Topics in Moufang Loops and Related Quasigroups

A Dissertation

Presented to

the Faculty of Natural Sciences and Mathematics

University of Denver

In Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

by

Nicholas Britten

Month/Year of Graduation

Advisor: Dr. Kinyon

Author: Riley Britten
Title: Topics in Moufang Loops and Related Quasigroups
Advisor: Michael Kinyon, Ph.D.
Degree Date:

ABSTRACT

We will begin by discussing power graphs of Moufang loops. We are able to show that as in groups the directed power graph of a Moufang loop is uniquely determined by the undirected power graph. In the process of proving this result we define the generalized octonion loops, a variety of Moufang loops which behave analogously to the generalized quaternion groups. We proceed to investigate para-F quasigroups, a variety of quasigroups which we show are antilinear over Moufang loops. We briefly depart from the context of Moufang loops to discuss solvability in general loops. We then prove some results on the cosets of subloops of Moufang loops. Finally, we investigate generalizations of the variety of Moufang loops, the varieties of universally and semi-universally flexible loops.

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1: Introduction

1.1 Overview

In this dissertation we will investigate Moufang loops and quasigroups related to them. In particular, we will attempt to transfer results from group theory to the context of Moufang loops and provide structural descriptions of varieties of quasigroups related to Moufang loops.

Our first major result will be the extension of a result on the power graphs of groups to Moufang loops. Namely, the undirected power graph of a groups uniquely determines the directed power graph. We were able to show that the same result holds for Moufang loops. In the process we describe a class of loops, which we have termed the generalized octonion loops, and prove several results showing that they behave analogously to the generalized quaternion groups.

We will next investigate a variety of quasigroups related to Moufang loops, that we have termed para-F quasigroups. The variety of medial quasigroups has been extensively studied and has two natural generalizations: F-quasigroups and semimedial quasigroups. The variety of paramedial quasigroups is defined analogously to the variety of medial quasigroups and has also been generalized to semiparamedial quasigroups, the analogue of semimedial quasigroups. We argue that our definition of para-F quasigroups is the correct analogue to F-quasigroups and prove analogous results to those that have been shown for medial, paramedial, semimedial, semiparamedial, and F-quasigroups.

We will then depart from the setting of Moufang loops to investigate definitions of solvability for general loops. The definition of solvability for groups is relatively easy to work with being based solely on subgroups generated by certain elements. It is well

known that the definition of solvability for groups coincides with the definition arising from universal algebra. We are able to find a sufficient condition under which this result extends to loops. Namely, the definitions of solvability coincide if $Q/\mathrm{Nuc}(Q)$ is an abelian group. Additionally, we are able to prove some results for loops Q such that $Q/\mathrm{Nuc}(Q)$ is a group.

The proof of Lagrange's Theorem for groups relies on the fact that cosets of a subgroup partition the group. While it is known that Lagrange's Theorem holds in Moufang loops the proof relies on the classification of finite simple Moufang loops and does not explicitly construct a partition of the loop. We attempted to adapt the proof of Lagrange's Theorem for groups to the context of Moufang loops by constructing a partition of the loop by cosets or orbits of the relative left multiplication group. We were ultimately unsuccessful in this endeavor, but were able to prove some intermediate results on the cosets of subloops of Moufang loops.

Finally, we will investigate another variety of loops closely related to Moufang loops, the semi-universally flexible (SUF) loops. Our goal was to construct a loop which is SUF and has the inverse property but is not Moufang. We were ultimately unsuccessful, but were able to negatively answer a conjecture that all universally flexible loops are middle Bol.

1.2 Definitions and basic results

While we intuitively think of quasigroups and loops as being generalizations of groups, a formal definition arises much more naturally by considering these objects as specific varieties of magmas. So we will begin by defining magmas and proceed by discussing successively more specific varieties.

1.2.1 Magmas.

Definition 1.1. A *magma* is a set Q along with a single binary operation $\cdot : Q \times Q \to Q$.

Definition 1.2. The *multiplication table* of a magma $(Q, \cdot)$ is the table labeled with magma elements x_i such that the entry at position (i, j) in the table is $x_i \cdot x_j$.

We use juxtaposition to denote the operation in a magma whenever convenient, and to avoid excessive parentheses, juxtaposition binds more tightly than the explicit operation, *e.g.*, $x \cdot yz$ denotes $x \cdot (y \cdot z)$.

Definition 1.3. For a magma Q and $x \in Q$ we define the *translation maps* $L_x, R_x : Q \to Q$ by

$$L_x(y) = x \cdot y$$

$$R_x(y) = y \cdot x$$

1.2.2 Quasigroups.

Definition 1.4. A *quasigroup* $(Q, \cdot)$ is a magma such that L_x, R_x are bijections for all $x \in Q$.

Definition 1.5. A *Latin square* is an nxn table with entries $x_1, \ldots, x_n$ such that each x_i appears exactly once in each row and each column.

Considering only finite quasigroups we have the following characterization:

Definition 1.6. A *finite quasigroup* $(Q, \cdot)$ is a magma whose multiplication table is a Latin square.

It is frequently convenient to use infix notation for the inverses of the translation maps, so we will also use the following equivalent definition of a quasigroup:

Definition 1.7. A *quasigroup* is a set Q along with three binary operations $\cdot, \backslash, / : Q \times Q \to Q$ satisfying:

$$(x/y) \cdot y = x, \qquad (x \cdot y)/y = x$$

$$x \cdot (x\backslash y) = y, \qquad x\backslash(x \cdot y) = y$$

Intuitively, we can also think of quasigroups as being groups without associativity. This intuition is formalized by the following result:

Fact 1.8. Let $(Q, \cdot)$ be a quasigroup which is also associative. Then $(Q, \cdot)$ is a group.

Standard references for quasigroup theory are [1, 2, 3, 4, 5].

1.2.3 Loops.

Definition 1.9. A *loop* $(Q, \cdot, \backslash, /, 1)$ is a quasigroup $(Q, \cdot, \backslash, /)$ with an element $1 \in Q$ satisfying:

$$1 \cdot x = x, \quad x \cdot 1 = x$$

Basic references for loop theory are [6], [2], [3]. Any uncited facts in the discussion that follows can be found in these references.

1.2.4 Multiplication groups.

Definition 1.10. Let $(Q, \cdot)$ be a quasigroup. The *left multiplication group* of Q is

$$\text{Mlt}_L(Q) = \langle L_x : x \in Q \rangle$$

.

The right multiplication group, $\text{Mlt}_R(Q)$ is defined dually.

Definition 1.11. Let $(Q, \cdot)$ be a quasigroup. The *multiplication group* of Q is

$$\text{Mlt}(Q) = \langle L_x, R_x : x \in Q \rangle$$

.

Definition 1.12. Let $(Q, \cdot, 1)$ be a loop. The *left inner mapping group* of Q is

$$\text{Inn}_L(Q) = \{f \in \text{Mlt}_L(Q) : f(1) = 1\}$$

The right inner mapping group is defined dually.

Definition 1.13. Let $(Q, \cdot, 1)$ be a loop. The *inner mapping group* of Q is

$$\text{Inn}(Q) = \{f \in \text{Mlt}(Q) : f(1) = 1\}$$

Elements of $\text{Inn}(Q)$ are called *inner mappings*.

Fact 1.14. Each inner mapping group is a subgroup of the corresponding multiplication group.

Fact 1.15. If $(Q, \cdot, 1)$ is a group, then $\text{Inn}(Q)$ is precisely the inner automorphism group of Q.

Definition 1.16. Let $(Q, \cdot)$ be a loop for all $x, y \in Q$ we define $L_{x,y}, R_{x,y}, T_x : Q \to Q$ by:

$$L_{x,y}(z) = (xy)\backslash(x \cdot yz)$$
$$R_{x,y}(z) = (zx \cdot y)/(xy)$$
$$M_{x,y}(z) = (y\backslash(yz \cdot x))/x$$
$$T_x(z) = (xz)/x$$

Fact 1.17. $L_{x,y}, R_{x,y}, T_x \in \text{Inn}(Q)$. Further

$$\text{Inn}(Q) = \langle L_{x,y}, R_{x,y}, T_x : x, y \in Q \rangle$$

$$\text{Inn}_L(Q) = \langle L_{x,y} : x, y \in Q \rangle$$

and

$$\text{Inn}_R(Q) = \langle R_{x,y} : x, y \in Q \rangle$$

1.2.5 Quotient loops.

Definition 1.18. Let $(Q, \cdot)$ be a loop and $S \leq Q$. Then S is a *normal subloop* of Q ($S \trianglelefteq Q$) iff

$$\varphi(S) = S \quad \forall \varphi \in \text{Inn}(Q)$$

Definition 1.19. Let $(Q, \cdot)$ be a loop with normal subloop S. Then the *quotient loop* Q/S is the loop with underlying set $\{qS : q \in S\}$, operation $xS \cdot yS = (x \cdot y)S$, and identity element $1S = S$.

Fact 1.20. The requirement that S be normal in the preceding definition ensures that Q/S is a loop with a well-defined operation.

1.2.6 Homotopy and isotopy.

Definition 1.21. Let $(Q, \cdot)$, $(P, +)$ be magmas. A *homomorphism* is a map $f : Q \to P$ satisfying:

$$f(x) + f(y) = f(x \cdot y)$$

Definition 1.22. A bijective homomorphism is an *isomorphism*.

Definition 1.23. Let $(Q, \cdot)$, $(P, +)$ be magmas. A *homotopy* is a triple of maps $(\alpha, \beta, \gamma) : Q \to P$ satisfying:

$$\alpha(x) + \beta(y) = \gamma(x \cdot y)$$

for all $x, y \in Q$.

Homotopy generalizes homomorphism in the following sense:

Fact 1.24. Let $(Q, \cdot)$, $(P, +)$ be magmas and $f : Q \to P$ be a homomorphism. Then (f, f, f) is a homotopy.

Definition 1.25. A homotopy in which each of α, β, γ is a bijection is an *isotopy*.

Fact 1.26. For a finite quasigroup an isotopy is equivalent to permuting rows of the multiplication table by α, permuting columns of the multiplication table by β, and relabeling elements by γ.

As above, isotopy is a generalization of isomorphism. In the context of groups isotopy and isomorphism are the same concept as shown in the following result:

Fact 1.27. Suppose that $(G, \cdot)$, $(H, +)$ are groups and $(\alpha, \beta, \gamma) : G \to H$ is an isotopy. Then $(G, \cdot)$, $(H, +)$ are isomorphic [2].

Fact 1.28. Let $(Q, \cdot)$ be a quasigroup, $(P, +)$ be a magma, and $(\alpha, \beta, \gamma) : (Q, \cdot) \to (P, +)$ be an isotopy. Then $(P, +)$ is a quasigroup [2].

Definition 1.29. $(Q, \cdot)$ and $(P, +)$ are said to be *istotopic* if there exists an isotopy from Q to P. Quasigroups isotopic to Q are said to be *isotopes* of Q.

Definition 1.30. Note that not all isotopes of a loop need be loops. Isotopes which happen to be loops are called *loop isotopes*.

Definition 1.31. Let $(Q, \cdot)$ be a quasigroup. An isotope of $(Q, \cdot)$ is *principal* if it has the same underlying set.

Fact 1.32. Let $(Q, \cdot)$ be a quasigroup, then up to isomorphism all principal loop isotopes of $(Q, \cdot)$ are of the form $(Q, +)$, where

$$x + y = (x/a) \cdot (b \backslash y)$$

for fixed $a, b \in Q$[2].

Fact 1.33. Let $(Q, \cdot)$ be a magma with an isotope $(P, *)$. Then there exists $+ : Q \times Q \to Q$ such that $(Q, +)$ is isomorphic to $(P, *)$ [2].

Remark. Note that together the preceding results tell us that up to isomorphism all loop isotopes of $(Q, \cdot)$ are of the form $(Q, +)$, where $x + y = (x/a) \cdot (b \backslash y)$ for fixed $a, b \in Q$.

Definition 1.34. Let $(Q, \cdot)$ be a quasigroup, a *left isotope* of $(Q, \cdot)$ is $(Q, +)$ with

$$x + y = (x/a) \cdot y$$

for fixed $a \in Q$.

Right isotope is defined dually.

Definition 1.35. A property of a quasigroup $(Q, \cdot)$ is *universal* if it holds in all isotopes of Q.

Definition 1.36. A property of a loop Q is *semi-universal* if it holds in all left and right isotopes of $(Q, \cdot)$.

1.2.7 Linearity.

Definition 1.37. A quasigroup $(Q, \cdot)$ is *linear over* a loop $(Q, +)$ if there exist $f, g \in \mathrm{Aut}(Q, +), c \in Q$ such that

$$x \cdot y = f(x) + (g(y) + c)$$

for all $x, y \in Q$.

As the following result shows, being linear over a loop is a stronger property than being isotopic to a loop.

Proposition 1.38. Suppose that $(Q, \cdot)$ is linear over $(Q, +)$. Then $(Q, +)$ is an isotope of $(Q, \cdot)$.

Proof. Suppose that $x \cdot y = (f(x) + g(y)) + c$ for all $x, y \in Q$, where $f, g \in \mathrm{Aut}(Q, +)$, $c \in Q$. Let $\gamma = \mathrm{id}$, $\alpha(x) = f(x)$, and $\beta(x) = g(x) + c$. It is immediate that α, β, γ are bijections. Let $x, y \in Q$ be given, then

$$\begin{aligned} \alpha(x) + \beta(y) &= f(x) + (g(y) + c) \\ &= x \cdot y \text{ by assumption} \\ &= \gamma(x \cdot y) \end{aligned}$$

Thus (α, β, γ) is an isotopy and $(Q, +)$ is an isotope of $(Q, \cdot)$. □

1.2.8 Inverse properties.

Definition 1.39. A loop $(Q, \cdot)$ has the *left inverse property* (LIP) if there exists a bijection $\lambda : Q \to Q$ such that for all $x, y \in Q$

$$\lambda(x) \cdot xy = y$$

Definition 1.40. Similarly, a loop $(Q, \cdot)$ has the *right inverse property* (RIP) if there exists a bijection $\gamma : Q \to Q$ such that for all $x, y \in Q$

$$xy \cdot \gamma(y) = x$$

Definition 1.41. A loop $(Q, \cdot)$ which has both the left and right inverse properties is said to be an *inverse property loop* (IP loop).

When working with IP loops we will frequently use the inversion map $^{-1} : Q \to Q$, where $x^{-1} = \lambda(x) = \gamma(x)$, instead of the left and right divisions.

Definition 1.42. A loop $(Q, \cdot, ^{-1})$ has the *automorphic inverse property* (AIP) if the following equation holds for all $x, y \in Q$

$$(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$$

Definition 1.43. A loop $(Q, \cdot, ^{-1})$ has the *antiautomorphic inverse property* (AAIP) if the following equation holds for all $x, y \in Q$

$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$$

Fact 1.44. All IP loops have the AAIP.

1.2.9 Automorphic loops.

Definition 1.45. A loop $(Q, \cdot, 1)$ is *left automorphic* if

$$\phi(x \cdot y) = \phi(x) \cdot \phi(y) \quad \forall \phi \in \text{Inn}_L(Q), x, y \in Q$$

Right automorphic is defined dually.

Definition 1.46. A loop $(Q, \cdot, 1)$ is *automorphic* if

$$\phi(x \cdot y) = \phi(x) \cdot \phi(y) \quad \forall \phi \in \text{Inn}(Q), x, y, \in Q$$

Remark. Note that ϕ is a bijection for all $\phi \in \text{Inn}(Q)$, so a loop is (left/right) automorphic if and only if all (left/right) inner mappings are automorphisms.

1.2.10 Conjugacy closed loops.

Definition 1.47. A loop $(Q, \cdot, 1)$ is *left conjugacy closed* (LCC) if it satisfies

$$z \cdot yx = ((zy)/z) \cdot zx$$

Right conjugacy closed (RCC) is defined dually.

Fact 1.48. A loop is left (right) conjugacy closed iff the set of left translations is closed under conjugation [7].

Definition 1.49. A loop $(Q, \cdot, 1)$ is *conjugacy closed* if it is both left and right conjugacy closed

1.2.11 Bol loops.

Definition 1.50. A loop $(Q, \cdot)$ is *left Bol* if the following identity holds for all $x, y, z \in Q$

$$x \cdot (y \cdot xz) = (x \cdot yx) \cdot z$$

Fact 1.51. $(Q, \cdot)$ is left Bol iff it is universally LIP [8].

Right Bol loops are defined dually and have a dual characterization.

Definition 1.52. A loop $(Q, \cdot)$ is *middle Bol* if the following identity holds for all $x, y, z \in Q$

$$x \cdot (yz \backslash x) = (x/z) \cdot (y \backslash x)$$

Fact 1.53. A loop $(Q, \cdot)$ is middle Bol iff it is universally AAIP [8].

1.2.12 Generalizations of associativity.

Definition 1.54. An *power associative loop* is a loop $(Q, \cdot)$ having the property that $\langle x \rangle$ is a group for all $x \in Q$.

Definition 1.55. A *diassociative loop* is a loop $(Q, \cdot)$ having the property that $\langle x, y \rangle$ is a group for all $x, y \in Q$.

Definition 1.56. A loop $(Q, \cdot)$ is *flexible* if the following identity holds for all $x, y \in Q$

$$xy \cdot x = x \cdot yx$$

Definition 1.57. A loop $(Q, \cdot)$ is *left alternative* if the following identity holds for all $x, y \in Q$

$$x \cdot xy = xx \cdot y$$

Right alternative is defined dually.

Definition 1.58. A loop $(Q, \cdot)$ is *alternative* if it is both left and right alternative.

1.2.13 Moufang loops.

Definition 1.59. A *Moufang loop* is a loop which is both left and right Bol.

Equivalently, a Moufang loop is a loop satisfying any (and hence all) of the Moufang identities:

$$z \cdot (x \cdot zy) = (zx \cdot z) \cdot y$$

$$x \cdot (z \cdot yz) = (xz \cdot y) \cdot z$$

$$zx \cdot yz = (z \cdot xy) \cdot z$$

$$zx \cdot yz = z \cdot (xy \cdot z).$$

Standard examples of nonassociative Moufang loops are the unit octonions with multiplication and the sphere S^7 with octonion multiplication.

Fact 1.60. All Moufang loops are IP loops [9].

Fact 1.61. All Moufang loops are diassociative [9].

Fact 1.62. All Moufang loops have the Lagrange property [10].

Definition 1.63. Let $(Q, \cdot)$ be a loop, the *Moufang center* of Q is

$$K(Q) = \{a \in Q : (a + a) + (x + y) = (a + x) + (a + y), \forall x, y \in Q\}$$

[11]

Fact 1.64. The Moufang center of any loop $(Q, \cdot)$ is a commutative Moufang subloop of Q

[2]

Definition 1.65. An *NK-loop* is a loop $(Q, \cdot)$ such that for all $a \in Q$ there exists $n \in \text{Nuc}(Q)$, k in the Moufang center of Q such that

$$a = n \cdot k$$

[11].

Fact 1.66. If $(Q, \cdot)$ is an NK loop, then it is an automorphic Moufang loop [11].

1.2.14 Partitions.

Definition 1.67. Let A be a set, a *partition* of A is $\mathcal{C} \subset \mathcal{P}(A)$ such that

$$\bigcup \mathcal{C} = A$$
$$A \cap B = \emptyset \quad \forall A, B \in \mathcal{C}$$

Definition 1.68. The elements of a partition are called *blocks*.

Definition 1.69. A partition is *uniform* if all blocks have the same size.

Chapter 2: Power graphs of Moufang loops

2.1 Introduction

Power graphs of both groups and semigroups have been widely studied, for example in [12], [13], [14], [15], [16], [17], [18]. While the power graph of a quasigroup can be defined analogously to that of a group, power graphs of quasigroups and loops have thus far been little studied. In this paper we begin transferring results on the power graphs of groups to the context of loops by addressing a question posed by Peter Cameron: if two Moufang loops have isomorphic undirected power graphs, must they have isomorphic directed power graphs? In [14] Cameron shows that two groups with isomorphic undirected power graphs must have isomorphic directed power graphs. We are able to extend that result to Moufang loops in our main theorem:

Theorem 2.1. Moufang loops with isomorphic undirected power graphs have isomorphic directed power graphs.

Cameron's proof in [14] relied on handling groups with multiple vertices connected to all others in the power graph separately. Groups with such power graphs are either cyclic or generalized quaternion. We take a similar approach here. In generalizing to Moufang loops, a third type of loop with such a power graph arises; we have termed these *generalized octonion loops*.

Theorem 2.2. A Moufang p-loop M with a unique subloop of order p is either a cyclic group, a generalized quaternion group, or a generalized octonion loop. These last two only occur when $p = 2$.

We will investigate the structure of generalized octonion loops, yielding the following equivalent characterizations of such loops:

Theorem 2.3. For a finite nonassociative Moufang loop M, the following are equivalent.

- every associative, commutative subloop of M is cyclic;
- M is isomorphic to the result of applying Chein's construction to a generalized quaternion group;
- M is isomorphic to a subloop of the unit octonions generated by $\{e^{\frac{i\pi}{n}}, j, e_5\}$;
- M is a finite Moufang 2-loop with a unique element of order 2;
- M is a p-loop with a unique subloop of order p

2.2 Preliminaries

2.2.1 Generalized quaternion groups. In the process of proving Theorem 2.1 we will investigate a class of loops which behave analogously to the generalized quaternion groups. We recall some results on generalized quaternion groups to illustrate this similarity here.

Definition 2.4. The generalized quaternion groups are given by the presentation:

$$Q_{4n} = \langle a, b : a^n = b^2, a^{2n} = 1, b^{-1}ab = a^{-1} \rangle$$

Fact 2.5. Let G be a group which is not cyclic. Then the following are equivalent:

- G is generalized quaternion.
- G is isomorphic to $\langle e^{\frac{i\pi}{n}}, j \rangle$ as a subgroup of the unit quaternions for some n [19].
- G is a finite p group in which every subgroup is cyclic [20].
- G is a finite p group with a unique subloop of order 2 [19].

Remark. A direct result of fact 2.5 is: *A finite p-group with a unique subloop of order p is either cyclic or generalized quaternion*. We will show that this result extends very naturally to Moufang loops.

Fact 2.6. Let $Q_{4n} = \langle a, b : a^n = b^2, a^{2n} = 1, b^{-1}ab = a^{-1} \rangle$. Then every element $x \in Q_{4n}$ can be written uniquely as $x = a^k$ or $x = a^k b$ for some $k \in \mathbb{N}$ [21].

2.2.2 Moufang loops. We now present some fundamental results on Moufang loops which we will need in later sections.

Theorem 2.7 (Moufang's Theorem)**.** Suppose that M is a Moufang loop and $x, y, z \in M$ are such that $x \cdot yz = xy \cdot z$. Then $\langle x, y, z \rangle$ is a group.

Proposition 2.8. Let M be a finite Moufang loop. Then

- M has the inverse property.
- M is diassociative (and thus power-associative).
- For all $x, y \in M$, $\langle x, y \rangle$ is a group [9].
- For all $x \in M$, $|x|$ divides $|M|$.
- Suppose that $|M| = p^k$ for p prime, $k \in \mathbb{Z}^+$. Then there exists $S \leq M$ with $|S| = p^{k-1}$.

Regarding the last statement, note that the center of a Moufang p-loop is nontrivial [22] [23]. So an inductive argument identical to that used to prove the last result for groups will also prove the existence of such a subloop.

2.2.3 Power graphs. To maintain generality, in what follows let $\mathbf{A} = (A, \cdot)$ be a magma with $\cdot$ a power-associative binary operation.

Definition 2.9. The *directed power graph* of **A** is the directed graph with vertex set A and an edge $x \to y$ if and only if $x^k = y$ for some $k \in \mathbb{Z}$.

Definition 2.10. The *undirected power graph* of **A** is the graph with vertex set A and an edge between x and y if and only if $x^k = y$ for some $k \in \mathbb{Z}$ or $y^k = x$ for some $k \in \mathbb{Z}$.

So the undirected power graph of **A** is the underlying undirected graph of the directed power graph of **A**. In the remainder of this paper, *power graph* will refer to the undirected power graph unless otherwise specified.

Recall that a group in which every commutative subgroup is cyclic is either cyclic or generalized quaternion [20]. We will use the following definition for generalized octonion loops in the interest of closely following this characterization of generalized quaternion groups. In §4 we will see that there are several alternate characterizations of generalized octonion loops.

Definition 2.11. Let M be a nonassociative Moufang p-loop such that every associative commutative subloop of M is cyclic, then we call M a *generalized octonion loop*.

2.2.4 Chein's construction.

Theorem 2.12. Let G be a group. For $1 \neq c \in Z(G)$ and u an indeterminate. Define $(M, \cdot)$ by $M = G \cup Gu$ and

$$g \cdot h = gh$$

$$g \cdot (hu) = (hg)u$$

$$gu \cdot h = (gh^{-1})u$$

$$gu \cdot hu = ch^{-1}g$$

for all $g, h \in G$. Then M is a Moufang loop [24]. Further, M is associative if and only if G is abelian [24].

Throughout the paper we will denote loops arising from this construction by $M(G, 2)$, where G is the underlying group. We will show that generalized octonion loops are precisely the loops $M(Q_{4n}, 2)$, where Q_{4n} is a generalized quaternion group.

Theorem 2.13. Suppose that M is a finite Moufang loop with a set of generators $\{u, u_1, \ldots, u_n\}$ such that

- $u \notin G = \langle u_1, \ldots, u_n \rangle$,
- $u^2 \in N(\langle , u^2, G \rangle)$,
- conjugation by u maps G into itself.

Let k be the smallest positive integer such that $u^k \in G$. Then

- each element of M can be expressed uniquely as gu^α where $g \in G$ and $0 \leq \alpha < k$; and
- multiplication of elements of M is given by

$$(g_1 u^\alpha)(g_2 u^\beta) = [\theta^{-\beta}(\theta^\beta(g_1)\theta^{\beta-\alpha}(g_2))g_0^\epsilon]u^\rho$$

where

$$\theta(g) = u^{-1}gu,\ g_0 = u^k \in G,\ \epsilon = \frac{\alpha+\beta}{k},\ \text{and}\ \rho = \alpha + \beta - \epsilon k$$

[24].

2.3 Moufang p-loops with a unique subloop of order p

We will begin by classifying Moufang p-loops M with a unique subloop of order p. In the proof of Theorem 2.1, we will handle such loops separately. Note that every nontrivial subloop of a Moufang loop of order p^n with a unique subloop of order p also has a unique subloop of order p.

Theorem 2.14. A Moufang p-loop M with a unique subloop of order p is either a cyclic group, a generalized quaternion group, or $M(Q_{4n}, 2)$. These last two only occur when $p = 2$.

We will first handle the simpler case that p is an odd prime.

Lemma 2.15. Let G be a group of order p^n, $p > 2$ prime with a unique subloop of order p^s for some $1 < s < n$. Then G is cyclic [25]

Lemma 2.16. Let M be a Moufang loop of order p^n for some prime $p > 2$ and $n \in \mathbb{N}$ such that M has a unique subloop of order p. Then M is a cyclic group.

