Quasigroups and Related Systems **15** (2007), 19 – 46

Central automorphisms of Latin square designs and loops

Jonathan I. Hall

Abstract

We discuss special automorphisms of Latin square designs or equivalently the 3-nets that are dual to them. We focus on the relationships between these automorphisms and the algebraic properties of the associated loops, especially Moufang loops.

1. Introduction

Let O be a set and consider a relation $\mathcal{R} \subset O^3$ with the property that projection onto any pair of coordinates gives a copy of O^2. That is, for every pair a and b of (not necessarily distinct) members of O there are unique triples $(a, b, *)$, $(a, *, b)$, and $(*, a, b)$ in $\mathcal{R}$.

Such relations $\mathcal{R}$ are equivalent to Latin squares, to quasigroups, to 3-nets, and to Latin square designs. Let R, C, E be a fixed permutation of the index set $\{1, 2, 3\}$. We construct a Latin square L from $\mathcal{R}$ by, for each triple $t = (t_1, t_2, t_3) \in \mathcal{R}$, letting t_E be the entry in row t_R and column t_C. The associated quasigroup $Q = (O, \circ)$ then has L as its Cayley (multiplication) table: if $a = t_R$, $b = t_C$, and $c = t_E$, then $a \circ b = c$. Each Latin square and quasigroup occurs naturally as one of six different conjugates, coming from a fixed $\mathcal{R}$ and one of the six permutations of R, C, E.

A *partial linear space* $(\mathcal{P}, \mathcal{L})$ is a set of points $\mathcal{P}$ and a set of lines $\mathcal{L}$ together with an incidence relation $\sim$ satisfying:

> There do not exist distinct points a, b and distinct lines k, l with $a \sim k \sim b \sim l \sim a$.

2000 Mathematics Subject Classification: 20N05.
Keywords:Latin square design, 3-net, Bol loop, Moufang loop, inverse property.
Partial support provided by the National Science Foundation, USA

The axiom is selfdual in the sense that $(\mathcal{P}, \mathcal{L})$ is a partial linear space if and only if $(\mathcal{L}, \mathcal{P})$ is. In almost all examples of interest to us we will have the further (selfdual) nondegeneracy axiom:

> Every point is incident to at least two lines, and every line is incident to at least two points.

In this case, we may identify each line with the subset of points incident to it.

The *Latin square design* associated with the relation $\mathcal{R}$ is the partial linear space with point set $\mathcal{P} = O_1 \cup O_2 \cup O_3$ (of size $3|O|$) and line set $\mathcal{L}$ (of size $|O|^2$) given by

$$\{a_1, b_2, c_3\} \in \mathcal{L} \iff (a, b, c) \in \mathcal{R}\,.$$

Every line contains exactly three points, and x_i is collinear with y_j if and only if $i \neq j$. The noncollinearity relation on $\mathcal{P}$ is an equivalence relation whose classes O_i are the *fibers* of the Latin square design. The cardinality $|O|$ of each fiber is the *order* of the Latin square design (and Latin square and quasigroup). A Latin square design is degenerate precisely when it has order $|O| = 1$, and even in that case we may identify the unique line with its set of three incident points.

The dual of a Latin square design is a 3-*net* (sometimes 3-*web*). The line set of the 3-net is naturally partitioned into the three parallel classes of lines O_i.

In this survey we are particularly interested in automorphisms of Latin square designs (or equivalently the 3-nets dual to them) and the relationships between certain geometrically defined automorphisms and the algebraic properties of the associated quasigroups and loops.

Much of what we present here is not new. Indeed such relationships have been studied for nearly one hundred years. The equivalence of algebraic identities to the existence of various geometric automorphisms and closure of configurations goes back to Veblen and Young [33] (who considered automorphisms of projective planes and their relationship to Desargues' configurations) and to Reidermeister [29], Thomsen [31], Bol [2], and their collaborators who, in a remarkable series of papers entitled "Topologische Fragen der Differentialgeometrie," worked on 3-nets (3-webs) of parallel classes of lines in the projective plane. Tits [32] studied automorphisms of nets and their connection to groups with triality specifically in the context of the octonions and Cartan's triality groups. Glauberman [12] and Doro

[8] later defined and studied abstract groups with triality and the loops that can be used to coordinatize them. The geometric study has been revived more recently, particularly in the paper of Funk and P. Nagy [9], which describes in detail the relationships between Bol reflections on a 3-net and coordinatizing Bol loops. The approach we take here is closer to that of Hall and G.P. Nagy [16] and G.P. Nagy and Vojtěchovský [24], which discusses the case of simple Moufang loops extensively.

Since the early work in this area dealt with the study of line sets in Euclidean planes, it was naturally phrased in terms of 3-nets. We prefer the equivalent but dual world of Latin square designs and will largely stay there.

Our general reference for combinatorics is M. Hall, Jr. [17], for group theory Aschbacher [1], and for general loop theory Bruck [3] and Pflugfelder [26]. For the octonions, see [30].

2. Automorphisms of Latin square designs

Let $\mathbb{D} = (\mathcal{P}, \mathcal{L})$ be a Latin square design of order n with fibers O_R, O_C, and O_E. The group $\mathrm{Aut}(\mathbb{D})$ is the automorphism group of $\mathbb{D}$, the set of all permutations σ of $\mathcal{P} = O_R \cup O_C \cup O_E$ that take lines to lines:

$$\{a, b, c\} \in \mathcal{L} \iff \{a^\sigma, b^\sigma, c^\sigma\} \in \mathcal{L}\,.$$

Any automorphism of $\mathbb{D}$ must preserve the noncollinearity equivalence relation whose equivalence classes are O_R, O_C and O_E. The automorphism group of this equivalence relation is the wreath product $Sym(O) \wr Sym(3)$ consisting of the normal *base subgroup* $Sym(O_R) \times Sym(O_C) \times Sym(O_E)$ extended by the symmetric group of degree 3, $Sym(\{R, C, E\}) \simeq Sym(3)$. The *base subgroup* $\mathrm{BAut}(\mathbb{D})$ of $\mathrm{Aut}(\mathbb{D})$ is its intersection with the base subgroup of the wreath product. (See Section 4.1 below for further discussion of full wreath products.)

A *subdesign* $\mathbb{D}_0 = (\mathcal{P}_0, \mathcal{L}_0)$ is given by a subset $\mathcal{P}_0$ of $\mathcal{P}$ with the property that, for $l \in \mathcal{L}$, we have $l \in \mathcal{L}_0$ and $l \subseteq \mathcal{P}_0$ if and only if $|l \cap P_0| \geqslant 2$. A subdesign is a Latin square design in its own right, although we must allow for degenerate examples with one line or no lines (which happens when $\mathcal{P}_0$ is contained in a single fiber). The subset $\mathcal{P}_0$ determines $\mathbb{D}_0$ completely, so we often (with mild abuse) identify a subdesign with its set of points.

Lemma 2.1. *If A is a subset of* $\mathrm{Aut}(\mathbb{D})$*, then the set of common fixed points of A in $\mathbb{D}$ is a subdesign of $\mathbb{D}$. In particular, the subgroup of* $\mathrm{Aut}(\mathbb{D})$ *that*

fixes a fiber pointwise is semiregular on the remaining points. (*That is, only the identity fixes additional points.*)

Proof. If an automorphism fixes two points of a line, then it fixes the line and so the third point of the line. Therefore the fixed points of A form a subdesign. The smallest subdesign of $\mathbb{D}$ containing a fiber and at least one point not in that fiber is $\mathbb{D}$ itself. □

A *shear* of $\mathbb{D}$ is an automorphism that fixes one fiber pointwise and fixes the other fibers globally (that is, belongs to the base subgroup of $\mathrm{Aut}(\mathbb{D})$). By the lemma, the group of all shears with fixed fiber Q is semiregular on each of the other fibers. A basic result of the sort we are interested in here is the following, due to Praeger [28]. (See [7] for another proof.)

Theorem 2.2. *Let $\mathbb{D}$ be a Latin square design, and let Q be a fiber. Then the group S of all shears with fixed fiber Q is regular on some other fiber if and only if $\mathbb{D}$ is the Latin square design associated with the Cayley table of the group S.* □

We now come to one of the fundamental concepts of this paper. A *central automorphism* τ_a of the Latin square design $\mathbb{D}$ with *center* $a \in \mathcal{P}$ is a nontrivial automorphism of $\mathbb{D}$ that fixes the point a and all lines through it. Therefore, if τ_a exists then, for all $\{a, b, c\} \in \mathcal{L}$, we have

$$a^{\tau_a} = a, \quad b^{\tau_a} = c, \quad c^{\tau_a} = b\,.$$

In particular τ_a switches the two fibers that complement the fiber F containing a. Since every line of $\mathcal{L}$ contains two points of this complement, the permutation induced on the line set $\mathcal{L}$ by τ_a is uniquely determined. The question is whether or not the action of τ_a can be defined on the remaining points of the fiber F to be consistent with this action on the lines.

