Computational analysis of flexible loops

By

Ikram Ullah

Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN

2010

Computational analysis of flexible loops

By

Ikram Ullah

Supervised

By

DR. ASIF ALI

Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN

2010

Computational analysis of flexible loops

By

Ikram Ullah

MASTER OF PHILOSOPHY

IN

MATHEMATICS

Supervised

By

DR. ASIF ALI

Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN

2010

Computational analysis of flexible loops

By

IKRAM ULLAH

CERTIFICATE

A DISSERTATION SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF THE MASTER OF PHILOSOPHY

We accept this dissertation as conforming to the required standard

1. ______________________
Prof Dr. Muhammad Ayub
(Chairman)

2. ______________________
Dr. Asif Ali
(Supervisor)

3. ______________________
Dr. Rauf-e-Azam
(External Examiner)

Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN
2010

Dedicated

To

Father & Mother

Who are the most precious gems
of my life.
Who've always given me perpetual love,
care, and cheers. Whose prayers have
always been a source of great
inspiration for me and whose
sustained hope in me led me
to where I stand today.

&

Then to my lovely brothers and sister
whose
love, care is unmatchable
and simply priceless for me.

PREFACE

The problem of counting of loops is difficult one, however many mathematicians counted the loops of certain order. In paper [8] John Slaney and Asif Ali has used better techniques with the help of FINDER to generate, enumerate and determine the inverse property loops up to the order of 13, and also commutative IP loops of order 14. Similarly Cawagas has used a program to count the NAFILs, but this program failed to count the NAFILs of order 7. So he forwarded his problem to professor Hantao Zhang, the latter after examining the problem, he discovered the order with the help of two softwares SEM and SATO.

J. D. Philips and Petr Vojtechovsky have given a construction of an infinite family of C-loops in their paper [7]. Following their method we gave the construction of an infinite family of flexible loops. However our main work is about the counting of certain kind of loops that is flexible loops.

This dissertation comprises three chapters. In chapter 1 there are three sections. In first section there is introduction, in second section there is quasigroups and loops, while the third section contains different kinds of loops with examples. In second chapter there are two sections. First section consists of introduction, construction of C-loop and some basic results proved about the flexible loops related to our work. In the second section some implications are given which are useful in our thesis. The third chapter consists of four sections. In section 1 introduction, history of the counting of loops and the counting of flexible loops up to order 9 are discussed. In section 2 the construction of flexible loop is given and it is proved that the loop constructed in such a way is also an IP loop and Jordon loop. In section 3 it is proved that if a loop is an ARIF loop such that it is right nuclear square loop (left nuclear square loop) then it is RC-loop (LC-loop). It is also proved that if a loop is an ARIF loop such that it is middle nuclear square loop then it is C-loop. In section 4 we proved that ARIF loop satisfies the squaring property if it is commutative and also we proved that every ARIF loop satisfies the Jordon identity and become Jordon loop if it is commutative.

Ikram Ullah
January 2010

Acknowledgement

All praises to almighty Allah, the most beneficent and most merciful, who created this universe and gave us the idea to discover. I am highly grateful to Almighty Allah for His blessing, guidance and help in each and every step of my life. He blessed us with the ***Holy Prophet Muhammad*** *(PBUH), who is forever source of guidance and knowledge for humanity.*

I cannot fully express my gratitude to my supervisor ***Dr. Asif Ali*** *for his cooperation, valuable instructions, beneficial remarks and superb guidance. He showed me the right way for doing research. His sympathetic attitude and encouragement broadened my vision of the subject, my knowledge and also increased my capabilities of research and hard work.*

I am also thankful to the Chairman, Department of Mathematics, Prof. ***Dr. Muhammad Ayub*** *for providing necessary facilities to complete my thesis.*

I am especially thankful to Mr. ***Muhammad Shah*** *(Ph.D. Scholar) for their concern and co-operation during the completion of my research work. I am also thankful to friends (Yousaf, Imran) whose cooperation makes me to complete my research work.*

Words cannot express my feeling of loves and thanks for my parents, sister and brothers (Inam Ullah, Sifat Ullah and Shafi Ullah) whose love, care and humble prayers left no stone unturned in arranging for my needs and educational requirement

May Almighty Allah shower His choicest blessing and prosperity on all those who assisted me in any way during completion of my thesis.

Ikram Ullah

Contents

Chapter 1

Preliminaries

1.1 Introduction

This chapter consists of basic concepts of quasigroups and loops. Although the whole subject could not be reviewed, nontheless important and necessary topics being helpful in the forthcoming literature are included.

1.2 Quasigroups and loops

According to the Hausmann and Ore a set G is defined to be *groupiod* relative to the operation $(\cdot)$ iff, to every ordered pair (a, b) of elements of G, there corresponds a uniquely defined element $a{\cdot}b$ of G. If f is any fixed element of a groupiod $G\,(\cdot)$ we may defined two single-valued mappings L_f, R_f of G into itself by

$$(a)\,L_f = f \cdot a \text{ , and } (a)\,R_f = a \cdot f \tag{1.1}$$

where (1.1) is to hold for all a of G. An element 1 of a groupiod $G\,(\cdot)$ is said to be a unit of $G\,(\cdot)$ if for every a of G,

$$a \cdot 1 = 1 \cdot a = a.$$

If e is also a unit then

$$e = e \cdot 1 = 1$$

and hence a unit, if it exists, is unique. An element f of $G\,(\cdot)$ is said to be *left nonsingular* if L_f is a permutation of G and similarly an element f of $G(\cdot)$ is said to be *right nonsingular* if R_f is a permutation of G.

Quasigroup $(Q, \cdot)$ is defined to be a groupiod in which every element x is nonsingular. Moreover a set Q is a quasigroup if and only if the following two laws are satisfied:

i) To every ordered pair x, y of elements of Q there corresponds a unique element xy of Q, called there product.

ii) If, in the equation $x \cdot y = z$, any two of the symbols x, y, z are assigned as elements of Q, the third is uniquely determined as an element of Q. An example of a quasigroup is given below

$\cdot$	1	2	3	4
1	3	1	4	2
2	4	2	3	1
3	1	4	2	3
4	2	3	1	4

Both left and right cancellative laws hold in quasigroup.

Which makes its multiplication table is a Latin square formally defined, each row and each column being a permutation of its elements.

A quasigroup Q is called *left distributive* if it satisfies $x(yz) = (xy)(xz)$ for all x, y, $z \in Q$ and *right distributive* if $(xy)z = (xz)(yz)$ for all x, y, $z \in Q$.

