IN THE NAME OF ALLAH
THE MOST GRACIOUS
THE MOST MERCIFUL

Semiassociative Relation Algebras and Inverse Property Loops

Asif Ali

February 2012

A thesis submitted for the degree of Doctor of Philosophy
of the Australian National University

THE AUSTRALIAN
LIBRARY
NATIONAL UNIVERSITY

To the last of the Prophets of ALLAH,

MUHAMMAD

(Peace and blessings of ALLAH be upon him and his family)

and to his humble follower:

Syed Abul A'Ala Maududi.

Declaration

The work in this thesis is my own, except where otherwise stated. Chapters 3 and 4 are my joint work with Dr. Thomas Kowalski and Chapter 5 is my joint work with Dr. John Slaney. The work of Chapter 5 has been published in [2, 64].

Asif Ali

Acknowledgements

I have no words to express my thankful feelings to Almighty Allah, who enabled me to complete this study.

I would like to express my deep gratitude and sincere thanks to my supervisors Dr. Thomas Kowalski and Professor Dr John Slaney for their keen interest, skillful guidance and valuable suggestions. Without their unlimited help and kind attitude my research would have been incomplete.

I am grateful to Diane Kossatz, Michelle Moravec and Debbie Pioch for all their support during my stay as a student. I had unlimited support from my PhD student Dr Muhammad Shah in Islamabad while re-writing my thesis and it was not possible for me to resubmit my thesis if Dr Shah's encouragement was not there; I really applaud his contributions.

Sincere thanks are due to my wife Asma Siddiqa and my children Sikandar, Pakeza, Dua, Saliha and Tayyaba for their sacrificing stay with me in Australia during my studies. Im not sure I would ever have been able to stay by myself.

I wish to express heartfelt thanks and deep gratitude to my father Haji Abdul Ghafoor and my Mother Razia Begum (late) for their sincere encouragement and for their special morning prayers which helped during almost every second of my stay in Australia. I am also thankful to my brothers Younas Ali, Akram Ali and specially Yousaf Ali and his lovely children for their endless support during my overseas stay. My thanks are also due to my sister Khalida Parveen and her wonderful children who never stopped praying for all my successes in my life. Finally I would like to take the opportunity and place on record my gratitude to the wonderful hardworking people of Australia and specially the NICTA and the Australian National University for their generous financial support. This gave me a unique chance to come to Australia for Ph.D. studies in one of the leading institutions of the world.

Abstract

Semiassociative relation algebras are among the three varieties of algebras introduced by Maddux (R. Maddux, *Some varieties containing relation algebras,* Trans. of Amer. Math. Soc., 272, 501-526, 1982.) and are obtained by replacing the associative law (among the conditions of a relation algebra) by a weaker law known as the semiassociative law.

This thesis mainly investigates the classes of groupoids and multigroupoids whose complex algebras are semiassociative relation algebras and vice versa. We managed to prove that the complex algebra of a groupoid is a semiassociative relation algebra if and only if the groupoid is an inverse property loop (IP loop). We also proved that the complex algebra of a multigroupoid is a semiassociative algebra if and only if the multigroupoid is a polyloop. These results generated enough interest in finding the library of small IP loops and hence we obtained the numbers of non-isomorphic IP loops having order up to 13. Since these were obtained by exhaustive enumeration, they are available for inspection.

We have also included in this thesis the classification of IP loops into some important subclasses; we established that the smallest non-abelian IP loop with the square property is of order 12 and there are 3 of order 12 and only 2 of order 13; the smallest non-associative non-Steiner IP loop that is both flexible and alternative is of order 12 and there are only 2 of order 12 but none of order 13. We also confirmed that the smallest non-associative Steiner loop is of order 10 and that the smallest non-Steiner non-associative C-loop is of order 12. We also listed the non-associative IP loops having Lagrange property and the smallest Hamiltonian non-associative IP loops. It is surprising to note that there are only 25 non-associative abelian IP loops among more than 12,000 small IP loops.

It is well known that the IP loops of exponent 2 are exactly the Steiner loops. In this thesis we also managed to count the IP loops of exponent 3 and exponent 5; there are only 66 non-associative IP loops of exponent 3 (64 are of order 13) and only 10 of exponent 5 (all of order 13).

Contents

Chapter 1

Introduction

1.1 Preliminary Comments

In the current AMS subject classification the theory of relation algebras is included as part of algebraic logic but historically it is the other way around. Indeed, first order predicate calculus originated from the calculus of relations. According to Maddux [41], "*The most important figures in the creation of calculus of relations in the nineteenth century were Augustus De Morgan, Charles Sanders Peirce, and F. W. K. Ernst Schröder. ... The calculus of relations is indeed the result of Peirce's efforts to create algebra out of logic, but these efforts took place decades before the emergence of first order logic in the 1920's and are instead based on the pioneering work of Boole [7]. Peirce's efforts to get a "good general algebra of logic" led him not only to the algebra of relations but also to find convenient ways to explicate and work with his algebra, ways which led directly to first order logic.*"

The earliest results in the field of relation algebras are due to DeMorgan but most of the work in the second half of the 19th century was carried out by Peirce and Schröder. The abstract notion of relation algebras and their initial facts were given by Tarski [66]. In 1951 Jónsson and Tarski [33] introduced the concept of Boolean Algebra with Operators (BAO) and relation algebras were looked on as a kind of BAO.

This thesis concerns one of the 'weaker' notions of the relation algebras known as semiassociative relation algebras. There are a number of ways of looking at these algebras but we consider them as Boolean algebras with operators.

1.1.1 Nonassociative Relation Algebras

A *Boolean algebra with operators* (BAO) is an algebra $\langle A, \wedge, \vee, \neg, 0, 1, (f_i)_{i\in I}\rangle$ such that $\langle A, \wedge, \vee, \neg, 0, 1\rangle$ is a Boolean algebra and each *operator* $f_i = f_i(x_1, \ldots, x_k)$ distributes over join in each coordinate and has 0 as an absorbing element (that is, $f_i(\ldots, 0, \ldots) = 0$). Tarski's *relation algebras* provide one example of a variety of BAOs.

In [39] Maddux introduced three varieties generalising relation algebras by weakening the associativity condition. Namely, a *nonassociative relation algebra* (NA) is a BAO $\langle A, \wedge, \vee, \neg, 0, 1, ;, ^\smile, 1'\rangle$, whose operators ; (binary), $^\smile$ (unary) and 1' (nullary) satisfy in addition:

- $(x\,;y)\wedge z = 0$ iff $(x^\smile\,;z)\wedge y = 0$ iff $(z\,;y^\smile)\wedge x = 0$
- $x\,;1' = 1'\,;x = x$

Chin and Tarski [16] has already proved that the following conditions are derivable from the above two conditions.

- $x^{\smile\smile} = x$
- $(x\,;y)^\smile = y^\smile\,;x^\smile$

The last three of the above four conditions make $\langle A, ;, ^\smile, 1'\rangle$ into an *involutive unital groupoid.*

If a NA satisfies moreover

$$((1'\wedge x)\,;1)\,;1 = (1'\wedge x)\,;1$$

it is a *weakly associative relation algebra* (WA).

If a NA satisfies moreover

$$(x\,;1)\,;1 = x\,;1$$

it is a *semiassociative relation algebra* (SA).

If a NA satisfies moreover

$$(x\,;y)\,;z = x\,;(y\,;z)$$

it is a *relation algebra* (RA).

Incidentally, but perhaps interestingly, at least some of the nonassociative algebras have a rather natural realisation in the "real world" as algebras of binary relations with *weak composition* (see, Definition 2) instead of the usual composition of relations. As far as we know, all nonassociative algebras considered in this connection are semiassociative. See, e.g., [22] for more.

1.1.2 Complex Algebras

For any relational structure $\mathbb{W} = (W, (R_i)_{i\in I})$, its *complex algebra* $\mathbf{Cm}(\mathbb{W})$ is the algebra $\langle \mathcal{P}(W), \cap, \cup, -, \emptyset, W, (f_i)_{i\in I}\rangle$, where each f_i is a k-ary function associated with the $k+1$-ary relation R_i, in the following way: for subsets $X_1, \ldots, X_k$ of W we put $f_i(X_1, \ldots, X_k) = \{w \in W\colon (\exists x_1 \in X_1, \ldots, x_k \in X_k)(w, x_1, \ldots, x_k) \in R_i\}$. Notice that functions f_i above are operators, so all complex algebras are BAOs.

1.1.3 Loops With Inverse Property

Although loops are usually defined as groupoids with unique solution property (i.e., quasigroups) and possessing a unit element, we will adopt a more universal-algebraic view and define a loop to be an algebra $(L, \cdot, \backslash, /, e)$ satisfying the following identities:

1. $x(x\backslash y) = y$
2. $x\backslash(xy) = y$
3. $(x/y)y = x$
4. $(xy)/y = x$
5. $xe = x = ex$

In each loop an element x has left and right inverses, respectively, e/x and $x\backslash e$. If these coincide, we write x^{-1} for both. A loop has the *inverse property*, if it satisfies

(6) $x\backslash e = e/x$

(7) $(y\backslash e)(yx) = x$

(8) $(xy)(e/y) = x$

Thus, loops with the inverse property (*IP loops*) form a subvariety of loops. In fact, it is easy to show that IP loops are term equivalent to the variety of algebras $(L, \cdot, ^{-1}, e)$ satisfying the following identities

(i) $xe = x = ex$

(ii) $xx^{-1} = e = x^{-1}x$

(iii) $x^{-1}(xy) = y$

(iv) $(xy)y^{-1} = x$

upon defining $x^{-1} = x\backslash e$ (or e/x) one way, and $x\backslash y = x^{-1}y$, $x/y = xy^{-1}$ the other. This will be our official definition of IP loops from now on. It is well known that *Moufang loops* (probably the most investigated variety of loops) defined by the identity

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

have the inverse property and thus form a subvariety of IP loops. For more on loops, see the old but still good [11].

1.1.4 Polyloops

We define another notion of multigroupoids which not only generalises IP loops, it also extends the concept of polygroup. The motivation of polyloops comes from the fact that there are well known multigroupoids that satisfy all other conditions of polygroups except the associative law. One of these examples is the weak composition table of RCC-10 given in [23].

1.2 Summary of Results and Outcomes

In this section we outline the main results and outcomes that were obtained in the thesis with precise references to their place of occurrence later.

1.2.1 Complex Algebras of IP Loops

Any groupoid $(G, \cdot)$ can be viewed as a relational structure $\mathbb{G} = (G, T)$ where T is a ternary relation defined by setting $T(a, b, c)$ iff $a = b \cdot c$. Although this agrees with the formal definition of complex algebras, in the context of groupoids it is customary to work instead with a relation T', defined by $T'(a, b, c)$ iff $a \cdot b = c$ iff $T(c, a, b)$. This agrees with the traditional definition of *complex multiplication* as $X \circ Y = \{xy\colon x \in X, y \in Y\}$. If G has a unit element e we may view G as the structure $\mathbb{G} = (G, T, \{e\})$. Similarly, if G has the unique solution property we may view G as $\mathbb{G} = (G, T, R, L, \{e\})$, where L and R are binary relations such that xRy (xLy) iff y is the right (left) inverse of x.

One natural example of such a complex algebra occurs when G is a group. In fact, Jónsson and Tarski showed (see [33], [34]) the following:

Theorem 1. *The complex algebra of a groupoid $(G, \cdot)$ is a relation algebra if and only if $(G, \cdot)$ is a group.*

This result outlines the exact contribution of the complex algebras of groupoid structure in the class of relation algebras. The class of subalgebras of this type is known as *Group Relation Algebras* or GRAs. In the presence of Theorem 1 it was a natural question to ask that "*What are the groupoid structures whose complex algebras are semiassociative algebras and vice versa*?" The answer to this question leads us to the findings recorded in Chapter 4. The main result that we managed to prove in Chapter 4 is given in the following:

Theorem 4 The complex algebra of a groupoid $(L, \cdot)$ is a semiassociative relation algebra if and only if $(L, \cdot)$ is an IP loop.

Remark 1. *Later on we found that this theorem has already been done by Maddux [38]. But we have done it independently and can be considered as a second proof.*

It is worth mentioning however that if L is not an IP loop then the complex algebra of L is not even a nonassociative relation algebra. In other words the complex algebras of groupoids is not a source for NA and WA that are not SA. By analogy with *group relation algebras* (GRAs) we defined *loop semiassociative relation algebras* (LSAs).

1.2.2 Complex Algebras of Polyloops

A multigroupoid is a non-empty set M together with a mapping $\cdot$ of $M \times M$ into the power set of M. That is for each ordered pair (a, b) of elements of M, $a \cdot b$ is a non-empty subset of M. A multigroupoid can be thought of as a relational structure $\mathbb{M} = (M, T)$ where T is a ternary relation defined by: $(x, y, z) \in T$ if and only if $x \in y \cdot z$. This defines a binary operation f on $\mathcal{P}(M)$ by:

$$f(X, Y) = \{a \in M \mid x \in X, y \in Y \text{ and } (a, x, y) \in T\}.$$

An example of such a complex algebra was seen in the case of M being a polygroup (see [18]). In that case Comer proved that the complex algebra of M is a complete atomic integral *relation algebra* and vice versa. Apart from defining another notion of multigroupoid by the name of 'Polyloop' and providing a variety of examples, Chapter 3 investigates the contribution of complex algebras of multigroupoids to the class of semiassociative relation algebras. The summary of our findings in this regard is recorded in the following:

Theorem 3

(1) $\mathbf{Cm}(\mathbb{M})$ is a complete atomic integral SA for every polyloop $\mathbb{M}$.

(2) For every complete atomic integral SA $\mathbb{A}$ the system

$$At(\mathbb{A}) = \langle At_{\mathbb{A}}, *, ^{-1}, e\rangle,$$

where $At_{\mathbb{A}}$ is the set of atoms of $\mathbb{A}$, is a polyloop.

(3) If $\mathbb{M}$ is a polyloop and $\mathbb{A}$ is a complete atomic Integral SA, then

$$\mathbb{M} \cong At(\mathbf{Cm}(\mathbb{M})$$

and

$$\mathbb{A} \cong \mathbf{Cm}[At(\mathbb{A})].$$

Apart from this result we managed to utilize a computer, using constraint programming, in order to produce polyloops and their double quotients, of a general as well as a particular interest.

In Chapter 4, we also establish a sufficient condition on some nice examples of polyloops that forces those polyloops to be polygroups.

1.2.3 Small IP Loops

Counting and listing different subclasses of loops has a long history. But it is surprising to note that although IP loops were defined in the 1940's there is no data available on small IP loops. Chapter 5 reports the numbers of non-isomorphic IP loops having order up to 13. Since these were obtained by exhaustive enumeration, they are available for inspection. We have also included the classification of IP loops into important subclasses. We will discuss this later on. For a quick view see Table 5.4, that gives the number of isomorphism classes of IP loops of each order up to 13 and tells how many of those are commutative.

Chapter 2

Definitions, notation and basic facts

2.1 Introduction

In this chapter we give definitions, notation and basic facts which are used throughout the thesis. This is partly for fixing terminology, partly to provide an easy reference to results we need to quote from the literature and partly for setting up notation. As a general rule we follow the notation and terminology used by Bruck's survey [11].

Other references will be to McKay and Myrvold [44], and Comer [18].

The reader should be able to bypass much of this chapter at a first reading, using it as a reference for results and terminology quoted in later chapters.

2.2 Normal Subloops, Quotient loops and others

A **Latin square** of order n is a $n \times n$ array $L = (l_{ij})$ such that each row and each column contains a permutation of $I_n = \{1, 2, ..., n\}$. A **quasigroup** G is a set together with a binary operation $\circ$ such that the equations $g \circ x = h$ and $y \circ g = h$ have unique solutions for each $g, h \in G$. A quasigroup G is a **loop** if it contains an element e such that $g \circ e = e \circ g = g$ for all $g \in G$.

A subloop H of a loop G is said to be **normal** if for all $x, y \in G$, we have $xH = Hx$, $(Hx)y = H(xy)$ and $y(xH) = (yx)H$. This means that any subloop contained in the **centre** of G (the set of those elements $z \in G$ such that $zx = xz$

for all $x \in G$) is normal in G. Also the intersection of any non-empty set of normal subloops of G is normal in G. For any normal subloop H of G and $y \in xH$ we have $y = xh$ for some $h \in H$ and hence $yH = (xh)H = x(hH) = xH$. This means that for all $y \in xH$ we get $xH = yH$ and consequently the left cosets of H in G partition G. Using this fact it is easy to see that, in finite loops, the order of a normal subloop divides the order of the loop. Consider the following loop:

$*$	1	2	3	4	5	6	7	8	9
$e=1$	1	2	3	4	5	6	7	8	9
2	2	3	1	6	7	8	9	4	5
3	3	1	2	8	9	4	5	6	7
4	4	8	6	5	1	9	3	7	2
5	5	9	7	1	4	3	8	2	6
6	6	4	8	9	2	7	1	5	3
7	7	5	9	2	8	1	6	3	4
8	8	6	4	7	3	5	2	9	1
9	9	7	5	3	6	2	4	1	8

x	x^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6
8	9
9	8

It has 4 subloops $\{1,2,3\}$, $\{1,4,5\}$, $\{1,6,7\}$ and $\{1,8,9\}$. Although all of them have orders dividing the order of the loop only $\{1,2,3\}$ is normal. This means it is not necessary that a subloop dividing the order of a loop be normal (already for groups this is not necessary).

For a normal subloop H of a loop G, let G/H be the set of all left cosets of H in G. Define $*$ on G/H by,

$$(xH) * (yH) = (xy)H$$

for $xH, yH \in G/H$. It is routine to show that G/H is a loop under $*$. This loop is called the **quotient loop** of G **modulo** H.

On this basis we can define $\theta : G \longrightarrow G/H$ by $\theta(x) = xH$ and see that it is a homomorphism of G onto G/H. Conversely if α is a homomorphism from a loop G to a loop M then the set K of all $g \in G$ such that $\alpha(g) = e_M$, is a normal subloop of G and is called the **kernel** of α.

A loop G is said to have a **right coset expansion modulo** its subloop H provided the right cosets of H partition G. The condition for a right coset expansion is:

If $y \in Hx$ *then* $Hx = Hy$ *or* $H(hx) = Hx$ *for all* $h \in H$ *and* $x, y \in G$. A loop G is said to have the **weak Lagrange property** if the order of each of its subloops divides the order of G and G is said to have the **strong Lagrange**

property if each subloop of G has the weak Lagrange property. A loop may have the weak Lagrange property but not the strong Lagrange property. Four of the six nonisomorphic loops of order 5 have subloops of order 2 and hence fail to satisfy the weak Lagrange property. Let K be one of these loops. As noted in [52], page 13, consider a loop G of order 10 that has K as its subloop. Then G has the weak but not the strong Lagrange Property. The following lemma explains it further.

Lemma 1. *([11], Lemma V.2.1) Let H be a normal subloop of the subloop K of the loop G. If H and K/H have the strong or the weak Lagrange property then so has K.*

Let $\mathbb{L}$ be any class of loops such that:

(1) Every subloop of a member of $\mathbb{L}$ is in $\mathbb{L}$.

(2) Every loop which is a homomorphic image of a member of $\mathbb{L}$ is in $\mathbb{L}$.

By a **nilpotency function** f for $\mathbb{L}$ we mean a function $f : \mathbb{L} \longrightarrow \mathbb{L}$ with the following properties:

(a) If G is in $\mathbb{L}$, $f(G)$ is a uniquely defined subloop of G.

(b) If G is in $\mathbb{L}$ and if H is a subloop of G then $H \cap f(G) \subseteq f(H)$.

(c) If G is in $\mathbb{L}$ and if θ is a homomorphism of G onto a loop M then $\theta(f(G)) \subseteq f(\theta(G))$.

(d) If G is in $\mathbb{L}$, N is a normal subloop of G and if A is the intersection of all normal subloops K of G such that NK/K is a subloop of $f(G/K)$ then NA/A is a subloop of $f(G/A)$.

If $\mathbb{L}$ is the whole class of loops and $f(G)$ is the centre of G then this nilpotency is called **central nilpotency**.

For each element a of G consider the mappings $L(a)$ and $R(a)$ on G defined by $xL(a) = ax$ and $xR(a) = xa$ which are clearly permutations of G. The subgroup of the permutation group of G generated by all $L(a)$ and $R(a)$ is called the **multiplication group** of G (let us denote it by $M(G)$) and the subgroup $I(G)$ of $M(G)$ consisting of elements α such that $e\alpha = e$ is called the **inner mapping group** of G. It is obvious that $M(G)$ is transitive in G and the subsets $A = \{L(a) \mid a \in G\}$ and $B = \{R(a) \mid a \in G\}$ are the left and right transversals of

$I(G)$ in $M(G)$ respectively. Also that A and B are $I(G)$-connected transversals means the commutator subgroup $[A, B] \subseteq I(G)$ and that the core of $M(G)$ in $I(G)$ is trivial (core of a subset S of a group G is the largest normal subgroup of G contained in S; it is denoted by $L_G(S)$). The relation between multiplication groups of loops and connected transversals is given by the following theorem:

Theorem 2. *([49], Theorem 4.1). A group G is isomorphic to the multiplication group of a loop if and only if there exists a subgroup H satisfying $L_G(H) = 1$ and H-connected transversals A and B such that G is generated by $A \cup B$.*

2.3 Important subclasses of Loops

Since the number of non-isomorphic loops of a given order is very large, most of the work in loop theory has been done in subvarieties of loops. Most of these varieties are defined by weakening the associative law which still makes them more general than groups. A loop G with identity element e is said to have the **flexible property** if for all $x, y \in G$ we have $x(yx) = (xy)x$; it is said to have the **right alternative property** if $x(yy) = (xy)y$ and the **left alternative property** if $y(yx) = (yy)x$. An **alternative loop** is a loop which is both left and right alternative.

Let G be a loop with identity element e. Then G is said to be a **left inverse property loop** if for all $x \in G$ there exists $x' \in G$ such that $x'x = e$ and for all $y \in G$ we have $x'(xy) = y$. Similarly G is said to be a **right inverse property loop** if for all $x \in G$ there exists $x'' \in G$ such that $xx'' = e$ and for all $y \in G$ we have $(yx)x'' = y$. Here G is said to have the **inverse property** (or IP) if it has both left and right inverse properties. In that case for $x \in G$ we have $x' = x'e = x'(xx'') = x''$ and we denote x', x'' by x^{-1}. G is said to have **anti-automorphic inverse property** if it satisfies the identity $(xy)^{-1} = y^{-1}x^{-1}$. Such loops are called **anti-automorphic inverse property loops or AAIP loops**. It is easy to see that IP loops satisfy the **anti-automorphic inverse property**. G is said to have **automorphic inverse property** if it satisfies the identity $(xy)^{-1} = x^{-1}y^{-1}$. Such loops are called **automorphic inverse property loops**.