In the dual world of 3-nets, a central automorphism is usually called a *Bol reflection* [9]. There the action of a putative Bol reflection on the points of the 3-net (that is, the lines of $\mathbb{D}$) is evident, and the question is whether or not this induces a permutation of the lines of the 3-net (the points of $\mathbb{D}$).

Proposition 2.3. *In* $\mathrm{Aut}(\mathbb{D})$ *there is at most one central automorphism τ_a with center a for each $a \in \mathcal{P}$. If τ_a exists in* $\mathrm{Aut}(\mathbb{D})$*, then it has order* 2 *and is central in the stabilizer of a in* $\mathrm{Aut}(\mathbb{D})$*, and $\tau_a^g = \tau_{a^g}$ for all $g \in \mathrm{Aut}(\mathbb{D})$.*

If τ_a and τ_b exist in $\mathrm{Aut}(\mathbb{D})$ *with a and b in different fibers, then $\tau_a\tau_b$ has order* 3 *and $\langle \tau_a, \tau_b \rangle$ is isomorphic to $Sym(3)$. If this is the case, then*

there is a unique conjugacy class T of central automorphisms in $\mathrm{Aut}(\mathbb{D})$*, and the centers of the members of T form a subdesign of $\mathbb{D}$.*

Proof. If t_1 and t_2 are two central automorphisms of $\mathbb{D}$ with center a, then the automorphism t_1t_2 of $\mathbb{D}$ is trivial on both fibers off a and so is the identity by Lemma 2.1. Therefore if there is a central automorphism with center a, then it is unique and has order 2.

For $g \in \mathrm{Aut}(\mathbb{D})$, the conjugate τ_a^g is clearly a central automorphism of $\mathbb{D}$ with center a^g. Therefore by uniqueness $\tau_a^g = \tau_{a^g}$ and, especially, τ_a is in the center of the stabilizer of a in $\mathrm{Aut}(\mathbb{D})$.

In particular if $\{a, b, c\} \in \mathcal{L}$, then

$$\tau_b\tau_a\tau_b = \tau_a^{\tau_b} = \tau_c = \tau_b^{\tau_a} = \tau_a\tau_b\tau_a$$

and therefore

$$(\tau_a\tau_b)^3 = (\tau_a\tau_b\tau_a)(\tau_b\tau_a\tau_b) = \tau_c^2 = 1\,.$$

If τ_x and τ_y are two central automorphisms of $\mathbb{D}$, then either they are in different fibers and so conjugate in $\langle \tau_x, \tau_y\rangle \simeq Sym(3)$, or they are in the same fiber and so both conjugate to τ_z where $z \in \{a, b\}$ is not in the fiber of x and y.

If l is a line of $\mathcal{L}$ with $l \cap \{p \,|\, \tau_p \in T\} \supset \{x, y\}$, say, then $\tau_z = \tau_x^{\tau_y} \in T$, where $l = \{x, y, z\}$. □

The stength of the proposition can be seen in

Corollary 2.4. *Suppose that a, b, c are from different fibers of $\mathbb{D}$ and that $\tau_a, \tau_b, \tau_c \in \mathrm{Aut}(\mathbb{D})$. Then $\langle \tau_a, \tau_b, \tau_c\rangle$ is a quotient of $(\mathbb{Z} \times \mathbb{Z}) : Sym(3)$.*

Proof. $(\mathbb{Z} \times \mathbb{Z}) : Sym(3)$ is the Weyl group of affine type $\tilde{A}_2$ with presentation $\langle x, y, z \,|\, 1 = x^2 = y^2 = z^2 = (xy)^3 = (xz)^3 = (yz)^3\rangle$. (This has a direct proof. The subgroup $N = \langle xyzy, yxzx, zxyx\rangle = \langle xyzy, yxzx\rangle$ is easily seen to be normal and abelian, and the whole group is N extended by $\langle x, y\rangle$ which is isomorphic to $Sym(3)$.) □

The proposition shows that there is a unique maximal subdesign $\mathbb{D}_0$ of $\mathbb{D}$ with the property that every central automorphism of $\mathbb{D}_0$ exists and extends to a central automorphism of $\mathbb{D}$. It is also true that (in a sense which will be made precise at the end of Section 4.2 below) there is a unique maximal quotient design of $\mathbb{D}$ that admits all possible central automorphisms.

3. Central automorphisms and loops

Let $\mathbb{D} = (\mathcal{P}, \mathcal{L})$ be a Latin square design with fibers O_R, O_C, and O_E for the underlying set O. Any permutation (α, β, γ) from the base group $Sym(O_R) \times Sym(O_C) \times Sym(O_E)$ acts on $\mathcal{P} = O_R \cup O_C \cup O_E$, producing a Latin square design isomorphic to $\mathbb{D}$. At the level of Latin squares, this corresponds to passing to an *equivalent* Latin square by permuting rows, permuting columns, and permuting the entry labels. In the quasigroup context, we are speaking of an *isotopic* quasigroup $(O, \diamond)$ given by

$$x \circ y = z \iff x^\alpha \diamond y^\beta = z^\gamma; \quad \text{that is,} \quad p \diamond q = (p^{\alpha^{-1}} \circ q^{\beta^{-1}})^\gamma .$$

It is well-known and easy to see that every Latin square on the set $O = \{1, 2, \ldots, n\}$ is equivalent to one whose first row and first column are $1, 2, \ldots, n$ in order. That is, every quasigroup is isotopic to a *loop*, a quasigroup with a two-sided identity element 1. In particular, in the equation $xy = 1$, the element x determines its right inverse y uniquely and y determines its left inverse x uniquely. We write $x^{-1} = y$ and ${}^{-1}y = x$.

For the loop $L = (L, \cdot)$ (with mild abuse) we let $\mathbb{D}(L) = \mathbb{D}$ be the Latin square design with point set $\mathcal{P} = L_R \cup L_C \cup L_E$ and line set $\mathcal{L}$ given by the Cayley table of L:

$$\{a_R, b_C, c_E\} \in \mathcal{L} \iff a \cdot b = c .$$

The basic question we approach here is: how is the existence of central automorphisms of $\mathbb{D}(L)$ reflected in the algebraic properties of the loop L?

To simplify our notation, for each $a \in L$ we will write ρ_a in place of τ_{a_R}; κ_a in place of τ_{a_C}; and ϵ_a in place of τ_{a_E}. (This notation indicates that the central automorphism has center corresponding to, respectively, a row, column, or entry of the associated Latin square.)

3.1. Inverse property loops

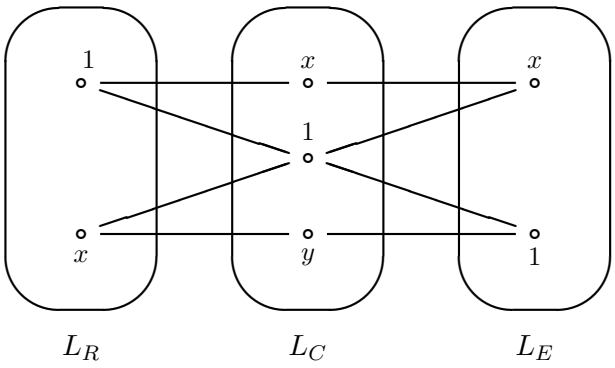
Lemma 3.1.

(a) $\kappa_1 \in \mathrm{Aut}(\mathbb{D}(L))$ *if and only if* L *has the right inverse property* $(xy)({}^{-1}y) = x$ *for all* $x, y \in L$. *In this case inverses are two-sided (that is,* ${}^{-1}x = x^{-1}$ *and* $(x^{-1})^{-1} = x$ *always) and* $x_C^{\kappa_1} = x_C^{-1}$.

(b) $\rho_1 \in \mathrm{Aut}(\mathbb{D}(L))$ *if and only if* L *has the left inverse property* $x^{-1}(xy) = y$ *for all* $x, y \in L$. *In this case inverses are two-sided and* $x_R^{\rho_1} = x_R^{-1}$.

(c) $\epsilon_1 \in \mathrm{Aut}(\mathbb{D}(L))$ *if and only if* L *has the anti-automorphic inverse property* $(xy)^{-1} = y^{-1}x^{-1}$ *for all* $x, y \in L$. *In this case inverses are two-sided and* $x_E^{\epsilon_1} = x_E^{-1}$.

Proof. We prove part (a) in detail, the other two parts being similar. (Indeed they are equivalent to (a) in conjugates of the loop L.) Pictures of the following type are helpful.



