)q(x) - q(u)q(x) \\ &= [q(v+u) - q(v) - q(u)]\, q(x) \\ &= (v|u)q(x).\end{aligned}$$

Since

$$\begin{aligned}(x|ux) + (x|uv) + (v|ux) + (v|uv) &= (x+v|u(x+v)) \\ &= (1|u)q(x+v) \\ &= (1|u)[(x|v) + q(x) + q(v)] \\ &= (1|u)(x|v) + (1|u)q(x) + (1|u)q(v) \\ &= (1|u)(x|v) + (x|ux) + (v|uv),\end{aligned}$$

one can subtract $(x|ux) + (v|uv)$ from both sides to obtain $(1|u)(x|v) = (v|ux) + (x|uv)$.

We can now use part two to prove part three.

$$\begin{aligned}(u|\bar{x}v) &= (u|(-x + (x|1)1)v) \\ &= (u| - xv + (x|1)v) \\ &= (u| - xv) + (u|(x|1)v) \\ &= -(u|xv) + (x|1)(u|v) \\ &= -(u|xv) + (xu|v) + (xv|u) \\ &= -(u|xv) + (xu|v) + (u|xv) \\ &= (xu|v)\end{aligned}$$

Also,

$$\begin{aligned}(u|v\bar{x}) &= (u|v(-x + (x|1)1)) \\ &= (u| - vx + (x|1)v) \\ &= (u| - vx) + (u|(x|1)v) \\ &= -(u|vx) + (u|v)(x|1) \\ &= -(u|vx) + (ux|v) + (vx|u) \\ &= -(u|vx) + (ux|v) + (u|vx) \\ &= (ux|v)\end{aligned}$$

□

Lemma 3.2. *For any* $v, u \in A$

1. $\bar{v}(vu) = q(v)u = (uv)\bar{v}$

2. $\overline{uv} = \bar{v}\bar{u}$

Proof. Since

$$\begin{aligned}(\bar{v}(vu) - q(v)u|x) &= (\bar{v}(vu)|x) - q(v)(u|x) \\ &= (vu|vx) - q(v)(u|x) \\ &= q(v)(u|x) - q(v)(u|x) \\ &= 0\end{aligned}$$

for all $x \in A$. by non-degeneracy, $\bar{v}(vu) = q(v)u$.

Also, since

$$\begin{aligned}((uv)\bar{v} - q(v)u|x) &= ((uv)\bar{v}|x) - q(v)(u|x) \\ &= (uv|xv) - q(v)(u|x) \\ &= q(v)(u|x) - q(v)(u|x) \\ &= 0\end{aligned}$$

for all $x \in A$, by non-degeneracy, $q(v)u = (uv)\bar{v}$.

Likewise, since

$$\begin{aligned}(\overline{uv} - \bar{v}\bar{u}|x) &= (\overline{uv}|x) - (\bar{v}\bar{u}|x) \\ &= (1|(uv)x) - (\bar{u}|vx) \\ &= (\bar{x}|uv) - (\bar{u}\bar{x}|v) \\ &= (\bar{x}|uv) - (\bar{x}|uv) \\ &= 0\end{aligned}$$

for all $x \in A$, by non-degeneracy, $\overline{uv} = \bar{v}\bar{u}$. □

Lemma 3.3. *For all* $x, v, u \in A$

1. $v(\bar{u}x) + u(\bar{v}x) = (v|u)x$

2. $(xv)\bar{u} + (xu)\bar{v} = (v|u)x$

Proof. By Lemma 3.2 $(u+v)((\overline{u+v})x) = q(u+v)x$. Therefore,

$$\begin{aligned}
0 &= (u+v)((\overline{u+v})x) - q(u+v)x \\
&= (u+v)((\bar{u}+\bar{v})x) - q(u+v)x \\
&= u(\bar{u}x) + v(\bar{v}x) + v(\bar{u}x) + u(\bar{v}x) - q(u+v)x \\
&= q(u)x + q(v)x + v(\bar{u}x) + u(\bar{v}x) - q(u+v)x \\
&= v(\bar{u}x) + u(\bar{v}x) - (v|u)x.
\end{aligned}$$

Hence, $v(\bar{u}x) + u(\bar{v}x) = (v|u)x$.

Likewise,

$$\begin{aligned}
0 &= (x(u+v))\overline{u+v} - q(u+v)x \\
&= (x(u+v))(\bar{u}+\bar{v}) - q(u+v)x \\
&= (xu)\bar{u} + (xv)\bar{v} + (xv)\bar{u} + (xu)\bar{v} - q(u+v)x \\
&= q(u)x + q(v)x + (xv)\bar{u} + (xu)\bar{v} - q(u+v)x \\
&= (xv)\bar{u} + (xu)\bar{v} - (v|u)x.
\end{aligned}$$

Thus, $(xv)\bar{u} + (xu)\bar{v} = (v|u)x$. □

Lemma 3.4. *For all* $v, u \in A$, $v(uv) = (vu)v$

Proof. For any $v, u \in A$,

$$\begin{aligned} v(uv) &= v(uv) + \bar{u}(\bar{v}v) - q(v)\bar{u} \\ &= (v|\bar{u})v - q(v)\bar{u} \\ &= (u|\bar{v})v - q(v)\bar{u} \\ &= (vu)v + (v\bar{v})\bar{u} - q(v)\bar{u} \\ &= (vu)v. \end{aligned}$$

□

Remark 3.5. *Notice that, by* 3.3, $x\bar{y} + y\bar{x} = (x|y)1$ *for any* $x, y \in A$. *So we obtain that* $(x\bar{y})x + q(x)y = (x|y)x$. *So by Lemma* 3.4, $x\bar{y}x + q(x)y = (x|y)x$. *Therefore, if* $q(x) \neq 0$ *then* $\rho_x(y) = y - \frac{(x|y)}{q(x)}x = \frac{-1}{q(x)}x\bar{y}x$.

Lemma 3.6. *Let* $a \in A$ *with* $q(a) = 0$ *and* $a \neq 0$, *then* $x \in aA$ *if and only if* $\bar{a}x = 0$.

Proof. If $x \in aA$ then $\bar{a}x \in \bar{a}(aA) = q(a)A = \{0\}$.

Now suppose $\bar{a}x = 0$. Let $y \in A$ such that $(a|y) = 1$. By Lemma 3.3, $a(\bar{y}x) + y(\bar{a}x) = (a|y)x$. Hence, $x = a(\bar{y}x) \in aA$. □

Theorem 3.7. *Let* $a, b \in A$ *with* $q(a) = 0 = q(b)$, $a \neq 0$, *and* $b \neq 0$. *Then* aA *and* bA *coincide if and only if* a *and* b *are linearly dependent; their intersection is a line, a subspace of dimension two, if and only if* $(a|b) = 0$ *with* a *and* b *linearly independent; their intersection is* 0 *if and only if* $(a|b) \neq 0$.

Proof. This is Theorem 4 of van der Blij and Springer [3]. □

Corollary 3.8. *There does not exist a singular plane, a totally singular subspace of dimension three, B, in $1^{\perp}$ such that $xy = 0$ for all $x, y \in B$.*

Proof. If $xy = 0$ for all $x, y \in B$ then $\bar{x}y = 0$ for all $x, y \in B$. Thus, by Lemma 3.6, $y \in xA$ for all $x, y \in B$. Therefore $B \subseteq xA$ for all $x \in B$. From Theorem 3.7 we have that $dim_F(yA \cap xA) \leq 2$ for any linearly independent elements $x, y \in B$. Therefore, $dim_F(B) \leq 2$. □

Proposition 3.9. *If A is a composition algebra then all of the Moufang identities are satisfied.*

Proof. Claim: $x(xy) = x^2y$ and $(yx)x = yx^2$ for all $x, y \in A$.

$$\begin{aligned} x(xy) - x^2y &= (x + \bar{x} - \bar{x})(xy) - ((x + \bar{x} - \bar{x})x)y \\ &= (x + \bar{x})(xy) - \bar{x}(xy) - ((x + \bar{x})x)y + (\bar{x}x)y \\ &= (\bar{x}x)y - \bar{x}(xy) && \text{since } x + \bar{x} = (x|1)1 \\ &= q(x)y - q(x)y && \text{by Lemma 3.2} \\ &= 0 \end{aligned}$$

for all $x, y \in A$. Likewise, $(yx)x = yx^2$ for all $x, y \in A$.

Let $f_1(x_1, x_2, x_3) = (x_1x_2)x_3 - x_1(x_2x_3)$. Since

$$\begin{aligned}(x_1x_2)x_3 - x_1(x_2x_3) &= (x_1x_2)x_3 - x_1(x_2x_3) + \\ &\quad + (x_1 + x_2)[(x_1 + x_2)x_3] - (x_1 + x_2)^2x_3 \\ &= (x_1x_2)x_3 - x_1(x_2x_3) + \\ &\quad + x_1(x_2x_3) + x_2(x_1x_3) - (x_1x_2)x_3 - (x_2x_1)x_3 \\ &= x_2(x_1x_3) - (x_2x_1)x_3 \\ &= -f_1(x_2, x_1, x_3)\end{aligned}$$

and

$$\begin{aligned}(x_1x_2)x_3 - x_1(x_2x_3) &= (x_1x_2)x_3 - x_1(x_2x_3) + \\ &\quad + x_1(x_2 + x_3)^2 - [x_1(x_2 + x_3)](x_2 + x_3) \\ &= (x_1x_2)x_3 - x_1(x_2x_3) + \\ &\quad + x_1(x_2x_3) + x_1(x_3x_2) - (x_1x_2)x_3 - (x_1x_3)x_2 \\ &= x_1(x_3x_2) - (x_1x_3)x_2 \\ &= -f_1(x_1, x_3, x_2)\end{aligned}$$

$f_1(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = sgn(\sigma)f_1(x_1, x_2, x_3)$.

Let $f_2 : A \times A \times A \times A \longrightarrow A$ be the Kleinfeld function [15],

$$\begin{aligned} f_2(x_1,x_2,x_3,x_4) = \quad & ((x_1x_2)x_3)x_4 - (x_1x_2)(x_3x_4) + \\ & - ((x_2x_3)x_4)x_1 + (x_2x_3)(x_4x_1) + \\ & + ((x_3x_4)x_1)x_2 - (x_3x_4)(x_1x_2) + \\ & - ((x_4x_1)x_2)x_3 + (x_4x_1)(x_2x_3). \end{aligned}$$

Notice that $f_2(x_1,x_2,x_3,x_4) = -f_2(x_2,x_3,x_4,x_1)$. Also,

$$\begin{aligned} f_2(x_1,x_2,x_3,x_4) = \quad & ((x_1x_2)x_3)x_4 - (x_1x_2)(x_3x_4) + \\ & - ((x_2x_3)x_4)x_1 + (x_2x_3)(x_4x_1) + \\ & + f_1(x_3x_4,x_1,x_2) \\ & - f_1(x_4x_1,x_2,x_3) \\ = \quad & ((x_1x_2)x_3)x_4 - (x_1x_2)(x_3x_4) + \\ & - ((x_2x_3)x_4)x_1 + (x_2x_3)(x_4x_1) + \\ & + f_1(x_2,x_3x_4,x_1) \\ & - f_1(x_2,x_3,x_4x_1) \\ = \quad & ((x_1x_2)x_3)x_4 - (x_1x_2)(x_3x_4) + \\ & - ((x_2x_3)x_4)x_1 + (x_2x_3)(x_4x_1) + \\ & + (x_2(x_3x_4))x_1 - x_2((x_3x_4)x_1) \\ & - (x_2x_3)(x_4x_1) + x_2(x_3(x_4x_1)) \\ = \quad & f_1(x_1x_2,x_3,x_4) - f_1(x_2,x_3,x_4)x_1 - x_2f_1(x_3,x_4,x_1). \end{aligned}$$

So $f_2(x_1, x_2, x_3, x_3) = 0$ for all $x_i \in A$. Thus

$$\begin{aligned} 0 &= f_2(x_1, x_2, x_3 + x_4, x_3 + x_4) \\ &= f_2(x_1, x_2, x_3, x_4) + f_2(x_1, x_2, x_4, x_3) + \\ &\quad + f_2(x_1, x_2, x_3, x_3) + f_2(x_1, x_2, x_4, x_4) \\ &= f_2(x_1, x_2, x_3, x_4) + f_2(x_1, x_2, x_4, x_3) \end{aligned}$$

meaning, $f_2(x_1, x_2, x_4, x_3) = -f_2(x_1, x_2, x_3, x_4)$. Therefore, since $f_2(x_1, x_2, x_3, x_4) = -f_2(x_2, x_3, x_4, x_1)$ and $f_2(x_1, x_2, x_4, x_3) = -f_2(x_1, x_2, x_3, x_4)$, $f_2(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}) = sgn(\sigma) f_2(x_1, x_2, x_3, x_4)$. So

$$\begin{aligned} 0 &= f_2(x_1, x_2, x_1, x_3) \\ &= f_1(x_1 x_2, x_1, x_3) - f_1(x_2, x_1, x_3) x_1 - x_2 f_1(x_1, x_3, x_1) \\ &= f_1(x_1 x_2, x_1, x_3) - f_1(x_2, x_1, x_3) x_1 - x_2 f_1(x_3, x_1, x_1) \\ &= f_1(x_1 x_2, x_1, x_3) - f_1(x_2, x_1, x_3) x_1 \end{aligned}$$

which implies that $f_1(x_1 x_2, x_1, x_3) = f_1(x_2, x_1, x_3) x_1$.