If $\mathbb{L}$ is the class of all IP loops then the nilpotency function $f(G)$ may be the **Moufang Nucleus** of G (the set of all a in G such that for all x, y in G we have $a((xy)a) = (ax)(ya)$).

A **RIF loop** is an IP loop G such that $(x^{-1})\alpha = (x\alpha)^{-1}$ for all $x \in G$ and all

$\alpha \in I(G)$.

A loop G is said to be **Steiner loop** if for all $x, y \in G$, we have $x^2 = e$ and $x(xy) = y$. It is easy to see that Steiner loops are exactly the IP loops of exponent 2 and are a subclass of RIF loops. RIF loops also include the most commonly known variety of loops which is defined by the following;

A loop G is said to be a **Moufang loop** if it satisfies the following properties: for all $x, y, z \in G$,

$$(x(yz))x = (xy)(zx),$$

$$((xy)z)y = x(y(zy))$$

and

$$((yz)y)x = y(z(yx)).$$

By Lemma VII.3.1 of Bruck [11] these equations are equivalent and it follows from Lemma VII.3.2 of [11] that every Moufang loop is RIF. It is also easy to see that the direct product of a non-associative Moufang loop and a non-associative Steiner loop is a RIF loop but is neither Moufang nor Steiner.

A loop G is said to be a **power-associative loop** if every subloop generated by a single element of G is a subgroup and is called **diassociative** if the subloop generated by any two elements of G is a subgroup of G. G is said to be **Hamiltonian** if every subloop of G is normal. It is obvious that diassociative loops are IP loops and are both flexible and alternative. Also by Moufang's Theorem (page 117 of [11]) every Moufang loop is diassociative.

A loop G is said to be a **C-loop** if for all $x, y, z \in G$ we have

$$x(y(yz)) = ((xy)y)z.$$

It is obvious that Steiner loops are C-loops; Phillips and Vojtěchovský [53] proved that C-loops are both alternative and IP loops. G is said to be an **A-loop** if each $\alpha \in I(G)$ is an automorphism and it is shown in Bruck and Paige [12] that every IP loop that is also an A-loop is diassociative.

2.4 Boolean Algebras With Operators and Related Terminology

A **first-order language** $\mathcal{L}$ is defined as a set consisting of a collection $\mathcal{R}$ of relation symbols and a collection $\mathcal{F}$ of function symbols and, for each member of $\mathcal{R}$ there exists a positive integer and a non-negative integer associated to each

member of $\mathcal{F}$ called the **arity** of the symbol. The subset of $\mathcal{R}$ containing symbols having arity n is denoted by $\mathcal{R}_n$ and the subset of $\mathcal{F}$ containing symbols of arity n is denoted by $\mathcal{F}_n$. The language $\mathcal{L}$ is called a **language of algebras** if $\mathcal{R} = \emptyset$ and is called a **language of relational structures** if $\mathcal{F} = \emptyset$.

A relation S is said to be an n**-ary relation** on a nonempty set A if $S \subseteq A^n$. If $n = 1$, S is called **unary**, for $n = 2, S$ is called **binary** and if $n = 3$ then S is said to be **ternary**.

Let $\mathcal{L}$ be a first-order language (as defined above) and A be a nonempty set then the ordered pair $\mathbb{A} = \langle A, L \rangle$ is called the **first order structure of type** $\mathcal{L}$. Here L consists of a family R of relations indexed by $\mathcal{R}$ and a family F of functions indexed by $\mathcal{F}$ and A is called the **universe** of $\mathbb{A}$. If $\mathcal{R} = \emptyset$ then $\mathbb{A}$ is called an **algebra** and if $\mathcal{F} = \emptyset$ then $\mathbb{A}$ is called a **relational structure**. If $\mathcal{L}$ is finite, if $\mathcal{R} = \{S_1, S_2, \ldots, S_n\}$ and $\mathcal{F} = \{f_1, f_2, \ldots, f_m\}$ then $\mathbb{A}$ is denoted by $\langle A, f_1, f_2, \ldots, f_m, S_1, S_2, \ldots, S_n \rangle$.

For any relational structure $\mathbb{A} = (A, (r_i)_{i \in I})$, its **complex algebra** $\mathbf{Cm}(\mathbb{A})$ is the algebra $\langle \mathcal{P}(A), \cap, \cup, -, \emptyset, A, (f_i)_{i \in I} \rangle$, where each f_i is a k-ary function associated with the $k+1$-ary relation r_i, in the following way: for subsets $X_1, \ldots, X_k$ of A we put $f_i(X_1, \ldots, X_k) = \{a \in A \colon (\exists x_1 \in X_1, \ldots, x_k \in X_k)(a, x_1, \ldots, x_k) \in r_i\}$.

Let $\mathbb{A}_1 = \langle A_1, L_1 \rangle$ and $\mathbb{A}_2 = \langle A_2, L_2 \rangle$ be structures of type $\mathcal{L}$. A **bounded morphism** $\alpha : \mathbb{A}_1 \longrightarrow \mathbb{A}_2$ is a mapping $\alpha : A_1 \longrightarrow A_2$ such that for each relational member r of L, if r_1, r_2 are the relations indexed by r in L_1, L_2, then

$$(c_0, c_1, \ldots, c_n) \in r_1$$

implies

$$(\alpha(c_0), \alpha(c_1), \ldots, \alpha(c_n)) \in r_2$$

and for each member $r_1 \in L_2$ if

$$(\alpha(c), d_1, \ldots, d_n) \in r_1$$

then there exists $r_2 \in L_1$ and $b_1, \ldots, b_n \in A_1$ such that $\alpha(b_l) = c_l$ for $1 \leq l \leq n$ and

$$(c, b_1, \ldots, b_n) \in r_2.$$

A **Boolean algebra with operators** (BAO) is an algebra $\langle A, \wedge, \vee, \neg, 0, 1, (f_i)_{i \in I} \rangle$ such that $\langle A, \wedge, \vee, \neg, 0, 1 \rangle$ is a Boolean algebra and each **operator** $f_i = f_i(x_1, \ldots, x_k)$ distributes over join in each coordinate and has 0 as an absorbing element (that is, $f_i(\ldots, 0, \ldots) = 0$).

Notice that functions f_i in the definition of complex algebra are operators, so all complex algebras are BAOs.

A nonempty class $\mathcal{V}$ of algebraic structures of type $\mathcal{L}$ is said to be a **variety** if it is the class of all algebras that satisfy a given set of identities. Equivalently by a result of Birkhoff a variety is a class that is closed under subalgebras, homomorphic images and direct products. A subclass $\mathcal{W}$ of $\mathcal{V}$ which is also a variety is called a **subvariety** of $\mathcal{V}$.

An algebra $\mathbb{A} = \langle A, \wedge, \vee, \neg, 0, 1, \circ, ^{\smile}, e\rangle$ is said to be a **relation algebra** if $\wedge, \vee$ and $\circ$ are binary operations on A, $\neg$ and $^{\smile}$ are unary operations on A, and $0, 1$ and e are constants satisfying the following properties (for $x, y, z \in A$):

(RA0) $\langle A, \wedge, \vee, \neg, 0, 1\rangle$ is a Boolean algebra;

(RA1) $(x \circ y) \circ z = x \circ (y \circ z)$;

(RA2) $x \circ e = x = e \circ x$;

(RA3) $(x \circ y) \wedge z = 0$ iff $(x^{\smile} \circ z) \wedge y = 0$ iff $(z \circ y^{\smile}) \wedge x = 0$;

and $(y \vee z) \circ x = (y \circ x) \vee (z \circ x)$;

This definition of relation algebras is due to Tarski [66]. In [39] Maddux noticed that most of the properties of relation algebras do not depend on the associativity of $\circ$. On this basis Maddux introduced three new varieties of algebras which extend the variety RA of relation algebras. In these varieties (RA1) is either omitted or replaced by one of the following two laws;

(SA) $x \circ (1 \circ 1) = (x \circ 1) \circ 1$.

(WA) $(1' \wedge x) \circ (1 \circ 1) = ((1' \wedge x) \circ 1) \circ 1$.

The largest of these varieties is called Nonassociative Relation Algebras (NA) which is obtained by omitting (RA1). The other two varieties are called Weakly Associative Relation Algebras (WA; when (RA1) is replaced by (WA)) and Semiassociative Relation Algebras (SA; when (RA1) is replaced by (SA)). It is immediate to see that $RA \subseteq SA \subseteq WA \subseteq NA$.

Chapter 3

Polyloops and SA relation Algebras

3.1 Introduction

In this chapter we introduce yet another notion of multigroupoid which has not been seen in the literature before. This generalises the concepts of both IP loop as well as polygroup and therefore, correctly speaking, it should be called polyloop with inverse property or polyIPloop. The only reason for adopting "polyloop" is that it is shorter. The motivation of this notion of multigroupoid comes from the fact that there are well known multigroupoids that satisfy all other conditions of polygroups except the associative law. The most interesting of these examples is the weak composition table of RCC-10 given in [23].

A good account of polygroups is given in [18] which is also the source of most ideas proven in this chapter.

In Section 1, we give a formal definition of polyloops and give important examples from different areas of interest while in Section 2 we establish a strong connection between SA relation algebras and polyloops. In Section 3 we give a sufficient condition which converts some nice examples of polyloops into polygroups.

3.2 Definition and Examples of Polyloops

Definition 1. *A polyloop is a system* $\mathbb{M} = \langle M, *, ^{-1}, e\rangle$ *(where* $e \in M$, $^{-1}$ *is a unary operation on* M *and* $*$ *is a multi-operation (namely* $x * y \subseteq M$ *is a non-empty set for every* $x, y \in M$*), which satisfies the following axioms for all*

$x, y, z \in M$:

(P_1) $x \in (x * y) * y^{-1}$ *and* $x \in y^{-1} * (y * x)$;

(P_2) $x * e = \{x\} = e * x$;

(P_3) $e \in x * x^{-1}$ *and* $e \in x^{-1} * x$;

(P_4) $x \in y * z$ *implies* $y \in x * z^{-1}$ *and* $z \in y^{-1} * x$.

We give a set of nice examples of the polyloops that are not loops or polygroups; they also demonstrate how polyloops occur naturally in a variety of research areas.

Example 1. *Polyloop of order 5.*

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	$\{1,4\}$	$\{1,2\}'$	$\{1\}'$	$\{1,2\}'$
3	3	$\{1,2\}'$	$\{4,5\}'$	2	2
4	4	$\{1\}'$	2	$\{1,2\}$	2
5	5	$\{1,2\}'$	2	2	$\{1,2\}$

Example 2. *Polyloop of order 6.*

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	$\{1,5\}$	$\{5,6\}$	$\{4,5,6\}$	$\{1\}'$	$\{1,2\}'$
3	3	$\{5,6\}$	$\{1,4\}$	3	2	2
4	4	$\{4,5,6\}$	3	$\{1,2\}$	2	2
5	5	$\{1\}'$	2	2	$\{1,2\}$	2
6	6	$\{1,2\}'$	2	2	2	$\{1,2\}$

Example 3. *Polyloop of order 7.*

$*$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	$\{1,4,6\}$	$\{6,7\}$	$\{1,3\}'$	$\{1,2,3\}'$	$\{1\}'$	$\{1,2\}'$
3	3	$\{6,7\}$	$\{1,4,5\}$	3	3	2	2
4	4	$\{1,3\}'$	3	$\{1,2\}$	2	2	2
5	5	$\{1,2,3\}'$	3	2	$\{1,2\}$	2	2
6	6	$\{1\}'$	2	2	2	$\{1,2\}$	2
7	7	$\{1,2\}'$	2	2	2	2	$\{1,2\}$

Example 4. *Polyloop of order 8.*

$*$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	$\{1,5,7\}$	$\{4,7,8\}$	$\{1,2\}'$	$\{1,3\}'$	$\{1,2,3\}'$	$\{1\}'$	$\{1,2\}'$
3	3	$\{4,7,8\}$	$\{2,7,8\}'$	$\{2,3\}$	3	3	2	2
4	4	$\{1,2\}'$	$\{2,3\}$	$\{1,2\}$	2	2	2	2
5	5	$\{1,3\}'$	3	2	$\{1,2\}$	2	2	2
6	6	$\{1,2,3\}'$	3	2	2	$\{1,2\}$	2	2
7	7	$\{1\}'$	2	2	2	2	$\{1,2\}$	2
8	8	$\{1,2\}'$	2	2	2	2	2	$\{1,2\}$

Before going to the next example, the following definition should be noted.

Definition 2. *[57]* Composition ($\circ$) *of two relations R and S is defined as the relation $R \circ S = \{(a,b) \mid \exists c : (a,c) \in R$ and $(c,b) \in S\}$. Let $\mathcal{A}$ be a set of atomic relations. A* Weak composition ($\square$) *of two relations S and T is defined as the strongest relation $R \in 2^{\mathcal{A}}$ which contains $S \circ T$, or formally, $S \square T = \{R_i \in \mathcal{A} \mid R_i \cap S \circ T \neq \emptyset\}$. if a weak composition is represented by a table then such a table is called* Weak composition table.

Example 5.

The Region Connection Calculus (RCC): This calculus was introduced by Randell et al. [19] to formalise intuitive reasoning about space. In RCC the base set is the set of abstract regions in an abstract space and the base relation is a connection C (for regions x and y, $C(x,y)$ means x is connected to y); other relations are defined by the following:

$P(x,y)$	x is a part of y	$\forall z$, $C(x,z)$ implies $C(y,z)$
$PP(x,y)$	x is a proper part of y	$P(x,y)$ but $\neg P(y,x)$
$O(x,y)$	x overlaps y	$\exists z$ such that $P(x,z)$ and $P(y,z)$
$PO(x,y)$	x properly overlaps y	$O(x,y)$ but $\neg P(x,y)$ and $\neg P(y,x)$
$EC(x,y)$	x is externally connected with y	$C(x,y)$ but $\neg O(x,y)$
$TPP(x,y)$	x is a tangential proper part of y	$PP(x,y)$ and $\exists z[EC(z,x)$ and $EC(z,y)]$
$NTPP(x,y)$	x is a non-tangential proper part of y	$PP(x,y)$ and $\neg\exists z[EC(z,x)$ and $EC(z,y)]$
$DC(x,y)$	x is disconnected from y	$\neg C(x,y)$
$EQ(x,y)$	x is identical to y	$P(x,y)$ and $P(y,x)$

Converses of all these relations are defined in the usual sense. Figure 3.1 explains these relations if x, y and z are considered as discs in the Euclidean plane.

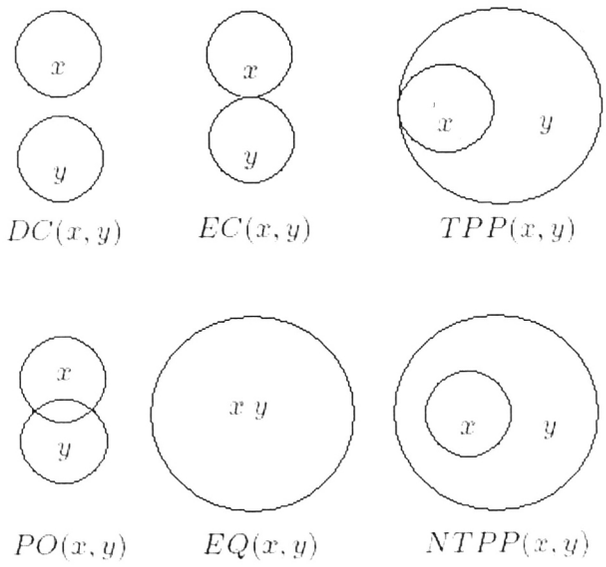

Figure 3.1: Figure 1.

RCC axioms:

A model for the RCC consists of:

(i) a base set $U = R \cup N$, where R, N are disjoint;

(ii) a binary relation C on R;

(iii) two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R \cup N$;

(iv) a special $u \in R$ and a unary operation $- : R_0 \to R_0$ where $R_0 = R \backslash \{u\}$.

Here R can be interpreted as the set of all non-empty regions; N as consisting of just the empty region 0; u as the universal region and R_0 as the set of all non-empty proper regions. The binary operations $+$ and $\cdot$ would then be the union and intersection of the regions while the unary operation $-$ would be the complement of regions.

There are 8 axioms for the *RCC*:

RCC 1. $\forall x \in R$, $C(x, x)$

RCC 2. $\forall x, y \in R$, $C(x, y) \Rightarrow C(y, x)$

RCC 3. $\forall x \in R$, $C(x, u)$

RCC 4. $\forall x \in R, y \in R_0$,

(a) $C(x, -y) \iff \neg NTPP(x, y)$

(b) $O(x, -y) \iff \neg P(x, y)$

RCC 5. $\forall x, y, z \in R$, $C(x, y + z) \iff C(x, y)$ or $C(x, z)$

RCC 6. $\forall x, y, z \in R$, $C(x, y \cdot z) \iff \exists w \in R$ such that ($P(w, y)$ and $P(w, z)$ and $C(x, w)$)

RCC 7. $\forall x, y \in R$, $x \cdot y \in R \iff O(x, y)$

RCC 8. If $P(x, y)$ and $P(y, x)$, then $x = y$.

It is easy to see that P is a partial order. If we denote the relations of RCC-8 by integers as in Table 3.1 then the weak composition table for RCC-8 is given by:

notation	Relations	notation	Relations
1	EQ	5	TPP
2	DC	6	$NTPP$
3	EC	7	$TPP^{\smile}$
4	PO	8	$NTPP^{\smile}$

Table 3.1: Alternate notation for RCC-8 relations

$\circ_w$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	$*$	$\{1,7,8\}'$	$\{1,7,8\}'$	$\{1,7,8\}'$	$\{1,7,8\}'$	2	2
3	3	$\{1,5,6\}'$	$\{6,8\}'$	$\{1,7,8\}'$	$\{3,4,5,6\}$	$\{4,5,6\}$	$\{2,3\}$	2
4	4	$\{1,5,6\}'$	$\{1,5,6\}'$	$*$	$\{4,5,6\}$	$\{4,5,6\}$	$\{1,5,6\}'$	$\{1,5,6\}'$
5	5	2	$\{2,3\}$	$\{1,7,8\}'$	$\{5,6\}$	6	$\{7,8\}'$	$\{1,5,6\}'$
6	6	2	2	$\{1,7,8\}'$	6	6	$\{1,7,8\}'$	$*$
7	7	$\{1,5,6\}'$	$\{3,4,7,8\}$	$\{4,7,8\}$	$\{1,4,5,7\}$	$\{4,5,6\}$	$\{7,8\}$	8
8	8	$\{1,5,6\}'$	$\{4,7,8\}$	$\{4,7,8\}$	$\{4,7,8\}$	$\{2,3\}'$	8	8

Here $*$ denotes the universal relation and $'$ denotes complement.

Let S be the incomparability relation which means $S(x,y)$ is defined as $\neg P(x,y)$ and $\neg P(y,x)$. This extends $RCC-8$ if we replace EC by

$$ECD = -(PP \circ PP^{\smile} \cup PP^{\smile} \circ PP),$$

$$ECN = EC \cap -ECD,$$

and PO by

$$PON = S \cap (PP^{\smile} \circ PP) \cap (PP \circ PP^{\smile}),$$

$$POD = S \cap (PP^{\smile} \circ PP) \cap -(PP \circ PP^{\smile}).$$

Here $\circ$ denotes the composition of relations. Then

- $ECD(x,y) \Longleftrightarrow EQ(x,-y)$,
- $ECN(x,y) \Longleftrightarrow EC(x,y)$ and $x+y \neq u$,
- $PON(x,y) \Longleftrightarrow S(x,y)$ with $x \cdot y \neq 0$ and $x+y \neq u$,
- $POD(x,y) \Longleftrightarrow S(x,y)$ with $x \cdot y \neq 0$ and $x+y = u$.

This gives us 10 base relations and the resulting system is called $RCC10$. Again, if we denote the relations by numbers as listed in Table 3.2 then the weak composition table of $RCC10$ is given here:

$\circ_w$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	$\{3,6\}'$	8	$\{2,4,6,7,8\}$	8	$\{2,4,6,7,8\}$	$\{2,4,6,7,8\}$	$\{1,9,10\}'$	2	2
3	3	10	1	9	$\{7,8\}$	6	5	5	4	2
4	4	$\{2,4,6,9,10\}$	7	$\{3,5,8,10\}'$	$\{7,8\}$	$\{2,4,6,7,8\}$	$\{1,2,9,10\}'$	$\{5,6,7,8\}$	$\{2,4\}$	2
5	5	10	$\{9,10\}$	$\{9,10\}$	$\{2,3,4\}'$	$\{5,6,9,10\}$	5	5	$\{1,2,7,8\}'$	$\{1,7,8\}'$
6	6	$\{2,4,6,9,10\}$	6	$\{2,4,6,9,10\}$	$\{5,6,7,8\}$	$*$	$\{5,6,7,8\}$	$\{5,6,7,8\}$	$\{2,4,6,9,10\}$	$\{2,4,6,9,10\}$
7	7	2	3	$\{2,4\}$	$\{1,2,9,10\}'$	$\{2,4,6,7,8\}$	$\{7,8\}$	8	$\{1,2,4,6,7,9\}$	$\{2,4,6,8,10\}$
8	8	2	2	4	$\{1,9,10\}'$	$\{2,4,6,7,8\}$	8	8	$\{2,4,6,7,8\}$	$\{3,5\}'$
9	9	$\{2,4,6,9,10\}$	5	$\{1,2,7,8\}'$	5	$\{5,6,9,10\}$	$\{1,5,6,7,9\}$	$\{5,6,7,8\}$	$\{9,10\}$	10
10	10	$\{1,7,8\}'$	5	$\{5,6,9,10\}$	5	$\{5,6,9,10\}$	$\{5,6,9,10\}$	$\{2,3,4\}'$	10	10

notation	Relations	notation	Relations
1	EQ	6	PON
2	DC	7	TPP
3	ECD	8	$NTPP$
4	ECN	9	$TPP^{\smile}$
5	POD	10	$NTPP^{\smile}$

Table 3.2: Alternate notation for RCC10 relations

This table shows that the multiplication is not associative; for example

$$(10 \circ_w 5) \circ_w 9 \neq 10 \circ_w (5 \circ_w 9).$$

This means the complex algebra of this multigroupoid is non-associative. However it has been verified by computer that this algebra is semiassociative.

