

Structure, Symmetry and Graphs of Inverse LA-semigroups



By

Irfan Younas

Supervised By

Professor Qaiser Mushtaq

**Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan 2019**

Structure, Symmetry and Graphs of Inverse LA-semigroups



By

Irfan Younas

A Thesis Submitted for the Partial Fulfillment of the Requirements for the

Degree of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

Supervised By

Professor Qaiser Mushtaq

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan 2019

Author's Declaration

I Irfan Younas hereby state that my PhD thesis titled Structure, Symmetry and Graphs of Inverse LA-semigroups is my own work and has not been submitted previously by me for taking any degree from the Quaid-i-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the university has the right to withdraw my PhD degree.



Name of Student: Irfan Younas

Date: 16-10-2019

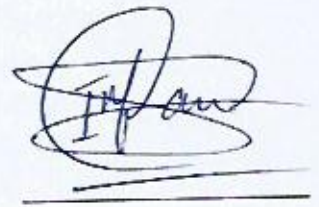
Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "Structure, Symmetry and Graphs of Inverse LA-semigroups" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and Quaid-i-Azam University towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Student/Author's Signature: _____



Name of student: Irfan Younas

Structure, Symmetry and Graphs of Inverse LA-semigroups

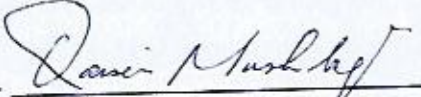
By

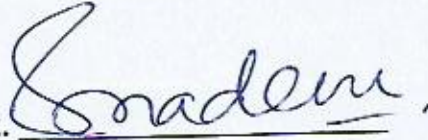
Irfan Younas

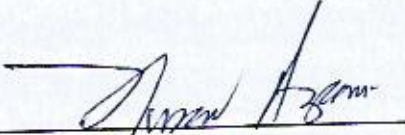
CERTIFICATE

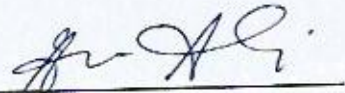
A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF
PHILOSOPHY

We accept this dissertation as conforming to the required standard.

1. 
Prof. Dr. Qaiser Mushtaq
Department of Mathematics
Quaid-i-Azam University
Islamabad
Ex. Vice Chancellor
Islamia University of Bahawalpur
(Supervisor)

2. 
Prof. Dr. Sohail Nadeem
Department of Mathematics
Quaid-i-Azam University
Islamabad
(Chairman)

3. 
Prof. Dr. Akbar Azam
Department of Mathematics
COMSATS University
Park Road, Chak Shahzad
Islamabad
(External Examiner)

4. 
Dr. Muhammad Irfan Ali
Associate Professor
Islamabad Model College for
Girls, F-6/2, Street 25
Islamabad
(External Examiner)

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2019

Certificate of Approval

This is to certify that the research work presented in this thesis entitled **Structure, Symmetry and Graphs of Inverse LA-semigroups** was conducted by **Mr. Irfan Younas** under the supervision of **Prof. Dr. Qaiser Mushtaq**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Field of Mathematics from Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan.

Student Name: **Irfan Younas**

Signature: _____



External committee:

a) **External Examiner 1:**

Signature: _____



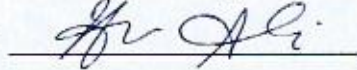
Name: **Dr. Akbar Azam**

Designation: Professor

Office Address: Department of Mathematics, COMSATS University, Islamabad.

b) **External Examiner 2:**

Signature: _____



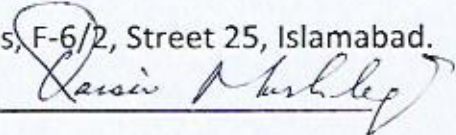
Name: **Dr. Muhammad Irfan Ali**

Designation: Associate Professor

Office Address: Islamabad Model College for Girls, F-6/2, Street 25, Islamabad.

c) **Internal Examiner:**

Signature: _____



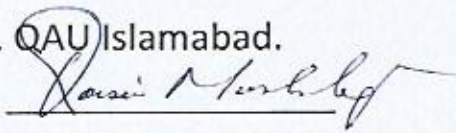
Name: **Dr. Qaiser Mushtaq**

Designation: Professor

Office Address: Department of Mathematics, QAU Islamabad.

Supervisor Name:

Signature: _____



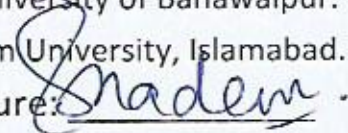
Name: **Dr. Qaiser Mushtaq**

Designation: Professor/ Ex. Vice Chancellor, Islamia University of Bahawalpur.

Office Address: Department of Mathematics, Quaid-i-Azam University, Islamabad.

Name of Dean/ HOD: **Dr. Sohail Nadeem**

Signature: _____



Contents

1	PRELIMINARIES	1
1.1	Introduction	1
1.2	LA-semigroup	1
1.3	Graphs of LA-semigroups	9
1.4	Enumeration of Finite LA-semigroups	15
2	INVERSE LA-SEMIGROUPS	17
2.1	Introduction	17
2.2	Natural Partial Order	20
2.3	Restricted Product and Green's Relations	22
2.4	Homomorphisms between Inverse LA-semigroups	24
2.5	Kernel and Trace	25
2.6	Conclusion	28
3	LEFT PERMUTABLE INVERSE LA-SEMIGROUPS	29
3.1	Introduction	29
3.2	Natural Partial Order and Compatibility Relations	30
3.3	Infinitely Distributive Left Permutable Inverse LA-semigroups	35
3.4	Conclusion	38
4	ENUMERATION OF FINITE INVERSE LA-SEMIGROUPS	39
4.1	Introduction	39
4.2	Methodology for Enumeration of Finite Inverse LA-semigroups	42

4.3	Enumeration Results	57
4.4	Source Code	59
4.5	Conclusion	68
5	PRESENTATION OF INVERSE LA-SEMIGROUPS	69
5.1	Introduction	69
5.2	Presentations and Graphs of Inverse LA-semigroups	71
5.3	Construction and Representation	81
5.4	Wreath Product of Inverse LA-semigroups	83
5.5	Conclusion	86
6	APPLICATION OF INVERSE LA-SEMIGROUPS IN CRYPTOGRAPHY	87
6.1	Introduction	87
6.2	Security Analysis of the Proposed Algorithm	94
6.3	Pixel Modification Based Measurements	102
6.4	Similarities Measure	104
6.5	Entropy Investigation	105
6.6	Conclusion	107

Chapter 1

PRELIMINARIES

1.1 Introduction

In this chapter, we provide general information for the rest of the thesis. The essential definitions and results regarding LA-semigroups are presented here. The chapter is divided into four sections. The areas covered here are magmas in general, LA-semigroups in particular. Similar algebraic concepts regarding semigroups are available in books such as Fundamentals of Semigroup Theory [24] by Howie, The Algebraic Theory of Semigroups [8] by Clifford and Preston, and Theory of Partial Symmetries [34] by Lawson.

The purpose of this chapter is to enable the readers to comprehend this work without consulting the references. However, references for more knowledge are provided throughout. Besides introducing the fundamental concepts of LA-semigroups that are available in existing literature, the chapter also provides some new ideas.

1.2 LA-semigroup

The algebraic objects dealt with in this thesis are left almost semigroups (abbreviated as LA-semigroups). In this section, we provide some basic definitions and results to introduce the frequently used notation. Readers are referred to find other sources in particular [40, 41, 43, 50, 52] for fundamentals of the LA-semigroups.

Definition 1 Let \mathbf{L} be a non-empty set.

- (i) A binary operation is a mapping $\star : \mathbf{L} \times \mathbf{L} \rightarrow \mathbf{L}$ and a magma is denoted by the pair (\mathbf{L}, \star) .
- (ii) A magma (\mathbf{L}, \star) is a left almost semigroup (abbreviated as LA-semigroup), if $(u \star v) \star w = (w \star v) \star u$ for all $u, v, w \in \mathbf{L}$.
- (iii) An element $e \in \mathbf{L}$ is a left identity (right identity) of (\mathbf{L}, \star) , if $e \star u = u$, $(u \star e = u)$ for all $u \in \mathbf{L}$. An LA-semigroup containing a left identity is a left almost monoid (abbreviated as LA-monoid).
- (iv) An LA-monoid (\mathbf{L}, \star) is left invertible, if for all $u \in \mathbf{L}$, there exists an element $u^{-1} \in \mathbf{L}$ such that $u^{-1} \star u = e$. Then u^{-1} is the left inverse of u . An LA-group is actually an LA-monoid containing every invertible element.

In the future, it is usually a common practice that a magma (\mathbf{L}, \star) is represented by the non-empty set \mathbf{L} and the operation \star is represented by simple adjacent positions of elements. When it seems ambiguous, operation \star is used. Generally, the multiplication is used as operation. The cardinality or order of L is the number of elements in magma (LA-semigroup, LA-monoid, and LA-group respectively). The period of an element $u \in \mathbf{L}$ is the least positive integer n such that $u^{n+1} = u$.

Commutativity is defined as $uvw = wvu$ in terms of ternary operations. Naseerudin used the brackets on the left of this identity to introduce a new rule, that is, $(uv)w = (vw)u$ and defined a magma satisfying the rule $(uv)w = (vw)u$ as a left almost semigroup[50]. Similarly, a magma satisfying the rule $u(vw) = w(vu)$ is named as right almost semigroup. Later, Mushtaq and Yusuf explored some fundamental properties [40]. They also introduced locally associative LA-semigroups and LA-semigroups derived from commutative inverse semigroups [41, 43]. LA-semigroups are also known as the right modular groupoids or left invertive groupoids [23, 27]. Dénes and Keedwell referred the name Abel Grassmann's law to represent the rule $u(vw) = w(vu)$ [9]. Later, Protić and Stevanović introduced the name Abel Grassmann's groupoids (shortly as AG-groupoid) for LA-semigroups [52]. In [40], Mushtaq and Yusuf pointed out that the medial identity, that is, $(uv)(wx) = (uw)(vx)$ holds naturally in an arbitrary LA-semigroup

by using left invertive law successively. It is important to mention here that every LA-semigroup is medial but a medial groupoid may not be an LA-semigroup. For instance, Table 1 satisfies the medial identity without being an LA-semigroup.

Table 1. Medial groupoid which is not LA-semigroup

*	0	1	2	3	4
0	4	4	4	2	4
1	4	0	0	4	4
2	4	0	4	2	4
3	0	2	2	0	0
4	4	4	4	4	4

Here, $(0 * 3) * 1 \neq (1 * 3) * 0$ substantiates it.

LA-semigroups are non-associative in general, but they are similar in behaviour to the semigroups and commutative semigroups. LA-semigroups can easily be transformed into semigroups or commutative semigroups under certain conditions. We provide the following examples to illustrate the connection between a semigroup and an LA-semigroup (especially a commutative semigroup).

Example 1 Let a be a fixed element of \mathbf{L} on which a binary operation \circ is defined by $u \circ v = (ua)v$, for all $u, v \in \mathbf{L}$.

Then it is easy to see that $u \circ v = v \circ u$ for all $u, v \in \mathbf{L}$. Additionally, if \mathbf{L} satisfies the identity $u(vw) = v(uw)$, then $(u \circ v) \circ w = ((ua)v) \circ w = (((ua)v)a)w = (wa)((ua)v)$ and $u \circ (v \circ w) = u \circ ((va)w) = (ua)((va)w) = (ua)((wa)v) = (wa)((ua)v)$. Consequently, (\mathbf{L}, \circ) is a commutative semigroup.

Example 2 Let \mathbb{Z} be the set of integers on which $*$ is taken as follows: $u * v = v - u$, for all $u, v \in \mathbb{Z}$.

Then clearly, it is an infinite LA-semigroup which is non-commutative as well as non-associative.

In order to define associative powers in \mathbf{L} , the identity $(uv)w = v(uw)$ was introduced in \mathbf{L} [45]. An LA-semigroup \mathbf{L} with this additional property is called an LA*-semigroup. In [44], Mushtaq and Kamran proved that $(uv)w = v(uw)$, and $(uv)w = v(wu)$ are equivalent identities in an LA*-semigroup. Consequently, the identity $u(vw) = u(wv)$ also holds in an LA*-semigroup. In [56], Protic defined congruences in LA*-semigroup, left permutable LA-semigroup and decomposed the structures using these congruences. In [13], Distler, Shah and Sorge proved that smallest non-associative LA*-semigroup is of order 6 and these are just nine in number. One of them is given in Table 2.

Table 2. An LA*-semigroup of least order

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

The rule $u(vw) = v(uw)$ is known as a left permutable law. An LA-semigroup \mathbf{L} which satisfies the left permutable law is called a left permutable LA-semigroup. Protic and Bozinovic introduced such LA-semigroups in [54]. A left permutable LA-semigroup \mathbf{L} is always paramedial, that is, $(uv)(wx) = (xv)(wu)$ for every $u, v, w, x \in \mathbf{L}$ but its converse is not true. For instance, Table 3(i) follows that \mathbf{L} is a left permutable groupoid which is also paramedial without being an LA-semigroup while \mathbf{L} is a left permutable groupoid with left identity without

being an LA-semigroup by Table 3(ii).

Table 3. LP-groupoids which are not LA-semigroup

	0	1	2	3	4		0	1	2	3	4
0	0	0	0	0	0	0	3	0	4	4	0
1	0	0	0	2	1	1	4	2	0	0	3
2	0	0	0	1	1	2	0	1	2	3	4
3	0	0	0	2	0	3	0	4	3	3	4
4	0	0	0	1	0	4	4	3	0	0	3
(i)						(ii)					

It is important to mention here that an LA-monoid is always left permutable, but a left permutable groupoid with the left identity may not be an LA-semigroup. For instance, Table 4(i) represents a left permutable groupoid with a left identity 2, but $(1 * 2) * 2 \neq (2 * 2) * 1$ substantiates that \mathbf{L} is not an LA-semigroup.

Table 4. Left permutable groupoid which are not LA-semigroup

*	0	1	2	3	4	*	0	1	2	3	4
0	3	0	4	4	0	0	2	2	2	2	2
1	4	2	0	0	3	1	3	4	2	0	1
2	0	1	2	3	4	2	2	2	2	2	2
3	0	4	3	3	4	3	2	2	2	2	2
4	4	3	0	0	3	4	2	1	2	2	4
(i)						(ii)					

On the other hand, Table 4(ii) represents a left permutable groupoid without being an LA-semigroup.

The following proposition (Proposition 2.2 in [40]) ensures the existence of an LA-monoid and the succeeding theorem (Theorem 2.3 in [40]) correlates LA-semigroups with the commu-

tative semigroups.

Proposition 1 *If $e \in \mathbf{L}$ is a left identity of \mathbf{L} , then it is unique.*

Theorem 1 *If $e \in \mathbf{L}$ is a right identity of \mathbf{L} , then \mathbf{L} is a commutative semigroup.*

In an LA-semigroup \mathbf{L} with left identity e , an element u^{-1} of \mathbf{L} is a right (left) inverse of $u \in \mathbf{L}$ if $uu^{-1} = e$ ($u^{-1}u = e$). Also, if u^{-1} is a left inverse of u , then $uu^{-1} = (eu)u^{-1} = (u^{-1}u)e = ee = e$. Consequently, any left inverse is also the right inverse in \mathbf{L} and so is the inverse. In particular, if $v \in \mathbf{L}$ is another left inverse of u , then $u^{-1} = eu^{-1} = (vu)u^{-1} = (u^{-1}u)v = ev = v$. This means that left inverse of each element in \mathbf{L} is unique. Moreover, every LA-group contains one idempotent element only, which is its left identity.

The following theorem (Theorem 1 in [42]) presents a necessary and sufficient condition for transforming \mathbf{L} into an abelian group. Some additional conditions are also investigated for such an LA-semigroup \mathbf{L} .

Theorem 2 *For any LA-semigroup \mathbf{L} , the following statements are equivalent:*

- (i) $u = (wv \cdot uv)w$ for all u, v, w in \mathbf{L} ;
- (ii) there exists a commutative group $(\mathbf{L}, *)$ such that $uv = v * u^{-1}$ for all u, v in \mathbf{L} ;
- (iii) \mathbf{L} is cancellative with left identity e and that $u^2 = e$ for all u in \mathbf{L} ;
- (iv) $e \in \mathbf{L}$ is a left identity and $u^2 = e$ for all u in \mathbf{L} .

An LA-semigroup \mathbf{L} satisfying the identity $(uv)u = u(vu)$ for each $u \in \mathbf{L}$ is locally associative LA-semigroup. A locally associative LA-monoid is defined analogously. Mushtaq and Iqbal [45] defined powers in \mathbf{L} as follows: For any u in \mathbf{L} , we put $u^1 = u$ and $u^{n+1} = u^n u$, where $n \in \mathbb{N}$. In \mathbf{L} , if $u^n u = u = uu^n$, for all $u \in \mathbf{L}$, then it has associative powers. We have taken the following propositions from [45] to explain the concept of associative powers in an arbitrary locally associative LA-monoid $\mathbf{L}_{\mathbf{M}}$.

Proposition 2 *Every $\mathbf{L}_{\mathbf{M}}$ has associative powers.*

Proposition 3 $u^m u^n = u^{m+n}$ for all $u \in \mathbf{L}_{\mathbf{M}}$, and $m, n \in \mathbb{N}$.

Proposition 4 $(u^m)^n = u^{mn}$ for all $a \in \mathbf{L}_M$, and $m, n \in \mathbb{N}$.

Proposition 5 $(uv)^n = u^n v^n$ for all $u, v \in \mathbf{L}_M$ and for a positive integer $n \geq 1$.

There is at least one element in every semigroup whose square is equal to itself, and therefore all powers are equal to itself (Proposition 1.2.3 in [24]). This element is known as an idempotent. A semigroup with all idempotent elements is known as band. An idempotent element in \mathbf{L} is defined analogously to the semigroup. The set of all idempotent elements in \mathbf{L} is denoted by $E(\mathbf{L})$. An LA-semigroup \mathbf{L} with all idempotent elements is known as LA-band. It is important to mention here that there are LA-semigroups of finite order which do not have any idempotent element. For example, Table 5 substantiates the existence of a finite LA-semigroup containing no idempotent element.

Table 5. An LA-semigroup containing no idempotent element

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

An idempotent element z is called left zero (right zero) if $zu = z$ ($uz = z$) for all $u \in \mathbf{L}$. A zero element is an idempotent element z , which is left as well as right zero of \mathbf{L} , that is, $zu = z$ and $uz = z$ for all $u \in \mathbf{L}$. A right zero LA-semigroup (left zero LA-semigroup) is an LA-semigroup in which each element is a right zero (left zero). An LA-semigroup with zero element, in which the product of two elements is always zero is called a zero LA-semigroup. A zero LA-semigroup is indeed a commutative semigroup.

A reflexive, anti-symmetric, and transitive relation \leq on an LA-semigroup \mathbf{L} is called partial order. The pair (\mathbf{L}, \leq) is called partial order set (abbreviated as poset). A natural partial order on \mathbf{L} is the partial order defined by using the binary operation in \mathbf{L} . This natural partial order was introduced by Hartwig [22], Nambooripad [49] and Mitsch [39] for a semigroup \mathbf{S} separately.

They also investigated many important results by using the multiplication of semigroup. The band $E(\mathbf{S})$ provides a good opportunity to collect information on the semigroup \mathbf{S} . A natural partial order on $E(\mathbf{S})$ is defined by

$$e_1 \leq e_2 \text{ if and only if } e_1 = e_1 e_2 = e_2 e_1, \quad \text{for all } e_1, e_2 \in E(\mathbf{S}).$$

Vagner introduced such an order for an arbitrary inverse semigroup \mathbf{S} as follows:

$$u \leq v \text{ if and only if } u = ev, \quad \text{for all } e \in E(\mathbf{S}).$$

Bozinovic, Protic and Stevanovic introduced the same notion for an LA-semigroup \mathbf{L} [3]. For example, consider $\mathbf{L} = \{0, 1, 2, 3\}$ having three idempotent elements 1, 2 and 3.

Table 6. An LA-semigroup with more than one idempotents

	0	1	2	3
0	2	3	0	3
1	3	1	3	3
2	0	3	2	1
3	3	3	3	3

Then, it is easy to observe that the relation $\leq : \{(1, 1), (2, 2), (3, 3), (3, 1)\}$ is a natural partial order with respect to the binary operation of \mathbf{L} defined in Table 6. The reason for showing the concern towards these natural partial orders is that such an order supply more knowledge on an LA-semigroup in a specific way since it follows the binary operation in a special sense.

A reflexive, symmetric, and transitive relation on \mathbf{L} is called an equivalence relation. A congruence relation is an equivalence relation ρ on \mathbf{L} which is compatible with respect to binary operation of \mathbf{L} in the following way:

$$u \leq v \text{ implies that } uv \leq uv \text{ and } uw \leq vw, \text{ for all } u, v, w \in \mathbf{L}.$$

A non-empty subset \mathbf{K} of \mathbf{L} is left ideal of \mathbf{L} if every product of the form lk such that $l \in \mathbf{L}$ and $k \in \mathbf{K}$. A right ideal of \mathbf{L} is defined analogously. Also, if \mathbf{K} is left as well as right ideal of \mathbf{L} , then \mathbf{K} is called ideal of \mathbf{L} . An ideal \mathbf{P} of \mathbf{L} is prime ideal if for any two ideals \mathbf{K}_1 and \mathbf{K}_2 of \mathbf{L} , $\mathbf{K}_1\mathbf{K}_2 \subseteq \mathbf{P}$ implies either $\mathbf{K}_1 \subseteq \mathbf{P}$ or $\mathbf{K}_2 \subseteq \mathbf{P}$. An LA-semigroup \mathbf{L} is called right(left) simple, if \mathbf{L} does not contain any right(left) ideals. For more details about the ideals of an LA-semigroup, the readers are referred to [47].

In [53], Protic and Stevanovic introduced a law by which an LA*-semigroup \mathbf{L} is a commutative semigroup if $\mathbf{L} = \mathbf{L}^2$. They also introduced the notion of LA-band which is an LA-semigroup whose all elements are idempotent elements [55]. One can observe that there is no left identity in an LA-band, because if it contains left identity, then the structure transforms into a commutative semigroup.

1.3 Graphs of LA-semigroups

The definitions and concepts regarding graphs of semigroups have been taken from PhD thesis of Distler [12]. Let U_1 be a set of vertices and $E_1 \subseteq U_1 \times U_1$ be a set of edges. If $e = (u_1, u_2) \in E_1$, then u_1 represents the initial vertex of an edge e , and u_2 is the terminating vertex. The pair (U_1, E_1) is called a digraph or directed graph.

If $\Gamma_2 = (U_2, E_2)$ is a second graph, then $\Gamma_1 \cup \Gamma_2$ is a graph $(U_1 \cup U_2, E_1 \cup E_2)$. A bijective mapping $\sigma : U_1 \rightarrow U_2$ between the vertices of two graphs Γ_1 and Γ_2 is isomorphic if: $(u_1, u_2) \in E_1$ if and only if $(\sigma(u_1), \sigma(u_2)) \in E_2$. In [12], Distler developed a scheme to find diagonals of multiplication tables of semigroups by defining a relationship between diagonals and certain digraphs.

A digraph is connected if every two of its vertices are connected. Otherwise it is called disconnected graph. A graph which can be embedded in a plane is called a planar graph. Khan, Mushtaq and Anis discussed planar graphs for LA-semigroups, LA-monoids and LA-bands [29]. According to them, a graph is n -partite, $n \geq 1$, if it is possible to partition the set of vertices U into n subsets U_1, U_2, \dots, U_n (are called partite sets) such that every element of E joins a vertex U_i to a vertex U_j , $i \neq j$. The sets U_1, U_2, \dots, U_n are called partite sets. For $n = 2$, graphs are called bipartite graphs, and $n = 3$ graphs are called tripartite graphs.

A subset $U = \{u_1, u_2, \dots, u_m\}$ of an LA-semigroup \mathbf{L} is called generating set if every element of \mathbf{L} is a product of finite length of the elements from U . Every element of U is a generator and we often write $\mathbf{L} = \langle U \rangle$ or $\mathbf{L} = \langle u_1, u_2, \dots, u_m \rangle$. An LA-semigroup \mathbf{L} , which is completely generated by a single element $u \in U$ is called cyclic or monogenic LA-semigroup. If $\mathbf{L} = \langle u \rangle = \{u^n \mid n \in \mathbb{N}\}$ is a finite monogenic LA-semigroup, then there are $m, r \in \mathbb{N}$ for which $u^{m+r} = u^m$. The least values of m and r are called index and period of the generator u . It is important to mention here that in any semigroups \mathbf{S} , due to associativity, we can put brackets on any two consecutive elements appearing in the following product: $s_1 s_2 \dots s_m$ for all $s_1, s_2, \dots, s_m \in \mathbf{S}$. But, in an LA-semigroup \mathbf{L} , we write $((u_1 u_2) u_3) \dots u_m$ in lieu of $u_1 u_2 u_3 \dots u_m$ for all $u_1, u_2, u_3, \dots, u_m \in U$. Consequently, $u^m = (((u u) u) \dots) u$ for any $u \in \mathbf{L}$ and $m \in \mathbb{N}$.

A Cayley diagram, also called a Cayley colour graph is a graphical expression of a group. It is used to conceal/ciphers the abstract structure of any group. Generally, if $\langle U \mid R \rangle$ is the presentation of an LA-semigroup \mathbf{L} , where U and R denote the set of generators and relations respectively. Here, we define $\Gamma = (\mathbf{L}, E)$ a Cayley graph of an LA-semigroup \mathbf{L} , where $E = \{(b, a \cdot b) \mid b \in \mathbf{L}, a \in U\}$. It is clear that the vertices of Γ are the elements of \mathbf{L} and two elements of \mathbf{L} are connected by an edge if and only if any generator in U maps one to the other. Different colours are used to differentiate edges related with different generators in these graphs. In this section, theorems and examples are taken from [29]. The following theorem explains that under certain conditions the subspace of a vector space turns out to be an LA-semigroup.

Theorem 3 *Let W_1 be a sub-space of a vector space V over the field F of cardinality $2r$ such that $r > 1$ and $*$ on W_1 is as follows: $w_1 * w_2 = \alpha^r w_1 + \alpha w_2$, where $\alpha \in F \setminus \{0\}$ is a generator and $w_1, w_2 \in W_1$. Then $(W_1, *)$ is an LA-semigroup. Such an LA-semigroup $(W_1, *)$ is called an LA-semigroup defined by a vector space $(V, +, \cdot)$.*

Remark 4 *If we take $a, b \in F$, taking α as the generator of F and $2r$ as the cardinal of F , then $(F, *)$ is an LA-semigroup defined by Galois field.*

Example 3 *If we take $r = 2$, in remark 4, we get Galois field of order 4. Moreover, consider an irreducible polynomial $x^2 + x + 1$ in $\mathbb{Z}_2 = \{0, 1\}$. Then $GF(2^2) = \{0, 1, u, u^2\}$ and the Galois field is given by the following tables.*

Table 7. Galois field of order 4

\cdot	0	1	u	u^2	+	0	1	u	u^2
0	0	0	0	0	0	0	1	u	u^2
1	0	1	u	u^2	1	1	0	u^2	u
u	0	u	u^2	1	u	u	u^2	0	1
u^2	0	u^2	1	u	u^2	u^2	u	1	0

Example 4 Consider $GF(2^2) \setminus \{0\} = F \setminus \{0\} = \{u : u^3 = 1\} = \{1, u, u^2\}$, and $w_1 \circ w_2 = \alpha^2 w_1 + \alpha w_2$, for all $w_1, w_2 \in F$. By taking $\alpha = u$, we have an LA-semigroup $\{0, 1, u, u^2\}$ whose multiplication table is given below:

Table 8. LA-semigroup over a Galois field of order 4

\circ	0	1	u	u^2
0	0	u	u^2	1
1	u^2	1	0	u
u	1	u^2	u	0
u^2	u	0	1	u^2

Figure 1 shows the Cayley graph of an LA-semigroup defined by Table 8. It is a tripartite, planar disconnected graph.