Proof. Let $x, y, z \in M$ be given. If $\langle x, y\rangle = M$, then M is a group by diassociativity and we are done by the result for groups [25]. Otherwise $\langle x, y\rangle \subsetneq M$ must be a p-group with a unique subgroup of order p and thus cyclic by Lemma 2.15. Say $\langle x, y\rangle = \langle g\rangle$ and $x = g^i$, $y = g^j$. Then $x \cdot yz = g^i \cdot g^j z = g^{i+j} z = xy \cdot z$ by diassociativity. Hence in either case M is a group and thus cyclic by Lemma 2.15. □

We will now handle the case $p = 2$. In what follows, let M be a nonassociative Moufang loop of order 2^n with a unique subloop of order 2.

Lemma 2.17. For all $x, y \in M$ exactly one of the following holds:

- $xy = yx$,
- $xy = y^{-1}x$ and $|x| = 4$,
- $xy = yx^{-1}$ and $|y| = 4$,
- $|x| = |y| = 4$.

Proof. If $\langle x, y\rangle$ is cyclic, then $xy = yx$, so assume that $G = \langle x, y\rangle = \langle a, b | a^{2n} = b^4 = 1, ab = ba^{-1}\rangle$ is generalized quaternion. All elements of G can be written in the form $a^i b$

or a^i for some $i \in \mathbb{N}$. If $x = a^i$, $y = a^j$, then $xy = yx$. If $x = a^i b$, $y = a^j b$, then $x^2 = a^i b a^i b = b a^{-i} a^i b = b^2$ and similarly $y^2 = b^2$, thus $|x| = |y| = 4$. If $x = a^i$, $y = a^j b$, then $xy = a^i a^j b = a^j b a^{-i} = yx^{-1}$. Finally, if $x = a^i b$, $y = a^j b$, then $xy = a^i b a^j = a^{-j} a^i b = y^{-1} x$. □

Lemma 2.18. If $|M| = 2^n$, then M has an element of order at least 2^{n-2} and thus an associative subloop of index 2.

Proof. We will proceed by induction, taking $|M| = 64 = 2^6$ as our base case. The case of $n = 64$ follows from the classification of Moufang loops of order 64 in [26]. The result for Moufang loops of order 2^n, $n < 6$ follows from the classification of Moufang loops of order < 64 in [24] [27].

Let M be a Moufang loop of order 2^n with a unique element of order 2. Then there exists $S \leq M$ with $|S| = 2^{n-1}$ by Proposition 2.8. By the inductive hypothesis, S contains an element x_0 of order 2^{n-3}.

First assume there exists $y \in M - \langle x_0 \rangle$ with $yx_0 = x_0 y$. Then $\langle x_0, y \rangle$ is a cyclic group strictly larger than $\langle x_0 \rangle$. Thus $\langle x_0, y \rangle$ contains an element of order at least 2^{n-2}. Hence we can assume without loss of generality that $x_0 y = y x_0^{-1}$ and $|y| = 4$ for all $y \in M \setminus \langle x_0 \rangle$ since $|x_0| > 4$.

Note that if $\langle x_0 \rangle$ is properly contained in a cyclic subgroup of M, then the proof is complete. The following lemmas show that $\langle x_0 \rangle$ must be contained in such a subgroup. Thus M contains an element of order 2^{n-2} and thus an associative subgroup of index 2. □

As above, let $x_0 \in M$ be the element of order 2^{n-3}.

Lemma 2.19. If $\langle x_0 \rangle$ is not properly contained in a cyclic subgroup of M, then $\langle x_0 \rangle$ is normal in M.

Proof. Let φ be an inner mapping and set $u = \varphi(x_0)$. Inner mappings preserve powers, so $|\langle u \rangle| = |\langle x_0 \rangle| > 4$. By Lemma 2.17, we conclude that $xu = ux$, that is, $\langle x_0, u \rangle = \langle z \rangle$ for

some z. By assumption $\langle x_0 \rangle = \langle z \rangle$, hence u must be a power of x, that is, $\varphi(x_0) = x_0^i$ for some i. Thus for all j, $\varphi(x_0^j) = x_0^{ij}$, that is, $\varphi[\langle x_0 \rangle] = \langle x_0 \rangle$. Since φ is an arbitrary inner mapping, $\langle x_0 \rangle$ is normal in M. □

Lemma 2.20. $\langle x_0 \rangle$ is properly contained in a cyclic subgroup of M.

Proof. Suppose toward a contradiction that $\langle x_0 \rangle$ is not contained in a cyclic subgroup. Then $\langle x_0 \rangle$ is normal in M from the preceding lemma. Note that $M/\langle x_0 \rangle \cong \mathbb{Z}_2^3$ since every element has order at most 2.

Choose $a, b \in M$ such that $a, b \notin \langle x_0 \rangle$ and $a\langle x_0 \rangle \neq b\langle x_0 \rangle$. Let $d = ab$. Then $d\langle x_0 \rangle$ is distinct from $\langle x_0 \rangle, a\langle x_0 \rangle$, and $b\langle x_0 \rangle$. Further, $b\langle x_0 \rangle d\langle x_0 \rangle = a\langle x_0 \rangle$. Thus

$$\begin{aligned} ab &= d \\ bd &= ax_0^i \text{ for some } i \\ a \cdot (ax_0^i \cdot d^{-1}) &= d \end{aligned}$$

Hence

$$\begin{aligned} ax_0^i \cdot d^{-1} &= a^{-1}d \\ &= a^3 d \\ &= aa^2 d \\ &= ad^2 \cdot d, \text{ since } a^2 = d^2 = \text{unique element of order 2} \\ &= ad^3 \\ &= ad^{-1} \end{aligned}$$

Thus $ax_0^i \cdot d^{-1} = ad^{-1}$ and $x_0^i = 1$ after canceling d^{-1} and a.

So $ab = d$ and $bd = a$ and $b \cdot ab = a$. Then

$$\begin{aligned} ab \cdot \langle x_0 \rangle &= (b \cdot ab)a \cdot \langle x_0 \rangle \\ &= (ab)^2 \cdot \langle x_0 \rangle \\ &= \langle x_0 \rangle \text{ since all squares are contained in } \langle x_0 \rangle \end{aligned}$$

But this last contradicts that $a\langle x_0 \rangle \neq b\langle x_0 \rangle$. This contradicts our assumption that $\langle x_0 \rangle$ is not properly contained in a cyclic subgroup. Thus $\langle x_0 \rangle$ must be properly contained in a cyclic subgroup and M must contain an element of order 2^{n-2}. □

With the above lemmas we can now prove Theorem 2.14.

Proof. Let M be a Moufang loop with a unique subloop of order p for each prime divisor p of $|M|$. By Proposition 2.16, we have that if $|M|$ is not a power of 2, then M is a cyclic group. So assume that $|M| = 2^n$ for some n. If M is associative, then it is either cyclic or generalized quaternion by the result for groups. So assume that M is not associative.

By Proposition 2.18, M has an associative index 2 subloop S. By the result for groups S is either cyclic or generalized quaternion. If S is cyclic, say $S = \langle s \rangle$, then $M = \langle s, x \rangle$ for $x \notin S$ since S is an index 2 subloop. But then M is associative by diassociativity, hence we can assume that S is generalized quaternion. Let $u \in M - S$ be given and $\{u_1, u_2\}$ be a generating set for S. Then $u \notin S = \langle u_1, u_2 \rangle$, $u^2 \in Z(M) \subseteq N(\langle u^2, S \rangle)$ and $S \trianglelefteq M$, so $u^{-1}Su = S$. Thus the hypotheses of Theorem 2.13 are satisfied. Hence M is isomorphic to $M(Q_{4n}, 2)$ and the proof is complete. □

2.4 Generalized octonion loops

To make the Theorem 2.14 more closely follow the result for groups we will investigate the loops $M(Q_{4n}, 2)$, which turn out to be precisely the generalized octonion loops. We will show that they behave analogously to generalized quaternion groups.

Theorem 2.21. A Moufang loop M is a generalized octonion loop if and only if it is isomorphic to $M(Q_{4n}, 2)$.

Proof. Let M be a generalized octonion loop. Note that every associative subloop of M is either cyclic or generalized quaternion since a finite p-group with every abelian subgroup cyclic is either cyclic or generalized quaternion [20].

We will show first that $p = 2$. Suppose toward a contradiction that $p \neq 2$. Then every associative subloop of M is cyclic. Let $x, y, z \in M$ be given. Then $\langle x, y\rangle$ is associative and thus cyclic, so there exists $x_0 \in M$ such that $x_0^i = x$, $x_0^j = y$. But then $x \cdot yz = x_0^i \cdot x_0^j z = x_0^{i+j} \cdot z = xy \cdot z$ by diassociativity. Thus M is associative by Moufang's Theorem and thus a cyclic group. But this contradicts our assumption that M is nonassociative, hence we must have that $p = 2$.

Thus M is a nonassociative Moufang 2-loop. By Theorem 2.14 it is sufficient to show that M has a unique element of order 2. Let $x, y \in M$ be given. Then $\langle x, y\rangle$ is either a cyclic 2-group or generalized quaternion and in either case contains a unique element, c, of order 2. Thus there exists $c \in M$ with $|c| = 2$. Suppose that $d \in M$ is another element of order 2 and consider $\langle c, d\rangle$, which is again either a cyclic 2-group or generalized quaternion and thus contains a unique element of order 2. Hence $c = d$ and M contains a unique element of order 2. Thus M is isomorphic to $M(Q_{4n}, 2)$ for some n.

Now let M be the loop $M(Q_{4n}, 2)$. It is shown in [24] that M is a nonassociative Moufang loop. So every associative subloop of M is either cyclic or generalized quaternion

and thus every commutative and associative subloop of M is cyclic. Thus M is generalized octonion. □

Lemma 2.22. $M(Q_{4n}, 2)$ contains a unique element of order 2.

Proof. Let c be the unique element of order 2 in Q_{4n}. Suppose that x is another element of order 2 in M. Since $x \neq c$ and c is unique in G we must have that $x = gu$ for some $g \in G$. But then $x^2 = (gu)^2 = cg^{-1}g = c \neq 1$. Thus $|x| > 2$ and c is the unique element of order 2 in M. □

Theorem 2.23. A nonassociative Moufang loop is generalized octonion if and only if it has order a power of 2 and a unique element of order 2.

Proof. Using the characterization of generalized octonion loops in Theorem 2.21 it is clear that all such loops have order a power of 2. By the preceding lemma all such loops have a unique element of order 2. The converse follows immediately from Theorem 2.14. □

Theorem 2.24. M is a generalized octonion loop if and only if it is isomorphic to a subloop of the unit octonions generated by $\{e^{\frac{e_2\pi}{n}}, e_3, e_5\}$ for some $n \in \mathbb{N}$.

Proof. Let $M = \langle e^{\frac{e_2\pi}{n}}, e_3, e_5\rangle$ and note that M is nonassociative. We will use Theorem 1 in [24] to show that this is precisely $M(Q_{4n}, 2)$, taking the presentation $Q_{4n} = \langle e^{\frac{e_2\pi}{n}}, e_3\rangle$. First note that $e_5 \notin Q_{4n}$. Further, $e_5^2 = -1 \in N(\langle -1, Q_{4n}\rangle)$. Finally

$$e_5 e_3 e_5^{-1} = (e^{\frac{e_2\pi}{n}})^{-1} \in Q_{4n}$$

Thus Q_{4n} is closed under conjugation by e_5 and by Theorem 2.13, M is precisely $M(Q_{4n}, 2)$. We showed in Theorem 2.21 that this is the same as M being a generalized octonion loop.

Since there is a unique nonassociative generalized octonion loop of each possible order, the above shows that any generalized octonion loop is isomorphic to such a subloop of the unit octonions. □

The above results complete the proof of Theorem 2.3. Note that with the above results, we can restate Theorem 2.14 as:

Theorem 2.25. A Moufang p-loop M with a unique subloop of order p is either a cyclic group, a generalized quaternion group, or a generalized octonion loop. These last two only occur when $p = 2$.

Recall that the generalized quaternion group of order $4n$ can be presented as $Q_{4n} = \langle a, b | a^n = b^2, a^{2n} = 1, b^{-1}ab = a^{-1} \rangle$. Viewing the generalized octonion loop of order 16 as $M(Q_8, 2)$ with this presentation yields the power graph of O_{16} presented above. Note that the non-identity vertex a^2 is connected to all other vertices. The fact that generalized octonion loops are the only nonassociative Moufang loops with this feature is the primary reason we are interested in generalized octonion loops in the context of power graphs.

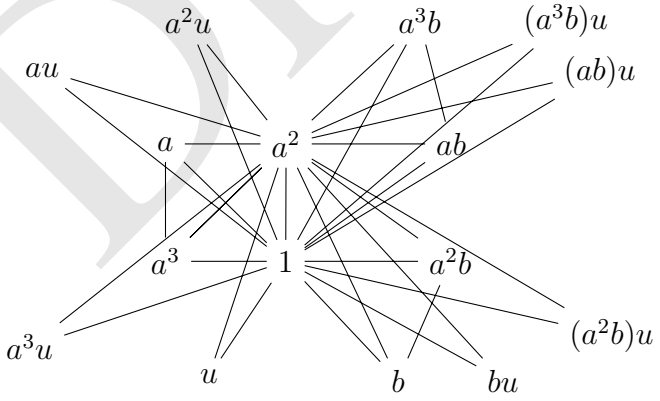

Figure 2.1: The (undirected) power graph of O_{16}

2.5 Undirected power graphs determine directed

With Theorem 2.2 at our disposal we can now translate the argument in [14] to the Moufang case to show that two Moufang loops with isomorphic undirected power graphs

must have isomorphic directed power graphs. As in [14] the proof is split into two cases depending on whether the identity vertex is the only one connected to all other vertices. In what follows, let M be a Moufang loop with power graph Γ.

2.5.1 Non-identity vertex connected to all others.

Lemma 2.26. Suppose that $x \in M$ with $x \neq 1$ and x connected to all other vertices in Γ and p is a prime divisor of $\mathrm{Exp}(M)$. Then M has a unique subgroup P of order p and $P = \langle x^n \rangle$ for some n.

Proof. Let $|x^p| = k$ and $y \in M$ such that $|y| = p$ be given. Since x and y are connected in Γ, either x is a power of y or y is a power of x. Suppose that $y^i = x$ where $1 \leq i < p$ without loss of generality. Then $(p, i) = 1$ and there exists $j \in \mathbb{N}$ such that $(y^i)^j = y = x^j$. Thus every element of Q of order p is a power of x.

Further $1 = y^p = x^{jp} = (x^p)^j$ and so $k \mid j$. Thus $y = x^j = (x^k)^m$ for some $m \in \mathbb{N}$. So every element of order p is contained in $\langle x^k \rangle$, a cyclic subgroup of order p. □

Thus if the power graph of a Moufang p-loop M has a non-identity vertex connected to all others, then M is either cyclic, generalized quaternion or generalized octonion by Theorem 2.2. We now handle the case that M does not have prime power order.

Lemma 2.27. Suppose that $x \in M$ with $x \neq 1$ and x connected to all other vertices in the power graph of M and $|M|$ is not a prime power. Then M is a cyclic group.

Proof. Since M is not a p-loop $\mathrm{Exp}(M)$ is not a prime power [26]. As in the proof of Lemma 2.26 $|x|$ is divisible by every prime divisor of $\mathrm{Exp}(M)$. Since $\mathrm{Exp}(M)$ has at least two distinct prime factors so does $|x|$ and for all $y \in M$ with $|y|$ a prime power we have that y is a power of x. Let $z \in M$ such that $|z|$ is not a prime power be given. If z is a power of x then we are done. We will show that z must be a power of x.

Suppose toward a contradiction that z is not a power of x. Then $x = z^k$ for some k. Say $|z| = p_0^{i_0} \cdots p_m^{i_m}$, where this is a factorization into distinct primes and $m \geq 1$. Then

$z^{p_1^{i_1}\cdots p_m^{i_m}}, \ldots, z^{p_0^{i_0}\cdots p_{m-1}^{i_{m-1}}}$ are all powers of x as elements of M with prime power order. Thus $p_0^{i_0}, \ldots, p_m^{i_m} || x|$ and $|z| || x|$. Then $|x| = |z^k| = \frac{|z|}{\gcd(k,|z|)}$ and $|x| = |z|$. But then $|\langle x \rangle| = |\langle z \rangle|$ while $\langle x \rangle \subsetneq \langle z \rangle$, a contradiction since $|x|$ is finite.

Hence every element of M is a power of x and $M = \langle x \rangle$ is a cyclic group. □

Note that if $|M|$ is not a power of 2, then M is a cyclic group and there is nothing to prove. So suppose that $|M|$ is a power of 2. Recall that the power graph of a cyclic p-group is complete [28]. If the largest complete subgraph in Γ has order 2^{n-2}, then M cannot be cyclic or generalized quaternion, since both of these have complete subgraphs of order at least 2^{n-1} in their power graphs. So in this case M must be generalized octonion. Similarly, if the largest complete subgraph in Γ has order 2^{n-1}, then M must be generalized quaternion. Finally, if Γ is complete, then M is cyclic.

The above shows that if the power graph of M has a non-identity vertex connected to all others, then we can identify M up to isomorphism. So in this case the undirected power graph determines the directed power graph up to isomorphism. We will next handle the case that the power graph of M has no such vertex.

2.5.2 Only identity connected to all others. Note that we have shown that if there is a non-identity vertex connected to all others in Γ, then M is either cyclic, generalized quaternion, or generalized octonion. In each of these cases the directed power graph is determined by the undirected power graph. So proceeding we will assume that M is not cyclic, generalized quaternion, or generalized octonion, and so the only vertex connected to all others in Γ is the identity.

In [14] the proof that the undirected power graph of a group with only the identity vertex connected to all others determines the directed power graph only required power associativity, the inverse property, and the element-wise Lagrange property. Since these properties all hold in Moufang loops the proof in [14] shows that the undirected power

graph of a Moufang loop in which only the identity vertex is connected to all others determines the directed power graph. This completes the proof of Theorem 2.1. We present an outline of the proof in [14] here for completeness.

Proof. Define two equivalence relations on M:

$$x \equiv y \text{ iff the closed neighborhoods of } x \text{ and } y \text{ coincide}$$

$$x \approx y \text{ iff } \langle x \rangle = \langle y \rangle$$

There are several key observations about these relations:

- Elements of $\equiv$-classes are indistinguishable up to graph isomorphism.
- In the directed power graph there are bidirectional arrows between elements of the same $\approx$-class.
- Between two $\approx$-classes either there are no connections or all arrows go the same way.
- A $\approx$-class has size $\phi(n)$, where n is the order of its elements and ϕ is the Euler ϕ function.

The proof proceeds by showing that each $\equiv$-class is a disjoint union of $\approx$-classes of known sizes. Since elements of $\equiv$-classes are indistinguishable up to graph isomorphism we can then partition $\equiv$-classes into $\approx$-classes arbitrarily. But $\equiv$-classes can be recognized with only the undirected power graph, so this reduces the problem to that of deciding which direction arrows between $\approx$-classes point. This is handled by noticing that if two $\approx$-classes have different sizes, then arrows point from the larger to the smaller. If two $\approx$-classes have the same size, then $\phi(m) = \phi(n)$, where m, n are the orders of elements in the respective classes. But this only occurs for ϕ when either $m = n$ or $2m = n$ for m odd. If $m = n$ the classes cannot be joined. In the other case exactly one class is connected to a non-identity

singleton class and arrows go from this class to the other. Thus directions of arrows can be determined using only information from the undirected power graph and the undirected power graph determines the directed. □

Chapter 3: Para-F quasigroups

3.1 Introduction

It has been shown that medial quasigroups are linear over abelian groups and similar results have been shown for semimedial and F-quasigroups. Similarly, paramedial quasigroups have been show to be linear over abelian groups and a similar result has been shown for semiparamedial quasigroups. Our goal in this chapter will be to find the correct definition of para-F quasigroups and prove an analogous linearity result. We will proceed by investigating candidate defining identities for para-F quasigroups, showing that para-F quasigroups are linear over Moufang loops, and finally proving a result analogous to the linearity of F-quasigroups.

3.1.1 Medial and F-quasigroups. We will first present the definitions and linearity results for medial, semimedial, F, paramedial, and semiparamedial quasigroups.

Definition 3.1. A quasigroup $(Q, \cdot)$ is said to be a *medial quasigroup* (or entropic quasigroup) if the following identity holds for all $x, y, u, v \in Q$:

$$xy \cdot uv = xu \cdot yv$$

Theorem 3.2 (Bruck-Murdoch-Toyoda)**.** Every medial quasigroup $(Q, \cdot)$ is linear over an abelian group $(Q, +)$ with the linearity given by

$$x \cdot y = \varphi(x) + \psi(y) + a$$

where $\varphi\psi = \psi\varphi$ [29].

Definition 3.3. A quasigroup $(Q, \cdot)$ is said to be a *semimedial quasigroup* if the following identities hold for all $x, y, z \in Q$:

$$xx \cdot yz = xy \cdot xz$$

$$zy \cdot xx = zx \cdot yx$$

Theorem 3.4. (Barnes, Kinyon) Every semimedial quasigroup $(Q, \cdot)$ is linear over a commutative Moufang loop $(Q, +)$ with the linearity given by

$$x \cdot y = \varphi(x) + (\psi(y) + c)$$

where $\varphi\psi = \psi\varphi$ [30].

Definition 3.5. A quasigroup $(Q, \cdot)$ is said to be an *F-quasigroup* if the following identities hold for all $x, y, z \in Q$:

$$x \cdot yz = xy \cdot (x\backslash x)z$$

$$zy \cdot x = z(x/x) \cdot yx$$

Theorem 3.6. (Kepka, Kinyon, Phillips) Every F-quasigroup $(Q, \cdot)$ is linear over an NK-loop $(Q, +)$ with the linearity given by

$$x \cdot y = \varphi(x) + \psi(y) + e$$

where $\varphi\psi = \psi\varphi$ [11] and $e \in Z(Q, +)$.

Note that since e is in the center, and thus the nucleus, we can omit parentheses from the equation describing the linearity.

Definition 3.7. A quasigroup $(Q, \cdot)$ is said to be a *paramedial quasigroup* if the following identity holds for all $x, y, u, v \in Q$:

$$xy \cdot uv = vy \cdot ux$$

Theorem 3.8 (Kepka-Němec)**.** Every paramedial quasigroup $(Q, \cdot)$ is linear over an abelian group $(Q, +)$ with the linearity given by

$$x \cdot y = \varphi(x) + \psi(y) + g$$

where $\varphi\varphi = \psi\psi$ [29].

Definition 3.9. A quasigroup $(Q, \cdot)$ is said to be a *semiparamedial quasigroup* if the following identities hold for all $x, y, z \in Q$:

$$xx \cdot yz = zx \cdot yx$$

$$zy \cdot xx = xy \cdot xz$$

Theorem 3.10 (Barnes, Kinyon)**.** Every semiparamedial quasigroup $(Q, \cdot)$ is linear over a commutative Moufang loop $(Q, +)$ with the linearity given by

$$x \cdot y = \varphi(x) + (\psi(y) + e)$$

where $\varphi\varphi = \psi\psi$ [30].

The relation between these varieties is shown below.

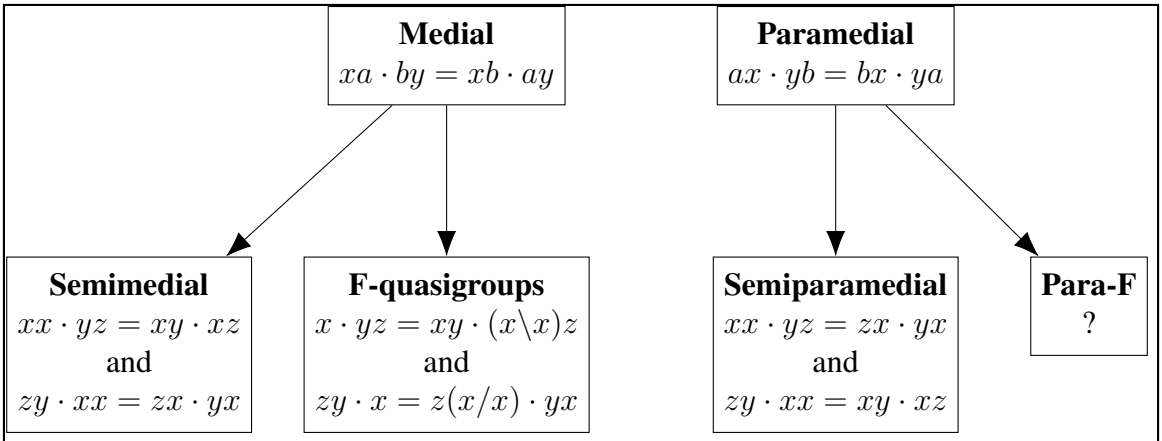

Figure 3.1: Generalizations of medial and paramedial

3.1.2 Candidates for para-F. As suggested by the above diagram we expect there to be a variety arising by weakening the paramedial identity in an analogous way to how the medial identity is weakened to define F-quasigroups. There are two natural ways to weaken the paramedial identity, we will show that each yields a distinct variety. We will now present these varieties and argue that one is the correct definition of para-F.

The first analogue is:

$$x \cdot yz = z(x\backslash x) \cdot yx$$
$$zy \cdot x = xy \cdot (x/x)z$$

We will call quasigroups satisfying these identities quasigroups of type (*).

The other analogue is:

$$x \cdot yz = zx \cdot y(x/x)$$
$$zy \cdot x = (x\backslash x)y \cdot xz$$

We will call quasigroups satisfying these identities quasigroups of type (**).

Proposition 3.11. Let Q be a quasigroup of type (*), then Q is semiparamedial and of type (**).

Proof. This result was proved using Prover9 [31]. The proof can be found in appendix A.2.1. □

This result indicates that the (*) identities are too strong to be an analogue of the F-quasigroup identities. We will take the (**) identities as our defining para-F identities.

Proposition 3.12. Let Q be a quasigroup that is both semiparamedial and of type (**), then Q is of type (*).

Proof. This result was proved using Prover9 [31]. The proof can be found in appendix A.2.2. □

3.1.3 Para-F quasigroups.

Definition 3.13. A quasigroup $(Q, \cdot)$ is said to be a *para-F quasigroup* if the following identities hold for all $x, y, z \in Q$:

$$x \cdot yz = zx \cdot y(x/x)\,, \tag{P1}$$

$$zy \cdot x = (x\backslash x)y \cdot xz\,. \tag{P2}$$

We will call a quasigroup satisfying only equation P1 *left para-F* and a quasigroup satisfying only equation P2 *right para-F*. The following quasigroup is left para-F, but not right para-F. Since these identities are dual this demonstrates that neither implies the other.