This example is recorded from [23].

Example 6.

Serial Partition: Let U be a non-empty set. Let M be a partition of $U \times U$ such that each $x \in M$ is a serial relation on U (a relation x is said to be serial if for each $a \in U$, there exists $b \in U$ such that $(a, b) \in x$) then M is known as serial partition. Suppose that the identity relation (denoted by e) on U is also a member of M and that the inverse of each $x \in M$ (denoted by x^{-1}) is also a member of M. Define $\circ_w$ (known as weak composition in the literature) on M as follows:

$$x \circ_w y = \{z \in M \mid z \cap (x \circ y) \neq \emptyset).$$

Here $\circ$ denotes the composition of relations. Using the fact that $x \circ y \in x \circ_w y$, it is easy to prove that $\mathbb{M} = \langle M, \circ_w, ^{-1}, e\rangle$ is a polyloop. It is worth mentioning that the weak composition on the members of a serial partition is not necessarily nonassociative and it is not necessarily associative either. For example the weak composition table of RCC10 is non-associative and hence gives an example of a polyloop which is not a polygroup. On the other hand the weak composition table of RCC-8 is associative and hence provides an example of a polyloop that is also a polygroup.

Example 7.

Chromatic Polyloops: Let $\mathbb{C}$ be a non-empty set of colours and e be an involution on $\mathbb{C}$. Let C_a be the set of edges (x, y) of a directed graph (V, E) that are coloured by 'a'; hence C_a is a binary relation on V. A colour scheme is a system $\mathbb{V} = \langle V, C_a \rangle_{a \in C}$ that satisfies the following conditions:

(1) $\{C_a \mid a \in \mathbb{C}\}$ partitions $\{(x, y) \in V \times V \mid x \neq y\}$;

(2) For each $a \in \mathbb{C}$ the set $C_{e(a)}$ is the converse relation $(C_a)^{-1}$;

(3) For each vertex x and the colour a, there exists a vertex y such that (x, y) is coloured a;

(4) For all $a, b, c \in \mathbb{C}$, there exists $c \in \mathbb{C}$ such that $C_c \cap (C_a \circ C_b) \neq \emptyset \Rightarrow C_c \subseteq (C_a \circ C_b)$.

The purpose of the involution e is to guarantee the colour assigned to edge (y, x) depends only on the colour of (x, y) (in the case of directed graphs) and therefore the colours a and $e(a)$ can be thought of as 'paired'. Clearly taking $a = e(a)$ these schemes can be used to colour undirected graphs.

Now let $\mathbb{V} = \langle V, C_a \rangle_{a \in \mathbb{C}}$ be a colour scheme with involution e on $\mathbb{C}$ and let I be a symbol that is not in $\mathbb{C}$. Let us define a system

$$\mathbb{A}_{\mathbb{V}} = \langle \mathbb{C} \cup \{I\}, *, ^{-1}, I \rangle$$

such that

$$a * b = \{c \in \mathbb{C} \mid C_c \cap C_a \circ C_b\} \cup \{I \mid b = a^{-1}\}$$

for $a, b \in \mathbb{C}$, $x * I = x = I * x$ for $x \in \mathbb{C} \cup \{I\}$, and for all $a \in \mathbb{C}, a^{-1} = e(a)$ while $I^{-1} = I$.

It is easy to verify that $\mathbb{A}_{\mathbb{V}}$ is a polyloop. We call a polyloop **chromatic** if it is isomorphic to a system $\mathbb{A}_{\mathbb{V}}$ derived from some colour scheme $\mathbb{V}$.

If we consider the regions in RCC-8 to be the vertices and the 8 relations to be the colours, then the ordered pair (x, y) can be thought of coloured DC (means $(x, y) \in C_{DC}$) if the regions x and y are not connected (topologically if $x \cap y = \emptyset$), so RCC-8 can be thought of as a chromatic polyloop.

Example 8.

Directed Graphs: Let (G, D) be a directed graph with the property that for any two vertices $a \neq b \in G$ either a is connected to b or b is connected to a. Define $*$ on G as:

$a * b = a$ if aDb but $\sim (bDa)$, $a * b = b$ if bDa but $\sim (aDb)$ and $a * b = \{a, b\}$ if aDb and bDa.

Consider $G^+ = G \cup \{e\}$ where $e \notin G$ and define $\circ$ on G^+ as $a \circ e = a = e \circ a$. $a \circ b = a * b$ if $a \neq b$, $a \circ b = \{g \in G \mid aDg\} \cup \{e\}$ if $a = b$.

If we define the inverse to be the identity map i on G^+, then the system $\mathbb{G} = \langle G^+, \circ, i, e\rangle$ is a commutative polyloop. This example is due to Jipsen, Kramer and Maddux [32].

Define a sequence of structures $\langle U_n, R_n\rangle$ where $U_n = \{a_{i,j} \mid i \in \mathbb{Z}, 1 \leq j \leq n\}$ and

$$R_n = \{\langle a_{i,j}, a_{k,l}\rangle \mid k<i \text{ or } (i = k \text{ and } j \geq l)\} \cup \{\langle a_{i,1}, a_{i+1,j}\rangle\} \cup \{\langle a_{i,j}, a_{i,j+1}\rangle\}$$

for $1 \leq j \leq n$. Then $\langle U_n, R_n\rangle$ gives us an infinite class of such polyloops.

Example 9.

Computer generated Polyloops: Constraint programming can also be used to generate polyloops. We list here a few, selecting one of each order ranging from 3 to 8; all elements in these polyloops are self-inversed.

$*$	1	2	3	4	5	6	7	8
$e = 1$	1	2	3	4	5	6	7	8
2	2	$\{1,5,7\}$	$\{4,7,8\}$	$\{1,2\}'$	$\{1,3\}'$	$\{1,2,3\}'$	$\{1\}'$	$\{1,2\}'$
3	3	$\{4,7,8\}$	$\{2,7,8\}'$	$\{2,3\}$	3	3	2	2
4	4	$\{1,2\}'$	$\{2,3\}$	$\{1,2\}$	2	2	2	2
5	5	$\{1,3\}'$	3	2	$\{1,2\}$	2	2	2
6	6	$\{1,2,3\}'$	3	2	2	$\{1,2\}$	2	2
7	7	$\{1\}'$	2	2	2	2	$\{1,2\}$	2
8	8	$\{1,2\}'$	2	2	2	2	2	$\{1,2\}$

$*$	1	2	3	4	5	6	7
$e = 1$	1	2	3	4	5	6	7
2	2	$\{1,4,6\}$	$\{6,7\}$	$\{1,3\}'$	$\{1,2,3\}'$	$\{1\}'$	$\{1,2\}'$
3	3	$\{6,7\}$	$\{1,4,5\}$	3	3	2	2
4	4	$\{1,3\}'$	3	$\{1,2\}$	2	2	2
5	5	$\{1,2,3\}'$	3	2	$\{1,2\}$	2	2
6	6	$\{1\}'$	2	2	2	$\{1,2\}$	2
7	7	$\{1,2\}'$	2	2	2	2	$\{1,2\}$

$*$	1	2	3	4	5	6
$e=1$	1	2	3	4	5	6
2	2	$\{1,5\}$	$\{5,6\}$	$\{4,5,6\}$	$\{1\}'$	$\{1,2\}'$
3	3	$\{5,6\}$	$\{1,4\}$	3	2	2
4	4	$\{4,5,6\}$	3	$\{1,2\}$	2	2
5	5	$\{1\}'$	2	2	$\{1,2\}$	2
6	6	$\{1,2\}'$	2	2	2	$\{1,2\}$

$*$	1	2	3	4	5
$e=1$	1	2	3	4	5
2	2	$\{1,4\}$	$\{1,2\}'$	$\{1\}'$	$\{1,2\}'$
3	3	$\{1,2\}'$	$\{4,5\}'$	2	2
4	4	$\{1\}'$	2	$\{1,2\}$	2
5	5	$\{1,2\}'$	2	2	$\{1,2\}$

$*$	1	2	3	4
$e=1$	1	2	3	4
2	2	$\{1,3\}$	$\{1\}'$	$\{1,2\}'$
3	3	$\{1\}'$	$\{1,2\}$	2
4	4	$\{1,2\}'$	2	$\{1,2\}$

$*$	1	2	3
$e=1$	1	2	3
2	2	$\{2\}'$	2
3	3	2	1

The last three-element polyloop has been given and studied by Maddux [42, Page 429]

Example 10.

Double Quotients of Polyloops: This is a way of getting more polyloops from given polyloops. The following notion is due to S. D. Comer [18].

Definition 3. *Let R be an equivalence relation on a polyloop $\mathbb{M} = \langle M, *, ^{-1}, e\rangle$. Then*

(1) R is a full conjugation on $\mathbb{M}$ if $(x,y) \in R$ implies $(x^{-1}, y^{-1}) \in R$ and $z \in x * y$ and zRz' implies there exist $x'Rx, y'Ry$ such that $z' \in x' * y'$.

(2) A full conjugation R is called a special conjugation if xRe implies $x = e$.

We can prove the following:

Proposition 1. *Let R be an equivalence relation on a polyloop $\mathbb{M} = \langle M, *, ^{-1}, e\rangle$. If R is a full conjugation on $\mathbb{M}$ then the system $\mathbb{R} = \langle \{[x]_R \mid x \in M\}, *, ^{-1}, [e]_R\rangle$, where $*$ and $^{-1}$ are the induced operations on R-classes, is a polyloop.*

Proof. Let R be a full conjugation on $\mathbb{M}$. We show that $\langle \{[x]_R \mid x \in M\}, *, ^{-1}, [e]_R\rangle$ is a polyloop. It is clear from the definition of full conjugation that $[x]_R^{-1} = [x^{-1}]_R \in \mathbb{R}$ for all $[x]_R \in \mathbb{R}$ and

$$[x]_R * [y]_R = \{[z]_R \mid z \in [x]_R * [y]_R\}.$$

(P_1) Since $x \in (x * y) * y^{-1}$, we have $[x]_R \in ([x]_R * [y]_R) * [y]_R^{-1}$. Similarly we can show that $[x]_R \in [y]_R^{-1} * ([y]_R * [x]_R)$.

(P_3) Since $e \in x * x^{-1}$, we have $[e]_R \in [x]_R * [x]_R^{-1}$ (also $[e]_R \in [x]_R^{-1} * [x]_R$).

(P_2) First we need to show that $[e]_R \in [x]_R * [y]_R$ if and only if $[y]_R = [x]_R^{-1}$. Suppose that $[e]_R \in [x]_R * [y]_R$ which means there exist $u \in [x]_R$ and $v \in [y]_R$ such that $e \in u * v$ and hence $v = u^{-1}$. This means by definition that $[y]_R = [x]_R^{-1}$. The converse follows from P_3. Now let $a \in [x]_R * [e]_R$. This means there exist $b \in [x]_R$ and $c \in [e]_R$ such that $a \in b * c$. This implies that $c \in b^{-1} * a$ and hence $[e]_R \in [x]_R^{-1} * [a]_R$ and therefore $a \in [x]_R$. This proves that $[x]_R * [e]_R = [x]_R$. Similarly we can show that $[e]_R * [x]_R = [x]_R$.

(P_4) Let $[x]_R \in [y]_R * [z]_R$. This implies there exist $a \in [y]_R$ and $b \in [z]_R$ such that $x \in a * b$ which means $a \in x * b^{-1}$ and $b \in a^{-1} * x$. Now by using the definition we conclude that $[y]_R \in [x]_R * [z]_R^{-1}$ and $[z]_R \in [y]_R^{-1} * [x]_R$. □

The systems in the above proposition are called double quotients of M. Obviously the collection of singleton subsets of M gives a trivial double quotient for M. Similarly the partition $\{\{e\}, \{e\}'\}$ also gives a double quotient. If we consider the smallest nonassociative IP loop $\mathbb{M}$ of order 7 then

$$\mathbb{R} = \{\{1\}, \{2, 3\}, \{4, 5\}, \{6, 7\}\}$$

provides the double quotient of $\mathbb{M}$.

It is easy to verify that all the polyloops from Example 9 have only double quotients that are either trivial or they are of the form $\{\{e\}, \{e\}'\}$.

The double quotients of a given finite loop can be generated on a computer by using constraint programming. For example the number of double quotients of RCC-8 turns out to be 25 including

$$\{\{1\}, \{2, 3, 4\}, \{5, 8\}, \{6, 7\}\}.$$

Similarly the number of double quotients of RCC-10 turns out to be 42 including

$$\{\{1\},\{2,4,5\},\{3\},\{6\},\{7,8,9,10\}\}.$$

It is worth mentioning that the polyloops generated by the computer in the above example have no non-trivial double quotients.

3.3 Connections with SA relation algebras

How a multigroupoid $(M,\cdot)$ can be viewed as a relational structure is given here:

Consider the ordered pair $\mathbb{M} = \langle M, R\rangle$ where R is a ternary relation on M defined by: $R(a,b,c)$ if and only if $a \in b\cdot c$. Although this agrees with the formal definition of complex algebras, in the context of multigroupoids it is customary to work instead with a relation T', defined by $R'(a,b,c)$ if and only if $c \in a\cdot b$ if and only if $R(c,a,b)$. This agrees with the traditional definition of **complex multiplication** of multigroupoids as $X \circ Y = \cup\{x\cdot y\colon x \in X, y \in Y\}$. If M has a unit element e, M can be viewed differently as the structure $\mathbb{M} = \langle M, R, \{e\}\rangle$. Similarly, if M has a unary operation $^{-1}$ then we may view M as $\mathbb{M} = (M, R, S, \{e\})$, where S is a binary relation on M such that xSy (and ySx) iff $x^{-1} = y$.

An example of such a complex algebra was seen in the case of M being a polygroup (see [18]). In that case Comer proved that the complex algebra of M is a complete atomic integral *relation algebra*. For the exact reference see Theorem 3.1 of [18].

An algebra A is said to be integral if for all $x, y \in A$, $x \circ y = 0$ implies $x = 0$ or $y = 0$. The following lemma gives an alternate condition for integral SA.

Lemma 2. *Let A be an SA. Then A is integral if and only if e is an atom of A.*

Remark 2. *Here too we proved this lemma without the knowledge of its existence previously but later on we found that this has been proved by Maddux on page 366 [42, Theorem 353] and was published in 1990 [40]. The version for relation algebras is Theorem 4.17 proved by B. Jónsson and A. tarski [34].*

Proof. Suppose that e is an atom of A and that there are $x \neq 0$ and $y \neq 0$ but $x \circ y = 0$. This means $(x \circ y) \wedge 1 = 0$, or $(x^{\smile} \circ 1) \wedge y = 0$ and hence $x^{\smile} \circ 1 \leq y^{-}$. Now $(x \circ e) \wedge x \neq 0$ and hence $(x^{\smile} \circ x) \wedge e \neq 0$. But since e is an atom, we have

$x^\smile \circ x \geq e$. Again $y = e \circ y \leq (x^\smile \circ x) \circ y \leq (x^\smile \circ 1) \circ 1 = x^\smile \circ 1$ or $y \leq x^\smile \circ 1$. Consequently we have

$$y \leq x^\smile \circ 1 \leq y^-$$

a contradiction since $y \neq 0$. Hence A is integral.

Conversely suppose that A is integral but e is not an atom. This means there exist $0 \neq x$ and $0 \neq y$ such that $x \vee y = e$ and $x \wedge y = 0$. Since $y \leq e$, $x \circ y \leq x \circ e = x$ and similarly $x \circ y \leq y$ which implies $x \circ y \leq x \cap y = 0$, a contradiction. Hence e is an atom. □

The complex algebra of a polygroup $\mathbb{M} = \langle M, *, ^{-1}, e\rangle$ is the system $\mathbf{Cm} = \langle \mathcal{P}(M), \cap, \cup, -, \emptyset, M, *, ^{-1}, \{e\}\rangle$ where $\langle \mathcal{P}(M), \cap, \cup, -, \emptyset, M\rangle$ is the Boolean algebra of all subsets of M and $*$ and $^{-1}$ denote the extensions of the polyloop operations to subsets.

The complex algebra construction gives a one-one correspondence (up to isomorphism) between polyloops and complete atomic integral SA's.

Theorem 3. *(1)* $\mathbf{Cm}(\mathbb{M})$ *is a complete atomic integral SA for every polyloop* $\mathbb{M}$.

(2) For every atomic integral SA $\mathbb{A}$ *the system*

$$At(\mathbb{A}) = \langle At_{\mathbb{A}}, *, ^{-1}, e\rangle,$$

where $At_{\mathbb{A}}$ *is the set of atoms of* $\mathbb{A}$*, is a polyloop.*

(3) If $\mathbb{M}$ *is a polyloop and* $\mathbb{A}$ *is a complete atomic integral SA, then*

$$\mathbb{M} \cong At(\mathbf{Cm}(\mathbb{M}))$$

and

$$\mathbb{A} \cong \mathbf{Cm}(At(\mathbb{A})).$$

Remark 3. *Though we did this theorem independently but later on we found that Theorem 3(1) is a special case of [32, Theorem 2.2], Theorem 3(2) follows from [32, Theorem 2.2] and the first equation in Theorem 3(3) is a special case of [32, Theorem 3.3] while the second equation in Theorem 3(3) is a special case of [32, Theorem 3.13(20)].*

Proof. (1) Let $(M, *, ^{-1}, e)$ be a polyloop. We show that $\langle \mathcal{P}(M), \cap, \cup, -, \emptyset, M, \circ, ^\smile, \{e\}\rangle$ is a semiassocitive algebra where $\circ$ is defined as

$$X \circ Y = \bigcup \{x * y \mid x \in X, y \in Y\}$$

and

$$X^{\smile} = \{x^{-1} \mid x \in X\}.$$

Since $\langle \mathcal{P}(M), \cap, \cup, ^c, \emptyset, M\rangle$ is Boolean algebra, we only need to prove the following:

(i) For all $X, Y, Z \in \mathcal{P}(M)$, we have

$$X \cap (Y \circ Z) = \emptyset \text{ iff } Y \cap (X \circ Z^{\smile}) = \emptyset \text{ iff } Z \cap (Y^{\smile} \circ X) = \emptyset.$$

(ii) For all $X \in \mathcal{P}(M)$, we have

$$(X \circ M) \circ M = X \circ M.$$

(i) Let $X \cap (Y \circ Z) \neq \emptyset$ so there exists $x \in X$ such that $x \in Y \circ Z$. This means there exist $y \in Y$ and $z \in Z$ such that $x \in y * z$. Since U is a polyloop, we have $y \in x * z^{-1}$ and $z \in y^{-1} * x$. This implies that $Y \cap (X \circ Z^{\smile}) \neq \emptyset$ and $Z \cap (Y^{\smile} \circ X) \neq \emptyset$.

(ii) Clearly

$$X \circ M = (X \circ M) \circ \{e\} \subseteq (X \circ M) \circ M.$$

We only have to show that

$$(X \circ M) \circ M \subseteq X \circ M.$$

For each $t \in (X \circ M) \circ M$ and $x \in X$, we have $t \in x * (x^{-1} * t) \in X \circ M$ which proves what we required.

Also for non-empty sets X and Y, we have $X \circ Y$ non-empty; proving $\mathcal{P}(M)$ to be integral.

(2) Suppose that $\mathbb{A} = \langle A, \wedge, \vee, \sim, 0, 1, \circ, ^{\smile}, e\rangle$ is a complete atomic integral semiassociative relation algebra. We show that $\langle At_{\mathbb{A}}, \circ, ^{\smile}, e\rangle$ is a polyloop. This means we only have to show that for all x and $y \in At_{\mathbb{A}}$

(P_1) $x \in (x \circ y) \circ y^{\smile}$ and $x \in y^{\smile} \circ (y \circ x)$.

(P_2) $e \in At_{\mathbb{A}}$.

(P_3) $x^{\smile} \in At_{\mathbb{A}}$.

(P_1) Let us suppose that $x \notin (x \circ y) \circ y^{\smile}$. This means $x \wedge [(x \circ y) \circ y^{\smile}] = 0$ which implies (by $RA3$) that $(x \circ y) \wedge (x \circ y) = 0$, a contradiction.

(P_2) Since $\mathbb{A}$ is integral, e is an atom of $\mathbb{A}$ (by lemma above) and hence lies in $At_{\mathbb{A}}$.

(P_3) Suppose not. Then $x^{\smile}$ is strictly above some $y \in At_{\mathbb{A}}$ which implies that $y^{\smile}$ lies strictly below x, a contradiction.

This completes the proof of (2).

(3) A map from a to $\{a\}$ gives the first isomorphism and the mapping from $x \in \mathbb{A}$ to $\{a \in At_{\mathbb{A}} \mid a \leq x\}$ gives the second. □

It is not hard to realise that a double quotient of a given polyloop $\mathbb{M}$ is a subalgebra of $\mathbf{Cm}(\mathbb{M})$. This means that the complex algebras of the loops given in Example 9 are all "minimal" semiassociative relation algebras.

3.4 A Link Between Polygroups and Polyloops

In this section we record a sufficient condition on polyloops (given in Example 2 and 3) that make them polygroups. We call a partition M of a set U **dense** if for x, y, z and $t \in M$, $(x \circ y) \cap (z \circ t) = \emptyset$ implies for all $s \in M$ either $(x \circ y) \cap s = \emptyset$ or $(z \circ t) \cap s = \emptyset$.

Proposition 2. *If M is a dense serial partition (as defined in Example 2) of a set $U \times U$ then $\mathbb{M} = \langle M, \circ_w, ^{-1}, e\rangle$ is a polygroup.*

Proof. Associativity is the only thing to be verified. This amounts to proving the following:

For all $a, b, c, d, f \in M$ if $c \leq a \circ_w b$ and $f \leq c \circ_w d$ then there exists $g \in M$ such that $g \leq b \circ_w d$ and $f \leq a \circ_w g$. By (P_4), we have $f \leq c \circ_w d$ iff $c \leq f \circ_w d^{-1}$ and $f \leq a \circ_w g$ iff $g \leq a^{-1} \circ_w f$.

