AN INVESTIGATION INTO THE STRUCTURE OF DIGROUPS

ANDREW MAGYAR, KYLE PRIFOGLE, DAVID WHITE, AND WILLIAM YOUNG

Abstract. In this paper we investigate the algebraic structure of digroups. We find a Lagrange-style correspondence between digroups and subdigroups. We also show how to construct a digroup containing any given number of identities whose order is any multiple of that number. Then, all digroups with inverse sets of prime order are classified. Additionally, the terms subdigroup, commutant, trivial digroup, idempotency class, are defined with basic results proven with regard to each term. Finally, various structural propositions are proven which may be useful in future digroup research.

1. Introduction

Since 2004, the notion of a digroup has been considered by Felipe [3], Kinyon [4], Phillips [12], Crompton and Scalici [2], and Liu [6]. Digroups were introduced to provide a partial solution to the Coquecigrue problem of generalizing Lie's Third Theorem for Leibniz Algebras, originally proposed in [7]. Kinyon's [4] definition of a digroup is as follows:

Definition 1.1. *A **digroup** is a set G with two binary operations, $\vdash$ and $\dashv$, a unary operation $^{-1}$ and a nullary operation 1, which satisfies:*

G1. *$(G, \vdash)$ and $(G, \dashv)$ are both semigroups*
G2. $(x \vdash y) \dashv z = x \vdash (y \dashv z)$
G3. $x \dashv (y \vdash z) = x \dashv (y \dashv z)$
G4. $(x \dashv y) \vdash z = (x \vdash y) \vdash z$
G5. $1 \vdash x = x = x \dashv 1$
G6. $x \vdash x^{-1} = 1 = x^{-1} \dashv x$

Phillips [12] proved that $G2, G3$, and $G4$ could be replaced with $G2^*$:

$G2^*$.$x \vdash (x \dashv z) = (x \vdash x) \dashv z$

The axiomatization was then shown to be equivalent to the following by Crompton and Scalici [2]:

$G1^*$ (G, $\vdash$) and (G, $\dashv$) are both **semi-Moufang**, or
$x \vdash ((y \vdash z) \vdash x) = (x \vdash y) \vdash (z \vdash x)$ and

Date: October 31, 2007.
1991 *Mathematics Subject Classification.* 20N05.
Key words and phrases. Bol, Moufang, loop, commutant, associator.

$x \dashv ((y \dashv z) \dashv x) = (x \dashv y) \dashv (z \dashv x)$
$G2$. $(x \vdash y) \dashv z = x \vdash (y \dashv z)$
$G5$. $1 \vdash x = x = x \dashv 1$
$G6$. $x \vdash x^{-1} = 1 = x^{-1} \dashv x$

It is possible that this axiomatization can still be simplified. For instance, Phillips [12] did not use $G1$ to prove $G2$ from $G2^*$, $G5$, and $G6$. Thus, Crompton could have replaced $G2$ by $G2^*$ and still have derived $G1$ from $G1^*$, making the axiomatization $G1^*$, $G2^*$, $G5$, $G6$ equivalent to Kinyon's [4]. The software program PROVER9 [9] was used to prove that the following two relations are equivalent to semi-Moufang in the axiomatization of digroups:

Semi-Extra: $x \vdash (y \vdash (z \vdash x)) = ((x \vdash y) \vdash z) \vdash x$ and
$x \dashv (y \dashv (z \dashv x)) = ((x \dashv y) \dashv z) \dashv x$

Semi-Bol: $x \vdash ((y \vdash z) \vdash x) = (x \vdash y) \vdash (z \vdash x)$,
$x \dashv ((y \dashv z) \dashv x) = (x \dashv y) \dashv (z \dashv x)$,
$((z \vdash x) \vdash y) \vdash x = z \vdash ((x \vdash y) \vdash x)$, and
$((z \dashv x) \dashv y) \dashv x = z \dashv ((x \dashv y) \dashv x)$

However, replacing $G1$ with either of these would be even more unwieldly, and we only present them as an example of other directions to go with the axiomatization. For our purposes in this paper, we shall use Phillips' definition. Namely,

Definition 1.2. *A **digroup** is a set G with two binary operations, $\vdash$ and $\dashv$, a unary operation $^{-1}$ and a nullary operation 1, which satisfies:*
G1. $(G, \vdash)$ and $(G, \dashv)$ are both semigroups
G2 $x \vdash (x \dashv z) = (x \vdash x) \dashv z$*
G5. $1 \vdash x = x = x \dashv 1$
G6. $x \vdash x^{-1} = 1 = x^{-1} \dashv x$

In the digroup, 1 is called a **bar unit** and x^{-1} is the **inverse** of x with respect to 1. It must be noted that a digroup can have multiple elements that act as bar units, but must always have at least one. An **identity** is an element $e \in G$ such that $e \vdash x = x = x \dashv e$ and $x \vdash x^{-1}_{\vdash} = e = x^{-1}_{\dashv} \dashv x$ for all $x \in G$ but $x^{-1}_{\vdash}$ is not necessarily equal to $x^{-1}_{\dashv}$. If they are equal for all $x \in G$, e is a bar unit. We shall call $x^{-1}_{\vdash}$ the **right inverse** of x and $x^{-1}_{\dashv}$ the **left inverse** of x.

It should be noted that Liu [6] uses a slightly different definition of digroup, in which none of the identities is necessarily a bar unit. Liu's $G6$ is as follows:

$G6_L$: for all $x \in G$, there exists $x^{-1}_{\vdash}$, $x^{-1}_{\dashv} \in G$ such that $x^{-1}_{\dashv} \dashv x = 1 = x \vdash x^{-1}_{\vdash}$.

For an example of a Cayley table that is a digroup under Lius definition, but not for Definition 1.2, see http://persweb.wabash.edu/facstaff/phillipj/research.html.

Next we define a **trivial digroup** as one which is composed entirely of identities:

$\vdash$	0	1	2	...	n
0	0	1	2	...	n
1	0	1	2	...	n
2	0	1	2	...	n
...	...	...	...	...	...
n	0	1	2	...	n

$\dashv$	0	1	2	...	n
0	0	0	0	...	0
1	1	1	1	...	1
2	2	2	2	...	2
...	...	...	...	...	...
n	n	n	n	...	n

We note that there is one such digroup of each order $n \in \mathbb{N}$, and that every element of a trivial digroup acts as a bar unit.

The next lemma requires a definition of right and left group. Given a semigroup $(G, \vdash)$, we say $(G, \vdash)$ is a **right group** if G contains a left identity $e \in G$ and a right inverse x^{-1} for each $x \in G$. Left group is defined in a similar fashion. If $(G, \vdash, \dashv)$ forms a digroup, then $(G, \vdash)$ forms a right group and $(G, \dashv)$ forms a left group.

Lemma 1.3. *Let $(G, \vdash)$ be a right group. We define the set of identities $E = \{e \in G | e \vdash x = x \text{ for all } x \in G\}$ and the set of inverses $J = \{x^{-1} | x \in G\}$ with respect to any bar unit. It has been proven (e.g. [4]) that*

(1) *J is a group*

(2) *$G = J \vdash E \cong (J \times E, \vdash)$*

(3) *A digroup is a group $\Leftrightarrow \vdash = \dashv \Leftrightarrow$ the bar unit is the only identity.*

(4) *$x \vdash 1 = (x^{-1})^{-1}$ for all $x \in G$*

(5) *$((x^{-1})^{-1})^{-1} = x^{-1}$ for all $x \in G$*

(6) *$(x \vdash y)^{-1} = y^{-1} \vdash x^{-1}$ for all x, $y \in G$*

(7) *$x \vdash 1 = x$ if and only if G is a group.*

Corollary 1.4. $|G| = |J| \cdot |E|$

Proof. Follows directly from (2). □

Corollary 1.5. *Let G be a digroup. If $|G| = p$ where p prime, then G is either the cyclic group $\mathbb{Z}_p$ or a trivial digroup.*

Proof. By 1.4 $|E| \Big| |G|$. Since $|G|$ is prime $|E| = |G|$ or $|E| = 1$. If $|E| = 1$ we know from 1.3 that G is a group. Since $|G|$ is prime, this means that G is a cyclic group. If $|E| = |G|$, then G is the trivial digroup of order $|G|$ by definition. □

In Section 3, statements corresponding to (1),(4),(5),(6), and (7) are proven to hold with respect to any identity in G.