$\cdot$	0	1	2	3	4	5	6	7
0	1	0	4	2	5	3	7	6
1	3	2	1	7	0	6	5	4
2	0	6	2	3	4	5	1	7
3	2	4	7	6	1	0	3	5
4	5	3	0	1	6	7	4	2
5	7	1	5	4	3	2	6	0
6	4	5	6	0	7	1	2	3
7	6	7	3	5	2	4	0	1

Table 3.1: A quasigroup which is left but not right para-F

As we will show later in this chapter, para-F quasigroups are antilinear over Moufang loops. We will use this antilinearity to explicitly construct a para-F quasigroup which is not a semiparamedial, semimedial, nor F-quasigroup. Let $D_8 = \langle a, b | a^4 = b^2 = 1, bab^{-1} = a^{-1} \rangle$ and define $\phi, \psi : D_8 \to D_8$ by $\phi(ab) = \psi(ab) = a^3b$, $\phi(a^3b) = \psi(a^3b) = ab$ and ϕ, ψ fix all other elements of D_8. Then ϕ, ψ are antiautomorphisms of D_8. Define a quasigroup $(Q, +)$ by

$$x + y = \phi(x) \cdot \psi(y) \cdot a^2$$

where $\cdot$ is the operation in D_8. This quasigroup is para-F but not semiparamedial, semimedial or F. Its multiplication table is below. Note that $(Q, +)$ is also neither medial nor paramedial since it is neither semimedial nor semiparamedial.

$+$	1	2	3	4	5	6	7	8
1	4	6	7	1	5	2	3	8
2	6	4	8	2	3	1	5	7
3	7	5	1	3	2	8	4	6
4	1	2	3	4	8	6	7	5
5	5	7	6	8	4	3	2	1
6	2	1	5	6	7	4	8	3
7	3	8	4	7	6	5	1	2
8	8	3	2	5	1	7	6	4

Table 3.2: A quasigroup which is para-F but not F, paramedial, nor semimedial

Note that all of the varieties of loops in diagram 3.1, with the exception of para-F quasigroups, have been shown to be linear over varieties of loops. Our goal in this chapter will be to prove an analogous result for para-F quasigroups. We will first show that as in the case of F-quasigroups, all loop isotopes of para-F quasigroups are Moufang. First note that Moufang loops are isotopically invariant, so we need only show that every para-F quasigroup has a Moufang loop isotope.

3.2 Loop isotopes are Moufang

In what follows let $(Q, \cdot)$ be a para-F quasigroup and $x, y, z \in Q$ be universally quantified. We will now prove a series of lemmas which will allow us to prove Theorem 3.27.

Lemma 3.14. $(x/y)\backslash x = y$ for all $x, y \in Q$.

Proof. Substituting $x \mapsto x/y$ into the loop identity $x\backslash(xy) = y$ we have $(x/y)\backslash((x/y) \cdot y) = y$ and so $(x/y)\backslash x = y$. □

Lemma 3.15. $(z \cdot ((y\backslash y)\backslash x)) \cdot y = x \cdot yz$ for all $x, y, z \in Q$.

Proof. Substituting $y \mapsto (y\backslash y)\backslash x$ and $x \mapsto y$ in the para-F identity $(x\backslash x)y \cdot xz = zy \cdot x$ we have that

$$\begin{aligned}(z \cdot ((y\backslash y)\backslash x)) \cdot y &= ((y\backslash y) \cdot ((y\backslash y)\backslash x)) \cdot yz \\ &= x \cdot yz\end{aligned}$$

So $x \cdot yz = (z \cdot ((y\backslash y)\backslash x)) \cdot y$ for all $x, y, z \in Q$. □

Lemma 3.16. $(((x\backslash x) \cdot y) \cdot z)/x = (x\backslash z) \cdot y$

Proof. Substituting $z \mapsto x\backslash z$ into the para-F identity $((x\backslash x) \cdot y) \cdot (x \cdot z) = (z \cdot y) \cdot x$ we have

$$((x\backslash x) \cdot y) \cdot (x \cdot (x\backslash z)) = ((x\backslash z) \cdot y) \cdot x$$

$$((x\backslash x)\cdot y)\cdot z = ((x\backslash z)\cdot y)\cdot x$$

$$(((x\backslash x)\cdot y)\cdot z)/x = (((x\backslash z)\cdot y)\cdot x)/x$$

$$(((x\backslash x)\cdot y)\cdot z)/x = (x\backslash z)\cdot y$$

So $(((x\backslash x)\cdot y)\cdot z)/x = (x\backslash z)\cdot y$ for all $x, y, z \in Q$. □

Lemma 3.17. $x\backslash(y\cdot z) = (z/(x/y))\cdot(y/y)$ for all $x, y, z \in Q$.

Proof. Note that

$$(x\cdot y)\cdot(z\cdot(y/y)) = y\cdot(z\cdot x)$$

$$(x\cdot y)\backslash((x\cdot y)\cdot(z\cdot(y/y))) = (x\cdot y)\backslash(y\cdot(z\cdot x))$$

$$z\cdot(y/y) = (x\cdot y)\backslash(y\cdot(z\cdot x))$$

Substituting $x \leftarrow\!\shortmid\, x/y$ into the above we have

$$z\cdot(y/y) = ((x/y)\cdot y)\backslash(y\cdot(z\cdot(x/y)))$$

$$z\cdot(y/y) = x\backslash(y\cdot(z\cdot(x/y)))$$

Substituting $z \leftarrow\!\shortmid\, z/(x/y)$ into the above we have

$$(z/(x/y))\cdot(y/y) = x\backslash(y\cdot((z/(x/y))\cdot(x/y)))$$

$$(z/(x/y))\cdot(y/y) = x\backslash(y\cdot z)$$

Thus $x\backslash(y\cdot z) = (z/(x/y))\cdot(y/y)$ for all $x, y, z \in Q$. □

Lemma 3.18. $(x\cdot y)/z = ((z/(y/y))\backslash y)\cdot x$ for all $x, y, z \in Q$.

Proof. Note that

$$(x \cdot y) \cdot (z \cdot (y/y)) = y \cdot (z \cdot x)$$
$$((x \cdot y) \cdot (z \cdot (y/y)))/(z \cdot (y/y)) = (y \cdot (z \cdot x))/(z \cdot (y/y))$$
$$x \cdot y = (y \cdot (z \cdot x))/(z \cdot (y/y))$$

Substituting $x \leftarrow\!\shortmid z\backslash y$, $y \leftarrow\!\shortmid x$ into the above we have

$$(z\backslash y) \cdot x = (x \cdot (z \cdot (z\backslash y)))/(z \cdot (y/y))$$
$$(z\backslash y) \cdot x = (x \cdot y)/(z \cdot (y/y))$$

Substituting $z \leftarrow\!\shortmid z/(y/y)$ into the above we have

$$((z/(y/y))\backslash y) \cdot x = (x \cdot y)/((z/(y/y)) \cdot (y/y))$$
$$((z/(y/y))\backslash y) \cdot x = (x \cdot y)/z$$

So $(x \cdot y)/z = ((z/(y/y))\backslash y) \cdot x$ for all $x, y, z \in Q$. □

Lemma 3.19. $(x/x) \cdot ((y\backslash y)\backslash(z \cdot x)) = z \cdot ((y\backslash y)\backslash x)$ for all $x, y, z \in Q$.

Proof. By Lemma 3.15 we have

$$(x \cdot ((y\backslash y)\backslash z)) \cdot y = z \cdot (y \cdot x)$$
$$((x \cdot ((y\backslash y)\backslash z)) \cdot y)/y = (z \cdot (y \cdot x))/y$$
$$x \cdot ((y\backslash y)\backslash z) = (z \cdot (y \cdot x))/y$$

Call this last line †. Substituting $x \leftarrow\!\shortmid x/x$, $z \leftarrow\!\shortmid z \cdot x$ into (*) we have that

$$(x/x) \cdot ((y\backslash y)\backslash(z \cdot x)) = ((z \cdot x) \cdot (y \cdot (x/x)))/y$$

$$(x/x) \cdot ((y\backslash y)\backslash(z \cdot x)) = (x \cdot (y \cdot z))/y$$

Applying † to the right hand side above we have that $(x/x)\cdot((y\backslash y)\backslash(z\cdot x)) = z\cdot((y\backslash y)\backslash x)$.

□

Lemma 3.20. $(x\backslash x)\backslash((y \cdot x)/z) = (x\backslash z)\backslash y$.

Proof. From the para-F identities we have that

$$((x\backslash x) \cdot y) \cdot (x \cdot (x\backslash z)) = ((x\backslash z) \cdot y) \cdot x$$

$$((x\backslash x) \cdot y) \cdot z = ((x\backslash z) \cdot y) \cdot x$$

substituting $y \leftarrow\!\shortmid (x\backslash z)\backslash y$

$$((x\backslash x) \cdot ((x\backslash z)\backslash y)) \cdot z = ((x\backslash z) \cdot ((x\backslash z)\backslash y)) \cdot x$$

$$((x\backslash x) \cdot ((x\backslash z)\backslash y)) \cdot z = y \cdot x$$

$$(((x\backslash x) \cdot ((x\backslash z)\backslash y)) \cdot z)/z = (y \cdot x)/z$$

$$((x\backslash x) \cdot ((x\backslash z)\backslash y)) = (y \cdot x)/z$$

$$(x\backslash x)\backslash(((x\backslash x) \cdot ((x\backslash z)\backslash y))) = (x\backslash x)\backslash((y \cdot x)/z)$$

$$(x\backslash z)\backslash y = (x\backslash x)\backslash((y \cdot x)/z)$$

Thus $(x\backslash z)\backslash y = (x\backslash x)\backslash((y \cdot x)/z)$ for all $x, y, z \in Q$. □

Lemma 3.21. $(x/(y/y))\backslash(z \cdot (x\backslash x)) = x\backslash(z \cdot (y/y))$

Proof. By Lemma 3.18 we have

$$((z/(x/x))\backslash y) \cdot x = (x \cdot y)/z$$

$$(((z/(x/x))\backslash y)\cdot x)/x = ((x\cdot y)/z)/x$$

$$(z/(x/x))\backslash y = ((x\cdot y)/z)/x$$

Call this last line †.

By Lemma 3.16 we have that $(((x\backslash x)\cdot y)\cdot z)/x = (x\backslash z)\cdot y$. Substituting $y \leftarrow\!\shortmid\, x$, $x \leftarrow\!\shortmid\, z$, $z \leftarrow\!\shortmid\, y\cdot(x/x)$ we have

$$(((z\backslash z)\cdot x)\cdot(y\cdot(x/x)))/z = (z\backslash(y\cdot(x/x)))\cdot x$$

$$x\cdot(y\cdot(z\backslash z))/z = (z\backslash(y\cdot(x/x)))\cdot x \text{ from the para-F identities}$$

$$(x\cdot(y\cdot(z\backslash z))/z)/x = ((z\backslash(y\cdot(x/x)))\cdot x)/x$$

$$(x\cdot(y\cdot(z\backslash z))/z)/x = z\backslash(y\cdot(x/x))$$

$$(z/(x/x))\backslash(y\cdot(z\backslash z)) = z\backslash(y\cdot(x/x)) \text{ by †}$$

Thus $(x/(y/y))\backslash(z\cdot(x\backslash x)) = x\backslash(z\cdot(y/y))$ for all $x, y, z \in Q$. □

Proposition 3.22.

$$((x\backslash x)\cdot((y/x)\backslash x))\cdot z = x\cdot(y\backslash(x\cdot z))$$

for all $x, y, z \in Q$.

Proof. Substituting $x \leftarrow\!\shortmid\, z$, $y \leftarrow\!\shortmid\, (y\backslash y)\backslash x$, $z \leftarrow\!\shortmid\, y$ in Lemma 3.16 we have

$$(z\backslash y)\cdot((y\backslash y)\backslash x) = (((z\backslash z)\cdot((y\backslash y)\backslash x)\cdot y))/z$$

$$= (x\cdot(y\cdot(z\backslash z)))/z \text{ by Lemma 3.15}$$

Call this identity (I).

From Lemma 3.18 with $z = z \cdot (x\backslash x)$ we have

$$((x/(y/y))\backslash(z \cdot (x\backslash x))) \cdot y = (y \cdot (z \cdot (x\backslash x)))/x$$
$$= (x\backslash z) \cdot ((z\backslash z)\backslash y) \text{ by (I)}$$

Call this identity (II).

But from Lemma 3.21 we have

$$(x/(z/z))\backslash(y \cdot (x\backslash x)) = x\backslash(y \cdot (z/z))$$
$$((x/(z/z))\backslash(y \cdot (x\backslash x))) \cdot z = (x\backslash(y \cdot (z/z))) \cdot z$$
$$(x\backslash y) \cdot ((y\backslash y)\backslash z) = (x\backslash(y \cdot (z/z))) \cdot z \text{ by (II)}$$

Call this last line (III)

Then from Lemma 3.18 we have

$$((x/(y/y))\backslash(z \cdot (y/y))) \cdot y = (y \cdot (z \cdot (y/y)))/x$$
$$((x/(y/y))\backslash z) \cdot ((z\backslash z)\backslash y) = (y \cdot (z \cdot (y/y)))/x \text{ from (III)}$$

Call this last line (IV)

Substituting $z \leftarrow\!\shortmid (z/(x/x))\backslash y$ in Lemma 3.19 we have

$$(x/x) \cdot ((y\backslash y)\backslash(((z/(x/x))\backslash y) \cdot x)) = ((z/(x/x))\backslash y) \cdot ((y\backslash y)\backslash x)$$
$$(x/x) \cdot ((y\backslash y)\backslash(((z/(x/x))\backslash y) \cdot x)) = (x \cdot (y \cdot (x/x)))/z \text{ from (IV)}$$
$$(x/x) \cdot ((y\backslash y)\backslash((x \cdot y)/z)) = (x \cdot (y \cdot (x/x)))/z \text{ from Lemma 3.18}$$
$$(x/x) \cdot ((y\backslash z)\backslash x) = (x \cdot (y \cdot (x/x)))/z \text{ from Lemma 3.20}$$
$$((x/x) \cdot ((y\backslash z)\backslash x)) \cdot z = ((x \cdot (y \cdot (x/x)))/z) \cdot z$$

$$((x/x)\cdot((y\backslash z)\backslash x))\cdot z = x\cdot(y\cdot(x/x))$$

substituting $y \leftarrow\!\shortmid\, z/y$ we have

$$((x/x)\cdot(((z/y)\backslash z)\backslash x))\cdot z = x\cdot((z/y)\cdot(x/x))$$

$$((x/x)\cdot(y\backslash x))\cdot z = x\cdot((z/y)\cdot(x/x)) \text{ using that } (z/y)\backslash z = y$$

Call this last line (V)

Now consider

$$x\cdot((y/(z/u))\cdot(u/u)) = x\cdot((y/(z/u))\cdot(u/u))$$

$$x\cdot(z\backslash(u\cdot y)) = x\cdot((y/(z/u))\cdot(u/u)) \text{ from Lemma 3.17}$$

$$x\cdot(y\backslash(x\cdot z)) = x\cdot((z/(y/x))\cdot(x/x)) \text{ renaming variables}$$

$$x\cdot(y\backslash(x\cdot z)) = ((x/x)\cdot((y/x)\backslash x))\cdot z \text{ from (V)}$$

So $x\cdot(y\backslash(x\cdot z)) = ((x/x)\cdot((y/x)\backslash x))\cdot z$ for all $x, y, z \in Q$. □

Proposition 3.23.

$$z\cdot((x/(x\backslash y))\cdot(x/x)) = ((z\cdot x)/y)\cdot x$$

for all $x, y, z \in Q$.

Proof. The defining identity of para-F quasigroups is symmetric, so this result follows from Proposition 3.22 by symmetry. □

Lemma 3.24. A loop $(Q, +, 1)$ is left Bol iff for all $x, y \in Q$ there exists $u \in Q$ such that

$$L_x L_y L_x = L_u$$

[30].

This result was shown in [30] and was likely known previously. We present a proof here to make this chapter self contained.

Proof. Suppose first that for all $x, y \in Q$ there exists $u \in Q$ such that $L_x L_y L_x = L_u$. Applying both sides of this equation to 1 we see that $u = x + (y + x)$. Thus

$$\begin{aligned} x + (y + (x + z)) &= L_x L_y L_x(z) \\ &= L_u(z) \\ &= L_{x+(y+x)}(z) \\ &= (x + (y + x)) + z \end{aligned}$$

Thus $(Q, +)$ is left Bol.

Conversely, if Q is left Bol then letting $u = x+(y+x)$ we have $L_x L_y L_x = L_{x+(y+x)} = L_u$ from the defining identity. □

Proposition 3.25. All loop isotopes of a quasigroup $(Q, \cdot)$ are left Bol iff for all $x, y \in Q$ there exists $u \in Q$ such that

$$L_x L_y^{-1} L_x = L_u$$

.

This result was proved in [30]. We present a proof here to make this chapter self contained.

Proof. All translations in this proof will be with respect to the quasigroup operation $\cdot$. Let $(Q, +)$ be a principal loop isotope of $(Q, \cdot)$, where $x + y = (x/a) \cdot (b\backslash y)$. Suppose first that for all $x, y \in Q$ there exists $u \in Q$ such that $L_x L_y^{-1} L_x = L_u$. Note that L_u is a bijection, so for all $x, y \in Q$ there exists $u \in Q$ such that $L_x^{-1} L_y L_x^{-1} = L_u^{-1}$. Consider

$$x + (y + (x + z)) = (x/a) \cdot (b\backslash(y + (x + z)))$$

$$
\begin{aligned}
&= (x/a) \cdot (b\backslash((y/a) \cdot (b\backslash(x+z)))) \\
&= (x/a) \cdot (b\backslash((y/a) \cdot (b\backslash((x/a) \cdot (b\backslash z))))) \\
&= (x/a) \cdot L_b^{-1} L_{y/a} L_b^{-1}((x/a) \cdot (b\backslash z)) \\
&= (x/a) \cdot L_{u_1}^{-1}((x/a) \cdot (b\backslash z)) \text{ for some } u_1 \in Q \\
&= L_{x/a} L_{u_1}^{-1} L_{x/a}(b\backslash z) \\
&= L_{u_2}(b\backslash z) \\
&= u_2 a + z
\end{aligned}
$$

Thus by Lemma 3.24 $(Q, +)$ is a left Bol loop and all loop isotopes of $(Q, \cdot)$ are left Bol.

Now suppose that all loop isotopes of $(Q, \cdot)$ are left Bol and let $(Q, +)$ have the operation $v + w = v \cdot (y\backslash w)$. Then for all $x, y, z \in Q$ we have

$$
\begin{aligned}
x + (y + (x + z)) &= (x + (y + x)) + z \\
x \cdot (y\backslash(y \cdot (y\backslash(x \cdot (y\backslash z))))) &= (x + (y + x)) + z \\
x \cdot (y\backslash(x \cdot (y\backslash z))) &= (x + (y + x)) \cdot (y\backslash z) \\
x \cdot (y\backslash(x \cdot z)) &= (x + (y + x)) \cdot z \; z \hookleftarrow yz \\
L_x L_y^{-1} L_x(z) &= L_{x+(y+x)}(z) \\
L_x L_y^{-1} L_x &= L_u
\end{aligned}
$$

So for all $x, y \in Q$ there exists $u \in Q$ such that $L_x L_y^{-1} L_x = L_u$ and the proof is complete.

□

Corollary 3.26. All loop isotopes of a quasigroup $(Q, \cdot)$ are right Bol iff for all $x, y \in Q$ there exists $u \in Q$ such that

$$R_x R_y^{-1} R_x = R_u$$

Proof. Dual to Proposition 3.25. □

Theorem 3.27. Every loop isotope of a para-F quasigroup is Moufang.

Proof. Note that Proposition 3.22 shows that in a para-F quasigroup $(Q, \cdot)$ we have that for all $x, y \in Q$ there exists $u \in Q$ such that $L_x L_y^{-1} L_x = L_u$. Thus by Proposition 3.25 all loop isotopes of a para-F quasigroup are left Bol. Dually, by Propositions 3.23 and 3.26 we have that all loop isotopes of a para-F quasigroup are right Bol. Thus all loop isotopes of a para-F quasigroup are Moufang. □

3.3 Para-F quasigroups are antilinear over Moufang loops

While para-F quasigroups are not linear over loops in general, they are antilinear over Moufang loops, which is an analogous property.

Definition 3.28. A quasigroup $(Q, \cdot)$ is *antilinear* over a loop $(Q, +)$ if there exists f, g antiautomorphisms of $(Q, +)$, $c \in Q$ such that

$$x \cdot y = f(x) + (g(y) + c)$$

for all $x, y \in Q$.

With this result we can prove an analogue to the linearity results in section 3.1 for para-F quasigroups.

Theorem 3.29. Every para-F quasigroup $(Q, \cdot)$ is antilinear over a Moufang loop $(Q, +)$ with the antilinearity given by

$$x \cdot y = \varphi(x) + \psi(y) + c$$

where $c \in Z((Q, +))$ and φ, ψ are antiautomorphisms.

Proof. This result was proved using Prover9. We will present an outline of the proof here. Suppose that $(Q, \cdot)$ is a para-F quasigroup and for all $u \in Q$ define:

$$x +_u y = (x/(u\backslash u)) \cdot ((u/u)\backslash y)$$

From Theorem 3.27 we have that $(Q, +_u)$ is a Moufang loop with identity $1_u = (u/u) \cdot (u\backslash u)$ for all $u \in Q$. Expressing $\cdot$ in terms of $+_u$ we have that

$$\begin{aligned} x +_u y &= (x/(u\backslash u)) \cdot ((u/u)\backslash y) \\ x \cdot y &= x(u\backslash u) +_u (u/u)y \\ x \cdot y &= (f_u(x) +_u A_u) +_u (B_u +_u g_u(y)) \end{aligned}$$

Set

$$\begin{aligned} f_u(x) &= x(u\backslash u) -_u 1_u(u\backslash u) \\ g_u(y) &= -_u(u/u)1_u +_u (u/u)y \\ A_u &= 1_u(u\backslash u) \\ B_u &= (u/u)1_u \end{aligned}$$

So that $f_u(1_u) = g_u(1_u) = 1_u$. We define $C_u = A_u + B_u$ and use Prover9 to prove the following sequence of results:

1. $1_{u \cdot u} = C_u$
2. A_u, B_u, C_u are in the commutant of $(Q, +_u)$
3. $(x +_x y) +_x z = x +_x (y +_x z)$
4. $A_u, B_u \in \text{Nuc}(Q, +_u)$

5. $A_u +_y x = x +_y A_u$

6. $B_u +_y x = x +_y B_u$

7. $1_u +_y x = x +_y 1_u$

8. $f_y(x) +_y f_y(z) = f_y(z +_y x)$

9. $g_y(x) +_y g_y(z) = g_y(z +_y x)$

Thus

$$x \cdot y = f(x) + C + g(y)$$

where $C \in Z(Q, +)$ and f, g are antiautomorphisms.

Note that steps 5, 6, and 7 above make use of our approach of considering all loop isotopes of $(Q, \cdot)$ of the form $(Q, +_u)$ simultaneously. These steps seem to be key in allowing Prover9 to find proofs of 8 and 9. □

With this result all of the varieties of quasigroups in diagram 3.2 have been shown to be linear or antilinear over varieties of Moufang loops.

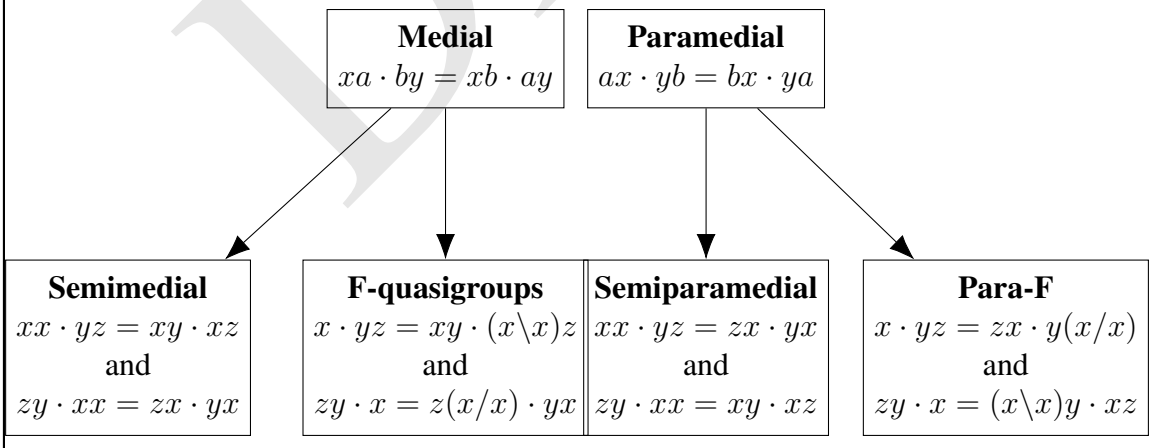

Figure 3.2: Generalizations of medial and paramedial with para-F

3.4 Para-FG quasigroups

It is shown in [32] that the collection of F-quasigroups which are isotopic to groups (called *FG-quasigroups*) form a variety characterized by two identities. We will now show that a similar result holds for para-F quasigroups.

Definition 3.30. A *para-FG quasigroup* is a para-F quasigroup which is isotopic to a group.

Note that all loop isotopes of a para-FG quasigroup must be groups.