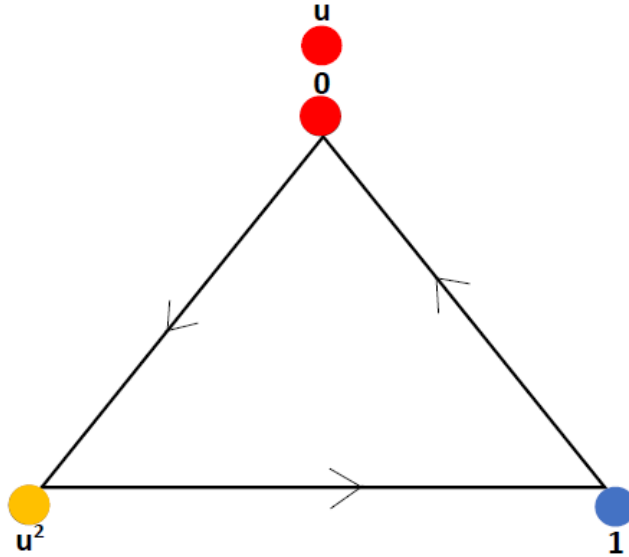


Figure 1. A tripartite, planar disconnected graph.

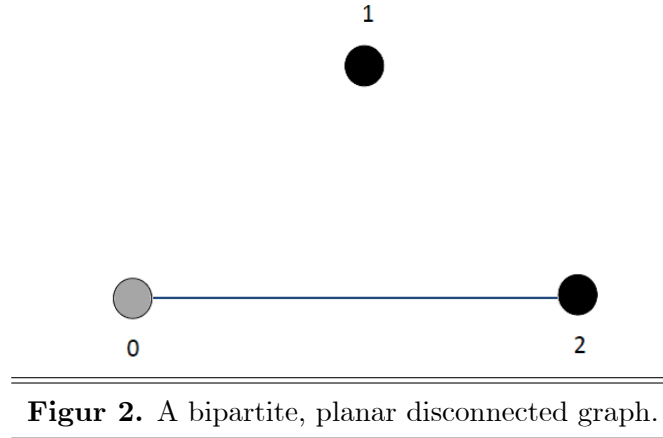
Theorem 5 Let W_1 be a sub-space of a vector space V over a field F of cardinal p^n for some prime $p \neq 2$ and $w_1 \otimes w_2 = \alpha^{\frac{p^n-1}{2}} w_1 + w_2$, where α is a generator of $F \setminus \{0\}$ and $w_1, w_2 \in W_1$. Then (W_1, \otimes) is an LA-monoid.

Example 5 Put $p = 3$ and $n = 1$ in Theorem 5, then $F = \mathbb{Z}_3 = \{0, 1, 2\} \text{ mod } 3$ and $w_1 \otimes w_2 = \alpha w_1 + w_2$, for all $w_1, w_2 \in F$. By taking $\alpha = 2$, we have an LA-monoid whose multiplication table is given below:

Table 9. An LA-monoid of order 3

\otimes	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Figure 2 shows the Cayley graph of an LA-monoid defined by the Table 9.



Example 6 Put $P = 5$ and $n = 1$, in Theorem 5, then we get $|F| = 5$ and $GF(5) = F = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \text{ mod } 5$. By taking $\alpha = 2$, we have the following multiplication table which is an LA-monoid.

Table 10. An LA-monoid of order 5

\otimes	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

Figure 3 represents the Cayley graph of an LA-monoid defined by the Table 10. It is again a bipartite, disconnected graph.

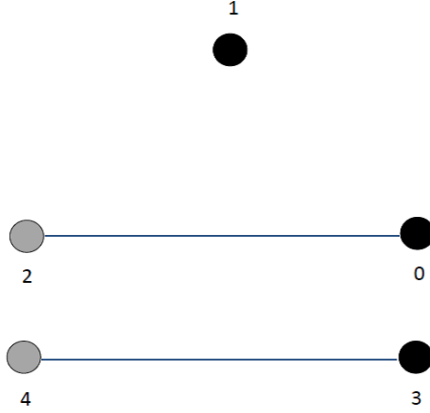


Figure 3. A bipartite, planar disconnected graph.

Theorem 6 Let W_1 be a sub-space of a vector space V over a field F of cardinal r such that $r > 1$ and $w_1 \otimes w_2 = \alpha w_1 + \alpha^2 w_2$, where α is a generator of $F \setminus \{0\}$ and $v_1, v_2 \in W_1$. Then (W_1, \otimes) is an LA-band.

Example 7 Let $|F| = 4$. Then $GF(2^2) \setminus \{0\} = \{u : u^3 = 1\} = \{1, u, u^2\}$. By putting $\alpha = u$ in $w_1 \otimes w_2 = \alpha w_1 + \alpha^2 w_2$, for all $w_1, w_2 \in F$, we have the following multiplication table which is an LA-band.

Table 11. An LA-band of order 4

\otimes	0	1	u	u^2
0	0	u^2	1	u
1	u	1	u^2	0
u	u^2	0	u	1
u^2	1	u	0	u^2

Figure 4 shows the Cayley graph of LA-band defined by the multiplication table 11.

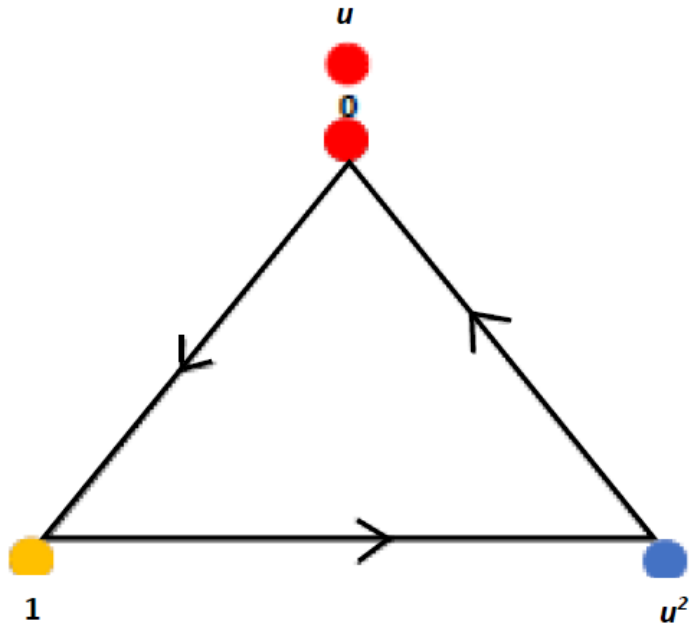


Figure 4. A tripartite planar directed graph.

1.4 Enumeration of Finite LA-semigroups

The first combinatorial result about an associative structure was obtained in 1955 with the help of a computer improvising that there are exactly 126 semigroups of order 4 [20]. Distler in his doctoral thesis [12] investigated that mostly semigroups are nilpotent and have nilpotency rank 3. He also found formulae to calculate the number of semigroups of any order up to isomorphism, and up to anti-isomorphism. A technique to calculate and classify multiplication tables of semigroups and their subclasses is also provided. This scheme incorporates the benefits of computer algebra and constraint satisfaction problem (abbreviated as CSP), to make an effective and rapid search. The difficulty of avoiding isomorphic and anti-isomorphic semigroups is compromised by using standardized schemes of CSPs and keeping the structural properties of the semigroups in mind. Distler used this scheme at various stages, and applied in the GAP and the constraint solver Minion. Consequently, he claimed that there are exactly 52 989 400 714 478 semigroups with 9 elements, 52 991 253 973 742 monoids with 10 elements, and 7 033 090 bands with 10 elements up to isomorphism and anti-isomorphism. In 2012, it was proved

that there are exactly 12 418 001 077 381 302 684 semigroups of order 10 [11]. Currently, after almost 63 years, the number of semigroups is known from order 1 to 10. There is a database of semigroups of order 1 through 8 [14]. Recently in 2015, an important result on the enumeration of finite inverse semigroups arises that there are 7 035 514 642 inverse semigroups of order 15 [38].

The approach to the semigroup enumeration in [11, 38] is based on the idea that any combinatorial enumeration problem can be written as a CSP. Distler and Kelsey in [11] worked out a collection of CSPs whose solutions comprise the semigroups of order which cannot be counted by any previously-known formula and feed those problems to the constraint satisfaction solver Minion. Malandro in [38] also adapted a CSP to count inverse semigroups by adding additional constraints to be satisfied.

In [13], Distler, Shah and Sorge found the enumeration of LA-semigroups in **Table 12** adopting the same approach as in [11]. But the situation is completely different for finite LA-semigroups which are non-associative structure in general. They investigated that there are 28 812 382 776 LA-semigroups of order 6 which are almost 1600 times more than semigroups of the same order out of these 40 104 513 are non-isomorphic to each other.. They obtained these results with the help of GAP, and constraint solver Minion by using both algebraic properties as well as symmetry breaking conditions regarding LA-semigroups to minimize the search. Table 12 is taken from [13].

Table 12. Isomorphic and non-isomorphic solutions of LA-semigroups					
Order n	2	3	4	5	6
Total Solutions	6	105	7 336	3 756 645	28 812 382 776
Time consumed in seconds	∈	∈	∈	25s	104 245s
Non-isomorphic solutions	3	20	331	31 913	40 104 513
Time consumed in seconds	∈	∈	∈	∈	121s

In Table 12, the symbol ∈ denotes the time less than 0.5 seconds. The results were obtained with the help of Minion 0.11 version on a machine with processor 2.80 GHz Intel X-5560.

Chapter 2

INVERSE LA-SEMIGROUPS

2.1 Introduction

Mushtaq and Iqbal introduced the notion of inverse LA-semigroup [46]. They investigated certain basic characteristics of inverses in any inverse LA-semigroup satisfying the identity $(uv)w = v(uw)$ known as inverse LA*-semigroup. They also proved a theorem analogous to Vagner-Preston representation theorem for inverse LA*-semigroups.

In this chapter, we find the fundamentals of inverse LA-semigroups where inverses commute: this includes the algebraic properties of inverse LA-semigroups related with inverses, ideals and homomorphisms. We investigate that a groupoid underlying an inverse LA-semigroup leads us to Green's equivalence relations, $H, \mathfrak{S}, \mathfrak{R}, D$ and J . The relationship $H = \mathfrak{S} = \mathfrak{R} = D = J$ is particularly interesting because inverse LA-semigroups are generally non-commutative and non-associative in nature.

The appearance of more than one idempotent element in an inverse LA-semigroup needs to work in two categories: The Kernel of congruence is the union of the congruence classes contains the idempotent elements and the trace of congruence is the restriction of congruence to the set of idempotent elements. We show that every congruence on an Inverse LA-semigroup is determined by a pair consisting of a normal sub-LA-semigroup and a normal congruence on the set of idempotents. We define a partially ordered function on two posets which is an ordered isomorphism whose inverse also preserves order. Finally, we provide congruences in inverse LA-semigroups by using their kernel and trace.

Definition 2 An LA-semigroup L in which for each $u \in L$, there exists $u' \in L$ such that $(uu')u = u$ and $(u'u)u' = u'$ is called inverse LA-semigroup. Here, u' is called an inverse of u . Let $V(u)$ be the set of all inverses of u . In the future, we use $\mathcal{L} = \{\mathcal{L} : \mathcal{L} \text{ is an inverse LA-semigroup}\}$ to represent the class containing all inverse LA-semigroups. An inverse LA-semigroup \mathcal{L} with a left identity e is inverse LA-monoid (denoted by $\mathcal{L}_{\mathbf{M}}$). Moreover, if \mathcal{L} has a left inverse for each element, that is, $u^{-1} \in \mathcal{L}$ for each $u \in \mathcal{L}$ such that $u^{-1}u = e$, it is called inverse LA-group (denoted by $\mathcal{L}_{\mathbf{G}}$).

We describe basic properties of inverse LA-semigroups in the following results. These results are useful in forthcoming studies. For instance, Lemma 1 explains the relationship of an inverse LA-semigroup and LA-group.

Lemma 1 An inverse LA-semigroup containing only one idempotent as its identity element is an LA-group.

Proof. Let $E(\mathcal{L}) = \{e\}$. Then $u = eu = (uu')u$, and $u' = eu' = (u'u)u'$ for all $u, u' \in \mathcal{L}$, which imply that $uu' = u'u = e$. Consequently, \mathcal{L} is an LA-group. ■

Consider $\mathcal{L} = \{0, 1, 2, 3, 4\}$ as defined by the following multiplication table.

Table 13. Inverse LA-semigroup with a single idempotent element

*	0	1	2	3	4
0	1	0	2	4	3
1	3	2	1	0	4
2	0	3	4	1	2
3	2	4	0	3	1
4	4	1	3	2	0

Then $(0 * 2) * 0 = 0$, $(2 * 0) * 2 = 2$, $(1 * 4) * 1 = 1$, $(4 * 1) * 4 = 4$, $(3 * 3) * 3 = 3$. Hence \mathcal{L} contains a single idempotent element 3, but it is not LA-group.

Also, it seems worthy to point out at this stage that every inverse LA-monoid is not an LA-group. We provide the following examples to substantiate the claim.

Table 14. Inverse LA-monoids

	0	1	2	3	4		0	1	2	3	4	
0	4	1	2	3	0	0	4	2	0	1	3	
1	2	3	1	2	2	1	1	4	3	0	2	
2	1	2	3	1	1	2	3	0	4	2	1	
3	3	1	2	3	3	3	2	3	1	4	0	
4	0	1	2	3	4	4	0	1	2	3	4	
	(i)							(ii)				

Table 14(i) is an inverse LA-monoid having more than one idempotent elements which is not an LA-group. Table 14(ii) is an inverse LA-group with only one idempotent 4 which is in fact its left identity.

In [4], Božinović, Protić and Stevanović provide an example to substantiate that these are inverse LA-semigroups having no idempotents (see Table 15).

Table 15. Inverse LA-semigroup having no idempotents

	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

Lemma 2 *In an inverse LA-monoid inverse of each element is unique.*

Proof. Consider an inverse LA-monoid $\mathcal{L}_{\mathbf{M}} \in \mathcal{L}$ with left identity e , and let $u \in \mathcal{L}_{\mathbf{M}}$, such that v and w are two inverses of u , that is, $(vu)v = v$, $(uw)u = u$, $(wu)w = w$, and $(uw)u = u$. Then, it is easy to prove that $v = w$, which proves the uniqueness of inverses in $\mathcal{L}_{\mathbf{M}}$. ■

Here, we establish some standard results regarding the natural partial orders by using the fundamental properties of an inverse LA-semigroup discussed in Proposition 6. The proposition

6 has been taken from [46]. It elaborates the basic characteristics of inverses in an inverse LA-semigroup $\mathcal{L} \in \mathcal{L}$.

Proposition 6 *Let $\mathcal{L} \in \mathcal{L}$. Then:*

- (i) $e' = e$ for all $e \in E(\mathcal{L})$;
- (ii) $(u')' = u$ for all $u \in \mathcal{L}$;
- (iii) $((((u_1 u_2) u_3) \dots) u_n)' = (((u_1' u_2') u_3') \dots) u_n'$ for all $u_1, u_2, \dots, u_n \in \mathcal{L}$, $n \geq 2$.

Proof. The proofs of (i) and (ii) are available in [46]. We just outline (iii), for $n = 2$, it is clear by definition that $((u_1 u_2) (u_1' u_2')) (u_1 u_2) = ((u_1 u_1') (u_2 u_2')) (u_1 u_2) = ((u_1 u_1') u_1) ((u_2 u_2') u_2) = u_1 u_2$ and $((u_1' u_2') (u_1 u_2)) (u_1' u_2') = ((u_1' u_1) (u_2' u_2)) (u_1' u_2') = ((u_1' u_1) u_1') ((u_2' u_2) u_2') = u_1' u_2'$. Hence, $(u_1 u_2)' = u_1' u_2'$. By induction, it is now straight forward to generalize the result. ■

The following remark has been taken from [4].

Remark 7 *For any $\mathcal{L} \in \mathcal{L}$. If $uu' = u'u$ for any $u \in \mathcal{L}$, then $(u'u)^2 = (u'u)(u'u) = (u'u)(uu') = ((uu')u)u' = uu' = u'u$. Imply that $u'u \in E(\mathcal{L})$.*

2.2 Natural Partial Order

We establish a relation \leq on $\mathcal{L} \in \mathcal{L}$ as follows: $u \leq v$ if and only if $u = ev = ve$ for $u, v \in \mathcal{L}$ and for some idempotent e . This relation can be considered on such an inverse LA-semigroup containing at least one idempotent element

Let Q be a subset of partial order set P . If $b \leq c \in Q$ implies $b \in Q$, then Q is called an order ideal. Moreover, $[b] = \{c \in P : c \leq b\}$ is called the principal or least-order ideal generated by b . More generally, $[Q] = \{c \in P : c \leq a \text{ for some } a \in Q\}$ is an order ideal which is generated by a subset Q of P .

By using the structural properties of an inverse LA-semigroup given in Proposition 6, we approach to the first classical result based on the relation of the natural partial order. We use this concept to prove the succeeding theorem, which is a basis of the forthcoming results. Here, we prove that the relation ' \leq ' is an order ideal.

Lemma 3 Let $\mathcal{L} \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}$, then for any $u, v \in \mathcal{L}$, the following are equivalent:

- (i) $u \leq v$;
- (ii) $u' \leq v'$;
- (iii) $u = (uu')v$.

Proof. (i) \Rightarrow (ii) : Let $u \leq v$. Then $u = ev = ve$ for some $e \in E(\mathcal{L})$. So $u' = ev' = v'e$ by Proposition 6. Hence $u' \leq v'$.

(ii) \Rightarrow (iii) : Let $u' \leq v'$. Then $u' = ev' = v'e$ for some $e \in E(\mathcal{L})$, which implies that $u = ev = ve$. Moreover, $uu' = (eu)u' = (u'u)e = e(uu')$. Thus $u = (uu')v$.

(iii) \Rightarrow (i) : Let $u = (uu')v$. Since uu' is an idempotent, then by definition $u \leq v$. ■

In (ii), it is important to point out that the inversion is not reversing the relation as in group theory or other algebras.

Theorem 8 Let $\mathcal{L} \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}$, and let $a, b, u, v \in \mathcal{L}$.

- (i) If $u \leq v$ and $w \leq x$, then $uw \leq vx$;
- (ii) If $u \leq v$ then $u'u \leq v'v$ and $uu' \leq vv'$;
- (iii) $E(\mathcal{L})$ is an order ideal of \mathcal{L} .

Proof. (i) Let $u \leq v$ and $w \leq x$ then $u = (uu')v$ and $w = (ww')x$. Now $uw = ((uu')v)((ww')x) = ((uu')(ww'))vx$, which implies that $uw \leq vx$.

(ii) It is immediate from Lemma 3 and Theorem 8(i).

(iii) Evidently, $E(\mathcal{L}) \subseteq \mathcal{L}$. Let $u \leq v \in E(\mathcal{L})$, then by definition $u = (uu')v$. This implies that $u \in E(\mathcal{L})$ and $E(\mathcal{L})$ becomes an order ideal of \mathcal{L} . ■

It is interesting to note that the natural partial order is compatible with respect to the multiplication defined in \mathcal{L} . Moreover, the natural partial order defines an order ideal on the set of idempotents of \mathcal{L} .

2.3 Restricted Product and Green's Relations

The smallest left ideal of a semigroup \mathbf{S} is $\mathbf{S}a$ for any element $a \in \mathbf{S}$. In [24], Howie named it a principal left ideal generated by a . The principal right ideal of a semigroup \mathbf{S} is defined analogously. A relation \mathfrak{S} is called left congruence on \mathbf{S} is described as: $a\mathfrak{S}b$ if and only if $\mathbf{S}a = \mathbf{S}b$. Similarly, a right congruence relation \mathfrak{R} is described as: $a\mathfrak{R}b$ if and only if $a\mathbf{S} = b\mathbf{S}$. These relations are introduced by Green in [21]. Moreover, by an alternative characterization in [24], more equivalences H , D and J are defined by taking:

$$\begin{aligned} H &= \mathfrak{S} \cap \mathfrak{R}, D = \mathfrak{S} \vee \mathfrak{R} \\ aJb &\Leftrightarrow \mathbf{S}a\mathbf{S} = \mathbf{S}b\mathbf{S}. \end{aligned}$$

In [34], Lawson defined the relations \mathfrak{S} and \mathfrak{R} in an inverse semigroup S by

$$(u, v) \in \mathfrak{S} \text{ if and only if } u'u = v'v \text{ and } (u, v) \in \mathfrak{R} \text{ if and only if } uu' = vv'.$$

Here, the relation \mathfrak{S} is a right congruence and \mathfrak{R} is a left congruence. By putting $H = \mathfrak{S} \cap \mathfrak{R}$, $D = \mathfrak{S} \circ \mathfrak{R}$, he obtained another equivalence relation. In [16, 17], Dudek and Gigon investigated left permutable inverse LA-semigroups. They also defined Green's relations in a left permutable inverse LA-semigroup and proved some important characteristics of Green's relations satisfying the condition $uu' = u'u$. Here, we define Green's relations in an inverse LA-semigroup $\mathcal{L} \in \mathcal{L}$ by using Lawson's approach. Also, we reproduce some results because it provides an easier way to understand the concepts and there is no need to impose extra conditions which are imposed in [16].

We define mappings $d, r : \mathcal{L} \rightarrow E(\mathcal{L})$, by $d(u) = u'u$ and $r(u) = uu'$ to establish the notion of restricted product in \mathcal{L} . Note that $d(u') = r(u)$ and $r(u') = d(u)$. Let $\mathcal{L} \in \mathcal{L}$, and $u, v \in \mathcal{L}$. Then the restricted product $u \cdot v$ exists only when $u'u = vv'$, which is then equal to uv .

Lemma 4 *Let $\mathcal{L} \in \mathcal{L}$. If $u \cdot v$ exists, then $d(u \cdot v) = d(v)$ and $r(u \cdot v) = r(u)$ for any $u, v \in \mathcal{L}$.*

Proof. If $u \cdot v$ exists, then $u'u = vv'$. Moreover, $d(u \cdot v) = d(uv) = (uv)'(uv) = (u'v')(uv) = (u'u)(v'v)$

$= (v'v)(v'v) = ((v'v)v')v = v'v = d(v)$. The other case is easy to prove analogously. ■

Theorem 9 *Let $\mathcal{L} \in \mathcal{L}$.*

(i) Let $u \in \mathcal{L}$, and e be an idempotent such that $e \leq u'u$. Then $v = ue = eu$ is the unique element in \mathcal{L} such that $v \leq u$ and $v'v = e$.

(ii) Let $u, v \in \mathcal{L}$. Then $uv = u' \cdot v'$ where $u' = eu = ue$ and $v' = ev = ve$ and $e = (u'u)(vv')$.

Proof. (i) If $e \leq u'u$, for any $u \in \mathcal{L}$ and $e \in E(\mathcal{L})$, then by definition $e = e(u'u) = (ee)(u'u) = (eu')(eu)$. Take $v = eu = ue$, which implies that $v \leq u$. Moreover, $v'v = (eu)'(eu) = (eu')(eu) = e(u'u) = e$. For uniqueness, if $w \leq u$, so that $w'w = e$. Then $w = (w'w)u = u(w'w)$. Consequently, $w = ue = eu = v$.

(ii) Consider $u' = eu = ue$, and $v' = ev = ve$, where $e = (u'u)(vv')$. Then $u' \leq u$ and $v' \leq v$. Therefore $d(u') = (u')'u' = (eu)'(eu) = e(u'u) = ((u'u)(vv'))(u'u) = (vv')(u'u) = e$. Similarly, it is easy to see that $r(v') = e$. Which concludes that $u' \cdot v'$ exists. Furthermore, we have $u' \cdot v' = u'v' = (eu)(ev) = e(uv) = ((u'u)(vv'))(uv) = ((uu')u)((vv')v) = uv$. ■

Here, we present Green's equivalence relations \mathfrak{S} , \mathfrak{R} , H , and D in an inverse LA-semigroup. We define \mathfrak{S} and \mathfrak{R} on an inverse LA-semigroup \mathcal{L} by

$$(a, b) \in \mathfrak{S} \text{ if and only if } a'a = b'b \text{ and } (a, b) \in \mathfrak{R} \text{ if and only if } aa' = bb'.$$

Remark 10 *By definition $(u, v) \in \mathfrak{S}$ if and only if $u'u = v'v$. This implies that $uu' = vv'$ if and only if $(u, v) \in \mathfrak{R}$. Consequently, $\mathfrak{S} = \mathfrak{R}$.*

Proposition 7 *Let $\mathcal{L} \in \mathcal{L}$. Then \mathfrak{S} is a congruence relation.*

Proof. It is easy to prove that \mathfrak{S} is reflexive and symmetric by definition. Now, suppose that $(u, v), (v, w) \in \mathfrak{S}$. Then $u'u = v'v$ and $v'v = w'w$. Therefore $(u, w) \in \mathfrak{S}$, and so \mathfrak{S} is transitive. Finally, let $(u, v) \in \mathfrak{S}$ and $a_1 \in \mathcal{L}$. Then

$$(a_1u)'(a_1u) = (a_1'u')(a_1u) = (a_1'a_1)(u'u) = (a_1'a_1)(v'v) = (a_1v)'(a_1v).$$

Similarly

$$(ua_1)'(ua_1) = (va_1)'(va_1).$$

Hence \mathfrak{S} is a congruence relation. ■

Proposition 8 *Let $\mathcal{L} \in \mathcal{L}$ and $v, w \in \mathcal{L}$. Then $v\mathfrak{S} w$ if and only if $\mathcal{L}v = \mathcal{L}w$.*

Proof. If $v\mathfrak{S} w$, then $v'v = w'w$. Further, $v' = (v'v)v' = (w'w)v' = (v'w)w' \Rightarrow v = (vw')w$ and $w = (wv')v$. Therefore $\mathcal{L}v = \mathcal{L}w$. Conversely, if $\mathcal{L}v = \mathcal{L}w$. Then $v = xw$ and $w = yv$ for some $x, y \in \mathcal{L}$, imply that $v'v = (xw)'(xw) = (x'w')(xw) = (x'x)(w'w) \leq w'w$. Similarly $w'w \leq v'v$. Hence $v'v = w'w$. ■

Let H, D , and J are defined exactly the same as for semigroups.

Proposition 9 *Let $\mathcal{L} \in \mathcal{L}$. Then $\mathfrak{S} = \mathfrak{R} = H = D = J$.*

Proof. It is easy to prove from the remark that $\mathfrak{S} = \mathfrak{R}$. ■

Proposition 10 *Let $\mathcal{L} \in \mathcal{L}$ and $v, w \in \mathcal{L}$. If $v\mathfrak{S}w$ and $v \leq w$, then $v = w$.*

Proof. Let $v\mathfrak{S}w$ and $v \leq w$. Then $v'v = w'w$ and $v = (vv')u$, imply that $vv' = ww'$ and $v = (vv')w = (ww')w = w$. ■

2.4 Homomorphisms between Inverse LA-semigroups

The concept of homomorphism between LA-semigroups is the same as in group theory. For example, a mapping $\theta : \mathcal{L} \rightarrow \mathcal{L}$ defined by $\theta(u) = u'$ for all $u \in \mathcal{L}$. Then θ is a homomorphism by virtue of Proposition 6. A mapping $\phi : P_1 \rightarrow P_2$ between two partial order sets P_1 and P_2 is called order preserving, if $u \leq v$ means $\phi(u) \leq \phi(v)$. Furthermore, if ϕ is bijective and ϕ^{-1} is also order preserving, then ϕ is called an order isomorphism.