Suppose we have $xy = 1$ in L. We then have

$$1 \cdot x = x\,, \quad x \cdot 1 = x\,, \quad \text{and} \quad x \cdot y = 1\,,$$

giving in $\mathbb{D}(L)$ the three lines $\{1_R, x_C, x_E\}$, $\{x_R, 1_C, x_E\}$, and $\{x_R, y_C, 1_E\}$, which are drawn in the picture along with the line $\{1_R, 1_C, 1_E\}$.

Assume that κ_1 is an automorphism of $\mathbb{D}(L)$. Then $1_C^{\kappa_1} = 1_C$ and the lines $\{1_R, 1_C, 1_E\}$ and $\{x_R, 1_C, x_E\}$ through 1_C are mapped to themselves via

$$1_R^{\kappa_1} = 1_E\,, \quad 1_E^{\kappa_1} = 1_R\,, \quad x_R^{\kappa_1} = x_E\,, \quad x_E^{\kappa_1} = x_R\,.$$

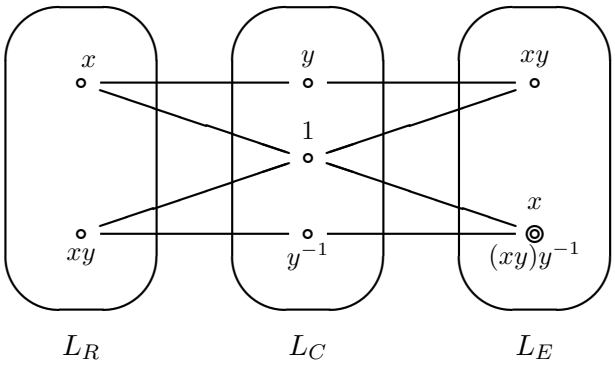
Therefore

$$\{1_R, x_C, x_E\}^{\kappa_1} = \{1_R^{\kappa_1}, x_C^{\kappa_1}, x_E^{\kappa_1}\} = \{1_E, x_C^{\kappa_1}, x_R\} = \{x_R, y_C, 1_E\}\,,$$

since a line of $\mathbb{D}$ is uniquely determined by any two of its points. In particular $x_C^{\kappa_1} = y_C$ and also $y_C^{\kappa_1} = x_C$ (as κ_1 has order 2). The first equality says that (in the fiber L_C) every element of L is moved by κ_1 to its right inverse, but the second equality says that every element is moved by κ_1 to its left inverse. Therefore right inverses are always equal to left inverses. That is,

each x has a two-sided inverse ${}^{-1}x = x^{-1}$, $(x^{-1})^{-1} = x$, and $x_C^{\kappa_1} = x_C^{-1}$, as claimed.

Next consider, for arbitrary $x, y \in \mathcal{P}$:



The lines here come from the equations

$$x \cdot y = xy\,, \quad xy \cdot 1 = xy\,, \quad x \cdot 1 = x\,, \quad (xy) \cdot y^{-1} = (xy)y^{-1}\,.$$

The image of the line $\{x_R, y_C, xy_E\}$ under κ_1 is the line

$$\{x_R^{\kappa_1}, y_C^{\kappa_1}, xy_E^{\kappa_1}\} = \{x_E, y_C^{-1}, xy_R\} = \{xy_R, y_C^{-1}, x_E\}\,.$$

As $\{xy_R, y_C^{-1}, (xy)y_E^{-1}\}$ is clearly a line of $\mathcal{L}$, we conclude that $x = (xy)y^{-1}$, proving the right inverse property.[1]

Now assume that L has the right inverse property. Thus $({}^{-1}yy)({}^{-1}y) = {}^{-1}y$, hence (by cancellation) inverses are two-sided. The line $\{x_R, y_C, xy_E\}$ is generic in $\mathcal{L}$, and the picture above shows that its image under κ_1 is also a line (with the image of y_C under κ_1 defined to be y_C^{-1}). Therefore this κ_1 is a central automorphism of $\mathbb{D}(L)$. □

If ρ_1, κ_1, and ϵ_1 are all automorphisms of $\mathbb{D}(L)$, then L is called an *inverse property loop*. Since the group $\langle \rho_1, \kappa_1, \epsilon_1 \rangle$ is a copy of $Sym(3)$ (by Proposition 2.3 or direct calculation) and so is generated by any two of the three central automorphisms in it, we have the immediate

[1] This argument illustrates how Reidermeister [29], Thomsen [31], Bol [2], and others were able to relate the closure of certain geometric configurations to identities satisfied by coordinatizing binary systems.

Corollary 3.2. *If the loop L has any two of the right inverse property, the left inverse property, and the anti-automorphic inverse property, then it is an inverse property loop and has all three properties.* □

3.2. Bol loops

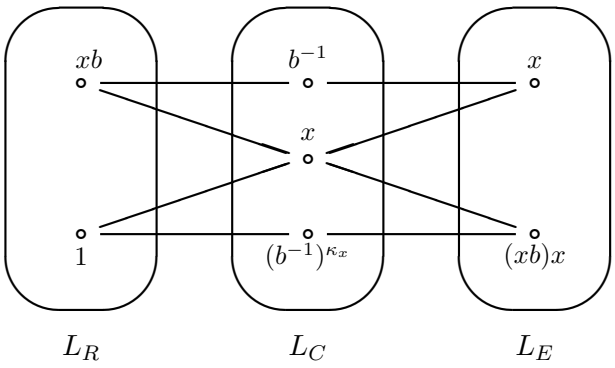
Proposition 3.3. *Let L be a loop with $\kappa_1 \in \mathrm{Aut}(\mathbb{D}(L))$. Then, for the element x of L, we have $\kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ if and only if we have*

$$a((xb)x) = ((ax)b)x$$

for all a, b in L. In this case $y^{\kappa_x} = (xy^{-1})x$ for all y in L.

Proof. As $\kappa_1 \in \mathrm{Aut}(\mathbb{D}(L))$ by hypothesis, L has the right inverse property by Lemma 3.1. In particular, inverses are two-sided.

Assume κ_x is an automorphism and consider

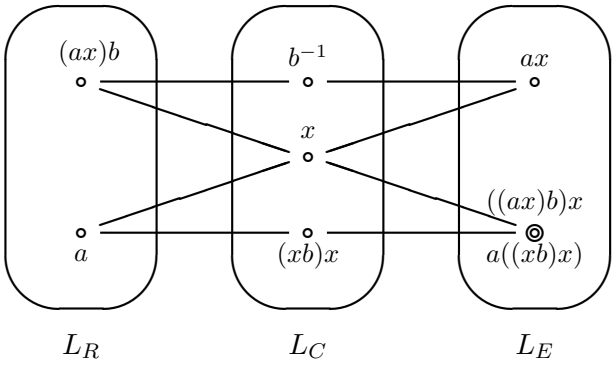


As L has the right inverse property, in picture the top line

$$\{xb_R, b_C^{-1}, (xb)b_E^{-1}\} = \{xb_R, b_C^{-1}, x_E\}$$

is indeed in $\mathcal{L}$. The image of this line under the automorphism κ_x is then the line $\{1_R, (b^{-1})_C^{\kappa_x}, (xb)x_E\}$. Therefore $(b^{-1})^{\kappa_x} = (xb)x$; and so $y^{\kappa_x} = (xy^{-1})x$, for all $y \in L$, as claimed.

The above picture is the $a = 1$ case of

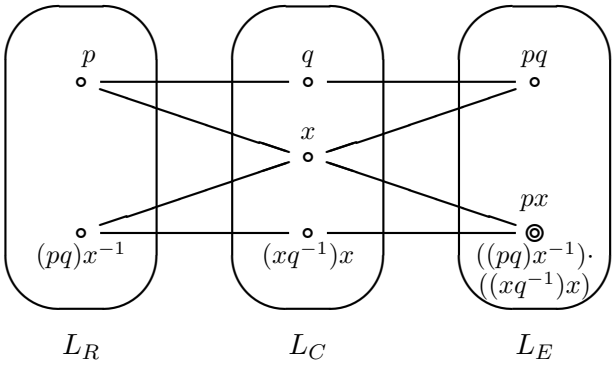


where again the top line is valid because of the right inverse property. We conclude that, for all $a, b \in L$,

$$a((xb)x) = ((ax)b)x$$

as desired.