A *Latin square* of order n is an $n \times n$ array in which n^2 symbols, taken from a set A, are arranged so that each symbol occurs only once in each row and exactly once in each column. The multiplication table of above quasigroup is the example of Latin square.

Loop is a quasigroup with neutral element (identity element). In other words, any quasigroup with neutral element is called loop. Thus we can say that a loop Q obeys (*i*), (*ii*) in the above definition of quasigroup and the following

(*iii*) There exists an element 1 of Q with the property

$$x \cdot 1 = 1 \cdot x = x$$

for every x of Q. A loop Q can have exactly one unit. Moreover if a subset H of Q obeys (*i*),

(ii) with respect to the operation $(\cdot)$ of Q, then it will contain unit 1 of Q. Such kind of subset is called subloop. If a loop Q is associative then it is a group. Thus loops are nonassociative groups. Every group is a loop that is loop is the generalization of group.

The smallest loop is of order 5, whose multiplication table is:

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

1.3 Different types of loops

Any loop L satisfying

$i)$ $x(xy) = (xx)y$, is called *left alternative loop.*

$ii)$ $x(yy) = (xy)y$, is called *right alternative loop.*

$iii)$ $x(yx) = (xy)x$, is called *flexible* loop.

$iv)$ $x(y(xz)) = (x(yz))x$, is called *left Bol loop.*

$v)$ $x((yz)y) = ((xy)z)y$, is called *right Bol loop.*

$vi)$ $(xx)(yz) = (x(xy))z$, is called *LC-loop.*

$vii)$ $x((yz)z) = (xy)(zz)$, is called *RC-loop.*

$viii)$ $(xy)(zx) = (x(yz))x$, is called *Moufang loop.*

$ix)$ $(xx)(yz) = ((xx)y)z$, is called *left nuclear square loop.*

$x)$ $x((yy)z) = (x(yy))z$, is called *middle nuclear square loop.*

$xi)$ $x(y(zz)) = (xy)(zz)$, is called *right nuclear square loop.*

The example of right nuclear square loop is the loop whose multiplication table is given above in the definition of loop. This is the example of such a loop which is left nuclear square loop, middle nuclear square loop, and also right nuclear square loop.

$xii)$ $x(y(yz)) = ((xy)y)z$, is called *C-loop.*

The smallest nonassociative C-loop is:

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

xiii) $x^2(yx) = (x^2y)x$, and also L is commutative, then L is called Jordon loop.
The smallest non-associative *Jordon loop* is

$\cdot$	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

xiii) $xy = yx$, is called *commutative loop*. The multiplication table of commutative loop is:

$\cdot$	e	a	b	c	d	g
e	e	a	b	c	d	g
a	a	e	d	b	g	c
b	b	d	e	g	c	a
c	c	b	g	e	a	d
d	d	g	c	a	e	b
g	g	c	a	d	b	e

xiii) $x(y(zx)) = ((xy)z)x$, is called *extra loop*.

A loop L is said to have the inverse property, and is called an *IP loop*, iff it is a loop with inverse such that for all elements $x, y \in L$

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

It is not hard to see that IP loop also satisfies the principle

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

IP loops are of interest as a strong and natural genralization of both groups and Steiner loops. The smallest IP loop that is not a group is of order 7:

$\cdot$	1	2	3	4	5	6	7
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

A *RIF loop* is an IP loop L with the property that

$$\theta^J = \theta \text{ for all } \theta \in Inn\,(L),$$

where J is a permutation of order 2 and $\theta^J = J^{-1}\theta J$. An *ARIF loop* is a flexible loop satisfying the following

$$\begin{aligned} (a)\ R_x R_{yxy} &= R_{xyx} R_y \\ \text{and } (b)\ L_x L_{yxy} &= L_{xyx} L_y. \end{aligned}$$

Left nucleus of a loop L is the subset of all elements x in L such that $x(yz) = (xy)z$ for every y, z in L. It is denoted by $N_\lambda(L)$.

Consider the loop of order 6, whose multiplication table is:

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

here $N_\lambda(L) = \{0\}$.

Right nucleus is the subset of all elements x in L such that $y(zx) = (yz)x$ for every y, z in L, it is denoted by $N_\varrho(L)$ and *middle nucleus* is the subset of all elements x in L such that $y(xz) = (yx)z$ for every y, z in L, it is denoted by $N_\mu(L)$.

Nucleus of a loop L is the intersection of the left nucleus, middle nucleus and right nucleus of L, it is denoted by $N(L)$. Consider the loop of order 6 given above, we have $N(L) = \{0\}$.

Let $(L, \cdot)$ be a loop, and let x be an element of L. Then the map $L_x : L \to L$ defined by $yL_x = x \cdot y$ is the *left translation* by x. and the map $R_x : L \to L$ defined by $yR_x = y \cdot x$ is the *right translation* by x.

Let $(L, \cdot)$ be a loop. The permutation group $Mlt(L, \cdot)$ generated by all left translations L_x and right translations R_x, where x is an element of L, is called the *multiplication group* of $(L, \cdot)$. Thus $Mlt(L, \cdot)$ be the permutation group consisting of the permutations R_x, R_x^{-1}, L_x, and L_x^{-1} for all x in L, and of all products of a finite number of these. We shall call $Mlt(L, \cdot)$ the group associated with L. Consider a loop L of order 6 with the following multiplication table:

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

here the order of $Mlt(L, \cdot)$ is 24. We can easily find the elements of $Mlt(L, \cdot)$ with the help of GAP (software). The subset of $Mlt(L)$ consisting of all maps fixing the neutral element of L is called the *inner mapping group* of L, and is denoted by $Inn(L)$. Note that

i) $Inn(L)$ be the group generated by the set of all permutations $R_{x,y}$, $M_{x,y}$

where

$$R_{x,y} = R_x R_y R_{xy}^{-1} \text{ and } M_{x,y} = R_y L_x R_{xy}^{-1}.$$

ii) The the set of all permutations

$$L_{x,y} = L_x L_y L_{yx}^{-1} \text{ and } N_{x,y} = L_y R_x L_{yx}^{-1},$$

may also generate the $Inn(L)$.

iii) The set consisting of all permutations $R_{x,y}$, $L_{x,y}$ and $T_x = R_x L_x^{-1}$ is another generating set.

A. Beg defines the *cenral element* of a loop L as follows:

If $(L, \cdot)$ is a loop, then $a \in L$ is called the *central element* of L if $[(xa)\,a]y = x[a\,(ay)]$ for all x, y in L. He further proved that for every central element a of inverse property loop L, a^2 is in the nucleus of L.