Proposition 11 *Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{L}$ and $\phi : \mathcal{L}_1 \rightarrow \mathcal{L}_2$ be a homomorphism. Then*

- (i) $\phi(u') = \phi(u)'$ for all $u \in \mathcal{L}_1$;
- (ii) if $\phi(e) \in E(\mathcal{L}_2)$ for all $e \in E(\mathcal{L}_1)$;
- (iii) For $\phi(u) \in E(\mathcal{L}_2)$, there exist $e \in E(\mathcal{L}_1)$ so that $\phi(u) = \phi(e)$;
- (iv) $\text{Im}(\phi)$ is an inverse sub-LA-semigroup of \mathcal{L}_2 ;

(v) For any inverse sub-LA-semigroup S of \mathcal{L}_2 , $\phi^{-1}(S)$ is inverse sub-LA-semigroup of \mathcal{L}_1 ;

(vi) ϕ is an order preserving map;

(vii) if $v, w \in \mathcal{L}_1$ so that $\phi(v) \leq \phi(w)$, then there exist $d \in \mathcal{L}_1$ for which $d \leq w$ and $\phi(d) = \phi(v)$.

Proof. (i) Since

$$(\phi(u)\phi(u'))\phi(u) = (\phi(uu')\phi(u)) = \phi((uu')u) = \phi(u),$$

and

$$(\phi(u')\phi(u))\phi(u') = (\phi(u'u)\phi(u')) = \phi((u'u)u') = \phi(u'),$$

therefore due to uniqueness of inverses, $\phi(u') = \phi(u)'$.

(ii) It is immediate from the fact that $\phi(e)^2 = \phi(e)\phi(e) = \phi(ee) = \phi(e)$.

(iii) If $\phi(u)^2 = \phi(u)$, then $\phi(u'u) = \phi(u')\phi(u) = \phi(u)'\phi(u) = \phi(u)\phi(u) = \phi(u)^2 = \phi(u)$. Since $u'u \in E(\mathcal{L}_1)$, take $u'u = e$, then $\phi(u) = \phi(e)$.

(iv) Since ϕ is a homomorphism and $\text{Im}(\phi)$ is closed under inverses from (i). Therefore, $\text{Im}(\phi)$ is an inverse sub-LA-semigroup of \mathcal{L}_2 .

(v) It is straightforward.

(vi) By definition $u \leq v$ if and only if $u = ev$ for some $e \in E(\mathcal{L}_1)$. Which implies that $\phi(v) = \phi(ev) = \phi(e)\phi(w)$, where $\phi(e)$ is an idempotent. Thus $\phi(v) \leq \phi(w)$.

(vii) Take $d = (vv')w$. Then $d \leq w$ and $\phi(d) = \phi(vv')\phi(w) = \phi(e)\phi(w) = \phi(v)$. ■

2.5 Kernel and Trace

In [4], Božinović, Protić and Stevanović presented the concepts of kernel normal systems of inverse LA^{**}-semigroups. Let η be a congruence on $\mathcal{L} \in \mathcal{L}$. Then kernel of η is defined by $\ker(\eta) = \{a \in \mathcal{L} : \exists e \in E(\mathcal{L}) \wedge (a, e) \in \eta\}$ and trace of η is defined by $\text{tr}(\eta) = \{(e, f) \in \eta : e, f \in E(\mathcal{L})\} = \eta \cap (E(\mathcal{L}) \times E(\mathcal{L}))$, where $E(\mathcal{L})$ denotes the set of idempotents in \mathcal{L} .

If $\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{L}$ such that $\mathcal{L}_2 \subseteq \mathcal{L}_1$, then \mathcal{L}_2 is called inverse sub-LA-semigroup. The inverse sub-LA-semigroup \mathcal{L}_2 is said to be full if $E(\mathcal{L}_2) = E(\mathcal{L}_1)$, and \mathcal{L}_2 is called self conjugate,

if $(a'\mathcal{L})a \subseteq \mathcal{L}_2$ for all $a \in \mathcal{L}_1$. A full, self conjugate \mathcal{L}_2 is called the normal inverse sub-LA-semigroup of \mathcal{L}_1 . A congruence η on the semilattice $E(\mathcal{L}_1)$ is said to be normal if $(e_1, e_2) \in \eta$ implies that $((a'e_1)a, (a'e_2)a) \in \eta$ for all $a \in \mathcal{L}_1$.

Proposition 12 *Let η be a congruence on $\mathcal{L} \in \mathcal{L}$. If $B = \ker(\eta)$ and $\omega = tr(\eta)$, then*

- (i) B is a full inverse sub-LA-semigroup of \mathcal{L} ;
- (ii) For any $u \in \mathcal{L}$ and $e \in E(\mathcal{L})$, if $eu \in B$ and $(e, uu') \in \omega$ then $u \in B$.

Proof. (i) To prove that B is an inverse sub-LA-semigroup of \mathcal{L} . If $u, v \in B$, by definition there exist $e_1, e_2 \in E(\mathcal{L})$ such that $(u, e_1), (v, e_2) \in \eta$. Now $(u, e_1)(v, e_2) = (uv, e_1e_2) \in \eta$. Which immediately implies that $uv \in B$, since $e_1e_2 \in E(\mathcal{L})$. Also $(u', e) \in \eta$ and $e' = e$, imply that $u' \in B$. Now to prove B is full. Obviously $E(B) \subseteq E(\mathcal{L})$. Now let $e \in E(\mathcal{L})$ then $(e, e) \in \eta$ implies that $e \in B$ which immediately follows that $e \in E(B)$. So $E(B) = E(\mathcal{L})$. Thus B is full.

(ii) From $(e, uu') \in \omega$ we get $(eu, (uu')u) \in \eta$. This implies that $(eu, u) \in \eta$. Thus $\eta(eu) = \eta(u)$. But $eu \in B$ implies that $\eta(eu) = \eta(u)$ holds an idempotent, which further implies that $u \in B$. ■

A congruence pair (B, ω) on \mathcal{L} contains a normal inverse sub-LA-semigroup B and a normal congruence ω for which if $ea \in B$ and $(e, aa') \in \omega$ then $a \in B$ and $e \in E(\mathcal{L})$.

Remark 11 *From above results it is clear that $(\ker(\eta), tr(\eta))$ is a congruence pair for every congruence η .*

Proposition 13 *Let η be a congruence on $\mathcal{L} \in \mathcal{L}$.*

- (i) If $(u, v) \in \eta$ then

$$(u', v') \in \eta, (uu', vv') \in \eta \text{ and } (u'u, v'v) \in \eta;$$

- (ii) If $(u, e) \in \eta$, where e is an idempotent, then

$$(u, u') \in \eta, (u, u'u) \in \eta \text{ and } (u, uu') \in \eta.$$

Proof. (i) Let $(u, v) \in \eta$. Then $\eta(u) = \eta(v)$ and by Proposition 11, $\eta(u') = \eta(u)'$ and $\eta(v') = \eta(v)'$. This implies that $\eta(u') = \eta(v')$, that is, $(u', v') \in \eta$. The remaining parts are straight forward to prove. ■

An inverse LA-smigroup \mathcal{L} is called E-unitary if $e \leq u$ for an $e \in E(\mathcal{L})$ implies $u \in E(\mathcal{L})$. A subset B of \mathcal{L} is called left (right) unitary if $b \in B, u \in \mathcal{L}$ and $bu \in B$ ($ub \in B$) imply $u \in B$. A left unitary and right unitary subset of \mathcal{L} is called unitary.

For all $b, c \in \mathcal{L}$, we define a left compatibility relation by $b \rightsquigarrow_l c$ if and only if $bc' \in E(\mathcal{L})$, the right compatibility relation is defined dually. The compatibility relation is a relation which is both left and right compatibility relation. These relations are reflexive and symmetric, but they are not transitive. However, from our investigation, the left compatibility relation and the right compatibility relation coincide in any \mathcal{L} . Because $b \rightsquigarrow_l c$ if and only if $bc' \in E(\mathcal{L})$, therefore $(b'c)^2 = ((bc')')^2 = ((bc')^2)' = (bc')' = b'c$. This implies that $b \rightsquigarrow_r c$. So the left compatibility relation or right compatibility relation is the compatibility relation in \mathcal{L} .

Proposition 14 *Let $\mathcal{L} \in \mathcal{L}$. Then the following assertions are equivalent:*

- (i) $E(\mathcal{L})$ is left unitary;
- (ii) $E(\mathcal{L})$ is right unitary;
- (iii) \mathcal{L} is E-unitary.

Proof. (i) \implies (ii) : If $E(\mathcal{L})$ is left unitary and $ue \in E(\mathcal{L})$ for $e \in E(\mathcal{L})$. By assumption $u \in E(\mathcal{L})$ for $eu, e \in E(\mathcal{L})$ and $u \in \mathcal{L}$. Also, idempotents commute in \mathcal{L} . Then $eu = ue$ and $E(\mathcal{L})$ is right unitary.

(ii) \implies (iii) : If $E(\mathcal{L})$ is right unitary and $e \leq u$ for $e \in E(\mathcal{L})$, and $u \in \mathcal{L}$. Then $e = fu = uf$ for some $f \in E(\mathcal{L})$. Now $uf \in E(\mathcal{L})$ for some $f \in E(\mathcal{L})$ implies that $u \in E(\mathcal{L})$, since $E(\mathcal{L})$ is right unitary. Consequently, \mathcal{L} is E-unitary.

(iii) \implies (i) : If \mathcal{L} is E-unitary. Then for $e \in E(\mathcal{L})$, if $e \leq u$, then $u \in E(\mathcal{L})$. This further implies that $e = fu = uf \in E(\mathcal{L})$ where $f, u \in E(\mathcal{L})$. ■

Theorem 12 *Let $\mathcal{L} \in \mathcal{L}$. Then \mathcal{L} is E-unitary if and only if the compatibility relation \sim is transitive.*

Proof. If \sim is transitive and $e \leq u$ for $e \in E(\mathcal{L})$. Then by definition of natural partial order $e = fu = uf$ and $e = fu' = u'f$. From both cases $fu', f'u \in E(\mathcal{L})$. Therefore $u \sim e$. By assumption $e \leq u'$, and so, $e \leq u'u$ by Theorem 8. This further implies that $e \sim u'u$. Now by transitivity $u \sim u'u$, that is, $(u'u)'u = (uu')u = u \in E(\mathcal{L})$. Therefore, \mathcal{L} is E-unitary.

Conversely, if \mathcal{L} is E-unitary and $u \sim v$ and $v \sim w$. Then $(v'u)(vw') \in E(\mathcal{L})$ and further $(v'u)(vw') = (v'v)(uw') \leq uw'$. Since \mathcal{L} is E-unitary, therefore $uw' \in E(\mathcal{L})$. This implies that $u \sim w$. ■

A congruence ρ on \mathcal{L} is called idempotent pure, if $u \in \mathcal{L}$, $e \in E(\mathcal{L})$ and $(u, e) \in \rho$, then $u \in E(\mathcal{L})$.

Proposition 15 *Let $\mathcal{L} \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}$. Then a congruence ρ on \mathcal{L} is idempotent pure if and only if $\rho \subseteq \sim$.*

Proof. Suppose that ρ is an idempotent pure congruence and $(u, v) \in \rho$. Then $(uv', vv') \in \rho$. Since $vv' \in E(\mathcal{L})$, therefore $uv' \in E(\mathcal{L})$ by assumption. Consequently, $u \sim v$. Conversely, suppose $\rho \subseteq \sim$ and let $(a, e) \in \rho$ for $e \in E(\mathcal{L})$. Then by proposition 13, $(u'u, u) \in E(\mathcal{L})$ and so, $u'u \sim u$. Since $(u'u)'u = (uu')u = u$, therefore $u \in E(\mathcal{L})$. Consequently, ρ is idempotent pure congruence. ■

2.6 Conclusion

In this chapter, we have discussed the fundamentals of an inverse LA-semigroup \mathcal{L} where inverses commute: this includes the algebraic properties of \mathcal{L} related with inverses, natural partial order, ideals, homomorphisms and kernel normal system in \mathcal{L} . Using these interesting properties, we have proved that the set of idempotent elements of \mathcal{L} is an order ideal. We have introduced the notions of restricted product to relate it with the Green's relations in \mathcal{L} . Furthermore, we have investigated a relationship $H = \mathfrak{S} = \mathfrak{R} = D = J$ which is particularly interesting due to the non-commutative and non-associative nature of \mathcal{L} . Finally, we have found congruences on \mathcal{L} by using their kernel and trace.

Chapter 3

LEFT PERMUTABLE INVERSE LA-SEMIGROUPS

3.1 Introduction

A Left permutable inverse LA-semigroup is the LA-semigroup \mathbf{L} satisfying the identity $u(vw) = v(uw)$ for all $u, v, w \in \mathbf{L}$ and contains inverse u' of each element u so that $(uu')u = u$ and $(u'u)u' = u'$. Alternatively, an inverse LA-semigroup \mathcal{L} satisfying the identity $u(vw) = v(uw)$ for all $u, v, w \in \mathcal{L}$ is called left permutable inverse LA-semigroup. We use the symbol \mathcal{L}_p to denote a left permutable inverse LA-semigroup. In this chapter, our discussion surrounds about \mathcal{L}_p in which inverses commute that is, $uu' = u'u$ for all $u \in \mathcal{L}_p$. Let $E(\mathcal{L}_p)$ be the set of idempotents in an \mathcal{L}_p . It is already proved that in an \mathcal{L}_p , $uu' = u'u$ if and only if $uu', u'u \in E(\mathcal{L}_p)$ [4].

Here, we investigate the order-theoretic properties of left permutable groupoids which arise by relating a natural partial order with the compatibility relations. Then, we use these to prove certain results of meets and joins in an \mathcal{L}_p . We discuss homomorphism between two inverse LA-semigroups. Also, we find the conditions under which an \mathcal{L}_p is infinitely distributive. At the end of this chapter, we prove that the $C(\mathcal{L}_p)$ is complete and infinitely distributive.

Before proving some interesting facts of natural partial order, it is essential to point out that every inverse LA-monoid is left permutable inverse LA-semigroup. But all the left permutable inverse LA-semigroups must not hold left identity. An example of the left permutable inverse

LA-semigroup, depicting that it may not contain an identity element is given in Table 16.

Table 16. A left permutable inverse LA-semigroup without any left identity

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

3.2 Natural Partial Order and Compatibility Relations

The following proposition is available in [4]. It establishes a connection between the commutativity of inverses and idempotents of a left permutable inverse LA-semigroup. In this chapter, almost all results of inverse LA-semigroups satisfy the condition discussed in Proposition 16.

Proposition 16 *Let $\mathcal{L}_p \in \mathcal{L}$. Then $uu' = u'u$ if and only if uu' and $u'u$ are idempotents for all $u \in \mathcal{L}_p$.*

Proof. The proof is available in [4]. ■

The following Proposition provides a connection between a left permutable inverse LA-semigroup and LA-group.

Proposition 17 *Every $\mathcal{L}_p \in \mathcal{L}$, in which $uu' = u'u$ for all $u \in \mathcal{L}_p$, with a unique idempotent is precisely an LA-group.*

Proof. Since every LA-group contains a left identity, therefore it is a left permutable inverse LA-semigroup with one idempotent only. Conversely, suppose $\mathcal{L}_p \in \mathcal{L}$ has one idempotent only. Then $uu' = u'u = e$, and $ea = (uu')u = u$ for every $u \in \mathcal{L}_p$. Therefore, \mathcal{L}_p contains a unique left identity e and each element invertible. Hence, \mathcal{L}_p becomes an LA-group. ■

The relation \leq on an \mathcal{L}_p is described as follows: $u \leq v$ if and only if $u = ev$ for some idempotent e .

Before proving that the relation ‘ \leq ’ defined above is a partial order, we use this concept to prove the following lemma, which is a basis of the forthcoming results. It is a modified version of the Lemma 3, we have reproduced this result for a left permutable inverse LA-semigroup because definition of a natural partial is different from previous sense.

Lemma 5 *Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$. Then for all $u, v \in \mathcal{L}_p$, the following are equivalent:*

- (i) $u \leq v$;
- (ii) $u' \leq v'$;
- (iii) $u = (uu')v$.

Proof. It is easy to prove by using Lemma 3. ■

Proposition 18 *Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$. Then*

- (i) \leq is a partial order on \mathcal{L}_p ;
- (ii) $l \leq m$ if and only if $l = lm = ml$ for all $l, m \in E(\mathcal{L}_p)$.

Proof. (i) Reflexivity is clear from $u = (uu')u$. Now let $u \leq v$ and $v \leq u$. Then $u = (uu')v$ and $v = (vv')u$, so that $u = (uu')v = (uu')((vv')u) = (vv')((uu')u) = (vv')u = v$. Therefore \leq is antisymmetric. Suppose that $u \leq v$ and $v \leq w$. Then $u = (uu')v$ and $v = (vv')w$. Hence $u = (uu')v = (uu')((vv')w) = (uu')(w(vv')) = (w(vv'))(u'u) = ((u'u)(vv'))w$, that is $u \leq w$.

(ii) If $l \leq m$. Then $l = em$ for some $e \in E(\mathcal{L}_p)$. Moreover, $lm = l$ and $ml = (mm)l = (lm)m = lm = l$. The converse is obvious. ■

Let (P, \leq) be a partial order set. If $w \leq u, v$, then w is known as a lower bound of u and v . If w is the largest lower bound among all the pairs u and v , then w is said to be the greatest lower bound and written as $u \wedge v$. A meet-semilattice is a partial order set containing the greatest lower bound for every pair of elements.

Now we prove some important conditions which relate a compatibility relation to a natural partial order defined on any \mathcal{L}_p .

Lemma 6 Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$. If $u \smile v$ for $u, v \in \mathcal{L}_p$, then the greatest lower bound $u \wedge v$ of u and v exists and

$$(u \wedge v)' (u \wedge v) = ((u'u) v') v.$$

Proof. If $u \smile v$, then by definition $uv', u'v \in E(\mathcal{L}_p)$. Let $z = (uv') v = (vv') u$. Then $z \leq v$ and $z \leq u$. If $w \leq u$ and $w \leq v$, then $ww' \leq uv'$ and so $w = (ww') w \leq (uv') v = z$ by Theorem 8(i). Hence $z = u \wedge v$. Moreover,

$$\begin{aligned} z'z &= ((uv') v)' ((uv') v) = ((uv')' v') ((uv') v) \\ &= ((u'v) v') ((uv') v) = ((u'v) (uv')) (v'v) \\ &= ((u'u) (vv')) (u'u) = ((u'u) v') ((vv') v) = ((u'u) v') v. \end{aligned}$$

■

Lemma 7 Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$. If $u \smile v$ for $u, v \in \mathcal{L}_p$, then

$$u \wedge v = (uv') v = (u'v) v = (vv') u = (vv) u' = (vu') u = (v'u) u.$$

Proof. It is immediate by the fact that $u \wedge v = (uv') v$. Since uv' is an idempotent, so obviously $uv' = (uv')' = u'v$. ■

Lemma 8 Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$. Then for any $u, v, w, x \in \mathcal{L}_p$,

- (i). $u \smile v$ and $w \smile x$ imply that $uw \smile vx$;
- (ii). $u \leq v$, $w \leq x$ and $v \smile x$ imply $u \smile w$.

Proof. (i) If $u \smile v$ and $w \smile x$, then $uv', wx' \in E(\mathcal{L}_p)$. Also, $(uw)(vx)' = (uw)(v'x') = (uv')(wx') \in E(\mathcal{L}_p)$, therefore $uw \smile vx$.

(ii) Let $u \leq v$, $w \leq x$ and $v \sim x$. Then $u = (uu')v$, $w = (ww')x$ and $vx' \in E(\mathcal{L}_p)$. This implies that

$$\begin{aligned} uw' &= ((uu')v)((ww')x)' = ((uu')v)((w'w)x') \\ &= ((uu')(w'w))(vx') \in E(\mathcal{L}_p). \end{aligned}$$

Hence $u \sim w$. ■

A subset B of \mathcal{L} is called compatible, if each pair in B is compatible.

Lemma 9 For elements u, v, w of $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$.

(i) $v \sim w$ and $vv' \leq w'w$ imply $v \leq w$;

(ii) $[u]$ is a compatible subset of \mathcal{L}_p .

Proof. (i) It is obvious.

(ii) Let $v, w \in [u] = \{v \in \mathcal{L}_p : v \leq u\}$, therefore $v \leq u$ and $w \leq u$, which imply that $v = eu$ and $w = fu$. Hence $vw' = (eu)(fu)' = (eu)(fu') = (ef)(uu') \in E(\mathcal{L}_p)$. Consequently, $[u]$ is a compatible subset of \mathcal{L}_p . ■

We use a single word subset instead of a non-empty subset throughout this section.

Lemma 10 Let $\mathcal{L} \in \mathcal{L}$ and B be a set of idempotent elements. Then

(i) $\wedge B$ is an idempotent, if it exists;

(ii) $\vee B$ is an idempotent, if it exists.

Proof. (i) It is straight forward because the set of idempotent elements is an order ideal.

(ii) If $b = \vee B$. Then for all $e \in B$, we have $e \leq b$ and $e \leq b'b$ by Theorem 8(ii). Consequently, $b \leq b'b$. ■

Lemma 11 Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$ and let $T = \{t_i : i \in I\}$ be a subset of \mathcal{L}_p , and $t = \vee T$. Then $t_1 \sim t_2$ for all $t_1, t_2 \in T$.

Proof. Let $t_1, t_2 \in T$. Then by definition $t_1, t_2 \leq t$. Therefore by Lemma 8(ii), we have $t_1 \sim t_2$. ■

Proposition 19 Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$ and let $T = \{t_i : i \in I\}$ be a subset of \mathcal{L}_p .

- (i) If $\vee t_i$ exists, then $\vee t_i t'_i$ exists and $(\vee t_i) (\vee t_i)' = \vee t_i t'_i$.
- (ii) If $\vee t_i$ exists, then $\vee t'_i t_i$ exists and $(\vee t_i)' (\vee t_i) = \vee t'_i t_i$.

Proof. (i) If $t = \vee t_i$, then $t_i \leq t$ implies that $t_i t'_i \leq t t'$. Furthermore, $t t'$ is an upper bound of $\{t_i t'_i : i \in I\}$. Suppose that $t_i t'_i \leq b$ for some $b \in \mathcal{L}_p$. Then $(t_i t'_i) t_i \leq b t_i \leq b t$ for each $i \in I$. Certainly, $t = \vee t_i \leq b t$. Moreover, $t = (t t') (b t) = b ((t t') t) = b t$ by Lemma 5, which directly means that $t t' = (b t) t' = (t' t) b$. It follows that $t t' \leq b$. Hence $\vee t_i t'_i = t t'$.

(ii) It is obvious due to (i). ■

Proposition 20 Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$ and let $T = \{t_i : i \in I\}$ be a subset of \mathcal{L}_p .

- (i) If $t = \vee t_i$ and $t_i t'_i \leq u'u$ for each $i \in I$. Then $\vee t_i u$ exists and $tu = \vee t_i u$.
- (ii) If $t = \vee t_i$ and $t'_i t_i \leq uu'$ for each $i \in I$. Then $\vee u t_i$ exists and $ut = \vee u t_i$.
- (iii) If $t = \wedge t_i$ exists, then $\wedge t_i u$ exists and $\wedge t_i u = tu$.
- (iv) If $t = \wedge t_i$ exists, then $\wedge u t_i$ exists and $\wedge u t_i = ut$.

Proof. (i) If $t = \vee t_i$. Then $t_i \leq t$, which follows that $t_i u \leq tu$. Thus tu is an upper bound of $\{t_i u : i \in I\}$. If $t_i u \leq b$ for some $b \in \mathcal{L}_p$. Then $(t_i u) u' \leq b u'$ implies that $(u'u) t_i \leq b u'$. Since $t_i t'_i \leq u'u$, therefore $(t_i t'_i) t_i \leq (u'u) t_i \leq b u'$. Hence $t_i \leq b u'$. It is then immediate that $tu \leq (b u') u = (u u') b \leq b$ and $tu = \vee t_i u$.

(ii) It is obvious from (i).

(iii) Since $t \leq t_i$, therefore $tu \leq t_i u$ and so tu is a lower bound of $\{t_i u : i \in I\}$. If $b \leq t_i u$ for some $b \in \mathcal{L}_p$. Then $b u' \leq (t_i u) u' = (u'u) t_i \leq t_i$, shows that $b u' \leq \wedge t_i = t$. Moreover, $(b b') b \leq ((t_i u) (t'_i u')) b = ((t_i t'_i) (u u')) b \leq (u u') b = (b u') u \leq tu$. Which immediately implies that $b \leq tu$ and $\wedge t_i u = tu$.

(iv) It is similar to (iii). ■

3.3 Infinitely Distributive Left Permutable Inverse LA-semigroups

Any $\mathcal{L} \in \mathcal{L}$ is left infinitely distributive, if $\vee B$ exists for a subset B of \mathcal{L} , then $\vee aB$ also exists for every $a \in \mathcal{L}$ and $a(\vee B) = (\vee aB)$. The right infinitely distributive is defined dually. Now \mathcal{L} is infinitely distributive if it is left as well as right infinitely distributive. The concept of join lead us to finalize the following assertions about \mathcal{L} .

Proposition 21 *For any $\mathcal{L}_p \in \mathcal{L}$ in which $uu' = u'u$ for all $u \in \mathcal{L}_p$, the following statements are equivalent:*

- (i) \mathcal{L}_p is infinitely distributive;
- (ii) the set of idempotents of \mathcal{L}_p is an infinitely distributive semilattice;
- (iii) for all subsets S and T of \mathcal{L}_p , if $s = \vee S$ and $t = \vee T$, then $\vee ST = (\vee S)(\vee T)$.

Proof. (i) \Rightarrow (ii) : It follows directly from Lemma 10.

(ii) \Rightarrow (iii) : Let $S = \{s_i : i \in I\}$ and $T = \{t_j : j \in J\}$ be any two subsets of \mathcal{L}_p so that $s = \vee S$ and $t = \vee T$. Obviously, st is an upper bound of ST . Now, we just need to show that $\vee ST = st$. Let h be an element which is another upper bounded of ST , such that $s_it_j \leq h$ for every $s_i \in S$ and $t_j \in T$. But $s_i \leq s$ and $t_j \leq t$ such that $(s_i s'_i) (t_j t'_j) = (s_i t_j) (s'_i t'_j) \leq h (s'_i t'_j)$. By definition $E(\mathcal{L}_p)$ is infinitely distributive, therefore

$$(ss') (t_j t'_j) = (((\vee S)(\vee S)') (t_j t'_j)) = (\vee (s_i s'_i)) (t_j t'_j) = \vee ((s_i s'_i) (t_j t'_j)) \text{ by Proposition 19.}$$

But $(s_i s'_i) (t_j t'_j) \leq h (s'_i t'_j)$ implies that $(ss') (t_j t'_j) \leq h (s'_i t'_j)$. Since $E(\mathcal{L})$ is infinitely distributive, therefore

$$(ss') (tt') = (ss') ((\vee T)(\vee T)') = (ss') (\vee (t_j t'_j)) = \vee ((ss') (t_j t'_j)) \text{ by Proposition 19.}$$

Consequently, $(ss') (tt') \leq h (s'_i t'_j)$. This implies that

$$st = (((ss') s) ((tt') t)) = ((ss') (tt')) (st) \leq (h (s'_i t'_j)) (st) = (h (st)') (st) \leq (hh') h = h.$$

Hence $st = \vee ST$.

(iii) \Rightarrow (i) : It is immediate from (iii). ■

A subset T of $\mathcal{L} \in \mathcal{L}$, which is a compatible order ideal is called a permissible subset of \mathcal{L} . Here, $C(\mathcal{L})$ represents the set of all permissible subsets of \mathcal{L} . Notice that if $\mathcal{L} \in \mathcal{L}$, then $E(\mathcal{L})$ is permissible and for each $a \in \mathcal{L}$, $[a]$ is also permissible.

Lemma 12 *Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$ and let T be a permissible subset of \mathcal{L}_p .*

(i) If $t_1, t_2 \in T$ and $t_1 t'_1 = t_2 t'_2$, then $t_1 = t_2$;

(ii) Both $T'T = \{t't : t \in T\}$, $TT' = \{tt' : t \in T\}$ and so $T'T = TT'$ is order ideal of \mathcal{L}_p .