Conversely assume that in the right inverse property loop L we have $a((xb)x) = ((ax)b)x$, for a fixed x and all a, b. Let $\{p_R, q_C, pq_E\}$ be an arbitrary line of $\mathbb{D}(L)$. Consider



We use the given property and the right inverse property (twice) to calculate

$$((pq)x^{-1})((xq^{-1})x) = (((pq)x^{-1})x)q^{-1})x = ((pq)q^{-1})x = px\,.$$

This shows that, with the image of q_C under κ_x defined to be $(xq^{-1})x$, the image of $\{p_R, q_C, pq_E\}$ is indeed a line. Therefore κ_x is a central automorphism of $\mathbb{D}(L)$ with center x_C, as desired. □

The identity

$$a((xb)x) = ((ax)b)x$$

is called the *right Bol identity*, and a loop in which this holds for all a, b, x is a *right Bol loop*.

Theorem 3.4. *Let L be a loop. Then L is a right Bol loop if and only if $\kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all x of L.*

Proof. Setting $b = {}^{-1}x$ in $a((xb)x) = ((ax)b)x$, we learn that a right Bol loop has the right inverse property. Therefore the theorem is an immediate consequence of Proposition 3.3. □

As already mentioned, trading L for an isotopic loop corresponds to replacing $\mathbb{D}(L)$ with an isomorphic Latin square design. Since this clearly does not affect the existence of central automorphisms, we have immediately the well-known

Theorem 3.5.

(*a*) *All loop isotopes of a right Bol loop are right Bol loops* [26, IV.6.15].

(*b*) *The loop L is a right Bol loop if and only if all its loop isotopes are right inverse property loops* [26, II.3.9]. □

Corresponding to the right Bol identity we have the *left Bol identity*

$$(x(ax))b = x(a(xb))\,.$$

A loop in which the left Bol identity holds for all a, b, x is a *left Bol loop*. The corresponding versions of the previous three results remain true (by passing to the opposite loop given by $x \diamond y = y \cdot x$).

Proposition 3.6. *Let L be a loop with $\rho_1 \in \mathrm{Aut}(\mathbb{D}(L))$. Then, for the element x of L, we have $\rho_x \in \mathrm{Aut}(\mathbb{D}(L))$ if and only if we have*

$$(x(ax))b = x(a(xb))$$

for all a, b in L. In this case $y^{\rho_x} = x(y^{-1}x)$ for all y in L. □

Theorem 3.7. *Let L be a loop. Then L is a left Bol loop if and only if $\rho_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all x of L.* □

Theorem 3.8.

(*a*) *All loop isotopes of a left Bol loop are left Bol loops.*

(*b*) *The loop L is a left Bol loop if and only if all its loop isotopes are left inverse property loops* [26, II.3.8]. □

Many of the properties of Bol loops can be easily derived in this context. For x in the loop L, define powers of x recursively by

$$x^0 = 1, \quad x^n = (x^{n-1})x, \text{ and } x^{-n} = (x^{-1})^n \text{ for } n \in \mathbb{Z}^+ .$$

The *order* of x, written $|x|$, is the smallest positive integer n (if any) with $x^n = 1$. Otherwise x has infinite order.

Lemma 3.9. *Let L be a loop with $\kappa_1, \kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some x of L.*

(*a*) *For arbitrary $a \in L$ and integers i, j, we have $(ax^i)(x^j) = ax^{i+j}$. In particular $x^{i+j} = x^i x^j$ and $(x^i)^{-1} = (x^{-1})^i$.*

(*b*) *$\kappa_{x^n} \in \mathrm{Aut}(\mathbb{D}(L))$ and $(\kappa_x\kappa_1)^n = \kappa_{x^n}\kappa_1$. In particular $|x| = |\kappa_x\kappa_1|$.*

Proof. (*a*) We show that (*a*) follows from (*b*) (indeed from (*b*) with $n \in \{i, j, i+j\}$). For arbitrary z with $\kappa_z \in \mathrm{Aut}(\mathbb{D}(L))$ and arbitrary $a \in L$, we have

$$a_R^{\kappa_z\kappa_1} = az_E^{\kappa_1} = az_R .$$

Therefore

$$ax_R^{i+j} = a_R^{\kappa_{x^{i+j}}\kappa_1} = a_R^{(\kappa_x\kappa_1)^{i+j}} = a_R^{(\kappa_x\kappa_1)^i(\kappa_x\kappa_1)^j} = a_R^{(\kappa_{x^i}\kappa_1)(\kappa_{x^j}\kappa_1)} = (ax^i)x_R^j ,$$

as claimed.

(*b*) For $\kappa_z \in \mathrm{Aut}(\mathbb{D}(L))$ and arbitrary $y \in L$ we have $y_C^{\kappa_z} = (zy^{-1})z_C$ by Proposition 3.3. Therefore if $\kappa_y \in \mathrm{Aut}(\mathbb{D}(L))$ then by Proposition 2.3 $\kappa_z\kappa_y\kappa_z = \kappa_{(zy^{-1})z}$. In particular $\kappa_1\kappa_y\kappa_1 = \kappa_{y^{-1}}$ and $(\kappa_y\kappa_1)^{-1} = \kappa_1\kappa_y = \kappa_{y^{-1}}\kappa_1$, so (*b*) for negative n follows from (*b*) for positive $-n$.

We prove $\kappa_{x^n} \in \mathrm{Aut}(\mathbb{D}(L))$ and $(\kappa_x\kappa_1)^n = \kappa_{x^n}\kappa_1$ for nonnegative n by induction, the result being clear for $n = 0, 1$. Let $n \geqslant 1$ and assume the result for $0 \leqslant k \leqslant n$. Using the previous paragraph, induction, and (*a*) with $\{i, j\} = \{1, n-1\}$, we find

$$\begin{aligned}
\kappa_{x^{n+1}}\kappa_1 &= \kappa_{x^n x}\kappa_1 \\
&= \kappa_{(xx^{n-1})x}\kappa_1 \\
&= \kappa_x\kappa_{(x^{n-1})^{-1}}\kappa_x\kappa_1 \\
&= \kappa_x\kappa_1\kappa_{x^{n-1}}\kappa_1\kappa_x\kappa_1 \\
&= \kappa_x\kappa_1(\kappa_x\kappa_1)^{n-1}\kappa_x\kappa_1 \\
&= (\kappa_x\kappa_1)^{n+1} ,
\end{aligned}$$

as desired. As κ_x and κ_1 are in $\mathrm{Aut}(\mathbb{D}(L))$, so is $\kappa_{x^{n+1}} = (\kappa_x\kappa_1)^{n+1}\kappa_1$. □

Corollary 3.10. [26, IV.6.6] *Right Bol loops are power associative.* □

Of course, the same result is true for left Bol loops as well.

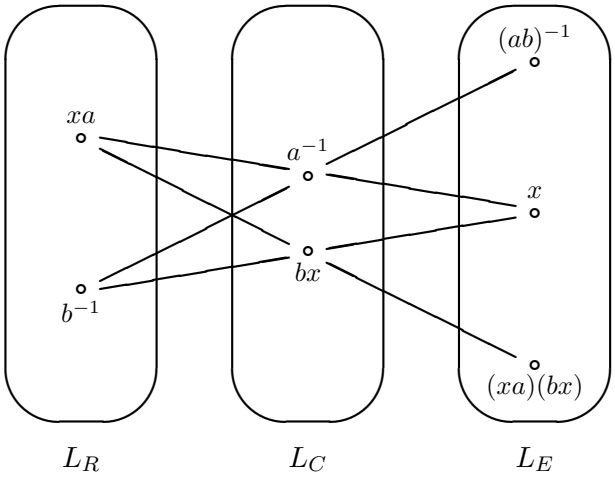
For loops admitting ϵ_1 and ϵ_x there does not seem to be a nice counterpart to the Bol identities. The following more specialized result is important in the next section.

Proposition 3.11. *Let L be an inverse property loop. Then, for the element x of L, we have $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ if and only if we have*

$$(xa)(bx) = (x(ab))x$$

for all a, b in L. In this case $(xy)x = x(yx)$ and $y^{\epsilon_x} = x(y^{-1}x)$, for all y in L.

Proof. Consider the picture



Here we have the line $\{xa_R, a_C^{-1}, x_E\}$ because of the right inverse property, line $\{b_R^{-1}, bx_C, x_E\}$ because of the left inverse property, and $\{b_R^{-1}, a_C^{-1}, (ab)_E^{-1}\}$ because of the anti-automorphic inverse property.

Suppose ϵ_x is an automorphism of $\mathbb{D}(L)$. Setting $b = 1$ we find $(a_E^{-1})^{\epsilon_x} = (xa)x_E$, and setting $a = 1$ we find $(b_E^{-1})^{\epsilon_x} = x(bx)_E$. Therefore ϵ_x can only be an automorphism if $y_E^{\epsilon_x} = x(y^{-1}x)_E$ and $(xy)x = x(yx)$ for all y in L.

