International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

PAIGE LOOPS AND SMARANDACHE SEMIGROUP ACTION PROBLEMS

Dr. V. Vasu, Department of Mathematics ,S.V. University, Tirupati
Email: vasuvaralakshmi@gmail.com

Abstract:

In this paper we introduced the concepts of loops, Smarandache loops, Sub-loops, Smarandache sub-loops, Normal loops, Smarandache normal loops, in section 1 we study structure of Moufang loops and Paige loops.

The necessary defini-tions and results are presented in the section 1.1 section 1.2 deals with the Paige loops and Moufang loops.

1. PRELIMINARIES

1.1 DEFINITION: A non-empty set L is said of form a loop, if on L is defined a binary operation called the product denoted by '$\bullet$' such that

a. For all a, b $\in$ L we have a $\bullet$ b $\in$ L (closure property).
b. There exists an element e $\in$ L such that a $\bullet$ e=e $\bullet$ a=a for all a $\in$ L (e is called the identity element of L).
c. For every ordered pair (a,b) $\in$ L x L there exists a unique pair (x,y) in L such that ax = b and ya = b.

Note: Throughout this chapter we take L to be a finite loop, unless otherwise we state it explicitly, L is an infinite loop. The binary operation '$\bullet$' in general need not be associative on L. We also mention all groups are loops but in general every loop is not a group. Thus loops are the more generalized concept of groups.

1.1a Example: Let (L, *) be a loop of order six given by the following table. This loop is a commutative loop but it is not associative.

*	e	a_1	a_2	a_3	a_4	a_5
e	e	a_1	a_2	a_3	a_4	a_5
a_1	a_1	e	a_4	a_2	a_5	a_3
a_2	a_2	a_4	e	a_5	a_3	a_1
a_3	a_3	a_2	a_5	e	a_1	a_4
a_4	a_4	a_5	a_3	a_1	e	a_2
a_5	a_5	a_3	a_1	a_4	a_2	e

Clearly (L, *) is non-associative as $(a_4 * a_3) * a_2 = a_4 * (a_3 * a_2) = a_4 * a_5 = a_2$.
Thus $(a_4 * a_3) * a_2 \neq a_4 * (a_3 * a_2)$.

1.2 DEFINITION: A loop (L, $\bullet$) is said to be a commutative loop if for all a, b $\in$ L we have a $\bullet$ b = b $\bullet$ a.

The loops given in examples 3.2.2 and 3.2.4 are commutative loops. If in a loop (L, $\bullet$) we have at least a pair a, b$\in$ L such that a $\bullet$ b $\neq$ b $\bullet$ a then we say (L, $\bullet$) is a non-commutative loop.

The loop given in example 3.2.3 is non-commutative.

1.2a Example: Now consider the following loop (L, $\bullet$) given by the table:

$\bullet$	e	g_1	g_2	g_3	g_4	g_5
e	e	g_1	g_2	g_3	g_4	g_5
g_1	g_1	e	g_3	g_5	g_2	g_4
g_2	g_2	g_5	e	g_4	g_1	g_3
g_3	g_3	g_4	g_1	e	g_5	g_2
g_4	g_4	g_3	g_5	g_2	e	g_1
g_5	g_5	g_2	g_4	g_1	g_3	e

We see a special quality of this loop viz. in this loop xy $\neq$ yx for any x, y $\in$ L / {e} with x $\neq$ y.

$g_1 \bullet g_2 = g_3,\ g_2 \bullet g_1 = g_5 \qquad \therefore g_1 \bullet g_2 \neq g_2 \bullet g_1$

$g_4 \bullet g_2 = g_5,\ g_2 \bullet g_4 = g_1,$

$\therefore g_2 \bullet g_4 \neq g_4 \bullet g_2$

$\therefore (L, \bullet)$ is non-commutative

$(g_1 \bullet g_2) \bullet g_3 = g_3 \bullet g_3 = e,$

$g_1 \bullet (g_2 \bullet g_3) = g_1 \bullet g_4 = g_2$

$(g_1 \bullet g_2) \bullet g_3 \neq g_1 \bullet (g_2 \bullet g_3)$ non-associative

$\therefore (L, \bullet)$ is neither commutative nor associative.