Proof. (i) If $t_1, t_2 \in T$, then $t_1 \sim t_2$. Additionally, $t_1 t'_1 = t_2 t'_2$ follows that $(t_1 t'_1) t_1 = (t_2 t'_2) t_1 = (t_1 t'_2) t_2$, and so $t_1 \leq t_2$. Similarly, $t_2 \leq t_1$. Thus $t_1 = t_2$.

(ii) Let $st' \in TT'$ for all $s, t \in T$. If $s \sim t$, then $u = (st')t = s \wedge t$ by Lemma 7. Since T is an order ideal, so $u \in T$. Moreover,

$$\begin{aligned} uu' &= ((st')t)((st')t') = (s't)((st')t') = (s't)((t't)(st')) \\ &= (s't)(s((t't)t')) = (s't)(st') = (st')'(st') = st'. \end{aligned}$$

Thus $TT' \subseteq \{tt' : t \in T\}$. The converse is obvious. Now let $e \leq ss'$. Take $t = es$. Then $t \leq s$ so that $t \in S$. But $tt' = (es)(es') = (ee)(ss') = e(ss')$, implies that $tt' \leq ss'$. Hence $tt' \in SS'$. Therefore SS' is an order ideal of \mathcal{L}_p . ■

An inverse LA-semigroup \mathcal{L} is said to be complete if every non-empty compatible subset has a join. Define a mapping $\iota : \mathcal{L} \longrightarrow C(\mathcal{L})$ by $\iota(u) = [u]$.

Theorem 13 *Let $\mathcal{L}_p \in \mathcal{L}$ and $uu' = u'u$ for all $u \in \mathcal{L}_p$. Then $C(\mathcal{L}_p)$ is a complete and infinitely distributive left permutable inverse LA-semigroup. Moreover, the mapping $\iota : u \longrightarrow [u]$ is an embedding of \mathcal{L}_p into $C(\mathcal{L}_p)$.*

Proof. Initially, we need to show that $C(\mathcal{L}_p) \in \mathcal{L}$. For this, we begin by proving the closure law under multiplication of subsets. Let $C, D \in C(\mathcal{L}_p)$. Now to prove that $CD \in C(\mathcal{L}_p)$, assume that $s \leq cd$ for some $s \in \mathcal{L}_p$, $c \in C$ and $d \in D$. Then $s = (s's)(cd) = c((s's)d)$. Since $(s's)d \leq d$, and D is an order ideal, therefore $(s's)d \in D$. Consequently, $s \in CD$ and CD is an

order ideal. To show that CD is compatible subset of \mathcal{L}_p , let $cd, ef \in CD$ where $c, e \in C$ and $d, f \in D$. But $(cd)'(ef) = (c'd')(ef) = (c'e)(d'f)$. By assumption $c'e$ and $d'f$ are idempotents. Thus $(cd)'(ef)$ is an idempotent. Similarly, $(cd)(ef)'$ is an idempotent. Hence $CD \in C(\mathcal{L}_p)$.

Next we show that $C(\mathcal{L}_p)$ is closed under inverses. We need to prove that if $T \in C(\mathcal{L})$, then $T' \in C(\mathcal{L}_p)$ such that $(TT')T = T$. First we prove that T' is an order ideal. Assume $s \leq t'$ for $s \in \mathcal{L}_p$ and $t \in T$. Then $s = (ss')t'$ and so $s' = (s's)t = (s'(s'))t$. Thus $s' \leq t$, that is $s' \in T$, because T is an order ideal. Hence $s \in T'$. Consequently, T' is an order ideal. To show that T' is compatible subset of \mathcal{L}_p . Consider two elements a' and b' of T' . As ab' and $a'b$ are idempotents, the elements $(a')'b' = ab'$ and $a'(b')' = a'b$ are idempotents. Hence T' is a compatible subset of \mathcal{L}_p . Consequently $T' \in C(\mathcal{L}_p)$. Next we prove that $(TT')T = T$. Evidently, $T \subseteq (TT')T$. Conversely, if $(bc')d \in (TT')T$ where $b, c, d \in T$. Since $bc' = tt'$ for some $t \in T$ by Lemma 12, therefore $(bc')d = (tt')d = (dt')t$. Moreover, take $dt' = zz'$ for some $z \in T$ by Lemma 12; then $(bc')d = (tt')d = (dt')t = (zz')t = t$ and $(TT')T \subseteq T$. Consequently, $(TT')T = T$.

We now describe the natural partial order \leq in $C(\mathcal{L}_p)$ defined by $S \leq T$ if and only if $S = (SS')T$. We show that $S \leq T$ for $S, T \in C(\mathcal{L}_p)$ if and only if $S \subseteq T$. Let $S, T \in C(\mathcal{L}_p)$ so that $S \leq T$. Let $s \in S$ be an arbitrary element. Then $s = (xx')t$ for some $x \in S$ and $t \in T$. Hence $s \leq t$ imply that $s \in T$ because T is an order ideal. Thus $S \subseteq T$. Conversely, assume that $S \subseteq T$. As $s = (ss')s$ and $s \in S \subseteq T$, it is obvious that $S \subseteq (SS')T$. To show the converse inclusion, let $(ss')t \in (SS')T$ be an arbitrary element ($s \in S, t \in T$). Since $S \subseteq T$, therefore $s \sim t$ and so $ts' \in E(\mathcal{L}_p)$. Hence $(ss')t = (ts')s$ implies $(ss')t \leq s$, that is $(ss')t \in S$, because S is an order ideal of \mathcal{L}_p . Consequently, $(SS')T \subseteq S$. Hence $S = (SS')T$. As $SS' = \{ss' : s \in S\}$, and $S'S = \{s's : s \in S\}$, we have $SS' = S'S$. Thus $C(\mathcal{L}_p) \in \mathcal{L}$.

Now we show that $S \sim T$ if and only if $SUT \in C(\mathcal{L}_p)$. Suppose $SUT \in C(\mathcal{L}_p)$. Then, for every $s \in S$ and $t \in T$, the elements $s't$ and st' are idempotents. Thus, for example, $s't = (s't)(s't) \in (S'T)(S'T)$ implying that $S'T \subseteq (S'T)(S'T)$. If $s_1, s_2 \in S$ and $t_1, t_2 \in T$ are arbitrary elements, then $(s'_1t_1)(s'_2t_2) \leq s'_2t_2 \in S'T \in C(\mathcal{L}_p)$ and so $(s'_1t_1)(s'_2t_2) \in S'T$. Hence $(S'T)(S'T) \subseteq S'T$. Consequently, $(S'T)(S'T) = S'T$, that is, $S'T$ is an idempotent of $C(\mathcal{L}_p)$. This implies that $S \sim T$. Conversely, if $S \sim T$ then $S'T$ is an idempotent of $C(\mathcal{L}_p)$. Now we show that $SUT \in C(\mathcal{L}_p)$ for $S, T \in C(\mathcal{L}_p)$. First we prove that SUT is compatible subset of

\mathcal{L}_p . For this, let $s_1, t_1 \in SUT$. Since S and T are compatible order ideals of \mathcal{L}_p . Then for some $s_2, t_2 \in SUT$, it is clear that $s_1 \leq s_2$ and $t_1 \leq t_2$. Hence $s_1 = es_2$ and $t_1 = ft_2$ for some $e, f \in E(\mathcal{L}_p)$. Thus $s_1 t_1' = (es_2)(ft_2)' = (es_2)(ft_2') = (ef)(s_2 t_2')$ implies that $s_1 t_1' \in E(\mathcal{L}_p)$ because $S \sim T$ and product of idempotents is again an idempotent. Consequently, SUT is a compatible subset of \mathcal{L}_p . Next we prove that SUT is order ideal of \mathcal{L}_p . Evidently, $SUT \subseteq \mathcal{L}_p$. The fact that $s \leq t \in SUT$ implies $s \leq t \in S$ or $s \leq t \in T$. In both cases $a \in SUT$ because S and T are compatible order ideals of \mathcal{L}_p . Hence $SUT \in C(\mathcal{L}_p)$, that is, the join of a compatible subset is just the union of its elements. Which immediately implies that $C(\mathcal{L}_p) \in \mathcal{L}$ is a complete infinitely distributive.

The function $\iota(s) = [s]$ is well defined being the compatible subset. It is obvious that the mapping ι is injective. Next to prove that $[s][t] = [st]$, let $u \in [s][t]$. Then $u = ab$ with $a \leq s$ and $b \leq t$. Hence $u = ab \leq st$, and so $u \in [st]$. Conversely, if $u \in [st]$ then $u \leq st \in [s][t]$. Which immediately tells that ι is a monomorphism. ■

3.4 Conclusion

First of all, we have improved some fundamental results for a left permutable inverse LA-semigroup based on results from the previous chapter. We have proved that every left permutable inverse LA-semigroup with a unique idempotent element in which inverses commute is an LA-group. We have also related the natural partial order with the compatibility relations in a left permutable inverse LA-semigroup. By using these relations, we have investigated the complementary behaviour of meets and joins. We have found the conditions under which a left permutable inverse LA-semigroup is infinitely distributive. At the end, we have proved that the set of all permissible subsets of a left permutable inverse LA-semigroup is complete and infinitely distributive.

Chapter 4

ENUMERATION OF FINITE INVERSE LA-SEMIGROUPS

4.1 Introduction

There has always been a necessity of the development of dynamical algorithms for the classification of algebraic structures of associative and non-associative types. Since LA-semigroups are non-associative in general. Therefore, our interest lies in developing an algorithm for the classification of LA-semigroups generally and inverse LA-semigroups particularly. In this regard, first of all, we investigate some fundamental results of inverse LA-semigroups which enable us to minimize our search of enumerating finite inverse LA-semigroups. We present partial classification of inverse LA-semigroups up to order 6 and inverse LA-monoids up to order 8. For this, we develop these results with the help of an efficient algorithm which we develop in C-Sharp. In Table 16, which provides the comparative study of the number of LA-semigroups and the number of semigroups up to order 6. The enumeration results regarding semigroups and LA-semigroups are taken from [10] and [13] respectively.

Table 17. Number of Semigroups and LA-semigroups up to order 6

n			2	3	4	5	6
Semigroups	Ref. [10]	Total Solutions	8	113	3 492	183 732	17 061 118
		Non-isomorphic	5	24	188	1 915	28 634
LA-semigroups	Ref. [13]	Total Solutions	6	105	7 336	3 756 645	28 812 382 776
		Non-isomorphic	3	20	331	31 913	40 104 513

The most recent result on the enumeration of LA-semigroup is that there are exactly 28 812 382 776 LA-semigroups of order 6 [13]. This result is obtained with the help of Minion 0.11 version on a machine with processor 2.80 GHz Intel X-5560. It takes almost 28.96 hours to complete the task. This chapter marks the first attempt to enumerate finite inverse LA-semigroups specifically. We develop a few algorithms to find the enumeration of various classes of LA-semigroups up to order n . On the bases of these algorithms, we develop a user-friendly Windows based machine Left Almost Semigroup Algebraic Machine (LASAM) in C-sharp. We run LASAM on a machine with processor 2.3 GHz Intel X-E5-2699v3 18c which produces all the LA-semigroups of order 6 in almost 22.3 hours. This proves the correctness and efficiency of our algorithm. Moreover, LASAM is capable of enumerating LA-semigroups, inverse LA-semigroups and their subclasses. It is a user-friendly windows based machine (see Figure 5).

One of the main features of LASAM is that it finds all equivalent solutions by providing any solution to the underlying problem. The algorithm also deals with algebraic questions related to enumeration and classification of finite LA-semigroups and subclasses like LA*-semigroups, LA**-semigroups, LA-monoids, LA-bands, LA-3-bands, Locally associative LA-semigroups, inverse LA-semigroups, inverse LA*-semigroups, inverse LA**-semigroups, inverse LA-bands, inverse LA-3-bands, inverse LA-monoids, and locally associative inverse LA-semigroups. It is also possible to select all non-isomorphic solutions for any of the subclasses of LA-semigroups.

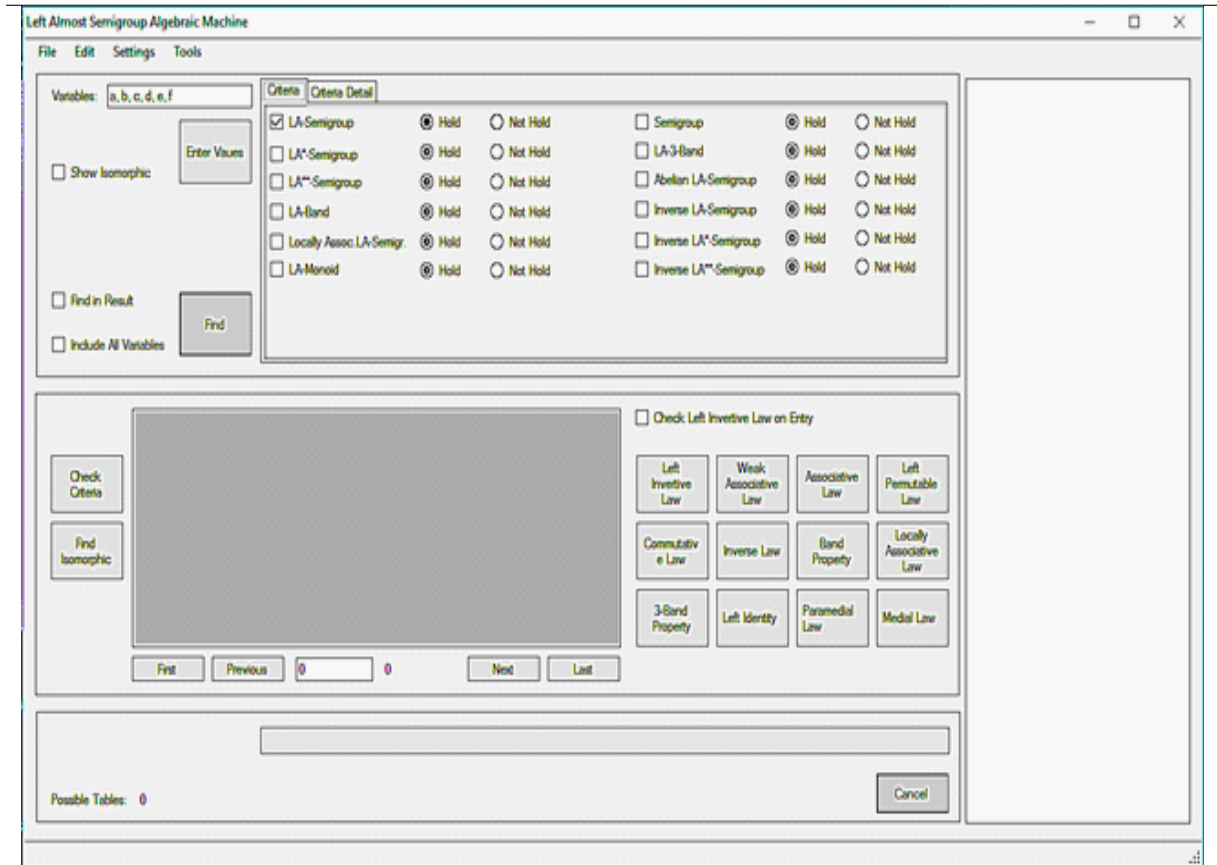


Figure 5. An image of newly developed Left Almost Semigroup Algebraic Machine.

An inverse LA-semigroup satisfying associative law $(ab)c = a(bc)$ is inverse left invertive semigroup (abbreviated as inverse LI-semigroup). Before describing the methodology used for enumeration of inverse LA-semigroups, we prove an important result. This result is instrumental in setting up a link between inverse LI-semigroup, inverse LA*-semigroup and commutative inverse LA-semigroup. It also provides us an opportunity to enumerate any one class from the three classes of inverse LA-semigroups.

Theorem 14 *For any $\mathcal{L} \in \mathcal{L}$, the following statements are equivalent:*

- (i) \mathcal{L} is an inverse LI-semigroup;
- (ii) \mathcal{L} is an inverse LA*-semigroup;

(iii) \mathcal{L} is commutative inverse LA-semigroup.

Proof. (i) \implies (ii) : Suppose that \mathcal{L} is an inverse LI-semigroup. Then \mathcal{L} is commutative, because for all $a, b, c \in \mathcal{L}$,

$$\begin{aligned} ab &= a((bb')b) = a(b(b'b)) = (ab)(b'b) \\ &= ((b'b)b)a = ((bb')b')a = (bb')(b'a) \\ &= (bb')(ba) = ((bb')b)a = ba, \end{aligned}$$

which directly states that $(ab)c = (cb)a = (bc)a = b(ca)$. Commutativity also implies that $(ab)c = b(ac)$.

(ii) \implies (iii) : If \mathcal{L} is an inverse LA*-semigroup, then $a(bc) = a(cb)$ for all $a, b, c \in \mathcal{L}$. Furthermore, we note that

$$\begin{aligned} ab &= ((aa')a)b = a((aa')b) = a((ba')a) = (aa)(ba') = (aa)(a'b) \\ &= a((a'b)a) = a((ab)a') = (a'a)(ab) = (a'a)(ba) \\ &= (a'b)(aa) = b(a'(aa)) = b((aa')a) = ba. \end{aligned}$$

Hence \mathcal{L} is commutative.

(iii) \implies (i) : From this it follows that, for every $a, b, c \in \mathcal{L}$, we have $(ab)c = (ba)c = a(bc)$.

■

4.2 Methodology for Enumeration of Finite Inverse LA-semigroups

To find all the inverse LA-semigroups of a certain order n , first, we find all LA-semigroups for n . These are huge in number as compared to semigroups [13]. The difference in numbers of semigroups and LA-semigroups of the same order is examined in Table 16. We have stored each solution of LA-semigroups and inverse LA-semigroups of orders 2 to 6 on the hard disk. Further, we have also stored each solution of inverse LA-monoids of orders 2 to 8. All these solutions are available in the form of text files. We note that the file containing all LA-semigroups of order 6 occupy 107 GB space for storage while for the file containing all LA-semigroups of order 5 it

was just 111 MB. It seems thousands of terabytes space is required to store all LA-semigroups of order 7 and above. We have developed our own machine named LASAM which is capable of doing enumeration up to order n . The two main factors which prevent us from working for higher orders are storage space and time limit. To avoid the storage space problem, we decide to enumerate the subclasses of LA-semigroups.

The LASAM is entirely based on the approach presented in [15, 13, 38] that any enumeration problem can be expressed as a constraint satisfaction problem (abbreviated as CSP).

Constraint Satisfaction Problem

A CSP is a set of limitations or restrictions which must satisfy a defined set of objects or variables, answerable by constraint solver techniques. More details about the class of CSPs are available in [11]. Mostly, the CSPs are highly symmetric. Symmetries are essential part of the problem, or may be generated in the process of expressing a problem in terms of a CSP. There are many solutions which are equivalent in the sense of a given problem. A CSP is constructed for each multiplication table representing generally an LA-semigroup or in particular an inverse LA-semigroup. The set of variables $\Delta := \{L_{11}, L_{12}, \dots, L_{1n}, L_{21}, \dots, L_{2n}, \dots, L_{n1}, \dots, L_{nn}\}$, consists of each entry in any $n \times n$ table. The main constraints are:

1. Each variable in Δ has a domain $\{1, 2, 3, \dots, n\}$.
2. $(a * b) * c = (c * b) * a$ for all possible values of a, b , and c in Δ .
3. For each element $a \in \Delta$, there exists a unique element $b \in \Delta$ such that $(a * b) * a = a$ and $(b * a) * b = b$.

The first constraint known as element constraint, is the domain $\mathbf{D} := \{1, 2, 3, \dots, n\}$. Each entry in the $n \times n$ multiplication table is filled with an element from the domain. Elements are repeatable in any row (column). Second constraint is the left invertive law, which in the algorithm is enforced by using element constraints. The constraint element $(vector, i, Val)$ specifies, in any solution $vector[i] = val$ [11]. We add a new variable $A_{((a,b),c)}$ for each triple $((a, b), c)$. The pair of constraints

element $(column(c), a * b, A_{((a,b),c)})$ and element $(column(a), c * b, A_{((c,b),a)})$.

It then implements left invertive law for each possible triple from the domain set. Constraint **1** turns n^2 variables into ground variables that is, $\{1, 2, 3, \dots, n\}$. While constraint **2** and **3** enforces to reduce the search space by implementing the left invertive law and inverse law.

In a first step, we use the underlying algebra that is, the left invertive law to reduce the search space by creating all the constraints of type **2** for a finite set of the variables. After finding all the LA-semigroups of certain finite order, we apply the constraints of type **3** which defines the inverse law to search out inverse LA-semigroups as a subclass of LA-semigroups. We also adjoin multiple constraints like commutative law, associative law, locally associative law, weak associative law, left identity law, left permutable law, band property, 3-band property, paramedial law, and medial law with the constraints of type **2** or type **3** to know more about the enumeration of the sub-classes of LA-semigroups and inverse LA-semigroups.

Theorem 15 *The number of constraints of type 2 for an LA-semigroup of order n is*

$$2\binom{n}{2} + 3\binom{n}{3} = \frac{n^2(n-1)}{2}, \text{ where } n \geq 2 \text{ is a positive integer.}$$

Proof. We prove this by mathematical induction. For this, we use Pascal triangle. For $n = 2$, $\mathbf{D} := \{a, b\}$, the possible triples produced are $((a, a), b)$ and $((b, b), a)$ only. They are equivalent to $((b, a), a)$ and $((a, b), b)$ respectively. For $n = 3$, $\mathbf{D} := \{a, b, c\}$, has three subsets containing two elements and one subsets containing three elements that is, \mathbf{D} itself. The the number of possible triples are $(2 \times 3) + (3 \times 1)$, which are $((a, a), b), ((b, b), a), ((a, a), c), ((c, c), a), ((b, b), c), ((c, c), b), ((a, b), c), ((b, a), c),$ and $((b, c), a)$. If there are some other triples, they are redundant or are equivalent to one of the element obtained earlier. Clearly, the number of triples in both cases satisfies the given formula.

Suppose it is true for $n = k$, that is, the set \mathbf{D} contains k elements. Then \mathbf{D} has $\binom{k}{2} = \frac{k(k-1)}{2}$ subsets with two elements and $\binom{k}{3} = \frac{k(k-1)(k-2)}{6}$ subsets with three elements. Now number of

possible triples are $2\frac{k(k-1)}{2} + 3\frac{k(k-1)(k-2)}{6} = \frac{k^2(k-1)}{2}$. For $n = k + 1$, we have

$$\begin{aligned}
2\binom{k+1}{2} + 3\binom{k+1}{3} &= 2\frac{(k+1)k}{2} + 3\frac{(k+1)k(k-1)}{6} = \\
&= \frac{k+1}{k-1} \left(\frac{2k(k-1)}{2} + \frac{3k(k-1)^2}{6} \right) \\
&= \frac{k+1}{k-1} \left(\frac{2k(k-1)}{2} + \frac{3k(k-1)(k-1)}{6} \right) \\
&= \frac{k+1}{k-1} \left(\frac{2k(k-1)}{2} + \frac{3k(k-1)(k-2+1)}{6} \right) \\
&= \frac{k+1}{k-1} \left(\left(\frac{2k(k-1)}{2} + \frac{3k(k-1)(k-2)}{6} \right) + \frac{3k(k-1)}{6} \right) \\
&= \frac{k+1}{k-1} \left(\frac{k^2(k-1)}{2} + \frac{3k(k-1)(k-2)}{6} \right) \\
&= \frac{k^2(k-1)}{2} + \frac{k(k+1)}{2} = \frac{k(k+1)(k+1)}{2} = \frac{(k+1)^2 k}{2},
\end{aligned}$$

showing that it is also true for $n = k + 1$. Hence the given statement is true for all positive integers $n \geq 2$. ■

By using the preceding Theorem, the minimum number of constraints of type **2** to find an LA-semigroup are given in Table 18.

Table 18. Minimum Number of constraints of type 2									
Order	2	3	4	5	6	7	8	9	10
Minimum number of constraints	2	9	24	50	90	147	224	324	450

The On-Line Encyclopedia of Integer Sequences (abbreviated as OEIS) [60] has many sequences of enumerations of algebraic and combinatorics structures. The sequence that is presented in Table 18 is A006002: the minimum number of constraints of type **2** is required to be satisfied to find an LA-semigroup of order n . It is also interesting to note that the sum of non-triangular numbers between successive triangular numbers,

$1, (2), 3, (4, 5), 6, (7, 8, 9), 10, (11, 12, 13, 14), 15, (16, 17, 18, 19, 20),$
 $21, (22, 23, 24, 25, 26, 27), 28, (29, 30, 31, 32, 33, 34, 35),$
 $36, (37, 38, 39, 40, 41, 42, 43, 44), 45,$
 $(46, 47, 48, 49, 50, 51, 52, 53, 54), \dots, (\text{Sum of terms in brackets}).$

is exactly the same sequence which is presented in Table 18.

Algorithm 1 *Algorithm for finding all LA-semigroups of certain order n .*

Our designed enumeration scheme is strictly based on the CSP. As demonstrated in Figure 6, an algorithm for finding all LA-semigroups of certain order is given below.

Step 1: Select n elements from the set containing numbers, characters and alphabets.

Step 2: Form an empty multiplication table of order $n \times n$ depending upon the selected elements in Step 1.

Step 3: Generate all the left invertive laws by following the preceding Theorem 15.

Step 4: Apply all the generated identities of left invertive law to fill each entry of the table obtained in Step 2.

Step 5: Consider all options separately, if there are multiple options to fill any one entry of the table. Moreover, delete the option where any of the identities obtained in Step 3 is violated.

Step 6: All LA-semigroups of order n are available on the respective location of the hard drive as text files. Currently, these results are available in the display window of LASAM which can be accessed one by one using the next button.

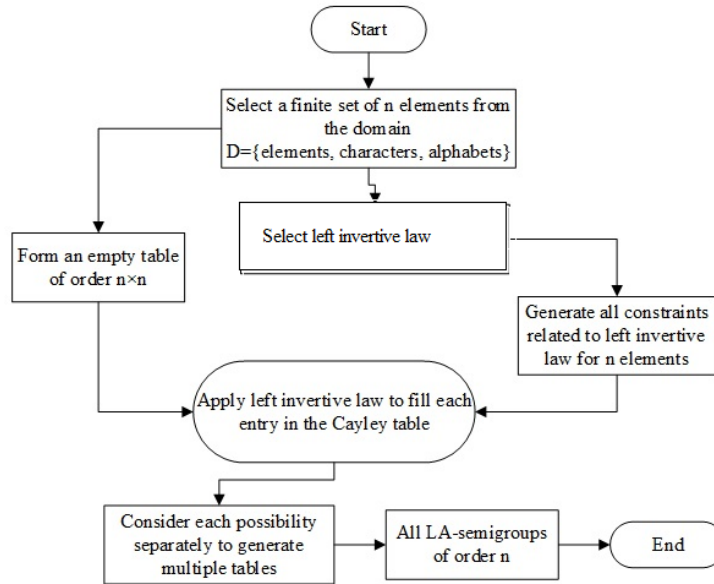


Figure 6. Proposed enumeration scheme for finding LA-semigroups of order n .

The implementation of Algorithm 1 in LASAM for finding all LA-semigroups is explained in Code 1.

Code 1

Find the enumeration of LA-semigroups up to order n .

```

private bool LeftInvertiveLaw(ref string[,] matrix)
{
    int limit = n;
    bool complete = true;
    for (int i = 0; i < limit; i++)
    {
        for (int j = 0; j < limit; j++)
        {
            for (int k = i + 1; k < limit; k++)
            {
                string a = input[i];
            }
        }
    }
}
  
```

```

        string b = input[j];
        string c = input[k];
        string abc = "", cba = "";
        string ab = matrix[i, j];
        if (ab != "" && ab != null)
            abc = matrix[Array.IndexOf(input, ab), k];
        string cb = matrix[k, j];
        if (cb != "" && cb != null)
            cba = matrix[Array.IndexOf(input, cb), i];
        if (abc != cba && abc != "" && cba != "" && abc != null && cba != null)
        {
            if (showViolation)
                MessageBox.Show("(" + a + b + ")" + c + " = (" + c + b + ")" + a,
"Violation of Left Invertive Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
            return false;
        }
        if (abc == "" || cba == "" || abc == null || cba == null)
            complete = false;
    }
}
}
}
if (complete)
    return true;
else
    return this.radioButtonLeftInvertiveHold.Checked;
} \
private void buttonLeftInvertive_Click(object sender, EventArgs e)
{
    if (CheckEmpty())
        return;

```



```

FillMatrix(ref mainMatrix);
showViolation = true;
if (LeftInvertiveLaw(ref mainMatrix))
    MessageBox.Show("Left Invertive Law Holds", "", MessageBoxButtons.OK, Mes-
sageBoxIcon.Information);
    showViolation = false;
}

```

Algorithm 2 *Algorithm for finding all inverse LA-semigroups of certain order n .*

Designed scheme is strictly based on algorithm 1. As demonstrated in Figure 7, an algorithm for proposed scheme is given below.