Definition 1.6. *We call a subset H of a digroup G a **subdigroup** if H has the structure of a digroup under the operations of G.*

This definition varies slightly from the one given in [3] in that it removes the condition that the bar unit of H must be the same bar unit in G. Thus, Felipe's subdigroup test needs to be modified appropriately:

Theorem 1.7. *H is a subdigroup of G if and only if H contains a bar unit e, and for all f, g, l, m, $n \in H$ the elements $f \vdash e$, $g^{-1} \vdash l$, and $m \dashv n^{-1}$ are in H.*

Proof. By adding the condition that H must contain a bar unit, the proof follows from Theorem 3.3 found in [3]. □

Felipe's definition of subdigroups and his test for subdigroups are such that everything Felipe proves to be a subdigroup is also a subdigroup under definition 1.6. We will, however, use Felipes definition of normal subdigroup (assuming subdigroup is defined according to definition 1.6):

Definition 1.8. *A subdigroup, H of digroup G is called a **normal subdigroup** if and only if $a^{-1} \vdash x \dashv a \in H$ for all $a \in G$ and any $x \in H$.*

2. Commutant

In [3], Felipe defined the commutant, or center, of a digroup as $Z(G) = \{x \in G | g \vdash x = x \dashv g \text{ for all } g \in G\}$ and proved it was a subdigroup. However, there are other possible definitions for a commutant that can be considered:

$C1 = \{x \in G | g \vdash x = x \vdash g \text{ for all } g \in G\}$
$C2 = \{x \in G | g \dashv x = x \dashv g \text{ for all } g \in G\}$
$C3 = \{x \in G | g \dashv x = x \vdash g \text{ for all } g \in G\}$
$C4 = \{x \in G | g \vdash x = x \dashv g \text{ for all } g \in G\} = Z(G)$

Problem 2.1. *It is still open to define the **centralizer** of an element in a digroup and prove it is a subdigroup.*

$C1$ and $C2$ are only subdigroups when G is a group because $1 \in C1$ if and only if $1 \vdash x = x \vdash 1 = x$, thus by Lemma 1.3 (7), G must be a group. A similar argument can be made for $C2$. Also, any union or intersection of $C1$ and $C2$ is insufficient as they only form subdigroups when G is a group. Thus, $C1$ and $C2$ do not represent proper generalizations of the center of a group as they do not necessarily form subdigroups of G.

Thus, we are left to consider $C3$. Using PROVER9 [9], it was proven that:

Proposition 2.2. *$C3$ is a normal subdigroup of digroup G, where 1 is a bar unit of G. We must show that:*

(1) *$C3$ contains a bar unit.*

(2) $x \in C3 \Rightarrow x^{-1} \in C3$.

(3) $x \in C3 \Rightarrow x \vdash 1 \in C3$.

(4) $x, y \in C3 \Rightarrow x^{-1} \vdash y \in C3$.

(5) $x, y \in C3 \Rightarrow x \dashv y^{-1} \in C3$.

(6) $x \in C3 \Rightarrow ((g^{-1} \vdash x) \dashv g) \in C3$ *for all* $g \in G$.

Proof. In this proof we shall also make use of the fact that if 1 is a bar unit, then $1 \in C4$; proven in [3]. Let $x \in C3$.

(1) $1 \vdash x = x = x \dashv 1 \Rightarrow 1 \in C3$.

(2) Since $x \in C3$, $x \vdash y = y \dashv x$ for all $y \in G \Rightarrow x \vdash (a \dashv b) \overset{(C3)}{=} (a \dashv b) \dashv x \overset{(G1)}{=} a \dashv (b \dashv x) \overset{(C3)}{=} a \dashv (x \vdash b)$ for all $a, b \in G$. If we let $b = x^{-1}$, this equation becomes $a = x \vdash (a \dashv x^{-1})$.

We know from Lemma 1.3 that $(c^{-1})^{-1} = c \vdash 1 \Rightarrow c^{-1} \vdash (c \vdash 1) = 1$ by the definition of inverse. Therefore $c^{-1} \vdash ((c \vdash 1) \vdash d) \overset{(G1)}{=} (c^{-1} \vdash (c \vdash 1)) \vdash d = 1 \vdash d = d$ for all $c, d \in G$.

Since $a = x \vdash (a \dashv x^{-1})$, $x^{-1} \vdash a = x^{-1} \vdash (x \vdash (a \dashv x^{-1})) = a \dashv x^{-1}$ by the above equation with $c = x$ and $d = a \dashv x^{-1}$. This proves $x^{-1} \in C3$.

(3) Since $x \in C3, (x \vdash 1) \vdash g \overset{(G1)}{=} x \vdash (1 \vdash g) = x \vdash g \overset{(C3)}{=} g \dashv x = (g \dashv 1) \dashv x \overset{(G1)}{=} g \dashv (1 \dashv x) \overset{(C3)}{=} g \dashv (x \vdash 1)$. Therefore, $x \vdash 1 \in C3$.

(4) Let $A, B \in C3$. Then $A \vdash x = x \dashv A$ and $B \vdash x = x \dashv B$ for all $x \in G$. Note that by (2) above, $A^{-1} \vdash x = x \dashv A^{-1}$ and $B^{-1} \vdash x = x \dashv B^{-1}$ for all $x \in G$.

$(A^{-1} \vdash B) \vdash x \overset{(G1)}{=} A^{-1} \vdash (B \vdash x) \overset{(C3)}{=} (B \vdash x) \dashv A^{-1} \overset{(C3)}{=} (x \dashv B) \dashv A^{-1} \overset{(G1)}{=} x \dashv (B \dashv A^{-1}) \overset{(C3)}{=} x \dashv (A^{-1} \vdash B)$ which proves $(A^{-1} \vdash B) \in C3$.

(5) $A, B \in C3 \Rightarrow A \vdash x = x \dashv A$ and $B \vdash x = x \dashv B$ for all $x \in G$.

$(A \dashv B^{-1}) \vdash x \overset{(G4)}{=} A \vdash B^{-1} \vdash x \overset{(C3)}{=} A \vdash (x \dashv B^{-1}) \overset{(G2)}{=} (A \vdash x) \dashv B^{-1} \overset{(C3)}{=} (x \dashv A) \dashv B^{-1} \overset{(G1)}{=} x \dashv (A \dashv B^{-1})$ proving $A \dashv B^{-1} \in C3$.

(6) $A \in C3 \Rightarrow A \vdash x = x \dashv A$.