1.3 DEFINITION: Let L be a loop. A non-empty subset H of L is called a subloop of L if H itself is a loop under the operation of L.

1.3a Example: Consider the loop L given in example 3.2.4 we see $H_i = \{e, g_i\}$ for i = 1,2,3,4,5,6,7 are subloops of L.

1.4 DEFINITION: Let L be a loop. A subloop H of L is said to be a normal subloop of L, if

1. xH = Hx

ISSN:2319-7900

2. (Hx)y = H(xy)
3. y(xH) = (yx)H

for all x, y $\in$ L.

1.5 DEFINITION: A loop L is said to be a simple loop if it does not contain and non-trivial normal subloop.

1.5a Example: The loops given in example 3.2.2 and 3.2.4 are simple loops for it is left for the reader to check that these loops do not contain normal subloops, in fact both of them constain subloops which are not normal.

$H_1 = \{e, a_3\}$ is a subloop

$H_2 = \{e, a_2\}$ is a subloop but these are normal subloops

1.6 DEFINITION: The commutator subloop of a loop L denoted by L' is the sub loop generated by all of its commutators, that is, $\langle \{x \in L / x = (y,z) \text{ for some } y, z \in L\} \rangle$ where for $A \subseteq L$, $\langle A \rangle$ denotes the subloop generated by A.

1.7 DEFINITION: If $x, y \text{ and } z$ are elements of a loop L an associator (x, y, z) is defined by, $(xy)z = (x(yz))(x, y, z)$.

1.8 DEFINITION: The associator subloop of a loop L (denoted by A(L)) is the subloop generated by all of its associators, that is $\langle \{x \in L / x = (a,b,c)$ for some $a, b, c \in L\} \rangle$.

1.9 DEFINITION: A loop L is said to be semi alternative if $(x, y, z) = (y, z, x)$ for all $x, y, z \in L$, where (x, y, z) denotes the associator of elements $x, y, z \in L$.

1.10 DEFINITION : Let L be a loop. The flexible law FLEX: $x \bullet yx = xy \bullet x$ for all $x, y \in L$. If a loop L satisfies left alternative laws that is $y \bullet yx = yy \bullet x$ then RLALT. L satisfies right alternative laws RALT: $x \bullet yy = xy \bullet y$.

1.11 DEFINITION : ARIF loop is an IP loop L with the property $\theta^j = \theta$ for all $\theta \in Mlt_1(L)$. Equivalently, inner mappings preserve inverses that is $(x^{-1})\theta = (x\theta)^{-1}$ for all $\theta \in Mlt_1(L) \text{ and for all } x \in L$.

1.12 DEFINITION: A map ϕ for a loop L to another loop L_1 is called a loop homomorphism if $\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in L$.

1.13 DEFINITION : Let L be a loop L is said to be a strictly non-commutative loop if $xy \neq yx \text{ for any } x, y \in L (x \neq y, x \neq e, y \neq e$ where e is the identity element of L).

1.14 DEFINITION: A loop L is said to be power-associative in the sense tht every element of L generates an abelian group.

1.15 DEFINITION: A loop L is diassociative loop if every pair of elements of L generates a subgroup.

1.15a Example: Let L be a loop given by the following table:

•	e	a_1	a_2	a_3	a_4	a_5
e	e	a_1	a_2	a_3	a_4	a_5
a_1	a_1	e	a_3	a_5	a_2	a_4
a_2	a_2	a_5	e	a_4	a_1	a_3
a_3	a_3	a_4	a_1	e	a_5	a_2
a_4	a_4	a_3	a_5	a_2	e	a_1
a_5	a_5	a_2	a_4	a_1	a_3	e

The nucleus of this loop is just {e}. The left nucleus of L, l N_λ (L) = {e}. The Moufang centre of the loop L is C(L) = {e}. Thus for this L we see the center is just {e}.