Step 1: Select n elements from the set containing numbers, characters and alphabets.

Step 2: Generate the all LA-semigroups of order n for selected elements..

Step 3: Generate all the sets of possibilities of inverse law for selected n elements.

Step 4: Apply all the generated sets of inverse laws on each multiplication table of LA-semigroup generated in step 2. Select the all multiplication tables obeying any set of inverse laws completely and discard the others.

Step 5: All inverse LA-semigroups of order n are available on the respective location of the hard drive as text files. Currently, these results are available in the display window of LASAM which can be accessed one by one using the next button.

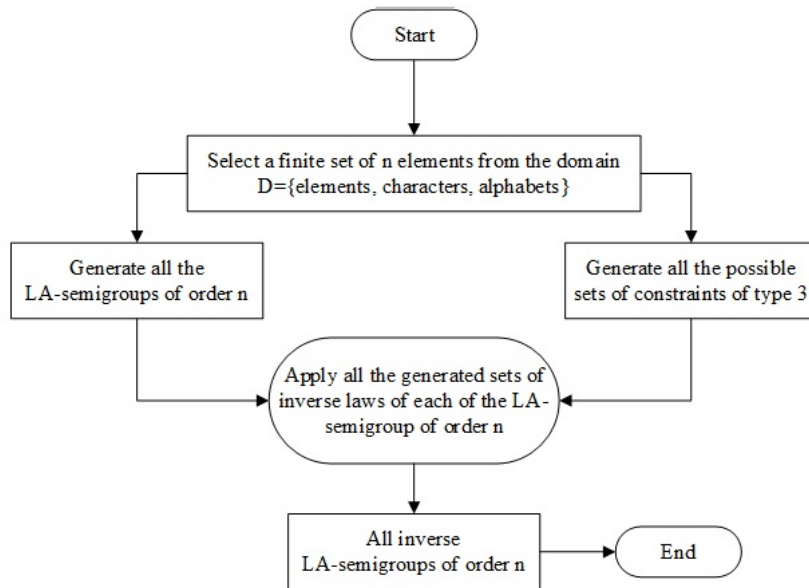


Figure 7. Proposed enumeration scheme for finding all inverse LA-semigroups of order n .

The implementation of Algorithm 2 in LASAM for finding the inverse LA-semigroups of certain order n is given in Code 2.

Code 2

Find the enumeration of inverse LA-semigroups up to order n .

Source code for the enumeration scheme for finding the inverse LA-semigroup discussed in Figure 7 is given below:

```

private bool InverseLaw(ref string[,] matrix)
{
    bool complete = true;
    string[] inverse = new string[n];
    for (int i = 0; i < n; i++)
    {
        for (int j = i; j < n; j++)
        {
            string a = input[i];

```

```

string b = input[j];
string aba = "", bab = "";
string ab = matrix[i, j];
string ba = matrix[j, i];
int index_ab = -1;
int index_ba = -1;
if (ab != "" && ab != null)
{
    index_ab = Array.IndexOf(input, ab);
    aba = matrix[index_ab, i];
}
if (ba != "" && ba != null)
{
    index_ba = Array.IndexOf(input, ba);
    bab = matrix[index_ba, j];
}
if (aba == a && bab == b)
{
    if (inverse[i] == null && inverse[j] == null)
    {
        inverse[i] = b;
        inverse[j] = a;
    }
}
if (this.checkBoxRestrictInverseLaw.Checked && this.checkBoxFindInResult.Checked)
{
    if (a != b && ab != ba)
    {
        if (showViolation)
            MessageBox.Show("Restriction 1 does not satisfy.", "Violation
of Inverse Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
        return false;
    }
}

```

```

        }
    }
    if (this.checkBoxRestrictInverseLawProduct.Checked & &
this.checkBoxFindInResult.Checked)
    {
        {
            if (matrix[index_ab, index_ab] != ab || matrix[index_ba,
index_ba] != ba)
                {
                    if (showViolation)
                        MessageBox.Show("Restriction 2 does not satisfy.",
"Violation of Inverse Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
                    return false;
                }
            }
        }
    }
    else
    {
        if (showViolation)
            MessageBox.Show("Inverse of " + a + " or " + b + " already
exist for another variable.", "Violation of Inverse LA-Semigroup", MessageBoxButtons.OK,
MessageBoxIcon.Warning);
        return false;
    }
}
if (aba == "" || bab == "" || aba == null || bab == null)
    complete = false;
}
}

```

```

if (complete)
{
    for (int k = 0; k < n; k++)
    {
        if (inverse[k] == null)
        {
            if (showViolation)
                MessageBox.Show("Inverses of all variables do not exist.", "Violation of
Inverse LA-Semigroup", MessageBoxButtons.OK, MessageBoxIcon.Warning);
            return false;
        }
    }
    return true;
}
else
    return this.radioButtonInverseLawHold.Checked;
}

```

Isomorphism Rejection

An isomorphism of LA-semigroups indicates an action between the set of elements in two multiplication tables which transforms one table to the other. If we have a permutation ϕ of the elements of A , we transform the given Cayley table by permuting the rows according to ϕ , then to each column. We obtain an isomorphic multiplication table by permuting the values at the end. An anti-isomorphism is an action followed by transposing the resulting multiplication table of an isomorphism. For example, by applying the permutation (b, d) on the table 19 (*i*) is given in table 19 (*iii*). Tables 19 (*i*) and 19 (*iii*) are isomorphic. If A has n elements, then the number of maximum multiplication tables isomorphic to LA-semigroup A are $n!$.

Table 19. A multiplication table is mapped to another multiplication

under permutation (1 3)

	0	1	2	3	4		0	3	2	1	4		0	1	2	3	4		
0	1	4	4	0	0	apply (1 3) \implies	0	3	4	4	0	0	arrange rows columns \implies	0	3	0	4	4	0
1	0	1	1	4	4		3	0	3	3	4	4		1	4	4	0	3	3
2	0	1	2	3	4		2	0	3	2	1	4		2	0	1	2	3	4
3	4	0	0	2	1		1	4	0	0	2	3		3	0	2	3	0	4
4	4	0	0	1	1		4	4	0	0	3	3		4	4	3	0	0	3
	(i)						(ii)						(iii)						

We reduce the search space by selecting any one of the two as a representative of these isomorphic multiplication tables and discarding the remaining ones.

Algorithm 3 *Algorithm for finding all non-isomorphic LA-semigroups of certain order n.*

The main purpose of designing this scheme is to reduce the space on hard disk which surely enables us to analyze the multiplication tables more easily and critically. We use all permutations to find isomorphic tables corresponding to each permutation as in Table 19 and to reduce the space by selecting just one multiplication table from all the isomorphic tables of each class representative instead of considering all isomorphic multiplication tables. The following algorithm gives the detailed description of the proposed scheme as demonstrated in Figure 8.

Step 1: Generate all LA-semigroups of order n.

Step 2: Generate all the permutations from the set for which all LA-semigroups are generated.

Step 3: Apply all the permutations on an LA-semigroup say \mathbf{L}_1 and find all the LA-semigroups isomorphic to \mathbf{L}_1 from the list generated in Step 1.

Step 4: Save \mathbf{L}_1 as representative of this class at another location and delete all others LA-semigroups isomorphic to \mathbf{L}_1 (generated in Step 3) from set of all LA-semigroups generated in

Step 1.

Step 5: Repeat the Steps 3 and 4 for the remaining LA-semigroups and save the representatives of each class on the same location as \mathbf{L}_1 .

Step 6: All isomorphic LA-semigroups of order n are available on the respective location of the hard drive as text files. Currently, these results are available in the display window of LASAM which can be accessed one by one using the next button.

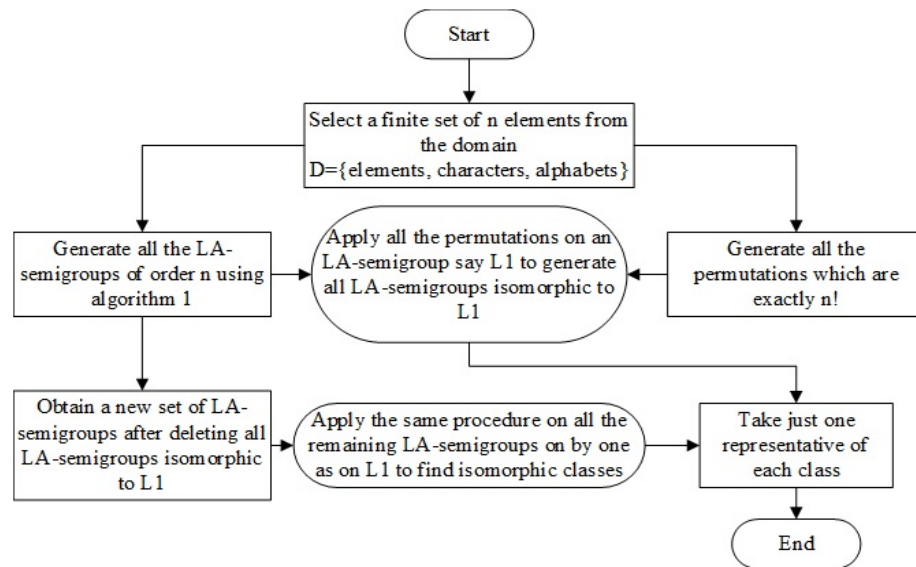


Figure 8. Proposed enumeration scheme for finding non-isomorphic LA-semigroups.

The implementation of Algorithm 3 for finding the non-isomorphic LA-semigroups or its subclasses are presented in Code 3.

Code 3

Find all non-isomorphic inverse LA-semigroups up to order n .

```

public void ProcessIsomorphic(object parameter)
{
    string[] th_Values = (string[])parameter;
    List<string> resultsTemp = new List<string>();
    List<string> resultsNew = new List<string>();
  
```

```

OpenResults(th_Values[0], ref resultsTemp);
Hashtable results = new Hashtable();
for (int i = 0; i < resultsTemp.Count; i++)
results.Add(resultsTemp[i], "");
List<string> isomorphic = new List<string>();
for (int i = 0; i < resultsTemp.Count; i++)
{
if (results.ContainsKey(resultsTemp[i]))
{
isomorphic.Clear();
mainMatrix = StringToMatrix(resultsTemp[i]);
FindIsomorphic(ref mainMatrix, ref isomorphic);
for (int j = 0; j < isomorphic.Count; j++)
{
if (isomorphic[j] != resultsTemp[i])
results.Remove(isomorphic[j]);
}
}
}
foreach (string mString in results.Keys)
resultsNew.Add(mString);
if (resultsNew.Count > 0)
{
mutex.WaitOne();
completed += resultsNew.Count;
mutex.ReleaseMutex();
this.SetCompletedTables(completed.ToString());
SaveResults(OutputDirectory + th_Values[1] + "0.bin", ref resultsNew);
}
}

```


4.3 Enumeration Results

The enumeration results for non-associative inverse LA-semigroups are given in Table 20.

n		3	4	5	6
Inverse LA-semigroups	Total Solutions	6	104	1 841	47 256
	Non-isomorphic	2	10	37	165
Inverse LA**-semigroups	Total Solutions	6	96	1 725	44 280
	Non-isomorphic	2	8	32	148
Inverse LA-monoids	Total Solutions	3	60	870	19 170
	Non-isomorphic	1	5	15	60
Inverse LA-bands	Total Solutions	0	2	56	1 296
	Non-isomorphic	0	1	3	8
Inverse LA-3-bands	Total Solutions	0	2	56	1 596
	Non-isomorphic	0	1	3	10
Locally associative Inverse LA-semigroups	Total Solutions	1	50	1 091	29 016
	Non-isomorphic	1	5	22	101
Paramedial Inverse LA-groups	Total Solutions	6	96	1 725	44 280
	Non-isomorphic	2	8	32	148

Table 21. Enumeration results of LA-monoids

n		3	4	5	6	7	8
LA-monoids	Total Solutions	30	448	9, 140	296, 520	12, 999, 084	809, 205, 280
	Non-isomorphic	6	25	107	609	3, 996	31, 872
Non-associative LA-monoids	Total Solutions	3	72	1, 710	63, 180	2, 985, 990	190, 873, 200
	Non-isomorphic	1	6	29	188	1, 359	11, 386

Table 22. Enumeration results of inverse LA-monoids

n		3	4	5	6	7	8
Inverse LA-monoids	Total Solutions	24	256	3 060	59 340	1 428 252	48 005 120
	Non-isomorphic	5	16	42	147	543	2 371
Inverse LA*-monoids	Total Solutions	21	196	2 190	40 170	940 002	31 347 080
	Non-isomorphic	4	11	27	87	3 000	1 259
Inverse LA**-monoids	Total Solutions	24	256	3 060	59 340	1 428 252	48 005 120
	Non-isomorphic	5	16	42	147	543	2 371
Locally ass. inv. LA-monoids	Total Solutions	21	208	2 490	48 000	1 188 852	40 574 480
	Non-isomorphic	4	12	32	111	418	1, 842
Inverse LA- monoid bands	Total Solutions	6	36	380	6 390	157 962	5 396 888
	Non-isomorphic	1	2	5	15	53	222
Inverse LA- monoid 3 bands	Total Solutions	18	160	1 740	32 070	777 462	26 596 040
	Non-isomorphic	3	8	19	62	221	955

Table 23. Enumeration results of non-associative inverse LA-monoids

n		3	4	5	6	7	8
Inverse LA-monoids	Total Solutions	3	60	870	3 195	488 250	16 658 040
	Non-isomorphic	1	5	15	60	243	1 112
Inverse LA**-monoids	Total Solutions	3	60	870	3 195	488 250	16 658 040
	Non-isomorphic	1	5	15	60	243	1 112
Locally ass. inv. LA-monoids	Total Solutions	0	12	300	1 305	248 850	9 227 400
	Non-isomorphic	0	1	5	24	118	583

4.4 Source Code

The code implemented in LASAM consists of thousands of lines of C-sharp. It is not possible to present full code here. Main parts of the code for various structures which are possible to enumerate using LASAM are given below.

Code 4

Find all groupoids or LA-semigroups satisfying weak associative law up to order n .

```
private bool WeakAssociativeLaw(ref string[,] matrix)
    bool complete = true;
    for (int i = 0; i < n; i++)
    {
        for (int j = 0; j < n; j++)
        {
            for (int k = 0; k < n; k++)
            {
                string a = input[i];
                string b = input[j];
                string c = input[k];
                string abc = "", bac = "";
                string ab = matrix[i, j];
                if (ab != "" && ab != null)
                    abc = matrix[Array.IndexOf(input, ab), k];
                string ac = matrix[i, k];
                if (ac != "" && ac != null)
                    bac = matrix[j, Array.IndexOf(input, ac)];
                if (abc != bac && abc != "" && bac != "" && abc != null && bac != null)
                {
                    if (showViolation)
                        MessageBox.Show("(" + a + b + ")" + c + " = " + b + "(" + a + c + ")",
"Violation of Weak Associative Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
```

```

        return false;
    }
    if (abc == "" || bac == "" || abc == null || bac == null)
        complete = false;
    }
}
}
if (complete)
    return true;
else
    return this.radioButtonWeakAssociativeHold.Checked;
}

```

Code 5

Find all associative/non-associative LA-semigroups of a certain order n .

```

private bool AssociativeLaw(ref string[,] matrix)
{
    bool complete = true;
    for (int i = 0; i < n; i++)
    {
        for (int j = 0; j < n; j++)
        {
            for (int k = 0; k < n; k++)
            {
                string a = input[i];
                string b = input[j];
                string c = input[k];
                string abc_l = "", abc_r = "";
                string ab = matrix[i, j];
                if (ab != "" && ab != null)
                    abc_l = matrix[Array.IndexOf(input, ab), k];
            }
        }
    }
}

```

```

        string bc = matrix[j, k];
        if (bc != "" && bc != null)
            abc_r = matrix[i, Array.IndexOf(input, bc)];
        if (abc_l != abc_r && abc_l != "" && abc_r != "" && abc_l != null &
& abc_r != null)
            {
                if (showViolation)
                    MessageBox.Show("(" + a + b + ")" + c + " = " + a + "(" + b + c +
)", "Violation of Associative Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
                return false;
            }
        if (abc_l == "" || abc_r == "" || abc_l == null || abc_r == null)
            complete = false;
    }
}
}
if (complete)
    return true;
else
    return this.radioButtonAssociativeHold.Checked;
}

```

Code 6

Find all commutative/non-commutative LA-semigroups of a certain order n .

```

private bool CommutativeLaw(ref string[,] matrix)
{
    bool complete = true;
    for (int i = 0; i < n; i++)
    {
        for (int j = i + 1; j < n; j++)
        {

```

```

        string a = input[i];
        string b = input[j];
        string ab = matrix[i, j];
        string ba = matrix[j, i];
        if (ab != ba && ab != "" && ba != "" && ab != null && ba != null)
        {
            if (showViolation)
                MessageBox.Show(a + b + " = " + b + a, "Violation of Commutative
Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
            return false;
        }
        if (ab == "" || ba == "" || ab == null || ba == null)
            complete = false;
    }
}
if (complete)
    return true;
else
    return this.radioButtonCommutativeLawHold.Checked;
}
private void buttonCommutativeLaw_Click(object sender, EventArgs e)
{
    if (CheckEmpty())
        return;
    FillMatrix(ref mainMatrix);
    showViolation = true;
    if (CommutativeLaw(ref mainMatrix))
        MessageBox.Show("Commutative Law Holds", "", MessageBoxButtons.OK, Mes-
sageBoxIcon.Information);
    showViolation = false;
}

```

```
}
```

Code 7

Find all LA-bands of a certain order n .

```
private bool LA_Band(ref string[,] matrix)

{
    bool complete = true;
    for (int i = 0; i < n; i++)
    {
        string a = input[i];
        string aa = matrix[i, i];
        if (aa != a && aa != "" && aa != null)
        {
            if (showViolation)
                MessageBox.Show(a + a + " = " + a, "Violation of LA-Band", Message-
BoxButtons.OK, MessageBoxIcon.Warning);
            return false;
        }
        if (aa == "" || aa == null)
            complete = false;
    }
    if (complete)
        return true;
    else
        return this.radioButtonLA_BandHold.Checked;
}
```

Code 8

Find all locally associative LA-semigroups of a certain order n .

```
private bool LocallyAssociativeLaw(ref string[,] matrix)

{
```

```

bool complete = true;
for (int i = 0; i < n; i++)
{
    string a = input[i];
    string aaa_l = "", aaa_r = "";
    string aa = matrix[i, i];
    if (aa != "" && aa != null)
        aaa_l = matrix[Array.IndexOf(input, aa), i];
    if (aa != "" && aa != null)
        aaa_r = matrix[i, Array.IndexOf(input, aa)];
    if (aaa_l != aaa_r && aaa_l != "" && aaa_r != "" && aaa_l != null && aaa_r
!= null)
    {
        if (showViolation)
            MessageBox.Show("(" + a + a + ")" + a + " = " + a + "(" + a + a + ")",
"Violation of Locally Associative Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
        return false;
    }
    if (aaa_l == "" || aaa_r == "" || aaa_l == null || aaa_r == null)
        complete = false;
}
if (complete)
    return true;
else
    return this.radioButtonLocallyAssociativeLawHold.Checked;
}

```

Code 9

Find all LA-3-band of a certain order n .

```

private bool AG_3_Band(ref string[, ] matrix)
{

```



```

bool complete = true;
for (int i = 0; i < n; i++)
{
    string a = input[i];
    string aaa_l = "", aaa_r = "";
    string aa = matrix[i, i];
    if (aa != "" && aa != null)
        aaa_l = matrix[Array.IndexOf(input, aa), i];
    if (aa != "" && aa != null)
        aaa_r = matrix[i, Array.IndexOf(input, aa)];
    if ((aaa_l != aaa_r || aaa_l != a) && aaa_l != "" && aaa_r != "" && aaa_l
!= null && aaa_r != null)
    {
        if (showViolation)
            MessageBox.Show("(" + a + a + ") " + a + " = " + a + "(" + a + a + ") =
" + a, "Violation of AG-3-Band", MessageBoxButtons.OK, MessageBoxIcon.Warning);
        return false;
    }
    if (aaa_l == "" || aaa_r == "" || aaa_l == null || aaa_r == null)
        complete = false;
}
if (complete)
    return true;
else
    return this.radioButtonAG_3_BandHold.Checked;
}

```

Code 10

Find all LA-monoids of a certain order n .

```

private bool LeftIdentityLaw(ref string[, ] matrix)
{

```

```

bool complete = true;
bool[] Identities = new bool[n];
for (int i = 0; i < n; i++)
{
    Identities[i] = true;
    for (int j = 0; j < n; j++)
    {
        string a = input[i];
        string b = input[j];
        string ab = matrix[i, j];
        if (ab != b && ab != "" && ab != null)
            Identities[i] = false;
        if (ab == "" || ab == null)
            complete = false;
    }
}
if (complete)
{
    for (int i = 0; i < n; i++)
        if(Identities[i] == true)
            return true;
    if (showViolation)
        MessageBox.Show("Left Identity Law does not satisfy", "Violation of Left
Identity Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
    return false;
}
else
    return this.radioButtonLeftIdentityLawHold.Checked;
}

```

Code 11

Find all left permutable LA-semigroups of a certain order n .

```
private bool LeftPermutableLaw(ref string[,] matrix)
{
    bool complete = true;
    for (int i = 0; i < n; i++)
    {
        for (int j = i + 1; j < n; j++)
        {
            for (int k = 0; k < n; k++)
            {
                string a = input[i];
                string b = input[j];
                string c = input[k];
                string abc = "", bac = "";
                string bc = matrix[j, k];
                if (bc != "" && bc != null)
                    abc = matrix[i, Array.IndexOf(input, bc)];
                string ac = matrix[i, k];
                if (ac != "" && ac != null)
                    bac = matrix[j, Array.IndexOf(input, ac)];
                if (abc != bac && abc != "" && bac != "" && abc != null && bac !=
null)
                {
                    if (showViolation)
                        MessageBox.Show(a + "(" + b + c + ") = " + b + "(" + a + c +
)", "Violation of Left Permutable Law", MessageBoxButtons.OK, MessageBoxIcon.Warning);
                    return false;
                }
                if (abc == "" || bac == "" || abc == null || bac == null)
            }
        }
    }
}
```

```

        complete = false;
    }
}
}
if (complete)
    return true;
else
    return this.radioButtonLeftPemutableHold.Checked;
}

```

4.5 Conclusion

First of all, we have produced results which minimize our search of enumerating finite inverse LA-semigroups. In this regard, we have investigated that inverse LI-semigroups, inverse LA*-semigroups and commutative inverse LA-semigroups are equivalent to each other. Furthermore, we have found a formula for finding the number of constraints of type 2 for an inverse LA-semigroup of certain order n . We have developed algorithms for the enumeration of LA-semigroups, inverse LA-semigroups and their subclasses. Moreover, we have developed an algorithm for finding non-isomorphic classes of inverse LA-semigroups and their subclasses. Finally, we have used these algorithms to develop a left almost algebraic machine (abbreviated as LASAM) in C-sharp. Main work of this machine to enumerate LA-semigroups in general and its subclasses in particular. We have presented a partial classification of inverse LA-semigroups up to order 6 and inverse LA-monoids up to order 8. With the help of this machine, we have also obtained many examples of inverse LA-semigroups of certain order by fixing some generators and relations which are presented throughout the thesis.

Chapter 5

PRESENTATION OF INVERSE LA-SEMIGROUPS

5.1 Introduction

This chapter of thesis marks the first attempt of finding and describing the (finite) presentations of inverse LA-semigroups which is still far from being comprehensive. It provides a foundation to the concept of defining an inverse LA-semigroup by generators and relations. If one is not careful enough to distinguish between the elements of an LA-semigroup and words that describe these elements, utter confusion is likely to ensue.

Our purpose is to devise a technique to write the inverse LA-semigroups in the form of (finite) presentation which enables us to study the finite inverse LA-semigroups in a more efficacious way. It also helps us to further investigate the enumeration results of the previous chapter combinatorially and graphically; such like groups and semigroups.

A vast literature on the presentations of groups and semigroups (and related structures) lays an outline for the development of the presentation of the inverse LA-semigroups but devising a presentation is not, by any means, trivial. Examples of semigroups defined by the presentations are available in [5], [6], [7] and [51]. In [7], the authors considered semigroup presentations of the form

$$\Pi = \langle x_1, \dots, x_n \mid s_1 = r_1, \dots, s_m = r_m \rangle$$

where $m, n \in \mathbb{N}$ and $s_i, r_i, i = 1, \dots, m$ are non-empty words in the symbols x_1, \dots, x_n . Every presentation can also be considered as a group presentation. They used the symbols $Sgp(\Pi)$ and $Gp(\Pi)$ to distinguish between the semigroup and group defined by Π . Also, they investigated necessary and sufficient conditions for the minimum two sided ideals of $Sgp(\Pi)$ to be disjoint union of copies of the group $Gp(\Pi)$.

The principal problem which arises is that of recognizing when two sets of generators and relations actually present the same LA-semigroup. For this, we describe LA-semigroups by exhibiting its multiplication table just like groups and semigroups. Of course, the use of a multiplication table is not possible for an infinite LA-semigroup, nor even practical for a finite LA-semigroup of large order. For instance, the Table 24 has sixteen entries, but using the data from table $t = s^2, u = ts = s^2s = s^3 \neq ss^2$, we reduce the information necessary to determine the elements of the LA-semigroup which are s, s^2, s^3 and v with the relations $us = s^3s = s$. Now, the LA-semigroup in question is more efficiently depicted because the elements s and v generate it and that the equations $s^4 = s$ and $vs = v = ss^2$ are satisfied. Thus the presentation $\langle s, v \mid s^4 = s, vs = v = ss^2 \rangle$ represents the LA-semigroup defined by Table 24.

Table 24. An LA-semigroup with two generators

	s	t	u	v
s	t	v	u	s
t	u	s	t	v
u	s	u	v	t
v	v	t	s	u

This leads to the method of describing an LA-semigroup by generators and relations. Let L be a set $\{x_1, x_2, \dots, x_n\}$. A word over L is a finite string

$$w = x_1x_2x_3\dots x_l = (((x_1x_2)x_3)\dots)x_l$$

with each $x_i \in L$. The length of w is $l = l(w) = |w|$. When $l = 0$, then this is an empty word, which we denote by ϵ .

We follow the terms and notations used in [59]. Let us denote the set of all (finite) words over L by L^* , and by L^+ the set of all words (non-empty) in L^* . Thus $L^* = L^+ \cup \{\epsilon\}$. The sets L^* and L^+ can be induced into the structure of LA-semigroups if we define multiplication of words such that it satisfies $(x_1x_2)x_3 = (x_3x_2)x_1$. The presentation of an LA-semigroup is an ordered pair $\langle L \mid \mathfrak{R} \rangle$, where $\mathfrak{R} \subseteq L^+ \times L^+$. An element x of L is called a generating symbol whereas an element (s, r) of \mathfrak{R} is called a defining relation, and is written by the usual notation $s_1 = s_2$. Likewise if $L = \{x_1, x_2, \dots, x_m\}$ and $\mathfrak{R} = \{s_1 = r_1, s_2 = r_2, \dots, s_n = r_n\}$, then $\langle L \mid \mathfrak{R} \rangle$ is used to represent the complete notation. Thus, a presentation is a sequence of alphabets and words. An LA-semigroup is defined by the presentation $\langle L \mid \mathfrak{R} \rangle$ is L^+ / ρ , where ρ is the smallest congruence on L^+ containing \mathfrak{R} . More generally, an LA-semigroup L is said to be defined by the presentation $\langle L \mid \mathfrak{R} \rangle$ if $L \cong \langle L \mid \mathfrak{R} \rangle$. Therefore, the elements of L are in one-one correspondence with the congruence classes of words from L^+ .