Suppose not, i.e. $b \dashv ((a^{-1} \vdash A) \dashv a) \neq ((a^{-1} \vdash A) \dashv a) \vdash b$. Note that $\underline{((a^{-1} \vdash A) \dashv a) \vdash b} \overset{(G4)}{=} (a^{-1} \vdash A) \vdash (a \vdash b) \overset{(G1)}{=} a^{-1} \vdash (A \vdash (a \vdash b)) \overset{(C3)}{=} a^{-1} \vdash ((a \vdash b) \dashv A) \overset{(G2)}{=} (a^{-1} \vdash (a \vdash b)) \dashv A \overset{(C3)}{=} A \vdash (a^{-1} \vdash (a \vdash b)) \overset{(G1)}{=} (A \vdash a^{-1}) \vdash (a \vdash b) \overset{(G1)}{=} A \vdash (a^{-1} \vdash (a \vdash b)) \overset{(G5)}{=} A \vdash (a^{-1} \vdash (a \vdash (1 \vdash$

$b))) \overset{(G1)}{=} A \vdash ((a^{-1} \vdash (a \vdash 1)) \vdash b) = A \vdash (1 \vdash b) \overset{(G5)}{=} \underline{A \vdash b}$ by Lemma 1.3 and $\underline{b \dashv ((a^{-1} \vdash A) \dashv a)} \overset{(G2)}{=} b \dashv ((a^{-1} \vdash A) \vdash a) \overset{(G1)}{=} b \dashv (a^{-1} \vdash (A \vdash a)) \overset{(G3)}{=} b \dashv a^{-1} \dashv (A \vdash a) \overset{(C3)}{=} b \dashv (a^{-1} \dashv (a \dashv A)) \overset{(G1)}{=} b \dashv ((a^{-1} \dashv a) \dashv A) \overset{(C3)}{=} b \dashv (A \vdash (a^{-1} \dashv a)) \overset{(G3)}{=} b \dashv A \dashv (a^{-1} \dashv a) \overset{(G1)}{=} (b \dashv A) \dashv a^{-1} \dashv a \overset{(C3)}{=} (A \vdash b) \dashv a^{-1} \dashv a \overset{(G2)}{=} A \vdash (b \dashv a^{-1} \dashv a) \overset{(G3)}{=} A \vdash (b \dashv (a^{-1} \vdash a)) \overset{(G5)}{=} A \vdash ((b \dashv 1) \dashv (a^{-1} \vdash a)) \overset{(G1)}{=} A \vdash (b \dashv (1 \dashv (a^{-1} \vdash a))) \overset{(C4)}{=} A \vdash (b \dashv ((a^{-1} \vdash a) \vdash 1)) \overset{(G1)}{=} A \vdash (b \dashv (a^{-1} \vdash (a \vdash 1))) \overset{(C4)}{=} A \vdash (b \dashv (a^{-1} \vdash (1 \dashv a))) \overset{(G2)}{=} A \vdash (b \dashv ((a^{-1} \vdash 1) \dashv a)) \overset{(C4)}{=} A \vdash (b \dashv ((1 \dashv a^{-1}) \dashv a)) \overset{(G1)}{=} A \vdash (b \dashv (1 \dashv (a^{-1} \dashv a))) \overset{(G6)}{=} A \vdash (b \dashv 1 \dashv 1) \overset{(G5)}{=} \underline{A \vdash b}$, a contradiction!

Therefore, $((a^{-1} \vdash A) \dashv a) \vdash b = b \dashv ((a^{-1} \vdash A) \dashv a)$.

□

Since $C3$ and $C4$ are normal subdigroups and are non-equivalent (for a digroup in which $C3 \neq C4$, see $D_2(6, \mathbb{Z}_2)$ in Section 6), both are candidates for the commutant of a digroup.

Felipe [3] defines an **abelian digroup** G as one in which $x \dashv y = y \vdash x$ for all $x, y \in G$. Note that in any abelian digroup G, $C3 = C4 = G$. Also, $E \subseteq C3$.

Many open problems still exist with regard to this aspect of digroups, and some are listed below.

Problem 2.3. *Find a correspondence for the* ***class equation*** *from group theory.*

Problem 2.4. *Define Nilpotency for digroups by taking the quotient structure of a digroup with $C3$ or $C4$ using the method from* [3].

Problem 2.5. *Do a comparative analysis of the two commutant definitions and find out which is better. Or, alternately, find a new definition based on $C3$ and $C4$ that encapsulates the best qualities of both.*

3. Subdigroups

In previous literature (e.g. [3], [4]), the set of inverses, J, was specifically the set of inverses with respect to the defined bar unit, 1. The following results rely upon the set of inverses with respect to any identity, e. We define $J_e^{\vdash} = \{h_{\vdash}^{-1} | h \vdash h_{\vdash}^{-1} = e\}$, where $h \in G$, $e \in E$, and G is a digroup. The notation, $h_{\vdash}^{-1}$ denotes the inverse of h under $\vdash$ with respect to e. We will use similar notation for $\dashv$. It is important to note that the identity $h_{\vdash}^{-1}$ is taken with respect to is not specified in the notation, but should be clear in the given context. Also, $h_{\vdash}^{-1}$ does not necessarily equal $h_{\dashv}^{-1}$, or in other words, an element of a digroup can have a different inverse under each operation with respect to the same identity. However, if the identity is also a bar unit, then $h_{\vdash}^{-1} = h_{\dashv}^{-1}$ and $J_e^{\vdash} = J_e^{\dashv}$.

The following Lemma shows that many of the results of Lemma 1.3 hold with respect to any arbitrary identity.

Lemma 3.1. *Let $(G, \vdash)$ be a right group. Let $J_e^{\vdash}$ be defined as above with $e \in E$. Let $x, y \in G$. Assume all inverses are with respect to e.*

(1) *for every $x \in G$, there exists an $x_{\vdash}^{-1}$*

(2) $x \vdash e = (x_{\vdash}^{-1})_{\vdash}^{-1}$

(3) $(x \vdash y)_{\vdash}^{-1} = y_{\vdash}^{-1} \vdash x_{\vdash}^{-1}$

(4) $((x_{\vdash}^{-1})_{\vdash}^{-1})_{\vdash}^{-1} = x_{\vdash}^{-1}$

(5) $x \vdash e = x$ *if and only if G is a group*

(6) $J_e^{\vdash} = J \vdash e = \{a \vdash e \mid a \in J\}$

(7) $J_e^{\vdash} \cong J$, *as groups under* $\vdash$

(8) *The sets $J_e^{\vdash}$ for all $e \in E$ partition G*

Proof. (1) Since $G = J \vdash E$, let $x = a \vdash e'$, for some $a \in J$ and $e' \in E$. Then, $(a \vdash e') \vdash (a^{-1} \vdash e) = a \vdash (e' \vdash a^{-1}) \vdash e = (a \vdash a^{-1}) \vdash e = 1 \vdash e = e$. Therefore, $a^{-1} \vdash e = x_{\vdash}^{-1}$.

(2) $x \vdash e = x \vdash (x_{\vdash}^{-1} \vdash (x_{\vdash}^{-1})_{\vdash}^{-1}) = e \vdash (x_{\vdash}^{-1})_{\vdash}^{-1} = (x_{\vdash}^{-1})_{\vdash}^{-1}$.

(3) Note that $(x \vdash y) \vdash y_{\vdash}^{-1} \vdash x_{\vdash}^{-1} = e$, thus $y_{\vdash}^{-1} \vdash x_{\vdash}^{-1} = (x \vdash y)_{\vdash}^{-1}$.

(4) $((x_{\vdash}^{-1})_{\vdash}^{-1})_{\vdash}^{-1} = (x \vdash e)_{\vdash}^{-1} = e \vdash x_{\vdash}^{-1} = x_{\vdash}^{-1}$, by (1) and (2).

(5) ($\Rightarrow$) Assume $e_1 \in G$, and let $x = e_1$, then $e_1 = e$. Therefore, e is the only identity in G, thus e must be a bar unit, and then by Lemma 1.3 (3), G is a group. ($\Leftarrow$) Trivial.