1.16 DEFINITION: A loop L is said to be a Moufang loop if it satisfies any one of the following identities:

$$1.(xy)(zx) = (x(yz))x$$

$$2.((xy)z)y = x(y(zy))$$

$$3.x(y(xz) = (xy)x)z$$

$$\text{for all } x, y, z \in L.$$

1.17 DEFINITION: Let be a loop, L is called a Bruck loop if $x(yx)z = x(y(xz))$ and $(xy)^{-1} = x^{-1}y^{-1} \text{ for all } x, y, z \in L$.

1.18 DEFINITION: A loop (L, •) is called a Bol loop if $((xy)z)y = x((yz)y)$ for all $x, y, z \in L$.

1.19 DEFINITION: A loop L is said to be right alternative if $(xy)y = x(yy)$ for all $x, y \in L \text{ and } L$ is left alternative if $(xx)y = x(xy) \text{ for all } x, y \in L. L$ is said to be an alternative loop if it is both a right and left alternative loop.

1.20 DEFINITION : A loop $(L, \bullet)$ is called a weak inverse property loop (WIP-loop) if $(xy)z = e \text{ imply } x(yz) = e \text{ for all } x, y, z \in L$.

ISSN:2319-7900

1.21 DEFINITION: A loop L is said to be semi alternative if $(x, y, z) = (y, z, x)$ for all $x, y, z \in L$, where (x, y, z) denotes the associator of elements $x, y, z \in L$.

1.22 DEFINITION: The Smarandache loop (S-loop) is defined to be a loop L such that a proper subset A of L is a subgroup (with respect to the same induced operation) that is $\phi \neq A \subset L$.

1.22a THEOREM The natural class of loops $L_n(m) \in L_n$ (n odd, n > 3, (m, n) = 1, (m, -1, n) =1 for varying m) are S-loops.

Proof: We see by the very construction of loops $L_n(m)$ in L_n each $i \in L_n(m)$ is such that $i \bullet i = e$ where e is the identity element of $L_n(m)$. Thus all proper subsets of he form $\{e, i\} \subset L_n(m)$ for varying I are groups. Thus the class of loops L_n are S-loops.

1.22b THEOREM : Let L be a Moufang loop which is centrally nilpotent of class 2. Then L is a S-loop.

Proof: We know if L is a Moufang loop which is centrally nilpotent of class 2, that is, a Moufang loop L such that the quotient of L by its centre Z(L) is an abelian group; and let L_p denote the set of all elements of L whose order is a power of p. That the nuclearly derived subloop, or normal associator subloop of L, which we denote by L^* is the smallest normal subloop of L such that L/L^* is associatie (i.e. a group). Also that the torsion subloop (subloop of finite order elements) of L is isomorphic to the (restricted) direct product of the subloops L_p where p runs over all primes.

1.23 DEFINITION : Let L be a loop. A proper subset A of L is said to be a Smarandache subloop (S-subloop) of L if A is a subloop of L and A is itself a S-subloop; that is A contains a proper subset B contained in A such that B is a group under the operations of L. We demand A to be a S-subloop which is not a subgroup.

1.23a THEOREM: Let L be a loop. If L has a S-subloop then L is a S-loop.

Proof: If a loop L has S-subloop then we have a subset $A \subset L$ such that A is a subloop and contains a proper subset B such that B is a group. Hence $B \subset A \subset L$ so L is a S-loop. So a subloop can have a S-subloop only when L is a S-loop.

1.23a Example: Consider the loop 0- is a subloop of the loop $L_{15}(2)$. Clearly H is a S-subloop of L. But it is interesting to note that in general all S-loop need not have every subloop to be a S-subloop or more particularly a S-loop need not have S-subloops at all

1.24 DEFINITION: Let L be a S-loop. If L has no subloops but only subgroups well call L a Smarandache subgroup (S-subgroup) loop.

1.24a THEOREM: Let $L_n(m) \in L_n$ where n is a prime. Then the class of loops L_n is a S-subgroup loop.

Proof: Given n is a prime. So $L_n(m) \in L_n$ has n + 1 elements and further no number t divides n. By the very construction of $L_n(m)$ we see $L_n(m)$ is a S-loop every element generates a cyclic group of order 2. Thus we have a class of loops L_n which are S-subgroup loops for each prime n = p, n > 3.