Theorem 3.31. A quasigroup is para-FG iff it satisfies the following two identities

$$(x/x)y \cdot zu = uy \cdot z(x/x) \tag{FG1}$$

$$xy \cdot z(u\backslash u) = (u\backslash u)y \cdot zx \tag{FG2}$$

Lemma 3.32. Let $(Q, \cdot)$ be a quasigroup satisfying FG1 and FG2. Then $(Q, \cdot)$ satisfies

$$y(x/((y\backslash y)\backslash z)) = z\backslash(xy)$$

Proof. By FG2 we have $(x\backslash x)y \cdot zu = uy \cdot z(x\backslash x)$. Consider

$$\begin{aligned}
(x\backslash x)y \cdot xz &= zy \cdot x && \text{substituting } u \leftarrow\!\shortmid z, z \leftarrow\!\shortmid x \\
x \cdot yz &= z((y\backslash y)\backslash x) \cdot y && \text{substituting } y \leftarrow\!\shortmid (y\backslash y)\backslash x, x \leftarrow\!\shortmid y \\
z \cdot y(x/((y\backslash y)\backslash z)) &= xy && \text{substituting } x \leftarrow\!\shortmid z, z \leftarrow\!\shortmid x/((y\backslash y)\backslash z) \\
y(x/((y\backslash y)\backslash z)) &= z\backslash(xy) && \text{left dividing by z}
\end{aligned}$$

So the proof is complete. □

Lemma 3.33. Let $(Q, \cdot)$ be a quasigroup satisfying FG1 and FG2. Then $(Q, \cdot)$ satisfies

$$x\backslash y = (z/(y/x)) \cdot ((y/(u\backslash(xz)))/x)$$

Proof. By FG1 we have $(x/x)y \cdot zu = uy \cdot z(x/x)$. Consider

$$\begin{aligned}
x \cdot yz &= zx \cdot y(x/x) && \text{substituting } y \leftarrow\!\shortmid x,\ z \leftarrow\!\shortmid y,\ u \leftarrow\!\shortmid z \\
(zx)\backslash(x \cdot yz) &= y(x/x) && \text{left dividing by } zx \\
x\backslash(y \cdot z(x/y)) &= z(y/y) && \text{substituting } z \leftarrow\!\shortmid x/y, x \leftarrow\!\shortmid y, y \leftarrow\!\shortmid z \\
x\backslash(yz) &= (z/(x/y)) \cdot (y/y) && \text{substituting } z \leftarrow\!\shortmid z/(x/y) \qquad \text{(I)}
\end{aligned}$$

Again using FG1 we have

$$\begin{aligned}
x \cdot yz &= zx \cdot y(x/x) && \text{substituting } y \leftarrow\!\shortmid x, z \leftarrow\!\shortmid y, u \leftarrow\!\shortmid z \\
z \cdot y(x/z) &= x \cdot y(z/z) && \text{substituting } z \leftarrow\!\shortmid y, y \leftarrow\!\shortmid z, x \leftarrow\!\shortmid x/z \\
z\backslash(x \cdot y(z/z)) &= y(x/z) && \text{left dividing by } z \\
x\backslash y &= z \cdot ((y/(z \cdot (x/x)))/x) && \text{substituting } z \leftarrow\!\shortmid x, y \leftarrow\!\shortmid z, x \leftarrow\!\shortmid y/(z \cdot (x/x)) \\
x\backslash y &= (z/(y/x)) \cdot ((y/((z/(y/x)) \cdot (x/x)))/x) && \text{substituting } z \leftarrow\!\shortmid z/(u/x) \\
x\backslash y &= (z/(y/x)) \cdot ((y/(u\backslash(xz)))/x) && \text{by I}
\end{aligned}$$

So the proof is complete. □

Lemma 3.34. Let $(Q, \cdot)$ be a quasigroup satisfying FG1 and FG2. Then $(Q, \cdot)$ satisfies

$$((xy)/(z/z)) \cdot u = x \cdot ((yz)/(u\backslash z))$$

Proof. From FG1 we have

$$\begin{aligned}
x \cdot yz &= zx \cdot y(x/x) && \text{substituting } y \leftarrow\!\shortmid x, z \leftarrow\!\shortmid y, u \leftarrow\!\shortmid z \qquad \text{(I)} \\
z \cdot y(x/z) &= x \cdot y(z/z) && \text{substituting } x \leftarrow\!\shortmid z, z \leftarrow\!\shortmid x/z \qquad \text{(II)}
\end{aligned}$$

$$(x/x)y \cdot zu = x \cdot z((uy)/x) \text{ applying II to FG1} \quad \text{(III)}$$

Further

$$\begin{aligned}
xy \cdot z &= y \cdot (z/(y/y))x && \text{substituting } x \leftarrow\!\shortmid y, y \leftarrow\!\shortmid z/(y/y), z \leftarrow\!\shortmid x \text{ in I} \\
y(x/z) &= z\backslash(x \cdot y(z/z)) && \text{left dividing by } z \text{ in II} \\
x\backslash((x/x)y \cdot z) &= (z/(y/y)) \cdot (y/x) && \text{from the preceding two lines} \\
x\backslash(x \cdot y((zu)/x)) &= ((yz)/(u/u)) \cdot (u/x) && \text{from III} \\
y \cdot ((zu)/x) &= ((yz)/(u/u)) \cdot (u/x) \\
x \cdot ((yz)/(u\backslash z)) &= ((xy)/(z/z)) \cdot u && \text{substituting } x \leftarrow\!\shortmid u\backslash z, y \leftarrow\!\shortmid x, z \leftarrow\!\shortmid y, u \leftarrow\!\shortmid z
\end{aligned}$$

So the proof is complete. □

Lemma 3.35. Let $(Q, \cdot)$ be a quasigroup satisfying FG1 and FG2. Then $(Q, \cdot)$ satisfies

$$z \cdot (y\backslash((u/w) \cdot x)) = ((z \cdot (y\backslash u))/w) \cdot x$$

Proof. By FG1 we have $(x/x)y \cdot zu = uy \cdot z(x/x)$. Consider

$$\begin{aligned}
x \cdot yz &= (z \cdot ((u/u)\backslash x)) \cdot y(u/u) \\
&\qquad \text{substituting } x \leftarrow\!\shortmid u, y \leftarrow\!\shortmid (u/u)\backslash x, z \leftarrow\!\shortmid y, u \leftarrow\!\shortmid z \\
(z \cdot ((u/u)\backslash x)) \cdot y(u/u) &= x \cdot yz \\
(x \cdot ((y/y)\backslash z)) \cdot u &= z \cdot (u/(y/y))x \\
&\qquad \text{substituting } z \leftarrow\!\shortmid x, x \leftarrow\!\shortmid z, u \leftarrow\!\shortmid y, y \leftarrow\!\shortmid u/(y/y) \quad \text{(I)} \\
x \cdot ((y/y)\backslash z) &= (z \cdot (u/(y/y))x)/u \text{ right dividing by } u \\
(z \cdot (u/(y/y))x)/u &= x \cdot ((y/y)\backslash z)
\end{aligned}$$

$$(x \cdot (u/(y/y))((z/(y\backslash(yu)))/y))/u = ((z/(y\backslash(yu)))/y) \cdot ((y/y)\backslash x)$$

substituting $z \leftarrow\!\shortmid x, x \leftarrow\!\shortmid (z/(y\backslash(yu)))/y$

$$(x \cdot (y\backslash z))/u = ((z/(y\backslash(yu)))/y) \cdot ((y/y)\backslash x) \text{ by Lemma 3.33}$$

$$(x \cdot (y\backslash z))/u = ((z/u)/y) \cdot ((y/y)\backslash x) \quad \text{(II)}$$

Call this last line †. Note that by FG2 we have $(x\backslash x)y \cdot zu = uy \cdot z(x\backslash x)$. Consider

$$(x\backslash x)y \cdot xz = zy \cdot x \quad \text{substituting } u \leftarrow\!\shortmid z, z \leftarrow\!\shortmid x$$

$$(x\backslash x)((y/y)\backslash z) \cdot x((u/w)/y) = ((u/w)/y)((y/y)\backslash z) \cdot x$$

substituting $y \leftarrow\!\shortmid (y/y)\backslash z, z \leftarrow\!\shortmid (u/w)/y$

$$(x\backslash x)((y/y)\backslash z) \cdot x((u/w)/y) = ((z \cdot (y\backslash u))/w) \cdot x \quad \text{by II}$$

$$z \cdot (((x \cdot ((u/w)/y))/(y/y)) \cdot (x\backslash x)) = ((z \cdot (y\backslash u))/w) \cdot x \quad \text{by I}$$

$$z \cdot (x \cdot ((((u/w)/y) \cdot y)/((x\backslash x)\backslash y))) = ((z \cdot (y\backslash u))/w) \cdot x \quad \text{by Lemma 3.34}$$

$$z \cdot (x \cdot ((u/w)/((x\backslash x)\backslash y))) = ((z \cdot (y\backslash u))/w) \cdot x$$

$$z \cdot (y\backslash((u/w) \cdot x)) = ((z \cdot (y\backslash u))/w) \cdot x \quad \text{by Lemma 3.32}$$

□

In what follows let $(Q, \cdot)$ be a para-FG quasigroup and define $x +_{u,v} y = (x/u) \cdot (v\backslash y)$.

Lemma 3.36. $(Q, \cdot)$ satisfies

$$x \cdot (y\backslash(z +_{w,y} u)) = (x \cdot (y\backslash z)) +_{w,y} y$$

Proof. Consider

$$(xw +_{w,y} z) +_{w,y} u = xw +_{w,y} (z +_{w,y} u) \text{ by associativity of } +_{w,y}$$

$$(x \cdot (y\backslash z)) +_{w,y} u = x \cdot (y\backslash(z +_{w,y} u)) \quad \text{by definition of } +_{w,y}$$

So the proof is complete. □

Lemma 3.37. $(Q, \cdot)$ satisfies

$$x \cdot (y +_{x/x,u} z) = (u\backslash z)x \cdot y$$

Proof. Since Q is para-F we have

$$\begin{aligned} xy \cdot z(y\backslash y) &= y \cdot zx \\ xy \cdot z &= y \cdot (z/(y/y))x \text{ substituting } z \leftarrow\!\shortmid z/(y/y) \\ (u\backslash z)x \cdot y &= x \cdot (y +_{x/x,u} z) \text{ substituting } x \leftarrow\!\shortmid u\backslash z, y \leftarrow\!\shortmid x, x \leftarrow\!\shortmid y \end{aligned}$$

So the proof is complete. □

Lemma 3.38. $(Q, \cdot)$ satisfies

$$(xy)/(yz) = (y\backslash y) \cdot (z\backslash x)$$

Proof. Since $(Q, \cdot)$ is para-F we have

$$\begin{aligned} (x\backslash x)y \cdot xz &= zy \cdot x \\ (x\backslash x) \cdot y &= (zy \cdot x)/(xz) \text{ right dividing by } xz \\ (y\backslash y) \cdot (z\backslash x) &= (xy)/(yz) \quad \text{substituting } x \leftarrow\!\shortmid y, y \leftarrow\!\shortmid z\backslash x \end{aligned}$$

So the proof is complete. □

Lemma 3.39. $(Q, \cdot)$ satisfies

$$(z/(x/x))\backslash y = ((xy)/z)/x$$

Proof. From the proof of Lemma 3.37 we have

$$\begin{aligned}
x \cdot (y/(x/x))z &= zx \cdot y \\
xy &= ((z/(x/x))\backslash y)x \cdot z \text{ substituting } y \leftarrow\!\shortmid z, z \leftarrow\!\shortmid (z/(x/x))\backslash y \\
(xy)/z &= ((z/(x/x))\backslash y) \cdot x \quad \text{right dividing by } z \\
((xy)/z)/x &= (z/(x/x))\backslash y \qquad \text{right dividing by } x
\end{aligned}$$

So the proof is complete. □

Lemma 3.40. $(Q, \cdot)$ satisfies

$$x +_{z,v_6} (v_5 +_{w,(u+_{w,v_6}v_5)/w} z) = x +_{z,u/w} y$$

Proof. Consider

$$\begin{aligned}
x +_{z,u} (y +_{z,u} w) &= (x +_{z,u} y) +_{z,u} w \\
x +_{z,u} (y +_{z,u} uw) &= ((x +_{z,u} y)/z) \cdot w \text{ substituting } w \leftarrow\!\shortmid uw \\
x +_{z,u} ((y/z) \cdot w) &= ((x +_{z,u} y)/z) \cdot w \\
x +_{z,u} ((y/z) \cdot (((x +_{z,u} y)/z)\backslash w)) &= w \qquad \text{substituting } w \leftarrow\!\shortmid ((x +_{z,u} y)/z)\backslash w \\
x +_{z,u} (y +_{z,(x+_{z,u}y)/z} w) &= w \qquad \text{(I)}
\end{aligned}$$

Further

$$x +_{y,z} u = (x/y) \cdot (z\backslash u)$$

$$(x/y)\backslash(x +_{y,z} u) = z\backslash u \qquad \text{left dividing by } x/y$$

$$x +_{y,w/v_5} (w +_{v_5,z} u) = (x/y) \cdot (z\backslash u) \text{ by definition of } +_{w,v_5}$$

$$x +_{y,w/v_5} (w +_{v_5,z} u) = x +_{y,z} u$$

$$x +_{z,v_6} (v_5 +_{w,(u+_{w,v_6}v_5)/w} z) = x +_{z,u/w} y \qquad \text{by I}$$

So the proof is complete. □

Lemma 3.41. $(Q, \cdot)$ satisfies

$$x +_{z\backslash(uw),z} y = x +_{w,u} y$$

Proof. Consider

$$\begin{aligned} x +_{z\backslash(uw),z} y &= (x/(z\backslash(uw))) \cdot (z\backslash y) \\ &= (x/w) \cdot (u\backslash y) \text{ substituting } z \leftarrow\!\shortmid u \\ &= x +_{w,u} y \end{aligned}$$

So the proof is complete. □

Lemma 3.42. $(Q, \cdot)$ satisfies FG2.

Proof. From I in the proof of Lemma 3.40 we have

$$x +_{u,w} (y +_{u,(x+_{u,w}y)/u} z) = z$$

$$(x \cdot (y\backslash u)) +_{v_5,y} (w +_{v_5,(u+_{v_5,y}z)/v_5} z) = x \cdot (y\backslash z) \qquad \text{applying the abo}$$

$$(x \cdot (y\backslash u)) +_{v_5,u/v_5} z = x \cdot (y\backslash z) \qquad \text{by Lemma 3.40}$$

$$x +_{z,u/z} y = (x/(w\backslash u)) \cdot (w\backslash y)$$

substituting $x \leftarrow\!\shortmid x/(w\backslash u), y \leftarrow\!\shortmid w, z \leftarrow\!\shortmid y, v_5 \leftarrow\!\shortmid z$

$$x +_{z,u/z} y = x +_{w\backslash u,w} y$$

$$((w/(x/x))\backslash z)x \cdot y = x \cdot (y +_{u\backslash w,u} z)$$

applying the above to Lemma 3.32

$$(((x \cdot z)/w)/x)x \cdot y = x \cdot (y +_{u\backslash w,u} z) \qquad \text{by Lemma 3.39}$$

$$((x \cdot z)/w) \cdot y = x \cdot (y +_{u\backslash w,u} z)$$

$$(z\backslash z)(w\backslash x) \cdot y = x \cdot (y +_{u\backslash (z\cdot w),u} z) \qquad \text{by Lemma 3.33}$$

$$(x\backslash x)(y\backslash z) \cdot u = z \cdot (u +_{y,x} x) \qquad \text{by Lemma 3.41}$$

$$(x\backslash x)y \cdot z = uy \cdot (z +_{u,x} x)$$

substituting $y \leftarrow\!\shortmid u, z \leftarrow\!\shortmid uy, u \leftarrow\!\shortmid z$

$$(x\backslash x)y \cdot zu = uy \cdot z(x\backslash x)$$

So $(Q, \cdot)$ satisfies FG2 and the proof is complete. □

Proof of Theorem 3.31. First suppose that $(Q, \cdot)$ satisfies FG1 and FG2. It is immediate that $(Q, \cdot)$ is para-F. Further, by Lemma 3.35 we have

$$z \cdot (y\backslash((u/y) \cdot x)) = ((z \cdot (y\backslash u))/y) \cdot x$$

$$zy +_{y,y} (u/y)x = ((zy +_{y,y} u)/y) \cdot x$$

$$zy +_{y,y} (u +_{y,y} yx) = (zy +_{y,y} u) +_{y,y} yx$$

Thus $(Q, +_{y,y})$ is a group and $(Q, \cdot)$ is a para-FG quasigroup.

Now suppose that $(Q, \cdot)$ is a para-FG quasigroup. Lemma 3.42 shows that $(Q, \cdot)$ satisfies FG2. The proof that $(Q, \cdot)$ satisfies FG1 is dual. So $(Q, \cdot)$ is a para-FG quasigroup iff it satisfies FG1 and FG2. □

Theorem 3.43. Every para-FG quasigroup $(Q, \cdot)$ is antilinear over a group $(Q, +)$ with the antilinearity given by

$$x \cdot y = f(x) + g(y) + c$$

where f, g are antiautmorphisms of $(Q, +)$ and $c \in Z((Q, +))$.

Proof. Let $(Q, \cdot)$ be a para-FG quasigroup. Then by Theorem 3.29 there exists a Moufang loop $(Q, +)$, antiautomorphisms $f, g : (Q, +) \to (Q, +)$, and $c \in Z(Q)$ such that

$$x \cdot y = f(x) + (g(y) + c)$$

. By an analogous proof to that of Proposition 1.38 $(Q, \cdot)$ is isotopic to $(Q, +)$. But $(Q, \cdot)$ is a para-FG quasigroup and so isotopic to some group $(Q, *)$. But then $(Q, *)$ and $(Q, +)$ are isotopic and $(Q, +)$ must be a group. Thus $(Q, \cdot)$ is antilinear over a group $(Q, +)$ as desired. □

Chapter 4: Solvability for loops

4.1 Introduction

Many properties from universal algebra have equivalent definitions specific to the context of groups. This leads to the natural question: under what conditions can these group definitions be extended to loops? In particular, we will be interested in the definitions of nilpotence and solvability for groups.

Definition 4.1. Let A be a universal algebra. $\phi \subseteq A \times A$ is a *congruence* on A iff

1. ϕ is an equivalence relation.
2. For each n-ary operation f of A $a_1 \phi a_1' \ldots a_n \phi a_n'$ implies $f(a_1, \ldots, a_n) \phi f(a_1', \ldots a_n')$.

Definition 4.2. Let G be a group and $N \leq G$. N is *normal* in G ($N \trianglelefteq G$) if and only if $xNx^{-1} = N$ for all $x \in G$.

Remark. The only non-trivial inner mappings of a group G are T_x for $x \in G$, so this is a special case of the definition of a normal subloop.

Fact 4.3. Let G be a group, then:

1. For every congruence ϕ on G there exists $N \trianglelefteq G$ such that $x \phi y$ iff $xy^{-1} \in N$.
2. For $N \trianglelefteq G$ the relation $x \phi y$ iff $xy^{-1} \in N$ is a congruence [33]

We now present some universal algebraic definitions and their equivalent definitions in the context of groups. We will closely follow the definitions given in [34] for the universal algebraic definitions.

Definition 4.4. Let A be a universal algebra and α, β, δ be congruences on A. Then α *centralizes* β *over* δ if for every $(n+1)$-ary term operation t, every pair $a\alpha b$ and every $u_1\beta v_1, \ldots, u_n\beta v_n$ we have

$$t(a, u_1, \ldots, u_n)\delta t(a, v_1, \ldots, v_n) \text{ implies } t(b, u_1, \ldots, u_n)\delta t(b, v_1, \ldots v_n)$$

Definition 4.5. Let A be a universal algebra and α, β be congruences on A. Then the *congruence (universal algebraic) commutator* of α and β is $[\alpha, \beta]_C = \delta$, where δ is the smallest congruence such that α centralizes β over δ.

Smallest here is in terms of the lattice of congruences of A with largest element $1_A = A \times A$ and smallest element $0_A = \{(a, a) : a \in A\}$.

Definition 4.6. Let G be a group and $H, K \trianglelefteq G$. Then the *classical (group theoretic) commutator* of H and K is $[H, K] = \langle [x, y] : x \in H, y \in K \rangle$.

Definition 4.7. An algebra A is *(congruence) nilpotent* if $\gamma_{(n)} = 0_A$ for some n, where

$$\gamma_{(0)} = 1_A, \quad \gamma_{(i+1)} = [\gamma_{(i)}, 1_A]_C$$

.

Definition 4.8. A loop L with identity 1 is *(classically) nilpotent* if $L_n = \{1\}$ for some n, where

$$L_0 = L, \quad L_{i+1} = [L_i, L]$$

.

Definition 4.9. An algebra A is *(congruence) solvable* if $\gamma^{(n)} = 0_A$ for some n, where

$$\gamma^{(0)} = 1_A, \quad \gamma^{(i+1)} = [\gamma^{(i)}, \gamma^{(i)}]_C$$

.

Definition 4.10. A loop L with identity 1 is *(classically) solvable* if $L^n = \{1\}$ for some n, where

$$L^0 = L, \quad L^{i+1} = [L^i, L^i]$$

.

Fact 4.11. Classical and congruence normality, nilpotency, and solvability coincide in groups [34].

Fact 4.12. Classical and congruence nilpotency coincide in loops [34].

Fact 4.13. Classical and congruence solvability do not coincide in loops. [34].

Our goal in this chapter will be to find conditions under which these definitions of solvability do coincide for loops. The main result of this chapter is the following theorem providing a sufficient condition for classical and congruence solvability degrees to coincide:

Theorem 4.14. If $Q/\mathrm{Nuc}(Q)$ is an abelian group, then classical and congruence solvability degrees of Q coincide.

Weakening our assumption on Q we are no longer able to show that classical and congruence solvability degrees coincide, but we do obtain the following result about $\mathrm{Inn}^*(Q)$:

Theorem 4.15. If $Q/\mathrm{Nuc}(Q)$ is a group, then $\mathrm{Inn}^*(Q)$ is abelian.

4.2 $Q/\mathrm{Nuc}(Q)$ an abelian group

We will now show that if $Q/\mathrm{Nuc}(Q)$ is an abelian group, then the classical and congruence definitions of solvability coincide. Denote the classical commutator of two normal subloops $A, B \trianglelefteq Q$ by $[A, B]$ and the congruence commutator by $[A, B]_C$.

Lemma 4.16. Let Q be a loop such that $Q/\text{Nuc}(Q)$ is an abelian group. Then for all $x, y \in Q$ we have that $[x, y]\backslash 1 = [y, x]$.

Proof. Let $x, y \in Q$ be given and consider

$$\begin{aligned} L_{xy,[x,y]}([x, y]\backslash 1) &= (xy \cdot [x, y])\backslash(xy \cdot ([x, y] \cdot ([x, y]\backslash 1))) \\ &= (xy \cdot [x, y])\backslash(xy)) \\ &= (xy \cdot ((xy)\backslash(yx)))\backslash(xy) \\ &= (yx)\backslash(xy) \\ &= [y, x] \end{aligned}$$

But on the other hand since $[x, y] \in \text{Nuc}(Q)$ we have that

$$\begin{aligned} L_{xy,[x,y]}([x, y]\backslash 1) &= (xy \cdot [x, y])\backslash(xy \cdot ([x, y] \cdot ([x, y]\backslash 1))) \\ &= (xy \cdot [x, y])\backslash((xy \cdot [x, y]) \cdot ([x, y]\backslash 1)) \\ &= [x, y]\backslash 1 \end{aligned}$$

Thus $[x, y]\backslash 1 = [y, x]$. □

Lemma 4.17. Let Q be a loop such that $Q/\text{Nuc}(Q)$ is an abelian group. Then for all $u, v, a \in Q$ we have $[u, a] \cdot (1/[v, a]) = [u, a]/[v, a]$.

Proof. Let $u, v, a \in Q$ be given and note that $[u, a], [v, a] \in \text{Nuc}(Q)$ since $Q' \subseteq \text{Nuc}(Q)$. Then

$$\begin{aligned} [u, a] &= [u, a] \\ [u, a] \cdot 1 &= [u, a] \\ [u, a] \cdot (1/[v, a])[v, a] &= [u, a] \end{aligned}$$

$$[u,a](1/[v,a]) \cdot [v,a] = [u,a] \text{ since } [u,a] \in \text{Nuc}(Q)$$

$$[u,a](1/[v,a]) = [u,a]/[v,a]$$

as desired. □

Lemma 4.18. Let Q be a loop such that $Q/\text{Nuc}(Q)$ is an abelian group. Then $x \cdot [y,z] = x/[z,y]$ for all $x, y, z \in Q$.

Proof. Let $x, y, z \in Q$ be given and consider

$$\begin{aligned} x/(L_{x,[y,z]}([y,z]\backslash 0)) &= x/([y,z]\backslash 0) \text{ since } [y,z] \in \text{Nuc}(Q) \\ &= x/[z,y] \qquad \text{by Lemma 4.16.} \end{aligned}$$

But on the other hand we have that

$$\begin{aligned} x/(L_{x,[y,z]}([y,z]\backslash 1)) &= x/((x \cdot [y,z])\backslash(x \cdot ([y,z] \cdot ([y,z]\backslash 1)))) \\ &= x/((x \cdot [y,z])\backslash x) \\ &= x \cdot [y,z] \end{aligned}$$

Thus $x/[z,y] = x \cdot [y,z]$. □

Theorem 4.19. Let Q be a loop such that $Q/\text{Nuc}(Q)$ is an abelian group. Then classical and congruence solvability degrees of Q coincide.

Proof. We will show by induction that the derived series are equal. First note that $[Q,Q]_C = [Q,Q]$ so our base case holds [34]. We will show that given $H \trianglelefteq Q$ with $H \subseteq [Q,Q]$ we have that $[H,H] = [H,H]_C$ to complete the proof.

From [34] and [35] we have that $[H,H]_C = Ng(W_{\bar{u}}(a)/W_{\bar{v}}(b) : W \in \mathcal{W}, a, u/v \in H)$, where $\mathcal{W}$ is a generating set for Inn(Q). We will take $\mathcal{W} = \{T_x, L_{x,y}, R_{x,y} : x, y \in$

$Q\}$ as our generating set. Further, from [7] we have that $T_x(y) = [x, y] \cdot y$. Finally, since $Q/\text{Nuc}(Q)$ is an abelian group we have that $[Q, Q] \subseteq \text{Nuc}(Q)$ and in particular all commutators are in the nucleus.

We will first show that $[H, H] \subseteq [H, H]_C$. Let $x, y \in H$ be given. Then $[x, y] = T_x(y)/y = T_x(y)/T_1(y) \in [H, H]_C$. Thus $[H, H]_C$ contains all generators of $[H, H]$ and $[H, H] \subseteq [H, H]_C$.

We will now show that $[H, H]_C \subseteq [H, H]$. Let $u_1, v_1, u_2, v_2, a \in Q$ such that $u_1/v_1, u_2/v_2, a \in H$ be given. Note that $L_{u_1,u_2}(a) = L_{v_1,v_2}(a) = R_{u_1,u_2}(a) = R_{v_1,v_2}(a) = 1$ since $a \in H \subseteq \text{Nuc}(Q)$. So we need only consider $T \in \mathcal{W}$. Consider

$$\begin{aligned}
T_{u_1}(a)/T_{v_1}(a) &= ([u_1, a] \cdot a)/([v_1, a] \cdot a) \\
&= [u_1, a](a/([v_1, a] \cdot a)) && \text{since } [u_1, a] \in \text{Nuc}(Q) \\
&= [u_1, a]((a/a)(1/[v_1, a])) && \text{since } [v_1, a] \in \text{Nuc}(Q) \\
&= [u_1, a](1/[v_1, a]) \\
&= [u_1, a]/[v_1, a] && \text{by Lemma 4.17} \\
&= [u_1, a] \cdot [a, v_1] && \text{by Lemma 4.18} \\
&\in [H, H]
\end{aligned}$$

So $[H, H]_C \subseteq [H, H]$ and $[H, H]_C = [H, H]$. Thus the derived series are equal by induction. □

4.3 $Q/\text{Nuc}(Q)$ a group

Define $\text{Inn}^*(Q) = \langle L_{x,y}, R_{x,y}, M_{x,y} | x, y \in Q \rangle$. Intuitively inner mappings measure the failure of elements to associate or commute, where M, L, R measure associativity and T measures commutativity. With this intuition, the group $\text{Inn}^*(Q)$ is the group of all inner mappings measuring associativity.

Define

$$[x,y,z]_R = x\backslash R_{z,y}(x)$$

$$[x,y,z]_L = z\backslash L_{x,y}(z)$$

$$[x,y,z]_M = y\backslash M_{z,x}(y)$$

Note that we could analogously define $[x,z]_T = z\backslash T_y(z)$ and recover the standard commutator. In what follows let $(Q,\cdot,1)$ be a loop and $x,y,z \in Q$ be arbitrary.