Therefore suppose that $c \leq a \circ_w b$ and $c \leq f \circ_w d^{-1}$. By definition of $\circ_w$, we have $(a \circ b) \cap c \neq \emptyset$ and $(f \circ d^{-1}) \cap c \neq \emptyset$. Now by the density of M, we get $(a \circ b) \cap (f \circ d^{-1}) \neq \emptyset$ and therefore $b \cap ((a^{-1} \circ f) \circ d^{-1}) \neq \emptyset$. Thus $(a^{-1} \circ f) \cap (b \circ d) \neq \emptyset$. This means there exits $g \in M$ such that $(a^{-1} \circ f) \cap g \neq \emptyset$ and $(b \circ d) \cap g \neq \emptyset$.

Thus $g \leq a^{-1} \circ_w f$ and $g \leq b \circ_w d$ and by (P_4), we get $f \leq a \circ_w g$.

□

Example: Let $M = \{e, R, S, T\}$ be a serial partition of $U \times U$ where $U = \{0, 1, 2, 3\}$ and R, S, T are defined by:

- $R = \{(0, 4), (4, 0), (1, 3), (3, 1), (1, 2), (2, 1)\}$,
- $S = \{(0, 1), (1, 0), (2, 3), (3, 2), (3, 4), (4, 3)\}$,

- $T = \{(0,3),(3,0),(4,1),(1,4),(2,4),(4,2)\}$.

Then the weak composition table of the elements of M is given by:

$\circ_w$	e	R	S	T
e	e	R	S	T
R	R	$\{e,S\}$	$\{T,R\}$	$\{S,T\}$
S	S	$\{T,R\}$	$\{e,T\}$	$\{R,S\}$
T	T	$\{S,T\}$	$\{R,S\}$	$\{e,R\}$

Table 3.3: Weak Composition Table for M

Table 3.3 shows that weak composition is different from composition. It is easy to check that the weak composition in this case is associative, and also that composition and weak composition of the elements of M satisfy the necessary conditions of Proposition 2 and hence Table 3.3 provides a polygroup.

Remark 4. *Table 3.3 already appears on page 443 in [42] where it is the relation algebra called* 39_{65}. *Table 3.3 not only provides a polygroup, but a group representable relation algebra (a GRA). In fact, this polygroup is embeddable in the complex algebra of the cyclic group of order 7.*

Chapter 4

Complex algebras of loops

4.1 Introduction

In this chapter we aim to investigate the class of groupoids whose complex algebras are semiassociative relation algebras and vice versa. Due to weak associativity of the multiplication of semiassociative algebras we always thought that such groupoids must carry some loop like structure. This investigation proved to be analogous to the one carried out by Jónsson and Tarski (see [33], [34]) for relation algebras.

In Section 2 we prove important lemmas which are crucial for our main result that provides a strong connection between IP loops and semiassociative algebras. In Section 3 we present our partial findings which were obtained during our search for Lyndon algebras that appear as subalgebras of complex algebras of selected IP loops. This generates much interest for future investigations in this area.

4.2 Complex Algebras of IP Loops

An IP loop $(G, *)$ together with the unique inverse function $^{-1}$ and identity element e can be easily seen as a relational structure $\mathbb{G} = (G, T, R, \{e\})$, where T is a ternary relation on G defined by: $(x, y, z) \in T$ if and only if $x = y * z$ which in turn defines a binary function on $\mathcal{P}(G)$ by:

$$f(X, Y) = \{a \in G \mid \exists x \in X, y \in Y \mid (x, y, a) \in T\},$$

and R is a binary relation on G defined by $(x, y) \in R$ iff $x^{-1} = y$ which defines an involution on $\mathcal{P}(G)$ by:

$$X^{-1} = \{a \in G \mid \exists b \in G \mid (a, b) \in R\}.$$

One natural example of such a complex algebra is seen when G is a group. Then, $\mathbf{Cm}(G)$ turns out to be a *relation algebra*. We will prove an analogue of this for semiassociative relation algebras, establishing a link between these and a certain quite well-known subvariety of loops. We begin with the following lemma:

Lemma 3. *If* $\mathbb{U} = (U, \cdot, ^{-1}, e)$ *is an IP loop, then* $\mathbf{Cm}(\mathbb{U})$ *is a SA.*

Proof. That $\{e\}$ is an identity element in $\mathbf{Cm}(\mathbb{U})$ is obvious. We then only need to show that complex multiplication $X \circ Y = \{xy \mid x \in X, y \in Y\}$ and converse $X^{\smile} = \{x^{-1} \mid x \in X\}$ satisfy the following for all $X, Y, Z \in \mathcal{P}(U)$.

$$X \cap (Y \circ Z) = \emptyset \quad \text{iff} \quad Y \cap (X \circ Z^{\smile}) = \emptyset \quad \text{iff} \quad Z \cap (Y^{\smile} \circ X) = \emptyset \qquad (a)$$

$$(X \circ U) \circ U = X \circ U \qquad (b)$$

For (a), let $X \cap (Y \circ Z) \neq \emptyset$, so there exists $x \in X$ with $x \in Y \circ Z$. Thus, there are $y \in Y$ and $z \in Z$ such that $x = yz$. By inverse properties, we have $y = xz^{-1}$ and $z = y^{-1}x$. This implies that $Y \cap (X \circ Z^{\smile}) \neq \emptyset$ and $Z \cap (Y^{\smile} \circ X) \neq \emptyset$. By symmetry of the situation this establishes (a). Notice that the coincidence of left and right inverses is essential.

For (b), firstly, it is clear that $X \circ U = (X \circ U) \circ \{e\} \subseteq (X \circ U) \circ U$. We only have to show that $(X \circ U) \circ U \subseteq X \circ U$. By the unique solution property, for $x \in X$ and $y, z \in U$ there exists $a \in U$ such that $(xy)z = xa$. Thus, $(xy)z \in X \circ U$ as required. Notice that $a = x^{-1}((xy)z)$, which in general is not equal to yz. □

The next lemma links the non-associative algebras (a much weaker class than that of semiassocitive algebras) with IP loops.

Lemma 4. *If* $\mathbf{Cm}(\mathbb{U})$ *is the complex algebra of a groupoid* $\mathbb{U} = (U, \cdot)$ *and* $\mathbf{Cm}(\mathbb{U})$ *is a NA, then there is an* $e \in U$ *and a unary operation* $^{-1}$ *on* U *such that* $(U, \cdot, ^{-1}, e)$ *is an IP loop.*

Proof. Let $E \subseteq U$ be the identity element of $\mathbf{Cm}(\mathbb{U})$. First, we show that E is a singleton. Suppose $x_1, x_2 \in E$. Since for all $u \in U$, we must have $\{u\} \circ E = \{u\} = E \circ \{u\}$, we get that

$$ux_1 = u = x_1u \quad \text{and} \quad ux_2 = u = x_2u$$

Replacing u by x_1 in the second equation and by x_2 in the first we get $x_1 = x_2$, so E is a singleton. Putting $E = \{e\}$ we obtain $eu = u = ue$ for all $u \in U$.

Secondly, we show that for all $x \in U$ there exists a unique $y \in Y$ such that $xy = e = yx$. To do this, observe that $\{x\}^{\smile}$ is singleton for all $x \in U$. The proof

of that is folklore in relation algebras and carries over without change, but since it nicely demonstrates some arithmetic of complex algebras (and BAOs in general), we repeat it here. Suppose $\{x\}^\smile$ contains y_1 and y_2. Then $\{x\}^\smile \supseteq \{y_1, y_2\} = \{y_1\} \cup \{y_2\}$ and therefore $\{x\}^{\smile\smile} = \{x\} \supseteq \{y_1, y_2\}^\smile = \{y_1\}^\smile \cup \{y_2\}^\smile$. Now, as $\emptyset^\smile = \emptyset$, none of $\{y_1\}^\smile$, $\{y_2\}^\smile$ can be empty, so we must have $\{x\} = \{y_1\}^\smile = \{y_2\}^\smile$. Thus, $\{x\}^\smile = \{y_1\} = \{y_2\}$, as needed. Hence, we obtain that for all singletons $\{x\}$, there is another singleton $\{x\}^\smile$ such that

$$\{x\} \circ \{x\}^\smile = E = \{x\}^\smile \circ \{x\}.$$

This immediately shows that for all $x \in U$ there exists a unique inverse y, namely the unique element of $\{x\}^\smile$. Thus, we can define a unary inverse function $^{-1}$ on U.

Finally, we show that for all $x, y \in U$ we have $x = (xy)y^{-1} = y^{-1}(yx)$. Suppose that $x \neq (xy)y^{-1}$. This means $\{x\} \cap (\{xy\} \circ \{y\}^\smile) = \emptyset$ which implies that $\{xy\} \cap (\{x\} \circ \{y\}) = \emptyset$, a contradiction. Hence $x = (xy)y^{-1}$, and the other equality is similar. This completes the proof. □

Combining the two lemmas we have:

Theorem 4. *The complex algebra of a groupoid $(L, \cdot)$ is a semiassociative relation algebra if and only if $(L, \cdot)$ is an IP loop.*

By analogy with *group relation algebras* (GRAs) we may define *loop semiassociative relation algebras* (LSAs) to be the class of (isomorphic copies of) subalgebras of products of complex algebras of IP loops.

4.3 Lyndon Algebras and IP Loops

For $n \geq 2$, the **Lyndon algebra** $\mathcal{A}_n$ is a finite relation algebra with $n + 2$ self-inversed atoms $e, a_0, \ldots, a_n$ that satisfy the following condition;

- $a_i \circ a_i = e \vee a_i$ if $n \geq 3$.
- $a_i \circ a_j = \bigvee_{k \neq i,j} a_k$ if $i \neq j$,

where $i, j, k \leq n$. Case $n = 2$ is special so we treat it separately. Notice that for $n = 2$ the definition we gave above still works, but it does not produce a relation algebra because multiplication ceases to be associative. This led many authors to alter the definition of multiplication for $n = 2$ into $a_i \circ a_i = e$ and

$a_i \circ a_j = \bigvee_{k \neq i,j} a_k$ if $i \neq j$. We do not do that here. Our reason is that the algebra $\mathcal{A}_2$ (under our definition) turns out to be a subalgebra of the complex algebra of the smallest nonassociative IP loop.

The algebra $\mathcal{A}_2$ coincides with the semiassociative relation algebra called $\mathcal{C}_4(\{1,3\})$ in Theorem 2.5(4)(a) of [32], which states that $\mathcal{A}_2$ is an SA, but not an RA.

Lyndon [36] proved that $A(G)$, the algebra of a given **geometry** G, together with an identity element that is not a point in G is a Lyndon algebra. Monk [47] used these Lyndon algebras to prove that the representable relation algebras (RRA's) are not finitely axiomatizable. Clearly if the above equivalence holds for LSA's, it would give an easy proof of nonfinite axiomatizability of LSA's. Although this could not be achieved, we managed to prove that there are members of LSAs that are clearly Lyndon algebras whose multiplication table coincides with the one suggested above in the definition of Lyndon Algebra.

It was not difficult to find such algebras having up to 7 atoms but despite considerable efforts we could not find one with 8 atoms. As this is the first nonrepresentable Lyndon algebra it may suggest that the equivalence does indeed hold.

We give here the details of Lyndon algebras among LSAs having exactly 6 and 7 atoms; they are the subalgebras of the complex algebras of IP loops of order 16 and 25 respectively. The atoms of these Lyndon algebras are

$$\{\{1\},\{2,3,4\},\{5,6,7\},\{8,9,10\},\{11,12,13\},\{14,15,16\}\}$$

and

$$\{\{1\},\{2,3,4,5\},\{6,7,8,9\},\{10,11,12,13\},\{14,15,16,17\},\{18,19,20,21\},\{22,23,24,25\}\}$$

respectively. To verify that these atoms form Lyndon algebras, we have included the composition tables of two non-isomorphic IP loops each of order 16 and 25; for the reader's interest we mention that one of each order was obtained manually and one using the first-order theorem prover PROVER9 and its associated propositional satisfiability solver Mace4 [43].

$*$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	3	4	1	8	11	14	13	15	7	16	9	5	10	12	6
3	3	4	1	2	15	9	12	16	6	11	10	7	14	13	5	8
4	4	1	2	3	13	16	10	5	12	14	6	15	8	7	9	11
5	5	8	12	16	6	7	1	15	11	4	2	14	10	9	3	13
6	6	14	9	13	7	1	5	12	3	16	15	8	4	2	11	10
7	7	11	15	10	1	5	6	2	14	13	9	3	16	12	8	4
8	8	16	13	5	11	14	2	9	10	1	4	6	15	3	7	12
9	9	12	6	15	16	3	13	10	1	8	14	2	7	11	4	5
10	10	7	14	11	4	12	15	1	8	9	5	16	3	6	13	2
11	11	10	16	7	14	2	8	3	5	15	12	13	1	4	6	9
12	12	15	5	9	3	10	16	14	4	6	13	1	11	8	2	7
13	13	6	8	14	9	15	4	7	16	2	1	11	12	5	10	3
14	14	13	10	6	2	8	11	4	7	12	3	5	9	15	16	1
15	15	9	7	12	10	13	3	11	2	5	8	4	6	16	1	14
16	16	5	11	8	12	4	9	6	13	3	7	10	2	1	14	15

x	x^{-1}
1	1
2	4
3	3
4	2
5	7
6	6
7	5
8	10
9	9
10	8
11	13
12	12
13	11
14	16
15	15
16	14

$*$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	3	4	1	8	11	14	15	12	7	10	16	5	9	13	6
3	3	4	1	2	15	9	12	13	6	16	14	7	8	11	5	10
4	4	1	2	3	13	16	10	5	14	11	6	9	15	7	8	12
5	5	8	12	16	6	7	1	11	15	4	2	14	9	10	3	13
6	6	14	9	13	7	1	5	16	3	12	15	10	4	2	11	8
7	7	11	15	10	1	5	6	2	13	14	8	3	16	12	9	4
8	8	13	14	5	16	12	2	9	10	1	3	15	7	6	4	11
9	9	16	6	12	11	3	15	10	1	8	5	4	14	13	7	2
10	10	7	11	15	4	14	13	1	8	9	16	6	2	3	12	5
11	11	15	10	14	2	9	4	16	5	15	12	13	1	8	6	3
12	12	9	5	14	3	8	16	6	2	15	13	1	11	4	10	7
13	13	6	16	8	10	15	4	14	7	3	1	11	12	5	2	9
14	14	12	8	6	2	10	11	7	4	13	9	5	3	15	16	1
15	15	10	7	11	9	13	3	12	5	2	4	8	6	16	1	14
16	16	5	13	9	12	4	8	3	11	6	7	2	10	1	14	15

x	x^{-1}
1	1
2	4
3	3
4	2
5	7
6	6
7	5
8	10
9	9
10	8
11	13
12	12
13	11
14	16
15	15
16	14

$*$	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
$e=1$	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
2	2	3	4	5	1	10	14	18	22	20	17	23	9	12	24	19	8	25	13	15	7	21	16	11	6
3	3	4	5	1	2	15	11	23	19	16	21	8	22	25	13	9	18	12	24	6	14	17	20	7	10
4	4	5	1	2	3	20	24	12	16	25	7	18	15	21	6	10	22	17	9	23	11	13	8	19	14
5	5	1	2	3	4	25	21	17	13	6	24	14	19	7	20	23	11	8	16	10	22	9	12	15	18
6	6	10	15	20	25	7	8	9	1	24	18	16	5	23	11	4	19	22	3	14	12	2	13	17	21
7	7	14	11	24	21	8	9	1	6	19	25	4	17	10	22	18	5	2	23	13	15	12	3	20	16
8	8	18	23	12	17	9	1	6	7	14	3	22	20	2	21	25	13	16	10	24	5	15	19	4	11
9	9	22	19	16	13	1	6	7	8	2	15	21	23	20	3	12	24	11	17	4	25	18	14	10	5
10	10	20	16	25	6	24	19	14	2	11	12	13	1	22	4	21	7	15	5	8	23	3	9	18	17
11	11	17	21	7	24	18	25	3	15	12	13	1	10	5	23	6	20	4	14	22	9	8	2	16	19
12	12	23	8	18	14	16	4	22	21	13	1	10	11	19	9	24	2	6	25	17	3	20	15	5	7
13	13	9	22	15	19	5	17	20	23	1	10	11	12	8	18	3	25	24	7	2	16	14	21	6	4
14	14	12	25	21	7	23	10	2	20	22	5	19	8	15	16	17	1	3	6	11	24	4	18	9	13
15	15	24	13	6	20	11	22	21	3	4	23	9	18	16	17	1	14	7	2	25	10	19	5	12	8
16	16	19	9	10	23	4	18	25	12	21	6	24	3	17	1	14	15	13	22	5	8	7	11	2	20
17	17	8	18	22	11	19	5	13	24	7	20	2	25	1	14	15	16	23	12	9	4	10	6	21	3
18	18	25	12	17	8	22	2	16	11	15	4	6	24	3	7	13	23	19	20	21	1	5	10	14	9
19	19	13	24	9	16	3	23	10	17	5	14	25	7	6	2	22	12	20	21	1	18	11	4	8	15
20	20	15	6	23	10	14	13	24	4	8	22	17	2	11	25	5	9	21	1	18	19	16	7	3	12
21	21	7	14	11	22	12	15	5	25	23	9	3	16	24	10	8	4	1	18	19	20	6	17	13	2
22	22	21	17	13	9	2	12	15	18	3	8	20	14	4	19	7	10	5	11	16	6	23	24	25	1
23	23	16	20	8	12	13	3	19	14	9	2	15	21	18	5	11	6	10	4	7	17	24	25	1	22
24	24	11	7	19	15	17	20	4	10	18	16	5	6	9	12	2	21	14	8	3	13	25	1	22	23
25	25	6	10	14	18	21	16	11	5	17	19	7	4	13	8	20	3	9	15	12	2	1	22	23	24

x	x^{-1}
1	1
2	5
3	4
4	3
5	2
6	9
7	8
8	7
9	6
10	13
11	12
12	11
13	10
14	17
15	16
16	15
17	14
18	21
19	20
20	19
21	18
22	25
23	24
24	23
25	22

$*$	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
$e=1$	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
2	2	3	4	5	1	10	14	18	22	17	21	25	9	11	19	24	6	12	23	16	7	13	15	20	8
3	3	4	5	1	2	23	11	15	19	20	24	8	16	18	12	9	25	22	13	6	17	14	10	7	21
4	4	5	1	2	3	20	24	12	16	23	7	15	19	22	8	13	21	14	9	10	25	18	6	11	17
5	5	1	2	3	4	17	21	25	13	6	14	18	22	7	23	20	10	8	15	24	11	9	19	16	12
6	6	10	15	20	25	7	8	9	1	24	19	16	5	2	18	22	13	23	3	12	14	21	17	4	11
7	7	22	11	16	21	8	9	1	6	18	15	4	23	10	25	19	5	2	24	17	13	12	3	14	20
8	8	18	23	12	17	9	1	6	7	14	3	22	21	24	11	4	20	10	16	25	5	2	13	19	15
9	9	14	19	24	13	1	6	7	8	2	25	20	17	21	3	12	23	15	11	4	22	16	18	10	5
10	10	25	20	15	6	14	18	24	2	11	12	13	1	5	22	21	7	17	4	23	8	19	9	3	16
11	11	21	16	7	22	19	25	3	15	12	13	1	10	23	20	8	2	5	14	9	24	6	4	17	18
12	12	17	8	23	18	22	4	16	20	13	1	10	11	19	9	3	24	25	6	15	2	5	14	21	7
13	13	9	24	19	14	5	17	21	23	1	10	11	12	6	4	25	18	7	22	3	16	15	20	8	2
14	14	13	18	22	9	24	19	2	10	21	23	5	8	15	16	17	1	6	25	11	4	20	7	12	3
15	15	19	10	6	23	11	3	20	25	22	4	7	18	16	17	1	14	24	12	5	9	8	21	2	13
16	16	24	7	11	20	4	12	22	21	3	6	19	25	17	1	14	15	13	2	8	23	10	5	18	9
17	17	8	25	21	12	18	23	13	5	9	20	24	2	1	14	15	16	3	7	22	10	4	11	6	19
18	18	12	22	14	8	25	2	10	17	15	5	23	7	13	24	6	3	19	20	21	1	11	16	9	4
19	19	23	13	9	15	3	22	14	11	4	16	6	24	25	7	2	12	20	21	1	18	17	8	5	10
20	20	16	6	10	24	12	15	23	4	25	9	17	3	8	5	11	22	21	1	18	19	7	2	13	14
21	21	7	17	25	11	16	13	5	24	8	22	2	14	4	10	23	9	1	18	19	20	3	12	15	6
22	22	11	14	18	7	2	16	19	12	5	8	21	15	20	6	10	4	9	17	13	3	23	24	25	1
23	23	15	12	8	19	13	20	17	3	7	18	14	4	9	21	5	11	16	10	2	6	24	25	1	22
24	24	20	9	13	16	21	10	4	14	19	17	3	6	12	2	18	8	11	5	7	15	25	1	22	23
25	25	6	21	17	10	15	5	11	18	16	2	9	20	3	13	7	19	4	8	14	12	1	22	23	24

x	x^{-1}
1	1
2	5
3	4
4	3
5	2
6	9
7	8
8	7
9	6
10	13
11	12
12	11
13	10
14	17
15	16
16	15
17	14
18	21
19	20
20	19
21	18
22	25
23	24
24	23
25	22

Chapter 5

Counting Loops with the Inverse Property

5.1 Introduction

A loop $(L, *)$ is said to have the inverse property if each $x \in L$ has a two-sided inverse x^{-1} such that for all $y \in L$ we have

$$x^{-1} * (x * y) = y = (y * x) * x^{-1}.$$

These loops are known as IP loops (for an account of their properties see Bruck's survey [11]). Clearly every group is an IP loop, but the converse is not the case. The smallest IP loop that is not a group is of order 7. Steiner loops are also IP loops, satisfying the extra condition $x^{-1} = x$. IP loops form a very important class, not only in that they represent a strong generalisation of both groups and Steiner loops, but also in that the Moufang nucleus (the set of $a \in L$ such that $a[(xy)a] = (ax)(ya)$ for all $x, y \in L$) of such loops behaves as a nilpotency function for this class. Moreover IP loops are exactly those groupoids whose complex algebras are semiassociative relation algebras [39].