Left conjugacy closed loop is a loop with left translations closed under conjugation that is a loop L in which $L_x^{-1}L_yL_x$ is a left translation for every x, y in L, *right conjugacy closed* loop is a loop with right translations closed under conjugation, this means that a loop L in which $R_x^{-1}R_yR_x$ is a right translation for every x, y in L and *conjugacy closed loop* is a loop with left and right translations closed under conjugation, that is a loop L in which $L_x^{-1}L_yL_x$ is a left translation and $R_x^{-1}R_yR_x$ is a right translation for every x, y in L.

An ordered triple (U, V, W) of permutations of the set L is called an *autotopism* of the loop $(L, \cdot)$ if and only if

$$xU \cdot yV = (x \cdot y)\, W \text{ for all } x, y \in L.$$

Remember that the set of all autotopisms of $(L, \cdot)$ forms a group under the composition of multiplication:

$$(U_1, V_1, W_1)\,(U_2, V_2, W_2) = (U_1U_2, V_1V_2, W_1W_2)\,.$$

The unit and inverse elements of the group are (I, I, I) and $(U, V, W)^{-1} = \left(U^{-1}, V^{-1}, W^{-1}\right)$. If L is any loop such that $x \in N_\lambda(L)$ then (L_x, id_L, L_x) is an autotopism.

A permutation P of a set L is said to be *pseudo-automorphism* of the loop $(L, \cdot)$ if and only if there exists an element c of L called a companion of P such that (P, PR_c, PR_c) is an autotopism of $(L, \cdot)$.

If L is any loop such that $x \in N_\rho(L)$ then (id_L, R_x, R_x) is an autotopism and hence id_L is pseudo-automorphism.

Let G be a multiplicative group with neutral element 1, and A be an abelian group written additively with neutral element 0. Any map

$$\mu : G \times G \to A$$

satisfying

$$\mu(1, g) = \mu(g, 1) = 0 \text{ for every } g \in G,$$

is called a *factor set*.

If L is any loop, then $J \in Mlt(L)$ is a permutation such that $xJ = x^{-1}$ that is J is a permutation of order 2.

Chapter 2

Flexible loops

2.1 Introduction

This chapter includes the construction of C-loop with the help of two commutative groups given by J. D. Philips and Petr Vojtechovsky in paper [4] . In this paper they proved that flexible C-loops are ARIF loops. Also some basic results about the flexible loops are proved in this chapter. There are also some implications and results are given which are useful in our work.

Theorem 1 *Let $\mu : G \times G \to A$ be a factor set. Then (G, A, μ) is a C-loop if and only if*

$$\mu(h,k) + \mu(h,hk) + \mu(g,h.hk) = \mu(g,h) + \mu(gh,h) + \mu(gh.h,k)$$

for every $g,\ h,\ k \in G$.

Proof. Since any loop L is C-loop if and only if

$$x(y(yz)) = ((xy)y)z \text{ for all } x,\ y \in L.$$

So (G, A, μ) is a C-loop if and only if

$$\begin{aligned}
(g,a)\left((h,b)\cdot(h,b)(k,c)\right) &= \left((g,a)(h,b)\cdot(h,b)\right)(k,c)\\
&\Leftrightarrow (g,a)\left((h,b)\cdot(hk, b+c+\mu(h,k))\right)\\
&= \left((gh, a+b+\mu(g,h))\cdot(h,b)\right)(k,c)\\
&\Leftrightarrow (g,a)\left(h\cdot hk, b+b+c+\mu(h,k)+\mu(h,hk)\right)\\
&= \left(gh\cdot h, a+b+\mu(g,h)+b+\mu(gh,h)\right)(k,c)\\
&\Leftrightarrow \left(g\left(h\cdot hk\right), a+b+b+c+\mu(h,k)+\mu(h,hk)+\mu(g,h.hk)\right)\\
&= \left(\left(gh\cdot h\right)k, a+b+\mu(g,h)+b+\mu(gh,h)+c+\mu(gh.h,k)\right)\\
&\Leftrightarrow \mu(h,k)+\mu(h,hk)+\mu(g,h.hk)\\
&= \mu(g,h)+\mu(gh,h)+\mu(gh.h,k)
\end{aligned}$$

Hence the result follows. ∎

Proposition 2 *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 $G = \{1,\ u,\ v,\ w\}$ be the Klein group with neutral element 1. Define*

$$\mu : G \times G \to A$$

by

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

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

Example 3 *The smallest noncommutatuve nonassociatice C-loop, which satisfies the above*

Proposition 2 is given by

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

Corollary 4 *For any integer $n > 1$ there is a nonassociative noncommutative C-loop with nucleus of size n.*

Lemma 5 *In flexible loops inverses are unique.*

Proof. Let x^{λ} be the left inverse of x and x^{ρ} be the right inverse of x, then

$$
\begin{aligned}
x^{\lambda}x &= e \text{ and } xx^{\rho} = e \\
&\Rightarrow x\left(x^{\lambda}x\right) = xe \text{ and } \left(xx^{\rho}\right)x = ex \\
&\Rightarrow x\left(x^{\lambda}x\right) = x \text{ and } \left(xx^{\rho}\right)x = x \\
&\Rightarrow x\left(x^{\lambda}x\right) = \left(xx^{\rho}\right)x \\
&\Rightarrow x\left(x^{\lambda}x\right) = x\left(x^{\rho}x\right) \text{ as } L \text{ is flexible} \\
&\Rightarrow x^{\lambda}x = x^{\rho}x \text{ as } L \text{ is cancellative} \\
&\Rightarrow x^{\lambda} = x^{\rho} \text{ as } L \text{ is cancellative}
\end{aligned}
$$

Thus the result follows. ■

Lemma 6 *Every commutative loop L is flexible.*

Proof. Since L is commutative, so

$$\begin{aligned} xy &= yx \\ &\Rightarrow (xy)\,x = x\,(xy) \\ &\Rightarrow (xy)\,x = x\,(yx)\,. \end{aligned}$$

This implies that L is flexible. ■

Lemma 7 *Every ARIF loop is alternative loop.*

Proof. Let L be an ARIF loop, then by definition

$$R_x R_{yxy} = R_{xyx} R_y$$

replacing x by e, we have

$$\begin{aligned} R_e R_{y^2} &= R_y R_y \\ &\Rightarrow R_{y^2} = R_y R_y \\ &\Rightarrow (x)\,R_{y^2} = (x)\,R_y R_y \\ &\Rightarrow (x)\,y^2 = (xy)\,y \\ &\Rightarrow x\,(yy) = (xy)\,y \end{aligned}$$

which implies that L is right alternative, similarly from definition the left alternativity of L follows. Hence every ARIF loop is alternative. ■