As $\{b_R^{-1}, a_C^{-1}, (ab)_E^{-1}\}$ is certainly a generic line of $\mathbb{D}(L)$, we see that ϵ_x (extended to L_E as in the previous paragraph) is an automorphism of $\mathbb{D}(L)$

if and only if $(xa)(bx)$ is equal to $((ab)^{-1})^{\epsilon_x}$ for all a, b. That is, if and only if

$$(xa)(bx) = (x((ab)^{-1})^{-1})x = (x(ab))x$$

for all a, b. □

3.3. Moufang loops

We begin with a result that could well have been in the previous section.

Theorem 3.12. *For the loop L, the following are equivalent:*

(1) *for each of its points p, the Latin square design $\mathbb{D}(L)$ admits a central automorphism with center p;*
(2) *$\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all $x \in L$ and L has the right inverse property;*
(3) *$\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all $x \in L$ and L has the left inverse property;*
(4) *L is an inverse property loop with $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all $x \in L$;*
(5) *L is right Bol and $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(6) *L is left Bol and $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(7) *L is right Bol and $\rho_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(8) *L is left Bol and $\kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(9) *L is right Bol and has the anti-automorphic inverse property;*
(10) *L is left Bol and has the anti-automorphic inverse property;*
(11) *L is right Bol and has the left inverse property;*
(12) *L is left Bol and has the right inverse property;*
(13) *L is an inverse property loop that is is right Bol;*
(14) *L is an inverse property loop that is is left Bol;*
(15) *L is right Bol and left Bol.*

Proof. By previous results, each of the conditions (2) – (15) is equivalent to there being a fiber F of $\mathbb{D}(L)$ and at least one additional point $p \notin F$ such that $\mathbb{D}(L)$ admits central automorphisms with center p and each f of F. This condition is clearly a consequence of (1), so it remains to prove that conversely this condition implies (1).

Let the fibers of $\mathbb{D}(L)$ be F, G, and H with $p \in G$. Then τ_p switches F and H, and so

$$\mathrm{Aut}(\mathbb{D}(L)) \supset \{\, \tau_h \,|\, h \in H \,\} = \{\, \tau_f \,|\, f \in F \,\}^{\tau_p}.$$

Next for $q \in H$ we have

$$\mathrm{Aut}(\mathbb{D}(L)) \supset \{\, \tau_g \,|\, g \in G \,\} = \{\, \tau_f \,|\, f \in F \,\}^{\tau_q}.$$

This gives (1). □

Theorem 3.13. *Let L be a loop. Then each of the following conditions is equivalent to the others and to all the condition of Theorem* 3.12.

(M1) $(xa)(bx) = (x(ab))x$ *for all* x, a, b *in* L.
(M2) $(xa)(bx) = x((ab)x)$ *for all* x, a, b *in* L.
(M3) $((ax)b)x = a(x(bx))$ *for all* x, a, b *in* L.
(M4) $((xa)x)b = x(a(xb))$ *for all* x, a, b *in* L.
(M5) *For each of its points* p, *the Latin square design* $\mathbb{D}(L)$ *admits a central automorphism with center* p.

Proof. Condition (M5) is, of course, condition (1) of Theorem 3.12.

If we substitute $a = 1$ into conditions (M1) and (M3) and $b = 1$ into (M2) and (M4), then we get the flexible law $(xc)x = x(cx)$, for all $c, x \in L$. In particular conditions (M1) and (M2) are equivalent, since they differ only by an application of the flexible law on the righthand side.

By Proposition 3.11, being an inverse property loop with condition (M1) is equivalent to condition (4) of Theorem 3.12. So we show that condition (M1) forces a loop to be an inverse property loop.

With $x = {}^{-1}b$ in (M1), an application of the flexible law gives

$$ {}^{-1}ba = ({}^{-1}ba)(b({}^{-1}b)) = ({}^{-1}b(ab))({}^{-1}b) = {}^{-1}b((ab)({}^{-1}b)) \,.$$

We cancel ${}^{-1}b$ on the left to get the right inverse property $a = (ab)({}^{-1}b)$. Similarly, setting $x = a^{-1}$, we find

$$ ba^{-1} = (a^{-1}a)(ba^{-1}) = (a^{-1}(ab))a^{-1} \,.$$

The two righthand a^{-1}'s cancel to give $b = a^{-1}(ab)$ for all a, b, and this is the left inverse property. Therefore conditions (M1) and (M2) are equivalent to all the conditions of Theorem 3.12.

Next consider condition (M3). An application of the flexible law gives $((ax)b)x = a((xb)x))$, the right Bol identity. Also $x = {}^{-1}a$ in (M3) yields

$$ b({}^{-1}a) = ((a({}^{-1}a))b)({}^{-1}a) = a({}^{-1}a(b({}^{-1}a))) \,,$$

which for $z = b({}^{-1}a)$ reads $z = a({}^{-1}az)$, a version of the left inverse property. Therefore (M3) implies condition (11) of Theorem 3.12. Conversely, assume as in (11) of Theorem 3.12 that the loop L is a right Bol loop with the left inverse property. (In particular, inverses are two-sided.) Set $a = x^{-1}$ in the right Bol identity to get

$$ bx = ((x^{-1}x)b)x = x^{-1}((xb)x)) \,.$$

The left inverse property then gives $x(bx) = (xb)x$, the flexible law. But given the flexible law, condition (M3) and the right Bol identity are equivalent. Therefore (M3) is equivalent to condition (11) of Theorem 3.12.

A similar argument to that of the previous paragraph shows that condition (M4) is equivalent to being a left Bol loop with the right inverse property, condition (12) of Theorem 3.12. (Alternatively, (M4) is (M3) in the opposite loop.) □

Loops that satisfy all the conditions of the two theorems above are called *Moufang loops* after Ruth Moufang [21] who first studied the four conditions (M1) – (M4) of Theorem 3.13. Bol [2] first proved the equivalence of these four conditions, and the further equivalence with conditions (9) – (15) is well-known. (See, for instance, [26, II.3.10,IV.6.9].) The identity (M4) was Moufang's original condition, but various authors choose any one of the four conditions to define Moufang loops. Bruck [3, p. 116] and Pflugfelder [26, p. 89] prefer (M1).

Here we are particularly interested in condition (M5). The equivalence of algebraic identities like those of Moufang and Bol with the existence of various geometric automorphisms, in turn equivalent to the closure of certain geometric figures (as seen in the proofs above), goes back to Veblen and Young [33] (who considered automorphisms of projective planes and their relationship to Desargues' configurations) and to Reidermeister [29], Thomsen [31], Bol [2], and their collaborators who worked on 3-nets (3-webs) of parallel classes of lines in the projective plane. See also Bruck [3] and Pickert [27]. Tits [32] studied automorphisms of nets and groups with triality specifically in the context of the octonions and Cartan's triality groups. The geometric study has been revived more recently, particularly in the paper of Funk and P. Nagy [9] which describes in detail the relationships between Bol reflections on a 3-net (the dual of central automorphisms of a Latin square design) and coordinatizing Bol loops. See also [16, 24].

As before, several of the well-known properties of Moufang loops are immediate from the Theorem 3.13.

Theorem 3.14.

(*a*) *All loop isotopes of a Moufang loop are Moufang loops* [26, IV.4.2].

(*b*) *The loop L is a Moufang loop if and only if all its loop isotopes are inverse property loops* [3, VII.2.3], [26, IV.4.3]. □

3.4. Multiplication groups

If L is a loop (indeed a quasigroup) then for all $x \in L$ the maps

$$\mathrm{R}(x)\colon L \longrightarrow L \quad \text{given by} \quad a^{\mathrm{R}(x)} = ax$$

and

$$\mathrm{L}(x)\colon L \longrightarrow L \quad \text{given by} \quad a^{\mathrm{L}(x)} = xa$$

are permutations of L. We then define within $Sym(L)$ the *right multiplication group*

$$\mathrm{M_R}(L) = \langle\, \mathrm{R}(x) \,|\, x \in L \,\rangle\,,$$

the *left multiplication group*

$$\mathrm{M_L}(L) = \langle\, \mathrm{L}(x) \,|\, x \in L \,\rangle\,,$$

and the *multiplication group*

$$\mathrm{M}(L) = \langle\, \mathrm{R}(x), \mathrm{L}(x) \,|\, x \in L \,\rangle = \langle\, \mathrm{M_R}(L), \mathrm{M_L}(L) \rangle.$$

The *inner mapping group* is then the stabilizer of the identity in the multiplication group:

$$\mathrm{I}(L) = \{\, \alpha \in \mathrm{M}(L) \,|\, 1^\alpha = 1 \,\}\,.$$

These groups are often useful. Indeed, in our proof of Lemma 3.9 we verified and made good use of the fact that the automorphism $\kappa_z\kappa_1$ acted as the permutation $\mathrm{R}(z)$ in its action on the fiber L_R:

$$a_R^{\kappa_z\kappa_1} = az_R = a_R^{\mathrm{R}(z)}\,.$$

Following on from this we easily find

Proposition 3.15. *Let L be a loop.*

(*a*) *If $\kappa_1, \kappa_z \in \mathrm{Aut}(\mathbb{D}(L))$ for some z of L, then*

$$\kappa_1\kappa_z \in Sym(L_R) \times Sym(L_C) \times Sym(L_E)$$

with

$$\kappa_1\kappa_z = (\,\mathrm{R}(z^{-1}),\, \mathrm{L}(z)\mathrm{R}(z),\, \mathrm{R}(z)\,)\,.$$

(*b*) *If $\rho_1, \rho_z \in \mathrm{Aut}(\mathbb{D}(L))$ for some z of L, then*

$$\rho_1\rho_z \in Sym(L_R) \times Sym(L_C) \times Sym(L_E)$$

with

$$\rho_1\rho_z = (\,\mathrm{R}(z)\mathrm{L}(z),\, \mathrm{L}(z^{-1}),\, \mathrm{L}(z)\,)\,. \qquad \square$$

We thus have

Theorem 3.16.