The present chapter reports the numbers of non-isomorphic IP loops having order up to 13. Since these were obtained by exhaustive enumeration, they are available for inspection. We have also included the classification of IP loops into several important subclasses.

In Section 2 we give a detailed account on the history of counting Latin squares, quasigroups and loops which tells us how old and how sorry this history has been. In Section 3 we give the number of isotopy classes, main classes and the isomorphism classes of quasigroups and loops (up to order 10); Sections 2 and

3 are reported from McKay *et al* [44]. In Section 4 we explain how we counted the number of isomorphism classes of IP loops of order up to 13 and then classify them into interesting subclasses.

5.2 History of Counting Latin Squares, Quasigroups and Loops

The history of counting Latin squares goes back to at least 1782 because the number of reduced squares of order 5 was known to Euler [24] and Cayley [15]. MacMahon [37] used a different method to find reduced squares of order 5, but obtained the wrong number. In 1890, Frolov [26] found the number of reduced squares of order 6 which was also done by Tarry [65]. About 30 years later Jacob [29] tried the same class (order 6) but failed to produce the right value. Frolov also tried to find the reduced squares of order 7 but could not give the correct number. In 1930, Schönhardt [62] found the correct numbers of main classes, isotopy classes and reduced squares up to order 6. Fisher and Yates [25] seemed to be unaware of the results by [62] but refers to the work of Tarry and confirmed his values. In 1939, Norton [50]) suggested that there are 146 main classes and 562 isotopy classes of latin squares of order 7 but also acknowledged that his method might be incomplete. It was proven in 1948 by Sade [58] and in 1951 by Saxena [61] that the reduced squares of order 7 were more than Norton found in 1939. In 1951, Sade [59] traced the actual error by Norton; he found the one main class that was missing in the findings of Norton. This raised correctly the number of main classes of squares of order 7 to 147 and the isotopy classes to 564; this was noted by Preece [54] in 1966. However, in 1968, Brown [9] published the incorrect value 563 and the error remains un-noticed as it is still being quoted ([17] and [21]).

Brown was also mistaken in counting the number of isotopy classes of order 8 and it was noticed that Arlazarov *et al.* [3] gave the incorrect number of the main classes of squares of order 8. However, the correct number of reduced squares of order 8 was already published by Wells [68] in 1967, and the number of isotopy and main classes was correctly found by Kolesova, Lan and Thiel in 1990 [35].

The number of reduced squares of order 9 was calculated by Bammel and Rothstein [6], order 10 by McKay and Rogoyski [45] and for order 11 by McKay and Wanless [46]. McKay claims that *In each case the same numbers have been computed independently at least twice, so they are likely to be correct. In view of*

the sorry history of the subject, we attempted to do as much of our computation in duplicate as possible. The number of isotopy or main classes of latin squares of order greater than 8 was published for the first time by McKay *et al* [44]; they gave these numbers for squares of order up to 10.

Although the correct number of non-isomorphic loops of order up to 6 was first published by Schönhardt [62] in 1930, it seems that this publication was not seen by Albert [1] or Sade [60] who published weaker results so late. In 1974, Dénes and Keedwell [21] also gave the count of loops of order up to 6, thinking that they counted the number of "quasigroups". The loops of order 7 were counted in 1985 by Brant and Mullen [8]. In 2001, "QSCGZ" [55] published the number of loops of order 8 in an electronic forum and the same value was found independently by Guérin ([28]). The number of quasigroups and loops of order up to 10 was published in 2007 by McKay *et al* [44].

The entire section on the history of counting Latin squares, quasigroups and loops is taken from [44].

5.3 Small Latin Squares, Quasigroups and Loops

The total number R_n of reduced Latin squares of order n are given in the following table while the total number of squares (reduced or not) is $L_n = n!(n-1)!R_n$.

n	reduced squares
1	1
2	1
3	1
4	4
5	56
6	9408
7	16942080
8	535281401856
9	377597570964258816
10	7580721483160132811489280
11	5363937773277371298119673540771840

Table 5.1: Reduced Latin squares of order n

The number of main classes, types and isotopy classes of Latin squares of order up to 10 are given in the table 5.2.

n	main classes	types	isotopy classes
1	1	1	1
2	1	1	1
3	1	1	1
4	2	2	2
5	2	2	2
6	12	17	22
7	147	324	564
8	283657	842227	1676267
9	19270853541	57810418543	115618721533
10	34817397894749939	104452188344901572	208904371354363006

Table 5.2: Isotopy classes, types and main classes of Latin squares of order n

The number of isomorphism classes of quasigroups and loops of order up to 10 are given in the table 5.3.

n	quasigroups	loops
1	1	1
2	1	1
3	5	1
4	35	2
5	1411	6
6	1130531	109
7	12198455835	23746
8	2697818331680661	106228849
9	15224734061438247321497	9365022303540
10	2750892211809150446995735533513	20890436195945769617

Table 5.3: Isomorphism classes of quasigroups of order n

5.4 IP loops of Small Order

As noted, the smallest IP loop which is not a group is of order 7. Here it is:

Example 11.

$*$	1	2	3	4	5	6	7
$e=1$	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

x	x^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6

Associativity fails in that $(2*2)*4 = 3*4 = 7$ while $2*(2*4) = 2*6 = 5$. This structure has proper subalgebras $\{1,2,3\}$, $\{1,4,5\}$ and $\{1,6,7\}$. Note that the order of these subloops does not divide the order of the loop, marking a significant difference between IP loops and groups. This structure also shows that IP loops of prime order are not abelian, in general; unlike groups.

Note also that the only element which is its own inverse is the identity e. This is a general feature of IP loops of odd order, as may be shown by a simple counting argument:

Observation 1. *IP loops of odd order have no subloops of even order.*

Proof. Let $(L,*)$ be an IP loop and let $(S,\underline{*})$ be a subloop of $(L,*)$ of even order. Clearly, S consists of e and some subset of elements of L along with their inverses. For this subset to be of even cardinality, some element in it other than e must be self-inverse and thus of order 2. Let $a \in L$ be such an element which means $L(a)$ is a permutation of order 2. Moreover, $L(a)$ has no fixed points, because if $xL(a) = x$ then $a*x = x$, so $a = e$, contradicting the assumption that a is of order 2. Hence $L(a)$ partitions L into pairs, so the cardinality of L must be even. □

This is not true in non IP loops because four of the six non-isomorphic loops of order 5 (all non-associative) contain self-inverse elements.

5.4.1 How We Counted IP Loops

The IP loops of small orders were counted by using a finite domain constraint solver to generate representatives of all isomorphism classes. The solver FINDER [63] has previously been used to generate results concerning the spectra of quasigroup identities [27]. It works by expressing each equation or other defining condition as the set of its ground instances on the domain of N elements, compiling these into constraints relating the cells $x*y$ of the "multiplication table" of

the algebra, and then conducting a backtracking search for solutions to the constraint satisfaction problem using standard techniques such as forward checking and nogood learning [20]. To break symmetries (reduce the size of isomorphism classes of solutions generated) we added clauses stipulating that e is always the element number 1, that x^{-1} is always either x or $x \pm 1$, and that any self-inverse elements are given lower numbers than the rest. That still leaves a great many isomorphic copies among the solutions, so it is necessary to remove them in a postprocessing step by rejecting any algebra that is not the canonical representative (here defined simply as the first in the obvious lexicographic order) of its isomorphism class.

The results for orders up to 11 are not hard to generate. As a check on the correctness of the method, the same results were obtained independently using the first order theorem prover PROVER9 and its associated propositional satisfiability solver Mace4 [43]. FINDER with its default settings was unable to solve completely the order 12 problem, so it was necessary to restrict its use of learned nogoods, after which it completed the search in a few days on a desktop computer. For the order 13 problem, further symmetry-breaking clauses were added, forcing solutions to be those early in the lexicographic order. Even so, the runtime to obtain the solutions of order 13 was over a week.[1] Nearly all of this time was taken up by the postprocessor reasoning about isomorphism, indicating that if any larger orders are to be addressed, improvements in the efficiency of the constraint solver are largely irrelevant: more sophisticated symmetry breaking is essential.

Table 5.4 gives the number of isomorphism classes of IP loops of each order up to 13, distinguishing between those which are groups and those which are not. In the cases of order 12 and order 13, the required searches are too hard for MACE and PROVER9, so we have only the results by FINDER in those cases.

The full list of these small IP loops, in a simple matrix format as for the order 7 example above, is available online at http://users.rsise.anu.edu.au/jks/IPloops.

By looking at the definition of IP loop it appears that these loops are a sort of 'weak' associative loop. But now that we have the number of loops (table 5.3) as well as the number of IP loops (table 5.4) we can see how strong the 'weakness' of the associative law is. We are amazed to see that out of 23746 isomorphism classes of loops of order 7 there are only two classes that are IP loops. The probability of

[1] Since these results were obtained, the software for eliminating isomorphic copies has been improved to the point that the IP loops of order 13 can be enumerated in a few hours. Order 14, however, remains out of reach.

size	groups	non-groups	total
1	1	0	1
2	1	0	1
3	1	0	1
4	2	0	2
5	1	0	1
6	2	0	2
7	1	1	2
8	5	3	8
9	2	5	7
10	2	45	47
11	1	48	49
12	5	2679	2684
13	1	10341	10342

Table 5.4: Number of IP loops of given order

a loop having inverse property drops really down when we see that out of almost 2.1×10^{20} isomorphism classes of loops of order 10 only 47 posess the inverse property. Does this inverse property of a loop put it closer to being group? In some sense not, because we found that out of 10342 isomorphism classes of IP loops of order 13 only one happens to be a group.

5.4.2 Subclasses of IP Loops

See Section 2.3 for the definitions of concepts referred to below.

Smallest Steiner loop:

The data of IP loops (of order up to 13) was first of all tested for finding Steiner loops. Although it is known, our search confirmed that the smallest non-associative Steiner loop is of order 10 and this is the only Steiner loop of order 10. Also this is the only Steiner loop among IP loops of order up to 13. Its table is given in :

Example 12.

$*$	1	2	3	4	5	6	7	8	9	10
$e=1$	1	2	3	4	5	6	7	8	9	10
2	2	1	4	3	6	5	8	7	10	9
3	3	4	1	2	7	9	5	10	6	8
4	4	3	2	1	10	8	9	6	7	5
5	5	6	7	10	1	2	3	9	8	4
6	6	5	9	8	2	1	10	4	3	7
7	7	8	5	9	3	10	1	2	4	6
8	8	7	10	6	9	4	2	1	5	3
9	9	10	6	7	8	3	4	5	1	2
10	10	9	8	5	4	7	6	3	2	1

We observed that Steiner loops exist only among IP loops of order $n \equiv 2 \pmod 6$ or $n \equiv 4 \pmod 6$ as can be verified by an easy counting argument.

Non-associative abelian IP loops: Next was to find the IP loops that are abelian but non-associative. Though it was not hard to find them, we must admit that the outcome was very much unexpected. The smallest non-associative abelian IP loop is also of order 10 but there are exactly 5 such IP loops (one of them is of course a Steiner loop). We give only one of them as Example 13.

Example 13.

$*$	1	2	3	4	5	6	7	8	9	10
$e=1$	1	2	3	4	5	6	7	8	9	10
2	2	1	4	3	6	5	9	10	7	8
3	3	4	1	2	7	8	5	6	10	9
4	4	3	2	1	9	10	8	7	5	6
5	5	6	7	9	2	1	10	3	8	4
6	6	5	8	10	1	2	3	9	4	7
7	7	9	5	8	10	3	4	1	6	2
8	8	10	6	7	3	9	1	4	2	5
9	9	7	10	5	8	4	6	2	3	1
10	10	8	9	6	4	7	2	5	1	3

x	x^{-1}
1	1
2	2
3	3
4	4
5	6
6	5
7	8
8	7
9	10
10	9

Table 5.5 gives the number of abelian IP loops of each order up to 13, distinguishing between those which are groups and those which are not.

IP loops with Square Property: We know that a group G is abelian if and only if $(x * y)^2 = x^2 * y^2$ for all $x, y \in G$. This also holds in Steiner loops

size	groups	non-groups	total
1	1	0	1
2	1	0	1
3	1	0	1
4	2	0	2
5	1	0	1
6	1	0	1
7	1	0	1
8	3	0	3
9	2	0	2
10	1	5	6
11	1	1	2
12	2	12	14
13	1	7	8

Table 5.5: Numbers of Abelian IP loops of given order

which are a subclass of IP loops. However this is not true in IP loops in general. The smallest counter example is the Example 13. The violation comes from the fact that $(3 * 7)^2 \neq 3^2 * 7^2$. Interestingly in IP loops, the converse of this fact is not true in general either. The smallest example of a non-abelian IP loop in which $(x * y)^2 = x^2 * y^2$ holds for all x and y is of order 12 and there are exactly 3 such of order 12. We also found out that there are exactly 2 such loops among IP loops of order 13. This means that in the given data of IP loops (of order up to 13) there are exactly 5 non-abelian IP loops with this property. We list here two out of these 5; one each of order 12 and 13:

Example 14.

$*$	1	2	3	4	5	6	7	8	9	10	11	12
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	7	8	5	6	11	12	9	10
3	3	4	2	1	9	10	11	12	7	8	5	6
4	4	3	1	2	11	12	9	10	5	6	7	8
5	5	7	11	9	6	1	8	2	12	4	10	3
6	6	8	12	10	1	5	2	7	4	11	3	9
7	7	5	9	11	8	2	6	1	10	3	12	4
8	8	6	10	12	2	7	1	5	3	9	4	11
9	9	11	5	7	12	3	10	4	8	1	6	2
10	10	12	6	8	3	11	4	9	1	7	2	5
11	11	9	7	5	10	4	12	3	6	2	8	1
12	12	10	8	6	4	9	3	11	2	5	1	7

x	x^{-1}
1	1
2	2
3	4
4	3
5	6
6	5
7	8
8	7
9	10
10	9
11	12
12	11

Example 15.

$*$	1	2	3	4	5	6	7	8	9	10	11	12	13
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12	13
2	2	4	1	5	3	8	9	10	11	12	13	7	6
3	3	1	5	2	4	13	12	6	7	8	9	10	11
4	4	5	2	3	1	9	8	12	13	7	6	11	10
5	5	3	4	1	2	11	10	7	6	13	12	8	9
6	6	13	8	11	9	12	1	5	3	4	10	2	7
7	7	12	9	10	8	1	13	3	5	11	4	6	2
8	8	6	10	7	12	4	2	11	1	9	3	13	5
9	9	7	11	6	13	2	4	1	10	3	8	5	12
10	10	8	12	13	7	5	11	9	2	6	1	4	3
11	11	9	13	12	6	10	5	2	8	1	7	3	4
12	12	10	7	8	11	3	6	13	4	5	2	9	1
13	13	11	6	9	10	7	3	4	12	2	5	1	8

x	x^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6
8	9
9	8
10	11
11	10
12	13
13	12

Abelian Non-associative IP loop of order p^2 : We also know that a group G of order p^2 (where p is prime) is abelian. This is not true in IP loops in general because none of the five non-associative IP loops of order 9 is abelian. However both IP loops of order 9 that are abelian happen to be groups. This lead us to ask whether all abelian IP loops of order p^2 are groups. This was also proven wrong in Example 16.

Example 16.

Consider the following non-associative abelian IP loop of order 11.

$*$	1	2	3	4	5	6	7	8	9	10	11
$e=1$	1	2	3	4	5	6	7	8	9	10	11
2	2	4	1	6	3	8	5	10	7	11	9
3	3	1	5	2	7	4	9	6	11	8	10
4	4	6	2	9	1	11	3	5	10	7	8
5	5	3	7	1	8	2	10	11	4	9	6
6	6	8	4	11	2	10	1	9	3	5	7
7	7	5	9	3	10	1	11	2	8	6	4
8	8	10	6	5	11	9	2	7	1	4	3
9	9	7	11	10	4	3	8	1	6	2	5
10	10	11	8	7	9	5	6	4	2	3	1
11	11	9	10	8	6	7	4	3	5	1	2

x	x^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6
8	9
9	8
10	11
11	10

If we take the direct product of this loop with itself or with C_{11} (cyclic group of order 11) then we get a non-associative abelian IP loop of order 11×11 which is not a group.

Flexible and Alternative IP loops: It is well known that the Steiner loops are both Flexible and Alternative. Apart from the Steiner loop of order 10 we found out that the smallest non-associative IP loop that is both flexible and alternative is of order 12 and there are exactly two of order 12. But as we found none of order 13, we conclude that there are exactly two non-Steiner non-associative IP loops of order less than or equal to 13 that are flexible and alternative. We provide the multiplication table for both of them here:

Example 17.

$*$	1	2	3	4	5	6	7	8	9	10	11	12
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	7	11	12	9	10
3	3	4	1	2	9	11	10	12	5	7	6	8
4	4	3	2	1	11	10	12	9	8	6	5	7
5	5	6	9	12	1	2	11	10	3	8	7	4
6	6	5	12	10	2	1	9	11	7	4	8	3
7	7	8	10	11	12	9	1	2	6	3	4	5
8	8	7	11	9	10	12	2	1	4	5	3	6
9	9	12	5	8	3	7	6	4	1	11	10	2
10	10	11	7	6	8	4	3	5	12	1	2	9
11	11	10	8	7	4	3	5	6	2	9	12	1
12	12	9	6	5	7	8	4	3	10	2	1	11

x	x^{-1}
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	12
12	11

Example 18.

$*$	1	2	3	4	5	6	7	8	9	10	11	12
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	7	11	12	9	10
3	3	4	1	2	9	11	10	12	5	7	6	8
4	4	3	2	1	12	10	11	9	8	6	7	5
5	5	6	9	11	1	2	12	10	3	8	4	7
6	6	5	12	10	2	1	9	11	7	4	8	3
7	7	8	10	12	11	9	1	2	6	3	5	4
8	8	7	11	9	10	12	2	1	4	5	3	6
9	9	12	5	8	3	7	6	4	1	11	10	2
10	10	11	7	6	8	4	3	5	12	1	2	9
11	11	10	8	5	7	3	4	6	2	9	12	1
12	12	9	6	7	4	8	5	3	10	2	1	11

x	x^{-1}
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	12
12	11

C-loops:

It is again known that Steiner loops are also C-loops. When we searched our data of IP loops (of order up to 13) for C-loops, we found that the smallest non-Steiner non-associative C-loop is of order 12 and this is the only such loop in our entire data. Here it is:

Example 19.

$*$	1	2	3	4	5	6	7	8	9	10	11	12
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	5	7	3	8	4	6	11	12	9	10
3	3	6	1	9	10	2	12	11	4	5	8	7
4	4	8	10	1	11	12	9	2	7	3	5	6
5	5	7	2	11	12	1	10	9	3	8	6	4
6	6	3	9	12	1	11	2	10	8	7	4	5
7	7	5	12	2	9	10	11	1	6	4	3	8
8	8	4	11	10	2	9	1	12	5	6	7	3
9	9	11	6	3	8	7	5	4	12	1	10	2
10	10	12	4	8	7	3	6	5	1	11	2	9
11	11	9	8	5	6	4	3	7	10	2	12	1
12	12	10	7	6	4	5	8	3	2	9	1	11

x	x^{-1}
1	1
2	2
3	3
4	4
5	6
6	5
7	8
8	7
9	10
10	9
11	12
12	11

Non-associative IP loop with Lagrange Property: In the data of IP loops that we have, the smallest non-associative IP loop that has the strong (and hence also the weak) Lagrange property is of order 8; its multiplication table is given here:

Example 20.

$*$	1	2	3	4	5	6	7	8
$e=1$	1	2	3	4	5	6	7	8
2	2	1	5	6	3	4	8	7
3	3	6	1	7	8	2	4	5
4	4	5	8	1	2	7	6	3
5	5	4	2	8	7	1	3	6
6	6	3	7	2	1	8	5	4
7	7	8	6	3	4	5	2	1
8	8	7	4	5	6	3	1	2

x	x^{-1}
1	1
2	2
3	3
4	4
5	6
6	5
7	8
8	7

It has only two proper non-trivial subloops $\{1,2,7,8\}$ and $\{1,2\}$ and the order of each of them divides the order of the loop. This means that the loop has the weak Lagrange property. But also since each of its subloops has the weak Lagrange property the loop itself has the strong Lagrange property.

Hamiltonian IP loop: The smallest non-associative IP loop that is also Hamiltonian is of order 9 and its table is given here:

Example 21.

$*$	1	2	3	4	5	6	7	8	9
$e=1$	1	2	3	4	5	6	7	8	9
2	2	3	1	6	7	8	9	4	5
3	3	1	2	8	9	4	5	6	7
4	4	8	6	7	1	5	3	9	2
5	5	9	7	1	6	3	4	2	8
6	6	4	8	5	2	9	1	7	3
7	7	5	9	2	4	1	8	3	6
8	8	6	4	9	3	7	2	5	1
9	9	7	5	3	8	2	6	1	4

x	x^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6
8	9
9	8

It has only one proper non-trivial subloop $\{1, 2, 3\}$ and it is also normal. Hamiltonian loops form an important subclass of loops with the strong Lagrange property. Example 20 is an IP loop that has the strong Lagrange property but is not Hamiltonian for the reason that $\{1, 2\}$ is not normal.

Spectrum of IP loops of exponent 3: IP loops of exponent 3 satisfy the following equivalent property:

$$x * x = x^{-1}$$

for all x. As we know that even order IP loop must have at least one self inverse element (other than the identity element), none of the even order IP loops fall into this spectrum and hence the same is true for Steiner loops. The smallest example of a non-associative IP loop that comes in this spectrum is that of order 7. When we searched our data for this particular spectrum we observed that only those IP loops come into this spectrum that have order either $n \equiv 1 \pmod 6$ or $n \equiv 3 \pmod 6$ which can again be verified by counting arguments. Table 5.6 gives the number of IP loops of each order up to 13 in the spectrum of exponent 3, distinguishing between those which are groups and those which are not.