Lemma 4.20. For any $n \in \text{Nuc}(Q)$ $L_{x,y}(zn) = L_{x,y}(z)\cdot n$ and $R_{x,y}(nz) = n \cdot R_{x,y}(z)$.

Proof. These are both immediate from the fact that $n \in \text{Nuc}(Q)$ and the definitions of $L_{x,y}, R_{x,y}$. □

We will follow the argument proving Lemma 4.2 in [36] to show that $[x,y,nz]_M = [x,y,z]_M$ for any $n \in \text{Nuc}(Q)$.

Lemma 4.21. $[nx,y,z]_M = [x,y,z]_M$ for $n \in \text{Nuc}(Q)$.

Proof. This is immediate from the fact that $n \in \text{Nuc}(Q)$ and the definition of $[x,y,z]_M$. □

Lemma 4.22. $[yn,z,x]_M = [y,nz,x]_M$ for $n \in \text{Nuc}(Q)$.

Proof. First note that $M_{x,y}(z)\backslash(y\backslash(yz\cdot x) = x$ by Lemma 3.14. Further $(n\backslash a)/(b\backslash a) = n\backslash b$ since $n \in \text{Nuc}(Q)$. So

$$\begin{aligned}(n\backslash(y\backslash(yz\cdot x)))/x &= (n\backslash(y\backslash(yz\cdot x)))/(M_{x,y}(z)\backslash(y\backslash(yz\cdot x)))\\ &= n\backslash M_{x,y}(z)\end{aligned}$$

Thus $(n\backslash(y\backslash(yz\cdot x)))/x = n\backslash M_{x,y}(z)$, call this †.

Further, since $n \in \text{Nuc}(Q)$ we have that $M_{x,yn}(z) = ((yn)\backslash((yn \cdot z) \cdot x))/x = ((yn)\backslash((y \cdot nz) \cdot x))/x$. Then

$$\begin{aligned} M_{x,yn}(z) &= ((yn)\backslash((y \cdot nz) \cdot x))/x \\ &= (n\backslash(y\backslash((y \cdot nz) \cdot x)))/x \end{aligned}$$

But by † we have that

$$\begin{aligned} M_{x,yn}(z) &= (n\backslash(y\backslash((y \cdot nz) \cdot x)))/x \\ &= n\backslash M_{x,y}(nz) \end{aligned}$$

So

$$\begin{aligned} z\backslash M_{x,yn}(z) &= z\backslash(n\backslash M_{x,y}(nz)) \\ z\backslash M_{x,yn}(z) &= (nz)\backslash M_{x,y}(nz) \text{ since } n \in \text{Nuc}(Q) \\ [yn, z, x]_M &= [y, nz, x]_M \end{aligned}$$

□

Lemma 4.23. If $\text{Nuc}(Q)$ is normal in Q, then $[y, nz, x]_M = [y, z, x]_M$.

Proof. This is immediate from the preceding two lemmas and the fact that since $\text{Nuc}(Q) \trianglelefteq Q$ we have $yn = n'y$ for some $n' \in \text{Nuc}(Q)$. □

Corollary 4.24. If $Q/\text{Nuc}(Q)$ is a group, then $M_{x,y}(nz) = n \cdot M_{x,y}(z)$ for $n \in \text{Nuc}(Q)$

Proof. Consider

$$M_{x,y}(nz) = nz \cdot [y, nz, x]_M$$

$$= nz \cdot [y, z, x]_M \text{ by Lemma 4.23}$$
$$= n \cdot z[y, z, x]_M$$
$$= n \cdot M_{x,y}(z)$$

□

Now define

$$[x, y, z]_{R'} = R_{z,y}(x)/x$$
$$[x, y, z]_{L'} = L_{x,y}(z)/z$$
$$[x, y, z]_{M'} = M_{z,x}(y)/y$$

Theorem 4.25. If $Q/\text{Nuc}(Q)$ is a group, then $\text{Inn}^*(Q)$ is abelian.

Proof. First note that all 6 of the associators defined above lie in the associator subloop, which is a subloop of the nucleus by assumption. Further by [7] Lemma 2.6 these associators commute. We will show that the generators of $\text{Inn}^*(Q)$ commute.

Consider

$$\begin{aligned}
M_{x,y}(M_{u,v}(z)) &= M_{x,y}([v, z, u]_{M'} \cdot z) \\
&= [v, z, u]_{M'} \cdot M_{x,y}(z) \qquad \text{by Corollary 4.24} \\
&= [v, z, u]_{M'} \cdot [y, z, x]_{M'} z \\
&= [y, z, x]_{M'} \cdot [v, z, u]_{M'} z \text{ as noted above} \\
&= [y, z, x]_{M'} \cdot M_{u,v}(z) \\
&= M_{u,v}([y, z, x]_{M'} z) \qquad \text{by Corollary 4.24} \\
&= M_{u,v}(M_{x,y}(z))
\end{aligned}$$

Further

$$\begin{aligned} L_{x,y}(M_{u,v}(z)) &= L_{x,y}(z[v,z,u]_M) \\ &= L_{x,y}(z) \cdot [v,z,u]_M \qquad \text{by Lemma 4.20} \\ &= [x,y,z]_{L'} z \cdot [v,z,u]_M \\ &= [x,y,z]_{L'} \cdot z[v,z,u]_M \\ &= [x,y,z]_{L'} \cdot M_{u,v}(z) \\ &= M_{u,v}([x,y,z]_{L'} z) \qquad \text{by Corollary 4.24} \\ &= M_{u,v}(L_{x,y}(z)) \end{aligned}$$

Next consider

$$\begin{aligned} R_{x,y}(M_{u,v}(z)) &= R_{x,y}([v,z,u]_{M'} z) \\ &= [v,z,u]_{M'} \cdot R_{x,y}(z) \qquad \text{by Lemma 4.20} \\ &= [v,z,u]_{M'} \cdot [z,y,x]_{R'} z \\ &= [z,y,x]_{R'} \cdot [v,z,u]_{M'} z \\ &= [z,y,x]_{R'} \cdot M_{u,v}(z) \\ &= M_{u,v}([z,y,x]_{R'} z) \qquad \text{by Corollary 4.24} \\ &= M_{u,v}(R_{x,y}(z)) \end{aligned}$$

Now consider

$$\begin{aligned} L_{x,y}(R_{u,v}(z)) &= L_{x,y}(z[z,v,u]_R) \\ &= L_{x,y}(z) \cdot [z,v,u]_R \qquad \text{by Lemma 4.20} \\ &= [x,y,z]_{L'} z \cdot [z,v,u]_R \end{aligned}$$

$$
\begin{aligned}
&= [x,y,z]_{L'} \cdot z[z,v,u]_R \\
&= [x,y,z]_{L'} \cdot R_{u,v}(z) \\
&= R_{u,v}([x,y,z]_{L'} z) \qquad \text{by Lemma 4.20} \\
&= R_{u,v}(L_{x,y}(z))
\end{aligned}
$$

Next

$$
\begin{aligned}
L_{x,y}(L_{u,v}(z)) &= L_{x,y}(z[u,v,z]_L) \\
&= L_{x,y}(z) \cdot [u,v,z]_L \qquad \text{by Lemma 4.20} \\
&= z[x,y,z]_L \cdot [u,v,z]_L \\
&= z[u,v,z]_L \cdot [x,y,z]_L \\
&= L_{u,v}(z) \cdot [x,y,z]_L \\
&= L_{u,v}(z[x,y,z]_L) \qquad \text{by Lemma 4.20} \\
&= L_{u,v}(L_{x,y}(z))
\end{aligned}
$$

Finally

$$
\begin{aligned}
R_{x,y}(R_{u,v}(z)) &= R_{x,y}([z,v,u]_{R'} z) \\
&= [z,v,u]_{R'} \cdot R_{x,y}(z) \qquad \text{by Lemma 4.20} \\
&= [z,v,u]_{R'} \cdot [z,y,x]_{R'} z \\
&= [z,y,x]_{R'} \cdot [z,v,u]_{R'} z \\
&= [z,y,x]_{R'} \cdot R_{u,v}(z) \\
&= R_{u,v}([z,y,x]_{R'} z) \qquad \text{by Lemma 4.20} \\
&= R_{u,v}(R_{x,y}(z))
\end{aligned}
$$

Thus all the generators of $\text{Inn}^*(Q)$ commute and $\text{Inn}^*(Q)$ is an abelian group. □

4.4 Further results

We will now present some further results dealing providing sufficient conditions for right inner mappings to commute.

4.4.1 Inverses preserved by right inner mappings.

Definition 4.26. Let $(Q, \cdot, 1)$ be a loop. A map $\phi : Q \to Q$ *preserves inverses* if

$$\phi(0/x) = 0/\phi(x)$$

for all $x \in Q$.

Theorem 4.27. Let Q be a loop such that right inner mappings preserve inverses and suppose that associators are in the left and middle nuclei. Then right inner mappings commute.

Proof. This result was proved using Prover9 [31]. The proof can be found in appendix A.3.1. □

4.4.2 Right automorphic.

Theorem 4.28. Let Q be a right automorphic loop and suppose that associators are in the left nucleus. Then right inner mappings commute.

Proof.

$$\begin{aligned} R_{u,v}(R_{x,y}(z)) &= R_{u,v}(R_{x,y}(R_{u,v}(z) \cdot R_{u,v}(z)\backslash z)) \\ &= R_{u,v}(R_{x,y}(R_{u,v}(z) \cdot R_{x,y}(R_{u,v}(z)\backslash z))) \\ &\quad \text{since } R_{x,y} \text{ is an automorphism} \\ &= R_{u,v}(R_{x,y}(R_{u,v}(z)) \cdot (R_{u,v}(z)\backslash z)) \end{aligned}$$

since $R_{u,v}(z)\backslash z$ is in the associator subloop and thus the left nucleus

$= R_{u,v}([R_{u,v}(z), x, y]R_{u,v}(z) \cdot (R_{u,v}(z)\backslash z))$

definition of $[\cdot, \cdot, \cdot]$

$= R_{u,v}([R_{u,v}(z), x, y] \cdot R_{u,v}(z)(R_{u,v}(z)\backslash z))$

associators in left nucleus

$= R_{u,v}([R_{u,v}(z), x, y]z)$

$= [R_{u,v}(z), x, y]R_{u,v}(z)$

$R_{u,v}$ is an automorphism

$= R_{x,y}(R_{u,v}(z))$

definition of $[\cdot, \cdot, \cdot]$

□

Below is a right automorphic loop with center $\{1, 2\}$, so $Q/\{1, 2\}$ is an abelian group (being of order 4). It is not an RCC loop. This shows that a right automorphic in which all associators lie in left nucleus need not be RCC. Thus the previous result is not a statement solely about RCC loops.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	7	8	5	6
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	8	7	2	1	4	3
7	7	8	5	6	4	3	2	1
8	8	7	6	5	3	4	1	2

Table 4.1: $Q/Z(Q)$ an abelian group and Q not RCC

4.4.3 Left nucleus and commutant.

Theorem 4.29. Suppose that all associators are in the left nucleus and the commutant. Then right inner mappings commute.

Proof. Note that since we assume all associators are in the left nucleus and commutant we are free to use whichever associator we choose. For this proof define the associator to be $[x, y, z] = R_{x,y}(z)/z$ and let $x, y, z, u, w \in Q$ be given. Then

$$\begin{aligned}
R_{x,y}(R_{z,u}(w)) &= R_{x,y}([z, u, w]w) \\
&= [z, u, w]R_{x,y}(w) \qquad \text{associators in } \mathrm{Nuc}_l(Q) \\
&= [z, u, w][x, y, w] \cdot w \\
&= [x, y, w][z, u, w] \cdot w \text{ associators in commutant} \\
&= [x, y, w]R_{z,u}(w) \\
&= R_{z,u}([x, y, w]w) \qquad \text{associators in } \mathrm{Nuc}_l(Q) \\
&= R_{z,u}(R_{x,y}(w))
\end{aligned}$$

Thus $R_{x,y}R_{z,u} = R_{z,u}R_{x,y}$ and $\mathrm{Inn}_R(Q)$ is abelian. □

4.5 Counterexamples

4.5.1 Inn(Q). Theorem 4.25 does not directly extend to all of $\mathrm{Inn}(Q)$. The following is the CC loop of order 6 (there is only one) and in any CC loop $Q/\mathrm{Nuc}(Q)$ is an abelian group. But in this loop the T's do not commute with the R's and in particular $\mathrm{Inn}^*(Q)$ is not abelian.

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	5	0	4
2	2	4	5	1	3	0
3	3	0	4	2	5	1
4	4	5	1	0	2	3
5	5	3	0	4	1	2

Table 4.2: $Q/\mathrm{Nuc}(Q)$ an abelian group but $R_{x,y}T_z \neq T_z R_{x,y}$

$R_{1,1}(T_1(1)) = 3$, while $T_1(R_{1,1}(1)) = 4$. There is an example in the same loop of T's not commuting with each other as well.

4.5.2 Left and middle nuclei. Theorem 4.28 does not directly extend to arbitrary loops. The following is a loop in which the left and middle nuclei coincide, are normal, and are isomorphic to S_3. The factor by the left (equivalently middle) nucleus is Z_4, so every associator and commutator is in the left and middle nuclei. However, the right inner mapping group is $S_3 \times S_3 \times S_3$. So associators and commutators in left and middle nuclei is not sufficient for right inner mappings to commute.

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15	18	17	20	19	22	21	24	23
3	3	5	1	6	2	4	9	11	7	12	8	10	15	17	13	18	14	16	21	23	19	24	20	22
4	4	6	2	5	1	3	10	12	8	11	7	9	16	18	14	17	13	15	22	24	20	23	19	21
5	5	3	6	1	4	2	11	9	12	7	10	8	17	15	18	13	16	14	23	21	24	19	22	20
6	6	4	5	2	3	1	12	10	11	8	9	7	18	16	17	14	15	13	24	22	23	20	21	19
7	7	8	9	10	11	12	19	20	21	22	23	24	1	2	3	4	5	6	13	14	15	16	17	18
8	8	7	10	9	12	11	20	19	22	21	24	23	2	1	4	3	6	5	14	13	16	15	18	17
9	9	11	7	12	8	10	21	23	19	24	20	22	3	5	1	6	2	4	15	17	13	18	14	16
10	10	12	8	11	7	9	22	24	20	23	19	21	4	6	2	5	1	3	16	18	14	17	13	15
11	11	9	12	7	10	8	23	21	24	19	22	20	5	3	6	1	4	2	17	15	18	13	16	14
12	12	10	11	8	9	7	24	22	23	20	21	19	6	4	5	2	3	1	18	16	17	14	15	13
13	13	14	15	16	17	18	1	2	3	4	5	6	19	20	21	22	23	24	7	8	9	10	11	12
14	14	13	16	15	18	17	2	1	4	3	6	5	20	19	22	21	24	23	8	7	10	9	12	11
15	15	17	13	18	14	16	3	5	1	6	2	4	21	23	19	24	20	22	9	11	7	12	8	10
16	16	18	14	17	13	15	4	6	2	5	1	3	22	24	20	23	19	21	10	12	8	11	7	9
17	17	15	18	13	16	14	5	3	6	1	4	2	23	21	24	19	22	20	11	9	12	7	10	8
18	18	16	17	14	15	13	6	4	5	2	3	1	24	22	23	20	21	19	12	10	11	8	9	7
19	19	20	21	22	23	24	13	14	15	16	17	18	7	8	9	10	11	12	2	1	5	6	3	4
20	20	19	22	21	24	23	14	13	16	15	18	17	8	7	10	9	12	11	1	2	6	5	4	3
21	21	23	19	24	20	22	15	17	13	18	14	16	9	11	7	12	8	10	5	3	2	4	1	6
22	22	24	20	23	19	21	16	18	14	17	13	15	10	12	8	11	7	9	6	4	1	3	2	5
23	23	21	24	19	22	20	17	15	18	13	16	14	11	9	12	7	10	8	3	5	4	2	6	1
24	24	22	23	20	21	19	18	16	17	14	15	13	12	10	11	8	9	7	4	6	3	1	5	2

Table 4.3: Associators and commutators in left and middle nuclei but Inn_R not abelian

Chapter 5: Cosets in Moufang loops

5.1 Introduction

It has been shown that Lagrange's Theorem holds in Moufang loops [10]. However, the proof relies on the classification of finite simple Moufang loops, which in turn relies on the classification of finite simple groups. The proof of Lagrange's Theorem for groups is much simpler because it uses the fact that cosets of a subgroup are a uniform partition of the group. In general, the cosets of a subloop of a Moufang loop need not partition the loop. However, based on extensive computational evidence (all Moufang loops of orders ≤ 64, 81, and 243 checked [37]) we make the following conjecture:

Conjecture 5.1. Let M be a Moufang loop, $S \leq M$ and $\mathcal{S}$ the family of all left cosets of S. Then there exists $A \subset S$ such that A is a partition of M.

That is, in Moufang loops there is always a subset of the family of all left cosets of a subloop which do partition the loop. Proving this conjecture would provide a proof of Lagrange's Theorem for Moufang loops very similar to that for groups. In particular, such a proof would be direct in the sense that it would not rely on the classification of finite simple Moufang loops. We were ultimately unsuccessful, but each of our attempts did yield results which are interesting in their own rights.

We will begin by attempting to directly construct such a uniform partition of cosets directly by proving results on the intersections of distinct cosets and the existence of disjoint cosets. When this approach does not prove fruitful we will try other approaches to proving Lagrange's Theorem for Moufang loops directly by constructing a partition of the loop with each block having order a multiple of the order of the subloop.

We will first define an equivalence relation on Q analogous to the natural equivalence relation of coset membership in groups. This has the advantage of providing us with a partition of Q, meaning we would need only show that each block of the partition has order a multiple of the order of the subloop.

Finally, we will consider orbits of the relative left multiplication groups of S in Q. These orbits are a different generalization of the definition of cosets in groups to the context of loops. This strategy again has the advantage of providing us with a partition of the loop, reducing the problem to that of showing that the order of each orbit is a multiple of the order of the subloop.

5.2 Coset intersections

5.2.1 A first Approach. Let G be a group with $S \leq G$ and $x \in xS \cap yS$. Since left cosets of S partition G, it is immediate that $xS = yS$ and $x^{-1}(xS \cap yS) = x^{-1}xS = S \leq G$. So in particular, $x^{-1}(xS \cap yS) \leq Q$. The question of whether this result can be extended to Moufang loops, that is: "If Q is Moufang and $x \in xS \cap yS$, is $x^{-1}(xS \cap yS)$ a subloop of S?" was posed in [38]. We are able to provide a negative answer:

Let

$$Q = \text{MoufangLoop}(48, 2) \text{ in the GAP LOOPS package},$$
$$S = \{1, 4, 8, 16, 25, 28, 32, 40\},$$
$$x = 3,$$
$$y = 27$$

Then $x \in yS$ (and so $x \in xS \cap yS$), but $x^{-1}(xS \cap yS)$ is not a subloop of S. In fact the subloop generated by $x^{-1}(xS \cap yS)$ is all of Q.

Further, there is in general no translation of $xS \cap yS$ which is a subloop. Let Q be the Moufang loop in the table below,

$$S = \{1, 2, 3, 5, 13, 14, 15, 17\},$$

$$X = 4S \cap 6S = \{16, 18, 19, 21\}$$

Then $S \leq Q$ but there is no $x \in Q$ such that $xX \leq Q$.

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	2	1	5	6	3	4	9	10	7	8	12	11	17	15	14	24	13	23	22	21	20	19	18	16
3	3	5	1	7	2	9	4	11	6	12	8	10	15	17	13	19	14	21	16	23	18	24	20	22
4	4	10	7	8	12	2	11	1	5	6	3	9	16	18	19	20	21	22	23	13	24	14	15	17
5	5	3	2	9	1	7	6	12	4	11	10	8	14	13	17	22	15	20	24	18	23	16	21	19
6	6	8	9	10	11	1	12	2	3	4	5	7	21	19	18	17	16	15	14	24	13	23	22	20
7	7	12	4	11	10	5	8	3	2	9	1	6	19	21	16	23	18	24	20	15	22	17	13	14
8	8	6	11	1	9	10	3	4	12	2	7	5	20	22	23	13	24	14	15	16	17	18	19	21
9	9	11	6	12	8	3	10	5	1	7	2	4	18	16	21	14	19	13	17	22	15	20	24	23
10	10	4	12	2	7	8	5	6	11	1	9	3	24	23	22	21	20	19	18	17	16	15	14	13
11	11	9	8	3	6	12	1	7	10	5	4	2	23	24	20	15	22	17	13	19	14	21	16	18
12	12	7	10	5	4	11	2	9	8	3	6	1	22	20	24	18	23	16	21	14	19	13	17	15
13	13	17	15	20	14	21	23	16	18	24	19	22	1	5	3	8	2	9	11	4	6	12	7	10
14	14	15	17	22	13	19	24	18	16	23	21	20	5	1	2	9	3	8	6	12	11	4	10	7
15	15	14	13	23	17	18	20	19	21	22	16	24	3	2	1	11	5	6	8	7	9	10	4	12
16	16	24	19	13	22	17	15	20	14	21	23	18	4	9	7	1	6	12	3	8	10	5	11	2
17	17	13	14	24	15	16	22	21	19	20	18	23	2	3	5	6	1	11	9	10	8	7	12	4
18	18	23	21	14	20	15	17	22	13	19	24	16	9	4	6	12	7	1	10	5	3	8	2	11
19	19	22	16	15	24	14	13	23	17	18	20	21	7	6	4	3	9	10	1	11	12	2	8	5
20	20	21	23	16	18	24	19	13	22	17	15	14	8	12	11	4	10	5	7	1	2	9	3	6
21	21	20	18	17	23	13	14	24	15	16	22	19	6	7	9	10	4	3	12	2	1	11	5	8
22	22	19	24	18	16	23	21	14	20	15	17	13	12	8	10	5	11	4	2	9	7	1	6	3
23	23	18	20	19	21	22	16	15	24	14	13	17	11	10	8	7	12	2	4	3	5	6	1	9
24	24	16	22	21	19	20	18	17	23	13	14	15	10	11	12	2	8	7	5	6	4	3	9	1

Table 5.1: Moufang loop with an intersection of cosets which cannot be translated to a subloop

5.2.2 An iterative approach. Our next approach was to attempt to iteratively construct a set of cosets partitioning the loop. The following series of lemmas provide restrictions on the intersections of distinct cosets and guarantee the existence of cosets disjoint from given sets.

Lemma 5.2. Let Q be a Moufang loop. Then for all $x, y, z \in Q$

$$xy \cdot (z \cdot xy) = x \cdot (yz \cdot xy)$$

Proof. Let $x, y, z \in Q$ be given and consider

$$\begin{aligned}
xy \cdot (z \cdot xy) &= (xy \cdot (z \cdot xy))y^{-1} \cdot y \\
&= ((xy \cdot z) \cdot xy)y^{-1} \cdot y && \text{since } Q \text{ is diassociative} \\
&= (xy \cdot (z \cdot (xy \cdot y^{-1}))) \cdot y && \text{since } Q \text{ is Moufang} \\
&= (xy \cdot zx) \cdot y \\
&= x(yz \cdot x) \cdot y && \text{since } Q \text{ is Moufang} \\
&= (x \cdot yz)x \cdot y && \text{since } Q \text{ is diassociative} \\
&= x \cdot (yz \cdot xy) && \text{since } Q \text{ is Moufang}
\end{aligned}$$

So $xy \cdot (z \cdot xy) = x \cdot (yz \cdot xy)$ as desired. □

Proposition 5.3. Let Q be a Moufang loop with $S \leq Q$. If $x \in Sy \cap Sz$ with $y \neq z$, then $xy^{-1} \cdot z \in Sy \cap Sz$. Further $x \neq xy^{-1} \cdot z$.

This result tells us that cosets in a Moufang loop cannot intersect in a single element. If two cosets have nontrivial intersection, then the intersection must contain at least two distinct elements.

Proof. Note that $(yx^{-1}) \cdot (xz^{-1})(yx^{-1}) \in S$ since $xy^{-1}, xz^{-1} \in S$ and S is closed under inversion. Then

$$y \cdot (x^{-1} \cdot xz^{-1})(yx^{-1}) \in S \text{ by Lemma 5.2}$$

$$y \cdot z^{-1}(yx^{-1}) \in S$$

$$(y \cdot z^{-1}(yx^{-1}))^{-1} \in S$$

$$(xy^{-1})z \cdot y^{-1} \in S$$

Thus $xy^{-1} \cdot z \in Sy$. Further $xy^{-1} \in S$, so $xy^{-1} \cdot z \in Sz$. So $xy^{-1} \cdot z \in Sy \cap Sz$ as desired.

Finally, note that if $x = xy^{-1} \cdot z$, then $xz^{-1} = xy^{-1}$ and $y = z$, a contradiction. So $x \neq xy^{-1} \cdot z$. □

Proposition 5.4. Let Q be a Moufang loop, $S \leq Q$, and $x \in Q$ such that x^k is the least power of x contained in S. Then $S, Sx, Sx^2, \ldots, Sx^{k-1}$ are disjoint cosets of S.

Proof. Suppose toward a contradiction that $y \in Sx^i \cap Sx^j$ for some $i < j < k$. Then there exist $s, s' \in S$ such that $sx^i = s'x^j$. So

$$\begin{aligned} sx^i &= s'x^j \\ s &= s'x^j \cdot x^{-i} && \text{since } Q \text{ is an IP loop} \\ s &= s'x^{j-i} && \text{since } Q \text{ is diassociative} \\ (s')^{-1}s &= x^{j-i} \end{aligned}$$

But S is a subloop, so in particular $x^{j-i} \in S$. But this contradicts our assumption that x^k is the least power of x contained in S. Thus $S, Sx, \ldots, Sx^{k-1}$ are disjoint. □

Lemma 5.5. Let Q be a Moufang loop and $x, y, z \in Q$ be given. Then

$$(u(yz)^{-1} \cdot x^{-1})(xy \cdot z(yu)^{-1}) = y^{-1}\,.$$

Proof. We have

$$xy \cdot z(yu)^{-1} = (xy \cdot z(yu)^{-1})y \cdot y^{-1} \qquad \text{by the IP}$$

$$
\begin{aligned}
&= x(yz \cdot (yu)^{-1}y) \cdot y^{-1} && \text{since } Q \text{ is Moufang} \\
&= x(yz \cdot (u^{-1}y^{-1} \cdot y)) \cdot y^{-1} && \text{by the IP} \\
&= x(yz \cdot u^{-1}) \cdot y^{-1} && \text{by the IP} \\
&= (u(yz)^{-1} \cdot x^{-1})^{-1} \cdot y^{-1} && \text{by the IP.}
\end{aligned}
$$

Multiplying both sides on the left by $u(yz)^{-1} \cdot x^{-1}$ and using the IP, we have the desired result. □

Lemma 5.6. Let Q be a Moufang loop, let $S \leq Q$, and let $a \in Q - S$ satisfy $a^2 \in S$. The following are equivalent.