(6) Let $a \vdash e \in J \vdash e$. Since $a \in J$, and J is a group under $\vdash$, there exists a $b \in J$ such that $b \vdash a = 1$. Thus, $b \vdash (a \vdash e) = (b \vdash a) \vdash e = 1 \vdash e = e$. This means that $a \vdash e = b_{\vdash}^{-1} \in J_e^{\vdash}$. Now, let $x \in J_e^{-1}$. Thus, there exists a $y \in G$ such that $y \vdash x = e$. Since $G = J \vdash E$, $y = a' \vdash e'$ and $x = a'' \vdash e''$, for some a',$a'' \in J$ and e',$e'' \in E$. So, $e = y \vdash x = (a' \vdash e') \vdash (a'' \vdash e'') = a' \vdash (e' \vdash a'') \vdash e'' = (a' \vdash a'') \vdash e''$. Since $e = 1 \vdash e$, $a' \vdash a'' = 1$ and $e'' = e$. Thus, $x = a'' \vdash e \in J \vdash e$.

(7) Consider $\phi : J_e^{\vdash} \to J$ defined by $\phi(a \vdash e) = a$, for every $a \in J$. Clearly, ϕ is bijective. To show that ϕ is a group homomorphism, consider $\phi((a_1 \vdash e) \vdash (a_2 \vdash e)) = \phi((a_1 \vdash a_2) \vdash e) = a_1 \vdash a_2 = \phi(a_1 \vdash e) \vdash \phi(a_2 \vdash e)$.

(8) This follows from the observation that $G = J \vdash E$ is partitioned into $J \vdash e = J_e^{\vdash}$, for all $e \in E$.

□

Lemma 3.2. *Let $(G, \vdash, \dashv)$ be a digroup, then $g \vdash J_e^{\vdash} = J_e^{\vdash}$ for all $g \in G$ and for all $e \in E$.*

Proof. ($\subseteq$) Take $a \in J$ and $g = a' \vdash e' \in G$. Then, $g \vdash (a \vdash e) = (a' \vdash a) \vdash e \in J \vdash e$. ($\supseteq$) Take $a \vdash e \in J \vdash e$ and $g = a' \vdash e' \in G$. Then, $g \vdash (((a')^{-1} \vdash a) \vdash e) = (a' \vdash ((a')^{-1} \vdash a)) \vdash e = 1 \vdash (a \vdash e) = a \vdash e$.

□

This result also holds for the corresponding $\dashv$ statement: $J_{\dashv}^{-1} \dashv g = J_{\dashv}^{-1}$.

Lemma 3.3. *Given a digroup G, all nonempty subsets of E form a subdigroup.*

Proof. A subset of G composed entirely of identities forms a trivial subdigroup in which all elements act as bar units. □

Theorem 3.4. *Let $(G, \vdash, \dashv)$ be a digroup. Consider any nonempty subset S of E such that $S = \{e_1, e_2, ..., e_n\}$, and there exists an $e_j \in S$ that is a bar unit. Let $H = J_{e_1}^{\vdash} \cup J_{e_2}^{\vdash} \cup ... \cup J_{e_n}^{\vdash}$, then H forms a subdigroup of G if $J_{e_1}^{\vdash} \cup J_{e_2}^{\vdash} \cup ... \cup J_{e_n}^{\vdash} = J_{e_1}^{\dashv} \cup J_{e_2}^{\dashv} \cup ... \cup J_{e_n}^{\dashv}$.*

Proof. According to Theorem 1.7, we must show there exists a bar unit $e \in H$ and that for all f, g, l, m, $n \in H$, the elements $f \vdash e$, $g^{-1} \vdash l$, and $m \dashv n^{-1}$ are contained in H. Clearly, $e_j \in H$. Now we must show that for each $x \in H$, x^{-1} with respect to e_i is also in H. By Lemma 3.2, we know $x \vdash J_{e_i}^{\vdash} = J_{e_i}^{\vdash}$. Since $e_i \in J_{e_i}^{\vdash}$, then $x^{-1} \in J_{e_i}^{\vdash} \subseteq H$. Now we consider closure: $f \vdash e_i \in f \vdash J_{e_i}^{\vdash} = J_{e_i}^{\vdash}$; we know $l \in J_{e_k}^{\vdash}$ for some k such that $1 \leq k \leq n$, thus $g^{-1} \vdash l \in J_{e_k}^{\vdash} \subseteq H$; and similarly, we know $m \in J_{e_r}^{\dashv}$ for some r such that $1 \leq r \leq n$, thus $m \dashv n^{-1} \in J_{e_r}^{\dashv} \subseteq H$. Thus, H is a subdigroup of G. □

Corollary 3.5. *The subset, K, of G defined as $K = J_{e_1} \cup J_{e_2} \cup ... \cup J_{e_m}$ where $e_j \in S$ is a bar unit for all j, $1 \leq j \leq m$, forms a subdigroup of G.*

Proof. By definition of bar unit, $J_{e_j}^{\vdash} = J_{e_j}^{\dashv}$ for all t such that $1 \leq j \leq m$. Thus, $K = H$ as defined in Theorem 3.4 for some S, making K a subdigroup of G. □

According to Corollary 3.5, we can form $\sum_{j=1}^{m} \begin{pmatrix} m \\ j \end{pmatrix}$ subdigroups of G where m is the number of bar units in G, simply by finding the union of the inverse sets with respect to any number of the bar units. However, Theorem 3.4 indicates that there are more subdigroups that can be formed from identities that are not necessarily bar units, provided they satisfy the additional property given to H. Additionally, by Lemma 3.2, $2^n - 1$ trivial subdigroups can be formed where n is the number of identities in G.

An observation that can be made from Theorem 3.4, is that the inverse sets determine, to a large extent, what subdigroups can be found in a given digroup. In sections 5 and 6, it is demonstrated that the structure of any given digroup can be understood by examining the structure of its set of inverses with respect to a bar

unit. This is helpful because the set of inverses with respect to a bar unit forms a group.

We now prove a generalization of **Lagrange's Theorem**.

Theorem 3.6. *Let G be a digroup, and $H \subseteq G$ a subdigroup of G. Define J_H as the set of inverses in H with respect to a bar unit in H, and E_H and E_G as the set of identities in H and G, respectively. Let J_G be the set of inverses in G with respect to the same bar unit as J_H. If $|E_H| \Big| |E_G|$ then $|H| \Big| |G|$.*

Proof. Since $J_H \subseteq J_G$, and J_H and J_G form groups, then by Lagrange's Theorem for groups, $|J_H| \Big| |J_G|$. By Corollary 1.4, $|G| = |J_G| \cdot |E_G| = n \cdot m \cdot |J_H| \cdot |E_H| = n \cdot m \cdot |H|$, where $n, m \in \mathbb{N}$. Thus, $|H| \Big| |G|$. □

In the case that H is a group, then $|E_H| = 1$ by Lemma 1.3 (3), thus by Theorem 3.6, $|H| \Big| |G|$. This shows that Theorem 3.6 provides an appropriate generalization of Lagrange's Theorem for groups. It is not the case, however, that the order of any given subdigroup will necessarily divide the order of the parent digroup.