(*a*) *If L is a right Bol loop, then the automorphism group*

$$\langle\, \kappa_1\kappa_z \,|\, z \in L \,\rangle = \langle\, \kappa_x\kappa_y \,|\, x, y \in L \,\rangle$$

acts as the right multiplication group $\mathrm{M_R}(L)$ *on the fibers L_R and L_E.*

(*b*) *If L is a left Bol loop, then the automorphism group*

$$\langle\, \rho_1\rho_z \,|\, z \in L \,\rangle = \langle\, \rho_x\rho_y \,|\, x, y \in L \,\rangle$$

acts as the left multiplication group $\mathrm{M_L}(L)$ *on the fibers L_C and L_E.*

(*c*) *If L is a Moufang loop, then the automorphism group*

$$\langle\, \rho_x\rho_y, \kappa_x\kappa_y \,|\, x, y \in L \,\rangle$$

acts as the multiplication group $\mathrm{M}(L)$ *on each of the fibers L_R, L_C, and L_E.* □

This theorem (phrased in the dual language of 3-nets and their Bol reflections) was one of the main results of Funk and Nagy [9]; and they went on to explore many of its consequences, particularly for Bol loops.

The maps of the lemma and theorem are special cases of autotopisms of the loop L. An *autotopism* of L is a triple

$$(\alpha, \beta, \gamma) \in Sym(L_R) \times Sym(L_C) \times Sym(L_E)$$

with

$$x \cdot y = z \iff x^\alpha \cdot y^\beta = z^\gamma \,.$$

So an autotopism is a self-isotopy (see Section).

It is immediate that the autotopism group of L is canonically isomorphic to $\mathrm{BAut}(\mathbb{D}(L))$, the normal base subgroup of $\mathrm{Aut}(\mathbb{D}(L))$ consisting of all automorphisms of $\mathbb{D}(L)$ that leave each fiber globally fixed.

Let $\mathrm{Aut}(\mathbb{D}(L))^0$ be the normal subgroup of $\mathrm{Aut}(\mathbb{D}(L))$ that is generated by all central automorphisms. Its base subgroup

$$\mathrm{BAut}(\mathbb{D}(L))^0 = \mathrm{Aut}(\mathbb{D}(L))^0 \cap \mathrm{BAut}(\mathbb{D}(L))$$

is in turn normal in $\mathrm{Aut}(\mathbb{D}(L))$. This is the subgroup of Theorem 3.16(c).

A permutation α of the loop L is called a *pseudo-automorphism* [2] of L if $1^\alpha = 1$ and there is an autotopism (α, β, γ). We thus have by Theorem 3.16(c)

Proposition 3.17. [3, Lemma VII.3.2], [26, IV.1.6]. *If L is a Moufang loop, then the inner mapping group $\mathrm{I}(L)$ is a normal subgroup of the group of all pseudo-automorphisms of L.* □

4. Wreath products and groups with triality

4.1. Wreath products

Let Ω be a finite set and K a group. For each $x \in \Omega$, let K_x be a copy of K and set $B = \bigotimes_x K_x$, the *base group*. The symmetric group $Sym(\Omega)$ acts on B via

$$k_x^g = k_{x.g}\,,$$

for each $g \in Sym(\Omega)$. The *full wreath product* $K \wr Sym(\Omega)$ is then the extension $B.Sym(\Omega)$.

The *projection homomorphism* is the map $\pi : K \wr Sym(\Omega) \longrightarrow Sym(\Omega)$ with kernel B. The *augmented wreath product* $\mathrm{Wr}(K, \Omega)$ is the normal subgroup of the full wreath product generated by the conjugacy class $T = (a, b)^{K \wr Sym(\Omega)}$ containing the 2-cycle class of $Sym(\Omega)$. We call T the set of *transpositions* of $K \wr Sym(\Omega)$. The quotient of $K \wr Sym(\Omega)$ by $\mathrm{Wr}(K, \Omega)$ is small – the largest abelian quotient of K. Therefore we can think of $K \wr Sym(\Omega)$ and $\mathrm{Wr}(K, \Omega)$ as essentially the same group.

Two distinct transpositions of $Sym(\Omega)$ have product of order 2 or 3. Surprisingly this restricted set of product orders maintains in the full wreath product. This is made precise in the following observation of Zara [34] and Doro [8]. (See also [14, Theorem 1.1].)

Theorem 4.1. *Let T be the transposition class of the full wreath product $K \wr Sym(\Omega)$ with $|\Omega| \geqslant 3$. Let the associated projection homomorphism be $\pi : K \wr Sym(\Omega) \longrightarrow Sym(\Omega)$. Then, for all $t, r \in T$, we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,. \qquad \square$$

[2] This definition is equivalent to the usual equational definition for a pseudo-automorphism of a loop; see [26, Theorem III.4.14].

That is, the product of two transpositions remains of order 2 or 3 in the full wreath product unless the transpositions are in the same coset of the base group. A nearly complete converse of this result was given in [14, Theorem 1.2]:

Theorem 4.2. *Let T be a conjugacy class of elements of order 2 in the group $G = \langle T \rangle$; and let $\pi : G \longrightarrow Sym(\Omega)$, with $|\Omega| \geq 4$, be a homomorphism in which $\pi(T)$ is the transposition class of $Sym(\Omega)$. Further assume, for all $t, r \in T$, that we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,.$$

Then there is a group K with

$$G/Z(G) \simeq \mathrm{Wr}(K, \Omega)/Z(\mathrm{Wr}(K, \Omega))\,. \qquad \square$$

4.2. Groups with triality

The case of Theorem 4.1 that is missing from the characterization Theorem 4.2 is that of $|\Omega| = 3$. The groups satisfying the hypotheses of Theorem 4.2 with $|\Omega| = 3$ have in fact been studied extensively, starting with Glauberman [12] and Doro [8], under the name of *groups with triality*; see [9, 16, 24, 32], for instance. Such groups need not arise from wreath products, Cartan's triality groups $\mathrm{P}\Omega_8^+(\mathbb{F}) : Sym(3)$, for $\mathbb{F}$ a field, furnishing the canonical example (and the name).

We have a version of Theorem 4.2 for groups with triality. (In that case the hypotheses can be streamlined somewhat.) This presents Glauberman and Doro's correspondence between groups with triality and Moufang loops.

Theorem 4.3. *Let T be a conjugacy class of elements of order 2 in the group $G = \langle T \rangle$, and let $\pi : G \longrightarrow Sym(3)$ be a surjective homomorphism. Further assume, for all $t, r \in T$, that we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = 3.$$

Then there is a Moufang loop L (unique up to isotopy) with

$$G/Z(G) \simeq \mathrm{Aut}(\mathbb{D}(L))^0\,,$$

where the class T of size $3|L|$ maps bijectively to the class of central automorphisms of $\mathrm{Aut}(\mathbb{D}(L))^0$, the subgroup of $\mathrm{Aut}(\mathbb{D}(L))$ generated by all central automorphisms.

Conversely if L is a Moufang loop, then the group $G = \mathrm{Aut}(\mathbb{D}(L))^0$ generated by the size $3|L|$ conjugacy class T of central automorphisms is a group with triality and has the above properties with respect to the projection map π given by

$$\pi(\rho_k) = (2,3), \quad \pi(\kappa_k) = (1,3), \quad \pi(\epsilon_k) = (1,2)\,,$$

for all $k \in L$.