From this we conclude that for any $x, y, z \in A$,

$$\begin{aligned} x(y(xz)) - ((xy)x)z &= x(y(xz)) - (xy)(xz) + (xy)(xz) - ((xy)x)z \\ &= -f_1(x, y, xz) - f_1(xy, x, z) \\ &= -f_1(xz, x, y) - f_1(xy, x, z) \\ &= -f_1(z, x, y)x - f_1(y, x, z)x \\ &= -f_1(z, x, y)x + f_1(z, x, y)x \\ &= 0 \end{aligned}$$

meaning, $x(y(xz)) = ((xy)x)z$ for any $x, y, z \in A$. Hence, A satisfies all the Moufang identities.

Another proof can be found in [22] (see Proposition 1.4.1, page 9). □

Proposition 3.10. *If B is a subalgebra of a composition algebra, A, and v is contained in $B^{\perp}$ then $B + Bv$ is also a subalgebra with $Bv \leq B^{\perp}$. Moreover, if $a = s + tv$ and $b = x + yv$ then $ab = (sx - q(v)\bar{y}t) + (t\bar{x} + ys)v$ for $s, t, x, y \in B$.*

Proof. Since B is a subspace containing the identity, $B + Bv$ is a subspace that

contains 1. For any $a = s + tv, b = x + yv \in B + Bv$ we get that

$$\begin{aligned}
ab =& (s+tv)(x+yv) \\
=& \; sx + (tv)x + s(yv) + (tv)(yv) \\
=& \; sx + [(v|\bar{x})t - (t\bar{x})\bar{v}] - s(\overline{yv}) + (-\overline{tv})(yv) \text{ by Lemma 3.3} \\
=& \; sx + [0 + (t\bar{x})v] - s(\bar{v}\bar{y}) + (-\bar{v}\bar{t})(yv) \qquad \text{by Lemma 3.2} \\
=& \; sx + (t\bar{x})v + s(v\bar{y}) + (v\bar{t})(yv) \\
=& \; sx + (t\bar{x})v + [(\bar{v}|s)\bar{y} - \bar{v}(\bar{s}\bar{y})] + v(\bar{t}y)v \qquad \text{by Lemma 3.3 and Moufang's identity} \\
=& \; sx + (t\bar{x})v + [0 + \overline{\bar{v}(\bar{s}\bar{y})}] + (-\overline{v(\bar{t}y)})v \\
=& \; sx + (t\bar{x})v + (ys)v + (-(\bar{y}t)\bar{v})v \qquad \text{by Lemma 3.2} \\
=& \; sx + (t\bar{x})v + (ys)v - q(v)\bar{y}t \qquad \text{by Lemma 3.2} \\
=& (sx - q(v)\bar{y}t) + (t\bar{x} + ys)v \quad \in B + Bv.
\end{aligned}$$

Therefore, $B + Bv$ is also a subalgebra and since $(b_1|b_2v) = (\bar{b_2}b_1|v) = 0$ for all $b_i \in B$, $Bv \leq B^{\perp}$. □

Theorem 3.11. (Dickson's Theorem) *If B is a non-degenerate subalgebra of a composition algebra, A, with $dim_F(B) = n$ and v is contained in $B^{\perp}$ with $q(v) \neq 0$ then $B + Bv$ is a non-degenerate subalgebra with $dim_F(B + Bv) = 2n$. Furthermore, if $a = s + tv$ and $b = x + yv$ then $ab = (sx - q(v)\bar{y}t) + (t\bar{x} + ys)v$ for $s, t, x, y \in B$.*

Proof. By Proposition 3.10, $B + Bv$ is a subalgebra of A. Since $q(v) \neq 0$, v is invertible with $v^{-1} = \frac{\bar{v}}{q(v)}$. Thus $dim_F(Bv) = dim_F B = n$. Suppose there exists an element $b_1 \in B$ such that $b_1v \in B$. Then, since B is nondegenerate, there exists

an element $b_2 \in B$ such that $(b_2|b_1 v) \neq 0$. Thus $(\bar{b_1} b_2|v) \neq 0$. But $\bar{b_1} b_2 \in B$ and $v \in B^{\perp}$. Hence, by contradiction, $B \cap Bv = 0$. Therefore, $B + Bv$ is a subalgebra of dimension $2n$. Let $s + tv$ be some fixed element in $B + Bv$ where $t \neq 0$. Since B is non-degenerate, there exists an element $y \in B$ such that $(y|t) \neq 0$. So

$$\begin{aligned}
(yv|s + tv) &= q(s + yv + tv) - q(yv) - q(s + tv) \\
&= (s|yv + tv) + q(s) + q(yv + tv) - q(yv) - (s|tv) - q(s) - q(tv) \\
&= 0 + q(s) + (yv|tv) + q(yv) + q(tv) - q(yv) - 0 - q(s) - q(tv) \\
&= (yv|tv) \\
&= (y|t)q(v) \quad \text{by Lemma 3.1} \\
&\neq 0.
\end{aligned}$$

Therefore $B + Bv$ is a non-degenerate subalgebra of dimension $2n$. □

Theorem 3.12. *If $B = F1$ is a proper subalgebra of a composition algebra, A, over the field F of characteristic two and v is contained in $A \setminus B$ with $(v|1) \neq 0$ then $B + Bv$ is a non-degenerate subalgebra with $dim_F(B + Bv) = 2$. Furthermore, if $a = s + tv$ and $b = x + yv$ then $ab = (sx - q(v)ty) + (sy + (v|1)ty)v$ for $s, t, x, y \in B$.*

Proof. First of all notice that such an element, v, exists since A is non-degenerate and

$$\begin{aligned}
(\alpha 1|\beta 1) &= q((\alpha + \beta)1) - q(\alpha 1) - q(\beta 1) \\
&= \alpha^2 + 2\alpha\beta + \beta^2 - \alpha^2 - \beta^2 \\
&= 0
\end{aligned}$$

for all $\alpha 1, \beta 1 \in F1$. Since B is a subspace containing the identity, $B + Bv$ is a subspace that contains 1. Since $v \in A$ which is non-degenerate,

$$\begin{aligned} v^2 &= v^2 + (v|1)v - (v|1)v \\ &= -v^2 + (v|1)v - (v|1)v \\ &= v(-v + (v|1)1) - (v|1)v \\ &= v\bar{v} + (v|1)v \\ &= q(v)1 + (v|1)v \end{aligned}$$

For any $a = s + tv, b = x + yv \in B + Bv$ we get that

$$\begin{aligned} ab =& (s+tv)(x + yv) \\ =& \ sx + (tv)x + s(yv) + (tv)(yv) \\ =& \ sx + (tx)v + (sy)v + (ty)v^2 \quad \text{since } s,t,x,y \in F1 \\ =& \ sx + (tx)v + (sy)v + (ty)(q(v)1 + (v|1)v) \\ =& (sx + q(v)ty) + (tx + sy + (v|1)ty)v \quad \in B + Bv. \end{aligned}$$

Therefore, $B + Bv$ is a subalgebra of dimension 2. Let $\alpha 1 + \beta v$ be some element in $B + Bv$ with $\alpha, \beta \in F$. If $\beta \neq 0$ then

$$\begin{aligned} (\alpha 1 + \beta v|1) &= (\alpha 1|1) + (\beta v|1) \\ &= \beta(v|1) \\ &\neq 0. \end{aligned}$$

If $\beta = 0$ and $\alpha \neq 0$ then

$$\begin{aligned}(\alpha 1 + \beta v|v) &= (\alpha 1|v) \\ &= \alpha(1|v) \\ &\neq 0.\end{aligned}$$

Hence $B + Bv$ is a non-degenerate subalgebra of dimension 2. □

Lemma 3.13. *If A is a composition algebra of dimension 8 then A is nonassociative.*

Proof. Suppose A is of odd characteristic. One can generate A using Dickson's Theorem 3.11 and letting $v_1, v_2, v_3 \in A$ with $q(v_i) \neq 0$ for all i, such that $v_1 \in 1^{\perp}$, $v_2 \in \langle 1, v_1 \rangle^{\perp}$, and $v_3 \in \langle 1, v_1, v_2 \rangle^{\perp}$. Then

$$\begin{aligned}v_1(v_2v_3) &= -v_1(\bar{v_3}\bar{v_2}) \\ &= -v_1(v_3v_2) \\ &= \bar{v_3}(\bar{v_1}v_2) \\ &= v_3(v_1v_2) \\ &= -(\overline{v_1v_2})\bar{v_3} \\ &= -(v_1v_2)v_3 \\ &\neq (v_1v_2)v_3.\end{aligned}$$

Therefore, if A is of odd characteristic then A is nonassociative.

Now suppose that A of of characteristic 2. One can generate A using Theorems 3.11 and 3.12 and letting $v_1, v_2, v_3 \in A$ such that $(v_1|1) \neq 0$, $v_2 \in \langle 1, v_1 \rangle^{\perp}$, and

$v_3 \in \langle 1, v_1, v_2 \rangle^{\perp}$. Then

$$\begin{aligned} v_1(v_2v_3) &= v_1(\bar{v_3}\bar{v_2}) \\ &= v_1(v_3v_2) \\ &= \bar{v_3}(\bar{v_1}v_2) \\ &= v_3\left((v_1 + (v_1|1)1)v_2\right) \\ &= v_3(v_1v_2) + (v_1|1)v_3v_2 \\ &= (\overline{v_1v_2})\bar{v_3} + (v_1|1)v_3v_2 \\ &= (v_1v_2)v_3 + (v_1|1)v_3v_2 \\ &\neq (v_1v_2)v_3. \end{aligned}$$

Hence, if A is of characteristic 2 then A is nonassociative. □

Theorems 3.11 and 3.12 along with Lemma 3.13 can be used to prove Hurwitz's Theorem 1.1.