Problem 3.7. *It is still open to find a correspondence for the **Cauchy Theorem** from group theory. The next step after this would be to consider correspondences for the **Sylow Theorems**.*

4. Order and Idempotency

In [6], finding a generalization for the order of an element in a digroup is left as an open problem. We provide a definition here:

Definition 4.1. *Let G be a digroup. If n is the **order** of an element $x \in G$, then n is the least possible number of times x occurs in the expansion $x \vdash x \vdash x \vdash ... \vdash x = x^n_{\vdash} = e$ for some $e \in E$.*

If order is defined according to $\dashv$, this definition would be identical to 4.1. The problem with this definition is that the order of all elements will be bounded by $|J_G|$ for reasons that will become clear in Section **??**, rather than ranging through the possible divisors of $|G|$ as is the case in group theory. A generalization of order, which holds for *every* element is Idempotency:

Definition 4.2. *The **Idempotency class (I-class)** of an element x is the natural number n such that $x^n = x^n_{\dashv} = x^n_{\vdash} = x$ and $x^i \neq x$ for all $1 < i < n$. The I-class of any identity element is 2. Let $o(x)$ be the order of x, and $I(x)$ be the I-class of x.*

Proposition 4.3. *Let x be an arbitrary element in G where $|G| = n$.*

1. *Every element on the diagonal is $1 \Rightarrow I(x) = 3$ for all $x \neq 1$.*
2. *$x^k_{\vdash} = 1 \Rightarrow x^k_{\dashv} = 1$ for all $k \leq n$.*
3. *The maximum order of an element is n.*
4. *The maximum I-class of an element is $n + 1$.*

(5) $I(x) - 1 = o(x) \Leftrightarrow G$ *is a finite group.*

Proof. Let x be an arbitrary element in G where $|G| = n$.

(1) If every element on the diagonal is 1, $x \vdash x = 1$ for all x which implies that $x \vdash x \vdash x = 1 \vdash x = x$, so that $I(x) = 3$ for all $x \neq 1$.
(2) $a \vdash x^{n-1} = 1 \Leftrightarrow x^{n-1} \dashv x = 1$.
(3) Suppose not. Then $x^2 \neq 1, x^3 \neq 1, ..., x^{n+1} \neq 1$. By the Pigeonhole Principle, $x^l = x^m$ for some $l, m < n + 1$, which implies a cycle exists in which none of the powers is 1. This implies that the order is infinite.
(4) This is a corollary of (3)
(5) ($\Leftarrow$) G is finite, so all elements have finite order, so $x^n = 1 \Rightarrow x^{n+1} = x$ trivially.
($\Rightarrow$) $x^{n+1} = x$ and $x^n = 1$, so we know that $x^{n+1} \vdash x^{-1} = x \vdash x^{-1} = 1 = x^n = x^n \vdash 1$. Therefore, since $\vdash$ is associative, $x \vdash 1 = 1$, which tells us G is a group by Remark 3.2 from [3].

□

In group theory, the order of an element $x \in G$ divides $|G|$. The following theorem is the generalization of this concept to digroups with Idempotency.

Theorem 4.4. *For any element x of digroup G, $I(x) - 1 \Big| |G|$.*

The proof of this theorem is delayed until the concepts it relies on are introduced in Section 5.

Problem 4.5. *With this concept of order, the next step is to consider the structure of cyclic digroups and theorems related to them.*

Problem 4.6. *It is also still open to define orbits and stabilizers in digroups and prove a correspondence of the* ***Orbit-Stabilizer Theorem****.*

5. Classification of (G,⊢)

Theorem 5.1. *For any group H of order n, and for any $m \in \mathbb{N}$ there exists a digroup G such that the order of G is $m \cdot n$ and the inverse set J of G is isomorphic to H.*

Proof. Let $H = \{1, 2, ..., n\}$, with binary operation $\circ$ and identity 1. Let $E = \{1 = e_1, e_2, ..., e_m\}$. Let $G = H \times E$. Clearly, G has $m \cdot n$ elements. Let $\vdash$: $G \times G \to G$ be defined by $(i_1, e_{j_1}) \vdash (i_2, e_{j_2}) = (i_1 \circ i_2, e_{j_2})$. Let $\dashv$: $G \times G \to G$ be defined by $(i_1, e_{j_1}) \dashv (i_2, e_{j_2}) = (i_1 \circ i_2, e_{j_1})$. First, we will show that G satisfies the four digroup axioms.

(1) Every element has an inverse with respect to $(1, e_1)$:
$(i, e_j) \vdash (i^{-1}, e_1) = (i \circ i^{-1}, e_1) = (1, e_1) = (i^{-1} \circ i, e_1) = (i^{-1}, e_1) \dashv (i, e_j)$

(2) $(1, e_1)$ is a bar unit:

$$(1, e_1) \vdash (i, e_j) = (1 \circ i, e_j) = (i, e_j) = (i \circ 1, e_j) = (i, e_j) \dashv (1, e_1)$$

(3) Associativity:

$$[(i_1, e_{j_1}) \vdash (i_2, e_{j_2})] \vdash (i_3, e_{j_3}) = (i_1 \circ i_2, e_{j_2}) \vdash (i_3, e_{j_3}) = ((i_1 \circ i_2) \circ i_3, e_{j_3}) = (i_1 \circ (i_2 \circ i_3), e_{j_3}) = (i_1, e_{j_1}) \vdash (i_2 \circ i_3, e_{j_3}) = (i_1, e_{j_1}) \vdash [(i_2, e_{j_2}) \vdash (i_3, e_{j_3})]$$

$$[(i_1, e_{j_1}) \dashv (i_2, e_{j_2})] \dashv (i_3, e_{j_3}) = (i_1 \circ i_2, e_{j_1}) \dashv (i_3, e_{j_3}) = ((i_1 \circ i_2) \circ i_3, e_{j_1}) = (i_1 \circ (i_2 \circ i_3), e_{j_1}) = (i_1, e_{j_1}) \dashv (i_2 \circ i_3, e_{j_2}) = (i_1, e_{j_1}) \dashv [(i_2, e_{j_2}) \dashv (i_3, e_{j_3})]$$

(4) Axiom $G2^*$:

$$[(i_1, e_{j_1}) \vdash (i_1, e_{j_1})] \dashv (i_2, e_{j_2}) = (i_1 \circ i_1, e_{j_1}) \dashv (i_2, e_{j_2}) = ((i_1 \circ i_1) \circ i_2, e_{j_1}) = (i_1 \circ (i_1 \circ i_2), e_{j_1}) = (i_1, e_{j_1}) \vdash (i_1 \circ i_2, e_{j_1}) = (i_1, e_{j_1}) \vdash [(i_1, e_{j_1}) \dashv (i_2, e_{j_2})]$$

Next, we will show that $J \cong H$.

(1) $J = \{(i, e_1) \mid 1 \leq i \leq n\}$

($\subseteq$) Assume $(i', e_j) \vdash (i, e_k) = (1, e_1)$. Then, $(i' \circ i, e_k) = (1, e_1)$, and $e_k = e_1$.