Spectrum of IP loops of exponent 5: IP loops of exponent 5 satisfy the following equivalent property:

$$x^2 * x^2 = x^{-1}$$

for all x and consequently $x^2 * x = x * x^2$ (call it x^3) and $x * x^3 = x^3 * x = x^{-1}$. Again for the obvious reason none of the even order IP loops (including Steiner loops of course) fall into this spectrum. The smallest example of a non-associative IP loop that comes in this spectrum is that of order 13 and there are exactly 10

size	groups	non-groups	total
1	1	0	1
2	0	0	0
3	1	0	1
4	0	0	0
5	0	0	0
6	0	0	0
7	0	1	1
8	0	0	0
9	1	1	2
10	0	0	0
11	0	0	0
12	0	0	0
13	0	64	64

Table 5.6: Numbers of IP loops of exponent 3 of given order

such of order 13. A simple counting argument shows that only those IP loops come into this spectrum that have order either $n \equiv 1 \pmod{12}$ or $n \equiv 5 \pmod{12}$. One of the smallest 10 is given here:

Example 22.

$*$	1	2	3	4	5	6	7	8	9	10	11	12	13
$e=1$	1	2	3	4	5	6	7	8	9	10	11	12	13
2	2	4	1	5	3	10	11	12	13	9	6	7	8
3	3	1	5	2	4	11	12	13	10	6	7	8	9
4	4	5	2	3	1	12	13	10	11	7	8	9	6
5	5	3	4	1	2	13	10	11	12	8	9	6	7
6	6	13	10	11	12	8	1	9	7	2	3	4	5
7	7	10	11	12	13	1	9	6	8	3	4	5	2
8	8	11	12	13	10	9	6	7	1	4	5	2	3
9	9	12	13	10	11	7	8	1	6	5	2	3	4
10	10	6	7	8	9	5	2	3	4	12	1	13	11
11	11	7	8	9	6	2	3	4	5	1	13	10	12
12	12	8	9	6	7	3	4	5	2	13	10	11	1
13	13	9	6	7	8	4	5	2	3	11	12	1	10

x	x^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6
8	9
9	8
10	11
11	10
12	13
13	12

Diassociative and A-loops among IP loops data: Since each proper subloop of any loop in our data is again an IP loop and has order less than or equal to 6, we conclude that all proper subloops of the IP loops in our data are groups and so are two-element generated ones. This means all IP loops in the data are diassociative. It is not easy to check the subclass of A-loops in the given data but since all of them are diassociative and none of them is a non-associative Moufang loop (the smallest non-associative Moufang loop is of order 16), we conclude that none of the IP loops in our data are A-loops (since diassociative A-loops are Moufang).

RIF IP loops: It is again not easy to test if the given IP loop is RIF or not, but we tested the smallest IP loop of order 7 (L_7) and this turned out to be not RIF because the permutation $\alpha = (234) \in I(L_7)$ but $(2^{-1})\alpha \neq ((2)\alpha)^{-1}$.

Chapter 6

Further Study of Inverse Property Loops

This chapter consists of three sections. In Section 1 we study a subclass of IP loops called C-loops and In Section 2, we study a generalization of IP loops called WIPLs. Section 3 gives re-counting of NAFILS , counting of some interesting subclasses of NAFILS and counting of AAIP loops. We had given definitions of some important subclasses of loops in Section 2.3. First we give definitions of some other classes that will be used in this chapter.

Let G be a loop. G is said to be **LC-loop** if it satisfies the identity $xx \cdot yz = (x \cdot xy)z$. G is said to be **RC-loop** if it satisfies the identity $yz \cdot xx = y(zx \cdot x)$ and it is said to be **C-loop** if it is both LC-loop and RC-loop. A direct definition of C-loop has also been given in Section 2.3. G is said to be **CIP loop** (crossed inverse property loop) if it satisfies any of the following equivalent identities.

$$xy \cdot x^{\rho} = y \text{ or } x \cdot yx^{\rho} = y \text{ or } x^{\lambda} \cdot (yx) = y \text{ or } x^{\lambda}y \cdot x = y.$$

where x^{λ} denotes left inverse of x and x^{ρ} denotes right inverse of x. G will be said to satisfy the **weak inverse property** or **WIP** if whenever three elements x, y, z of G satisfy the relation $xy \cdot z = 1$, they also satisfy the relation $x \cdot yz = 1$. Such loops are called **WIP loops** or **WIPLs**. The study of WIPLs was initiated by J. M. Osborn [51] as a class of loops which contains both IP loops and CIP loops. He proved that WIP loop is a loop which satisfies one of the following equivalent identities

$$x(yx)^{\rho} = y \text{ or } (xy)^{\lambda}x = y^{\lambda}.$$

A NAFIL is a nonassociative finite invertible loop G [14].

Remark 5. *Since NAFILs are invertible loops so inverses will be unique i.e. left inverse and right inverse of an element will be equal.*

The following notion of loop theory should be also noted. Let L be a loop we then define left nucleus N_λ, middle nucleus N_μ, and right nucleus N_ρ of L as the sets

$$N_\lambda = \{x \in L; x(yz) = (xy)z \text{ for every } y, z \in L\}$$
$$N_\mu = \{x \in L; y(xz) = (yx)z \text{ for every } y, z \in L\}$$
$$N_\rho = \{x \in L; y(zx) = (yz)x \text{ for every } y, z \in L\}$$

The nucleus N of L is the defined as $N = N_\lambda \cap N_\mu \cap N_\rho$. N is subgroup of L and, in particular, for C-loops we have $N = N_\lambda = N_\mu = N_\rho$.
L is called left nuclear square if for all $x \in L$, $x^2 \in N_\lambda$, middle nuclear square if $x^2 \in N_\mu$, and right nuclear square if $x^2 \in N_\rho$. L is said to be nuclear square if $x^2 \in N$.
Let L be a loop and $x \in G$. Then L_x and R_x are both permutations of L defined as follows:

$$\begin{aligned} yL_x &= xy \\ yR_x &= yx \end{aligned}$$

These are called the *left* and *right translation maps* respectively.
Also note that $\forall x, y \in L$, $L_{x,y} = L_x L_y L_{yx}^{-1}$.
Also to avoid excessive parenthesization, we will use the usual juxtaposition conventions , e.g., $ab \cdot c = (a \cdot b) \cdot c$.

Remark 6. *We have used the GAP package LOOPS [48] for checking the various properties of the Cayley tables of loops. In particular we have used it in Examples 23 and 24.*

6.1 A Study of IP Loops

This section has two subsections. In Subsection 1 we discuss C-loops which is a subclass of IP loops. In Subsection 2 we discuss some results about IP loops.

6.1.1 Characterizations of C-loops

Here we discuss two characterizations of C-loops. C-loops can characterized one way as:

Theorem 5. *C-loops are exactly alternative loops with all squares in the nucleus.*

We can characterize C-loops in the following way as well:

Theorem 6. *C-loops are exactly IP loops with all squares in the nucleus.*

We do not claim these characterizations to be new but the second characterization seems to be at least not explicitly known. Consider the following lemma:

Lemma 5. *[53, Corollary 2.4]. Let L be a C-loop. Then (i) L is both left alternative and right alternative,*

(ii) L has the inverse property,

(iii) L is a nuclear square loop, i.e., x^2 belongs to the nucleus of L for every $x \in L$.

From Lemma 5 the direct parts of Theorem 5 and Theorem 6 follow obviously. The converse of Lemma 5 follows from parts (i) and (iii) by [56, Proposition 1] for RC-loop and can easily be proved for LC-loop. Thus Theorem 5 follows. In the following we prove that the converse of Lemma 5 and hence the converse of Theorem 6 also follows from parts (ii) and (iii).

Lemma 6. *Let L be an IP Loop. If L is a left (resp. right) nuclear square loop then L is a LC-loop (resp. RC-loop).*

Proof. Suppose L is left nuclear square loop then by definition

$$(xx)(yz) = [(xx)y]z, \text{ for every } x, y, z \in L. \tag{1}$$

Now consider

$$\begin{aligned}
(xx)(yz) &= [(xx)y]z = [(xx)(x^{-1} \cdot xy)]z \\
&= [(xx)(x^{-1}y_1)]z \text{ where } y_1 = xy \\
&= [(xx)x^{-1} \cdot y_1]z, \text{ by using (1)} \\
&= (xy_1)z = [x(xy)]z \\
&\Rightarrow (xx)(yz) = [x(xy)]z.
\end{aligned}$$

Hence L is a LC-loop. The proof of part (ii) is similar. □

Corollary 7. *Let L be an IP Loop. Then the following are equivalent:*

(i) L is a nuclear square loop,

(ii) L is a C-loop.

Hence Theorem 6 also follows. The converse of Lemma 5 does not follow from parts (i) and (ii) as every non-associative Moufang loop is an alternative IP loop but obviously does not have to be a C-loop.

Theorem 8. *Let $L = (S, *)$ be a finite IP loop. Then the cardinality of S is even iff L has an element of order 2-that is an element a such that $a \neq e$ but $a^2 = e$ [2, theorem 1].*

Corollary 9. *Let L be an IP loop. Then L has even order iff L has a subgroup of order 2.*

Finally from Theorem 8, [53, Proposition 3.1] and [53, Corollary 4.2], we have

Corollary 10. *Every nonassociative C-loop has even exponent.*

6.1.2 Some Results on IP Loops

Recall that an IP loop satisfies $R_x^{-1} = R_{x^{-1}}$ and $L_x^{-1} = L_{x^{-1}}$ for all $x \in L$ see [10]. Next we define $(y)\, D_x = (x)\, L_y^{-1} = y \backslash x$ and $(x)\, J = (x)\, D_1 = x^{-1} = x \backslash 1$.

Theorem 11. *An IP loop L is right alternative $\Leftrightarrow D_{x^2} = D_x J D_x$*

for all $x, y \in L$ and $D_x, J \in \mathrm{Mlt}(L)$.

Proof. Suppose that an IP loop is right alternative then

$$\begin{aligned}
yD_xJD_x &= (yD_x)\, JD_x \\
&= \left(xL_y^{-1}\right) JD_x \\
&= \left(xL_{y^{-1}}\right) JD_x = \left(y^{-1}x\right) JD_x \\
&= \left(y^{-1}x\right)^{-1} D_x = \left(x^{-1}y\right) D_x \\
&= (x)\, L_{x^{-1}y}^{-1} = (x)\, L_{(x^{-1}y)^{-1}} \\
&= (x)\, L_{(y^{-1}x)} = \left(y^{-1}x\right) x \\
&= y^{-1}x^2 \ \because L \text{ is right alternative} \\
&= x^2 L_{y^{-1}} = x^2 L_y^{-1} \\
&= yD_{x^2} \\
\Rightarrow\ & D_xJD_x = D_{x^2}
\end{aligned}$$

Conversely suppose that $D_{x^2} = D_x J D_x$ then

$$\begin{aligned}
(y)\, D_{x^2} &= (y)\, D_x J D_x \\
&\Rightarrow x^2 L_y^{-1} = \left(x L_y^{-1}\right) J D_x \\
&\Rightarrow x^2 L_{y^{-1}} = \left(x L_{y^{-1}}\right) J D_x \\
&\Rightarrow y^{-1} x^2 = \left(y^{-1} x\right) J D_x \\
&\Rightarrow y^{-1} x^2 = \left(y^{-1} x\right)^{-1} D_x \\
&\Rightarrow y^{-1} x^2 = \left(x^{-1} y\right) D_x \\
&\Rightarrow y^{-1} x^2 = (x)\, L_{x^{-1} y}^{-1} \\
&\Rightarrow y^{-1} x^2 = (x)\, L_{(x^{-1} y)^{-1}} \\
&\Rightarrow y^{-1} x^2 = (x)\, L_{(y^{-1} x)} \\
&\Rightarrow y^{-1}(xx) = \left(y^{-1} x\right) x \\
&\Rightarrow L \text{ is right alternative}
\end{aligned}$$

Hence the result follows. □

Theorem 12. *If $y \in N(L)$, then the following identities hold in IP loops.*

(1) $(x^n)\, L_{y,x^m} = x^n$

(2) $L_{x^n} L_{y,x^m} = L_{y,x^m} L_{x^n}$

(3) $D_{x^n} L_{y,x^m} = L_{y,x^m} D_{x^n}$

where $L_{y,x^m}, L_{x^n}, D_{x^n} \in \mathrm{Mlt}(L)$ and $x, y, z \in L$.

Proof. (1)

$$\begin{aligned}
L.H.S &= (x^n)\, L_{y,x^m} = (x^n)\, L_y L_{x^m} L_{x^m y}^{-1} \\
&= (yx^n)\, L_{x^m} L_{\left(x^m y\right)^{-1}} = \left(x^m (yx^n)\right) L_{\left(x^m y\right)^{-1}} \\
&= \left((x^m y)\, x^n\right) L_{\left(x^m y\right)^{-1}}, \text{ since } y \in N(L) \\
&= (x^m y)^{-1} \left((x^m y)\, x^n\right) \\
&= x^n \because L \text{ is IPloop} \\
&= R.H.S
\end{aligned}$$

(2) Since

$$\begin{aligned}
(z)\, L_{x^n} L_{y,x^m} &= (x^n z)\, L_{y,x^m} \\
&= x^n z \text{ by part(1)} \\
&= (z)\, L_{x^n} \\
&= (z L_{y,x^m})\, L_{x^n} \text{ by part(1)} \\
&= (z)\, L_{y,x^m} L_{x^n} \\
\Rightarrow\ & L_{x^n} L_{y,x^m} = L_{y,x^m} L_{x^n}
\end{aligned}$$

(3) Since

$$\begin{aligned}
(z)\, D_{x^n} L_{y,x^m} &= \left(x^n L_z^{-1}\right) L_{y,x^m} \\
&= (x^n L_{z^{-1}}) L_{y,x^m} = \left(z^{-1} x^n\right) L_{y,x^m} \\
&= z^{-1} x^n \text{ by part(1)} \\
&= x^n L_{z^{-1}} = x^n L_z^{-1} \\
&= (z)\, D_{x^n} \\
&= (z L_{y,x^m})\, D_{x^n} \text{ by part(1)} \\
&= (z)\, L_{y,x^m} D_{x^n} \\
\Rightarrow\ & D_{x^n} L_{y,x^m} = L_{y,x^m} D_{x^n}
\end{aligned}$$

Hence the result follows. □

The following proposition generalizes a result of C-loops to IP loops.

Proposition 3. *For any natural number n there is a non-associative non-commutative IP loop with nucleus of size n.*

Proof. By [53, corollary 3.5] for $n \geq 2$ there is a non-associative non-commutative C-loop and hence an IP loop with nucleus of size n. Now it remains to show that there is a non-associative non-commutative IP loop with nucleus of size 1. This is shown in the following example. □

Example 23. *A non-associative non-commutative IP loop with nucleus of size 1.*

·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	4	6	2	7	3	5
2	2	7	5	0	3	1	4	6
3	3	5	0	4	6	2	7	1
4	4	6	3	1	7	0	5	2
5	5	3	7	2	0	6	1	4
6	6	4	1	7	5	3	2	0
7	7	2	6	5	1	4	0	3

While studying a large number of IP loops we were about to make a conjecture that the inner mapping group of an (non Moufang) IP loop is always even but finally we found one of order 12 whose inner mapping group is of order 27. Since such IP loops are very rare, we display this IP loop below:

Example 24. *A non-associative non-commutative IP loop of order 12.*

·	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	0	4	6	2	7	3	5	10	11	8	9
2	2	5	0	8	9	1	11	10	3	4	7	6
3	3	7	9	0	10	11	8	1	6	2	4	5
4	4	6	1	10	11	0	9	8	2	7	5	3
5	5	2	8	11	0	10	1	9	7	6	3	4
6	6	4	11	1	8	9	10	0	5	3	2	7
7	7	3	10	9	1	8	0	11	4	5	6	2
8	8	10	5	2	7	6	4	3	11	0	9	1
9	9	11	3	7	6	2	5	4	0	10	1	8
10	10	8	7	4	5	3	2	6	9	1	11	0
11	11	9	6	5	3	4	7	2	1	8	0	10

6.2 A Study of WIPLs

This section has also two subsections. In Subsection 1 we discuss some sufficient conditions for WIPLs. In Subsection 2 we give some constructions of WIPLs.

6.2.1 Some Sufficient Conditions for WIPLs

LC-loops, RC-loops, C-loops, ARIF loops are subclasses of WIPLs. WIPLs do not have invertible (two-sided) inverses necessarily. Throughout this section we consider only invertible WIPLs. We prove here some sufficient conditions for a WIPL to be one of these loops. We define $L_x : a \longrightarrow xa$, $R_x : a \longrightarrow ax$, $J : x \longrightarrow x^{-1}$ and $P_x = R_x \circ L_x \; \forall \; x \in L$.

Theorem 13. *Let L be a WIPL. Then $(JP_x)^n = I$ for any $n \in 2\mathbb{Z}^+$, where $\mathbb{Z}^+$ denotes the set of positive integers.*

Proof. *Let $y \in L$. Since $P_x = R_x \circ L_x$ then for $(JP_x)^n = I$ where $n \in 2Z^+$. Consider $n = 2$ then*

$$\begin{aligned}(y)(JP_x)^2 &= (y)JP_xJP_x = x((x(y^{-1}x))^{-1}x) = x(y^{-1}x)^{-1} \\ &= y\end{aligned}$$

Thus $(JP_x)^2 = I$. Now if any $n \in 2\mathbb{Z}^+$, then $n = 2m$ for some $m \in \mathbb{Z}^+$

$$\text{so } (JP_x)^n = (JP_x)^{2m} = ((JP_x)^2)^m = (I)^m = I$$

□

Corollary 14. *$(JP_x)^n = I$ for all $n \in \mathbb{Z}^+$ if the loop is a WIPL of exponent 2.*

Proof. Let L be a WIPL of exponent 2, and consider

$$\begin{aligned}(y)(JP_x) &= y^{-1}R_x \circ L_x \\ &= x(y^{-1}x) \\ &= x(y^{-1}x)^{-1} \text{ since } L \text{ is of exponent 2} \\ &= y^{-1} \text{ by WIP} \\ &= y\end{aligned}$$

Thus $JP_x = I$ and hence $(JP_x)^n = I$ for all $n \in \mathbb{Z}^+$ if the loop is WIPL of exponent 2. □

Next we prove necessary and sufficient conditions for WIPL to be left alternative, and right alternative.

Theorem 15. *L be a WIPL, then L is left alternative if and only if $L_x = R_xJL_{x^2}JP_x$.*

Proof. Let L be a WIPL satisfying $L_x = R_x J L_{x^2} J P_x$ then consider

$$\begin{aligned} L_x &= R_x J L_{x^2} J P_x \\ J R_x^{-1} J &= R_x J L_{x^2} J P_x \text{ since } L_x = J R_x^{-1} J \\ R_x^{-1} J &= L_x^{-1} L_{x^2} J P_x \text{ since } L_x^{-1} = J R_x J \\ L_x R_x^{-1} P_x &= L_{x^2} (J P_x)^2 \\ L_x R_x^{-1} R_x L_x &= L_{x^2} I \text{ by Theorem 13} \\ L_x L_x &= L_{x^2} \end{aligned}$$

Conversely, consider that L satisfies left alternativity, that is $x(xy) = x^2 y \ \forall$ $x, y \in L$ which implies that $L_x L_x = L_{x^2} \ \forall \ x \in$L. Thus we have that

$$\begin{aligned} L_x L_x &= L_{x^2} \\ L_x L_x P_x^{-1} &= L_{x^2} P_x^{-1} \\ L_x R_x^{-1} &= L_{x^2} (J P_x)^2 P_x^{-1} \text{ by Theorem 13} \\ R_x^{-1} &= L_x^{-1} L_{x^2} J P_x J \\ L_x &= R_x J L_{x^2} J P_x \text{ by left and right cancellation of } J \end{aligned}$$

□

Theorem 16. *Let L be WIPL, then L is right alternative if and only if $R_x = P_x J R_{x^2} J L_x$.*

Proof. Let L satisfies $R_x = P_x J R_{x^2} J L_x$ then we have

$$\begin{aligned} J R_x J &= J P_x J R_{x^2} J L_x J \text{ by multiplication of } J \text{ on both sides} \\ P_x L_x^{-1} &= P_x J P_x J R_{x^2} R_x^{-1} \text{ by multiplication of } P_x \text{ on both sides} \\ R_x R_x &= R_{x^2} \end{aligned}$$

Conversely, let L be right alternative. Then

$$\begin{aligned} R_x R_x &= R_{x^2} \\ P_x^{-1} R_x R_x &= P_x^{-1} R_{x^2} \\ L_x^{-1} I R_x &= P_x^{-1} R_{x^2} \\ L_x^{-1} R_x &= I P_x^{-1} R_{x^2} \\ R_x &= P_x J R_{x^2} J L_x \end{aligned}$$

□

Here we are proving a necessary and sufficient condition for WIPL to be a LC-loop.

Theorem 17. *L be WIPL, then L is a LC-loop if and only if it satisfies that* $JL_{x^2}T_z = L_zT_xJP_xL_z$.

Proof. Let L be an LC-loop then by LC property we have that

$$\begin{aligned} xx \cdot yz &= (x \cdot xy)z \\ (y)R_zL_{x^2} &= (y)L_xL_xR_z \text{ implies that} \\ R_zL_{x^2} &= L_xL_xR_z \\ R_zL_{x^2}T_z &= L_xL_xR_zT_z \\ JL_{x^2}T_z &= L_zR_x^{-1}L_xJR_xJJL_xL_z \text{ putting } L_x^{-1} = JR_xJ \\ JL_{x^2}T_z &= L_zT_xJP_xL_z \end{aligned}$$

Conversely suppose that L. satisfies that $JL_{x^2}T_z = L_zT_xJP_xL_z$ Then

$$\begin{aligned} JL_{x^2}T_z &= L_zT_xJP_xL_z \\ JR_zL_{x^2}R_z^{-1} &= T_xJP_x \\ R_zL_{x^2} &= L_xL_xR_z \\ (y)R_zL_{x^2} &= (y)L_xL_xR_z \ \forall \ y \in \mathrm{L}. \end{aligned}$$

□

Theorem 18. *A loop L (WIPL) is a C-loop if and only if* $R_x = P_xJR_{x^2}JL_x$ *and* $JL_{x^2}T_z = L_zT_xJP_xL_z$ *[30, Theorem* 4.2*].*

6.2.2 Construction of Non-associative WIPLs Loops Via Extension of Loops

Here we give some constructions of the infinite families of non-associative WIPLs by extension of loops. Our method is essentially that by which C-loops have been constructed in [53]. Indeed Every C-loop is a WIPL and the family of C-loops constructed in [53] is a family WIPLs too. Yet our constructions are needed due to the following reasons.