Proof. Assume there exists a composition algebra of dimension higher than eight, namely A, that contains $B_1 = F1$. By Theorem 3.11 or 3.12, there exists a non-degenerate subalgebra of A, B_2, that is of dimension 2. If B_{2^n} is a non-degenerate composition algebra of dimension 2^n that is properly contained in A then by Theorem 3.11, there exists a non-degenerate subalgebra of A, $B_{2^{n+1}}$, that is of dimension 2^{n+1}, $B_{2^{n+1}}$. Since A is of dimension higher than eight, by induction on n, A contains a non-degenerate subalgebra of dimension sixteen, $B + Bv$, where B is of dimension eight. By Proposition 3.9, $B + Bv$ satisfies the Moufang identities. Thus, for every

$x + yv, s + tv \in B + Bv$ we get that

$$\begin{aligned}
0 &= (x + yv)\left((x + yv)(s + tv)\right) - (x + yv)^2(s + tv) \\
&= \left[x(xs) - x^2 s - q(v)s(\bar{y}y) + q(v)(s\bar{y})y - q(v)\bar{x}(\bar{t}y) + q(v)(\bar{x}\bar{t})y\right] \\
&\quad + \left[tx^2 - (tx)x + y(\bar{s}\bar{x}) - (y\bar{s})\bar{x} + q(v)y(\bar{y}t) - q(v)(y\bar{y})t\right] v \\
&= \left[0 - q(v)(0) - q(v)\left[\bar{x}(\bar{t}y) - q(v)(\bar{x}\bar{t})y\right]\right] \\
&\quad + \left[0 + y(\bar{s}\bar{x}) - (y\bar{s})\bar{x} + q(v)(0)\right] v.
\end{aligned}$$

Therefore, $y(\bar{s}\bar{x}) = (y\bar{s})\bar{x}$ for all $y, \bar{s}, \bar{x} \in B$. Hence, the octonion algebra B is associative. But, by Lemma 3.13, the octonion algebra B is nonassociative. So by contradiction, there does not exist a composition algebra of dimension higher than eight. □

4 Moufang Loops

The following are some well known properties of Moufang loops that will be used later in this paper. See Bruck [4, Chapter VII] for unexplained material.

Lemma 4.1. *For a Moufang loop, L, every element $x \in L$ has a unique two sided inverse, x^{-1}.*

Lemma 4.2. *If $x, y \in L$ where L is a Moufang loop then:*

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

4. $y = (yx^{-1})x$,

and

5. $x(yx) = (xy)x$.

Lemma 4.3. *Let $x, y \in L$ for some Moufang loop, L.*

1. *If $k \geq 0$ then $x^k y = x(x(...x(xy)...))$ with k copies of x.*

2. *If $k < 0$ then $x^k y = (x^{-1}(x^{-1}(...x^{-1}(x^{-1}y)...))$ with $-k$ copies of x^{-1}.*

3. *If $k \geq 0$ then $yx^k = ((...(xy)x...)x)x$ with k copies of x.*

4. *If $k < 0$ then $yx^k = ((...(yx^{-1})...)x^{-1})x^{-1}$ with $-k$ copies of x^{-1}.*

Proof. Part one is easy to see for $k = 0$ or 1. Suppose it is true for all $0 \leq k \leq n$. Then

$$\begin{aligned} x^{n+1}y &= (x \cdot x \cdots x)y && \text{with } (n+1) \text{ copies of } x \\ &= ((x(x \cdots x))x)y \\ &= x((x \cdots x)(xy)) && \text{by the Moufang identity} \\ &= x(x(\cdots x(xy) \cdots)) \end{aligned}$$

Thus, $x^{n+1}y = x(x(\cdots x(xy)\cdots))$ with $n+1$ copies of x. So, by induction, for all $k \geq 0$, $x^k y = x(x(\cdots x(xy)\cdots))$ with k copies of x. Similarly, if $k \geq 0$ then $yx^k = ((\cdots(xy)x\cdots)x)x$ with k copies of x.

Part two is easy to see for $k = -1$. Now suppose that it is true for all $n \leq k \leq -1$. Then

$$\begin{aligned} x^{n-1}y &= (x^{-1} \cdot x^{-1} \cdots x^{-1})y && \text{with } (1-n) \text{ copies of } x \\ &= ((x^{-1}(x^{-1} \cdots x^{-1}))x^{-1})y \\ &= x^{-1}((x^{-1} \cdots x^{-1})(x^{-1}y)) && \text{by the Moufang identity} \\ &= x^{-1}(x^{-1}(\cdots x^{-1}(x^{-1}y) \cdots)) \end{aligned}$$

Thus, $x^{n-1}y = x^{-1}(x^{-1}(\cdots x^{-1}(x^{-1}y) \cdots))$ with $1-n$ copies of x^{-1}. So, by deduction, for all $k < 0$, $x^k y = (x^{-1}(x^{-1}(\cdots x^{-1}(x^{-1}y) \cdots))$ with $-k$ copies of x^{-1}. Similarly, if $k < 0$ then $yx^k = ((\cdots(yx^{-1}) \cdots)x^{-1})x^{-1}$ with $-k$ copies of x^{-1}. □

Lemma 4.4. *If x and y are contained in some Moufang loop, L, then $x^n(x^m y) = x^{n+m}y$ and $(yx^n)x^m = yx^{n+m}$.*

Proof. This follows from Lemmas 4.3 and 4.2. □

From this one can show that any Moufang loop is *diassociative.* That is, any two elements of a Moufang loop generate a group. This was proven by R. Moufang [19] herself back in 1935. However, there are many diassociative loops that are not Moufang loops. Furthermore, as seen in Table 2, there exist diassociative loops that do not satisfy the Lagrange property. In this example we have the Steiner loop of order ten where any two elements generate a group of order four, namely $Z_2 \times Z_2$.

	1	a	bc	a(bc)	b	ca	b(ca)	c	ab	c(ab)
1	1	a	bc	a(bc)	b	ca	b(ca)	c	ab	c(ab)
a	a	1	a(bc)	bc	ab	c	c(ab)	ca	b	b(ca)
bc	bc	a(bc)	1	a	c	c(ab)	ab	b	b(ca)	ca
a(bc)	a(bc)	bc	a	1	c(ab)	ab	c	b(ca)	ca	b
b	b	ab	c	c(ab)	1	b(ca)	ca	bc	a	a(bc)
ca	ca	c	c(ab)	ab	b(ca)	1	b	a	a(bc)	bc
b(ca)	b(ca)	c(ab)	ab	c	ca	b	1	a(bc)	bc	a
c	c	ca	b	b(ca)	bc	a	a(bc)	1	c(ab)	ab
ab	ab	b	b(ca)	ca	a	a(bc)	bc	c(ab)	1	c
c(ab)	c(ab)	b(ca)	ca	b	a(bc)	bc	a	ab	c	1

Table 2: The Steiner loop of order ten

A *Latin square design* is a pair (P, A) of points, P, and lines, A, such that:

1. P is a disjoint union of three parts R, C, and E;

2. each line $l \in A$ contains three points and meets each part R, C, and E exactly once;

3. any pair of points that are contained in different parts belongs to exactly one line.

For a loop, L, there is a Latin square design of L, D_L, that has a point set $P = L_R \cup L_C \cup L_E$, where $L_i = \{a_i | a \in L\}$ is a copy of L, and a line set $A = \{\{a_R, b_C, c_E\} = [a, b, c] \mid (ab)c = 1 \in L\}$.

The automorphism group, $Aut(D_L)$, of the Latin square design D_L is the set of all bijections $f : P \longrightarrow P$ that take lines to lines. So $[a, b, c] \in A$ if and only if $\{f(a), f(b), f(c)\} \in A$. For $a \in R$, let τ_a be the map that exchanges the sets C and E such that $\tau_a(b) = c$ and $\tau_a(c) = b$ if and only if $[a, b, c] \in A$.

Suppose there exist elements $f, g \in Aut(D_L)$ such that $f|_{C \cup E} = \tau_a = g|_{C \cup E}$. Then fg^{-1} is trivial on $C \cup E$ and therefore is trivial on P. Thus, $f = g$. Therefore, τ_a has at most one extension, and if it exists then it has order two. So we will just call this extension τ_a. If L is a Moufang loop then such an extension exists, namely:

$$\tau_a : \begin{cases} x_R \mapsto a x^{-1} a_R \\ y_C \mapsto y^{-1} a_E^{-1} \\ z_E \mapsto a^{-1} z_C^{-1} \end{cases}.$$

This is because if $(xy)z = 1$ then:

$$\begin{aligned} & xy = z^{-1} \\ \Longrightarrow\ & 1 = (x^{-1}z^{-1})y^{-1} \\ \Longrightarrow\ & a\left[(x^{-1}z^{-1})y^{-1}\right]a^{-1} = 1 \\ \Longrightarrow\ & \left[a(x^{-1}z^{-1})\right]\left[y^{-1}a^{-1}\right] = 1 \\ \Longrightarrow\ & \left[a\left(x^{-1}\left(a(a^{-1}z^{-1})\right)\right)\right]\left[y^{-1}a^{-1}\right] = 1 \\ \Longrightarrow\ & \left[(ax^{-1}a)(a^{-1}z^{-1})\right]\left[y^{-1}a^{-1}\right] = 1. \end{aligned}$$

We will call such an extension a *central automorphism* of D_L with center a. The same holds for central automorphisms τ_y and τ_z with the centers $y \in C$ and $z \in E$. (See [10] and [8] for discussion.)

For a Moufang loop, L, we call $G_L = \langle \tau_x | x \in L_R \cup L_C \cup L_E \rangle$ the *triality group of* L. In general, a triality group, G, is a group generated by a normal subset, T, of elements that are of order two along with a homomorphism $\pi : G \longrightarrow S_3$ such that for any $g, h \in T$, $|gh| = 3$ when $\pi(g) \neq \pi(h)$, G_L being an example (see [8, 10]).

Lemma 4.5. *Let L be a subloop of C^* where C is an octonion algebra. Suppose L spans C and $f, g \in G_L$ with $f|_i = g|_i$, $i \in \{R, C, E\}$. Then $g(x_j) = sf(x_j)$ and $g(x_k) = s^{-1}f(x_k)$ where $s \in F^*$ and $\{i, j, k\} = \{R, C, E\}$.*

Proof. Without loss of generality we may assume that $f|_E = g|_E$. Thus, fg^{-1} is trivial on E.

Case 1. If $fg^{-1} : 1_R \mapsto a_R$ then $fg^{-1} : \begin{cases} x_R \mapsto xa_R \\ y_C \mapsto a^{-1}y_C \\ z_E \mapsto z_E \end{cases}$. Assume that $a \notin F1$. Since L spans C, there exist elements $x, y \in L$ such that $(xa)y \neq x(ay)$. Also, since $[x, ay, (ay)^{-1}x^{-1}] \in A$, $[fg^{-1}(x), fg^{-1}(ay), fg^{-1}((ay)^{-1}x^{-1})] = [xa, y, (ay)^{-1}x^{-1}] \in A$. But $((xa)y)((ay)^{-1}x^{-1}) \neq (x(ay))((ay)^{-1}x^{-1}) = 1$. Hence, by contradiction, $a \in F1$ meaning $g(x_R) = sf(x_R)$ and $g(x_C) = s^{-1}f(x_C)$ for some $s \in F$.

Case 2. Suppose $fg^{-1} : 1_R \mapsto a_C$. Then $fg^{-1} : \begin{cases} x_R \mapsto ax_C \\ y_C \mapsto ya_R^{-1} \\ z_E \mapsto z_E \end{cases}$. Assume that $a \notin F1$. Since L spans C, there exists an element $x \in L$ such that $xa \neq ax$. Also, since $[x^{-1}, xa, a^{-1}] \in A$, $[fg^{-1}(x^{-1}), fg^{-1}(xa), fg^{-1}(a^{-1})] = [x, ax^{-1}, a^{-1}] \in A$. But $xax^{-1}a^{-1} \neq xx^{-1}aa^{-1} = 1$. Hence, by contradiction, $a \in F1$ meaning $fg^{-1} : \begin{cases} x_R \mapsto sx_C \\ y_C \mapsto s^{-1}y_R \\ z_E \mapsto z_E \end{cases}$ for some $s \in F$. Since L spans C, there exist elements $x, y \in L \setminus F1$ such that $xy \neq yx$. But $[fg^{-1}(x), fg^{-1}(y), fg^{-1}(y^{-1}x^{-1})] = [s^{-1}y, sx, y^{-1}x^{-1}] \notin A$ since $s^{-1}y(sx)y^{-1}x^{-1} = yxy^{-1}x^{-1} \neq xyy^{-1}x^{-1} = 1$. Hence $fg^{-1}(1_R) \notin L_C$.