5.2 Presentations and Graphs of Inverse LA-semigroups

First, we define some presentations of inverse LA-semigroups generated by one or two generators. We have also generalized some of these to study the symmetries. Then we draw the Cayley graphs of these finite presentations to explain the obscure symmetries or partial symmetries hidden in these inverse LA-semigroups. We observe that there are many partial symmetries of rotation and reflection in the Cayley graphs of inverse LA-semigroups which may be explored by deleting the symmetry spoilers.

In group theory, the coloured edges are used to represent the product of one generator to another and arrow head on the edge discloses the output element which is written at the pointed/directed vertex of the edge. The circle on any vertex indicates that the product of any particular element with the vertex element again yield the vertex element. It is a central tool of combinatorial and geometric group theory. Here, we draw the graphs from the presentations of inverse LA-semigroups keeping the following facts in mind: we use two colour edges for product of each element: one for the left and the other for right multiplication. An arrow head is pointed towards the output. There is no need to point direction on the circle because the colour of its edges indicates the product of generator from the left or right whereas it yields again the same

element in the circle. The discussed Cayley graphs are connected and transitive. Their cycles represent the relations. These graphs are partially symmetric means that deleting the one or more symmetry spoilers (specific edges), the resultant Cayley graph is symmetric.

We construct some examples first which establishes a foundation for more general and composite structures. Which are helpful to elaborate the products (direct and wreath) of the inverse LA-semigroups in the next sections.

Example 8 The presentation $\langle a, b \mid aa^2 = b = ba, a^4 = a \rangle$ defines an inverse LA-semigroup of order 4 with the left inverses $a' = a^3$ and $b' = a^2$.

Table 25. Inverse LA-semigroup having two generators				
	a	a^2	a^3	b
a	a^2	b	a^3	a
a^2	a^3	a	a^2	b
a^3	a	a^3	b	a^2
b	b	a^2	a	a^3

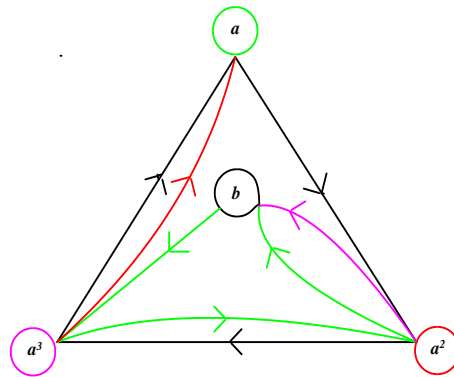


Figure 9. Cayley graph of an inverse LA-semigroup generated by two generators a and b .

Figure 9 allow us to visualize the abstract structure of the inverse LA-semigroup defined by Table 25. Black edges in the diagram show the right multiplication a with any vertex and arrows are directed towards the output of the product. For example, output of the product a^2a is a^3 . The output of the product ba is b which is denoted by undirected black circle. Right

multiplication with b is shown by the green edges. Similarly, left multiplication of a and b with any vertex are denoted by purple and red edges respectively. The Cayley graph is connected and transitive.

Example 9 The presentation $\langle c \mid c^5 = c = cc^2, cc^3 = c^4 \rangle$ defines an inverse LA-monoid of order 4 where the left inverse of c is $c' = c^3$, and c^4 is the left identity.

Table 26. Non-commutative cyclic inverse LA-monoid of order 4
by presentation $\langle c \mid c^5 = c = cc^2, cc^3 = c^4 \rangle$

	c	c^2	c^3	c^4
c	c^2	c	c^4	c^3
c^2	c^3	c^4	c	c^2
c^3	c^4	c^3	c^2	c
c^4	c	c^2	c^3	c^4

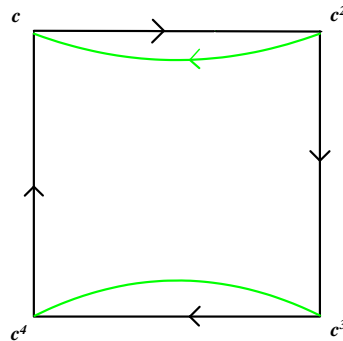


Figure 10. Cayley graph of a cyclic inverse LA-semigroup of order 4.

Figure 10 represents the abstract structure of cyclic inverse LA-semigroup of order 4. Here, c is the only generator having period 4. Black edges indicate the right multiplication of c with any vertex element and green edges are used to represent the left multiplication of c . A green edge between c^3 and c^4 is bidirectional which indicates that $cc^4 = c^3$ and $cc^3 = c^4$. This Cayley graph is connected and transitive. Also, it is symmetric in many senses.

Inverse LA-semigroup

Here, we find presentations of inverse LA-semigroups of particular form of order 5, 9, 11 and 19 which contain two generators and at most 4 relations. Furthermore, we note that there is no other inverse LA-semigroup of this kind between these orders. These presentations are of particular importance in the sense that they have same kind of inverse LA-semigroups but of different order. The inverse LA-semigroups representing by these presentations are non-commutative, non-associative and non-left permutable.

Example 10 *The presentation $\langle a, b : a^5 = a, aa^3 = b = ba \rangle$ defines an inverse LA-semigroup of order 5, which is explicated by the following multiplication table.*

Table 27. Inverse LA-semigroup defined by the presentation

$$\langle a, b : a^5 = a, aa^3 = b = ba \rangle$$

	a	a^2	a^3	a^4	b
a	a^2	a	b	a^4	a^3
a^2	a^3	a^4	a	a^2	b
a^3	a^4	b	a^3	a	a^2
a^4	a	a^3	a^2	b	a^4
b	b	a^2	a^4	a^3	a

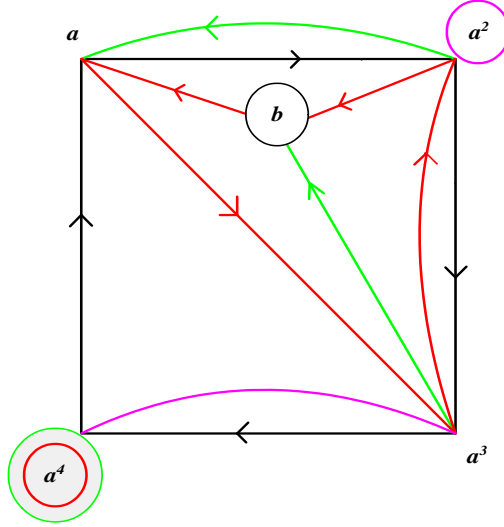


Figure 11. Cayley graph of inverse LA-semigroup defined by Table 27.

Figure 11 allows to study the abstract properties of an inverse LA-semigroup defined by the presentation $\langle a, b : a^5 = a, aa^3 = b = ba \rangle$. It is a graph based on four colours and two generators. Black edges in the diagram show the right multiplication of a with any vertex and arrows are directed towards the output of the product. The output of the product ba is b which is denoted by undirected black circle. Right multiplication of b with any vertex is shown by the red edge. Similarly, left multiplication of a and b are denoted by green and purple edges respectively. Black edges form a squares and a circle which has many symmetries of rotation and reflection.

Example 11 *The presentation $\langle a, b : a^9 = a, aa^7 = b = ba, bb = a^7 \rangle$ is an inverse LA-semigroup of order 8, which is explicated by the following multiplication table.*

Table 28. Inverse LA-semigroup defined by the presentation

$$\langle a, b : a^9 = a, aa^7 = b = ba, bb = a^7 \rangle$$

	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	b
a	a^2	a^6	a	a^7	a^4	a^3	b	a^8	a^5
a^2	a^3	a^4	a^5	a^6	a^7	a^8	a	a^2	b
a^3	a^4	a	a^8	b	a^5	a^7	a^3	a^6	a^2
a^4	a^5	a^8	a^6	a^3	a^2	b	a^7	a	a^4
a^5	a^6	b	a^3	a^5	a	a^4	a^2	a^7	a^8
a^6	a^7	a^5	a^2	a	b	a^6	a^8	a^4	a^3
a^7	a^8	a^7	b	a^4	a^6	a^2	a^5	a^3	a
a^8	a	a^3	a^7	a^2	a^8	a^5	a^4	b	a^6
b	b	a^2	a^4	a^8	a^3	a	a^6	a^5	a^7

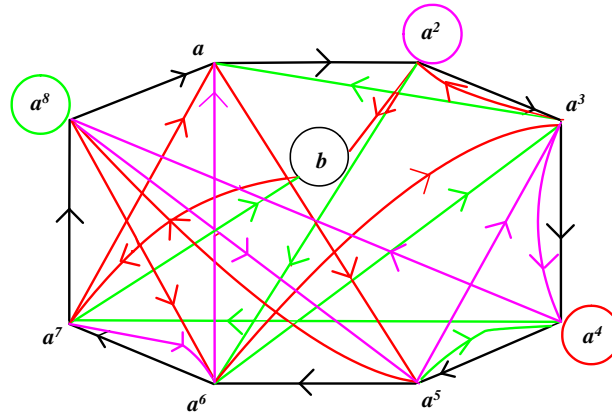


Figure 12. Cayley graph of commutative inverse LA-semigroup defined by Table 28.

Figure 12 allow us to study the abstract properties of an inverse LA-semigroup defined by the presentation $\langle a, b : a^9 = a, aa^7 = b = ba, bb = a^7 \rangle$. It is a graph based on four colours and two generators. Black edges in the diagram show the right multiplication of a with any vertex and arrows are directed towards the output of the product. The output of the product ba is b which is denoted by undirected black circle. Right multiplication of b with any vertex is shown

by the red edge. Similarly, left multiplication of a and b are denoted by green and purple edges respectively.

Example 12 The presentation $\langle a, b : a^{11} = a, aa^9 = b = ba, bb = a^8 \rangle$ defines an inverse LA-semigroup of order 11, which is explicated by the following multiplication table.

Table 29. Inverse LA-semigroup defined by the presentation
 $\langle a, b : a^{11} = a, aa^9 = b = ba, bb = a^8 \rangle$

	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	b
a	a^2	a^9	a^7	a^3	a^8	a	a^5	a^4	b	a^{10}	a^6
a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a	a^2	b
a^3	a^4	a^7	a	a^{10}	b	a^6	a^8	a^5	a^3	a^9	a^2
a^4	a^5	a	a^6	a^9	a^3	a^2	b	a^8	a^{10}	a^7	a^4
a^5	a^6	a^{10}	a^9	b	a^5	a^7	a^4	a^2	a^8	a^3	a
a^6	a^7	b	a^3	a^5	a^2	a^{10}	a^6	a	a^4	a^8	a^9
a^7	a^8	a^6	a^2	a^7	a^{10}	a^4	a^3	b	a^9	a	a^5
a^8	a^9	a^8	b	a^4	a^6	a^3	a	a^7	a^2	a^5	a^{10}
a^9	a^{10}	a^5	a^8	a^2	a	b	a^7	a^9	a^6	a^4	a^3
a^{10}	a	a^3	a^{10}	a^8	a^4	a^9	a^2	a^6	a^5	b	a^7
b	b	a^2	a^4	a	a^9	a^5	a^{10}	a^3	a^7	a^6	a^8

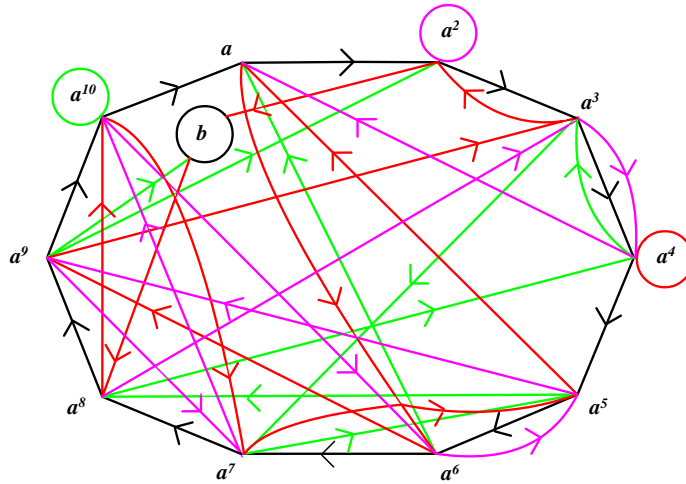


Figure 13. Cayley graph of inverse LA-semigroup defined by Table 9.

Figure 13 depicts the abstract properties of an inverse LA-semigroup defined by the presentation $\langle a, b : a^{11} = a, aa^9 = b = ba, bb = a^8 \rangle$. It is a graph based on four colours and two generators. Black edges in the diagram show the right multiplication of a with any vertex and arrows are directed towards the output of the product. The output of the product ba is b which is denoted by undirected black circle. Right multiplication of b with any vertex is shown by the red edge. Similarly, left multiplication of a and b are denoted by green and purple edges respectively. The presentations for such inverse LA-semigroups of order 19 and 25 are $\langle a, b : a^{19} = a, aa^{17} = b = ba, bb = a^{12} \rangle$ and $\langle a, b : a^{25} = a, aa^{23} = b = ba, bb = a^{15} \rangle$ respectively.

Cyclic inverse LA-group

We define cyclic inverse LA-group to be generated by a single element which may have one or more relations. The succeeding theorem provides a general presentation for the cyclic inverse LA-group of order n . This presentation is of significance as the identity exists in the structure and there is no need to prove it.

Theorem 16 *The presentation*

$$\Pi_1 = \left\langle a \mid a^{n+1} = a = aa^{\frac{n}{2}}, a^m a^{n-m} = a^n, 1 \leq m \leq n-1, n = 4k, m, k \in \mathbb{Z} \right\rangle$$

defines an LA-group.

Proof. Here, a is the only generator with period n , that is, $a^{n+1} = a$. Further, $a^m = \underbrace{(((aa)a) \dots)}_{m\text{-times}} a = (((a^{n+1}a) a) \dots) a = ((a^{n+2}a) \dots) a = \dots = a^{n+m}$. Since $a^m a^{n-m} = a^n$ for each $1 \leq m \leq n-1$. By the variation of m , it is clear that $a^m a^{n-m} = a^n = a^{n-m} a^m$. Also, $(a^m a^{n-m})^2 = (a^m a^{n-m})(a^m a^{n-m}) = (a^m a^{n-m})(a^{n-m} a^m) = ((a^{n-m} a^m) a^{n-m}) a^m = a^{n-m} a^m = a^m a^{n-m}$. So $a^n = a^m a^{n-m}$ is the idempotent element in Π_1 . Next we prove that a^n is the left identity element. Since for each $1 \leq m \leq n-1$ we have $a^n a^m = (a^m a^{n-m}) a^m = a^m$. Showing that a^n is the left identity and unique idempotent of Π_1 . Hence by Proposition 17, Π_1 represents an inverse LA-group. ■

The next example explains the finite presentation of the cyclic inverse LA-semigroup in detail.

Example 13 For $n = 8$, $\Pi_1 = \langle a \mid a^9 = a = aa^4, a^m a^{8-m} = a^8, 1 \leq m \leq 7 \rangle$, we have $aa^7 = a^8, a^2a^6 = a^8, a^3a^5 = a^8, a^4a^4 = a^8, a^5a^3 = a^8, a^6a^2 = a^8, a^7a = a^8$. The following multiplication table explicates the structure of the cyclic inverse LA-semigroup.

Table 30. Cyclic inverse LA-semigroup defined by the presentation $\langle a \mid a^9 = a = aa^4, a^m a^{8-m} = a^8, 1 \leq m \leq 7 \rangle$

	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
a	a^2	a^7	a^4	a	a^6	a^3	a^8	a^5
a^2	a^3	a^4	a^5	a^6	a^7	a^8	a	a^2
a^3	a^4	a	a^6	a^3	a^8	a^5	a^2	a^7
a^4	a^5	a^6	a^7	a^8	a	a^2	a^3	a^4
a^5	a^6	a^3	a^8	a^5	a^2	a^7	a^4	a
a^6	a^7	a^8	a	a^2	a^3	a^4	a^5	a^6
a^7	a^8	a^5	a^2	a^7	a^4	a	a^6	a^3
a^8	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8

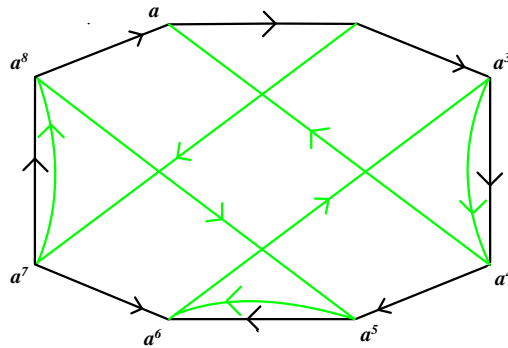


Figure 14. Cayley graph of a cyclic inverse LA-semigroup of order 8 defined by Table 30.

Figure 14 depicts the abstract structure of cyclic inverse LA-semigroup. All edges are unidirectional. The diagram is symmetric about vertical axis. Black edges indicate the right

multiplication of a with any vertex element and green edges are used to represent the left multiplication of a with any vertex element.

Commutative Inverse LA-semigroup

Theorem 17 *If $\langle a \mid a^{n+1} = a, aa^n = a \rangle$ is the presentation of an inverse LA-semigroup then by adding a generator b along with the relations $ba^k = b = bb, 1 \leq k \leq n$ defines an inverse LA-semigroup*

$$\Pi_2 = \langle a, b \mid a^{n+1} = a, aa^n = a, ba^k = b = bb, 1 \leq k \leq n \rangle$$

of order $n + 1$.

Example 14 *For $n = 2$, $\Pi_2 = \langle a, b \mid a^3 = a = aa^2, ba^k = b = b^2, 1 \leq k \leq 2 \rangle$ establishes a commutative inverse LA-semigroup of order 3, whose multiplication table is:*

Table 31. Commutative inverse LA-semigroup of order 3

$$\langle a, b \mid a^3 = a = aa^2, ba^k = b = b^2, 1 \leq k \leq 2 \rangle$$

	a	a^2	b
a	a^2	a	b
a^2	a	a^2	b
b	b	b	b

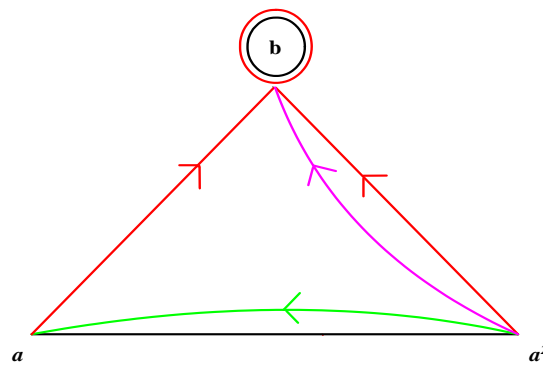


Figure 15. Cayley graph of commutative inverse LA-semigroup.

Figure 15 allow us to study the abstract properties of a commutative inverse LA-semigroup. It is a graph based on four colours and two generators. Black edges in the diagram show the right multiplication of a with any vertex and arrows are directed towards the output of the product. The output of the product ba is b which is denoted by undirected black circle. Right Multiplication of b with any vertex is shown by the red edge. Similarly, left multiplication of a and b with any vertex are denoted by green and purple edges respectively.

5.3 Construction and Representation

Given two monoids M_1 and M_2 by presentations $\langle M_1 \mid R_1 \rangle$ and $\langle M_2 \mid R_2 \rangle$, and if U is the direct product $M_1 \times M_2$, then U has a presentation

$$\langle A_1, A_2 \mid R_1, R_2, a_1 a_2 = a_2 a_1, a_1 \in A_1, a_2 \in A_2 \rangle, \quad (5.1)$$

while the free product $M_1 * M_2$ has a presentation

$$\langle A_1, A_2 \mid R_1, R_2 \rangle.$$

We highlight the fact that if \mathcal{L}_1 and \mathcal{L}_2 are presumed to be inverse LA-semigroups instead of monoids, then the presentation mentioned in equation 5.1 does not necessarily demonstrates a presentation for $\mathcal{L}_1 \times \mathcal{L}_2$ in general.

We have found two ways of constructing an inverse LA-semigroup U from two different inverse LA-semigroups L_i ; the direct product and the wreath product.

The Direct Product

The structure of direct products is well-versed in groups; given the finite presentation of two groups $G_1 = \langle A_i \mid R_i \rangle$ and $G_2 = \langle B_j \mid R_j \rangle$, having no common element except e , and if all elements of G_1 commute with those of G_2 , then $m + n$ elements A_i and B_j generate the direct product. A presentation for the direct product includes all the generators and relations of G_1

and G_2 along the relations

$$A_i^{-1}B_j^{-1}A_iB_j = e \quad (i = 1, \dots, m; j = 1, \dots, n).$$

Though, generally the number of generators and relations may be reduced or simplified.

We incorporate the same layout for the inverse LA-semigroups but the composition differentiates substantially. We observe that the direct product of groups require two groups with identity and inverses, which may or may not be present in an inverse LA-semigroup. To accommodate this essentiality we take two inverse LA-semigroups \mathcal{L}_1 and \mathcal{L}_2 , both with inverses of the generators and at least one of them should have an identity (left or right). Also, the extra relations considered to have a specific order

$$\left(A_i^{-1}B_j^{-1}\right)(A_iB_j) = e \quad (i = 1, \dots, m; j = 1, \dots, n)$$

which follows the left invertive law.

Theorem 18 *An inverse LA-semigroup has the presentation by taking the direct product of an inverse LA-semigroup \mathcal{L} and an inverse LA-monoid $\mathcal{L}_{\mathbf{M}}$ with identity e , after adding $m \times n$ relations of the form $\left(a_i^{-1}b_j^{-1}\right)(a_ib_j) = e$, which follows the left invertive law, where a_i and b_j , $1 \leq i \leq m$, $1 \leq j \leq n$ are generators of \mathcal{L} and $\mathcal{L}_{\mathbf{M}}$ respectively.*

Proof. The invertive law in the direct product follows by imposing it on the relations $\left(a_i^{-1}b_j^{-1}\right)(a_ib_j) = e$, since \mathcal{L} and $\mathcal{L}_{\mathbf{M}}$ are already LA-semigroups and the inverses exist naturally. Hence, the direct product of \mathcal{L} and $\mathcal{L}_{\mathbf{M}}$ is an inverse LA-semigroup. ■

We explain the direct product of LA-semigroups with the help of the following example.

Example 15 *Consider the inverse LA-semigroup $\mathcal{L} = \langle a, b \mid aa^2 = b = ba, a^4 = a \rangle$, and the inverse LA-monoid $\mathcal{L}_{\mathbf{M}} = \langle c \mid c^5 = c, cc^3 = c^4 \rangle$ where $e = c^4$. Introduce the two new relations*

$$(a^{-1}c^{-1})(ac) = c^4, \text{ and } (b^{-1}c^{-1})(bc) = c^4,$$

which reduces to

$$(a^3c^3)(ac) = c^4, \text{ and } (a^2c^3)(bc) = c^4.$$

By the medial law

$$(a^3a)(c^3c) = c^4, \text{ and } (a^2b)(c^3c) = c^4.$$

This gives relations mentioned in Table 8

Table 32. Direct product of \mathcal{L} and $\mathcal{L}_{\mathbf{M}}$

	a	a^2	a^3	b	c	c^2	c^3	c^4
a	a^2	b	a^3	a	c	c^2	c^3	c^4
a^2	a^3	a	a^2	b	c	c^2	c^3	c^4
a^3	a	a^3	b	a^2	c	c^2	c^3	c^4
b	b	a^2	a	a^3	c	c^2	c^3	c^4
c	c^3	c^3	c^3	c^3	c^2	c	c^4	c^3
c^2	c^2	c^2	c^2	c^2	c^3	c^4	c	c^2
c^3	c	c	c	c	c^4	c^3	c^2	c
c^4	c^4	c^4	c^4	c^4	c	c^2	c^3	c^4

which is an inverse LA-semigroup. So the direct product of \mathcal{L} and $\mathcal{L}_{\mathbf{M}}$.

$$\mathcal{L} \times \mathcal{L}_{\mathbf{M}} = \langle a, b, c \mid aa^2 = b = ba, a^4 = a, c^5 = c, cc^3 = c^4, (a^3a)(c^3c) = c^4, (a^2b)(c^3c) = c^4 \rangle \quad (5.2)$$

is an inverse LA-semigroup of order 8.

5.4 Wreath Product of Inverse LA-semigroups

In this section, we deal with a presentation for the (restricted) wreath product of two inverse LA-semigroups. Our approach depends upon the pattern inscribed in [59]. Foremost, the definition of the wreath product has been recollected here; for more details see [18].

Let M_1 and M_2 be two monoids. The Cartesian product of $|M_2|$ copies of the monoid M_1 is denoted by $M_1^{\times M_2}$, and the direct product which conforms to it is denoted by $M_1^{\oplus M_2}$. The elements of $M_1^{\times M_2}$ is regarded as the set of all functions from M_2 into M_1 , and $M_1^{\oplus M_2}$ as the set of all such functions f with finite support, which is having the property that $(x)f = 1_{M_1}$

for all but finitely many $x \in M_2$. If $M_1^{\times M_2}$ and $M_1^{\oplus M_2}$ are equipped with the component wise multiplication, two monoids with the function

$$\bar{I} : M_2 \rightarrow M_1, \quad (x) \bar{I} = I_{M_1},$$

as the right identity are obtained.