Theorem 8 *Every C-loop is nuclear square loop.*

Proof. Let L be a C-loop, then by definition we can write

$$x\,(y\,(yz)) = ((xy)\,y)\,z \text{ for all } x,\ y, z \in L.$$

But we know that every C-loop is alternative, so

$$\begin{aligned} x\left(y^2 z\right) &= \left(xy^2\right) z \\ &\Rightarrow y^2 \in N\left(L\right). \end{aligned}$$

But in C-loop

$$N\left(L\right) = N_{\varrho}\left(L\right) = N_{\mu}\left(L\right) = N_{\lambda}\left(L\right)$$

which implies that L is left, right, and middle nuclear square loop and hence L is nuclear square loop. ■

Lemma 9 *If L is an IP loop and R_x, $L_x \in Mlt(L)$, then $R_x^J = L_{x^{-1}}$ and $L_x^J = R_{x^{-1}}$.*

Proof. Consider

$$\begin{aligned} (y)\, R_x^J &= (y)\, J^{-1} R_x J = (y)\, J R_x J \\ &= \left(y^{-1}\right) R_x J = \left(y^{-1}x\right) J \\ &= \left(y^{-1}x\right)^{-1} = x^{-1}\left(y^{-1}\right)^{-1} \\ &= x^{-1}y = (y)\, L_{x^{-1}} \\ &\Rightarrow R_x^J = L_{x^{-1}} \end{aligned}$$

Similarly we can prove that $L_x^J = R_{x^{-1}}$. ■

Lemma 10 *Every ARIF loop is flexible.*

Lemma 11 *Every RIF loop is an ARIF loop.*

Lemma 12 *The following are equivalent for an IP loop L:*

i) L is a RIF loop.

ii) L is flexible and $R_{x,y} = L_{x^{-1},y^{-1}}$ for all $x, y \in L$.

iii) $R_{xy}L_{xy} = L_y L_x R_x R_y$ for all $x, y \in L$.

iv) $R_{xy}L_{xy} = R_x R_y L_y L_x$ for all $x, y \in L$.

Lemma 13 *Every power alternative loop is alternative.*

Lemma 14 *Let L be a commutative, alternative, inverse property loop. Then L satisfying the squaring property.*

Theorem 15 *An element a of an IP loop L is a central iff* $a^2 \in N(L)$.

Lemma 16 *Let L be a loop and a its element. Then:*

i) $a \in N_\lambda(L) \Leftrightarrow (L_a, id_L, L_a)$ is an autotopism,

ii) $a \in N_\varrho(L) \Leftrightarrow (id_L, R_a, R_a)$ is an autotopism, and

iii) $a \in N_\mu(L) \Leftrightarrow \left(R_a^{-1}, L_a, id_L\right)$ is an autotopism.

Proposition 17 *A loop L is CCL iff both of the triples* (T_x, L_x, L_x) *and* $\left(R_x, T_x^{-1}, R_x\right)$ *are autotopisms, for* $x \in L$.

Theorem 18 *Any loop L is moufang loop iff* $(L_x, R_x, L_x R_x)$ *is autotopism for each* $x \in L$.

Theorem 19 *For a loop* $(L, \cdot)$ *the following identities are equivalent:*

i) $(xy \cdot z)\, x = x\, (y \cdot zx)$,

ii) $yx \cdot xz = (y \cdot xz)\, x$,

iii) $xy \cdot xz = x\, (yx \cdot z)$.

Theorem 20 *A loop* $(L, \cdot)$ *is an extra loop iff for all* $x \in L$, $(L, \cdot)$ *satisfies any one of the following (equivalent) conditions:*

i) $\left(L_x, R_x^{-1}, L_x R_x^{-1}\right)$ is an autotopism of $(L, \cdot)$,

ii) $\left(R_x, L_x^{-1} R_x, R_x\right)$ is an autotopism of $(L, \cdot)$,

iii) $\left(R_x^{-1} L_x, L_x, L_x\right)$ is an autotopism of $(L, \cdot)$.

Theorem 21 *Every extra loop* $(L, \cdot)$ *is a Moufang loop.*

Proposition 22 *The following are equivalent on any loop L:*

i) L is right central loop.

ii) L is right alternative and for all $x \in L$, x^2 belongs to the right nucleus of L.

iii) (id_L, R_{x^2}, R_{x^2}) is an autotopism of L.

iv) If A, B belong to $R(L)$ then AB^2 also belongs to $R(L)$.

v) $L_x R_{y^2} = R_{y^2} L_x$ for all x, y in L.

Theorem 23 *All IP loops are antiautomorphic.*

Theorem 24 *Every IP loop is WIP loop.*

Theorem 25 *Every steiner loop is C-loop.*

Theorem 26 *If L is nuclear square loop such that L is moufang loop, then L is extra loop.*

Theorem 27 *Every moufang loop is diassociative.*

Theorem 28 *If L is flexible loop such that L is C-loop, then L is diassociative.*

Theorem 29 *If L is IP loop, then* $N(L) = N_\varrho(L) = N_\mu(L) = N_\lambda(L)$. *Where* $N(L)$,

$N_\varrho(L)$, $N_\mu(L)$, and $N_\lambda(L)$ represents the nucleus, right nucleus, middle nucleus and left nucleus respectively.

Theorem 30 *In IP loops the inverse of left (right) translation is left (right) translation.*

2.2 Implications

1) Diassociative loop $\Rightarrow$ Power alternative loop.

2) Diassociative loop $\Rightarrow$ Flexible loop.

3) Extra loop $\Rightarrow$ Moufangloop.

4) C-loop $\Rightarrow$ RC-loop.

5) C-loop $\Rightarrow$ LC-loop.

6) C-loop and Flexible loop $\Rightarrow$ Diassociative loop.

7) RC-loop and LC-loop $\Rightarrow$ C-loop.

8) LC-loop $\Rightarrow$ Left nuclear square loop.

9) LC-loop $\Rightarrow$ Middle nuclear square loop.

10) RC-loop $\Rightarrow$ Right nuclear square loop.

11) RC-loop $\Rightarrow$ Middle nuclear square loop.

12) Moufangloop $\Rightarrow$ Left Bol loop.

13) Moufangloop $\Rightarrow$ Right Bol loop.

14) Left Bol loop $\Rightarrow$ Left Power alternative loop.