1. $Q = S \cup Sa$;
2. For every $x \in Q$, if $x \notin S$, then $Sx \cap Sa \neq \emptyset$.

Proof. Assume (1) holds and assume $x \in Q - S$. Then $x \in Sx \cap Sa$, and so $Sx \cap Sa \neq \emptyset$.

Conversely, assume (2) holds. Then for each $u \in Q - S$, there exists $u' \in Su \cap Sa$, and so $u'u^{-1}, u'a^{-1}, u(u')^{-1}, a(u')^{-1} \in S$. Let $x \in Q \setminus S$ be given.

For all $y \in Q - S$, we have

$$(y'a^{-1} \cdot x'a^{-1})^{-1} \cdot y'y^{-1} \in S\,. \tag{5.1}$$

Set $y = a^2(x')^{-1}a$ and suppose $y \in Q - S$. We have

$$
\begin{aligned}
y'y^{-1} &= y'(a^2(x')^{-1}a)^{-1} \\
&= y'(a^{-1}x'a^{-2}) && \text{by the IP} \\
&= y'(a^{-1} \cdot x'a^{-1} \cdot a^{-1}) && \text{by diassociativity} \\
&= (y'a^{-1} \cdot x'a^{-1})a^{-1} && \text{since } Q \text{ is Moufang.}
\end{aligned}
$$

Thus by (5.1) and the IP,

$$(y'a^{-1} \cdot x'a^{-1})^{-1} \cdot (y'a^{-1} \cdot x'a^{-1})a^{-1} = a^{-1} \in S\,.$$

This contradicts the assumption that $a \notin S$, and so we must have $a^2(x')^{-1}a \in S$. Since $a^2 \in S$ and hence $a^{-2} \in S$, we use the IP again to get $(x')^{-1}a \in S$. Therefore

$$a^{-1}x' \in S\,. \tag{5.2}$$

Next, for all $y \in Q - S$, we have

$$y(y')^{-1} \cdot (y'a^{-1} \cdot x'x^{-1}) \in S\,. \tag{5.3}$$

Set $y = ax \cdot (a^{-1}x')^{-1}$. If $y \notin S$, then using (5.3) and the IP, we have

$$(ax \cdot (a^{-1}x')^{-1})(y')^{-1} \cdot (y'a^{-1} \cdot x'(a^{-1} \cdot ax)^{-1}) \in S\,.$$

By Lemma 5.5 this implies $a^{-1} \in S$, and so $a \in S$. This is a contradiction, and so we must have

$$ax \cdot (a^{-1}x')^{-1} \in S\,. \tag{5.4}$$

Finally, by (5.2), (5.4) and the IP, we obtain $ax \in S$. Thus $x \in a^{-1}S$ and so $x^{-1} \in Sa$.

We have proven that for all $x \in Q - S$, $x^{-1} \in Sa$. Since $x \in Q \setminus S$ implies $x^{-1} \in Q \setminus S$, we conclude that for all $x \in Q \setminus S$, $x \in Sa$. It follows that $Q = S \cup Sa$, that is, (1) holds. □

Proposition 5.7. Let Q be a Moufang loop, $S < Q$, and assume there exists $a \in Q - S$ such that $S \cup Sa \subsetneq Q$. Then there exists $b \in Q$ such that $Sb \cap S = Sb \cap Sa = \emptyset$.

Proof. Assume first that $a^2 \notin S$. Then by Proposition 5.4 we may take $b = a^2$. Now assume $a^2 \in S$. If no such b exists, then for all $x \in Q$, $Sx \cap S \neq \emptyset$ or $Sx \cap Sa \neq \emptyset$. Note that $Sx \cap S \neq \emptyset$ if and only if $x \in S$. Thus for all $x \in Q$, if $x \notin S$, then $Sx \cap Sa \neq \emptyset$. By Lemma 5.6 $Q = S \cup Sa$, contradicting our assumption. □

Lemma 5.8. Let Q be a commutative Moufang loop and $x, y, z \in Q$ be given. Then

$$z \cdot (y \cdot x^3) = x \cdot (x \cdot (yz \cdot x))$$

Proof. Let $x, y, z \in Q$ be given. Then

$$\begin{aligned} x \cdot (x \cdot (yz \cdot x)) &= x \cdot (xy \cdot zx), \text{ since } Q \text{ is Moufang} \\ &= x \cdot (xy \cdot xz), \text{ since } Q \text{ is commutative} \\ &= (x \cdot xy)x \cdot z, \text{ since } Q \text{ is Moufang} \\ &= (x^3 \cdot y) \cdot z \quad \text{, since } Q \text{ is diassociative and commutative} \\ &= z \cdot (y \cdot x^3) \quad \text{, since } Q \text{ is commutative} \end{aligned}$$

So the proof is complete. □

Lemma 5.9. Let Q be a commutative Moufang loop and $S \leq Q$ such that $x^2 \in S$ for all $x \in Q$. Then $S \trianglelefteq Q$.

Proof. First note that since Q is commutative $T_y(x) = x$ and $R_{y,z}(x) = L_{y,x}(x)$. So it is sufficient to show that for all $x \in S$, $y, z \in Q$ $L_{y,z}(x) \in S$. Suppose toward a contradiction that there exist $c_1 \in S$, $c_2, c_3 \in Q$ such that $L_{c_2,c_3}(c_1) \notin S$. Then

$$\begin{aligned} x \cdot c_1 x &\in S, \text{ since } x^2 \in S \text{ for all } x \in Q \\ (x \cdot c_1 x) \cdot y^2 &\in S \end{aligned}$$

$$
\begin{aligned}
(xc_1 \cdot x) \cdot y^2 &\in S \\
x \cdot (c_1 \cdot (x \cdot y^2)) &\in S, \text{ since } Q \text{ is Moufang} \\
x \cdot (c_1 \cdot (y \cdot xy)) &\in S, \text{ since } Q \text{ is commutative and diassociative} \\
x^{-1} \cdot (c_1 \cdot (y \cdot xy)) &\in S, \text{ since } x^{-2} \in S \\
(xy)^{-1} \cdot (c_1 \cdot (c_1 \cdot (xy \cdot c_1))) &\in S, \text{ substituting } x \leftarrow\!\shortmid xy,\ y \leftarrow\!\shortmid c_1 \\
(xy)^{-1} \cdot (x \cdot (y \cdot c_1^3)) &\in S, \text{ by Lemma 5.8} \\
L_{x,y}(c_1^3) &\in S
\end{aligned}
$$

But by assumption $L_{c_2,c_3}(c_1) \notin S$ and since Q is automorphic and $x^2 \in S$ we have $L_{c_2,c_3}(c_1^2) \in S$. Thus $L_{c_2,c_3}(c_1) \cdot L_{c_2,c_3}(c_1^2) = L_{c_2,c_3}(c_1^3) \notin S$, contradicting the last line above. Hence, a contradiction and the proof is complete. □

We freely use commutativity and diassociativity in what follows, especially in calculations of the form $(xy)^2 = x^2y^2$.

Lemma 5.10. Let Q be a commutative Moufang loop, $S < Q$, and assume there exists $a, b \in Q - S$ such that $a^2, b^2 \in S$ and $Sa \cap Sb = \emptyset$. The following are equivalent:

1. $Q = S \cup Sa \cup Sb$,
2. For all $x \in Q$, if $x \notin S$, then $Sx \cap (Sa \cup Sb) \neq \emptyset$

When these equivalent conditions occur, S is normal in Q.

Proof. Assume (1) holds and let $x \in Q - S$ be given. Then $Sx \cap S = \emptyset$. By (1), $Sx \cap (Sa \cup Sb) \neq \emptyset$. Thus (2) holds.

Conversely, assume (2) holds and let $x \in Q - S$ be given. Then there exists $x' \in Sx \cap (Sa \cup Sb)$. Thus $x'x^{-1} \in S$ and $x'a^{-1} \in S$ or $x'b^{-1} \in S$.

If $x'a^{-1} \in S$, then $(x')^2a^{-2} = (x'a^{-1})^2 \in S$, and so $(x')^2 \in S$ since $a^2 \in S$. Similarly, if $x'a^{-1} \in S$, then $(x')^2 \in S$ since $b^2 \in S$. In either case, we shown that $(x')^2 \in S$.

Now since $x'x^{-1} \in S$, we have $(x')^2x^{-2} = (x'x^{-1})^2 \in S$, and thus $x^{-2} \in S$ since $(x')^2 \in S$. We have shown that for all $x \in Q - S$, we have $x^2 \in S$. On the other hand, this is also true for all $x \in S$. Therefore for all $x \in Q$, $x^2 \in S$. By Lemma 5.9 S is a normal subloop of Q and hence the cosets of S partition Q. Since there are no cosets disjoint from S, Sa and Sb, we must have $S \cup Sa \cup Sb = Q$. Therefore (1) holds and we have also established the initial assertion. □

Proposition 5.11. Let Q be a commutative Moufang loop, $S < Q$, and assume there exists $a, b \in Q - S$ such that $a^2, b^2 \in S$, $Sa \cap Sb = \emptyset$ and $S \cup Sa \cup Sb \subsetneq Q$. Then there exists $c \in Q$ such that $Sc \cap S = Sc \cap Sa = Sc \cap Sb = \emptyset$.

Proof. If no such c exists, then for all $x \in Q$, $Sx \cap S \neq \emptyset$ or $Sx \cap Sa \neq \emptyset$ or $Sx \cap Sb \neq \emptyset$. Note that $Sx \cap S \neq \emptyset$ if and only if $x \in S$. Thus for all $x \in Q$, if $x \notin S$, then $Sx \cap Sa \neq \emptyset$ or $Sx \cap Sb \neq \emptyset$. Equivalently, for all $x \in Q$, if $x \notin S$, then $Sx \cap (Sa \cup Sb) \neq \emptyset$. By Lemma 5.10, $Q = S \cup Sa \cup Sb$, contradicting our assumption. □

5.3 An Equivalence Relation

We previously attempted to partition the loop by sets known to have order a multiple of that of the subloop. We will now instead start with a partition of the loop and attempt to show that its blocks have orders multiples of that of the subloop. We will see that this approach does not work, but the result is still of some interest.

Proposition 5.12. For an IP loop Q, $H \leq Q$ the relation $\sim_H$ defined by $x \sim_H y$ iff $xy^{-1} \in H$ and $H(yx^{-1}) \cdot x = Hy$ is an equivalence relation.

This proposition actually holds for arbitrary loops. However, we are primarily concerned with Moufang loops here and using inversion instead of left and right division substantially simplifies notation, so we will prove it only for IP loops.

Proof. First note that $xx^{-1} = 1 \in H$ and $H(xx^{-1}) \cdot x = H1 \cdot x = Hx$. So $\sim_H$ is reflexive.

Now suppose that $x \sim_H y$. Then $xy^{-1} \in H$, so $(xy^{-1})^{-1} = yx^{-1} \in H$ since IP loops have the AAIP.

$$\begin{aligned} H(yx^{-1}) \cdot x &= Hy \text{ since } x \sim_H y \\ Hx &= Hy \text{ since } yx^{-1} \in H \\ H(yx^{-1}) \cdot x &= Hy \text{ since } yx^{-1} \in H \end{aligned}$$

Thus $yx^{-1} \in H$ and $H(yx^{-1}) \cdot x = Hy$, so $y \sim_H x$.

Finally, suppose that $x \sim_H y$ and $y \sim_H z$. Then $xy^{-1}, yz^{-1} \in H$, $H(yx^{-1}) \cdot x = Hy$, and $H(zy^{-1}) \cdot y = z$. Then

$$\begin{aligned} x \in Hy = H(zy^{-1}) \cdot y &\text{ since } (yz^{-1})^{-1} = zy^{-1} \in H \\ x \in Hz &\text{ since } H(zy^{-1}) \cdot y = Hz \\ xz^{-1} \in H &\text{ since } Q \text{ is an IP loop} \end{aligned}$$

Then

$$\begin{aligned} H(zx^{-1}) \cdot x = Hx &\text{ since } zx^{-1} = (xz^{-1})^{-1} \in H \\ = H(yx^{-1}) \cdot x &\text{ since } yx^{-1} = (xy^{-1})^{-1} \in H \\ = Hy & \\ = H(zy^{-1}) \cdot y &\text{ since } zy^{-1} = (yz^{-1})^{-1} \in H \\ = Hz & \end{aligned}$$

Thus $xz^{-1} \in H$ and $H(zx^{-1}) \cdot x = Hz$. So $x \sim_H z$ completing the proof that $\sim_H$ is an equivalence relation. □

Note that it is possible that all equivalence classes other than the subloop itself are singletons. The Moufang loop of order 12 below with subloop $H = \{1, 2, 7, 8\}$ is one such example.

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	7	12	11	10	9
3	3	6	5	2	1	4	9	10	11	12	7	8
4	4	5	6	1	2	3	10	9	8	7	12	11
5	5	4	1	6	3	2	11	12	7	8	9	10
6	6	3	2	5	4	1	12	11	10	9	8	7
7	7	8	11	10	9	12	1	2	5	4	3	6
8	8	7	12	9	10	11	2	1	4	5	6	3
9	9	12	7	8	11	10	3	4	1	6	5	2
10	10	11	8	7	12	9	4	3	6	1	2	5
11	11	10	9	12	7	8	5	6	3	2	1	4
12	12	9	10	11	8	7	6	5	2	3	4	1

Table 5.2: Moufang loop and subloop with trivial $\sim_H$-classes

5.4 Orbits of $\mathbf{Mlt}_L(Q; S)$

Having been unable to prove Lagrange's Theorem for Moufang loops directly using cosets we will now try another approach.

Definition 5.13. Let Q be a loop, $S \leq Q$ and recall that $\text{Mlt}_L(Q) = \langle L_x : x \in Q \rangle$. We then define the *relative left multiplication group of S in Q* as

$$\text{Mlt}_L(Q; S) = \langle L_x : x \in S \rangle \leq \text{Mlt}_L(Q)$$

Note that left translations in $\text{Mlt}_L(Q; S)$ act on all of Q, so $\text{Mlt}_L(Q; S) \neq \text{Mlt}_L(S)$.

For a group G with $S \leq G$ the orbits of $\text{Mlt}_L(G; S)$ are precisely the right cosets of S in G. This observation suggests that perhaps in Moufang loops the proper generalization of cosets to use to prove Lagrange's Theorem directly is orbits of $\text{Mlt}_L(Q; S)$.

The orbits of $\text{Mlt}_L(Q;S)$ partition Q so we would need to show that the orders of orbits of $\text{Mlt}_L(Q;S)$ are multiples of the order of S. We were not able to prove this result, but we were able to show that if it holds in simple Moufang loops M, then it holds in all Moufang loops. Additionally, we were able to show that the order of orbits of $\text{Mlt}_L(Q;S)$ are multiples of $\frac{|\text{Mlt}_L(Q;S)}{\text{Inn}_L(Q)}$.

Definition 5.14. Let $S\backslash Q$ be the set of orbits of $\text{Mlt}_L(Q;S)$ on the set Q.

Definition 5.15. The *action matrix* of $x \in Q$, $R_{S\backslash Q}(x)$, is the transition matrix of a Markov chain on the state space of orbits of $\text{Mlt}_L(Q;S)$ where the probability of transition from orbit X to orbit Y is

$$\frac{|X \cap R_x^{-1}(Y)|}{X}$$

[5].

Informally, for fixed $x \in Q$ this Markov chain represents applying R_x to an orbit X of $\text{Mlt}_L(Q;S)$ and considering the probability that a randomly chosen element is sent to the orbit Y.

Proposition 5.16. Suppose that $R_{S\backslash Q}(x) = R_{S\backslash Q}(y)$, then x and y lie in the same orbit of $\text{Mlt}_L(Q;S)$.

Proof. Let Q be a loop $S \leq Q$. Let $x, y \in Q$ such that $R_{S\backslash Q}(x) = R_{S\backslash Q}(y)$. Suppose that X is the orbit of $\text{Mlt}_L(Q;S)$ containing x.

Since $R_{S\backslash Q}(x) = R_{S\backslash Q}(y)$ we have that $|S \cap R^{-1}(y)(X)| = |S \cap R^{-1}(x)(X)| \geq 1$ by Theorem 4.1 in [5]. So there exists $p \in S$ such that $py \in X$. By our choice of X there exists $\phi \in \text{Mlt}_L(Q;S)$ such that $py = \phi(x)$. But then $y = L_p^{-1}(\phi(x))$ and thus x, y lie in the same orbit of $\text{Mlt}_L(Q;S)$. □

Definition 5.17. A partition is *uniform* if all blocks have the same size.

Proposition 5.18. The partition of Q into orbits of $\mathrm{Mlt}_L(Q;S)$ is uniform iff all action matrices are doubly stochastic.

Proof. Let $s_Y(x)$ be the sum of entries in the column corresponding to Y in the matrix $R_{S\backslash Q}(x)$. Note that

$$s_Y(x) = \sum_{Z \in S\backslash Q} \frac{|R_x^{-1}(Y) \cap Z|}{|Z|}$$

and since $S\backslash Q$ is a partition of Q and R_x is a permutation of Q we have

$$|Y| = \sum_{Z \in S\backslash Q} |R_x^{-1}(Y) \cap Z|.$$

Suppose first that all action matrices are doubly stochastic and let $x \in Q$ be given. Suppose that X is the orbit of $\mathrm{Mlt}_L(Q;S)$ containing x. From the previous proposition the entry corresponding to row S and column X is a 1. Since $R_{S\backslash Q}(x)$ is doubly stochastic the remaining entries in this column are 0. Thus $s_Y(x) = \sum_{Z \in S\backslash Q} \frac{|R_x^{-1}(X) \cap Z|}{|Z|} = \frac{|R_x^{-1}(X) \cap S|}{|S|} = 1$ and $|X| = \sum_{Z \in S\backslash Q} |R_x^{-1}(X) \cap Z| = |R_x^{-1}(X) \cap S| = |S|$. So for all $X \in S\backslash Q$ $|X| = |S|$ and the partition is uniform.

Now suppose that the partition $S\backslash Q$ is uniform and let $x \in Q$, $Y \in S\backslash Q$ be given. We will show that $s_Y(x) = 1$. Consider

$$|Y| = \sum_{Z \in S\backslash Q} |R_x^{-1}(Y) \cap Z| \quad \text{from the above}$$

Dividing by $|Y|$ we have

$$\begin{aligned} 1 &= \sum_{Z \in S\backslash Q} \frac{|R_x^{-1}(Y) \cap Z|}{|Y|} \\ &= \sum_{Z \in S\backslash Q} \frac{|R_x^{-1}(Y) \cap Z|}{|Z|} && \text{since the partition is uniform} \\ &= s_Y(x) && \text{by definition} \end{aligned}$$

Thus $s_Y(x) = 1$, so $R_{S\backslash Q}(x)$ is doubly stochastic for all $x \in Q$. □

Proposition 5.19. If there is a Moufang loop Q with subloop S and an orbit X of $\mathrm{Mlt}_L(Q; S)$ such that $|S|$ does not divide $|X|$, then there is such a simple Moufang loop.

Proof. Note that $|S|$ fails to divide $|X|$ iff every representation of X as a union of cosets contains at least 2 with nontrivial intersection. This passes directly to the quotient loop. □

Proposition 5.20. Let Q be a Moufang loop with $S \leq Q$ and $x \in Q$. Then $\frac{|\mathrm{Mlt}_L(Q;S)|}{|\mathrm{Inn}_L(Q)|}$ divides $|\mathrm{Orb}_{\mathrm{Mlt}_L(Q;S)}(x)|$.

Proof. Let $G = \mathrm{Mlt}_L(Q; S)$ and define $F : \mathrm{Stab}_G(x) \to \mathrm{Inn}_L(Q)$ by $F(\phi) = L_{x^{-1}}\phi L_x$. First note that F is injective since $L_{x^{-1}}\phi L_x = L_{x^{-1}}\psi L_x$ implies $\phi = \psi$. Further, F is a homomorphism, since

$$\begin{aligned} F(\phi\psi) &= L_{x^{-1}}\phi\psi L_x \\ &= L_{x^{-1}}\phi L_x L_{x^{-1}}\psi L_x \\ &= F(\phi)F(\psi) \end{aligned}$$

and

$$\begin{aligned} F(\phi^{-1}) &= L_{x^{-1}}\phi^{-1}L_x \\ &= (L_x^{-1}\phi L_{x^{-1}}^{-1})^{-1} \\ &= (L_{x^{-1}}\phi L_x)^{-1} \\ &= F(\phi)^{-1} \end{aligned}$$

Thus $\mathrm{Stab}_G(x)$ is isomorphic to some subloop of $\mathrm{Inn}_L(Q)$ and in particular $\frac{|\mathrm{Inn}_L(Q)|}{|\mathrm{Stab}_G(x)|} = n$ for some $n \in \mathbb{N}$. So $|\mathrm{Orb}_G(x)| = n \cdot \frac{|G|}{|\mathrm{Inn}_L(Q)|}$. □

Chapter 6: Universally and semi-universally flexible loops

6.1 Introduction

We refer the reader to the introduction of this dissertation for definitions of flexibility and isotope. In this chapter we will be concerned with loops which are universally flexible and semi-universally flexible.

Definition 6.1. A loop $(Q, \cdot)$ is *universally flexible* (UF) if all of its isotopes are flexible.

Definition 6.2. A loop $(Q, \cdot)$ is *semi-universally flexible* (SUF) if all of its left and right isotopes are flexible.

It was shown in [8] that every SUF IP loop is diassociative. It is conjectured that there exists a SUF IP loop which is not Moufang, meaning that this result is not simply a consequence of Moufang's Theorem. However, no such example has yet been found. Our attempt to construct such an example is described below.

Recall that left SUF loops are loops all of whose left isotopes are flexible, right SUF loops are defined dually, and SUF loops are loops which are both left and right SUF. In practice we will define these varieties of loops equationally. We now present identities which define the varieties of SUF and UF loops:

Left SUF:

$$(x/u) \cdot (y/u)x = (((x/u)y)/u) \cdot x$$

Right SUF:

$$x \cdot (v\backslash(y(v\backslash x))) = x(v\backslash y) \cdot (v\backslash x)$$

Universally flexible:

$$(x/u)\cdot(v\backslash((y/u)\cdot(v\backslash x))) = (((x/u)\cdot(v\backslash y))/u)\cdot(v\backslash x)$$

6.2 Basic examples

Below is a loop of order 6 which is left SUF but not right SUF. By symmetry of the definitions of left (right) SUF this shows that neither implies the other.

$\cdot$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	2	5	4
2	2	4	0	5	1	3
3	3	5	4	0	2	1
4	4	3	5	1	0	2
5	5	2	1	4	3	0

Table 6.1: A loop which is left SUF but not right SUF

Note that for some properties universality and semi-universality coincide. This is the case for LIP, for example, a quasigroup is semi-universally LIP iff it is universally LIP. We conjecture that this is not the case for flexibility, that is we conjecture that there exists a SUF quasigroup which is not universally flexible. However such a quasigroup has not yet been constructed.

6.3 Central extensions of Moufang loops

It is conjectured in [8] that there exists an SUF IP loop which is not Moufang, meaning that the result in [8] showing that such loops are diassociative does not follow from Moufang's Theorem. However, no such loop has been found. Our goal in this chapter is to construct such a loop. Naive searches with MACE4 up to order 20 were unsuccessful.

An approach allowing the constructing of SUF IP loops of larger order is to emulate the central extension construction in [26].

Definition 6.3. Let Q, K be loops, $A \trianglelefteq Q$, $A \leq Z(Q)$ such that $Q/A \simeq K$. Then Q is a *central extension* of A by K [26].

The advantage of this approach is that it allows us to construct SUF IP loops which are much larger than those that can be investigated by MACE4. We were able to construct SUF IP loops of orders up to 729. However, unlike MACE4 searches, we were not able to exhaustively check all SUF IP loops of a given order using this approach. Following the approach in [26] we will construct Q given A and K. The central extension construction proceeds as follows:

Given:

$$(K, \cdot, 1) \text{ a loop,}$$

$$(A, +, 0) \text{ an abelian group, and}$$

$$f : K \times K \to A \text{ satisfying } f(1, k) = f(k, 1) = 0$$

We construct $(Q, *)$, where:

$$Q = K \times A$$

$$(x, a) * (y, b) = (x \cdot y, a + b + f(x, y))$$

By Proposition 5 in [26] Q is a central extension of K by A. By imposing additional conditions on K and f we can ensure that Q has properties we desire. In particular, by choosing K SUF IP (and thus in practice Moufang) and imposing the conditions on f given below we can ensure that Q is SUF and IP.

To ensure that Q is IP we require:

$$f(x, x^{-1}) = 0,$$

$$f(y,x) + f(yx, x^{-1}) = 0, \text{ and}$$

$$f(x,y) + f(x^{-1}xy) = 0$$

To ensure that Q is SUF we require:

$$f(y, vx) + f(v, y \cdot vx) + f(x, v \cdot (y \cdot vx)) - f(v,y) - f(x, vy) - f(x \cdot vy, vx) = 0$$

Professor Vojtěchovský provided us with GAP code to efficiently carry out the construction as described in [26]. This allowed us to search many SUF loops arising as central extensions for one which is not Moufang. However, we were unable to find such a loop. The Moufang library in the GAP LOOPS package provided us with an exhaustive list of non-associative Moufang loops of orders ≤ 64 and 81 to serve as bases for our central extensions. The extensions we searched are listed below.

K		A
Moufang loops of order 16	by	$\mathbb{Z}_2$
Central extensions of Moufang loops of order 16 by $\mathbb{Z}_2$	by	$\mathbb{Z}_2$
Moufang loops of order 32	by	$\mathbb{Z}_2$
Central extensions of Moufang loops of order 32 by $\mathbb{Z}_2$	by	$\mathbb{Z}_2$
Moufang loops of order 64	by	$\mathbb{Z}_2$
Moufang loops of order 81	by	$\mathbb{Z}_3$
Central extensions of Moufang loops of order 81 by $\mathbb{Z}_3$	by	$\mathbb{Z}_3$
Moufang loops of order 64	by	$\mathbb{Z}_p$, $p \leq 13$ prime

Table 6.2: Loops checked for SUF IP and not Moufang

Given the extent of loops checked we conjecture the following:

Conjecture 6.4. Let Q be an SUF IP loop which is also a central extension of a Moufang loop by a cyclic group, then Q is a Moufang loop.

6.4 A UF loop which is not middle Bol

It had been conjectured that all universally flexible loops are middle Bol. The central extension approach did allow us to construct a UF loop which is not middle Bol. The multiplication table of such a loop is below, it is a central extension of a middle Bol loop of order 16 by $\mathbb{Z}_2$. The central extension structure can clearly be seen in the multiplication table, $K \times \{0\}$ is the upper left quadrant.

In particular, this loop is universally flexible and does not have the AAIP and thus is not middle Bol. Further, it is commutative and has the semiautomorphic inverse property $(xyx)^{-1} = x^{-1}y^{-1}x^{-1}$. Further, one of its isotopes has the AAIP, but being an isotope is UF and not middle Bol.