1. The construction of [53] is only for order $4n \geq 12$ while our constructions consider other orders also.

2. The construction of [53] is on the basis of Klien group while we consider other groups also.

3. Our WIPLs are not necessarily C-loops.

Remark 7. *We will use once again the adaptation of the same construction discovered in [53] for the construction of AAIP loops in Subsection 6.3.5.*

For this purpose we take a multiplicative group G with neutral element 1, and an additive abelian group A with neutral element 0. Any map $\mu : G \times G \to A$ satisfying $\mu(1, g) = \mu(g, 1) = 0$ for every $g \in G$ is called a factor set. So let $\mu : G \times G \to A$ is a factor set. Define multiplication on $G \times A$ by

$$(g, a)(h, b) = (gh, a + b + \mu(g, h)) \tag{A}$$

The groupoid we get as a result is clearly a loop with neutral element $(1, 0)$. We denote this by (G, A, μ). Additional requirements on μ can enforce additional properties of (G, A, μ).

Lemma 7. *Let $\mu : G \times G \to A$ be a factor set. Then (G, A, μ) is a WIPL iff*

$$\mu(h, h^{-1}) + \mu(g, g^{-1}h^{-1}) = \mu(h, g) + \mu(hg, g^{-1}h^{-1}) \tag{D}$$

for every $g, h \in G$.

Proof. The loop (G, A, μ) is a WIPL iff $(g, a)[(h, b)(g, a)]^{-1} = (h, b)^{-1}$ hold for every $g, h \in G$ and every $a, b \in A$. Straight forward calculation with (A) shows that this happens iff (D) holds. □

We call a factor set μ satisfies (A) and (D) a W-factor set. We now use a particular W-factor set to construct the above-mentioned families of WIPLs.

Proposition 4. *Let $n \geq 2$ be an integer and let A be an abelian group of order n, and $\alpha \in A$ be an element of order bigger than 2. Let $G = \{1, x, x^2\}$ be the cyclic group of order 3 with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(h, g) = \begin{cases} \alpha, if\ (h, g) = (x, x), \\ 0, \text{ otherwise.} \end{cases}$$

Then (G, A, μ) is a non-alternative (hence non-associative) commutative WIPL with $N = \{(1, a) : a \in A\}$.

Proof. The map μ is clearly a factor set depicted as follows:

μ	1	x	x^2
1	0	0	0
x	0	α	0
x^2	0	0	0

To show that (G, A, μ) is a WIPL, we verify (D). Since μ is a factor set, there is nothing to prove when $g = 1$. Assume that $g = x$ then (D) becomes $\mu(h, h^{-1}) + \mu(x, x^2h^{-1}) = \mu(h, x) + \mu(hx, x^2h^{-1})$. If $h = 1$, then $\mu(1, 1) + \mu(x, x^2) = \mu(1, x) + \mu(x, x^2)$ and both sides of this equation are equal to 0. If $h = x$, then $\mu(x, x^2) + \mu(x, x) = \mu(x, x) + \mu(x^2, x)$ and both sides of this equation are equal to α. Assume $h = x^2$, then $\mu(x^2, x) + \mu(x, 1) = \mu(x^2, x) + \mu(1, xx)$ and both sides of this equation are equal to 0. Next assume that $g = x^2$, then (D) becomes $\mu(h, h^{-1}) + \mu(x^2, xh^{-1}) = \mu(h, x^2) + \mu(hx^2, xh^{-1})$. If $h = 1$, then both sides of this equation are equal to 0. Assume $h = x$, then both sides of this equation are equal to 0, Assume $h = x^2$, then $\mu(x^2, x) + \mu(x^2, x^2) = \mu(x^2, x^2) + \mu(x, x^2)$ and both sides of this equation are equal to 0. since $\alpha \neq 0$, we have that, $(x, a)(x, a) \cdot (x^2, a) \neq (x, a) \cdot (x, a)(x^2, a)$. Thus (G, A, μ) is non-alternative and hence non-associative. Also neither $(x, a) \in N$ nor $(x^2, a) \in N$ for all $a \in A$. Also we have that $(1, a)((h, b)(g, c)) = ((1, a)(h, b))(g, c)$ for all $h, g \in G$ and $a, b, c \in A$. Which implies that $(1, a)$ belongs to the nucleus. Thus $\{(1, a); a \in A\}$ is the nucleus of the loop (G, A, μ). □

Corollary 19. *For each natural number n there exists a nonassociative non-alternative commutative WIPL having nucleus of order n.*

Proof. It remains to show that there exist non-alternative commutative WIPL having nucleus of order 1. This requirement is fulfilled by the following example. □

Example 25. *A commutative, non-alternative WIPL of order 10 having trivial nucleus.*

·	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	8	9	6	7
2	2	3	0	1	6	7	4	5	9	8
3	3	2	1	0	8	9	7	6	4	5
4	4	5	6	8	1	0	9	2	7	3
5	5	4	7	9	0	1	2	8	3	6
6	6	8	4	7	9	2	3	0	5	1
7	7	9	5	6	2	8	0	3	1	4
8	8	6	9	4	7	3	5	1	2	0
9	9	7	8	5	3	6	1	4	0	2

Example 26. *The smallest group A satisfying the assumption of Proposition 4 is the cyclic group $\{0,1\}$ of order 2. The construction of Proposition 4 with $\alpha = 1$ then yields the following non-alternative commutative WIPL of order 6.*

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

Proposition 5. *Let $n \geq 3$ be an integer and let A be an abelian group of order n, and $\alpha \in A$ be an element of order bigger than 2. Let $G = \{1, u, v, w\}$ denotes the Klein group with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(x,y) = \begin{cases} \alpha, if\ (x,y) = (u,v),(v,w),(w,u), \\ 0,\ otherwise. \end{cases}$$

Then (G, A, μ) is a non-alternative, non-commutative WIPL with nucleus $N = \{(1,a);\ a \in A\}$.

Proof. The map μ is clearly a factor set depicted as follows:

μ	1	u	v	w
1	0	0	0	0
u	0	0	α	0
v	0	0	0	α
w	0	α	0	0

To show that (G, A, μ) is a WIPL, we verify (D). Since μ is a factor set, there is nothing to prove when $g = 1$. Assume that $g = u$ then (D) becomes $\mu(h, h^{-1}) + \mu(u, uh^{-1}) = \mu(h,u) + \mu(hu, uh^{-1})$. If $h = 1$, then both sides of this equation are equal to 0, Assume $h = v$, then $\mu(v,v) + \mu(u,w) = \mu(v,u) + \mu(w,w)$ and both sides of this equation are equal to 0. Assume $h = w$, then $\mu(w,w) + \mu(u,v) = \mu(w,u) + \mu(v,v)$ and both sides of this equation are equal to α. Next assume that $g = v$, then (D) becomes $\mu(h, h^{-1}) + \mu(v, vh^{-1}) = \mu(h,v) + \mu(hv, vh^{-1})$. If $h = 1$, then both sides of this equation are equal to 0. Assume $h = u$, $\mu(u,u) + \mu(v,w) = \mu(u,v) + \mu(w,w)$ and both sides of this equation are equal to α, Assume $h = v$, then $\mu(v,v) + \mu(v,1) = \mu(v,v) + \mu(1,1)$ both sides of this

equation are equal to 0. Assume $h = w$, then $\mu(w,w)+\mu(v,u) = \mu(w,v)+\mu(u,u)$ and both sides of this equation are equal to 0. Next assume that $g = w$, then (D) becomes $\mu(h,h^{-1}) + \mu(w,wh^{-1}) = \mu(h,w) + \mu(hw,wh^{-1})$. If $h = 1$, then both sides of this equation are equal to 0. Assume $h = u$, then this equation is equal to $\mu(u,u) + \mu(w,v) = \mu(u,w) + \mu(v,v)$ and both sides of this equation are equal to 0. Assume $h = v$, then $\mu(v,v) + \mu(w,u) = \mu(v,w) + \mu(u,u)$ and both sides of this equation are equal to α. Assume $h = w$, then $\mu(w,w) + \mu(w,1) = \mu(w,w) + \mu(1,1)$ and both sides of this equation are equal to 0. Since $\alpha \neq 0$, and we have that, $(u,a)(u,a)\cdot(v,a) \neq (u,a)\cdot(u,a)(v,a)$ also we have that, $(w,a)(u,a)\cdot(u,a) \neq (w,a)\cdot(u,a)(u,a)$. Thus (G,A,μ) is non-alternative and hence non-associative. Also $(u,a),(v,a),(w,a) \notin N$ for all $a \in A$. Also we have that $(1,a)((h,b)(g,c)) = ((1,a)(h,b))(g,c)$ for all $h,g \in G$ and $a,b,c \in A$. Which implies that $(1,a)$ belongs to the nucleus. Thus $\{(1,a);\ a \in A\}$ is the nucleus of the loop (G,A,μ). □

Corollary 20. *For each $n \geq 1$ there exists a non-alternative non-commutative WIPL having nucleus of order n.*

Proof. It remains to show that there exist a non-alternative non-commutative WIPL having nuclei of order 1 and 2. The first requirement follows by Example 23 while the second requirement follows by the following example.

Example 27. *A non-alternative non-commutative WIPL having nucleus of order 2.*

□

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

Example 28. *The smallest group A satisfying the assumption of Proposition 5 is the cyclic group $\{0,1,2\}$ of order 3. The construction of Proposition 5 with $\alpha = 1$ then yields the following non-alternative commutative WIPL of order 12.*

·	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	0	4	5	3	7	8	6	10	11	9
2	2	0	1	5	3	4	8	6	7	11	9	10
3	3	4	5	0	1	2	11	9	10	6	7	8
4	4	5	3	1	2	0	9	10	11	7	8	6
5	5	3	4	2	0	1	10	11	9	8	6	7
6	6	7	8	9	10	11	0	1	2	5	3	4
7	7	8	6	10	11	9	1	2	0	3	4	5
8	8	6	7	11	9	10	2	0	1	4	5	3
9	9	10	11	8	6	7	3	4	5	0	1	2
10	10	11	9	6	7	8	4	5	3	1	2	0
11	11	9	10	7	8	6	5	3	4	2	0	1

GAP gives these extra informations about the above Cayley table of WIPL. It is (1) power associative (2) not a Moufang loop (3) neither automorphic nor anti-automorphic (4) neither a left nor right bol loop.

Proposition 6. *Let $n \geq 3$ be an integer and let A be an abelian group of order n, and $\alpha \in A$ be an element of order bigger than 2. Let $G = \{1, u, v, w\}$ denotes the Klein group with respect to multiplication with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(x,y) = \begin{cases} \alpha, & \text{if } (x,y) = (u,v),(v,u),(u,w),(w,u),(v,w),(w,v), \\ 0, & \text{otherwise.} \end{cases}$$

Then (G, A, μ) is a non-alternative, commutative WIPL with nucleus $N = \{(1,a);\ a \in A\}$.

Proof. The map μ is clearly a factor set and can be depicted as follows:

μ	1	u	v	w
1	0	0	0	0
u	0	0	α	α
v	0	α	0	α
w	0	α	α	0

To show that (G, A, μ) is a WIPL, we verify (D). Since μ is a factor set, there is nothing to prove when $g = 1$. Assume that $g = u$ then (D) becomes $\mu(h, h^{-1}) + \mu(u, uh^{-1}) = \mu(h,u) + \mu(hu, uh^{-1})$. If $h = 1$, then $\mu(h, h^{-1}) + \mu(u,u) =$

$\mu(1,u)+\mu(u,u)$ both sides of this equation are equal to 0, Assume $h=u$ then $\mu(u,u)+\mu(u,1)=\mu(u,u)+\mu(1,1)$ both sides of this equation are equal to 0. Assume $h=v$, then $\mu(v,v)+\mu(u,w)=\mu(v,u)+\mu(w,w)$ and both sides of this equation are equal to α. Assume $h=w$, then $\mu(w,w)+\mu(u,v)=\mu(w,u)+\mu(v,v)$ and both sides of this equation are equal to α. Next assume that $g=v$, then (D) becomes $\mu(h,h^{-1})+\mu(v,vh^{-1})=\mu(h,v)+\mu(hv,vh^{-1})$. If $h=1$, then $\mu(1,1)+\mu(v,v)=\mu(1,v)+\mu(v,v)$ and both sides of this equation are equal to 0. Assume $h=u$, then $\mu(u,u)+\mu(v,w)=\mu(u,v)+\mu(w,w)$ and both sides of this equation are equal to α, Assume $h=v$, then $\mu(v,v)+\mu(v,1)=\mu(v,v)+\mu(1,1)$ both sides of this equation are equal to 0. Assume $h=w$, then $\mu(w,w)+\mu(v,u)=\mu(w,v)+\mu(u,u)$ and both sides of this equation are equal to α. Next assume that $g=w$, then (D) becomes $\mu(h,h^{-1})+\mu(w,wh^{-1})=\mu(h,w)+\mu(hw,wh^{-1})$. If $h=1$, then $\mu(1,1)+\mu(w,w)=\mu(1,w)+\mu(w,w)$ both sides of this equation are equal to 0. Assume $h=u$, then $\mu(u,u)+\mu(w,v)=\mu(u,w)+\mu(v,v)$ and both sides of this equation are equal to α. Assume $h=v$, then $\mu(v,v)+\mu(w,u)=\mu(v,w)+\mu(u,u)$ then both sides of this equation are equal to α. Assume $h=w$, then $\mu(w,w)+\mu(w,1)=\mu(w,w)+\mu(1,1)$ then both sides of this equation are equal to 0. Since $\alpha\neq 0$, and we have that, $(u,a)(u,a)\cdot(v,a)\neq(u,a)\cdot(u,a)(v,a)$. Also we have that, $(w,a)(u,a)\cdot(u,a)\neq(w,a)\cdot(u,a)(u,a)$. Thus (G,A,μ) is non-alternative and hence non-associative. Also $(u,a),(v,a),(w,a)\notin N$ for all $a\in A$. Also we have that $(1,a)((h,b)(g,c))=((1,a)(h,b))(g,c)$ for all $h,g\in G$ and $a,b,c\in A$. Which implies that $(1,a)$ belongs to the nucleus. Thus $\{(1,a);$ $a\in A\}$ is the nucleus of the loop (G,A,μ). □

Example 29. *The smallest group A satisfying the assumption of Proposition 6 is the cyclic group $\{0,1,2\}$ of order 3. The construction of Proposition 6 with $\alpha=1$ then yields the following non-alternative commutative WIPL of order 12.*

·	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	0	4	5	3	7	8	6	10	11	9
2	2	0	1	5	3	4	8	6	7	11	9	10
3	3	4	5	0	1	2	11	9	10	8	6	7
4	4	5	3	1	2	0	9	10	11	6	7	8
5	5	3	4	2	0	1	10	11	9	7	8	6
6	6	7	8	11	9	10	0	1	2	5	3	4
7	7	8	6	9	10	11	1	2	0	3	4	5
8	8	6	7	10	11	9	2	0	1	4	5	3
9	9	10	11	8	6	7	5	3	4	0	1	2
10	10	11	9	6	7	8	3	4	5	1	2	0
11	11	9	10	7	8	6	4	5	3	2	0	1

GAP [48] gives these extra informations about the above Cayley table of WIPL. It is (1) power associative (2) not automorphic inverse property loop (3) neither LC-Loop nor RC-Loop.

Proposition 7. *Let $n \geq 2$ be an integer and let A be an abelian group of order n, and $\alpha \in A$ be an element of order bigger than 2. Let $G = \{1, x, x^2, x^3, x^4\}$ be the Cyclic group of order 5 with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(h,g) = \begin{cases} \alpha, & \text{if } (h,g) = (x^2,x^2),(x,x^2),(x^2,x), \\ 0, & \text{otherwise.} \end{cases}$$

Then (G, A, μ) is a non-alternative commutative WIPL with nucleus $N = \{(1, a);\ a \in A\}$.

Proof. The map μ is clearly a factor set. Its Cayley table is as follows:

μ	1	x	x^2	x^3	x^4
1	0	0	0	0	0
x	0	0	α	0	0
x^2	0	α	α	0	0
x^3	0	0	0	0	0
x^4	0	0	0	0	0

To show that (G, A, μ) is a WIPL, we verify (D). Since μ is a factor set, there is nothing to prove when $g = 1$. Assume that $g = x$ then (D) becomes $\mu(h, h^{-1}) + \mu(x, x^4h^{-1}) = \mu(h, x) + \mu(hx, x^4h^{-1})$. If $h = 1$, then $\mu(h, h^{-1}) + \mu(x, x^4h^{-1}) =$

$\mu(h,x)+\mu(hx,x^4h^{-1})$ and both sides of this equation equals to 0. $h=x$, then $\mu(x,x^4)+\mu(x,x^3)=\mu(x,x)+\mu(x^2,x^3)$ then both sides of this equation are equal to 0,Assume $h=x^2$, then $\mu(x^2,x^3)+\mu(x,x^2)=\mu(x^2,x)+\mu(x^3,x^2)$ and both sides of this equation are equal to α. Assume $h=x^3$, then $\mu(x^3,x^2)+\mu(x,x)=\mu(x^3,x)+\mu(x^4,x)$ and both sides of this equation are equal to 0 Assume $h=x^4$, then $\mu(x^4,x)+\mu(x,1)=\mu(x^4,x)+\mu(1,1)$and both sides of this equation are equal to 0 assume that $g=x^2$, then (D) becomes $\mu(h,h^{-1})+\mu(x^2,x^3h^{-1})=\mu(h,x^2)+\mu(hx^2,x^3h^{-1})$. If $h=1$, then $\mu(1,1)+\mu(x^2,x^3)=\mu(1,x^2)+\mu(x^2,x^3)$ and both sides of this equation equals to 0. Assume $h=x$, then $\mu(x,x^4)+\mu(x^2,x^2)=\mu(x,x^2)+\mu(x^3,x^2)$ then both sides of this equation are equal to α, Assume $h=x^2$, then $\mu(x^2,x^3)+\mu(x^2,x)=\mu(x^2,x^2)+\mu(x^4,x)$ and both sides of this equation are equal to α. Assume $h=x^3$, then $\mu(x^3,x^2)+\mu(x^2,1)=\mu(x^3,x^2)+\mu(1,1)$ and both sides of this equation are equal to 0. Assume $h=x^4$, then $\mu(x^4,x)+\mu(x^2,x^4)=\mu(x^4,x^2)+\mu(x,x^4)$ and both sides of this equation are equal to 0. Assume that $g=x^3$, then $\mu(h,h^{-1})+\mu(x^3,x^2h^{-1})=\mu(h,x^3)+\mu(hx^3,x^2h^{-1})$. If $h=1$, then $\mu(1,1)+\mu(x^3,x^2)=\mu(1,x^3)+\mu(x^3,x^2)$ and both sides of this equation equals to 0. Assume $h=x$, then this equation equals to $\mu(x,x^4)+\mu(x^3,x)=\mu(x,x^3)+\mu(x^4,x)$ then both sides of this equation are equal to 0, Assume $h=x^2$, then $\mu(x^2,x^3)+\mu(x^3,1)=\mu(x^2,x^3)+\mu(1,1)$ and both sides of this equation are equal to 0. Assume $h=x^3$, then $\mu(x^3,x^2)+\mu(x^3,x^4)=\mu(x^3,x^3)+\mu(x,x^4)$ and both sides of this equation are equal to 0. Assume $h=x^4$, then $\mu(x^4,x)+\mu(x^3,x^3)=\mu(x^4,x^3)+\mu(x^2,x^3)$ and both sides of this equation are equal to 0, Assume that $g=x^4$, then (D) becomes $\mu(h,h^{-1})+\mu(x^4,xh^{-1})=\mu(h,x^4)+\mu(hx^4,xh^{-1})$. If $h=1$, then $\mu(1,1)+\mu(x^4,x)=\mu(1,x^4)+\mu(x^4,x)$ both sides of this equation equals to 0. Assume $h=x$, then $\mu(x,x4)+\mu(x^4,1)=\mu(x,x^4)+\mu(1,1)$ and both sides of this equation are equal to 0, Assume $h=x^2$, then $\mu(x^2,x^3)+\mu(x^4,x^4)=\mu(x^2,x^4)+\mu(x,x^4)$ and both sides of this equation are equal to 0. Assume $h=x^3$, then $\mu(x^3,x^2)+\mu(x^3,x^4)=\mu(x^3,x^3)+\mu(x,x^4)$ and both sides of this equation are equal to 0. Assume $h=x^4$, then $\mu(x^4,x)+\mu(x^4,x^2)=\mu(x^4,x^4)+\mu(x^3,x^2)$ and both sides of this equation are equal to 0. Since $\alpha\neq 0$, we have that, $(x^3,a)\cdot(x^2,a)(x^2,a)\neq(x3,a)(x^2,a)\cdot(x^2,a)$. Also $(x^2,a)\cdot(x,a)(x^3,a)\neq(x,3a+\alpha)=(x^2,a)(x,a)\cdot(x^3,a)$. Thus (G,A,μ) is non-alternative and hence non-associative WIPL. Also neither $(x,a),(x^2,a),(x^3,a)\in N$ for all $a\in A$. Similarly $(x^4,a)\notin A$. Also we have that $(1,a)((h,b)(g,c))=((1,a)(h,b))(g,c)$ for all $h,g\in G$ and $a,b,c\in A$. Which implies that $(1,a)$ belongs to the nucleus. Thus $\{(1,a);$ $a\in A\}$ is the nucleus of the loop (G,A,μ). □

Example 30. *The smallest group A satisfying the assumption of Proposition 7 is the cyclic group $\{0,1,2\}$ of order 3. The construction of Proposition 7 with $\alpha = 1$ then yields the following non-alternative commutative WIPL of order 10.*

$\cdot$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	7	6	9	8
2	2	3	4	5	7	6	8	9	0	1
3	3	2	5	4	6	7	9	8	1	0
4	4	5	7	6	9	8	0	1	2	3
5	5	4	6	7	8	9	1	0	3	2
6	6	7	8	9	0	1	2	3	4	5
7	7	6	9	8	1	0	3	2	5	4
8	8	9	0	1	2	3	4	5	6	7
9	9	8	1	0	3	2	5	4	7	6

GAP shows that the following properties do not hold in the above Cayley table of WIPL.

(1) automorphic inverse property (2) anti-automorphic inverse property (3) LC (4) RC (5) left Bol (6) right Bol (7) Moufang (8) power alternative (9) power associative (10) left nuclear square (13) right nuclear square (14) left inverse and (15) right inverse property.