15) Right Bol loop $\Rightarrow$ Right Power alternative loop.

16) Power alternative loop $\Rightarrow$ Alternative loop.

17) Left Bol loop and Right Bol loop $\Rightarrow$ Moufangloop.

18) Left Power alternative loop and commutative loop $\Rightarrow$ Right Power alternative loop.

19) LC-loop and commutative loop $\Rightarrow$ C-loop.

20) LCC loop and commutative loop $\Rightarrow$ RCC loop.

Chapter 3

Counting and construction

3.1 Introduction

This chapter consists of four sections. In Section 1 the introduction and the history of counting of loops is given. The counting of flexible loops up to order 9 is also there in Section 1. In Section 2 the construction of flexible loop is given and it is proved that the loop constructed in such a way is also an IP loop and Jordon loop. In Section 3 it is proved that if a loop is an ARIF loop such that it is right nuclear square loop (left nuclear square loop) then it is RC-loop (LC-loop). It is also proved that if a loop is an ARIF loop such that it is middle nucleare square loop then it is C-loop. In Section 4 we showed that ARIF loop satisfies the squaring property if it is commutative, also we proved that every ARIF loop satisfies the Jordon identity and become Jordon loop if it is commutative.

3.1.1 Definition

A flexible loop is a loop L which satisfies the following identity

$$x\,(yx) = (xy)\,x \text{ for all } x, y \in L.$$

Clearly every group is flexible loop, but not conversely.

We present the number of non-isomorphic flexible loops having order upto 9. These loops are obtained by exhaustive enumeration.

3.1.2 History of loops

The history of counting of loops is very interesting. Many people worked on the counting of different kinds of loops of different order. Also they used various ways for the counting of loops. Raoul E. Cawagas is one of those who developed a program known as ICONSTRUCT, and with the help of this program he generated and determined non-isomorphic finite invertable loops of order $n \leqslant 6$. Cawagas also enumerated the non-isomorphic finite invertable commutative loops of order 7 with the help of this program. Cawagas found only the finite invertable loops of order 6. Where as it was Schonhardt who found in 1930 all kinds of non-isomorphic loops of order 6. After the lapse of 55 years, Brant and Mullen enumerated all kinds of loops of order 7. So in different times loops of different order by different people are found. Till now loops upto order 10 are found. For details see [1].

Our work is based on the counting, but we counted only flexible loops upto order 9 and for this purpose we used the solver FINDER, prior to us this was also used by Asif Ali and John Slaney for counting IP loops. Besides the above mentioned software they also confirmed the counting with the help of solver MACE-4. We used the same program used by the Asif Ali and John Slaney with necessary changes of constrains for flexible loops. With the help of solver FINDER it is not so difficult to generate the flexible loops upto order 9, but solver FINDER failed to count the flexible loops of order 10.

3.1.3 Flexible loop of small order

The smallest flexible loop which is not a group is of order 5 whose multiplication table is given in chapter 1.

We used FINDER to enumerate all flexible loops upto order 9. We used the symmetry breakers in order to get the non-isomorphic loops. Counting of flexible loops is given below

order	flexible loops	groups
1	1	1
2	1	1
3	1	1
4	2	2
5	2	1
6	12	2
7	19	1
8	2291	5
9	31071	2

3.2 Construction of flexible loops

Let G be a multiplicative group with neutral element 1, and A be an abelian group written additively with neutral element 0. Any map

$$\mu : G \times G \to A$$

satisfying

$$\mu(1, g) = \mu(g, 1) = 0 \text{ for every } g \in G,$$

is called a factor set. When $\mu : G \times G \to A$ is a factor set, we can define the multiplication on $G \times A$ by

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

The resulting groupiod is clearly a loop with neutral element $(1, 0)$. It will be denoted by (G, A, μ). Additional properties of (G, A, μ) can be enforced by additional requirements on μ.

We construct flexible loop with the help of two groups such that one is multiplicative group and other is additive abelian group.

Theorem 31 *Let $\mu : G \times G \to A$ be a factor set. Then (G, A, μ) is a flexible loop if and only* *if*

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

Proof. By definition the loop (G,A,μ) is flexible loop if and only if

$$\begin{aligned}(g,a)((h,b)(g,a)) &= ((g,a)(h,b))(g,a)\\ &\Rightarrow (g,a)(hg,b+a+\mu(h,g))\\ &= (gh,a+b+\mu(g,h))(g,a)\\ &\Rightarrow (g(hg),a+b+a+\mu(h,g)+\mu(g,hg))\\ &= ((gh)g,a+b+\mu(g,h)+a+\mu(gh,g)).\end{aligned}$$

Compairing both sides we get

$$\mu(h,g)+\mu(g,hg)=\mu(g,h)+\mu(gh,g)$$

Hence the result follows. ■

Theorem 32 *Let $n>2$ be an integer. Let A be an abelian group of order n, and $\alpha\in A$ be an element of order bigger than 2. Let $G=\{1,u,v,w\}$ be the Klein group with neutral element 1. Define*

$$\mu: G\times G\to A$$

by

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

Then $L=(G,A,\mu)$ is a flexible loop with $N(L)=\{(1,a):a\in A\}$.

Proof. The map μ is flexible factor set. It can be depicted as follows:

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

To show that $L = (G, A, \mu)$ is flexible loop, we verify equation (B) as follows.

Take $h = 1$ in equation (B) we have

$$\mu(1, g) + \mu(g, g) = \mu(g, 1) + \mu(g, g),$$

which is true for all $g \in G$.

Take $h = u$ and $g = u, v, w$ respectively, we get the following results:

$$\begin{aligned}
\mu(u, u) + \mu(u, 1) &= \mu(u, u) + \mu(1, u) = 0, \\
\mu(u, v) + \mu(v, w) &= \mu(v, u) + \mu(w, v) = -\alpha, \\
\mu(u, w) + \mu(w, v) &= \mu(w, u) + \mu(v, w) = \alpha.
\end{aligned}$$

All of which are true.

Now take $h = v$ and $g = u, v, w$ respectively, we get the following results:

$$\begin{aligned}
\mu(v, u) + \mu(u, w) &= \mu(u, v) + \mu(w, u) = 0, \\
\mu(v, v) + \mu(v, 1) &= \mu(v, v) + \mu(1, v) = 0, \\
\mu(v, w) + \mu(w, u) &= \mu(w, v) + \mu(u, w) = \alpha.
\end{aligned}$$

which are true.