Proof. Given the group G with triality (as in the hypothesis), we form a partial linear space $\mathbb{D}$ whose points are the members of the class T and whose lines are the various triples of elements of T in a subgroup $S \simeq Sym(3)$ generated by members of T and having $\pi(S) = Sym(3)$. Then $\mathbb{D}$ is a Latin square design whose fibers are the three sets

$$T_R = T \cap \pi^{-1}((2,3)), \quad T_C = T \cap \pi^{-1}((1,3)), \quad T_E = T \cap \pi^{-1}((1,2))\,.$$

G acts naturally by conjugation on $\mathbb{D}$, the kernel of the action being $Z(G)$, the center of G. Each element $t \in T$ acts on $\mathbb{D}$ as the central automorphism τ_t with center t. Therefore by Theorem 3.13 there is a Moufang loop L, unique up to isotopy, with $\mathbb{D}$ isomorphic to $\mathbb{D}(L)$.

The converse follows from Proposition 2.3 and Theorem 3.13. □

In particular, we see that the Zara-Doro Theorem 4.1 in the case $|\Omega| = 3$ is associated with the fact that a group is a special type of Moufang loop. In the split octonions over the field $\mathbb{F}$, the units of norm 1 form a Moufang loop whose associated group with triality is Cartan's triality group $\mathrm{P}\Omega_8^+(\mathbb{F}) : Sym(3)$.

The previous two theorems show that there are uniquely determined minimal groups with triality (and "Ω-ality"), namely those with trivial center. There are also uniquely determined maximal (universal) groups, those with the largest possible center compatible with the hypotheses. This comes from intermediate results in [14] that also emphasize the connection between Theorems 4.2 and 4.3. (See also [11, Prop. 2.5].) We first need a definition.

Definition 4.4. For a loop L and finite set Ω of size at least 3, the group $\mathrm{UWr}(L, \Omega)$ has the following presentation:

Generators:

$\langle\langle k\,;\, a\,, b\rangle\rangle$ for arbitrary $k \in L$ and distinct $a, b \in \Omega$;

Relations:

for arbitrary $k, h \in L$ and distinct $a, b, c, d \in \Omega$ (as possible):

(1) $\langle\langle k\,;\,a\,,b\rangle\rangle^2 = 1$;
(2) $\langle\langle k\,;\,a\,,b\rangle\rangle = \langle\langle k^{-1}\,;\,b\,,a\rangle\rangle$;
(3) $\langle\langle k\,;\,a\,,b\rangle\rangle^{\langle\langle h\,;\,b\,,c\rangle\rangle} = \langle\langle kh\,;\,a\,,c\rangle\rangle$;
(4) $\langle\langle k\,;\,a\,,b\rangle\rangle^{\langle\langle h\,;\,c\,,d\rangle\rangle} = \langle\langle k\,;\,a\,,b\rangle\rangle$.

The relation (4) is empty when $|\Omega| = 3$.

By (3) the set $T = \{\,\langle\langle k\,;\,a\,,b\rangle\rangle \mid k \in L, a, b \in \Omega\,\}$ is a conjugacy class of $\mathrm{UWr}(L,\Omega)$. The class need not be in bijection with the set of the various $(k,\{a,b\})$ (for instance, by (2) if L does not have two-sided inverses).

It is routine to check that $\mathrm{UWr}(L,\Omega)$ satisfies the hypotheses of Theorem 4.2 (for $|\Omega| \geqslant 3$) with respect to the class T and $\pi(\langle\langle k\,;\,a\,,b\rangle\rangle) = (a,b) \in Sym(\Omega)$. Indeed, if L is a group, then $\mathrm{Wr}(L,\Omega)$ is a quotient of $\mathrm{UWr}(L,\Omega)$ (as suggested by Theorem 4.1) with the transposition class and T in bijection (and so the kernel is central).

If L is a Moufang loop and $\Omega = \{R, C, E\}$ then, by Proposition 2.3 and Theorem 3.13, $\mathrm{Aut}(\mathbb{D}(L))^0$ is a homomorphic image of the group with triality $\mathrm{UWr}(L,\Omega)$ and the class T of $\mathrm{UWr}(L,\Omega)$ is in bijection with the class of central automorphisms (so again the kernel is central). The homomorphism and bijection are given by

$$\langle\langle k\,;\,2\,,3\rangle\rangle \mapsto \rho_k, \quad \langle\langle k\,;\,1\,,3\rangle\rangle \mapsto \kappa_k, \quad \langle\langle k\,;\,1\,,2\rangle\rangle \mapsto \epsilon_k\,.$$

(This also explains why we do not need relations describing the conjugations $\langle\langle k\,;\,a\,,b\rangle\rangle^{\langle\langle h\,;\,a\,,b\rangle\rangle}$; by Corollary 2.4 such relations are consequences of those already specified.)

These two classes of examples are essentially all there are.

Theorem 4.5. *Let T be a conjugacy class of elements of order 2 in the group $G = \langle T\rangle$; and let $\pi : G \longrightarrow Sym(\Omega)$, with $|\Omega| \geqslant 3$, be a homomorphism in which $\pi(T)$ is the transposition class of $Sym(\Omega)$. Further assume, for all $t, r \in T$, that we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,.$$

Then there is a Moufang loop L (unique up to isotopy) and a central subgroup Z of $\mathrm{UWr}(L,\Omega)$ with

$$G \simeq \mathrm{UWr}(L,\Omega)/Z\,.$$

Here the class T has size $3|L|$ and is in bijection with the class $\{\langle\langle k\,;\,a\,,b\rangle\rangle\}$ of $\mathrm{UWr}(L,\Omega)$. The map π factors through the natural map that takes each $\langle\langle k\,;\,a\,,b\rangle\rangle$ to $(a,b) \in Sym(\Omega)$.

If additionally $|\Omega| \geqslant 4$, then the Moufang loop L is a group. □

For $|\Omega| \geqslant 4$ this is essentially [14, Theorem 3.7], which is the major step in the proof of Theorem 4.2 (that is, [14, Theorem 1.2]). For $|\Omega| = 3$ this is essentially [14, Theorem 4.1] and is an easy consequence of Theorem 4.3 above and intermediate results proven in [14].

For $|\Omega| = 3$ this theorem can also be thought of as locating a unique largest Moufang quotient of a given loop or, equivalently, for each Latin square design giving the unique maximal quotient design (possibly of order 1) that admits all possible central automorphisms (as promised at the end of Section 2).

4.3. Generalized dihedral loops

The previous section suggests that one way of finding nice Moufang loops is to find nice groups with triality.[3]

A dihedral group G is one that has a normal cyclic subgroup H of index 2 such that every element g of $G \setminus H$ has order 2 and by conjugation inverts all elements h of H; that is, $gh = h^{-1}g$.

We say that the loop L is *generalized dihedral* precisely when it has a subloop H of index 2 such that every element g of $L \setminus H$ has order 2 and by conjugation inverts all elements h of H via $gh = h^{-1}g$. Dihedral groups provide examples of generalized dihedral Moufang loops.

A result of Chein [4, Theorem 1] gives

Theorem 4.6. *If L is a generalized dihedral Moufang loop, then the subloop H is a group. For any group H there is a generalized dihedral Moufang loop L with H as its distinguished subloop of index 2, and such an L is uniquely determined up to isomorphism.* □

A construction equivalent to Chein's was given by R.T. Curtis [6] but was not published. Chein and Curtis gave the Cayley table of L in a simple form which is derived from that of H.

Here the crucial but elementary observation is this:

> The symmetric group $Sym(3) = Sym(\{1,2,3\})$ is a homomorphic image of $Sym(4) = Sym(\{1,2,3,4\})$ with transpositions mapped to transpositions.

Therefore by Theorem 4.1 for any group H the augmented wreath product group $\mathrm{Wr}(H, \{1,2,3,4\})$ is a group with triality and so is associated as

[3] Equally well, nice groups with triality can be found from nice Moufang loops. Witness the unit octonions and Cartan's triality groups.

in the previous section with a Moufang loop L. The loop turns out to be generalized dihedral.

Theorem 4.7. [14, Theorem 4.4] *Let H be a group. Then the group* $\mathrm{UWr}(H, \{1,2,3,4\})$ *is isomorphic to* $\mathrm{UWr}(L, \{1,2,3\})$*, the universal group with triality associated with the generalized dihedral Moufang loop L having H as its distinguished subloop of index* 2. □

The theorem says that generalized dihedral Moufang loops come up naturally, namely as those Moufang loops arising from groups with triality that are full wreath products by the symmetric group of degree 4.

5. Simple Moufang loops

A nonidentity loop is *simple* if every surjective loop homomorphism is either bijective or has image the identity. For instance, if in the split octonions over a field $\mathbb{F}$ we take the Moufang loop of norm 1 elements and factor out the center $\{\pm 1\}$, then we have a simple loop $\mathrm{P}(\mathbb{F})$, called a *Paige loop* after L.J. Paige who first observed and proved simplicity [25].