This completes the proof of Lemma 4.5. □

5 Structure of Octonion Algebras

Here we will let C be an octonion algebra over a field F.

Lemma 5.1. *If L is a subloop of C then the subspace spanned by L over F, $span_F(L)$, is a subalgebra of C.*

Proof. For $k_1l_1 + \cdots + k_nl_n, k'_1l'_1 + \cdots + k'_ml'_m \in A$ where $k_i, k'_i \in F$ and $l_i, l'_i \in L$, $(k_1l_1 + \cdots + k_nl_n)(k'_1l'_1 + \cdots + k'_ml'_m) = k_1k'_1(l_1l'_1) + \cdots + k_nk'_m(l_nl'_m) \in A$. Hence, A is a subalgebra of C. □

Lemma 5.2. *Let $L_1 \leq L_2$ be subloops of C that span C over F. Then $R(L_1) = R(L_2)$ if and only if $L_2 \subseteq F^* \cdot L_1$.*

Proof. Suppose $R(L_1) = R(L_2)$. Then, for every $x \in L_2 \setminus L_1$, $\rho_x = \rho_{y_1}\rho_{y_2}\cdots\rho_{y_n}$ for some $\rho_{y_i} \in L_1$. Thus, $\rho_x(L_1) \subset F^* \cdot L_1$ and $\left\{\frac{(l|x)}{q(x)}x | l \in L_1\right\} \subset F \cdot L_1$. Hence, since L_1 spans C over F, $\{(l|x)|l \in L_1\} \neq \{0\}$ and $x \in F^* \cdot L_1$. Therefore, if $R(L_1) = R(L_2)$ then $L_2 \subseteq F^* \cdot L_1$.

Now suppose that $L_2 \subseteq F^* \cdot L_1$. Then for any $x \in L_2$, $x = ky$ for some $y \in L_1$ and $k \in F^*$. Since $\rho_x \in O(C, q)$, $\rho_x = \rho_{ky} = \rho_y$. So for all $x \in L_2$ we get that $\rho_x \in R(L_1)$. Therefore, if $L_2 \subseteq F^* \cdot L_1$ then $R(L_1) = R(L_2)$. □

Lemma 5.3. *Let L be a subloop of C^* such that L spans C over F and $R(L)$ is irreducible on C. Then a copy of either $R(L)$ or $R(L)/\{\pm I\}$ is contained in $G_{L/L\cap F1}$ with a normal subgroup of index two.*

Proof. Let $\varphi : R(L) \longrightarrow G_{L/L\cap F1}$ be defined as:

$$\varphi(\rho_x) = \tau_{x_E}$$

Claim : φ is well defined.

Proof of claim

If $\rho_{x_1} = \rho_{x_2}$ then by Lemma 5.2, $x_2 = kx_1$ for some $k \in F$. Thus, $x_1 = x_2 \in L/L \cap F1$ and $\tau_{x_1} = \tau_{x_2}$. Δ

Claim : φ is a homomorphism.

Proof of claim

The map φ is a homomorphism as long as

$$\varphi(\rho_{x_1}\rho_{x_2}\cdots\rho_{x_n}) = \tau_{x_{1_E}}\tau_{x_{2_E}}\cdots\tau_{x_{n_E}}$$

is well defined. Suppose $\rho_{x_1}\rho_{x_2}\cdots\rho_{x_n} = \rho_{y_1}\rho_{y_2}\cdots\rho_{y_m}$ where m and n are both odd.

Thus,

$$\frac{-x_n(\cdots(\overline{x_2}(x_1\bar{z}x_1)\overline{x_2})\cdots)x_n}{q(x_1)q(x_2)\cdots q(x_n)} = \frac{-y_m(\cdots(\overline{y_2}(y_1\bar{z}y_1)\overline{y_2})\cdots)y_m}{q(y_1)q(y_2)\cdots q(y_m)}$$

for all $z \in L$. Therfore,

$$q(z)q(x_2)\cdots q(x_{n-1})\frac{x_n(\cdots(x_2^{-1}(x_1z^{-1}x_1)x_2^{-1})\cdots)x_n}{q(x_1)q(x_3)\cdots q(x_n)} =$$

$$= q(z)q(y_2)\cdots q(y_{m-1})\frac{y_m(\cdots(y_2^{-1}(y_1z^{-1}y_1)y_2^{-1})\cdots)y_m}{q(y_1)q(y_3)\cdots q(y_m)}$$

for all $z \in L$. Thus,

$$x_n(\cdots(x_2^{-1}(x_1 z^{-1} x_1)x_2^{-1})\cdots)x_n = y_m(\cdots(y_2^{-1}(y_1 z^{-1} y_1)y_2^{-1})\cdots)y_m$$
$$\in L/L \cap F1$$

for all $z \in L/L \cap F1$. Hence $\tau_{x_{1_E}}\tau_{x_{2_E}}\cdots\tau_{x_{n_E}}(z_E) = \tau_{y_{1_E}}\tau_{y_{2_E}}\cdots\tau_{y_{m_E}}(z_E)$ for all $z \in L/L \cap F1$. So, by Lemma 4.5, $\tau_{x_{1_E}}\tau_{x_{2_E}}\cdots\tau_{x_{n_E}} = \tau_{y_{1_E}}\tau_{y_{2_E}}\cdots\tau_{y_{m_E}}$. Likewise, reguardless of what m and n are, if $\rho_{x_1}\rho_{x_2}\cdots\rho_{x_n} = \rho_{y_1}\rho_{y_2}\cdots\rho_{y_m}$ then $\tau_{x_{1_E}}\tau_{x_{2_E}}\cdots\tau_{x_{n_E}} = \tau_{y_{1_E}}\tau_{y_{2_E}}\cdots\tau_{y_{m_E}}$. Hence, φ is a homomorphism. $\triangle$

Claim : There is a one-to-one correspondance between the reflections, ρ_v, of $R(L)$ and the central automorphisms, τ_{x_E}, for $x \in L/L \cap F1$.

Proof of claim

Clearly, by definition of φ, for every $x \in L/L \cap F1$ there exists an element $v \in L$ such that $\varphi(\rho_v) = \tau_{x_E}$. If $v, u \in L$ such that $\varphi(\rho_v) = \tau_{x_E} = \varphi(\rho_u)$ then $u = \alpha v$ for some $\alpha \in F$. Thus, $\rho_u(z) = -\frac{u\bar{z}u}{q(u)} = -\frac{\alpha v \bar{z} \alpha v}{q(\alpha v)} = -\frac{\alpha^2 v \bar{z} v}{\alpha^2 q(v)} = -\frac{v\bar{z}v}{q(v)} = \rho_v(z)$ for all $z \in L$. Therefore $\rho_v = \rho_u$ and there is a one-to-one correspondance between the reflections, ρ_v, and the central automorphisms, τ_{x_E}. $\triangle$

Moreover, if $\varphi(\rho_{x_1}\rho_{x_2}\cdots\rho_{x_{2n}}) = \tau_{x_{1_E}}\tau_{x_{2_E}}\cdots\tau_{x_{2n_E}} = 1$ then

$$x_{2n}(\cdots x_2(x_1^{-1} z x_1^{-1})x_2\cdots)x_{2n} = z$$

for all $z \in L/L \cap F1$. Thus, for all $z \in L$ there exists an element $k_z \in F$ such that

$$q(x_1)\cdots q(x_{2n-1})\frac{x_{2n}(\cdots(x_2(x_1^{-1}zx_1^{-1})x_2)\cdots)x_{2n}}{q(x_2)q(x_4)\cdots q(x_{2n})} = k_z z.$$

Hence,

$$\rho_{x_1}\rho_{x_2}\cdots\rho_{x_{2n}}(z) = \frac{x_{2n}(\cdots(x_2(\overline{x_1}z\overline{x_1})x_2)\cdots)x_{2n}}{q(x_1)q(x_2)\cdots q(x_{2n})} = k_z z$$

for all $z \in L$. Furthermore, since

$$\begin{aligned} q(z) &= q(\rho_{x_1}\rho_{x_2}\cdots\rho_{x_{2n}}(z)) \\ &= q(k_z z) \\ &= k_z^2 q(z), \end{aligned}$$

$k_z \in \{\pm 1\}$ for all $z \in L$.

Now suppose $z_1, z_2 \in L$ such that $k_{z_1} \neq k_{z_2}$. Then $charF \neq 2$ and without loss of generality we may assume that $k_{z_1} = 1$ and $k_{z_2} = -1$. Therefore, since $\rho_{x_i} \in O(C,q)$, $(z_1|z_2) = (z_1|-z_2)$ which implies that $(z_1|z_2) = 0$. Thus, $L = \{z \in L|k_z = 1\} \cup \{z \in L|k_z = -1\} \leq U \cup U^{\perp}$ for some subalgebra, U, of C. Notice that for all $x, u \in U \cap L$ and $v \in U^{\perp} \cap L$, $\rho_v(x) = x \in U \cap L$ and $\rho_u(x) = x - \frac{(x|u)}{q(u)}u \in U \cap L$. But since $R(L)$ is irreducible on C, either $U \cap L = \varnothing$ or $U^{\perp} \cap L = \varnothing$. Hence, $k_{z_1} = k_{z_2}$ for all $z_1, z_2 \in L$.

Therefore $ker(\varphi) \leq \{\pm I\}$. Hence, there exists a copy of either $R(L)$ or $R(L)/\{\pm I\}$ in $G_{L/L\cap F1}$ with a normal subgroup, (the rotation subgroup), of index two. □

Proposition 5.4. *If a composition algebra of a given dimension, C, over a field, F, is split then it is unique up to isomorphism. Moreover, if F is a finite field and*

C is of dimension greater than one then C is split. Such an algebra of dimension eight is of type $O_8^+(F)$.

Proof. Let C be a composition algebra over the field F that is split. Suppose there does not exist an element $x \in C$ such that $q(x) = 0$ and $(x|1) \neq 0$. So for every $x \in C$ with $q(x) = 0$, $x + \bar{x} = 0$. Choose a nonzero element $y \in C$ such that $q(y) = 0$. Since $q(yx) = q(y)q(x) = 0$ for all $x \in C$, $yx + \overline{yx} = 0$ for all $x \in C$. So $(y|x)1 = y\bar{x} + x\bar{y} = 0$ for all $x \in C$. But C is a non-degenerate algebra. By contradiction, there exists an element $x \in C$ such that $q(x) = 0$ and $(x|1) = 1$. Note that $x + \bar{x} = (x|1)1 = 1$. Thus C contains a subalgebra, $Fx + F\bar{x} = F1 + Fx$, of dimension two over F that is isomorphic to $F \oplus F$. So any two split composition algebras of dimension two over some field, F, are isomorphic.

Now suppose that A_1 and A_2 are proper composition subalgebras of C_1 and C_2, respectively, and are of dimension greater than one with $A_1 \cong A_2$. Let $b_i \in A_i^\perp$ for $i \in \{1, 2\}$. Since C_i is non-degenerate, there exists an element $c_i \in C_i$ such that $(b_i|c_i) \neq 0$. Let $c_i = a_i + a_i'$ where $a_i \in A_i$ and $a_i' \in A_i^\perp$. Thus,

$$\begin{aligned} q(a_i' + b_i) - q(a_i') - q(b_i) &= (b_i|a_i') \\ &= (b_i|a_i) + (b_i|a_i') \\ &= (b_i|a_i + a_i') \\ &\neq 0. \end{aligned}$$

Hence, there exists an element $s_i \in A_i^\perp$ with $q(s_i) \neq 0$. Let $a_i'' \in A_i$ such that $q(a_i'') = \frac{1}{q(s_i)}$. Then there exists an element $t_i = a_i'' s_i \in A_i^\perp$ such that $q(t_i) = 1$.

Therefore, by Dickson's Theorem 3.11, $A_1 + A_1t_1 \leq C_1$ and $A_2 + A_2t_2 \leq C_2$ are isomorphic composition algebras of dimension twice that of A_1.