($\supseteq$) $(i^{-1}, e_j) \vdash (i, e_1) = (i^{-1} \circ i, e_1) = (1, e_1)$

(2) $J \cong H$

Consider $\phi : J \to H$ defined by $\phi((i, e_1)) = i$. Clearly, ϕ is bijective. To show that ϕ preserves the groups' operations:

$$\phi((i_1, e_1) \vdash (i_2, e_1)) = \phi((i_1 \circ i_2, e_1)) = i_1 \circ i_2 = \phi((i_1, e_1)) \circ \phi((i_2, e_1))$$

□

Definition 5.2. *Two digroups G, with operations $\vdash$ and $\dashv$, and G', with operations $\vdash'$ and $\dashv'$, are **(digroup) isomorphic** if there exists a bijective function $f : G \to G'$ that preserves the operations of G; that is, $f(x \vdash y) = f(x) \vdash' f(y)$ and $f(x \dashv y) = f(x) \dashv' f(y)$, for all x,$y \in G$. If only the first of these holds, G and G' are said to be $\vdash$**-isomorphic**, and similarly for $\dashv$-isomorphisms.*

Theorem 5.3. *Two digroups $(G, \vdash, \dashv)$ and $(G', \vdash', \dashv')$ with non-isomorphic inverse sets must be non-isomorphic.*

Proof. Assume $G \cong G'$. Let 1 be the bar unit of G. Let ϕ be a digroup isomorphism from G onto G'. For any $x \in G$, $1 \vdash x = x = x \dashv 1$ and $\phi(1 \vdash x) = \phi(x) = \phi(x \dashv 1)$. So, $\phi(1) \vdash' \phi(x) = \phi(x) = \phi(x) \dashv' \phi(1)$. Similarly, $\phi(x \vdash x^{-1}) = \phi(1) = \phi(x^{-1} \dashv x)$ and $\phi(x) \vdash' \phi(x^{-1}) = \phi(1) = \phi(x^{-1}) \dashv' \phi(x)$. Thus, $\phi(1)$ is the bar unit of G'. Let J and J' be the inverse sets of G and G', respectively. Now, we will show that ϕ

restricted to J is a group isomorphism between J and J'. Let $a \in J$. Then, there exists an $b \in G$ such that $b \vdash a = 1$. So, $\phi(b) \vdash' \phi(a) = \phi(1)$. Thus, $\phi(a) \in J'$. Similarly, if $\phi(a) \in J'$, then $a \in J$. This shows that ϕ restricted to J maps into J' and is bijective (since ϕ itself is injective). Since ϕ preserves the operation $\vdash$ of G, which is the group operation of J, it also preserves that operation for J. Therefore, $J \cong J'$. □

Theorem 5.4. *Two digroups of the same order with isomorphic inverse sets must be $\vdash$-isomorphic.*

Proof. Let $(G, \vdash, \dashv)$ and $(G', \vdash', \dashv')$ be digroups of the same order whose inverse sets J and J', respectively, are isomorphic. Let $\phi : J \to J'$ be an isomorphism. Let $E = \{e_1, e_2, ..., e_n\}$ and $E' = \{e_1{}', e_2{}', ..., e_n{}'\}$ be the sets of identities of G and G', respectively, with e_1 and $e_1{}'$ as the bar units of those respective digroups. Note that since the digoups have the same order and their inverse sets also have the same order (since they are isomorphic), the sets of identities must have the same order, which we assumed is n. Now, consider the function $\Phi : G \to G'$ defined by $\Phi(a_j \vdash e_i) = \phi(a_j) \vdash' e_i{}'$, where the elements of J are enumerated a_1, a_2, ..., a_m. Clearly, Φ is bijective. To show that Φ preserves the operation $\vdash$ for G, consider $\Phi((a_{j_1} \vdash e_{i_1}) \vdash (a_{j_2} \vdash e_{i_2})) = \Phi((a_{j_1} \vdash a_{j_2}) \vdash e_{i_2}) = \phi(a_{j_1} \vdash a_{j_2}) \vdash' e_{i_2}{}' = (\phi(a_{j_1}) \vdash' e_{i_1}{}') \vdash' (\phi(a_{j_2}) \vdash' e_{i_2}{}') = \Phi(a_{j_1} \vdash e_{i_1}) \vdash' \Phi(a_{j_2} \vdash e_{i_2})$. Therefore, G and G' are $\vdash$-isomorphic. □

Theorem 5.5. *The number of distinct $\vdash$-structures of digroups of order n is $\Sigma_{i=I} g(m_i)$, where the m_i are the factors of n, and $g(m)$ is the number of groups of order m.*

Proof. Consider all digroups of order n. It is known that all of those digroups' inverse sets must be groups of orders that divide n. From Theorem 5.1, we know that all such groups can be realized as the inverse set of some digroup of order n. Then, from Theorem 5.3, we know that there are at least $\sum_{i=I} g(m_i)$ distinct digroups of order n, corresponding to each possible group that could be an inverse set. Finally, Theorem 5.4 insures this lower bound on the number of digroups of order n is actually an equality, when considering the distinct $\vdash$-structures. □

Of course, the question still remains of how many digroups of order n there are. It is known how many distinct $\vdash$-structures there can be of such digroups, but there are examples of digroups that are $\vdash$-isomorphic and $\dashv$-isomorphic, but not digroup isomorphic. In the next section, we examine this issue in further detail, and obtain some preliminary results.

Now, consider any digroup G of order mn that has $J = \{a_1, a_2, ..., a_n\}$ as its inverse set and $E = \{e_1, ..., e_m\}$ has its set of identities. Rearrange the rows and columns of the Cayley table of $\vdash$ for G in such a way that the first row and the first column (that is, the row and column that list the multiplicands) are in the following order: $a_1 \vdash e_1, a_2 \vdash e_1, ..., a_n \vdash e_1, a_1 \vdash e_2, a_2 \vdash e_2, ..., a_n \vdash e_2, ..., a_1 \vdash e_m, a_2 \vdash e_m, ..., a_n \vdash e_m$. (see the following table).

$\vdash$	$a_1 \vdash e_1 \quad a_2 \vdash e_1 \quad \cdots \quad a_n \vdash e_1$	$\cdots$	$a_1 \vdash e_m \quad a_2 \vdash e_m \quad \cdots \quad a_n \vdash e_m$
$a_1 \vdash e_1$ $a_2 \vdash e_1$ $\vdots$ $a_n \vdash e_1$	$(J \vdash J) \vdash e_1$		$(J \vdash J) \vdash e_m$
$\vdots$			
$a_1 \vdash e_m$ $a_2 \vdash e_m$ $\vdots$ $a_n \vdash e_m$	$(J \vdash J) \vdash e_1$		$(J \vdash J) \vdash e_m$

The columns are grouped according to their inverse sets and the first n rows are all distinct, with the next n rows repeating the first, in exact order, and so on, until the last n rows, which are the first n repeated in exact order. Thus, once the first n rows are determined, the entire Cayley table will be determined by just rewriting the first n rows $m-1$ more times. The first n rows and columns correspond to J (since they form the inverse set of e_1, which is the actual inverse set of G). Thus, the top-left $n \times n$ square of the Cayley table is just the Cayley table for J. Since $(a_{i_1} \vdash e_1) \vdash (a_{i_2} \vdash e_j) = (a_{i_1} \vdash a_{i_2}) \vdash e_j$, the next $n \times n$ square (since we are now only considering the first n rows) is just $(J \vdash J) \vdash e_2$, and so on, until the last $n \times n$ sqaure is just $(J \vdash J) \vdash e_m$, where $(J \vdash J) \vdash e_i$ means that the element in the k_1-th row and k_2-th column of $(J \vdash J) \vdash e_i$ is $(a_{k_1} \vdash a_{k_2}) \vdash e_i$. This means that since the first row is just the identity row, however the elements of J are permuted in each new row is exactly how the elements of every $n \times n$ square will be permuted. Thus, from J alone, the entire Cayley table is determined up to isomorphism. This construction is the main idea behind the proof of Theorem 5.4. As noted above, while a similar construction can be done with the $\dashv$ Cayley table of a digroup of order mn, so that two such digroups with J as their inverse sets will be both $\vdash$-isomorphic and $\dashv$-isomorphic, there is no guarantee that the digroups will be digroup isomorphic. This problem arises because the partitioning of the digroups into $J \vdash E$ and $E \dashv J$ may not yield the same partitions since the identities are not necessarily bar units.