A group G with $S \leq \mathrm{Aut}(G)$ is *S-simple* if the identity and G are the only S-invariant normal subgroups of G. The group G is *triality-simple* if it is S-simple for $S \simeq Sym(3)$ and additionally the group $G.S$ is a group with triality with respect to the conjugacy class containing the transpositions of S and $\ker \pi = G$.

Lemma 5.1. [8, Cor.1.1] *Let L be a Moufang loop. Then L is simple if and only if* $\mathrm{BAut}(\mathbb{D}(L))^0$ *is triality-simple.* □

Lemma 5.2. [8, 23] *Let G be a nonabelian triality-simple group. Then one of:*

(a) *$G.S \simeq N \wr Sym(3)$ for a nonabelian simple group N,*

(b) *G is simple.* □

In the second lemma, since $S \simeq Sym(3)$ and G is nonabelian and S-simple, there must be a nonabelian simple group N with G the direct product of k copies of N for $k \in \{1,2,3,6\}$. The case $k = 1$ is conclusion (b). Doro showed that, for a triality-simple group, $k = 6$ is not possible and $k = 3$ leads to conclusion (a). He also showed that in the special case of finite nonabelian triality-simple groups $k = 2$ cannot occur. Nagy and Valsecchi later proved that for arbitrary nonabelian triality-simple groups $k = 2$ leads to a contradiction.

5.1. Finite simple Moufang loops

Liebeck [19], using the classification of finite simple groups, proved

Theorem 5.3. *If G is a nonabelian finite triality-simple group, then $G.S$ is one of:*

(a) $N \wr Sym(3)$ *for a nonabelian finite simple group N,*

(b) $\mathrm{P}\Omega_8^+(\mathbb{F}) : Sym(3)$ *for a finite field $\mathbb{F}$.* □

With Lemmas 5.1 and 5.2 this yields

Theorem 5.4. [19, Theorem] *A finite simple Moufang loop is either associative (and so a finite simple group) or is isomorphic to a Paige loop $\mathrm{P}(\mathbb{F})$ over a finite field $\mathbb{F}$.* □

Lagrange's Theorem says that every subgroup of the finite group G has order that divides the order of G. It had long been conjectured [5] that Lagrange's Theorem remains true for finite Moufang loops. A result of Bruck [3, Lemma V.2.1] shows that Lagrange's Theorem is true for all finite Moufang loops if and only if it is true for all finite simple Moufang loops. It is certainly true in the finite simple groups, so by Liebeck's Theorem 5.4 it remained to check whether or not Lagrange's Theorem holds in finite Paige loops. This was recently done by several groups of people independently, the first being Grishkov and Zavarnitsine [13]. Therefore we have

Theorem 5.5. [10, 11, 13, 20] *Every subloop of the finite Moufang loop L has order that divides the order of L.* □

All of the proofs relate subloops of the octonions to subgroups of the associated group with triality $\mathrm{P}\Omega_8^+(\mathbb{F}) : Sym(3)$ and then carefully study the subgroup structure of this group.

Just a few years ago, it was possible to say [5] that the two most important problems in loop theory were the Lagrange Property for finite Moufang loops and the existence of finite simple Bol loops that are not Moufang. Now both problems have been resolved positively. Nevertheless, as pointed out by the referee, it is still open as to whether all finite Bol loops have the Lagrange Property. Bruck's result [3, Lemma V.2.1] again reduces this to the case of simple loops. But Nagy's examples [22] of finite simple Bol loops that are not Moufang show that much remains to be done. In particular, the corresponding result to Doro's Lemma 5.1 is false, since Nagy's smallest example L (of order 24) has $\mathrm{Aut}(\mathbb{D}(L))^0$ solvable.

5.2. Locally finite simple Moufang loops

An algebraic object is *locally finite* if each subobject generated by a finite subset is itself finite. For example the algebraic closure $\overline{\mathbb{F}}_p$ of any finite field $\mathbb{F}_p$ is a locally finite field since any finite subset of $\overline{\mathbb{F}}_p$ lies in a extension that has finite degree over $\mathbb{F}_p$ and so is itself finite. Indeed a field is locally finite precisely when it is isomorphic to a subfield of $\overline{\mathbb{F}}_p$ for some prime p.

A great deal of work has been done in the last twenty-five years on the classification and properties of locally finite simple groups (for instance, [15, 18]). Certain techniques go over to Moufang loops, allowing us to extend Liebeck's theorems by replacing every instance of "finite" by "locally finite."

Theorem 5.6. *If G is a nonabelian locally finite triality-simple group, then $G.S$ is one of:*

(*a*) $N \wr Sym(3)$ *for a nonabelian locally finite simple group N,*

(*b*) $\mathrm{P}\Omega_8^+(\mathbb{F}) : Sym(3)$ *for a locally finite field $\mathbb{F}$.* □

Theorem 5.7. *A locally finite simple Moufang loop is either associative (and so a locally finite simple group) or is isomorphic to a Paige loop $\mathrm{P}(\mathbb{F})$ over a locally finite field $\mathbb{F}$.* □

All locally finite fields are countable, and a finite dimensional algebra over a countable field is countable. Therefore we have the remarkable

Corollary 5.8. *An uncountable locally finite simple Moufang loop is associative and so is a locally finite simple group.* □

The proofs will appear elsewhere. A crucial initial observation is that the Moufang loop L is locally finite if and only if the associated universal group with triality $\mathrm{UWr}(L, 3)$ is locally finite. This is proven using Theorem 4.5 above. The rest of the argument then uses the techniques of locally finite group theory as found in [15, 18].

References

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

[2] **G. Bol**: *Gewebe und Gruppen* (*Topologische Fragen der Differentialgeometrie* 65.), Math. Ann. **114** (1937), 414 – 431.

[3] **R. H. Bruck**: *A Survey of Binary Systems*, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

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

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

[6] **R. T. Curtis**: *Rayleigh Prize essay*, University of Cambridge, 1970.

[7] **A. Devillers and J. I. Hall**: *Rank* 3 *Latin square designs*, J. Combin. Theory, Ser. A, **113** (2006), 894 – 902.

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

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

[10] **S. M. Gagola III**: *Subloops of the unit octonions*, Acta Sci. Math. (Szeged) **72** (2006), 837 – 861.

[11] **S. M. Gagola III and J. I. Hall**: *Lagrange's theorem for Moufang loops*, Acta Sci. Math. (Szeged) **71** (2005), 45 – 64.

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

[13] **A. N. Grishkov and A. V. Zavarnitsine**: *Lagrange's theorem for Moufang loops*, Math. Proc. Cambridge Philos. Soc. **139** (2005), 41 – 57.

[14] **J. I. Hall**: *A characterization of the full wreath product*, J. Algebra **300** (2006), 529 – 554.

[15] **J. I. Hall**: *Periodic simple groups of finitary linear transformations*, Ann. of Math. **163** (2006), 445 – 498.

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

[17] **M. Hall, Jr.**: *Combinatorial Theory*, Second edition, John Wiley & Sons, Inc., New York, 1986.

[18] **B. Hartley**: *Simple locally finite groups*, in: "Finite and locally finite groups (Istanbul, 1994)," eds. B. Hartley, G.M. Seitz, A.V. Borovik, R.M. Bryant, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., **471** (1995), 1 – 44.

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

[20] **G. E. Moorhouse**: personal communication, August 2004.

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

[22] **G. P. Nagy**: `www.math.u-szeged.hu/~nagyg/pub/simple_bol_loops.html`

[23] **G. P. Nagy and M. Valsecchi**: *Splitting automorphisms and Moufang loops*, Glasg. Math. J. **46** (2004), 305 – 310.

[24] **G. P. Nagy and P. Vojtěchovský**: *Octonions, simple Moufang loops and triality*, Quasigroups Related Systems **10** (2003), 65 – 94.

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

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

[27] **G. Pickert**: *Projektive Ebenen*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.

[28] **C. E. Praeger**: *A note on group Latin squares*, J. Combin. Math. Combin. Comput. **5** (1989), 41 – 42.

[29] **K. Reidermeister**: *Topologische Fragen der Differentialgeometrie. V. Gewebe und Gruppen*, Math. Z. **29** (1929), 427 – 435.

[30] **T. A. Springer and F.D. Veldkamp**: *Octonions, Jordan Algebras and Exceptional Groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

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

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

[33] **O. Veblen and J. W. Young**: *Projective Geometry*, Ginn and Co., Boston, 1916, 1917.

[34] **F. Zara**: *Classification des couples fischeriens*, Thése, Amiens, 1985.

Department of Mathematics
Michigan State University
East Lansing
Michigan 48824
U.S.A.
E-mail: jhall@math.msu.edu

Received June 8, 2007