So by induction on the dimension of A_i, we get that any two split composition algebras of the same dimension over some field, F, are isomorphic. □

Definition 5.5. *A hexagon line of a split octonion algebra C is a totally singular 2-space that is contained in $1^\perp$ such that the multiplication is zero.*

A hexagonic structure contains points and lines where any two points can be joined by a path containing at most three lines and there does not exist any 2, 3, 4, or 5-gons. For an octonion algebra, C, we will call a point, a singular 1-space, P, with $P^2 = 0$. We say that a point P is incident to a hexagon line E if $P \subset E$. This induces a hexagonic structure which we call the *generalized hexagon.* Details of this construction can be found in [21].

Theorem 5.6. *The automorphism group of a split octonion algebra, C, is of type $G_2(F)$ and is transitive on the hexagon lines (see chap. 2 in [22]).*

Definition 5.7. *The stabilizer of a subspace, U, of C is the subspace $Stab_C(U) = \{x \in C \mid xu \in U \text{ for all } u \in U\}$.*

Let H be an additive subgroup of an octonion algebra, C, such that $\{h-1|h \in H\}$ is contained in a hexagon line of C. Also, let Q be a subalgebra of C that is contained in the stabilizer of $\{h - 1 \mid h \in H\}$. The product $Q \bullet H$ is defined to be the algebra with underlying set $\{(x, h)|x \in Q, h \in H\}$ and the binary operation $(x, g)(y, h) = (xy, 1 + x(h - 1) + (g - 1)y)$.

Example 5.8. *For a field F let C be the split octonion algebra defined in section 2.*

$$C = \left\{ \begin{pmatrix} a & (v_1, v_2, v_3) \\ (u_1, u_2, u_3) & b \end{pmatrix} | a, b, v_i, u_i \in F \right\}$$

The subspace $S = \left\{ \begin{pmatrix} 0 & (0, v_2, 0) \\ (0, 0, u_3) & 0 \end{pmatrix} | v_2, u_3 \in F \right\} \subset C$ *is an example of a hexagon line of C. The stabilizer of such a hexagon line in C is the subspace*

$$\left\{ \begin{pmatrix} a & (v_1, v_2, 0) \\ (u_1, 0, u_3) & b \end{pmatrix} \right\} = S^{\perp}$$

$$\cong \left\{ \begin{pmatrix} a & (v_1, 0, 0) \\ (u_1, 0, 0) & b \end{pmatrix} \right\} \bullet \left\{ \begin{pmatrix} 1 & (0, v_2, 0) \\ (0, 0, u_3) & 1 \end{pmatrix} \right\}$$

$$\cong M_2(F) \bullet F^2.$$

Such a subspace is an algebra that is maximal in C (see section 6).

Now let K be a subloop of $GLL(F)$ such that $K \leq L = \left(S^{\perp}\right)^*$ for some hexagon line S. Without loss of generality, by Theorem 5.6, we may assume that $S = \left\{ \begin{pmatrix} 0 & (0, s, 0) \\ (0, 0, t) & 0 \end{pmatrix} | s, t \in F \right\}$.
Thus

$$S^{\perp} = \left\{ \begin{pmatrix} a & (v_1, v_2, 0) \\ (u_1, 0, u_3) & b \end{pmatrix} | a, b, v_1, v_2, u_1, u_3 \in F \right\}.$$

Define

$$\pi : L \longrightarrow \left\{ \begin{pmatrix} a & (v_1, 0, 0) \\ (u_1, 0, 0) & b \end{pmatrix} | a, b, v_1, u_1 \in F, ab - v_1 u_1 \neq 0 \right\} \cong GL_2(F)$$

as

$$\pi\left(\begin{pmatrix} a & (v_1,v_2,0) \\ (u_1,0,u_3) & b \end{pmatrix}\right) = \begin{pmatrix} a & (v_1,0,0) \\ (u_1,0,0) & b \end{pmatrix}$$

Note that

$$\pi\left(\begin{pmatrix} a & (v_1,v_2,0) \\ (u_1,0,u_3) & b \end{pmatrix}\begin{pmatrix} c & (\alpha_1,\alpha_2,0) \\ (\beta_1,0,\beta_3) & d \end{pmatrix}\right)$$

$$= \pi\left(\begin{pmatrix} ac+v_1\beta_1 & (a\alpha_1+dv_1, a\alpha_2+dv_2+u_1\beta_3-u_3\beta_1,0) \\ (b\beta_1+cu_1,0,b\beta_3+cu_3+v_1\alpha_2-v_2\alpha_1) & bd+u_1\alpha_1 \end{pmatrix}\right)$$

$$= \begin{pmatrix} ac+v_1\beta_1 & (a\alpha_1+dv_1,0,0) \\ (b\beta_1+cu_1,0,0) & bd+u_1\alpha_1 \end{pmatrix}$$

$$= \begin{pmatrix} a & (v_1,0,0) \\ (u_1,0,0) & b \end{pmatrix}\begin{pmatrix} c & (\alpha_1,0,0) \\ (\beta_1,0,0) & d \end{pmatrix}$$

$$= \pi\left(\begin{pmatrix} a & (v_1,v_2,0) \\ (u_1,0,u_3) & b \end{pmatrix}\right)\pi\left(\begin{pmatrix} c & (\alpha_1,\alpha_2,0) \\ (\beta_1,0,\beta_3) & d \end{pmatrix}\right).$$

So π is a homomorphism with $ker(\pi) \leq \left\{\begin{pmatrix} 1 & (0,v_2,0) \\ (0,0,u_3) & 1 \end{pmatrix} | v_2, u_3 \in F\right\}$.

Note that both the $ker(\pi|_K)$ and $Im(\pi|_K)$ are groups. This brings up the question: "Does there exist a homomorphism ϕ from $Im(\pi|_K) \bullet ker(\pi)$ onto $Im(\pi|_K) \bullet ker(\pi|_K)$?" If so then $\phi|_K$ is a one-to-one homomorphism from K onto $Im(\pi|_K) \bullet ker(\pi|_K)$ and

$$K = \phi|_K^{-1}(Im(\pi|_K)) \bullet ker(\pi|_K)$$

$$\cong G \bullet H$$

where $G \leq GL_2(F)$ and $H \leq F^2$.

Now let L be a subloop of C^* such that $L \leq Q \cup Q^\perp$ for some quaternion subalgebra Q. If $L \leq Q$ then L is associative and therefore a group that is isomorphic to a subgroup of $GL_2(F)$. Otherwise if $L \not\leq Q$ then $G = L \cap Q$ is a subgroup of L with $[L : G] = 2$ and $G \cong H \leq GL_2(F)$. So $L = G \cup Gv$ for some $v \in L \cap Q^\perp$ and by Dickson's Theorem 3.11 $(g + hv)(x + yv) = (gx - q(v)q(y)y^{-1}h) + (q(x)hx^{-1} - yg)v$ for any $g, h, x, y \in G$.

Lemma 5.9. *If F_o is a subfield of F then $GLL(F_o) \leq GLL(F)$.*

6 Proof of Theorem 1.3

In this section we will let L be a subloop of an octonion algebra, C, over a field F and $R = R(L)$ will be the reflection group of L.

Lemma 6.1. *If L is a subloop of C and U is a subspace of C that is left invariant under $R(L)$ then $L \subseteq U \cup U^\perp$ and $U^\perp$ is also left invariant under $R(L)$.*

Proof. Since U is an invariant subspace of C, for every $x \in L$ and every $u \in U$ we have that $\rho_x(u) \in U$. Therefore, $u - \frac{(x|u)}{q(x)}x \in U$ for any $x \in L$ and $u \in U$. So if x is an element of L then $x \in U$ unless $(x|u) = 0$ for all $u \in U$. Hence, $L \subseteq U \cup U^\perp$. Moreover, if $v \in U^\perp$ and $x \in L$ then either $x \in U^\perp$ or $(x|v) = 0$. Therefore, $\rho_x(v) = v - \frac{(x|v)}{q(x)}x \in U^\perp$ and $U^\perp$ is left invariant under $R(L)$. □

Lemma 6.2. *Suppose $1 \in U$ where U is a subspace invariant under $R(L)$. Then for any $y \in L$, yU is an $R(L)$-invariant subspace of C.*

Proof. Let y be some fixed element in L. Note that for any $x \in L$

$$\begin{aligned}\rho_x(yu) &= yu - \frac{(x|yu)}{q(x)}x \\ &= yu - \frac{(\bar{y}x|u)}{q(x)}x\end{aligned}$$

for all $u \in U$. If $(\bar{y}x|u) \neq 0$, then $\bar{y}x \notin U^{\perp}$. By 6.1, $\frac{\bar{y}}{q(y)}x \in U \cup U^{\perp}$. Therefore, $\frac{\bar{y}}{q(y)}x = v$ for some $v \in U$. Thus, $yv = y(\frac{\bar{y}}{q(y)}x) = x$. Hence $\rho_x(yu) = yu - \frac{(\bar{y}x|u)}{q(x)}yv \in yU$. Therefore, yU is an invariant subspace of C. □

Lemma 6.3. *Let U be a non-degenerate subalgebra of C with $dim_F(U) = n$. If U is invariant under $R(L)$ and $x \in L \setminus U$ then $U + xU$ is an invariant non-degenerate subalgebra of dimension $2n$.*

Proof. By 6.1 $x \in U^{\perp}$, so by Dickson's Theorem 3.11 $U + xU$ is a non-degenerate subalgebra of dimension $2n$. In Lemma 6.2 we showed that xU is an invariant subspace. Therefore, the non-degenerate subalgebra, $U + xU$, is also invariant under $R(L)$. □

Now suppose L is a subloop of C^* such that L does not span C. For any set $S \subseteq C$ we will denote the vector space spanned by S over F as $span_F(S)$. The symbol A will always be used to denote the span of L over the field F.

Lemma 6.4. *If C is not split and A is properly contained in C then $A \subset Q$ for some quaternion subalgebra, Q, of C or A is totally isotropic.*

Proof. Since C is not split, for every $0 \neq x \in C$, $q(x) \neq 0$. Let $B_1 = F1 \leq A$.

If $A = B_1$ then by Theorem 3.11 or 3.12, there exists a non-degenerate subalgebra of C, B_2, that contains A and is of dimension 2. Since $q(x) \neq 0$ for all $x \in B_2^{\perp}$, by Dickson's Theorem 3.11, there exists a non-degenerate subalgebra of C, Q, that contains A and is of dimension 4.

If $A \neq B_1$ and A is not totally isotropic then by Theorem 3.11 or 3.12, there exists a non-degenerate subalgebra of A, B_2, that is of dimension 2. If $A = B_2$ then since $q(x) \neq 0$ for all $x \in B_2^{\perp}$, by Dickson's Theorem 3.11, there exists a non-degenerate subalgebra of C, Q, that contains A and is of dimension 4. Otherwise, if $A \neq B_2$ then there exists some element $y \in A \cap B_2^{\perp}$ with $q(y) \neq 0$. Thus, by Dickson's Theorem 3.11, there exists a non-degenerate subalgebra of C, Q, that is contained in A and is of dimension 4. Assume $A \neq Q$. Then there exists some element $z \in A \cap Q^{\perp}$ with $q(z) \neq 0$ and by Dickson's Theorem 3.11, A contains the non-degenerate subalgebra, C. But A is properly contained in C. Hence, $A \subset Q$ for some quaternion subalgebra, Q, of C. □

For now on, in this proof of Theorem 1.3, we will assume that C is split. We now want to prove the following proposition.

Proposition 6.5. *If a subloop L_1 of C does not span C, then we have one of the following:*

1. *$L_1 \leq S^{\perp}$ for some hexagon line S;*

2. *$L_1 \leq Q$ for some nonsplit quaternion subalgebra Q;*

3. *L_1 is totally isotropic and F is a nonperfect field of characteristic two.*

Definition 6.6. *The radical of an algebra, B, which we will denote by $Rad(B)$, is the subspace $\{b \in B \mid q(b) = 0 \text{ and } (x|b) = 0 \text{ for all } x \in B\}$ of B.*

Lemma 6.7. *$Rad(A)$ is an ideal of A.*

Proof. Here we want to show that for $v \in Rad(A)$ and $u \in A$, both uv and vu are in the radical of A. So suppose $v \in Rad(A)$ and $u \in A$. By Lemma 3.1, $(1|u)(x|v) = (v|ux) + (x|uv)$ for any $x \in A$. Thus, $(1|u)0 = 0 + (x|uv)$ which tells us that $(x|uv) = 0$. Also, $q(uv) = q(u)q(v) = q(u)0 = 0$. Therefore, $uv \in Rad(A)$. A similar argument shows that $vu \in Rad(A)$.