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15	18	17	20	19	22	21	24	23	26	25	28	27	30	29	32	31
3	3	4	7	8	9	10	11	12	13	14	1	2	15	16	5	6	27	28	23	24	31	32	19	20	29	30	17	18	25	26	21	22
4	4	3	8	7	10	9	12	11	14	13	2	1	16	15	6	5	28	27	24	23	32	31	20	19	30	29	18	17	26	25	22	21
5	5	6	9	10	1	2	14	13	3	4	16	15	8	7	12	11	21	22	25	26	17	18	29	30	19	20	31	32	23	24	27	28
6	6	5	10	9	2	1	13	14	4	3	15	16	7	8	11	12	22	21	26	25	18	17	30	29	20	19	32	31	24	23	28	27
7	7	8	11	12	14	13	1	2	16	15	3	4	6	5	10	9	23	24	27	28	29	30	17	18	31	32	19	20	21	22	25	26
8	8	7	12	11	13	14	2	1	15	16	4	3	5	6	9	10	24	23	28	27	30	29	18	17	32	31	20	19	22	21	26	25
9	9	10	13	14	3	4	16	15	7	8	6	5	12	11	2	1	31	32	29	30	27	28	25	26	23	24	21	22	19	20	17	18
10	10	9	14	13	4	3	15	16	8	7	5	6	11	12	1	2	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
11	11	12	1	2	16	15	3	4	6	5	7	8	10	9	14	13	19	20	17	18	25	26	27	28	21	22	23	24	31	32	29	30
12	12	11	2	1	15	16	4	3	5	6	8	7	9	10	13	14	20	19	18	17	26	25	28	27	22	21	24	23	32	31	30	29
13	13	14	15	16	8	7	6	5	12	11	10	9	1	2	3	4	30	29	32	31	24	23	22	21	28	27	26	25	18	17	20	19
14	14	13	16	15	7	8	5	6	11	12	9	10	2	1	4	3	29	30	31	32	23	24	21	22	27	28	25	26	17	18	19	20
15	15	16	5	6	12	11	10	9	2	1	14	13	3	4	7	8	26	25	22	21	20	19	32	31	18	17	30	29	28	27	24	23
16	16	15	6	5	11	12	9	10	1	2	13	14	4	3	8	7	25	26	21	22	19	20	31	32	17	18	29	30	27	28	23	24
17	17	18	27	28	21	22	23	24	31	32	19	20	30	29	26	25	13	14	11	12	7	8	5	6	16	15	3	4	2	1	9	10
18	18	17	28	27	22	21	24	23	32	31	20	19	29	30	25	26	14	13	12	11	8	7	6	5	15	16	4	3	1	2	10	9
19	19	20	23	24	25	26	27	28	29	30	17	18	32	31	22	21	11	12	5	6	16	15	3	4	1	2	13	14	9	10	8	7
20	20	19	24	23	26	25	28	27	30	29	18	17	31	32	21	22	12	11	6	5	15	16	4	3	2	1	14	13	10	9	7	8
21	21	22	31	32	17	18	29	30	27	28	25	26	24	23	20	19	7	8	16	15	13	14	2	1	11	12	9	10	5	6	3	4
22	22	21	32	31	18	17	30	29	28	27	26	25	23	24	19	20	8	7	15	16	14	13	1	2	12	11	10	9	6	5	4	3
23	23	24	19	20	29	30	17	18	25	26	27	28	22	21	32	31	5	6	3	4	2	1	13	14	9	10	11	12	7	8	16	15
24	24	23	20	19	30	29	18	17	26	25	28	27	21	22	31	32	6	5	4	3	1	2	14	13	10	9	12	11	8	7	15	16
25	25	26	29	30	19	20	31	32	23	24	21	22	28	27	18	17	16	15	1	2	11	12	9	10	5	6	8	7	3	4	13	14
26	26	25	30	29	20	19	32	31	24	23	22	21	27	28	17	18	15	16	2	1	12	11	10	9	6	5	7	8	4	3	14	13
27	27	28	17	18	31	32	19	20	21	22	23	24	26	25	30	29	3	4	13	14	9	10	11	12	8	7	5	6	16	15	1	2
28	28	27	18	17	32	31	20	19	22	21	24	23	25	26	29	30	4	3	14	13	10	9	12	11	7	8	6	5	15	16	2	1
29	29	30	25	26	23	24	21	22	19	20	31	32	18	17	28	27	2	1	9	10	5	6	7	8	3	4	16	15	13	14	11	12
30	30	29	26	25	24	23	22	21	20	19	32	31	17	18	27	28	1	2	10	9	6	5	8	7	4	3	15	16	14	13	12	11
31	31	32	21	22	27	28	25	26	17	18	29	30	20	19	24	23	9	10	8	7	3	4	16	15	13	14	1	2	11	12	5	6
32	32	31	22	21	28	27	26	25	18	17	30	29	19	20	23	24	10	9	7	8	4	3	15	16	14	13	2	1	12	11	6	5

Table 6.3: A loop which is UF and not middle Bol

Chapter 7: Future directions of research

7.1 Power graphs

The *enhanced power graph* of a group, which lies between the power graph and the commuting graph as a subgraph, was recently defined in [39]. They were able to prove a similar result, that two finite groups with isomorphic power graphs must have isomorphic enhanced power graphs. One natural progression of our research would be to attempt to transfer this result to the context of Moufang loops.

There has been some work in describing properties of the power graph of a group and how they relate to properties of the group itself as in [12], line graphs citation, and undirected power graphs of semi-groups citation. Another natural progression of this research would be to attempt to characterize properties of the power graphs of Moufang loops.

7.2 Para-F quasigroups

There are several outstanding problems regarding para-F quasigroups. The first is the lack of a human readable proof that para-F quasigroups are affine over Moufang loops. An example of a para-F quasigroup which is not paramedial is also still needed.

There is another generalization of medial quasigroups which we have not considered above, the trimedial quasigroups. The relation of trimedial quasigroups to other varieties is shown in figure 7.1 [40]. It seems that the variety of quasigroups defined by the (*) identities in section 3.1.2 may be the analogous triparamedial quasigroups [40]. To formalize this would require proving that a quasigroup satisfies (*) if and only if it is triparamedial. Another natural next step would be to attempt to prove a linearity result for the triparamedial quasigroups.

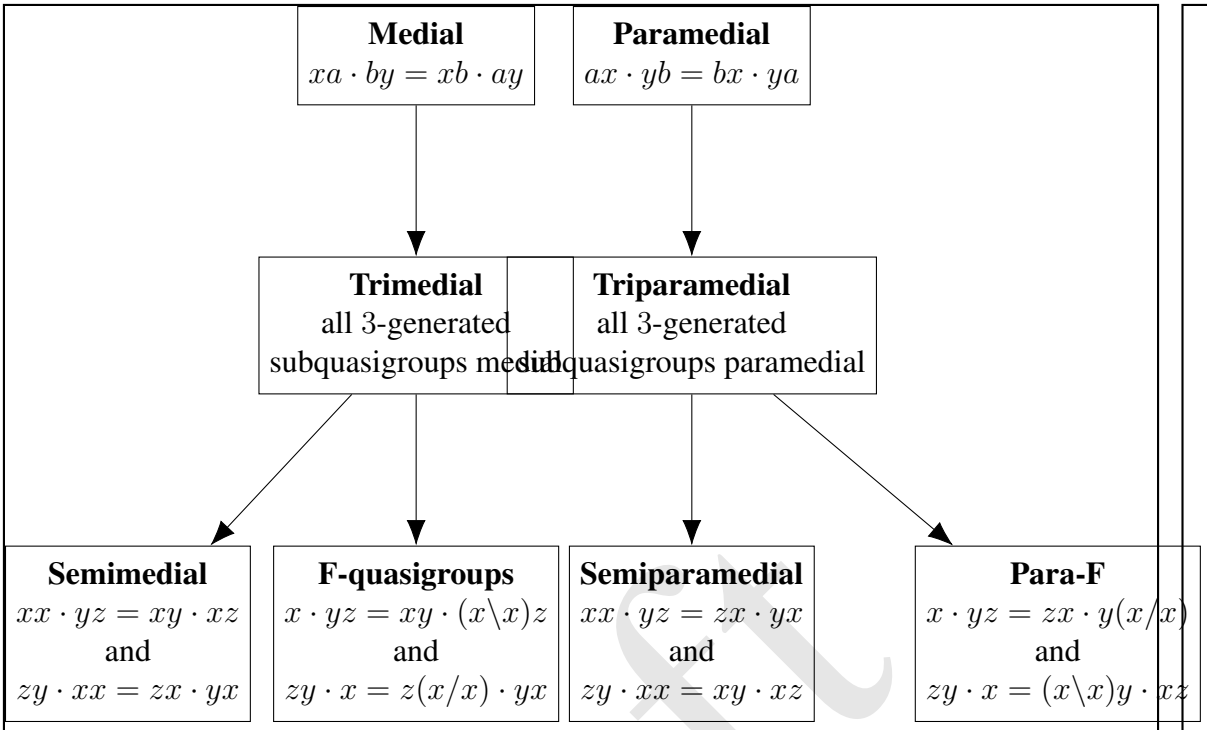

Figure 7.1: Generalizations of medial and paramedial with trimedial

7.3 Solvability for loops

In this chapter we succeeded in finding a sufficient condition for classical and congruence solvability degrees to coincide in loops. A natural next step would be to attempt to weaken this sufficient condition or find an equivalent condition for solvability degrees to coincide.

7.4 Cosets in Moufang loops

The question we set out to answer here, namely ”for any subloop of a Moufang loop does there exist a subset of its cosets partitioning the loop?”, remains open. We conjecture that the answer is negative, however no example has yet been constructed.

7.5 SUF loops

The first open question to address here is whether there exists an SUF loop which is not UF. We conjecture that such a loop does exist, but we have thus far been unable to construct one.

There is also the remaining question of whether SUF and IP implies Moufang. As above, it is conjectured that there is an SUF IP loop which is not Moufang, but none has yet been constructed. Not that an affirmative answer to the first question would provide an affirmative answer to this question as it is known [8] that a UF IP loop must be Moufang.

Bibliography

[1] V. D. Belousov. *Foundations of the theory of quasigroups and loops*. Nauka, 1967. in Russian.

[2] R. H. Bruck. *Survey of binary systems*. Springer Verlag, 1971.

[3] H. O. Pflugfelder. *Quasigroups and loops: introduction*. Heldermann Verlag, 1990.

[4] V. Shcherbacov. *Elements of quasigroup theory and applications*. Monographs and Research Notes in Mathematics. CRC Press, 2017.

[5] J.D.H. Smith. *An introduction to quasigroups and their representations*. Studies in Advanced Mathematics. Chapman & Hall/CRC, 2007.

[6] V. D. Belousov. Foundations of the theory of quasigroups and loops. *Izdat. Nauka*, 1967.

[7] M. Kinyon and K. Kunen. Power-associative, conjugacy closed loops. *J. Algebra*, 304:679–711, 2006.

[8] M. Kinyon, K. Kunen, and J.D. Phillips. Loops with universal and semi-universal flexibility. *preprint*, 2021.

[9] R. Moufang. Zur struktur von alternativkörpern. *Mathematische Annalen*, 110:416–430, 1935.

[10] A. Grishkov and A. V. Zavarnitsine. Lagrange's theorem for moufang loops. *Math. Proc. Camb. Phil. Soc.*, 139(01):41–57, 2005.

[11] T. Kepka, M. Kinyon, and J.D. Phillips. The structure of f-quasigroups. *J. Algebra*, 317:435–461, 2007.

[12] G. Aalipour, S. Akbari, P. J. Cameron, R. Nikandish, and F. Shaveisi. On the structure of the power graph and the enhanced power graph of a group. *Electron. J. Comb.*, 24(3), 2017.

[13] P. J. Cameron and S. Ghosh. The power graph of a finite group. *Discrete Mathematics*, 311(13), 2011.

[14] P. J. Cameron. The power graph of a finite group, ii. *Discrete Mathematics*, 311(6), 2011.

[15] P. J. Cameron, H. Guerra, and S. Jurina. The power graph of a torsion-free group. *J. Algebr. Comb.*, 49(1):83–98, 2019.

[16] M. Feng, X. Ma, and K. Wang. The structure and metric dimension of the power graph of a finite group. *Eur. J. Comb.*, 43:82–97, 2015.

[17] A. R. Moghaddanfar, S. Rahbariyan, and W. J. Shi. Certain properties of the power graph associated with a finite group. *Filomat*, 26(6), 2014.

[18] R. P. Panda and K. V. Krishna. On connectedness of power graphs of finite groups. *J. Algebr. Appl.*, 17(10), 2018.

[19] K. Brown. *Cohomology of groups*. Springer-Verlag, 1982.

[20] H. Cartan and S. Eilenberg. *Homological algebra*. Princeton University Press, 1999.

[21] K. Conrad. Generalized quaternions.

[22] G. Glauberman and C. R. B. Wright. Nilpotence of finite moufang 2-loops. *Journal of Algebra*, 8(4), 1968.

[23] G. Glauberman. On loops of odd order. *Journal of Algebra*, 1:374–396, 1964.

[24] O. Chein. Moufang loops of small order. *Memoirs of the AMS*, 13(197), 1978.

[25] W. Burnside. *Theory of groups of finite order*. Dover Publ., 1955. reprint.

[26] G. P. Nagy and Petr Vojtěchovský. The moufang loops of order 64 and 81. *Journal of Symbolic Computation*, 42, 2007.

[27] E. G. Goodaire, S. May, and M. Raman. *The Moufang loops of order less than 64*. Nova Science Publishers, Inc., 1999.

[28] I. Chakrabarty, S. Ghosh, and M.K. Sen. Undirected power graphs of semigroups. *Semigroup Forum*, 78:410–426, 2009.

[29] V.A. Shcherbacov and D.I. Pushkashku. On the structure of finite paramedial quasigroups. *Comment. Math. Univ. Carolin.*, 51:357–370, 2010.

[30] M. Barnes and M. Kinyon. Quasigroups isotopic to commutative moufang loops. *preprint*, 2021.

[31] W. McCune. Prover9. software, 2009.

[32] T. Kepka, M. K. Kinyon, and J. D. Phillips. F-quasigroups isotopic to groups. *preprint*, 2006.

[33] S. Burris and H. P. Sankappanavar. A course in universal algebra. 1981.

[34] D. Stanovsky and P. Vojtěchovský. Commutator theory for loops. *J. Algebra*, 399:290–322, 2014.

[35] M. Barnes and M. Kinyon. Inner mapping group result. *preprint*, 2021.

[36] M. Kinyon, K. Kunen, and J.D. Phillips. Diassociativity in conjugacy closed loops. *Com. Algebra*, 32:767 – 786, 2004.

[37] G. Nagy and P. Vojtěchovksỳ. Gap loops package.

[38] M. Kinyon, K. Pula, and P. Vojtěchovksỳ. Incidence properties of cosets. *J. Combinatorial Designs*, 20:161–197, 2012.

[39] S. Zahirović, I. Bošnjak, and R. Madaraász. A study of enhanced power graphs of finite groups. *J. Algebra Appl.*, 2020.

[40] M. Kinyon and J.D. Phillips. Axioms for trimedial quasigroups. *Comment. Math. Univ. Carolin.*, 2003.

Chapter A: Automated proofs

A.1 Notation

Prover9 format	=	standard notation
		$0 = 1$
		$x * y = x \cdot y$
		$i(x) = x^{-1}$
		$R(x, y, z) = R_{x,y}(z)$
		$L(x, y, z) = L_{x,y}(z)$
		$T(x, y) = T_x(y)$
		$A(x, y, z) = [x, y, z]$
		$C(x, y) = [x, y]$

A.2 Para-F

A.2.1 Prover9 proof of Proposition 3.11.

Proof. The following shows that the (*) identities imply one of the para-F identities. The other para-F identity is dual.

```
1 (x * y) * z = ((z \ z) * y) * (z * x) #
    ↪ label(non_clause) #label(goal).  [].
 2 x * (x \ y) = y.  [].
 3 x \ (x * y) = y.  [].
```

```
4 (x / y) * y = x.  [].
5 (x * y) / y = x.  [].
6 x * (y * z) = (z * (x \ x)) * (y * x).  [].
7 (x * (y \ y)) * (z * y) = y * (z * x).  [6].
8 (x * y) * z = (z * y) * ((z / z) * x).  [].
9 (x * y) * ((x / x) * z) = (z * y) * x.  [8].
10 ((c3 \ c3) * c2) * (c3 * c1) != (c1 * c2) * c3.
   ↪ [1].
11 (x / y) \ x = y.  [4,3].
12 x / (y \ x) = y.  [2,5].
13 (x * (y \ y)) \ (y * (z * x)) = z * y.  [7,3].
14 x * (y * (z / (x \ x))) = z * (y * x).  [4,7].
15 (x * (y \ y)) * z = y * ((z / y) * x).  [4,7].
16 (x * (y * z)) / (y * x) = z * (x \ x).  [7,5].
17 (x * (y \ z)) * y = z * ((y / y) * x).  [2,9].
18 (((x / x) \ y) * z) * x = (x * z) * y.  [2,9].
19 (x * y) \ ((z * y) * x) = (x / x) * z.  [9,3].
20 ((x * y) * z) / ((z / z) * x) = z * y.  [9,5].
21 (x * (y \ y)) \ (y * z) = (z / x) * y.  [4,13].
22 x \ (y * (z * x)) = z * (y / (x \ x)).  [14,3].
23 (x * ((y / x) * z)) / y = z * (x \ x).  [15,5].
24 x * ((((y / y) * z) / x) * y) = x * ((y / x) *
   ↪ z).  [15,9,15].
25 (x * y) / (z * x) = (z \ y) * (x \ x).  [2,16].
26 x * ((y / y) * (z / (y \ x))) = z * y.  [4,17].
27 (x * ((y / y) * z)) / y = z * (y \ x).  [17,5].
28 (x * (((x / x) \ y) \ z)) * y = z * x.  [2,18].
29 (((x / y) * z) / x) * y = (x / x) * z.
   ↪ [15,19,21].
30 (x * y) / ((y / y) * z) = y * (z \ x).  [2,20].
31 (x * (y \ y)) \ z = ((y \ z) / x) * y.  [2,21].
```

```
32 (x / y) * (z / (y \ y)) = y \ (z * x).  [4,22].
33 x * ((y / (x * z)) / (z \ z)) = z \ y.  [4,22].
34 ((x / y) \ z) * (y \ y) = (y * z) / x.  [2,23].
35 (x \ (y \ z)) * (y \ y) = z / (x * y).  [2,25].
36 (x / x) * (y / (x \ z)) = z \ (y * x).  [26,3].
37 ((x / x) \ y) * (x \ z) = (z * y) / x.  [2,27].
38 (x / (y \ y)) * (z \ y) = y * (z \ x).
   ↪ [14,27,27].
39 x * (((x / x) \ y) \ z) = (z * x) / y.  [28,5].
40 (x / x) * ((x / y) \ z) = (z / x) * y.  [2,29].
41 ((x / y) * z) / x = ((x / x) * z) / y.  [29,5].
42 x / ((y / y) * z) = y * (z \ (x / y)).  [4,30].
43 (x / y) \ (y \ (z * x)) = z / (y \ y).  [32,3].
44 (x / (y * z)) / (z \ z) = y \ (z \ x).  [33,3].
45 ((x * y) / z) / (x \ x) = (z / x) \ y.  [34,5].
46 (x \ (y \ z)) \ (z / (x * y)) = y \ y.  [35,3].
47 (((x / x) * y) / z) * x = (x / z) * y.  [24,3,3].
48 (x / x) \ (y \ (z * x)) = z / (x \ y).  [36,3].
49 (x * (y \ (z * u))) / u = (z / (u \ y)) * (u \
   ↪ x).  [36,27].
50 (x / (y \ y)) \ (y * (z \ x)) = z \ y.  [38,3].
51 (x * (y \ z)) / (y \ x) = z / (x \ x).  [38,5].
52 (x / (y \ y)) * z = y * ((y / z) \ x).  [11,38].
53 ((x / x) \ y) \ z = x \ ((z * x) / y).  [39,3].
54 (x / x) \ ((y / x) * z) = (x / z) \ y.  [40,3].
55 (((x / y) \ z) * u) * x = (x * u) * ((z / x) *
   ↪ y).  [40,9].
56 (x / y) * (z \ y) = (y / y) * (z \ x).  [12,40].
57 ((x / x) * y) / (z \ x) = (z * y) / x.  [12,41].
58 x * ((y / (x \ z)) \ (u / x)) = u / (z \ (y *
   ↪ x)).  [36,42].
```

```
59 (x / y) \ (y \ z) = (z / x) / (y \ y).  [4,43].
60 (x / y) * ((x / x) \ z) = (z / y) * x.  [2,47].
61 (x / (y \ ((x / x) * z))) * z = y * x.  [12,47].
62 (x / x) \ (y \ z) = (z / x) / (x \ y).  [4,48].
63 x / (y \ ((x * y) / z)) = (y / y) \ z.  [11,48].
64 (x / (y \ z)) * (z \ z) = y * (z \ x).
   ↪ [48,35,42,5].
65 (x * (y \ z)) / (y \ y) = z / (x \ y).
   ↪ [48,44,42,5].
66 (x / (y \ z)) \ (y * (z \ x)) = z \ z.
   ↪ [48,46,42,5].
67 (x / (y \ y)) \ (y * z) = (x / z) \ y.  [11,50].
68 (x * y) / (z \ z) = (z * y) / (x \ z).  [3,51].
69 (x * y) / ((z / y) \ x) = z / (x \ x).  [11,51].
70 x * ((x / y) \ ((x * z) / u)) = ((u / x) \ z) *
   ↪ y.  [45,52].
71 (x / y) \ (z * x) = (x / x) \ (z * y).  [5,54].
72 (x / x) * (y \ (z * x)) = z * (y \ x).  [5,56].
73 (x * (y / (z \ u))) / z = (u \ (y * z)) / (x \
   ↪ z).  [36,57].
74 (x * (y \ z)) / y = z / (x \ (y * y)).
   ↪ [59,37,52,58].
75 (x / (y \ z)) * z = y * ((z / z) \ x).  [12,60].
76 x / (y \ ((x / x) * z)) = (y * x) / z.  [61,5].
77 (x / y) * (z \ z) = (z / y) * (z \ x).  [11,64].
78 ((x * y) / (z \ x)) \ (z * y) = x \ x.  [3,66].
79 (x * y) / ((x * z) \ (x * z)) = ((x * z) * y) /
   ↪ z.  [3,68].
80 ((x * y) / (z \ x)) * u = x * ((x / u) \ (z *
   ↪ y)).  [68,40,40,52].
```

```
81 ((x * y) * (x \ x)) / ((z / y) \ x) = z / ((x *
   ↪ y) \ (x * y)).  [67,69].
82 (x / x) \ (y * (z \ x)) = z \ (y * x).  [12,71].
83 x * (((y \ (z * (x * x))) / x) * (x \ x)) = z *
   ↪ (y \ (x * x)).  [25,72,15].
84 (x * (y \ z)) / (u \ z) = (x / (z \ y)) * (z \
   ↪ u).  [72,57,49].
85 x * ((x / (x \ (y / z))) \ (x * z)) = y / ((x *
   ↪ z) \ (x * z)).  [81,84,52].
86 (x * y) / (z \ (x * x)) = (z * y) / x.  [3,74].
87 (x / (y \ (z * z))) * z = y * (z \ x).  [74,4].
88 (x / (y \ z)) \ (y * ((z / z) \ x)) = z.  [75,3].
89 (x * y) / (z \ (u * y)) = y / (x \ (u * (z \
   ↪ y))).  [72,76].
90 x / (y \ (z * ((z * x) \ x))) = z * ((z / x) \
   ↪ y).  [78,69,84,80,67,89].
91 x \ (y * (z * z)) = z * (y / (z \ x)).
   ↪ [25,82,31,52,62,49,65,11].
92 x * (y \ (z * z)) = z * (y \ (x * z)).
   ↪ [83,91,73,4].
93 ((x * y) / z) \ (z * y) = x \ (z * z).  [86,11].
94 ((x * x) / y) / (y \ z) = x / (y \ ((z * y) /
   ↪ x)).  [86,63,62].
95 (x / y) * ((y / y) \ z) = y * ((y / (y \ z)) \
   ↪ x).  [67,87,75,52].
96 (x / (y \ ((y * y) / x))) * (y \ ((z * y) / x))
   ↪ = y * ((y / (y \ x)) \ z).  [88,87,95,53,53].
97 (x / (y \ ((z * y) / x))) * (y \ u) = (x * (z \
   ↪ (u * x))) / y.  [92,37,62,94].
98 x / (y \ (x * (z \ x))) = x * ((x / (x \ z)) \
   ↪ y).  [96,97,4,74,89].
```

```
99 x * ((x / (x \ y)) \ (x * z)) = x * ((x / z) \
   ↪ y).  [93,69,89,98,89,90].
100 x / ((y * z) \ (y * z)) = y * ((y / z) \ (x /
   ↪ z)).  [85,99].
101 ((x * y) * z) / y = ((y / x) \ z) * y.
   ↪ [79,100,70].
102 (x * x) * ((y / x) * z) = (z * x) * y.
   ↪ [101,4,55].
103 ((x \ y) * z) * x = ((x \ x) * z) * y.
   ↪ [77,102,102].
104 ((x \ x) * y) * (x * z) = (z * y) * x.  [3,103].
105 \$F.  [104,10].
```