Now take $h = w$ and $g = u, v, w$ respectively, we get the following results:

$$\begin{aligned}
\mu(w, u) + \mu(u, v) &= \mu(u, w) + \mu(v, u) = 0, \\
\mu(w, v) + \mu(v, u) &= \mu(v, w) + \mu(u, v) = \alpha, \\
\mu(w, w) + \mu(w, 1) &= \mu(w, w) + \mu(1, w) = 0.
\end{aligned}$$

which all are true. Hence $L = (G, A, \mu)$ is flexible. Now we check that $L = (G, A, \mu)$ is not associative. For this consider

$$(u, a)((v, a)(v, a)) = (u, a)(1, 2a) = (u, 3a),$$

and

$$((u, a)(v, a))(v, a) = (w, 2a - \alpha)(v, a) = (u, 3a - \alpha),$$

this implies that $(u, a)((v, a)(v, a)) \neq ((u, a)(v, a))(v, a)$, and $(v, a), (u, a) \notin N(L)$ because $\alpha \neq 0$. Also $(w, a) \notin N(L)$ because

$$\begin{aligned}
(u, a)((w, a)(w, a)) &\neq ((u, a)(w, a))(w, a), \\
\text{as } (u, 3a) &\neq (u, 3a + \alpha).
\end{aligned}$$

Thus $L = (G, A, \mu)$ is nonalternative and hence nonassociative flexible loop. Now it remains to show that $N(L) = \{(1, a) : a \in A\}$. For this consider

$$\begin{aligned}
((g, b)(1, a))(h, c) &= (g, b)((1, a)(h, c)) \\
&\Rightarrow (g, b + a + \mu(g, 1))(h, c) \\
&= (g, b)(h, a + c + \mu(1, h)) \\
&\Rightarrow (g, b + a + 0)(h, c) \\
&= (g, b)(h, a + c + 0) \\
&\Rightarrow (gh, b + a + c + \mu(g, h)) \\
&= (gh, b + a + c + \mu(g, h)),
\end{aligned}$$

which is true, so

$$\Rightarrow (1, a) \in N_\mu(L).$$

Similarly, we can show that

$$(1, a) \in N_\lambda(L) \text{ and } (1, a) \in N_\rho(L).$$

Hence

$$\begin{aligned}(1,a) &\in N(L)\\ &\Rightarrow N(L)=\{(1,a):a\in A\}.\end{aligned}$$

Which is the required result. ■

Corollary 33 *For any abelian group A of order $n>2$ there exists a flexible loop L such that $order(A)=order(N(L))$.*

Example 34 *Let $G=\{1_G,u,v,w\}$ and $A=\{0,1,2\}$, then*

$$\begin{aligned}(G,A,\mu) &= G\times A=\{(1_G,0),(1_G,1),(1_G,2),(u,0),(u,1),(u,2),\\ &\quad (v,0),(v,1),(v,2),(w,0),(w,1),(w,2)\}\end{aligned}$$

is the flexible loop whose multiplication table is given by

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

where

$$\begin{aligned}(1_G,0) &= 0,(1_G,1)=1,(1_G,2)=2,\\(u,0) &= 3,(u,1)=4,(u,2)=5,\\(v,0) &= 6,(v,1)=7,(v,2)=8,\\(w,0) &= 9,(w,1)=10,(w,2)=11,\end{aligned}$$

and

$$N((G,A,\mu))=\{(1_G,0),(1_G,1),(1_G,2)\}.$$

Lemma 35 *If $\mu: G\times G\to A$ be a factor set and (G,A,μ) is a flexible loop, then for $(g,a)\in(G,A,\mu)$, $(g,a)^{-1}=\left(g^{-1},-a-\mu\left(g,g^{-1}\right)\right)$.*

Proof. Let

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

then

$$\begin{aligned}(g,a)(h,b) &= (1,0)\\&\Rightarrow (gh,a+b+\mu(g,h))=(1,0) \text{ using equation } (A)\\&\Rightarrow gh=1 \text{ and } a+b+\mu(g,h)=0\\&\Rightarrow h=g^{-1} \text{ and } b=-a-\mu(g,h)\\&\Rightarrow h=g^{-1} \text{ and } b=-a-\mu\left(g,g^{-1}\right) \text{ as } h=g^{-1}\end{aligned}$$

Thus $(g,a)^{-1}=(h,b)=\left(g^{-1},-a-\mu\left(g,g^{-1}\right)\right)$. As the loop is flexible, so the inverses are unique. Hence the result follows. ∎

Lemma 36 *Let $\mu: G\times G\to A$ be a factor set, then the loop (G,A,μ) is commutative if and only if*

$$gh=hg \text{ and } \mu(g,h)=\mu(h,g) \text{ for all } g,h\in G.$$

Proof. Let $(g, a), (h, b) \in (G, A, \mu)$, then (G, A, μ) is commutative

$$\begin{aligned} &\Leftrightarrow \quad (g, a)(h, b) = (h, b)(g, a) \\ &\Leftrightarrow \quad (gh, a + b + \mu(g, h)) = (hg, b + a + \mu(h, g)) \text{ using equation } (A) \\ &\Leftrightarrow \quad gh = hg \text{ and } \mu(g, h) = \mu(h, g), \end{aligned}$$

where $g, h \in G$ are orbitrary, hence the required result follows.

Next we will prove that the loop constructed by Theorem 32 is also an IP loop. ∎

Theorem 37 *Let $\mu : G \times G \to A$ be a factor set defined in the same way as in Theorem 32, where G is Klein group and A is any abelian group of order $n > 2$, then (G, A, μ) is a flexible non-alternative IP loop.*

Proof. Flexibility and non-alternativity of (G, A, μ) follows from Theorem 32, and by Lemma 36 (G, A, μ) is commutative, so

$$\mu(g, h) = \mu(h, g). \tag{C}$$

Since (G, A, μ) is flexible, then by Theorem 31 we can write

$$\begin{aligned} & \mu(h, g) + \mu(g, hg) \\ = \quad & \mu(g, h) + \mu(gh, g) \text{ for every } g,\ h \in G \\ \Rightarrow \quad & \mu(g, h) + \mu(g, hg) \\ = \quad & \mu(h, g) + \mu(gh, g) \text{ using equation } (C) \end{aligned}$$