□

Lemma 6.8. *The stabilizer of a hexagon line of C is a subalgebra of C.*

Proof. Let $U = span_F(v, u)$ be a hexagon line of C. Certainly, the stabilizer, $stab_C(U)$, is a subspace of C that contains 1. Also, for any $x \in stab_C(U)$ and $a \in U$, $(x|a) = (1|\bar{x}a) = 0$ since $\bar{x}a = [(x|1)1 - x]a \in U$. Thus, $stab_C(U) \subseteq U^{\perp}$. If $x, y \in stab_C(U)$ then for any $a \in U$, we get that

$$\begin{aligned}(xy)a &= -(xy)\bar{a} \\ &= a(\bar{y}\bar{x}) \\ &= -y(\bar{a}\bar{x}) \\ &= y(xa) \\ &= yb \\ &= c\end{aligned}$$

for some $b, c \in U$. Therefore, $stab_C(U)$ is a subalgebra of C. $\square$

For now, the symbol B will always be used to represent a maximal composition subalgebra of A such that $1 \in B$.

Lemma 6.9. *Either B is nondegenerate and $B \dot{+} Rad(A) = A$ or $B = F1$ and A is totally isotropic.*

Proof. If B is non-degenerate then, by definition of $Rad(A)$, $B \cap Rad(A) = \{0\}$. Suppose there exists an element $v \in B^{\perp} \cap A$ such that $q(v) \neq 0$. Then, by Dickson's Theorem 3.11, $B + Bv$ is a composition algebra contained in A. But B is a maximal composition subalgebra of A. Thus, $q(v) = 0$ for all $v \in B^{\perp} \cap A$. Since $q(v) = 0 = q(u)$ for all $v, u \in B^{\perp} \cap A$, $(v|u) = q(v+u) - q(v) - q(u) = 0$. Hence, $B^{\perp} \cap A \subseteq Rad(A)$ and therefore $B^{\perp} \cap A = Rad(A)$. So if B is non-degenerate then $B \dot{+} Rad(A) = A$.

Now suppose $B = F1$ where F is of characteristic 2 and A is not totally isotropic. Then $B \cap Rad(A) = \{0\}$ since $q(x) = 0$ for all $x \in Rad(A)$. Therefore, if there exists an element $v \in A$ such that $(v|1) \neq 0$ then, by Theorem 3.12, $B + Bv$ is a composition algebra contained in A. Since B is a maximal composition subalgebra of A, $(v|1) = 0$ for all $v \in A$. Moreover, $(v|u) = (v\bar{u}|1) = 0$ for any $v, u \in A$. Let y be any element in A and let $\alpha = q(y)$. There exists a unique element $\beta \in F$ such that $\beta^2 = \alpha$. Since $q(y - \beta 1) = (y, \beta 1) + q(y) + q(\beta 1) = 0 + \alpha + \alpha = 0$, there exists an element $\beta 1 = y_1 \in B$ and an element $y - \beta 1 = y_2 \in Rad(A)$ such that $y = y_1 + y_2$. Hence if $B = F1$ where F is of characteristic 2 then $B \dot{+} Rad(A) = A$. $\square$

Lemma 6.10. *Suppose $dim_F(B) = 4$. If $dim_F(A) = 6$ then A is the stabilizer of a hexagon line, $Rad(A)$. Otherwise, A is either properly contained in the stabilizer of a hexagon line or is a nonsplit quaternion subalgebra.*

Proof. Suppose there exists an element $v \in A \cap B^{\perp}$. We will first show that $B + Bv$ is an algebra of dimension 6 over the field F. So suppose that $s+tv, x+yv \in B+Bv$. By Proposition 3.10 we have that

$$\begin{aligned}(s + tv)(x + yv) &= (sx - q(v)(\bar{y}t)) + (t\bar{x} + ys)v \\ &= sx + (t\bar{x} + ys)v \quad \in B + Bv.\end{aligned}$$

Let $u \in B^{\perp}$ with $q(u) \neq 0$. Since $dim_F(B) = 4$, B is non-degenerate and, by Dickson's Theorem 3.11, $B + Bu = C$. Let $v' \in C$ such that $q(v') = 0$ and $(v|v') \neq 0$. Since Cv and Cv' are totally singular and $C = C(v + v')$ is non-degenerate, $dim_F(Cv) = 4 = dim_F(Cv')$. So

$$\begin{aligned}4 &= dim_F(Cv) \\ &= dim_F(Bv + (Bu)v) \\ &= dim_F(Bu \cap Cv) + dim_F(B \cap Cv)\end{aligned}$$

since $Bv \subseteq B^{\perp} = Bu$ and $(Bu)v \subseteq (Bu)B^{\perp} \subseteq (Bu)(Bu) \subseteq B$ by Proposition 3.10. Thus, since Cv is totally singular and B, Bu are non-degenerate subspaces of dimension four, $dim_F(Bu \cap Cv) \leq 2$ and $dim_F(B \cap Cv) \leq 2$. Thus, we get that $dim_F(Bv) = dim_F(Bu \cap Cv) = 2$. Since $dim_F(B + Bv) = 4 + 2 = 6$, $dim_F(A) \geq 6$ with $Bv \subseteq Rad(B + Bv)$.

We now want to show that $Bv = Rad(A)$. For any $r \in Rad(A)$ we have that $dim_F(B+Bv+Br) \leq dim_F(A) < 8$. Thus $Bv \cap Br \neq \varnothing$. So $dim_F(Bv \cap Br) \in \{1, 2\}$. But $dim_F((B+Bv) \cap (B+Br)) \neq 5$, otherwise $B+Bx \subseteq (B+Bv) \cap (B+Br)$ for some $x \in Rad(A)$ and $dim_F(B+Bx) = 6$ for all $x \in Rad(A)$. Hence, $dim_F(Bv \cap Br) = 2$ and $r \in B + Bv$. Now if $tv, yv \in Bv = Rad(A)$ then $(tv)(yv) = -q(v)\bar{y}t = 0$. Therefore, $A = B + Bv$ is a maximal subalgebra of C and stabilizes a totally singular 2-space with multiplication zero, $Rad(A)$. By Lemma 6.8, $stab_C(Rad(A))$ is a subalgebra of C. Therefore, either $A = stab_C(Rad(A))$ or $C = stab_C(Rad(A))$. But for any $v \in Rad(A)$, $dim_F(Cv) = 4$. Hence, $C \neq stab_C(Rad(A))$ and $A = stab_C(Rad(A))$.

Now suppose $A = B$ and is split. Let v be an element in $A^{\perp}$ such that $q(v) = 0$. Then A is properly contained in $B + Bv$ which is the stabilizer of a hexagon line, $Rad(B + Bv)$. □

Lemma 6.11. *Let H be a hexagon line and let $x \in H \setminus \{0\}$. Then $xC \leq Stab_C(H)$.*

Proof. Let $y \in H \setminus Fx$ and $v \in C$. By Lemma 3.3, $y(xv) + \bar{x}(\bar{y}v) = (\bar{y}|x)v = 0$. Thus, $y(xv) = -\bar{x}(\bar{y}v) = x(\bar{y}v) \in xC \cap yC$. But, by Theorem 3.7, $xC \cap yC = H$. Hence, $y(xC) \subseteq H$ and $xC \leq Stab_C(H)$. □

Lemma 6.12. *If $dim_F(B) \leq 2$ then A is not maximal. Moreover, A is properly contained in the stabilizer of some hexagon line.*

Proof. Case 1. If $dim_F(Rad(A)) = 0$ then $A = B$ and $A = B$ is properly contained in a quaternion subalgebra. Moreover, by Lemma 6.10, A is contained in the stabi-

lizer of a hexagon line.

Case 2. If $dim_F(Rad(A)) = 1$ then $Rad(A) = Fx$ with $x \neq 0$. Since $Ax \subseteq Rad(A)$, $dim_F(A/Ann_A(x)) = 1$. Thus $A = Ann_A(x) + F1$. Let H be a hexagon line containing x. Therefore, by Lemma 6.11, $Ann_A(x) = xC \leq Stab_C(H)$. Hence $A \leq Stab_C(H)$.

Case 3. If $dim_F(Rad(A)) = 2$ then, since $Rad(A)$ is an ideal of A, A is properly contained in the stabilizer of $Rad(A)$. Let $Rad(A) = span_F(a, b)$. Suppose $ab = k_1a + k_2b$ for $k_1, k_2 \in F$ then $0 = a^2b = a(ab) = k_1a^2 + k_2(ab) = k_2(ab)$. Thus either $k_2 = 0$ or $ab = 0$. If $k_2 = 0$ then $ab = k_1a$ and $0 = ab^2 = (ab)b = k_1ab$. Hence $ab = 0$. Therefore, A is properly contained in the stabilizer of a totally singular 2-space with multiplication zero, $Rad(A)$.

Case 4. Suppose $dim_F(Rad(A)) = 3$ with $Rad(A) = span_F(a_1, a_2, a_3)$. By corollary 3.8 there exists some $a \neq b \in \{a_1, a_2, a_3\}$ such that $ab \neq 0$. Notice that $ab \notin span_F(a, b)$. Otherwise, if it were then $ab = k_1a + k_2b$ and $0 = a^2b = k_1a^2 + k_2ab = k_2ab \neq 0$. Thus, $Rad(A) = span_F(a, b, ab)$.

Since $Rad(A)$ is an ideal of A, for any $x \in B$ we have that $xb = k_1a + k_2b + k_3(ab)$ for some $k_1, k_2, k_3 \in F$. By multiplying both sides of the equation on the right by b we get that $0 = k_1(ab) + 0 + 0$. Thus, $k_1 = 0$ and $Bb \subseteq span_F(b, ab)$.

Now for any $x \in B$ we have that $x(ab) = k_1a + k_2b + k_3(ab)$ for some $k_1, k_2, k_3 \in F$.

By multiplying both sides of the equation on the right by b we get that

$$\begin{aligned} k_1(ab) + 0 + 0 &= (x(ab))b \\ &= -[(\overline{ab})\bar{x}]b \\ &= [(ab)\bar{x}]b \\ &= a(b\bar{x}b) \\ &= -a(\overline{b\bar{x}}b) \\ &= -a(x\bar{b}b) \\ &= 0. \end{aligned}$$

Thus, $k_1 = 0$ and $B(ab) \subseteq span_F(b, ab)$. Moreover, $b(ab) = -b(\bar{b}\bar{a}) = b(ba) = b^2a = 0$. Hence, A is properly contained in the stabilizer of a totally singular 2-space with multiplication zero, $span_F(b, ab)$. □

Thus, if C is split and L is a subloop that does not span C then L is contained in the stabilizer of a hexagon line, S. This completes the proof of proposition 6.5.

We will now show that L spans V if and only if $V = [V, R]$. Since C is non-degenerate, for every $x \in L$ there exists some $v \in V$ such that $(x|v) \neq 0$. Therefore,

we know that:

$$\begin{aligned}
[V,R] &= span\left(\{-v+v^r \mid r\in R, v\in V\}\right)\\
&= span\left(\left\{-v+v-\frac{(x|v)}{q(x)}x \mid x\in L, v\in V\right\}\right)\\
&= span\left(\left\{\frac{-(x|v)}{q(x)}x \mid x\in L, v\in V\right\}\right)\\
&= span(L).
\end{aligned}$$

Thus $V = [V,R]$ if and only if L spans V. So if $V > [V,R]$ then L does not span V and therefore L is either contained in a quaternion subalgebra or, by Proposition 6.5, $L \leq S^{\perp}$ for some hexagon line S.