The following shows that the (*) identities imply one of the semiparamedial identities. The other semiparamedial identity is dual.

```
1 (x * y) * (z * z) = (z * y) * (z * x) #
   ↪ label(non_clause) # label(goal).  [].
2 x * (x \ y) = y.  [].
3 x \ (x * y) = y.  [].
4 (x / y) * y = x.  [].
5 (x * y) / y = x.  [].
6 x * (y * z) = (z * (x \ x)) * (y * x).  [].
7 (x * (y \ y)) * (z * y) = y * (z * x).  [6].
8 (x * y) * z = (z * y) * ((z / z) * x).  [].
9 (x * y) * ((x / x) * z) = (z * y) * x.  [8].
10 (c1 * c2) * (c3 * c3) != (c3 * c2) * (c3 * c1).  [1].
11 (c3 * c2) * (c3 * c1) != (c1 * c2) * (c3 * c3).
   ↪ [10].
12 (x / y) \ x = y.  [4,3].
13 x / (y \ x) = y.  [2,5].
14 (x * (y \ y)) \ (y * (z * x)) = z * y.  [7,3].
```

```
15 x * (y * (z / (x \ x))) = z * (y * x).  [4,7].
16 (x * (y \ y)) * z = y * ((z / y) * x).  [4,7].
17 (x * (y * z)) / (y * x) = z * (x \ x).  [7,5].
18 (x * (y \ z)) * y = z * ((y / y) * x).  [2,9].
19 (x * y) \ ((z * y) * x) = (x / x) * z.  [9,3].
20 ((x * y) * z) / ((z / z) * x) = z * y.  [9,5].
21 (x * (y \ y)) \ (y * z) = (z / x) * y.  [4,14].
22 x \ (y * (z * x)) = z * (y / (x \ x)).  [15,3].
23 (x * ((y / x) * z)) / y = z * (x \ x).  [16,5].
24 x * ((((y / y) * z) / x) * y) = x * ((y / x) * z).
   ↪ [16,9,16].
25 x * (y * (((z / (x \ x)) / y) * u)) = z * (y * ((x /
   ↪ y) * u)).  [16,15,16].
26 (x * y) / (z * x) = (z \ y) * (x \ x).  [2,17].
27 x * ((y / y) * (z / (y \ x))) = z * y.  [4,18].
28 (x * ((y / y) * z)) / y = z * (y \ x).  [18,5].
29 (x * y) \ (z * x) = (x / x) * (z / y).  [4,19].
30 (((x / y) * z) / x) * y = (x / x) * z.  [16,19,21].
31 (x * y) / ((y / y) * z) = y * (z \ x).  [2,20].
32 (x / (y / (z \ z))) * z = y \ (z * x).  [4,21].
33 (x / y) * (z / (y \ y)) = y \ (z * x).  [4,22].
34 ((x / y) \ z) * (y \ y) = (y * z) / x.  [2,23].
35 ((x * x) * y) * (x * ((z / x) * (x \ x))) = (z * y)
   ↪ * (x * x).  [26,9,16].
36 (x / x) * (y / (x \ z)) = z \ (y * x).  [27,3].
37 ((x / x) \ y) * (x \ z) = (z * y) / x.  [2,28].
38 (x / (y \ y)) * (z \ y) = y * (z \ x).  [15,28,28].
39 (x / x) * ((x / y) \ z) = (z / x) * y.  [2,30].
40 ((x / y) * z) / x = ((x / x) * z) / y.  [30,5].
41 ((x * y) / z) * (x \ z) = (z / z) * y.  [13,30].
42 x / ((y / y) * z) = y * (z \ (x / y)).  [4,31].
```

```
43 (x / (y / (z \ z))) \ (y \ (z * x)) = z.  [32,3].
44 (x / y) \ (y \ (z * x)) = z / (y \ y).  [33,3].
45 ((x * y) / z) / (x \ x) = (z / x) \ y.  [34,5].
46 (((x / x) * y) / z) * x = (x / z) * y.  [24,3,3].
47 (x * (y \ (z * u))) / u = (z / (u \ y)) * (u \ x).
   ↪ [36,28].
48 (x / (y \ y)) \ (y * (z \ x)) = z \ y.  [38,3].
49 (x * (y \ z)) / (y \ x) = z / (x \ x).  [38,5].
50 x * (y \ (z * (x \ x))) = z * (y \ x).  [5,38].
51 (x / (y \ y)) * z = y * ((y / z) \ x).  [12,38].
52 (x / y) * (z \ y) = (y / y) * (z \ x).  [13,39].
53 ((x / x) * y) / (z \ x) = (z * y) / x.  [13,40].
54 x * ((y / (x \ z)) \ (u / x)) = u / (z \ (y * x)).
   ↪ [36,42].
55 (x / ((x * y) / (z \ z))) \ ((x / x) * (z / y)) = z.
   ↪  [29,43].
56 (x / y) \ (y \ z) = (z / x) / (y \ y).  [4,44].
57 x \ (((x * y) / z) * u) = (u / x) * ((z / x) \ y).
   ↪ [45,33].
58 (x / y) * ((x / x) \ z) = (z / y) * x.  [2,46].
59 (x / (y \ y)) \ (y * z) = (x / z) \ y.  [12,48].
60 (x * y) / (z \ z) = (z * y) / (x \ z).  [3,49].
61 (x * ((x / y) \ z)) / y = z / (x \ x).  [12,49].
62 x \ (y * (z \ z)) = z \ (y * (x \ z)).  [50,3].
63 x * ((x / y) \ ((x * z) / u)) = ((u / x) \ z) * y.
   ↪ [45,51].
64 (x / x) * (y \ (z * x)) = z * (y \ x).  [5,52].
65 (x * y) * ((z / x) * (u \ x)) = ((u \ z) * y) * x.
   ↪ [52,9].
66 (x * (y \ z)) / y = z / (x \ (y * y)).
   ↪ [56,37,51,54].
```

```
67 (x / (y \ z)) * z = y * ((z / z) \ x).  [13,58].
68 ((x / y) * z) / (x \ x) = (x * z) / y.  [12,60].
69 (x * ((x / y) \ z)) / (z \ z) = (z * y) / (x \ x).
   ↪ [59,61].
70 (x / y) \ (z * (x \ x)) = x \ (z * y).  [12,62].
71 (x * (y \ z)) / (u \ z) = (x / (z \ y)) * (z \ u).
   ↪ [64,53,47].
72 (x / (y \ (x / z))) * (y \ y) = (y * z) / (x \ x).
   ↪ [69,71].
73 (x / (y \ (z * z))) * z = y * (z \ x).  [66,4].
74 ((x * x) * y) / z = ((z / x) \ y) * x.
   ↪ [68,66,57,65,5].
75 (x / y) \ ((x / x) * z) = (y / x) * ((x / x) \ z).
   ↪ [41,70,57].
76 (((x * y) / (z \ z)) / x) * ((x / x) \ (z / y)) = z.
   ↪  [55,75].
77 (x / y) * ((y / y) \ z) = y * ((y / (y \ z)) \ x).
   ↪ [59,73,67,51].
78 (((x \ x) / y) \ z) * (y \ (x / z)) = x.  [76,77,63].
79 ((x \ x) / y) \ z = x / (y \ (x / z)).  [78,5].
80 (x * y) * (z * z) = (z * y) * (z * x).
   ↪ [35,25,74,79,5,72,15].
81 \$F.  [80,11].
```

□

A.2.2 Prover9 proof of Proposition 3.12.

Proof. This proves one of the candidate (*) identities follows from semiparamedial and para-F. The proof of the other (*) identity is dual.

```
1 x * (y * z) = (z * (x \ x)) * (y * x) #
   ↪ label(non_clause) # label(goal).  [].
```

```
2 x * (x \ y) = y.  [].
3 x \ (x * y) = y.  [].
4 (x / y) * y = x.  [].
5 (x * y) / y = x.  [].
6 (x * x) * (y * z) = (z * x) * (y * x).  [].
7 (x * y) * (z * y) = (y * y) * (z * x).  [6].
8 (x * y) * (z * z) = (z * y) * (z * x).  [].
9 x * (y * z) = (z * x) * (y * (x / x)).  [].
10 (x * y) * (z * (y / y)) = y * (z * x).  [9].
11 (x * y) * z = ((z \ z) * y) * (z * x).  [].
12 ((x \ x) * y) * (x * z) = (z * y) * x.  [11].
13 (c3 * (c1 \ c1)) * (c2 * c1) != c1 * (c2 * c3).  [1].
14 (x / y) \ x = y.  [4,3].
15 ((x \ y) * (x \ y)) * (z * x) = y * (z * (x \ y)).
   ↪ [2,7].
16 ((x \ y) * z) * (x * z) = (z * z) * y.  [2,7].
17 (x * y) \ ((y * y) * (z * x)) = z * y.  [7,3].
18 (x * x) * ((y / x) * z) = (z * x) * y.  [4,7].
19 (x * (y \ z)) * (y * y) = z * (y * x).  [2,8].
20 x * (y * (z / z)) = z * (y * (x / z)).  [4,10].
21 ((x \ y) * z) * x = ((x \ x) * z) * y.  [2,12].
22 ((x \ x) * y) \ ((z * y) * x) = x * z.  [12,3].
23 ((x \ y) * (x \ z)) * z = ((x \ z) * (x \ z)) * y.
   ↪ [2,16].
24 (x * y) \ ((y * y) * z) = (z / x) * y.  [4,17].
25 ((x \ y) * (x \ y)) * z = y * ((z / x) * (x \ y)).
   ↪ [4,15].
26 ((x \ y) * (x \ z)) * z = z * ((y / x) * (x \ z)).
   ↪ [23,25].
27 (x * (y * z)) / (y * y) = z * (y \ x).  [19,5].
```

```
28 x * ((((y / (x \ x)) * z) / x) * (x \ x)) = (z * (x
   ↪ \ x)) * y.  [21,18,26].
29 ((x \ x) * y) \ (z * x) = x * (z / y).  [4,22].
30 (x * y) \ ((z * y) * u) = (((u / y) * z) / x) * y.
   ↪ [18,24].
31 (x * y) / (z * z) = (z \ y) * (z \ x).  [2,27].
32 (x / y) * (z \ y) = (y / y) * (z \ x).  [20,27,31,3].
33 (((x / y) * z) / (x \ x)) * y = x * z.  [5,29,30].
34 ((x * y) / z) * (x \ z) = (z / z) * y.  [3,32].
35 (x / x) * ((x / y) \ z) = (z / x) * y.  [14,32].
36 (x / (y \ y)) * z = y * ((y / z) \ x).  [2,33].
37 (x * (y \ y)) * z = y * ((z / y) * x).
   ↪ [28,36,34,35].
38 \$F.  [13,37,5].
```

□

A.3 $Q/\mathbf{Nuc}(Q)$

A.3.1 Prover9 proof of Theorem 4.27.

Proof.

```
1 R(x,y,R(z,u,w)) = R(z,u,R(x,y,w)) #
   ↪ label(non_clause) # label(goal).  [].
2 0 * x = x.  [].
3 x * 0 = x.  [].
4 x * (x \ y) = y.  [].
5 x \ (x * y) = y.  [].
6 (x / y) * y = x.  [].
7 (x * y) / y = x.  [].
8 L(x,y,z) = (x * y) \ (x * (y * z)).  [].
9 (x * y) \ (x * (y * z)) = L(x,y,z).  [8].
10 R(x,y,z) = ((z * x) * y) / (x * y).  [].
11 ((x * y) * z) / (y * z) = R(y,z,x).  [10].
```

```
12 T(x,y) = (x * y) / x.  [].
13 (x * y) / x = T(x,y).  [12].
14 A(x,y,z) = (x * (y * z)) / ((x * y) * z).  [].
15 (x * (y * z)) / ((x * y) * z) = A(x,y,z).  [14].
16 C(x,y) = (x * y) / (y * x).  [].
17 (x * y) / (y * x) = C(x,y).  [16].
18 A(A(x,y,z),u,w) = 0.  [].
19 A(x,A(y,z,u),w) = 0.  [].
20 R(x,y,0 / z) = 0 / R(x,y,z).  [].
21 0 / R(x,y,z) = R(x,y,0 / z).  [20].
22 R(c1,c2,R(c3,c4,c5)) != R(c3,c4,R(c1,c2,c5)).  [1].
23 R(c3,c4,R(c1,c2,c5)) != R(c1,c2,R(c3,c4,c5)).  [22].
24 0 \ x = x.  [4,2].
25 x / 0 = x.  [6,3].
26 (x / y) \ x = y.  [6,5].
27 x / x = 0.  [2,7].
28 x / (y \ x) = y.  [4,7].
29 L(0,x,y) = y.  [2,9,2,5].
30 (x * y) * L(x,y,z) = x * (y * z).  [9,4].
31 x \ (y * ((y \ x) * z)) = L(y,y \ x,z).  [4,9].
32 L(x,y,y \ z) = (x * y) \ (x * z).  [4,9].
33 x \ ((x / y) * (y * z)) = L(x / y,y,z).  [6,9].
34 R(x \ y,z,x) = (y * z) / ((x \ y) * z).  [4,11].
35 ((x * y) * (y \ z)) / z = R(y,y \ z,x).  [4,11].
36 R(x,y,z) * (x * y) = (z * x) * y.  [11,6].
37 R(x,y,z / x) = (z * y) / (x * y).  [6,11].
38 T(x / y,y) = x / (x / y).  [6,13].
39 A(x,y,z) * ((x * y) * z) = x * (y * z).  [15,6].
40 ((x \ y) * x) / y = C(x \ y,x).  [4,17].
41 x / (y * (x / y)) = C(x / y,y).  [6,17].
42 R(x,y,0 / z) * R(x,y,z) = 0.  [21,6].
```

```
43 R(x,y,0 / z) \ 0 = R(x,y,z).  [21,26].
44 (x * (y * z)) / L(x,y,z) = x * y.  [9,28].
45 (x \ 0) * x = C(x \ 0,x).  [40,25].
46 (C(x \ 0,x) * y) / (x * y) = R(x,y,x \ 0).  [45,11].
47 x * (0 / x) = C(x,0 / x).  [26,45,26].
48 0 / C(x,0 / x) = C(0 / x,x).  [47,17,6].
49 L(x,R(y,z,0 / u),R(y,z,u)) = (x * R(y,z,0 / u)) \ x.
   ↪  [42,9,3].
50 R(x,y,z) \ 0 = R(x,y,z \ 0).  [28,43].
51 x * L(y,y \ x,z) = y * ((y \ x) * z).  [4,30].
52 (x * (y * z)) \ (x * (y * (z * u))) = L(x,y *
   ↪ z,L(y,z,u)).  [30,9].
53 (x * (y * z)) / (y * L(x,y,z)) = R(y,L(x,y,z),x).
   ↪ [30,11].
54 L(x,y,y \ 0) = (x * y) \ x.  [3,32].
55 L(x,y,y \ (x \ z)) = (x * y) \ z.  [4,32].
56 L(x / y,y,y \ 0) = x \ (x / y).  [6,54].
57 x / L(x,y,y \ 0) = x * y.  [54,28].
58 C(x \ 0,x) \ (x \ 0) = L(x \ 0,x,x \ 0).  [45,54].
59 C(x,0 / x) \ x = L(x,0 / x,x).  [47,54,26].
60 ((x * y) * z) / ((R(y,z,x) * y) * z) =
   ↪ A(R(y,z,x),y,z).  [36,15].
61 (R(x,y,z) * ((x * y) * u)) / (((z * x) * y) * u) =
   ↪ A(R(x,y,z),x * y,u).  [36,15].
62 R(x,y,0 / x) = y / (x * y).  [2,37].
63 R(x,y,(z / y) / x) = z / (x * y).  [6,37].
64 R(x,y,z / x) \ (z * y) = x * y.  [37,26].
65 R(x,x \ y,0 / x) = (x \ y) / y.  [4,62].
66 R(x,y,0 / x) \ y = x * y.  [62,26].
67 (0 / x) / C(x,0 / x) = R(x,0 / x,0 / x).  [47,62].
68 R(x,y,x) = (y / (x * y)) \ 0.  [62,50,26].
```

```
69 x / L(x / (y * z),y,z) = (x / (y * z)) * y.  [6,44].
70 (x * ((y * z) * u)) / L(x,R(z,u,y),z * u) = x *
   ↪ R(z,u,y).  [36,44].
71 R(C(x,0 / x),L(x,0 / x,x),C(0 / x,x)) = L(x,0 / x,x)
   ↪ / x.  [59,65,48,59].
72 (0 / x) * (x * y) = L(0 / x,x,y).  [33,24].
73 L(0 / x,x,x \ y) = (0 / x) * y.  [4,72].
74 (0 / x) \ L(0 / x,x,y) = x * y.  [72,5].
75 C(0 / x,x) \ L(C(0 / x,x),C(x,0 / x),y) = C(x,0 / x)
   ↪ * y.  [41,74,47,48,47,47].
76 (x * y) * (y \ 0) = R(y,y \ 0,x).  [35,25].
77 R(x,x \ 0,y / x) = y * (x \ 0).  [6,76].
78 C(x,0 / x) * x = R(0 / x,x,x).  [47,76,26,26].
79 R(x,x \ 0,x) = (x \ 0) \ 0.  [68,76,76,4,25].
80 (x \ 0) * R(0 / x,x,x) = 0.  [79,42,26,26].
81 R(0 / x,x,x) = (x \ 0) \ 0.  [80,5].
82 C(x,0 / x) * x = (x \ 0) \ 0.  [78,81].
83 A(x / y,y,z) * (x * z) = (x / y) * (y * z).  [6,39].
84 (A(x,y,z) * u) * w = A(x,y,z) * (u * w).  [18,39,2].
85 (x * A(y,z,u)) * w = x * (A(y,z,u) * w).  [19,39,2].
86 L(A(x,y,z),u,w) = w.  [84,5,9].
87 (A(x,y,z) * (u * w)) / w = A(x,y,z) * u.  [84,7].
88 L(A(x,y,z) * u,w,v5) = L(u,w,v5).  [84,9,84,52,86].
89 R(x,y,A(z,u,w)) = A(z,u,w).  [84,11,7].
90 (x * (A(y,z,u) * (w * v5))) / ((x * (A(y,z,u) * w))
   ↪ * v5) = A(x,A(y,z,u) * w,v5).  [84,15].
91 R(x,y,0 / A(z,u,w)) = 0 / A(z,u,w).  [89,21].
92 L(A(x,y,z) \ u,w,v5) = L(u,w,v5).  [4,88].
93 ((0 / A(x,y,z)) * u) * w = (0 / A(x,y,z)) * (u * w).
   ↪  [91,36].
94 (0 / A(x,y,z)) \ u = A(x,y,z) * u.  [91,66].
```

```
95 A(x,y,z) \ 0 = 0 / A(x,y,z).  [91,79,26].
96 C(0 / A(x,y,z),A(x,y,z)) = 0.  [95,40,6,27,95].
97 x / L(x,A(y,z,u),0 / A(y,z,u)) = x * A(y,z,u).
   ↪ [95,57].
98 L(x / A(y,z,u),A(y,z,u),0 / A(y,z,u)) = x \ (x /
   ↪ A(y,z,u)).  [95,56].
99 L(0 / A(x,y,z),u,w) = w.  [95,92,29].
100 ((0 / A(x,y,z)) * u) \ w = u \ (A(x,y,z) * w).
   ↪ [99,55,94].
101 (0 / A(x,y,z)) * u = A(x,y,z) \ u.  [99,73].
102 (A(x,y,z) \ u) \ w = u \ (A(x,y,z) * w).  [100,101].
103 A(x,y,z) \ (u * w) = (A(x,y,z) \ u) * w.
   ↪ [93,101,101].
104 L(x,0 / A(y,z,u),A(y,z,u) * (x \ w)) = (x * (0 /
   ↪ A(y,z,u))) \ w.  [94,55].
105 ((x * (0 / A(y,z,u))) * w) / (A(y,z,u) \ w) = R(0 /
   ↪ A(y,z,u),w,x).  [101,11].
106 L(x,A(y,z,u),w) = w.  [85,5,9].
107 R(A(x,y,z),u,w) = w.  [85,11,7].
108 A(x * A(y,z,u),w,v5) = A(x,A(y,z,u) * w,v5).
   ↪ [85,15,85,90].
109 x \ (x / A(y,z,u)) = 0 / A(y,z,u).  [98,106].
110 x / (0 / A(y,z,u)) = x * A(y,z,u).  [97,106].
111 (x * A(y,z,u)) \ w = A(y,z,u) \ (x \ w).  [106,55].
112 (x / A(y,z,u)) \ (x * w) = A(y,z,u) * w.  [107,64].
113 x * (0 / A(y,z,u)) = x / A(y,z,u).  [109,4].
114 L(x,0 / A(y,z,u),w) = w.  [109,31,101,112,4,109].
115 (x / A(y,z,u)) * w = x * (A(y,z,u) \ w).
   ↪ [109,51,114,109,101].
116 R(0 / A(x,y,z),u,w) = w.  [105,113,115,7].
```

```
117 (x / A(y,z,u)) \ w = A(y,z,u) * (x \ w).
    ↪ [104,114,113].
118 x / (A(y,z,u) \ w) = (x / w) * A(y,z,u).
    ↪ [116,63,110,115,2].
119 (A(x,y,z) * u) / w = A(x,y,z) * (u / w).  [6,87].
120 A(x,y,z) * R(u,w,v5) = R(u,w,A(x,y,z) * v5).
    ↪ [87,37,84,119,11].
121 L(x / A(y,z,u),w,v5) = L(x,A(y,z,u) \ w,v5).
    ↪ [115,9,115,103,9].
122 A(x / A(y,z,u),w,v5) = A(x,A(y,z,u) \ w,v5).
    ↪ [115,15,103,115,15].
123 A(x,y,z) * (0 / u) = A(x,y,z) / u.  [3,119].
124 A(x,y,z) * ((0 / u) * w) = (A(x,y,z) / u) * w.
    ↪ [123,30,86].
125 L(A(x,y,z) / u,w,v5) = L(0 / u,w,v5).  [123,88].
126 R(C(x,0 / x),x,R(x,0 / x,0 / x)) = x \ 0.
    ↪ [67,63,82,28].
127 L((x / y) * (y * z),u,w) = L(x * z,u,w).  [83,88].
128 (A(R(x,0 / x,0 / x),C(x,0 / x),y) / x) * y = R(x,0
    ↪ / x,0 / x) * (C(x,0 / x) * y).  [67,83,124,67].
129 L(L(0 / x,x,y),z,u) = L(y,z,u).  [2,127,72].
130 L(x \ 0,y,z) = L(0 / x,y,z).  [54,129,6,24].
131 C(x \ 0,x) \ (x \ 0) = 0 / x.  [58,130,73,3].
132 R(C(x,0 / x),x,R(x,0 / x,0 / (0 / x))) = x.
    ↪ [126,21,28,21].
133 R(R(x,y,z) * x,y,(z * x) / (R(x,y,z) * x)) =
    ↪ A(R(x,y,z),x,y).  [60,37].
134 A(R(x,0 / x,0 / x),C(x,0 / x),y) / x = (R(x,0 / x,0
    ↪ / x) * (C(x,0 / x) * y)) / y.  [128,7].
135 ((x \ 0) \ 0) / x = C(x,0 / x).  [82,7].
```

```
136 (x * ((y \ 0) \ 0)) / (C(y,0 / y) * L(x,C(y,0 /
    ↪ y),y)) = R(C(y,0 / y),L(x,C(y,0 / y),y),x).
    ↪ [82,53].
137 L(x,0 / x,x) = 0 / (0 / x).  [26,131,26,59].
138 R(C(x,0 / x),0 / (0 / x),C(0 / x,x)) = (0 / (0 /
    ↪ x)) / x.  [71,137,137].
139 C(x,0 / x) * (0 / (0 / x)) = x.  [137,30,47,6,3].
140 C(x,0 / x) * T(0 / x,x) = x.  [38,139].
141 (x * y) / (C(y,0 / y) * L(x,C(y,0 / y),0 / (0 /
    ↪ y))) = R(C(y,0 / y),L(x,C(y,0 / y),0 / (0 /
    ↪ y)),x).  [139,53].
142 (x * y) / (C(y,0 / y) * L(x,C(y,0 / y),T(0 / y,y)))
    ↪ = R(C(y,0 / y),L(x,C(y,0 / y),0 / (0 / y)),x).
    ↪ [38,141].
143 ((x * y) * z) / (x * (y * z)) = 0 / A(x,y,z).
    ↪ [39,46,95,96,2,95,91].
144 A(x,y,z) \ x = R(y,z,x).
    ↪ [143,69,121,29,11,143,115,2].
145 x / R(y,z,x) = A(x,y,z).  [144,28].
146 R(x,y,z) / z = 0 / A(z,x,y).  [144,65,91,144].
147 (x * y) / (R(z,u,x) * y) = A(x,z,u).
    ↪ [144,34,89,144].
148 A(R(x,y,z),x,y) = A(z,x,y).
    ↪ [133,144,147,18,147,24].
149 R(x,y,z \ 0) = z \ A(z,x,y).  [145,56,50,86,145].
150 x * R(y,z,x \ 0) = A(x,y,z).  [145,77,50,89,50].
151 (R(x,y,z) / z) * u = A(z,x,y) \ u.  [146,73,106].
152 L(x,R(y,z,u) / u,w) = w.  [146,114].
153 L(R(x,y,z) / z,u,w) = w.  [146,125,121,86].
154 L(x,C(y,0 / y),z) = z.  [79,152,135].
```

```
155 R(C(x,0 / x),0 / (0 / x),y) = y.
    ↪ [142,154,140,7,154].
156 R(C(x,0 / x),x,y) = y.  [136,154,82,7,154].
157 C(0 / x,x) \ y = C(x,0 / x) * y.  [75,154].
158 (0 / (0 / x)) / x = C(0 / x,x).  [138,155].
159 R(x,0 / x,0 / (0 / x)) = x.  [132,156].
160 R(x,0 / x,0 / x) = x \ 0.  [126,156].
161 A(x \ 0,C(x,0 / x),y) / x = ((x \ 0) * (C(x,0 / x)
    ↪ * y)) / y.  [134,160,160].
162 (x * (C(y,0 / y) * z)) / z = x * C(y,0 / y).
    ↪ [154,44].
163 R(C(x,0 / x),y,z) = z.  [154,53,7,154].
164 A(x \ 0,C(x,0 / x),y) / x = (x \ 0) * C(x,0 / x).
    ↪ [161,162].
165 A(x,C(y,0 / y),z) = 0.  [163,145,27].
166 (x \ 0) * C(x,0 / x) = 0 / x.  [164,165].
167 L(C(x,0 / x),y,z) = z.  [79,153,135].
168 A(x,y,z) \ R(u,w,v5) = R(u,w,A(x,y,z) \ v5).
    ↪ [153,70,151,103,103,11,151].
169 (C(x,0 / x) * y) * z = C(x,0 / x) * (y * z).
    ↪ [167,30].
170 A(0 / (0 / x),x,0 / x) = C(0 / x,x).  [159,145,158].
171 A(x,x,0 / x) = C(0 / x,x).  [159,148,170].
172 A(x,A(y,z,u) * w,v5) = A(x,w,v5).
    ↪ [150,85,108,111,120,4,150].
173 A(x,A(y,z,u) \ w,v5) = A(x,w,v5).
    ↪ [150,115,122,117,168,5,150].
174 A(x * A(y,z,u),w,v5) = A(x,w,v5).  [108,172].
175 (x \ 0) * (C(x,0 / x) * y) = (0 / x) * y.
    ↪ [166,30,154].
```

```
176 A(x \ 0,C(x,0 / x) * y,z) = A(0 / x,y,z).
    ↪ [166,61,163,169,175,15,163].
177 A(x,C(y,0 / y) * z,u) = A(x,z,u).  [171,173,157].
178 A(x \ 0,y,z) = A(0 / x,y,z).  [176,177].
179 A(R(x,y,z \ 0),u,w) = A(R(x,y,0 / z),u,w).
    ↪ [21,178,50].
180 A(x \ A(y,z,u),w,v5) = A(0 / x,w,v5).
    ↪ [102,178,3,118,174].
181 A(0 / (A(x,y,z) / u),w,v5) = A(u,w,v5).  [26,180].
182 A(R(x,y,0 / (A(z,u,w) / v5)),v6,v7) =
    ↪ A(R(x,y,v5),v6,v7).  [49,180,86,120,123,21].
183 A(R(x,y,0 / z),u,w) = A(0 / z,u,w).  [149,180,179].
184 A(R(x,y,z),u,w) = A(z,u,w).  [182,183,181].
185 R(x,y,R(z,u,w)) = R(z,u,R(x,y,w)) #
    ↪ label(non_clause) # label(goal).
    ↪ [184,144,168,144].
186 \$F.  [185,23].
```

□