We define the unrestricted wreath product of the inverse LA-semigroup \mathcal{L} by the inverse LA-monoid $\mathcal{L}_{\mathbf{M}}$, denoted by $\mathcal{L} Wr \mathcal{L}_{\mathbf{M}}$, by the set $\mathcal{L}^{\times \mathcal{L}_{\mathbf{M}}} \times \mathcal{L}_{\mathbf{M}}$ with the multiplication defined by

$$(f, u)(g, u') = (fg^{u'u}, uu'), \quad (5.3)$$

where $g^u : \mathcal{L}_{\mathbf{M}} \rightarrow \mathcal{L}$ is defined by

$$(x) g^u = (xu)g, \quad x \in \mathcal{L}_{\mathbf{M}}, \quad (5.4)$$

$fg^{tt'}$: $\mathcal{L}_{\mathbf{M}} \rightarrow \mathcal{L}$ is defined by

$$(x) fg^{tt'} = [I_{\mathcal{L}_{\mathbf{M}}}] \cdot [(tt') I_{\mathcal{L}_{\mathbf{M}}} \cdot (x) f] g, \quad \text{for all } x \in \mathcal{L}_{\mathbf{M}} \quad (5.5)$$

and $f^{(tt')u''} g^{tt'}$: $\mathcal{L}_{\mathbf{M}} \rightarrow \mathcal{L}$ is defined by

$$(x) f^{(tt')u''} g^{tt'} = [(tt') u''] \cdot [(tt') u'' \cdot ((x) f)] g. \quad (5.6)$$

Theorem 19 *The unrestricted wreath product of the inverse LA-semigroup \mathcal{L} by the inverse LA-monoid $\mathcal{L}_{\mathbf{M}}$, $\mathcal{L}^{\times \mathcal{L}_{\mathbf{M}}} \times \mathcal{L}_{\mathbf{M}}$, is an inverse LA-semigroup with the right identity $(\bar{I}, I_{\mathcal{L}_{\mathbf{M}}})$.*

Proof. Let $\mathcal{L}^{\times \mathcal{L}_{\mathbf{M}}} \times \mathcal{L}_{\mathbf{M}}$ satisfy the above mentioned equations, then by equation 5.3 the left invertive law states that:

$$\begin{aligned} [(h, u'')(g, u)](f, u) &= (hg^{u''u'}, u''u')(f, u) \\ &= \left((hg^{u''u'}) f^{(u''u')u}, (u''u')u \right) \end{aligned} \quad (5.7)$$

Focusing on the first element of the ordered pair, we get

$$(hg^{u\prime\prime u\prime}) f^{(u\prime\prime u\prime)u} = \left(f^{(u\prime\prime u\prime)u} g^{u\prime\prime u\prime} \right) h.$$

From equation 5.5,

$$(x) \left(\left(f^{(u\prime\prime u\prime)u} g^{u\prime\prime u\prime} \right) h \right) = \left[(x) \left(f^{(u\prime\prime u\prime)u} g^{u\prime\prime u\prime} \right) \right] h.$$

From equation 5.6,

$$\begin{aligned} (x) \left(\left(f^{(u\prime\prime u\prime)u} g^{u\prime\prime u\prime} \right) h \right) &= \left[(x) \left(f^{(u\prime\prime u\prime)u} g^{u\prime\prime u\prime} \right) \right] h \\ &= [[(u\prime\prime u\prime) u] \cdot [[(u\prime\prime u\prime) u \cdot (x) f] g]] h \\ &= [[(tt\prime) u\prime\prime] \cdot [[(tt\prime) u\prime\prime \cdot (x) f] g]] h \\ &= [[(tt\prime) u\prime\prime \cdot (x) f] g] h^{(tt\prime)u\prime\prime} \\ &= \left[(x) \left(fg^{(tt\prime)u\prime\prime} \right) \right] h^{(tt\prime)u\prime\prime} \\ &= (x) \left[\left(fg^{(tt\prime)u\prime\prime} \right) h^{(tt\prime)u\prime\prime} \right]. \end{aligned}$$

Referring back to equation 5.7,

$$\begin{aligned} [(h, u\prime\prime)(g, u\prime)](f, u) &= \left((hg^{u\prime\prime u\prime}) f^{(u\prime\prime u\prime)u}, (u\prime\prime u\prime) u \right) \\ &= \left(\left(fg^{(tt\prime)u\prime\prime} \right) h^{(tt\prime)u\prime\prime}, (tt\prime) u\prime\prime \right) \\ &= [(f, u)(g, u\prime)](h, u\prime\prime). \end{aligned}$$

and

$$\begin{aligned} (f, u) (\bar{I}, I_{\mathcal{L}_{\mathbf{M}}}) &= \left(f \cdot \bar{I}^{u \cdot I_{\mathcal{L}_{\mathbf{M}}}}, u \cdot I_{\mathcal{L}_{\mathbf{M}}} \right) \\ &= (f, u). \end{aligned}$$

Hence, $\mathcal{L}^{\times \mathcal{L}_{\mathbf{M}}} \times \mathcal{L}_{\mathbf{M}}$ is an inverse LA-semigroup with right identity $(\bar{I}, I_{\mathcal{L}_{\mathbf{M}}})$. ■

The *restricted* wreath product of the inverse LA-semigroup \mathcal{L} by the inverse LA-monoid

$\mathcal{L}_{\mathbf{M}}$, denoted by $\mathcal{L} \text{ wr } \mathcal{L}_{\mathbf{M}}$, is the set $\mathcal{L}^{\oplus \mathcal{L}_{\mathbf{M}}}$, with the same multiplication. Also, $\mathcal{L} \text{ Wr } \mathcal{L}_{\mathbf{M}} = \mathcal{L} \text{ wr } \mathcal{L}_{\mathbf{M}}$ if and only if $|\mathcal{L}| = 1$ or $\mathcal{L}_{\mathbf{M}}$ is finite.

Corollary 20 *The restricted wreath product of the inverse LA-semigroup \mathcal{L} by the inverse LA-monoid $\mathcal{L}_{\mathbf{M}}$, $\mathcal{L}^{\oplus \mathcal{L}_{\mathbf{M}}}$, is an inverse LA-semigroup with the right identity $(\bar{I}, I_{\mathcal{L}_{\mathbf{M}}})$.*

5.5 Conclusion

In this chapter, we have produced examples of inverse LA-semigroups, left permutable inverse LA-semigroups, Cyclic inverse LA-semigroups and LA-groups by fixing generators and relations in LASAM. Then we have expressed them in the form of presentation. For this purpose, we have provided a foundation for expressing an inverse LA-semigroup in terms of generators and relations. We have found presentations for inverse LA-semigroups, commutative inverse LA-semigroups, left permutable inverse LA-semigroups and generated by two generators. We have also found presentations for cyclic inverse LA-semigroups. Then, we have generalized these presentations. Also, we have presented Cayley graphs using these presentations to investigate symmetries, that is, permutation inverse LA-semigroups. The direct and wreath products of inverse LA-semigroups have been introduced here which have enabled us to study and analyse the inverse LA-semigroups in a more efficacious way.

Chapter 6

APPLICATION OF INVERSE LA-SEMIGROUPS IN CRYPTOGRAPHY

6.1 Introduction

The study of LA-semigroups has wide applications in the soft sets, neutrosophic sets, locally associative LA-semigroups, abelian groups, the theory of fuzzy LA-semigroups, ternary semi-hypergroups, Γ -semihypergroups and the theory of non-commutative groupoids [1, 30, 41, 42, 45, 48, 62, 63].

There are a number of information security techniques that have been designed in cryptography whose algorithms are based on non-associative structures. Cryptography is one of the most important branches of cryptology which is used to make an encryption scheme to secure information. Classical encryption techniques usually utilize either substitution or permutation to develop a cryptosystem. So far, different types of mathematical structures were utilized namely Group, Ring, Galois field and Galois ring for the development of a substitution box (S-box), which is a main nonlinear component of a smart block cypher. Here, by an S-box, we mean a Latin square of size 256×256 whose entries are selected from a set of 256 different symbols having no repetition in any row and column of the table. The desire for new mathematical

structures in the development of encryption techniques is the most important area of research in security analysis [26, 32, 33, 57].

In the previous chapter, we came to conclude a generalized presentation

$$\Pi_1 = \langle a \mid a^{n+1} = a = aa^{\frac{n}{2}}, a^m a^{n-m} = a^n, 1 \leq m \leq n-1, n = 4k, m, k \in \mathbb{Z} \rangle$$

of an LA-group. Every LA-group is in fact an inverse LA-semigroup with a unique idempotent element which behaves as a unique left identity. In this chapter, we make use of an inverse LA-semigroup of order 256 described by the presentation $\langle a \mid a^{257} = a = aa^{128}, a^m a^{256-m} = a^{256} \rangle$. We use this inverse LA-semigroup to construct a S-box which produces confusion in the proposed algorithm. Thus, increasing its measure of nonlinearity and compelling the system to be more secure and impregnable.

According to Edward Lorenz, chaos takes place "when the present determines the future, but the approximate present does not approximately determine the future." The logistic map uses a differential equation in which time behaves as a continuous variable. This map is iterative in the sense that its value at any time interval maps to the value at the succeeding time interval.

Chaos theory has always been practised extensively for the development of image encryption and decryption mechanisms [35, 25]. The three fundamental characteristics of chaos that have made it possible to use it in the development of encryption algorithms are: sensitive to the initial condition, topological mixing, and dense periodic orbits. These three properties were closely related to cryptography. Due to the cryptographically robust characteristics of chaos, we have utilized the chaotic sequence using a modified Lorenz chaotic differential equations with a logistic map while designing our novel image encryption technique. Decryption scheme may also be achieved by reversing the orders of chaotic sequence and S-box in the given algorithm 4.

Here, we suggest a novel design for the encryption of images based on an inverse LA-semigroup and a modified non-linear chaotic map, which has better confusion and diffusion characteristics that are necessary for a modern substitution-permutation network. The numerical measures are also discussed to examine the response of suggested scheme against differential attacks.

Algorithm 4 *Proposed digital encryption algorithm.*

The present section elaborates the encryption procedure. The designed image encryption technique comprises of confusion and diffusion. As illustrated in Figure 16, the encryption method is based on the steps given below:Step 1.

Step 1. Take a standard digital colour image of size $n \times n$.

Step 2. Read the inverse LA-semigroup of order $n \times n$.

Step 3. Apply a substitution transformation by using the LA-semigroup as listed in Step 2, which adds confusion to the proposed algorithm.

Step 4. Generate chaotic sequence using Lorenz chaotic differential equations with a logistic map $u_{n+1} = ru_n(1 - u_n)$ where the variable r is given different value, ranging from 2 to 4.(seed values for each iteration comes from the Lorenz chaotic differential equation utilized three chaotic logistic maps used seeds from x , y and z directions solutions of Lorenz chaotic differential equations).

Step 5. Apply a bit wise addition under modulo 2, of confused image produced in Step 3 with the chaotic sequences generated in Step 4 for each layer of the digital image that uses x component values for the red layer, y component values from the green layer and z component values of the logistic map for the blue layer of a given image.

Step 6. Apply all of the above steps on each layer of the digital image.

Step 7. Display the encrypted image.

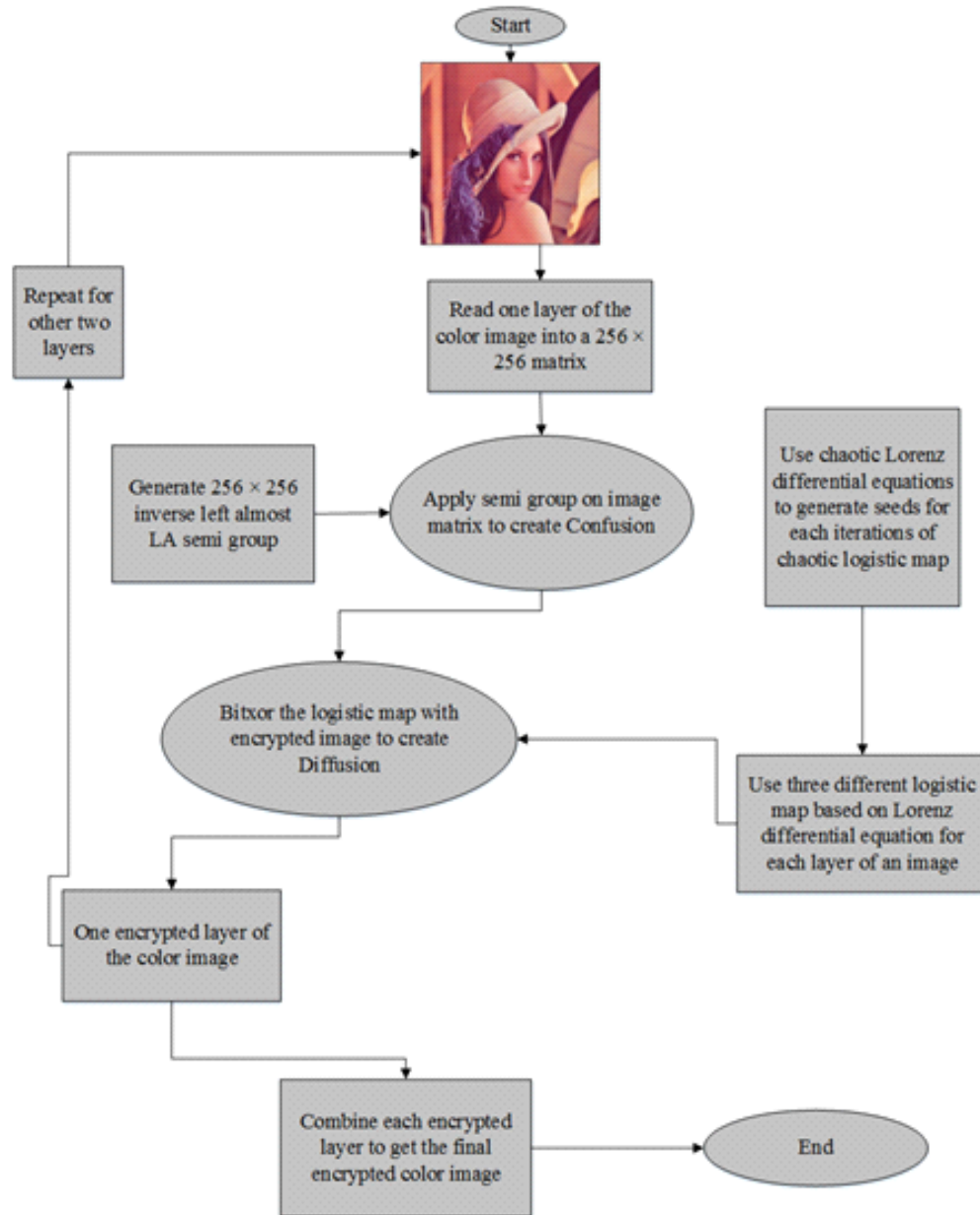


Figure 16. Proposed encryption algorithm.

Algorithm 5 *Proposed digital decryption algorithm.*

This process is actually the reverse process of the encryption scheme provided in the previous algorithm.

Step 1: Obtain three layers from the encrypted coloured image.

Step 2: Generate the chaotic sequence using Lorenz chaotic differential equations with inverse logistic map to obtain a sequence of length $n \times n$.

Step 3: Apply a bit wise addition under modulo 2 of the diffused images produced in Step 1 and the sequence generated in step 2.

Step 4: Read the inverse LA-semigroup of order $n \times n$.

Step 5: Apply substitution transformation by using the inverse LA-semigroup enlisted in Step 4.

Step 6. The decrypted Red, Green and Blue layers are obtained separately.

Step 7. Combine all the three layers to get the original coloured image.

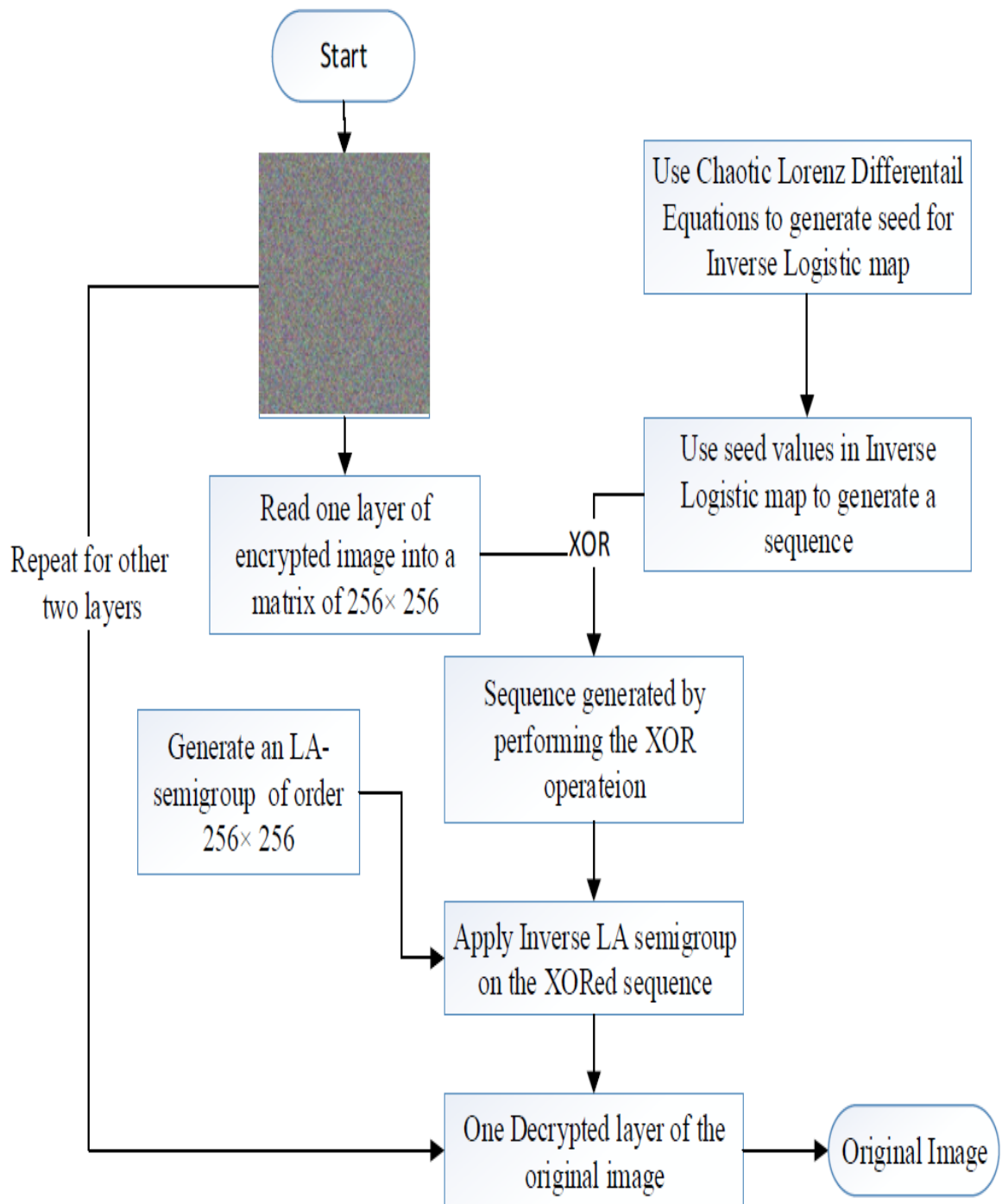


Figure 17. Proposed decryption algorithm.

The encrypted images through our proposed algorithm are provided in Figures 18, 19 for images of Lena and Baboon respectively.

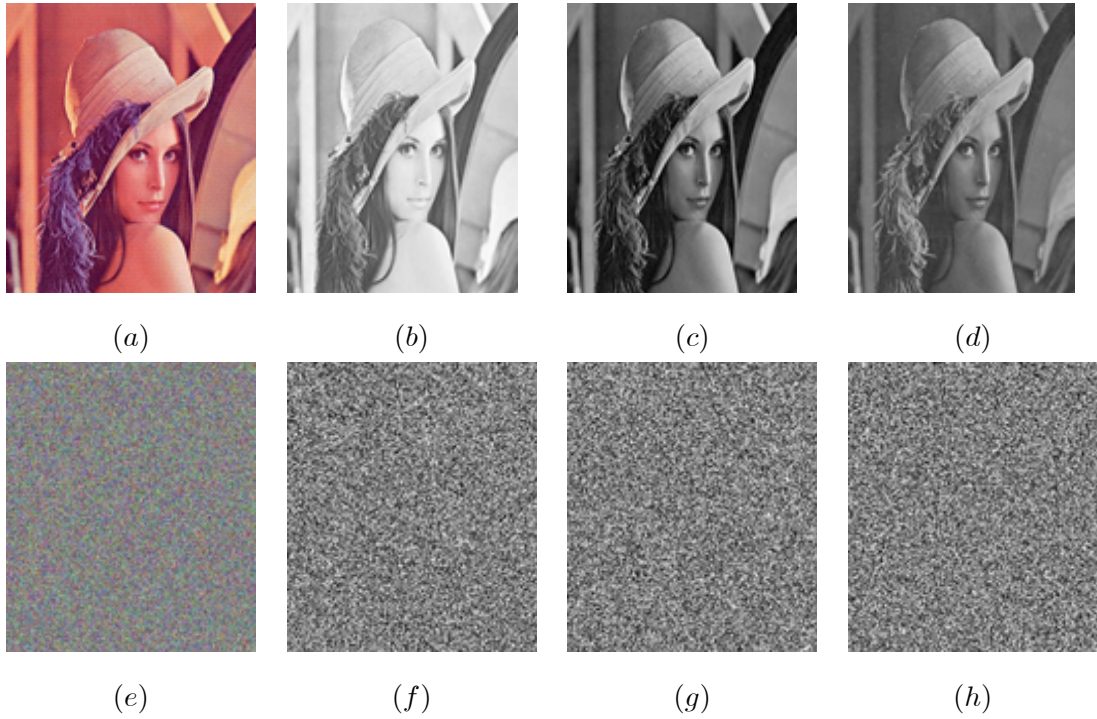
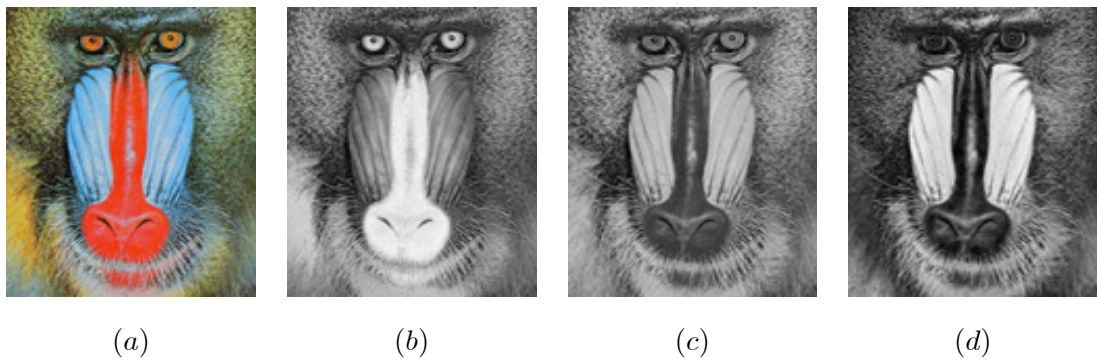


Figure 18. The images (e), (f), (g) and (h) are encrypted results for Lena's (a) standard (b) red (c) green and (d) blue layers respectively.



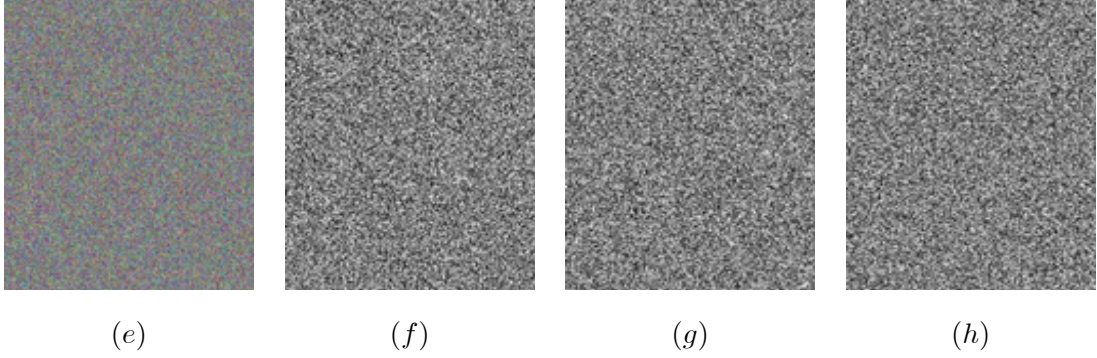


Figure 19. The images (e), (f), (g) and (h) are encrypted results for Baboon's (a) standard; (b) red (c) green and (d) blue layers respectively.

6.2 Security Analysis of the Proposed Algorithm

Here, we apply some statistical measures on the typical digital contents to examine the safety during execution of the proposed encryption scheme. These measurements are strictly based on a precise evaluation, a realistic inspection and an inconsistency criterion for the encryption of images.

Uniformity Analysis of Image Pixels

A histogram in image analysis provides information about the circulation of pixel intensity esteems for an image. A protected framework in encryption has an identical histogram to resist statistical assaults. The histograms in Figures 20, 21 represent the standard and encrypted images of Lena and Baboon. From Figures 20, 21, we analyze that the standard images do not have uniform histograms, whereas the encrypted digital images have uniform histograms. The uniformity of pixel heights in the histograms creates difficulty for attackers to find the clue for

the maximum information region.

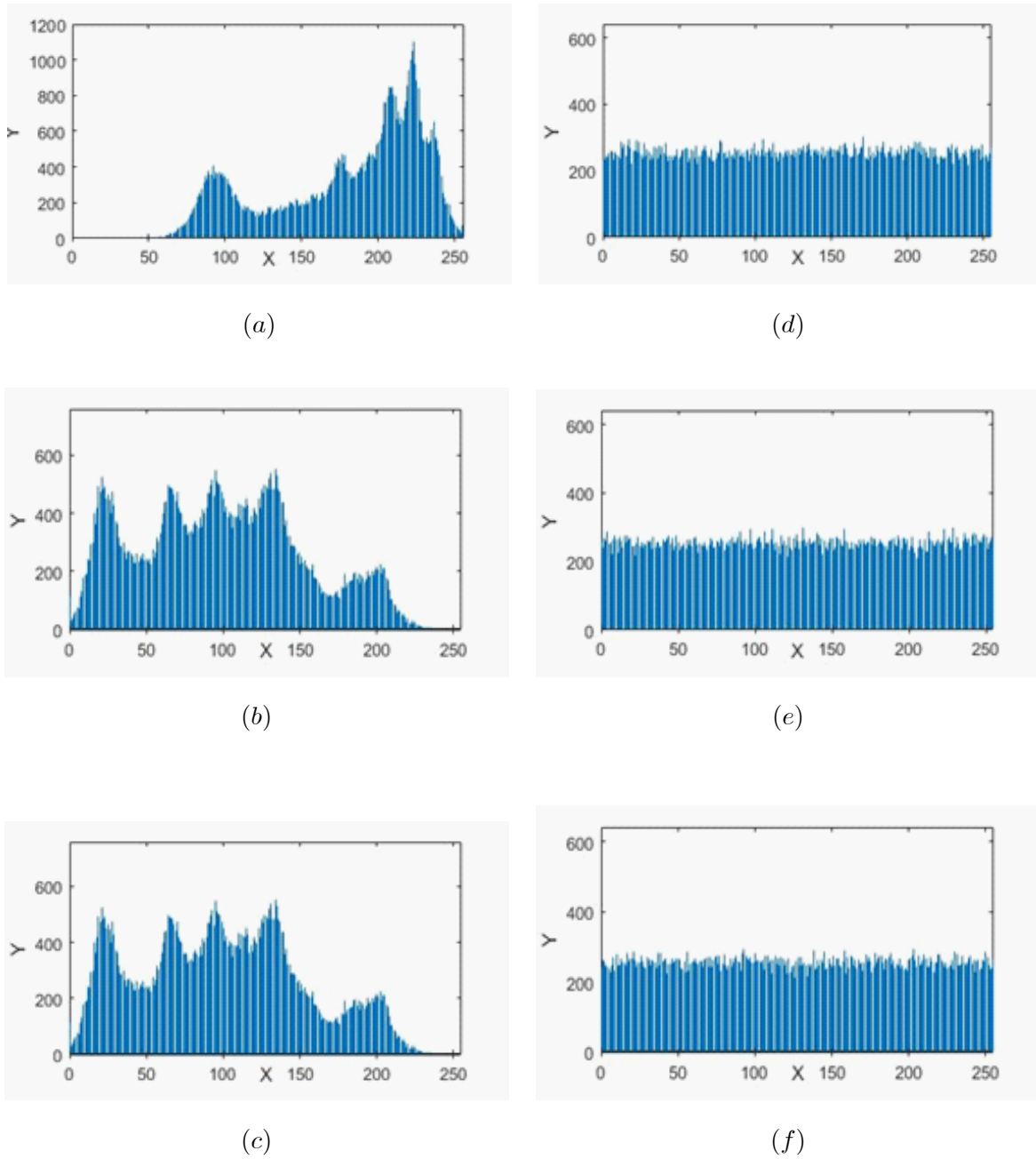
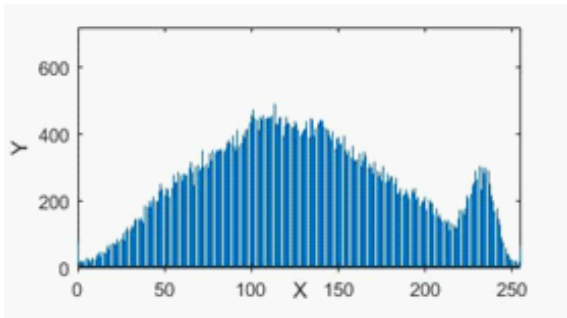
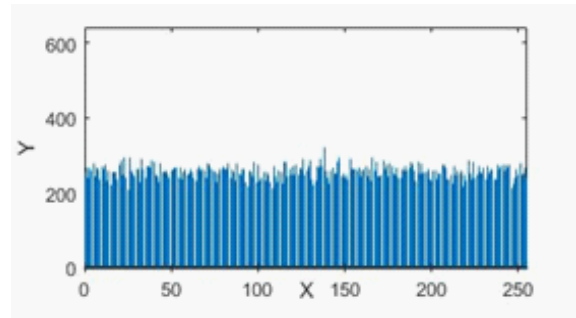


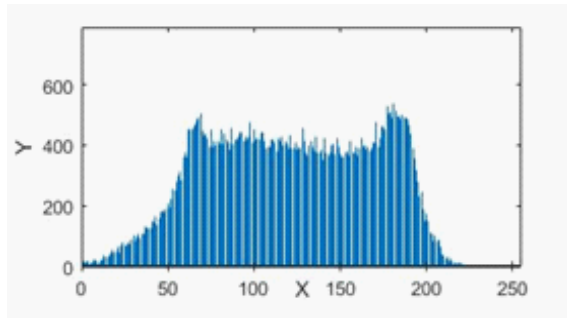
Figure 20. Histograms (a) red; (b) green and (c) blue layers for Lena's standard images with size 256×256 . Histograms (d) red; (e) green; (f) blue layers for Lena's encrypted images.