Now let us suppose that $V = [V,R]$ and that R is reducible. Thus, V contains some proper invariant subspace. We showed in Lemma 6.1 that there exists some proper invariant subspace of V that contains the identity, 1. Let U be a minimal invariant subspace of V such that $1 \in U$.

Lemma 6.13. *$Rad(U) = \{0\}$.*

Proof. Since $\rho_y(u) = u - \frac{(y|u)}{q(y)}y \in U$ for all $u \in U$, $(y|u) = 0$ for all $y \in L \setminus U$. Therefore $Rad(U) \subset Rad(span_F(L)) = Rad(V) = \{0\}$ □

We now want to show that U is a composition algebra. By Lemma 3.2, for every $x \in U \cap L$, $x^{-1} = \frac{1}{q(x)}\bar{x} = \frac{-1}{q(x)}x + \frac{(x|1)}{q(x)}1 \in U$. We showed in Lemma 6.2 that xU is an invariant subspace of V for any $x \in U$. Since both U and xU are invariant subspaces that contain the identity, 1, $xU \cap U$ is also an invariant subspace containing the identity. By minimality of U, $xU = U$. Therefore for all $x, y \in U \cap L$,

$x, y \in U \cap L$, $xy \in U$. Since U is invariant under R, $L \subset U \cup U^{\perp}$. Also, since C is non-degenerate, $dim_F(U) + dim_F(U^{\perp}) = 8$. So if $V = [V, R]$ then $dim_F(U \cap U^{\perp}) = 0$ and $U = span(U \cap L)$. Hence, U is closed under multiplication and is therefore a composition algebra of dimension 1, 2, or 4.

If $dim_F(U) \leq 2$ then, since $span(L) = V$, by Lemma 6.1, there exists an element $x \in L \cap U^{\perp}$. So from Lemma 6.3 one can use Dickson's Theorem 3.11 and Theorem 3.12 to find an invariant composition algebra of dimension 4, Q. Hence, we showed in Lemma 6.1 that L is contained in $Q \cup Q^{\perp}$.

We now have the material to prove Theorem 1.3.

Proof. If $V = [V, R]$ and $R = R(L)$ is reducible then, from the material above, $L \subseteq Q \cup Q^{\perp}$ for some quaternion subalgebra Q. If $V > [V, R]$ and C is not split then, by Lemma 6.4, L is contained a quaternion subalgebra, Q. If $V > [V, R]$ and C is split then, by Proposition 6.5, L is contained in $S^{\perp}$ for some hexagon line S. □

7 Proof of Theorem 1.4

Proposition 7.1. *Let $G \leq GL_n(F)$ with $n \geq 2$, be generated by reflections for $char(F) \neq 2$ and generated by transvections for $char(F) = 2$. Suppose that G is irreducible but imprimitive on $V = F^n$. Then there exists an element $g \in GL_n(F)$ with G^g monomial. Indeed, $G^g = D : S_n$, where S_n is the group of permutation matrices and D is a group of diagonal matrices. Also, there is a subgroup A of F^* with either $D \cong A^n$, being the group of all diagonal matrices with entries from A,*

or $D \cong A^{n-1}$, *being the subgroup of determinant* 1 *matrices.*

Proof. Let $T = T^G$ be the generating set of reflections (transvections), elements of order 2 with $[V,t]$ of dimension 1, for all $t \in T$.

For W a proper block of imprimitivity in V, there is an element $t \in T$ such that $W^t \neq W$. Thus, $[W,t]$ has dimension at least that of W. Therefore W and $[W,t]$ both have dimension exactly 1. Let $\Omega = \{W_i | 1 \leq i \leq n\}$ be the n blocks of W^G, each a 1-space. The group G permutes Ω. Therefore, G may be conjugated by some g into the group of all monomial matrices. Identify G with this conjugate. Let D be the kernel of the action of G on Ω, that is, the subgroup of the diagonal matrices that are contained in G. By irreducibility, the group G/D induced on Ω is a transitive subgroup of $Sym(\Omega) \cong S_n$.

Every $t \in T$ is either in the diagonal subgroup D, and fixes W_i for all i, or exchanges two of the blocks, say W_i and W_j, and induces the transposition (i,j) on the block set, Ω. A transitive subgroup of S_n that contains transpositions is the whole group S_n. Therefore, $G/D \cong Sym(\Omega)$ and every $t \in T \setminus D$ acts as a transposition. In the monomial group we get that, for any $t, s \in T \setminus D$ with $tD \neq sD$, ts has the same order, 2 or 3, as $tD.sD$ of the corresponding transpositions in $G/D \cong S_n$.

For $1 \leq j \leq n-1$, let $t_{j,j+1} \in T$ inducing $(j, j+1)$ on Ω. Thus, $S = \langle t_{1,2}, \ldots, t_{n-1,n} \rangle \cong W(A_{n-1}) \cong S_n$ with $G = D : S$. If $0 \neq e_1 \in W_1$ then $E = e_1^S = \{e_1, \ldots e_n\}$ is a basis with $e_j \in W_j$, which S permutes as it does Ω.

We will write our matrices with respect to the basis E, so that S is the group of all permutation matrices.

Let $t = t_{i,j}$ be the transposition $(i,j) \in T \cap S$. On $Fe_i + Fe_j$ it acts as

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and the monomial conjugates of t inducing the same transposition on Ω are of the form

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$$

for $a \in F^*$. Therefore there exists a subgroup $A \leq F^*$ such that $tD \cap T$ consists exactly of these elements with $a \in A$.

Therefore, the elements $t(tD \cap T) \in D$ generate the determinant 1 group isomorphic to A^{n-1}. If $T \cap D = \varnothing$ then this subgroup is all of D. If $T \cap D \neq \varnothing$, then D is the full diagonal group with entries from A.

□

For a finite field K, the group $O^\epsilon_8(K)$ has a quasisimple derived group $\Omega^\epsilon_8(K)$. (See [25] for this and other facts about orthogonal groups.) If K is of characteristic 2 then $\Omega^\epsilon_8(K)$ has index 2 in $O^\epsilon_8(K)$, which is generated by its unique conjugacy class of transvections. If K is not of characteristic 2 then $\Omega^\epsilon_8(K)$ has index 4 in $O^\epsilon_8(K)$, which is generated by its two conjugacy classes of reflections. Let ${}^+\Omega^\epsilon_8(K)$ be the subgroup of index 2 in $O^\epsilon_8(K)$ that is generated by the reflections, ρ_x, with center, x, of square norm. Also, let ${}^-\Omega^\epsilon_8(K)$ be the subgroup of index 2 in $O^\epsilon_8(K)$ which is

generated by the reflections, ρ_y, with center, y, of nonsquare norm. Here we also write ${}^{\pm}\Omega_8^{\epsilon}(K)$ for $O_8^{\epsilon}(K)$. The rest of this section is devoted to a proof of Theorem 1.4. In particular, we let L, C, F, and R be as in the statement of the theorem.

Theorem 7.2. *R is one of the following and unique up to conjugacy in $O(V,q)$:*

1. *$R = {}^{\delta}\Omega_8^{\epsilon}(F_o)$ for some finite subfield F_o of F of odd characteristic with ϵ equal to $-$ or $+$ and δ equal to $-, +$, or $\pm$;*

2. *$R = O_8^{\epsilon}(F_o)$ for some finite subfield F_o of F of characteristic 2 with ϵ equal to $-$ or $+$;*

3. *$R = W(E_8) \cong 2O_8^{+}(2)$ where $F = F_p$ for some odd prime p;*

4. *$R = S_9$ where $charF \neq 3$;*

5. *$R = S_{10}$ where $charF = 5$;*

6. *$R = A^n : S_8$ where $1 \neq A \leq F^*$ and n=7 or 8.*

Proof. As R is generated by a conjugacy class of reflections (transvections) of $O(V,q)$, it has a derived group R' of index 2. Also, R is irreducible on V.

In characteristic 2, the theorem follows from Proposition 7.1 and Kantor [14, Theorem II]. (Kantor restricts attention to transvection groups over finite fields, but this immediately implies the results for any finite group generated by transvections; see [5, Theorem 3.4B].)

For now we will assume that the characteristic of F is not 2. For R imprimitive, the theorem holds by Proposition 7.1. In the case where R is primitive we may apply

the work of Wagner on primitive finite groups generated by reflections [26, Result, Table II, p. 520]. (Note that this table contains some misprints.) In addition to the conclusions of the theorem, Wagner's results include groups with derived group $SL_8(F_o)$ and $SU_8(F_o)$, for F_o a finite subfield of F. These groups contain transvections and therefore cannot be contained in any orthogonal groups of characteristic other than 2. □

Remark 7.3.

1. In the first two cases of the theorem, R' contains Siegel elements (long root elements) s. Such elements have $[V, s]$ totally singular, so these cases can only occur when C is split.

2. Wagner's results are elementary and self-contained. Kantor's proof makes use of several big classification theorems from the theory of finite groups. It is likely that in the special case used here (finite groups generated by orthogonal transvections in characteristic 2) can be given an elementary proof following the work of Wagner.

Lemma 7.4. *$R \not\geq O_8^-(F_o)$ and $R \not\geq {}^\delta\Omega_8^-(F_o)$ for any subfield $F_o \leq F$.*

Proof. By [6, Corollary 4], there exists a copy of S_3 in the outer automorphism group of R. But, by [23, Theorem 30], S_3 is not contained in the outer automorphism group of either $O_8^-(F_o)$ or ${}^\delta\Omega_8^-(F_o)$. Thus $R \not\geq O_8^-(F_o)$ and $R \not\geq {}^\delta\Omega_8^-(F_o)$. □

Lemma 7.5. *$R \not\geq S_9$, $R \not\geq S_{10}$, and $R \not\geq A^n : S_8$ for $n = 7$ or 8.*

Proof. Suppose $R \cong S_m$ for some $m \in \{9, 10\}$. Since S_m does not contain a normal subgroup of order two, by Lemma 5.3, R contains a subgroup, A_m, of index two that

is isomorphic to the rotation group of $G_{L/L\cap F1}$. Thus, by [6, Corollary 4], there exists a copy of S_3 in the outer automorphism group of A_m. But, by [11, Chapter II.5], $|Out(A_n)| = 2$ for all $n \neq 6$. Hence, $R \ncong S_9$ and $R \ncong S_{10}$.

Assume $R \cong A^n : S_8$ for $n = 7$ or 8. By Lemma 5.3, either R contains a subgroup, $A^n : A_8$, of index two that is isomorphic to the rotation group of $G_{L/L\cap F1}$ or $R/\{\pm I\}$ contains a subgroup, $H : A_8$, of index two that is isomorphic to the rotation group of $G_{L/L\cap F1}$. Since $G_1 = A^n : A_8$, and $G_2 = H : A_8$ have a normal subgroup, N_i, with $G_i/N_i \cong A_8$, by [6, Corollary 1] and [6, Corollary 4], there exists a copy of S_3 in the outer automorphism group of $G_i/N_i \cong A_8$. But, by [11, Chapter II.5], $|Out(A_8)| = 2$. Hence, $R \ncong A^n : S_8$.

□

Lemma 7.6. *If L is a maximal subloop of $B = \{x \in GLL(F) | q(x) \in G\}$ and $R(L)' = \Omega_8^+(F_o)$ then $SLL(F_o) \leq L \leq F^* \cdot GLL(F_o)$.*

Proof. By maximality of L, $L = F^* \cdot L \cap B$. Since $q(1) = 1$, a square, we have that $R(L) \in \{{}^+\Omega_8^+(F_o), O_8^+(F_o)\}$. Thus by 5.2, either $F^* \cdot L = GLL(F_o)$ or $F^* \cdot L = F^* \cdot \{v \in GLL(F_o) | q(v) \text{ is a square}\}$. Thus for any element $x \in SLL(F_o)$ there exist elements $a \in F^*$ and $y \in L$ such that $x = ay$. Hence, since $ay \in F^* \cdot L \cap B$, $x \in L$. Therefore $SLL(F_o) \leq L \leq F^* \cdot GLL(F_o)$. □

Therefore, by Theorem 7.2, if $R(L)$ is irreducible then either $R(L) \cong {}^+\Omega_8^+(F_o)$ for $F_o \leq F$, $R = O_8^+(F_o)$ for $F_o \leq F$, or $R(L) \cong 2O_8^+(2)$. Furthermore, by Lemma 5.2, if $L \leq GLL(F)$ then $L \cong L_1$ where either $SLL(F_o) \leq L_1 \leq F^* \cdot SLL(F_o)$ or

$2SLL(2) \leq L_1 \leq F^* \cdot 2SLL(2)$. This completes the proof of Theorem 1.4.