As G is klien group, so $g = g^{-1}$ and $hg = gh$ for all $g, h \in G$ and above equation becomes

$$
\begin{aligned}
& \mu(g,h) + \mu(g^{-1}, gh) \\
= \;& \mu(h,g) + \mu(hg, g^{-1}) \\
\Rightarrow \;& -a - \mu(g, g^{-1}) + a + b + \mu(g,h) + \mu(g^{-1}, gh) \\
= \;& b + a + \mu(h,g) - a - \mu(g, g^{-1}) + \mu(hg, g^{-1}) \\
\Rightarrow \;& (h, -a - \mu(g, g^{-1}) + a + b + \mu(g,h) + \mu(g^{-1}, gh)) \\
= \;& (h, b + a + \mu(h,g) - a - \mu(g, g^{-1}) + \mu(hg, g^{-1})) \\
\Rightarrow \;& (g^{-1}(gh), -a - \mu(g, g^{-1}) + a + b + \mu(g,h) + \mu(g^{-1}, gh)) \\
= \;& ((hg) g^{-1}, b + a + \mu(h,g) - a - \mu(g, g^{-1}) + \mu(hg, g^{-1})) \\
\Rightarrow \;& (g^{-1}, -a - \mu(g, g^{-1}))(gh, a + b + \mu(g,h)) \\
= \;& (hg, b + a + \mu(h,g))(g^{-1}, -a - \mu(g, g^{-1})).
\end{aligned}
$$

So by Lemma 35 we can write

$$
\begin{aligned}
& (g,a)^{-1}(gh, a + b + \mu(g,h)) \\
= \;& (hg, b + a + \mu(h,g))(g,a)^{-1} \\
\Rightarrow \;& (g,a)^{-1}((g,a)(h,b)) = ((h,b)(g,a))(g,a)^{-1}.
\end{aligned}
$$

This implies that (G, A, μ) is an IP loop. Hence the result. ■

Now we are going to prove that the loop constructed by Theorem 32 is also Jordon loop.

Theorem 38 *Let $\mu : G \times G \to A$ be a factor set defined in the same way as in Theorem 32, where G is Klein group and A is any abelian group of order $n > 2$, then (G, A, μ) is a flexible non-alternative Jordon loop.*

Proof. Flexibility and non-alternativity of (G, A, μ) follow from Theorem 32 and according to the definition of $\mu : G \times G \to A$ we can write

$$\begin{aligned}
\mu(h,g) &= \mu(h,g) \text{ for all } h,g \in G \\
&\Rightarrow \mu(h,g) + \mu(1,hg) = \mu(1,h) + \mu(h,g) \\
&\Rightarrow \mu(h,g) + \mu\left(g^2,hg\right) = \mu\left(g^2,h\right) + \mu\left(g^2h,g\right) \\
&\Rightarrow a + a + \mu(g,g) + b + a + \mu(h,g) + \mu\left(g^2,hg\right) \\
&= a + a + \mu(g,g) + b + \mu\left(g^2,h\right) + a + \mu\left(g^2h,g\right) \\
&\Rightarrow \left(g^2(hg), a + a + \mu(g,g) + b + a + \mu(h,g) + \mu\left(g^2,hg\right)\right) \\
&= \left(\left(g^2h\right)g, a + a + \mu(g,g) + b + \mu\left(g^2,h\right) + a + \mu\left(g^2h,g\right)\right) \\
&\Rightarrow \left(g^2, a + a + \mu(g,g)\right)(hg, b + a + \mu(h,g)) \\
&= \left(g^2h, a + a + \mu(g,g) + b + \mu\left(g^2,h\right)\right)(g,a) \\
&\Rightarrow [(g,a)(g,a)][(h,b)(g,a)] = \left[\left(g^2, a + a + \mu(g,g)\right)(h,b)\right](g,a) \\
&\Rightarrow (g,a)^2[(h,b)(g,a)] = [\{(g,a)(g,a)\}(h,b)](g,a) \\
&\Rightarrow (g,a)^2[(h,b)(g,a)] = \left[(g,a)^2(h,b)\right](g,a)
\end{aligned}$$

which is jordon identity, also by Lemma 36 (G,A,μ) is commutative. Hence (G,A,μ) is a flexible non-alternative Jordon loop. ∎

3.2.1 Autotopism and flexibility

Now we will make a relation between autotopisim and flexibility that is what will be the kind of autotopisim so that the loop is flexible.

Lemma 39 *Let L be any loop and (R_{xz}, Id_L, R_{xz}) is an autotopisim for all $x,z \in L$, then L is an extra loop.*

Proof. Let L be a loop such that (R_{xz}, Id_L, R_{xz}) is an autotopisim for all $x,z \in L$, then by the definition of autotopisim we can write

$$\begin{aligned}
(u)R_{xz} \cdot (v)Id_L &= (uv)R_{xz} \text{ for all } x,z,u,v \in L \\
&\Rightarrow (u)(xz) \cdot v = (uv)(xz).
\end{aligned}$$

Now replacing u by y and v by x we get

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

or

$$((y)(xz))x = (yx)(xz)$$

So by Theorem 1 in [5], it follows that L is an extra loop. ■

Theorem 40 *Any loop L is flexible if for each $x \in L$, (R_x, Id_L, R_x) is an autotopisim.*

Proof. Let (R_x, Id_L, R_x) is an autotopisim for each $x \in L$,this implies that (R_{xz}, Id_L, R_{xz}) is an autotopisim.

So by above Lemma 39 L is an extra loop and extra loop is subloop of moufang loop. So L is flexible. ■

3.3 ARIF loops and nuclear square loops

In this section we will show that for which kind of loops the square of left (right) translation will be left (right) translation. It is already proved that every RC-loop implies right nuclear square loop and also middle nuclear square loop. Similarly, every LC-loop implies left nuclear square loop and also middle nuclear square loop. But here we will prove that every right nuclear square ARIF loop is RC-loop, every left nuclear square ARIF loop is LC-loop and every middle nuclear square ARIF loop is C-loop.