As an example of the above construction, consider the following $\vdash$ Cayley table of a digroup of order 6 :

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

Now consider the Cayley tables of the partitions $\{0,1\}$,$\{2,3\}$,$\{4,5\}$:

$\vdash$	0	1
0	1	0
1	0	1

$\vdash$	2	3
2	3	2
3	2	3

$\vdash$	4	5
4	5	4
5	4	5

Notice how these tables correspond to $\mathbb{Z}_2$. Every digroup generated using MACE4 has a $\vdash$ -structure that can be arranged in this form. The digroup whose $\dashv$ Cayley table can be arranged in the same way with the same partitions we call the **Principal Digroup**. The above example with the same $\dashv$ Cayley table would be called the principal digroup of order 6 based upon $\mathbb{Z}_2$. The notation $\mathrm{D}_i(n, J)$ can be used to represent digroups where $i = 1$ corresponds to the principal digroup, $n = |\mathrm{G}|$, and J corresponds to the basis group, or the set of inverses. The above example would be represented $\mathrm{D}_1(6,\mathbb{Z}_2)$. The following table generated by MACE4 [9] shows this classification for all the digroups up to order 15. The ISOFILTER function ensured that only non-isomorphic structures were considered.
Note that with this notion of digroups based upon groups we can prove Theorem 4.4:

Proof. We know

(1) $I(x) - 1 = o(x) \Leftrightarrow$ H is a finite group from (5) above.
(2) $o(x) \Big| |H|$ for all $x \in H$.
(3) $|H| \Big| |G|$.

From these, we can see that $o(x) \Big| H \Rightarrow (I(x) - 1) \Big| H \Rightarrow (I(x) - 1) \Big| |G|$.

□

Table 1: Digroups up to order 15

Order	$\lvert J\rvert$	Name
2	2	$\mathbb{Z}_2$
	1	trivial
3	3	$\mathbb{Z}_3$
	1	trivial
4	4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
	2	$D_1(4, \mathbb{Z}_2)$
	1	trivial
5	5	$\mathbb{Z}_5$
	1	trivial
6	6	$\mathbb{Z}_6$, D_3
	3	$D_1(6, \mathbb{Z}_3)$
	2	$D_1(6, \mathbb{Z}_2)$, $D_2(6, \mathbb{Z}_2)$
	1	trivial
7	7	$\mathbb{Z}_7$
	1	trivial
8	8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q
	4	$D_1(8, \mathbb{Z}_4)$, $D_1(8, \mathbb{Z}_2 \times \mathbb{Z}_2)$
	2	$D_1(8, \mathbb{Z}_2)$, $D_2(8, \mathbb{Z}_2)$
	1	trivial
9	9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
	3	$D_1(9, \mathbb{Z}_3)$
	1	trivial
10	10	$\mathbb{Z}_{10}$, D_5
	5	$D_1(10, \mathbb{Z}_5)$
	2	$D_1(10, \mathbb{Z}_2)$, $D_2(10, \mathbb{Z}_2)$, $D_3(10, \mathbb{Z}_2)$
	1	trivial
11	11	$\mathbb{Z}_{11}$
	1	trivial
12	12	$\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, A_4, D_6, T
	6	$D_1(12, \mathbb{Z}_6)$, $D_1(12, D_3)$
	4	$D_1(12, \mathbb{Z}_4)$, $D_1(12, \mathbb{Z}_2 \times \mathbb{Z}_2)$, $D_2(12, \mathbb{Z}_4)$, $D_2(12, \mathbb{Z}_2 \times \mathbb{Z}_2)$
	3	$D_1(12, \mathbb{Z}_3)$, $D_2(12, \mathbb{Z}_3)$
	2	$D_1(12, \mathbb{Z}_2)$, $D_2(12, \mathbb{Z}_2)$, $D_3(12, \mathbb{Z}_2)$
	1	trivial
13	13	$\mathbb{Z}_{13}$
	1	trivial
14	14	$\mathbb{Z}_{14}$, D_7
	7	$D_1(14, \mathbb{Z}_7)$
	2	$D_1(14, \mathbb{Z}_2)$, $D_2(14, \mathbb{Z}_2)$, $D_3(14, \mathbb{Z}_2)$, $D_4(14, \mathbb{Z}_2)$
	1	trivial
15	15	$\mathbb{Z}_{15}$
	5	$D_1(15, \mathbb{Z}_5)$
	3	$D_1(15, \mathbb{Z}_3)$, $D_2(15, \mathbb{Z}_3)$
	1	trivial

6. The classification of $D_i(n, J)$

There are some digroups, however, which do not qualify as Principal Digroups because the partitioning of the $\dashv$ Cayley table for those digroups do not correspond to the $\vdash$ partitions. However, since every structural property of the $\vdash$ Cayley table holds for the $\dashv$ Cayley table and since the inverse sets for the two tables must be isomorphic, the entire $\dashv$ Cayley table is uniquely determined by how the digroup partitions into its inverse sets for all of its identities. Therefore, determining which permutations of the partitions of $\dashv$ yield distinct digroup structures completes the classification of D_i(n,J) for all i.

Lemma 6.1. *Consider an arbitrary digroup $(G, \vdash, \dashv)$, with. Let $\sim$ indicate the grouping of two elements within the same $\dashv$ partition. Notice that $\sim$ is an equivalence relation. If $x, c \in G$ and $x \sim c$, then $(x \vdash x) \sim (x \vdash c)$.*

Proof. Assume $x \sim c$. Then, there exists some $z \in G$ such that $x \dashv z = c$. So, $x \vdash (x \dashv z) = x \vdash c$ also, $(x \vdash x) \dashv z = x \dashv c$. Thus, by $G2^*$, $(x \vdash x) \sim (x \vdash c)$. □

Lemma 6.2. *If $|J| = p$, and $a_i \vdash e \sim e$ then the partition is equal to the set of inverses J.*

Proof. Let $a_i \vdash e \sim e$. $a_i \vdash e \sim e \Rightarrow a_i^2 \vdash e \sim a_i \vdash e$ or $a_i^2 \vdash e \sim e$. Therefore by induction, assume $a_i^k \vdash e \sim e$. $a \vdash e \sim a_i^k \vdash e \Rightarrow a_i^2 \vdash e \sim a_i^{k+1} \vdash e$. Therefore $a_i^{k+1} \sim e$.

□

Theorem 6.3. *Consider a digroup $(G, \vdash, \dashv)$ with $|G| = n$. The number of digroups with $|E| = \frac{n}{p}$ is exactly*

$$\left\lfloor \frac{\frac{n}{p} - 1}{p} \right\rfloor + 1$$

Proof. Consider the digroup axiom $x \vdash (x \dashv z) = (x \vdash x) \dashv z$. Let $J = \mathbb{Z}_p$. Consider $a_i \vdash e_{j_1} \sim e_2$. $a_i \vdash e_{j_1} \sim e_{j_2} \Rightarrow (a_i \vdash a_i) \vdash e_{j_1} \sim a_i \vdash e_{j_2} \sim (a_i \circ a_i) \vdash e_{j_1} \sim a_i^2 \vdash e_{j_1}$, where $\circ$ indicates the binary operation of $\mathbb{Z}_p$.
We know that each partition should have order p therefore these two elements must be with another element, one of which must be an identity. By Lemma 6.2 we know that it cannot be either e_{j_1} or e_{j_2}, therefore it must be e_{j_3}. Therefore, $a_i^2 \vdash e_{j_1} \sim a_i \vdash e_{j_2} \Rightarrow a_i^4 \vdash e_{j_1} \sim a_i^3 \vdash e_{j_2}$, and $a_i \vdash e_{j_2} \sim e_{j_3} \Rightarrow a_i^2 \vdash e_{j_2} \sim a_i \vdash e_{j_3}$. Creating a table the pattern becomes apparent.