8 Proof of Theorem 1.5

In this section we will let C be a finite, and therefore split, octonion algebra over a field F. Also, we will let L be a maximal subloop of loop B where $SLL(F) \leq B \leq GLL(F)$.

Lemma 8.1. *$B = \{x \in GLL(F) | q(x) \in G\}$ for some multiplicative group $G \leq F^*$.*

Proof. Note that φ defined in the follow way:

$$\varphi : B \longrightarrow F^*$$

$$x \mapsto q(x)$$

is a group homomorphism from B to F^* with $ker(\varphi) = SLL(F)$. Thus

$$B = \bigcup_{k \in Im(\varphi)} x_k ker(\varphi) \text{ where } q(x_k) = k$$

$$= \{x \in GLL(F) | q(x) \in Im(\varphi)\}$$

□

Proof of Theorem 1.5. If L is a maximal subloop of $B = \{x \in GLL(F) | q(x) \in G\}$ that contains $SLL(F)$ then, by 8.1, $L = \{x \in GLL(F) | q(x) \in H\}$ for some subgroup $H \leq G$. Furthermore, by maximality of L, H is a maximal subgroup of G.

Suppose L is a maximal subloop of B that does not contain $SLL(F)$. If L does not span C then, by Theorem 1.3, L is contained in and therefore equal to

$(S^{\perp})^{*} \cap B$ for some hexagon line S. If L spans C and $R(L)$ is reducible then by Theorem 1.3, L is contained in and therefore equal to $(Q \cup Q^{\perp})^{*} \cap B$ for some quaternion subalgebra, Q, of C. If L spans C and $R(L)$ is irreducible on C then, by Theorem 1.4 and Lemma 7.6, $R(L)$ is one of the following:

1. ${}^{+}\Omega_8^{+}(F_o)$ for some proper subfield F_o of F;

2. $O_8^{+}(F_o)$ for some proper subfield F_o of F;

3. $2O_8^{+}(2)$ when $F = F_p$ for some odd prime p.

Thus, since $R(GLL(F_o)) = O_8^{+}(F_o)$, $R(2GLL(2)) = 2O_8^{+}(F_o)$, and the reflection group of $\{v \in GLL(F_o) | q(v)$ is a square$\}$ is ${}^{+}\Omega_8^{+}(F_o)$, by Lemma 5.2, if $R(L)$ is one of these groups then L is one of the following:

1. $L = (F^{*} \cdot GLL(F_o)) \cap B$ for some maximal subfield F_o of F;

2. $L = (F^{*} \cdot \{v \in GLL(F_o) | q(v)$ is a square$\}) \cap B$ for some maximal subfield, F_o, of F;

3. $L = (F^{*} \cdot 2GLL(2)) \cap B$ where $F = F_p$ for some odd prime p.

But, since $\{v \in GLL(F_o) | q(v)$ is a square $\} \leq GLL(F_o)$ and $(F^{*} \cdot GLL(F_o)) \cap B \lneq B$, L is one of the following:

1. $L = (F^{*} \cdot GLL(F_o)) \cap B$ for some maximal subfield F_o of F;

2. $L = (F^{*} \cdot 2GLL(2)) \cap B$ where $F = F_p$ for some odd prime p.

Therefore, if L is a maximal subloop of B then L is one of the following:

1. $L = \left(S^{\perp}\right)^{*} \cap B$ for some hexagon line S;

2. $L = \left(Q \cup Q^{\perp}\right)^{*} \cap B$ for some quaternion subalgebra Q;

3. $L = F^{*} \cdot GLL(F_o) \cap B$ for some maximal subfield F_o of F;

4. $L = \{x \in B | q(x) \in G\}$ for some maximal subgroup, G, of $\{q(x) | x \in B\}$;

5. $L = F^{*} \cdot 2GLL(2) \cap B$ where $F = F_p$ for some odd prime p.

Corollary 8.2. *If $B = SLL(F)$ then L is one of the following:*

1. $L = \left(S^{\perp}\right)^{*} \cap SLL(F) = SL_2(F) \bullet F^2$ *for some hexagon line S;*

2. $L = \left(Q \cup Q^{\perp}\right)^{*} \cap SLL(F) = H \cup xH$ *where* $H = Q^{*} \cong SL_2(F)$ *for some quaternion subalgebra Q;*

3. $L = F^{*} \cdot GLL(F_o) \cap SLL(F) =$

$$= \begin{cases} SLL(F_o) & \text{if } F \text{ is of characteristic two or } dim_{F_o} F \text{ is odd} \\ SLL(F_o)2 & \text{if } F \text{ is of odd characteristc} \end{cases}$$

for some maximal proper subfield F_o of F;

4. $L = F^{*} \cdot 2GLL(2) \cap SLL(F) = 2SLL(2)$ *where F is of odd characteristic.*

Proof. Parts (1) and (2) follow from Theorem 1.5.

If $L_1 = GLL(F_o) \leq GLL(F)$ then there is a group homomorphism $q : GLL(F) \longrightarrow F^{*}$ such that $q(L_1) = F_o^{*}$ and $q(kx) = k^2 q(x)$ for all $k \in F$. Let k be an element of F and x be in L_1 such that kx is in $SLL(F)$. So, since $k^2 q(x) = q(kx) = 1$, we have

that $k^2 = q(x)^{-1} \in F_o$.

Case 1. If F is of characteristic two then $k \in F_o$ and $F^* \cdot GLL(F_o) \cap SLL(F) = F_o^* \cdot GLL(F_o) \cap SLL(F) = SLL(F_o)$.

Case 2. If F is of odd characteristic then $k \in H \leq F^*$ where $F_o^* \leq H$ is of index two. Thus $F^* \cdot GLL(F_o) \cap SLL(F) = H \cdot GLL(F_o) \cap SLL(F_o) = 2SLL(F_o)$.

This concludes part (3).

Now suppose $L_1 = 2GLL(2) \leq GLL(F)$ where F is of odd characteristic. Since $L_1/\{\pm I\}$ is simple and $q : L/\{\pm I\} \longrightarrow F$ is a homomorphism, $ker(q|_{L_1/\{\pm I\}}) = L_1/\{\pm I\}$. Thus, if $k \in F$ and $x \in L_1$ such that $kx \in SLL(F)$ then $k^2 = k^2 q(x) = q(kx) = 1$. Hence, $F^* \cdot 2GLL(2) \cap SLL(F) = 2GLL(2) \cap SLL(F) = 2SLL(2)$. □

9 Lagrange's Theorem for Moufang Loops

Proof. Assume that the theorem is not true and let L be a Moufang loop of minimum order such that the Lagrange property does not hold. It was proven by Bruck [4, *p.* 92] that if H is a normal subloop of L such that the Lagrange property holds for both H and L/H then Lagrange's property also holds for L. Thus, by minimality of L, L does not have any normal subloops. Since Lagrange's Theorem is true for all finite groups, L has to be a finite nonassociative simple Moufang loop. Liebeck [17] classified such loops as Paige loops, $P(q) = PSLL(q)$. By minimality of $L = P(q)$, there exists a maximal subloop $M \leq L = P(q)$ such that $|M|$ does not divide $|L|$. By Corollary 8.2, there are five possibilities for M.

Case 1. For $M \cong PSL_2(q) \bullet F_q^2$,

$$|M| = \frac{q^3(q^2-1)}{gcd(q+1,2)} \mid \frac{q^3(q^4-1)}{gcd(q+1,2)} = |P(q)|$$

Case 2. For $M = H \cup xH$ where $H \cong PSL_2(q)$, $x \in H^{\perp}$, and $q(x) = 1$,

$$|M| = \frac{2q(q^2-1)}{gcd(q+1,2)} \mid \frac{q^3(q^4-1)}{gcd(q+1,2)} = |P(q)|$$

Case 3. For $M = SLL(q_o)/\{\pm I\}$ where $F_{q_o} \leq F$,

$$|M| = \frac{q_o^3(q_o^4-1)}{gcd(q+1,2)} \mid \frac{q^3(q^4-1)}{gcd(q+1,2)} = |P(q)|$$

Case 4. For $M = 2SLL(q_o)/\{\pm I\}$ where $F_{q_o} \leq F$ and is of odd characteristic,

$$|M| = \frac{2q_o^3(q_o^4-1)}{2} \mid \frac{q^3(q^4-1)}{gcd(q+1,2)} = |P(q)|$$

Case 5. For $M = 2SLL(2)/\{\pm I\}$ where F is of odd characteristic,

$$|M| = \frac{2 \cdot 120}{2} \mid \frac{q^3(q^4-1)}{gcd(q+1,2)} = |P(q)|$$

Hence, by contradiction, there does not exist a Moufang loop of minimal order such that the Lagrange property fails. □

References

[1] M. Aschbacher, On finite groups generated by odd transpositions. I, II, III, IV, Math Z., **127** (1972), 45-56 and J. Algebra **26** (1973), 451-491

[2] M. Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math. **76** (1984), 469-514

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

[4] R.H. Bruck, "A Survey of Binary Systems", Springer-Verlag New York (1971).

[5] J.D. Dixon, "The structure of linear groups," Van Nostrand Reinhold Co., London, (1971)

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

[7] B. Fischer, Finite groups generated by 3-transpositions, Invent. Math. **13** (1971), 232-246

[8] S.M. Gagola III and J.I. Hall, Lagrange's theorem for Moufang loops, Acta Sci. Math. (Szeged), to appear.

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

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

[11] B. Huppert "Endliche Gruppen," Berlin, Heidelberg, New York, Springer, (1967)

[12] A. Hurwitz, Über die Komposition der quadratischen Formen von beliebig vielen Variabeln, Nachr. Ges. Wiss. Göttingen, (1898) 309-316

[13] N. Jacobson, "Basic Algebra", San Francisco, W. H. Freeman, (1974)

[14] W.M. Kantor, Subgroups of classical groups generated by long root elements, Trans. Amer. Math. Soc. **248** (1979), 347-379

[15] E. Kleinfeld, Generalization of alternative rings, J. Algebra, **18** (1971), 304-325

[16] P. 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

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

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

[19] R. Moufang, Zur Struktur von Alternativ Körpern, Math. Ann., **110** (1935), 416-430

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

[21] G.L. Schellekens, On a hexagonic structure. I, II, Koninkluke Nederlandse Akademie Van Wetenschappen, **65** (1962), 201-234

[22] F. Veldkamp and T. A. Springer, Octonions, Jordan Algebras and Exceptional Groups, Springer Monographs in Mathematics (Springer- Verlag), (2000)

[23] R. Steinberg, "Lectures on Chevalley groups," Notes prepared by John Faulkner and Robert Wilson, Yale University, New Haven, Conn., (1968)

[24] M. Suzuki,"Group theory I," Translated from the Japanese by the author. Grundlehren der Mathematischen Wissenschaften, **247,** Springer-Verlag, Berlin-New York, (1982)

[25] D. Taylor, "The geometry of the classical groups," Sigma Series in Pure Mathematics, 9. Heldermann Verlag, Berlin, (1992)

[26] A. Wagner, Determination of the finite primitive reflection groups over an arbitrary field of characteristic not two. I, II, III, Geometriae Dedicata, **9** (1980), no. 2, 239-253 and **10** (1981), no. 1-4, 191-203, 475-523

[27] A. Zavarnitsine, Maximal subloops of finite simple Moufang loops, to appear.