1.25 DEFINITION: Let L be a loop. We say a non-empty subset A of L is a Smarandache normal subloop (S-normal subloop) of L if

1. A is itself a normal subloop of L.
2. A contains a proper subset B where B is a subgroup under the operations of L. If L has no S-normal subloop we say the loop L is Smarandache simple (S-simple).

1.25a THEOREM: Let L be a loop. If L has a S-normal subloop then L is a S-loop.

Proof: Obvious by the Let L be a loop. We say a non-empty subset A of L is a Smarandache normal subloop (S-normal subloop) of L if

1. A is itself a normal subloop of L.
2. A contains a proper subset B where B is a subgroup under the operations of L. If L has no S-normal subloop we say the loop L is Smarandache simple (S-simple).

of S-normal subloop we see L is a S-loop.

Now we see that a loop may have normal subloops but yet that normal subloop may not be a S-normal subloop.

1.25b THEOREM : Let L be a loop. If L has a S-normal subloop then L has a normal subloop, so L is not simple.

Proof: We say a non-empty subset A of L is a Smarandache normal subloop (S-normal subloop) of L if

1. A is itself a normal subloop of L.
2. A contains a proper subset B where B is a subgroup under the operations of L. If L has no S-normal subloop we say the loop L is Smarandache simple (S-simple).

Of S-normal subloop in a loop L we are guaranted, that the loop L must have a normal subloop so L is not simple. Hence the claim.

1.26 DEFINITION: Let L be a S-loops unlike in groups or loops remain at a very dormant state.

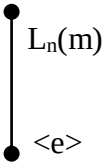
1.27 DEFINITION : Let L be a loop. L is said to be a Smarandache strongly commutative (S-strongly commutative) loop if every proper subset which is a group is a commutative group.

ISSN:2319-7900

1.27a THEOREM: Let $L_n(m) \in L_n$ be the class of S-loops. The Smarandache lattice representation of S-normal subloops of the loop $L_n(m)$ from a two element chain lattice.

Proof: Every $L_n(m) \in L_n$ has no S-normal subloops.

So the only trivial S-normal subloops are e and $L_n(m)$ giving the two element chain



This can be compared with the normal subgroups in the alternating group $A_n, n \geq 5.$

1.28 DEFINITION: For all a,b in L. A congruence relation in a loop L is an equivalence relation ~ such that

$$a \square b \Rightarrow \begin{cases} ac \square bc \, \forall c \in L, \\ ca \square cb \, \forall c \in L. \end{cases}$$

This notion is closer to the notion of congruence relation in groups than in Smarandache semigroups. Indeed, the following proposition shows that both are equivalent, contrary to the case of Smarandache semigroups where the notion of c-simplicity had to be created to capture the essence we were looking for.

REFERENCES:

1. Blake, I ., G. Seroussi, and N. Smart. Elliptic Curves in Cryptography. Lecture Note Series 265. London Mathematical Society, 1999.
2. Chin Long Chen. Formulas for the solutions of quadratic equations over GF(2^m). IEEE Trans. Inform. Theory, 28(5): 792-794, 1982.
3. Menezes, A.J. and Y. –H. Wu. The discrete logarithm problem in Gl(n,q). Ars Combin., 47:23-32,1992.
4. Moufang. R., Zur Struktur von Alternativk ö rpern. Math. Ann., 110:416-430, 1935.
5. Paige. L.J.A class of simple Moufang loops. Proc. Amer, Math. Soc., 7:471-482.1956.
6. Ueli Maurer and Stefan Wolf. Lower bounds on generic algorithms in groups. In Advances in cryptology – EUROCRYPT'98 (Espoo), volume 1403 of Lecture Notes in Comput. Sci., pages 72-84. Springer, Berlin, 1998.
7. Vojtechovsky. P. Finit simple Moufang loops. Ph.D thesis, Iowa State University, 2001. Available at http://www.public. iastate.edu/ petr.