6.3 Counting AAIP Loops and Some Subclasses of NAFILs

Counting of algebraic structures is difficult as well as important. Difficult because it requires a suitable choice of softwares, some programming and logical skills and fast computer systems. The use of suitable software can make your task easy. Different softwares have different behavior for different tasks. Important because the mathematicians can then draw several conclusions about the structure from the counting. They can use the counting for making conjectures and for counterexamples and for several other purposes.

This section has five subsections. In subsection 1 we discuss the counting of general NAFILs of order $n = 5, 6, 7$ and also commutative NAFILs up to order $n = 9$. In subsection 2 we discuss the counting of its subclass general NAFIL CIP loops up to order $n = 13$ and the counting of its subclass general NAFIL AIP

loops up to order $n = 8$ is in subsection 3. The counting of AAIP loops up to order $n = 9$ has been done in subsection 4. In the subsection 5 of this section we provide an infinite family of non-associative non-commutative AAIP loops via extension of loop whose smallest member is a loop of order 12. Examples of the smallest non-associative commutative and non-commutative loop of each class of counted loops are also given wherever needed.

6.3.1 Re-enumeration of NAFILs

According to [14], Cowagas has started the counting of NAFILs in 1998 with the help of a pascal program called ICONSTRUCT and was able only to find NAFILs of order $n = 5, 6$. But it took a lot of his time. Then with the cooperation of Zhang and using other two other softwares SEM and SATO, they counted NAFILs of order $n = 7$. They used a supercomputer of 48 pentium II 400 processors for the purpose. They finished with all the checkings in three days. We instead used the finite domain enumerator FINDER [63] for enumeration. It easily enumerated NAFILs of order $n = 5, 6, 7$ within a minute on ordinary desktop computer. By doing so we also confirmed the previous counting to be correct. The counting is listed in the following table.

Order	NAFILs
5	1
6	33
7	2333

The efficiency of FINDER is notable. FINDER has been used in counting previously e.g. for counting IP loops in [2] and [64]. Our symmetry breaking is the same as used in [2] except $x^{-1} = x \Leftrightarrow x = e$. Because this is the special property of IP loops of odd order.

The smallest non-commutative NAFIL is of order 5:

·	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	0	1	3
3	3	2	4	0	1
4	4	3	1	2	0

The smallest commutative NAFIL is of order 6:

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

As for order 8 and onward the number of NAFILs become too big to be counted. Though a certain NAFIL of order 8 can be found. So we will have to focus on the subclasses of NAFILs.

In [13] it has been proved that there exists at least one NAFIL of every finite order $n \geq 5$.

Next we enumerate commutative NAFILs up to order 9. FINDER determined them within ten minutes. The following table shows their counting.

Order	Commutative NAFILs
5	0
6	7
7	16
8	2262
9	30581

6.3.2 Enumerating NAFIL CIP Loops

CIP loops are special automorphic inverse property loops see R. Artzy [4]. R. Artzy [5] proved that isotopes of CIP loops are not necessarily CIP. It is also shown in that paper that isotopes of CIP loops are isomorphic. Holomorph of CIP loops has been considered in [67]. Crossed inverse quasigroups have applications in cryptography [31].Next we enumerate the number of non-isomorphic NAFIL CIP loops having order up to 13. The counting is given in the following table.

Order	NAFIL CIP loops
1	0
2	0
3	0
4	0
5	1
6	0
7	0
8	6
9	2
10	47
11	≥ 246
12	≥ 2314
13	≥ 9009

The smallest non-commutative NAFIL CIP loop is of order 8:

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

The smallest commutative NAFIL CIP loop is of order 10:

·	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	8	9	6	7
2	2	3	1	0	6	8	9	5	7	4
3	3	2	0	1	9	7	4	8	5	6
4	4	5	6	9	1	0	7	3	2	8
5	5	4	8	7	0	1	2	6	9	3
6	6	8	9	4	7	2	5	0	3	1
7	7	9	5	8	3	6	0	4	1	2
8	8	6	7	5	2	9	3	1	4	0
9	9	7	4	6	8	3	1	2	0	5

Commutative CIP loops coincide with IP loops. FINDER took one hour to enumerate NAFIL CIP loops up to order 13 on a little bit speedy computer. For order 14, there is a huge number of NAFIL CIP loops. So it requires huge computer memory and a great amount of time. So FINDER is unable to count that.

Since the counting of IP loops has been checked by Mace4 and since we have used the same program and the same symmetry breaking (except the given one above) provided us by John Slaney, so we do not have to use Mace4 again to re-check the counting.

6.3.3 Enumerating NAFIL Automorphic Inverse Property (AIP) Loops

Next we enumerate AIP loops. We are able to enumerate them all up to order 8. Since after this order the number of AIP loops becomes so huge which is difficult and much time consuming for FINDER.

Order	NAFIL AIP loops
5	1
6	13
7	21
8	11144

The smallest commutative NAFIL AIP loop is of order 6:

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

Remark 8. *The smallest non-commutative non-associative NAFIL of order 5 is AIP.*

6.3.4 Enumerating Anti-automorphic Inverse Property(AAIP) Loops

Next we enumerate AAIP loops. We are able to enumerate them all up to order 9. Since after this order the number of AAIP loops becomes so huge which is difficult and much time consuming for FINDER.

Order	Non-group AAIP loops	Group AAIP loops
6	6	2
7	11	1
8	704	5
9	16473	2

The smallest non-commutative non-associative AAIP loop is of order 6:

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

and the smallest commutative non-associative AAIP loop is also of order 6:

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

Symmetry breaking: We have used the same symmetry breaking which had been used for enumeration of IP loops in [2] and [64] with only one change, that is, eliminating $x^{-1} = x \Leftrightarrow x = e$ because this is the speciality of IP loops.

Thus our basic symmetry breakers are:

$e \leq x$

$x^{-1} < (x + 2)$

$(x^{-1} = x \wedge x < y) \Rightarrow y^{-1} = y.$

For odd values of N :

$x^{-1} < (x + 2)$

$f(1) < (e + 4)$

$(x > 1 \wedge 2x < N) \Rightarrow f(x) < (e + 2x)$

For even values of N :

$f(1) = e$

$(-FLAG \wedge 0 < x < N = 2) \Rightarrow f(x) < (e + 2x + 1)$

$(FLAG) \Rightarrow (e + 5)^{-1} = (e + 5)$

$(FLAG \wedge x > 1 \wedge (e + x)^{-1} = (e + x)) \Rightarrow (f(x)^{-1}) \neq f(x)$

$(FLAG \wedge 1 < x < y \wedge (e + y)^{-1} = (e + y)) \Rightarrow f(x) < f(y)$

where $0 < x < N$ and e denotes the min element.

One of the aim of this chapter is to report all the above enumerations. Since these were obtained by exhaustive enumeration, they are available for inspection. Anybody wants these enumerations can get them by an e-mail request to us.

6.3.5 Construction of Non-commutative and Non-associative AAIP Loops Via Extension of Loops

We now construct an infinite family of non-associative AAIP loops via extension of loop whose smallest member is a loop of order 12. We adopt the same procedure as done for the construction of non-associative and non-commutative C-loops in [53]. Note that in [53] Klien group is used for the construction of C-loops but we did not succeed with Klien group. However we got it by using C_4. For further details about the mentioned construction please read Subsection 6.2.2.

Lemma 8. *Let $\mu : G \times G \to A$ be a factor set. Then (G, A, μ) is an AAIP loop iff*

$$\mu(g,h) + \mu(gh, h^{-1}g^{-1}) = \mu(h,h^{-1}) + \mu(g,g^{-1}) - \mu(h^{-1},g^{-1}) \text{ for every } g,h \in G. \tag{B}$$

Proof. The loop (G, A, μ) is a AAIP loop iff

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

holds for every $g, h \in G$ and every $a, b \in A$. Here

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

Straight forward calculation with equation (A) shows that this happens iff equation (B) is satisfied. We call a factor set μ satisfying equation (B) an A-factor set. We now use a particular A-factor set to construct the above mentioned family of anti-automorphic inverse property loops. □

Proposition 8. *Let $n > 2$ be an integer. Let A be an abelian group of order n, and $\alpha \in A$ an element of order bigger than 2. Let $G = C_4 = \{1, u, v, w\}$ be the cyclic group of order 4 with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(x,y) = \begin{cases} \alpha, if (x,y) = (u,v),(w,v), \\ -\alpha, if (x,y) = (v,u),(v,w), \\ \quad = 0, \text{ otherwise} \end{cases}$$

then (G, A, μ) is a non-flexible AAIP loop with nucleus $N = \{(1,a) : a \in A\}$.

Proof. The map μ is clearly an anti-automorphic inverse property-factor set. It can be depicted as follows

$\cdot$	1	u	v	w
1	0	0	0	0
u	0	0	α	0
v	0	$-\alpha$	0	$-\alpha$
w	0	0	α	0

The Cayley table of the $G = C_4 = \{1, u, v, w\}$ is

$\cdot$	1	u	v	w
1	1	u	v	w
u	u	v	w	1
v	v	w	1	u
w	w	1	u	v

To show that (G, A, μ) is a AAIP loop, we verify (B). Since μ is a factor set, there is nothing to prove when $g = 1$. Assume that $g = u$ then (B) becomes $\mu(u, h) + \mu(uh, h^{-1}w) = \mu(h, h^{-1}) + \mu(u, w) - \mu(h^{-1}, w)$. Then both sides of this equation are equal to 0 when $h = 1, u, w$ and equal to α when $h = v$. Assume that $g = v$ then (B) becomes $\mu(v, h) + \mu(vh, h^{-1}v) = \mu(h, h^{-1}) + \mu(v, v) - \mu(h^{-1}, v)$. Then both sides of this equation are equal to 0 when $h = 1, v$ and equal to $-\alpha$ when $h = u, w$. Assume that $g = w$ then (B) becomes $\mu(w, h) + \mu(wh, h^{-1}u) = \mu(h, h^{-1}) + \mu(w, u) - \mu(h^{-1}, u)$. Then both sides of this equation are equal to 0 when $h = 1, u, w$ and equal to α when $h = v$. Since $\alpha \neq 0$, and we have that, $(u, a)(v, a) \cdot (u, a) = (1, 3a + \alpha) \neq (1, 3a - \alpha) = (u, a) \cdot (v, a)(u, a)$ and thus (G, A, μ) is non-flexible and hence non-associative AAIP loop. From definition of μ it is clear that (G, A, μ) is non-commutative. Also we have that $(u, a), (v, a) \notin N$ for all $a \in A$. Similarly $(w, a) \notin N$ for all $a \in A$. Also we have that $(1, a)((h, b)(g, c)) = ((1, a)(h, b))(g, c)$ for all $h, g \in G$ and $a, b, c \in A$. Which implies that $(1, a)$ belongs to the nucleus. Thus $\{(1, a);\ a \in A\}$ is the nucleus of the loop (G, A, μ). □

Corollary 21. *For any integer n there is a non-associative non-commutative AAIP loop with nucleus of size n.*

Proof. By Proposition 8 there is a non-associative non-commutative AAIP loop with nucleus of size $n > 2$. Now it remains to show that there is a non-associative non-commutative AAIP loop with nucleus of size 1 and 2. This is shown in the following examples 31 and 32. □

Example 31. *A non-associative non-commutative AAIP loop with nucleus of size 1.*

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

Example 32. *A non-associative non-commutative AAIP loop with nucleus of size 2.*

·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	6	7	4	5
2	2	3	1	0	5	4	7	6
3	3	2	0	1	7	6	5	4
4	4	6	7	5	2	0	3	1
5	5	7	6	4	0	3	1	2
6	6	4	5	7	3	1	2	0
7	7	5	4	6	1	2	0	3

Remark 9. *There is no non-associative non-commutative AAIP loop of order 7 with nucleus of size 2.*

Example 33. *The smallest group A satisfying the assumption of Proposition 8 is the 3-element cyclic group $\{0, 1, 2\}$. The construction of Proposition 8 with $\alpha = 1$ then gives rise to the following non-associative non-commutative AAIP loop of order 12.*

·	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	0	4	5	3	7	8	6	10	11	9
2	2	0	1	5	3	4	8	6	7	11	9	10
3	3	4	5	6	7	8	11	9	10	0	1	2
4	4	5	3	7	8	6	9	10	11	1	2	0
5	5	3	4	8	6	7	10	11	9	2	0	1
6	6	7	8	10	11	9	0	1	2	4	5	3
7	7	8	6	11	9	10	1	2	0	5	3	4
8	8	6	7	9	10	11	2	0	1	3	4	5
9	9	10	11	0	1	2	5	3	4	6	7	8
10	10	11	9	1	2	0	3	4	5	7	8	6
11	11	9	10	2	0	1	4	5	3	8	6	7

Bibliography

Bibliography

[1] A. A. Albert. Quasigroups. II. *Transactions of the American Mathematical Society*, 55:401–409, 1944.

[2] A. Ali and J. Slaney. Counting loops with the inverse property. *Quasigroups and related Structures*, 16:13–16, 2008.

[3] V. L. Arlazarov, A. M. Baraev, Y. Y. Golfand, and I. A. F. zev. Construction with the aid of a computer of all latin squares of order 8. *Algorithmic investigations in combinatorics*, 187:129–141, 1978.

[4] R. Artzy. Crossed inverse and related loops. *Trans. Amer. Math. Soc*, 91-3:480–492, 1959.

[5] R. Artzy. Relations between loops identities. *Proc. Amer. Math. Soc*, 11-6:847–851, 1960.

[6] S. E. Bammel and J. Rothstein. The number of 9×9 latin squares. *Discrete Mathematics*, 11:83–95, 1975.

[7] G. Boole. *The mathematical analysis of logic, being an essay toward a calculus of deductive reasoning.* Cambridge, 1847.

[8] L. J. Brant and G. L. Mullen. A note on isomorphism classes of reduced latin squares of order 7. *Utilitas Mathematica*, 27:261–263, 1985.

[9] J. W. Brown. Enumeration of latin squares with application to order 8. *Journal of combinatorial theory*, 5:177–184, 1972.

[10] R. H. Bruck. Contributions to the theory of loops. *Trans. Amer. Soc*, 55:245–354, 1944.

[11] R. H. Bruck. *A survey of binary systems.* Springer-Verlag, 1971.

[12] R. H. Bruck and L. J. Paige. Loops whose inner mappings are automorphisms. *Ann. of Math.*, (2)63:308–323, 1956.

[13] R. E. Cawagas. Introduction to: non-associative finite invertible loops. *to appear (PUPJST).*

[14] R. E. Cawagas. Generation of NAFIL loops of small order. *Quasigroups and related Structures*, 7:1–5, 2000.

[15] A. Cayley. On latin squares. *Oxford Camb. Dublin Messenger of Math.*, 19:85–239, 1890.

[16] L. H. Chin and A. Tarski. Distributive and modular laws in the arithmetic of relation algebras. *J. Assoc. Comput. Mach.*, 24:44–67, 1977.

[17] C. J. Colbourn and J. H. D. (eds.). *The CRC Handbook of Combinatorial Designs. CRC Press series on Discrete Mathematics and its Applications.* CRC Press, 1996.

[18] S. D. Comer. Combinatorial aspects of relations. *Algebra Universalis*, 18:77–94, 1984.

[19] A. C. D. A. Randell and Z. Cui. Computing transitivity tables: A challenge for automated theorem provers. In *Proceedings of CADE 11*, pages 786–790, 1992.

[20] R. Dechter. *Constraint Processing.* Morgan Kaufmann, 2003.

[21] J. Dénes and A. D. Keedwell. *Latin squares and their applications.* Academic Press, 1974.

[22] I. Düntsch. Relation algebras and their application in temporal and spatial reasoning. *Artificial Intelligence Review*, 23:315–357, 2005.

[23] I. Düntsch, H. Wang, and H. McCloskey. A relation - algebraic approach to the region connection calculus. *Theoretical Computer Science*, 255:63–83, 2001.

[24] L. Euler. Recherches sur une nouvelle espéce de quarrés magiques combinatorial aspects of relations. *Verhandelingen / uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen*, 9:85–239, 1782.

[25] R. A. Fisher and F. Yates. The 6 × 6 latin squares. *Proc. of Cambridge Philos. Soc.*, 30:492–507, 1934.

[26] M. Frolov. Sur les permutations carrées. *J. de Math. spéc*, IV:8–11, 25–30, 1890.

[27] M. Fujita, J. Slaney, and F. Bennett. Automatic generation of some results in finite algebra. In *Proceedings of the 13th International Joint Conference on Artificial Intelligence*, pages 52–57, 1993.

[28] P. Guérin, 2001.

[29] S. M. Jacob. The enumeration of the latin rectangle of depth three by means of a formula of reduction, with other theorems relating to non-clashing substitutions and latin squares. *Proc. London Math. Soc.*, 31:329–354, 1930.

[30] T. G. Jaiyeola and J. O. Adeniran. On central loops and central square property. *Available at arXive.*

[31] T. G. Jaiyeola and J. O. Adeniran. A double cryptography using the keedwell cross inverse quasigroup. *International Journal of Mathematical Combinatorics*, 3:28–33, 2008.

[32] P. Jipsen, R. L. Kramer, and R. D. Maddux. total tense algebras and symmetric semiassociative relation algebras. *Algebra Universalis*, 34:404–423, 1995.

[33] B. Jónsson and A. tarski. Boolean algebras with operators I. *Amer. J. Math.*, 73:891–939, 1951.

[34] B. Jónsson and A. Tarski. Boolean algebras with operators II. *Amer. J. Math.*, 74:127–162, 1952.

[35] G. Kolesova, C. W. H. Lam, and L. Thiel. On the number of 8 × 8 latin squares. *J. Combin. Theory Ser. A*, 54:143–148, 1990.

[36] R. C. Lyndon. Relation algebras and projective geometries. *J. Michigan Math.*, 8:21–28, 1961.

[37] P. A. Macmahon. *Combinatory Analysis.* Cambridge, 1915.

[38] R. Maddux. *Topics in Relation Algebras.* Ph.D thesis.

[39] R. Maddux. Some varieties containing relation algebras. *Transactions of the American Mathematical Society*, 272:501–526, 1982.

[40] R. Maddux. Necessary subalgebras of simple nonintegral semiassociative relation algebras. *Algebra Universalis*, 27(4):544–558, 1990.

[41] R. Maddux. The origin of relation algebras in the development and axiomatization of the calculus of relations. *Studia Logica*, 50:421–456, 1991.

[42] R. Maddux. *Relation Algebras*, volume 150. Elsevier, 2006.

[43] W. W. McCune. *Prover9 Manual and Examples*. University of New Mexico, 2006. http://www.cs.unm.edu/ mccune/prover9/manual-examples.html.

[44] B. D. McKay, A. Meynert, and W. Myrvold. Small latin squares, quasigroups and loops. *Journal of Combinatorial Designs*, 15:98–119, 2007.

[45] B. D. McKay and E. Rogoyski. Latin squares of order 10. *Electron. J. Combin.*, 2, 1995.

[46] B. D. McKay and I. M. Wanless. On the number of latin squares. *Ann. Combin.*, 9:335–344, 2005.

[47] J. D. Monk. Nonfinitizability of classes of representable cylindric algebras. *The Journal of Symbolic Logic*, 34:331–343, 1969.

[48] G. P. Nagy and P. Vojtěchovský. Loops: Computing with quasigroups and loops in GAP, version 1.0.0, computational package for GAP. *http://www.math.du.edu/loop*.

[49] M. Niemenmaa and T. Kepka. On multiplication groups of loops. *J. Algebra*, 135:233–236, 1990.

[50] H. W. Norton. The 7 × 7 squares. *Ann. Eugenics*, 9:269–307, 1939.

[51] J. M. Osborn. Loops with the weak inverse property. *Pac. J.Math*, 10:295–304, 1961.

[52] H. O. Pflugfelder. *Quasigroups and Loops: Introduction*, volume Sigma Series in Pure Math. 8. Heldermann-Verlag, 1990.

[53] J. D. Phillips and P. Vojtěchovský. C-loops: an introduction. *Publicationes Mathematicae Debrecen*, 68/1-2:115–137, 2006.

[54] D. A. Preece. Classifying Youden rectangles. *J. Royal Stat. Soc. Series B (Meth.)*, 28:118–130, 1966.

[55] Q. (pseudonym). Anonymous electronic posting to Loopforum, October 2001. http://groups.yahoo.com/group/loopforum/.

[56] V. S. Ramamurthi and A. R. T. Solarin. On finite right central loops. *Publ. Math.Debrecen*, 35:260–264, 1988.

[57] J. Renz and G. Ligozat. Weak composition for qualitative spatial and temporal reasoning. *Lecture Notes in Computer Science*, 3709:534–548, 2005.

[58] A. Sade. Enuméation des carrés latins. Application au 7^e order. conjectures pour les orders supérieurs. *privately published*, page 8pp, 1948.

[59] A. Sade. An omission in Norton's list of 7×7 squares. *Ann. Math. Stat.*, 22:306–307, 1951.

[60] A. Sade. Morphismes de quasigroupes: Tables. *Revista da Faculdade de Ciências de Lisboa, 2: A - Ciências Matemáticas*, 13:149–172, 1970/71.

[61] P. N. Saxena. A simplified method of enumerating latin squares by Macmahon's differential operators; ii. the 7×7 latin squares. *J. Indian Soc. Agric. Statistics*, 3:24–79, 1951.

[62] E. Schönhardt. Über lateinische Quadrate und Unionen. *Journal für die reine und angewandte Mathematik*, 163:183–230, 1930.

[63] J. Slaney. FINDER: Finite domain enumerator, system description. In *Proceedings of the 12th Conference on Automated Deduction*, pages 798–801, 1994.

[64] J. Slaney and A. Ali. Generating loops with the inverse property. *Sutcliffe G., Colton S., Schulz S. (eds.); Proceedings of ESARM*, 55:55–66, 2008.

[65] G. Tarry. Le probléme des 36 officiers. *Ass. Franc. Paris*, 29:170–203, 1900.

[66] A. Tarski. On the calculus of relations. *Journal of Symbolic Logic*, 6:73–89, 1941.

[67] G. Temitope and T. G. Jaiyeola. An holomorph study of Smarandache automorphic and cross inverse property loops. *Scientia Magna Journal*, 4:1:102–108, 2008.

[68] M. B. Wells. The number of latin squares of order eight. *J. Combinatorial Theory*, 3:98–99, 1967.