Lemma 41 *Any loop L is alternative iff*

$$L_{x^2} = L_x^2 \text{ and } R_{x^2} = R_x^2 \text{ for all } x \in L.$$

Proof. We know that any loop L is alternative if and only if L is left alternative and right alternative

$$\begin{aligned}
&\Leftrightarrow\ (xx)\,y = x\,(xy) \text{ and } (yx)\,x = y\,(xx) \\
&\Leftrightarrow\ x^2y = ((y)\,L_x)\,L_x \text{ and } ((y)\,R_x)\,R_x = (y)\,R_{x^2} \\
&\Leftrightarrow\ (y)\,L_{x^2} = (y)\,L_xL_x \text{ and } (y)\,R_xR_x = (y)\,R_{x^2} \\
&\Leftrightarrow\ (y)\,L_{x^2} = (y)\,L_x^2 \text{ and } (y)\,R_x^2 = (y)\,R_{x^2} \\
&\Leftrightarrow\ L_{x^2} = L_x^2 \text{ and } R_x^2 = R_{x^2}.
\end{aligned}$$

Hence the result follows. ∎

Corollary 42 *If L is an ARIF loop, then*

$$L_{x^2} = L_x^2 \text{ and } R_{x^2} = R_x^2 \text{ for all } x \in L.$$

Theorem 43 *Let L be an ARIF loop such that it is right nuclear square loop, then L is RC-loop.*

Proof. Since L is an ARIF loop, so by above Corollary 42, we can write

$$\begin{aligned}
R_{x^2} &= R_x^2 \text{ for all } x \in L \\
&\Rightarrow\ (y)\,R_x^2 = (y)\,R_{x^2} \\
&\Rightarrow\ ((y)\,R_x)\,R_x = (y)\,R_{x^2} \\
&\Rightarrow\ (yx)\,x = y\,(xx) \\
&\Rightarrow\ z\,((yx)\,x) = z\,(y\,(xx)).
\end{aligned}$$

Replace x by z and z by x, we have

$$x\,(y\,(zz)) = x\,((yz)\,z).$$

As L is right nuclear square loop, so

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

Which is the right central identity. Hence L is RC-loop.

Corollary 44 *Let L be an ARIF loop, then L is RC-loop if and only if L is right nuclear square loop.*

■

Theorem 45 *Let L be an ARIF loop such that it is left nuclear square loop, then L is LC-loop.*

Proof. Since L is an ARIF loop, so by above Lemma 42, we can write

$$\begin{aligned} L_{x^2} &= L_x^2 \text{ for all } x \in L \\ &\Rightarrow (y)L_x^2 = (y)L_{x^2} \\ &\Rightarrow ((y)L_x)L_x = (y)L_{x^2} \\ &\Rightarrow x(xy) = (xx)y \\ &\Rightarrow (x(xy))z = ((xx)y)z. \end{aligned}$$

As L is left nuclear square loop, so

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

Which is the left central identity. Hence L is LC-loop. ■

Corollary 46 *Let L be an ARIF loop, then L is LC-loop if and only if L is left nuclear square loop.*

Theorem 47 *Let L be an ARIF loop such that it is middle nuclear square loop, then L is C-loop.*

Proof. Since L is an ARIF loop, so by above Lemma 42, we can write

$$\begin{aligned} R_{x^2} &= R_x^2 \text{ for all } x \in L \\ &\Rightarrow (y) R_x^2 = (y) R_{x^2} \\ &\Rightarrow ((y) R_x) R_x = (y) R_{x^2} \\ &\Rightarrow (yx) x = y (xx). \end{aligned}$$

Interchanging x and y, we have

$$\begin{aligned} (xy) y &= x (yy) \\ &\Rightarrow ((xy) y) z = (x (yy)) z. \end{aligned}$$

As L is middle nuclear square loop, so we can write

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

Using Lemma 42, we get

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

Which is central identity. Hence L is C-loop. ∎

3.4 ARIF loops and squaring property, Jordon identity

In this section we will find the condition on ARIF loop such that it satisfies the squaring property. Also we will prove that ARIF loop satisfies the Jordon identity and becomes Jordon loop if it is commutative.

Theorem 48 *Let L be a commutative ARIF loop, then $(xy)^2 = x^2y^2$ for all $x, y \in L$.*

Proof. Since by corollary 2.8 in [6], it follows that every ARIF loop is alternative and also IP loop. But L is also commutative, so by Lemma 5.1 in [7] the result follows. ∎

Theorem 49 *Every ARIF loop satisfies the Jordon identity.*

Proof. Since every ARIF loop is flexible and also alternative. So consider

$$\begin{aligned} (x^2y)\,x &= ((xx)\,y)\,x = (x\,(xy))\,x \\ &= x\,((xy)\,x) = x\,(x\,(yx)) \\ &= (xx)\,(yx) = x^2\,(yx) \\ &\Rightarrow (x^2y)\,x = x^2\,(yx)\,. \end{aligned}$$

Which is Jordon identity. Hence the result follows. ■

Corollary 50 *Every commutative ARIF loop L is Jordon loop.*

Proof. By Theorem 49 and commutativity we get that L is a Jordon loop. ■

Theorem 51 *Let L be an ARIF loop such that (L_x^2, Id_L, L_x^2) is an autotopisim for each $x \in L$, then L satisfies the Jordon identity.*

Proof. Since L is an ARIF loop and (L_x^2, Id_L, L_x^2) is an autotopisim for each $x \in L$, then by definition of autotopisim we can write

$$\begin{aligned} (y)\,L_x^2 \cdot (z)\,Id_L &= (yz)\,L_x^2 \\ &\Rightarrow ((y)\,L_x)\,L_x \cdot z = ((yz)\,L_x)\,L_x \\ &\Rightarrow x\,(xy) \cdot z = x\,(x\,(yz))\,. \end{aligned}$$

As L is alternative, so

$$\begin{aligned} (xx)\,y \cdot z &= (xx)\,(yz) \\ &\Rightarrow (x^2y)\,z = x^2\,(yz) \\ &\Rightarrow (x^2y)\,x = x^2\,(yx)\,. \end{aligned}$$

Which is the Jordon identity. Hence the result follows. ■

Bibliography

[1] Asif Ali and John Slaney, Counting loops with the inverse property, Quasigroups and Related Systems 16(2008), $13 - 16$.

[2] R. H. Bruck (1944), Contributions to the theory of loops, Trans. Amer. Soc. 55, $245 - 354$.

[3] Raoul E. Cawagas, Generation of NAFIL loops of small order, Quasigroups and Related Systems 7(2001), $1 - 5$.

[4] Ales Drapal, Conjugacy closed loops and their multiplication groups, Journal of Algebra 272(2004), $838 - 850$.

[5] Ferenc Fenyves, Extra loops II, On loops with identities of Bol-Moufang type, Publ. Math. Debrecen 16(1969), $187 - 192$.

[6] Michael K.Kinyon, Kaneeth Kunen, and J. D. Phillips, A genration of Moufang and Steiner loops, Algebra Universalis 48(2002), no. $1, 81 - 101$.

[7] J. D. Philips and Petr Vojtechovsky, C-Loops: An Introduction, Publicationes Mathematicae Debrecen 68(2006), nos. $1 - 2, 115 - 137$.

[8] John Slaney and Asif Ali, Generating Loops with the Inverse Property, Sutcliffa G., Schulz S. (eds.); Proceedings of ESARM 2008, pp. $55 - 66$.