Partition						
1	$a_i \vdash e_1$	e_2	$a_i^{p-1} \vdash e_3$	$a_i^{p-2} \vdash e_4$	$\cdots$	$a_i^2 \vdash e_p$
2	$a_i^2 \vdash e_1$	$a_i \vdash e_2$	e_3	$a_i^{p-1} \vdash e_4$	$\cdots$	$a_i^3 \vdash e_p$
3	$a_i^3 \vdash e_1$	$a_i^2 \vdash e_2$	$a_i \vdash e_3$	e_4	$\cdots$	$a_i^4 \vdash e_p$
4	$a_i^4 \vdash e_1$	$a_i^3 \vdash e_2$	$a_i^2 \vdash e_3$	$a_i \vdash e_4$	$\cdots$	$a_i^5 \vdash e_p$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
p	e_1	$a_i^{p-1} \vdash e_2$	$a_i^{p-2} \vdash e_3$	$a_i^{p-3} \vdash e_4$	$\cdots$	$a_i \vdash e_p$

Therefore every partition is linked p ways, and a permutation in the partitions would have to have order p. This means the total number of permutations available will correspond to the number of partitions, $\frac{n}{p}$, minus 1 for the partition containing the bar unit, divided by p for the p-wise linking:

$$|\mathrm{D}_i(\mathrm{G})| = \left\lfloor \frac{\frac{n}{p} - 1}{p} \right\rfloor + 1, \text{ where } |\mathrm{J}| = p$$

□

It is clear that it does not matter which p partitions are changed as long as p are changed. Consider the previous table only with $\bar{a_i} \vdash \bar{e_j}$, the grouping of p different partitions together. Simply permute, or relabling these all of the elements in this table by $(\bar{a_i}\ a_i)(\bar{e_j}\ e_j)$, this gives the first table, therefore the digroup structures are isomorphic. Since we are only considering non-isomorphic structures we only consider the first.
Note that Corollary 1.5 on digroups of prime order follows trivially from Theorem 6.3. It is natural to consider digroups of order p^2 and $p \cdot q$ where p, q prime:

Corollary 6.4. *There are only four digroups of order p^2: the trivial digroup, $D_1(p^2$, $\mathbb{Z}_p$, and the groups $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. Let G be a digroup of order p^2 and E its identity set. The only possible decompositions of p^2 are $p^2 \cdot 1$, $p \cdot p$, and $1 \cdot p^2$. Therefore, we only have to consider the cases where $|E| = 1, p$, or p^2.

(1) If $|E| = 1$, then the digroup is a group and it is known that it must be either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.
(2) If $|E| = p$, then Theorem 6.3 tells us there is only $\left\lfloor \frac{\frac{p^2}{p} - 1}{p} \right\rfloor + 1 = \left\lfloor \frac{p-1}{p} \right\rfloor + 1 = 1$ digroup of order p^2. We label this digroup $\mathrm{D}_1(p^2, \mathbb{Z}_p)$.
(3) If $|E| = p^2$, then the digroup is trivial.

□

Corollary 6.5. *Let G be a digroup. If $|G| = p \cdot q$ where p, q prime and $p > q$, then there are only $\left\lfloor \frac{q-1}{p} \right\rfloor + 2$ non-trivial non-group possibilities for G.*

Proof. Let G be a digroup of order $p \cdot q$ and E its identity set. Let $p > q$ without loss of generality. The only possible decompositions of $p \cdot q$ are $(p \cdot q) \cdot 1$, $p \cdot q$, $q \cdot p$, and $1 \cdot (p \cdot q)$. Therefore, we only have to consider the cases where $|E| = 1, p, q$, or $p \cdot q$.

(1) If $|E| = 1$, G is a group.
(2) If $|E| = p$, then Theorem 6.3 tells us there are only $\left\lfloor \frac{\frac{p \cdot q}{q} - 1}{q} \right\rfloor + 1 = \left\lfloor \frac{p-1}{q} \right\rfloor + 1 = 1$ digroups of order $p \cdot q$. In this case, $G = \mathrm{D}_1(p \cdot q, \mathbb{Z}_q)$.
(3) If $|E| = q$, then Theorem 6.3 tells us there is only $\left\lfloor \frac{\frac{p \cdot q}{p} - 1}{p} \right\rfloor + 1 = \left\lfloor \frac{q-1}{p} \right\rfloor + 1$ digroups of order $p \cdot q$.
(4) If $|E| = p \cdot q$, G is trivial.

□

7. Conclusion

While an analogue of Lie's Third Theorem for Leibniz Algebra has yet to be found it has been conjectured by some that the answer still lies within the structure of digroups. Our hopes is that a more detailed structural analysis of digroups can help to point out possibilities for finding that answer.

8. Acknowledgements

This research was conducted as part of the Wabash College Summer Institute in Algebra (WSIA) under the advisement of J.D. Phillips. This work was supported by NSF grant number DMS-0453387.

References

[1] Orin Chein, D.A. Robinson, An "extra" law for characterizing Moufang loops, *Proceedings of the American Mathematical Society* **33** (1) (1972) 29-32.
[2] Catherine Crompton, Linda Scalici, The Structure of Digroups *American Journal of Undergraduate Research*, **5** (2) (2006), 21-27.
[3] Raul Felipe, Generalized Loday algebras and digroups *Communicaciones del CIMAT*, no. I-04-01/21-01-2004.
[4] Michael K. Kinyon, Leibniz algebras, Lie racks, and digroups, *Journal of Lie Theory,* arXiv: math. RA/0403598 **2** 31 Mar 2004.
[5] Michael K. Kinyon, *The Coquecigrue of a Leibniz algebra*, presented at *AlanFest*, a conference in honor of the 60th birthday of Alan Weinstein, Erwin Schrodinger Institute, Vienna, Austria, 4 August 2004; `w3.impa.br/jair/alanposter/coquecigrue.pdf`
[6] Keqin Liu, *Transformation digroups*, arXiv: math.GR/0409265 **1** 16 Sep 2004.
[7] J. L. Loday, *Une version non commutative desalgbres de Lie: Les Algebras de Leibniz*, Enseign. Math. **39** (1993) 269 - 293.
[8] J. L. Loday, *Dialgebras and Related Operands* [Lecture Notes in Math. Series, 1763] (Springer, Berlin, 2001) 7 - 66.
[9] William W. McCune, Prover9, equational reasoning tool, and Mace4, finite model builder Argonne National Laboratory, 2003; `http://www.cs.unm.edu/ mccune/mace4/`
[10] William W. McCune, *Mace 4.0 Reference Manual and Guide*, Argonne National Laboratory Technical Memorandum ANL/MCS-TM-264, 2003; `http://www.mcs.anl.gov/AR/mace4/July-2005/doc/mace4.pdf`
[11] William W. McCune, Prover9 Manual, 2006; `http://www.cs.unm.edu/ mccune/prover9/manual/June-2006C/`
[12] J. D. Phillips, A short basis for the variety of digroups, *Semigroup Forum*, **70** (2005), 466-470.
[13] J.D. Phillips, See Otter digging for algebraic pearls, *Quasigroups and Related Systems*, **10** (2003), 95–114.

Department of Mathematics, Ohio Northern University, 525 S. Main Street, Ada, OH 45810 USA
E-mail address: a-magyar@onu.edu

Department of Mathematics & Computer Science, Wabash College, Crawfordsville, IN 47933 USA
E-mail address: prifoglk@wabash.edu

Department of Mathematics, Bowdoin College, 987 Smith Union, Brunswick, ME 04011 USA
E-mail address: David.White@bowdoin.edu

Department of Mathematics, Purdue University, 465 Northwestern Avenue, West Lafayette, IN 47907 USA
E-mail address: wjyoung@purdue.edu