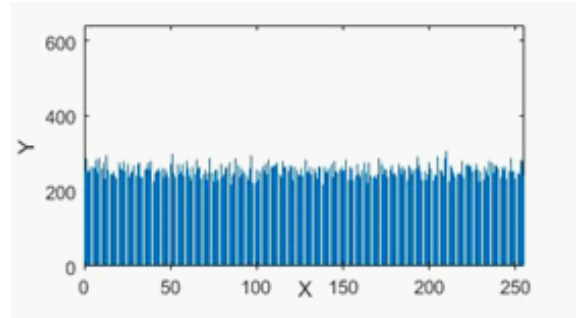
(a)



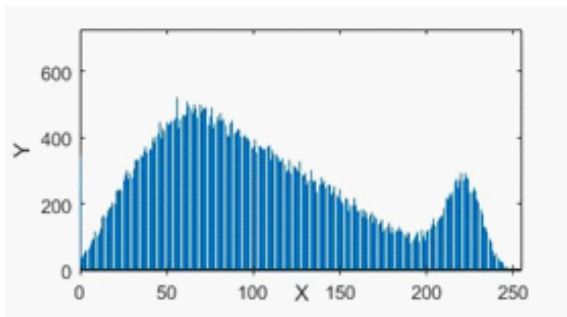
(d)



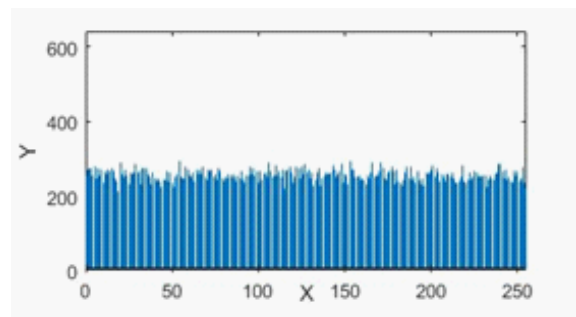
(b)



(e)



(c)



(f)

Figure 21. Histograms (a) red; (b) green and (c) blue layers for Baboon's standard images with size 256×256 . Histograms (d) red; (e) green; (f) blue layers for Baboon's encrypted images.

Correlation Analysis for Adjacent Pixels

The purpose of the correlation analysis is to examine the connection of neighboring pixels in the standard and encrypted images. Mathematically, the correlation coefficient $r_{U,V}$ of two neighboring pixels is defined as:

$$r_{U,V} = \frac{Cov(U, V)}{\sqrt{Var(U) Var(V)}},$$

where U and V are the estimations of two neighboring pixels of gray scale image, $Var(U)$ and $Var(V)$ are deviations of U and V individually and $Cov(U, V)$ represents the covariance. The correlation coefficients of the plain and encrypted digital images have distinctive results displayed in Tables 33 – 36 which are depicted by the plain and enciphered digital images provided in Figures 22, 23. In addition, Table 33 contains the quantified evaluation of the correlation coefficient demonstrating the diffusion of the unique and encoded images horizontally, vertically and diagonally. Presently, we consider 2000 pairs of randomly selected neighboring pixels to look over the original and the enciphered images horizontally, vertically and diagonally. In Table 36, the correlation coefficients for the red, green and blue layers of the encrypted images are quite small, which implies a correlation between adjoining pixels.

Table 33. Colour components-wise correlation coefficient of cipher images

Image	Layer	Correlation of Encrypted Image	Correlation of Altered Encrypted Image
Lena	Red	-0.019408	-0.026560
	Green	0.005199	0.016749
	Blue	-0.057938	-0.013504
Baboon	Red	-0.017262	-0.062436
	Green	-0.018564	-0.039240
	Blue	-0.011867	0.037551

Table 34. Correlation coefficients of original and encrypted images

Standard Images	Original Image			Encrypted Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9339	0.9652	0.9076	-0.0043	-0.0090	-0.0031
Baboon	0.8310	0.7737	0.7723	-0.0029	-0.0079	0.0026

Table 35. Correlation coefficients of the plain and cipher image for the Lena colour image of size 256×256

Standard Images	Original Image			Encrypted Image		
	Red	Green	Blue	Red	Green	Blue
Horizontal	0.9339	0.9044	0.8609	-0.0084	-0.0028	-0.0072
Vertical	0.9652	0.9464	0.9086	-0.0052	-0.0066	-0.0098
Diagonal	0.9076	0.8796	0.8371	-0.0016	0.0012	0.0013

Table 36. Comparison between the correlation coefficients of the proposed scheme and recent techniques using Lena image

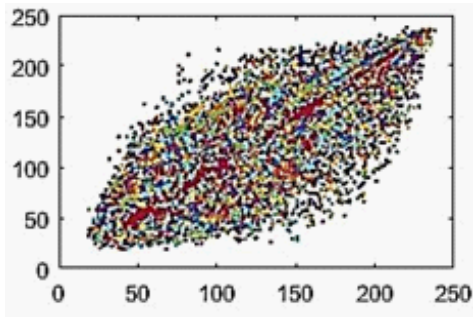
	Correlation Directions		
	Horizontal	Vertical	Diagonal
Proposed encryption scheme	-0.0043	-0.0090	-0.00310
Ref. [58]	0.06810	0.08450	-
Ref. [26]	0.21570	0.05810	0.05040
Ref. [19]	0.00720	0.00580	0.00310
Ref. [66]	0.02140	0.04650	-0.0090
Ref. [64]	0.08200	0.04000	0.00500
Ref. [67]	0.01200	0.02700	0.00700
Ref. [2]	0.00500	0.01100	0.02300



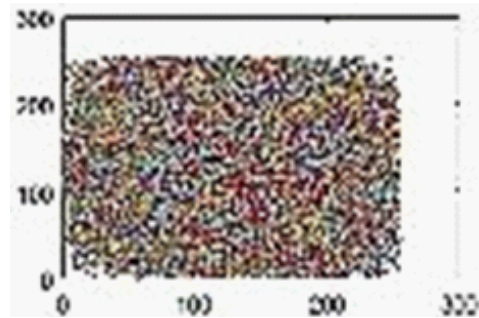
(a)



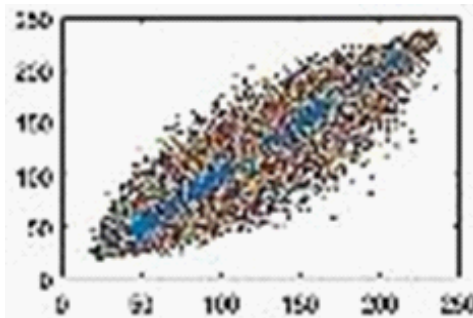
(e)



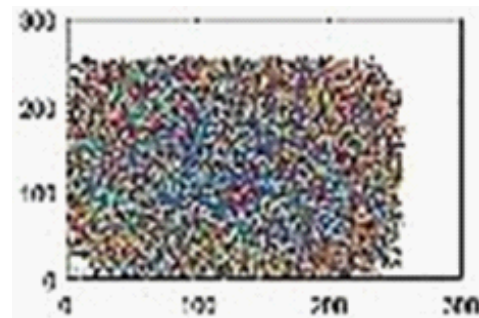
(b)



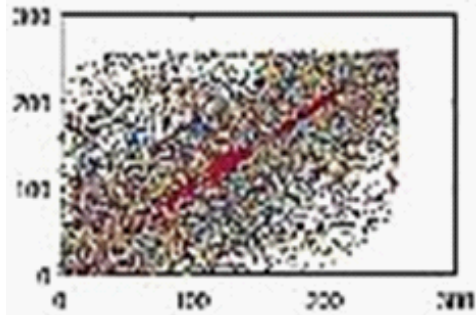
(f)



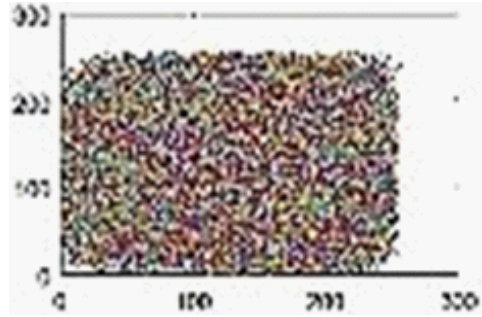
(c)



(g)

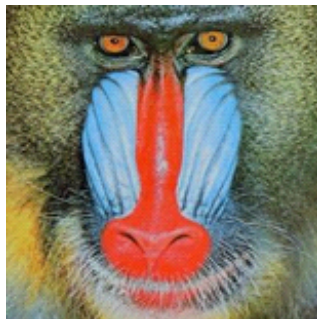


(d)

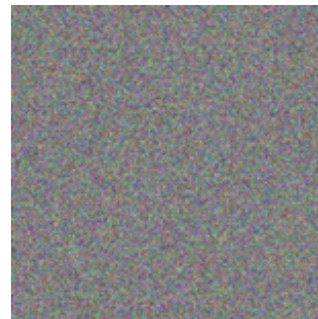


(h)

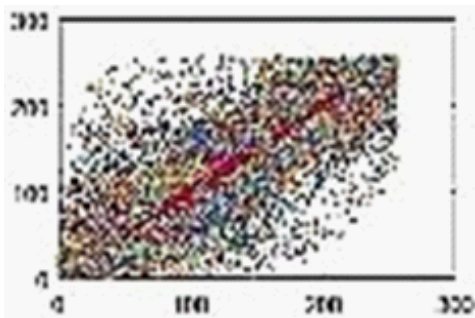
Figure 22. Correlation coefficients between the pixels of Lena's image (a) Standard (b) horizontal (c) vertical and (d) diagonal (e) encrypted (f) horizontal (g) vertical (h) diagonal.



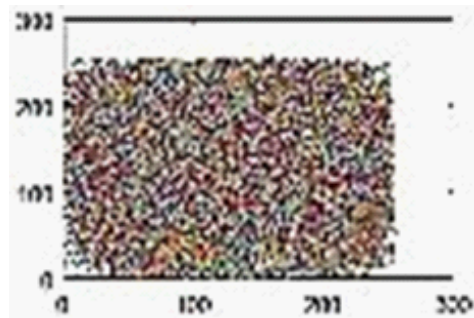
(a)



(e)



(b)



(f)

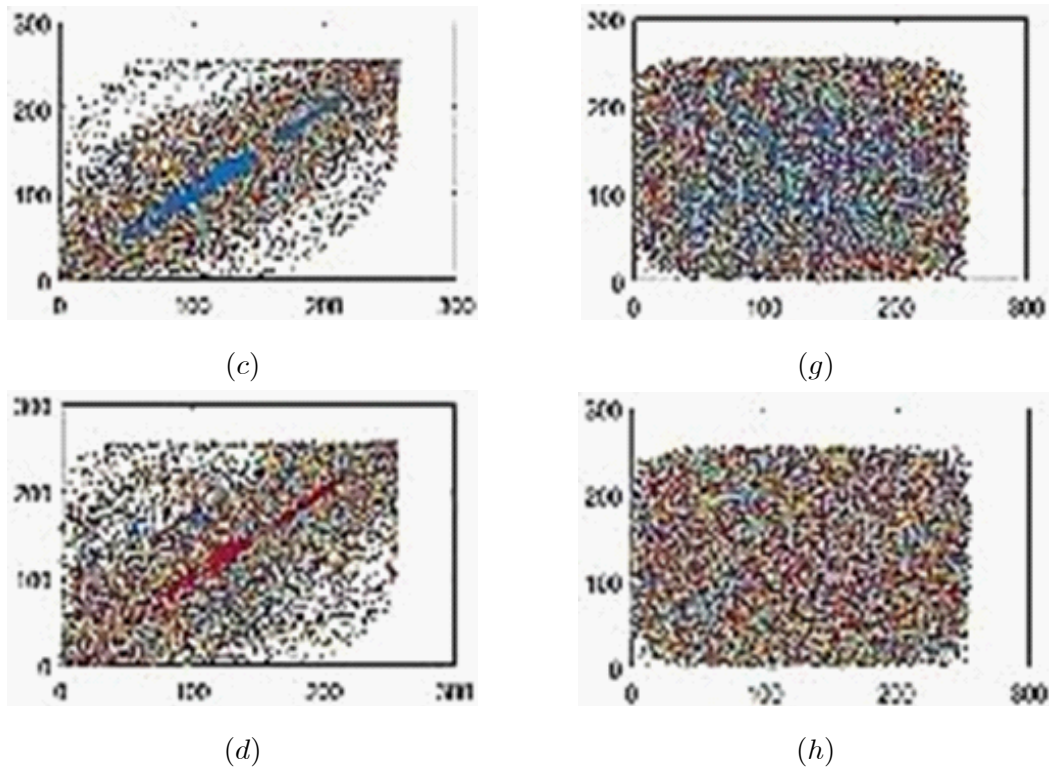


Figure 23. Correlation coefficients between the pixels of Baboon's image (a) Standard (b) horizontal (c) vertical and (d) diagonal (e) encrypted (f) horizontal (g) vertical (h) diagonal.

In addition, high correlation coefficients of red, green and blue layers of the standard image make data spillage conceivable. Table 35 provides us with similar position correlations for the red, green and blue parts, while Table 36 gives the adjoining position correlations for the red, green and blue layers. From Tables 35 and 36, we analyze that the correlation coefficients of the encrypted digital images for the red, green and blue layers are all lower than -0.003 , while the greatest correlation coefficient for the original images is 0.9652 in the Lena image and 0.8310 for the Baboon. Which indicates that the correlations for the red, green and blue layers of the encrypted images are adequately diminished. Therefore, our encryption scheme is highly defensive against statistical attacks. Furthermore, we plotted the correlation coefficients for the red, green and blue layers of the original images in Figures 22a – d, 23a – d and the encrypted images Figures 22e – h, 23e – h vertically, horizontally and diagonally. The correlation

coefficients between the adjacent pixels of the layers of standard image are shown by slanted spots Figures 22b – d, 23b – d. However, these spots scattered over the whole plane in Figures 22f – h, 23f – h, showing that the correlation is fully diminished in the encrypted images.

6.3 Pixel Modification Based Measurements

The quality of an image depends upon the pixel difference which is calculated by means of Mean Square Error (MSE), Average Difference (AD), Maximum Difference (MD), Normalized Absolute Error (NAE), Normalized Cross Correlation (NCC), Structure Content (SC) and Peak Signal to Noise Ratio (PSNR) values. These metrics are used for the comparison of unlike images.

Mean Square Error (MSE)

An encrypted image should not be equivalent to the original image due to the application of the encryption scheme, which surely adds some noise to the actual digital content. To analyze the level of enciphering, we calculate the MSE of the standard and encrypted images by using the formula:

$$MSE = \frac{\sum_{j=1}^m \sum_{k=1}^n (P_{jk} - C_{jk})^2}{m \times n}$$

where P_{jk} and C_{jk} represent the pixels positioned at j th row and k th column of the standard and encrypted images. A larger value of the MSE enhances the security of the encryption algorithm.

Peak Signal to Noise Ratio (PSNR)

PSNR is defined as:

$$PSNR = 20 \log_{10} \left[\frac{I_{MAX}}{\sqrt{MSE}} \right],$$

where I_{MAX} is the maximum value of pixel. The low value of PSNR shows the high difference of the original and enciphered images. In Table 37, we evaluate the values MSE and PSNR to

ensure the versatility of the suggested scheme.

Table 37. MSE and PSNR of the suggested scheme

Images	Pixel Difference Based Measures	
	MSE	PSNR
Lena	4859.03	11.30
Baboon	6399.05	10.10

Normalized Absolute Error (NAE)

NAE is defined as:

$$NAE = \frac{\sum_{j=1}^m \sum_{k=1}^n |P_{jk} - C_{jk}|}{\sum_{j=1}^m \sum_{k=1}^n |C_{jk}|}.$$

It is the proportion of the encrypted digital content to the original image. A longer estimation of NAE demonstrates the result of the scrambled image after the encryption process.

Maximum Difference (MD)

MD is defined as:

$$MD = \text{Max} |P_{jk} - C_{jk}|,$$

where $j = 1, 2, \dots, m$ and $k = 1, 2, \dots, n$. It measures the maximum value of the error signal. A higher value of the maximum difference indicates better quality of the encryption scheme.

Average Difference (AD)

The average difference measures the pixel contrast between the original image and its corresponding enciphered image. This quantitative measure is only utilized in object revealing and pattern recognition applications. A larger estimation of the AD represents the high quality of the digital image encryption (see Table 38). The zero value of AD represents that the two digital images are identical. Mathematically, the average difference is defined as:

$$AD = \frac{\sum_{j=1}^m \sum_{k=1}^n (P_{jk} - C_{jk})}{m \times n}.$$

6.4 Similarities Measure

The likenesses between two signals are estimated through a cross-correlation, structure similarity, and structure content. These are the standard devices for assessing how much two signals are comparable. It is a basic way to match two image patches for highlight recognition. This method has a few favorable circumstances. We have used a standardized correlation and structure content with the end goal to demonstrate the dissimilarities among the original and scrambled images.

Normalized Cross Correlation (NCC)

A normalized cross-correlation (NCC) is used to analyse the level of likeness (or difference) between the standard and encrypted images. It ranges from -1 to 1 and measures the cosy connection of any two images: they might be standard and encrypted images. The setting of the location edge esteem is significantly less difficult than the cross-correlation. Normalized cross-correlation measurement approaches to 1 if the difference between the two digital images approaches to zero. Normalized cross-correlation is defined as:

$$NCC = \frac{\sum_{j=1}^m \sum_{k=1}^n P_{jk} \times C_{jk}}{\sum_{k=1}^n (P_{jk})^2},$$

where $m \times n$ is taken as the size of standard and encrypted images.

Structural Content (SC)

It deals with the structural place of pixels in any image. It is used to measures the likeliness of any two images. This metric yields the close connections of two images so that one can differentiate between two images. Its higher value represents the low quality of an image. When two approximately similar images are considered, its value approaches to 1. Also, it is used in steganographic and radar applications. Hence it is a worldwide measurement which is calculated by the formula:

$$SC = \frac{\sum_{j=1}^m \sum_{k=1}^n (P_{jk})^2}{\sum_{j=1}^m \sum_{k=1}^n (C_{jk})^2}.$$

On account of the plain and encrypted images, the estimation of SC is always different from

unity because the encryption scheme includes confusion and diffusion-like noise and commotion in the original image. The estimation of SC isn't near one if there should be an occurrence of all advanced standard shading images (red, green and blue layers) (see Table 38).

Table 38. Pixel modification based and similarity measurements

Image	Layer	Pixel Difference Measures					Similarity Measures	
		MSE	PSNR	AD	MD	NAE	NCC	SC
Lena	Red	10637	7.8625	52.3109	255	0.4674	0.6598	1.6004
	Green	9245.2	8.4716	-28.9211	235	0.7968	0.9983	0.5788
	Blue	7169.4	9.5760	-22.2776	229	0.6713	1.0952	0.5632
Baboon	Red	8740.1	8.7156	1.9610	255	0.5938	0.8259	0.9174
	Green	7802.8	9.2083	-5.9805	230	0.6025	0.9106	0.7810
	Blue	9714.3	8.2567	-21.8818	244	0.7670	0.9038	0.6819

6.5 Entropy Investigation

It is used to examine the amount of divergence of the grayscale estimations of the standard and encrypted images. Its bigger value indicates the poor quality of an image. The most suitable encrypted image in 256 greyscales has entropy 8 in the perfect world [31]. On the off chance that, if the entropy of an encrypted image is under 8, then the encrypted algorithm is supposed weak which increases the possible risk of anticipating the security. Mathematically, the entropy E of a data source y is defined as:

$$E = - \sum_{i=0}^{2^N-1} P(y_i) \log_2 P(y_i),$$

where 2^N are all possible states of information and y_i are the source images. In Table 39, the entropies of different plain and enciphered image entropies are given as demonstrated by the plain images in figures 17, 18. These values are very close to the theoretical value which is 8. Consequently, information spillage in our encryption is negligible and well secured for physical attacks. We have looked at data entropy for our proposed encryption method with the

already developed encryption plans. Table 40 shows that the entropy of the offered scheme for the scrambled images are better than the already available algorithms.

Table 39. Entropies of standard and encrypted images

Image	Layer	Standard	Altered	Encrypted	Encrypted Altered
Lena	Red	7.2352	7.2353	7.9965	7.9975
	Green	7.5812	7.5814	7.9970	7.9970
	Blue	7.5682	7.5683	7.9971	7.9971
Baboon	Red	7.7766	7.7766	7.9965	7.9967
	Green	7.4911	7.4911	7.9968	7.9973
	Blue	7.7546	7.7546	7.9973	7.9973

Table 40. Comparison between the entropies for 256×256 Lena image

Algorithm	Entropy
Proposed	7.9968
Sun's algorithm [65]	7.9965
Baptista's algorithm [65]	7.9260
Wong's algorithm [65]	7.9690
Xiang's algorithm [65]	7.9950

In Tables 40 and 41, we compare the entropy of the proposed algorithm to the already defined algorithms. Our entropies are approximately equal to 8, which is the most suitable value. This minimizes the chance of data spillage during the encryption. Consequently, the proposed cryptosystem is perfectly secure against any entropy assault. Besides, the entropy investigations of the proposed scheme are better than the previously proposed encryption schemes [58, 61, 37,

Table 41. Comparison between entropy investigations of the proposed and already defined algorithms

Encryption Techniques	Test Image	colour Components of Original Image			colour Components of Encrypted Image		
		Red	Green	Blue	Red	Green	Blue
		Proposed scheme	Lena	7.2933	7.5812	7.5682	7.9965
Reference [61]	Lena	7.2933	7.5812	7.5682	7.9903	7.9890	7.9893
Reference [37]	Lena	7.2933	7.5812	7.5682	7.9732	7.9750	7.9715
Reference [36]	Lena	7.2933	7.5812	7.5682	7.9791	7.9802	7.9827
Reference[37]	Lena	7.2933	7.5812	7.5682	7.9871	7.9881	7.9878
Reference [36]	Lena	7.2933	7.5812	7.5682	7.9874	7.7872	7.7866
Reference [28]	Lena	7.2933	7.5812	7.5682	7.9278	7.9744	7.9705

6.6 Conclusion

In this chapter, we have provided a new idea for the construction of an image encryption technique using an algebraic structure namely inverse LA-group, which is non-commutative as well as non-associative simultaneously. This structure is one of the most important components in symmetric encryption. This new mechanism has added confusion, which is fundamentally responsible for breaking the pattern between the original and encrypted images.

Bibliography

- [1] S. Anis and M. Khan, Fuzzy soft set approach to ideal theory of regular AG-groupoids, *Seria Matematica*, 24(2016), 1-18.
- [2] S. E. Borujeni and M. Eshghi, Chaotic image encryption design using tompkins-paige algorithm, *Mathematical Problems in Engineering*, 2009, doi:10.1155/2009/762652.
- [3] M. Božinović, P. V. Protić and N. Stevanović, The natural partial order on the Abel-Grassmann's groupoids, *Filomat (Niš)*, 10(1996), 107-116.
- [4] M. Božinović, P. V. Protić and N. Stevanović, Kernel normal system of inverse AG^{**}-groupoids, *Quasigroups and Related Systems*, 17(2008), 1-8.
- [5] C. M. Campbell, E. F. Robertson and R. M. Thomas, On a class of semigroups with symmetric presentations, *Semigroup Forum*, 46(1993), 286-306.
- [6] C. M. Campbell, E. F. Robertson, N. Ruskuc and R. M. Thomas, Fibonacci semigroups, *Journal of Pure and Applied Algebra*, 94(1994), 49-57.
- [7] C. M. Campbell, E. F. Robertson, N. Ruskuc and R. M. Thomas, Semigroup and group presentations, *Bulletin of the London Mathematical Society*, 27(1995), 46-50.
- [8] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, American Mathematical Society, Vol. I, 1961.
- [9] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Akadémia Kiadó, Budapest, 1974.

- [10] A. Distler and J. D. Mitchell, Smallsemi-a GAP package (2008), <http://turnbull.mcs.st-and.ac.uk/~jamesm/smallsemi/>.
- [11] A. Distler and T. Kelsey, The monoids of orders eight, nine & ten, *Annals of Mathematics and Artificial Intelligence*, 56(2009), 3-21.
- [12] A. Distler, Classification and enumeration of finite semigroups, PhD Thesis, University of St Andrews, Scotland, 2010.
- [13] A. Distler, M. Shah and V. Sorge, Enumeration of AG-groupoids, In *Intelligent Computer Mathematics. CICM 2011. Lecture Notes in Computer Science*, 6824(2011), 1-14.
- [14] A. Distler and J. D. Mitchell, Smallsemi-a GAP package, (2012), <http://tinyurl.com/jdmitchell/smallsemi/>.
- [15] A. Distler, C. Jefferson, T. Kelsey and L. Hotthoff, The semigroups of order 10, In *Principles and Practice of Constraint Programming. CP 2012. Lecture Notes in Computer Science*, 7514(2012), 883-889.
- [16] W. A. Dudek and R. S. Gigoń, Congruences on completely inverse AG^{**}-groupoids, *Quasigroups and Related Systems*, 20(2012), 203-209.
- [17] W. A. Dudek and R. S. Gigoń, Completely inverse AG^{**}-groupoids, *Semigroup Forum*, 87(2013), 201-229.
- [18] S. Eilenberg, *Automata, languages and machines*, Vol. B, Academic Press, London, 1976.
- [19] R. Enayatifar, H. Abdullah and I. F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, *Optics and Lasers in Engineering*, 56(2014), 83-93.
- [20] G. E. Forsythe, SWAC computes 126 distinct semigroups of order 4, *Proceedings of the American Mathematical Society*, 6(1955), 443-447.
- [21] J. A. Green, On the structure of semigroups, *Annals of Mathematics*, 54(1951), 163-172.
- [22] R. Hartwig, How to partially order regular elements, *Mathematica Japonica*, 25(1980), 1-13.

- [23] P. Holgate, Groupoids satisfying a simple invertive law, *The Mathematics Student*, 61(1992), 101-106.
- [24] J. M. Howie, *An introduction to semigroup theory*, Academic Press, London, 1976.
- [25] Z. Hua, F. Jin, B. Xu and H. Huang, 2D Logistic-Sine-coupling map for image encryption, *Signal Processing*, 149(2018), 148-161.
- [26] C. K. Huang and H. H. Nien, Multi chaotic systems based pixel shuffle for image encryption, *Optics Communications*, 282(2009), 2123-2127.
- [27] J. Ježek and T. Kepka, Modular groupoids, *Czechoslovak Mathematical Journal*, 34(1984), 477-487.
- [28] A. Kadir, A. Hamdulla and W. Guo, Colour image encryption using skew tent map and hyper chaotic system of 6th-order CNN, *Optik-International Journal of Light and Electron Optics*, 125(2014), 1671-1675.
- [29] M. Khan, Q. Mushtaq and S. Anis, A Note on Abel-Grassmann's groupoids, *Research Journal of Applied Sciences, Engineering and Technology*, 7(2014), 1705-1709.
- [30] M. Khan, F. Smarandache and S. Afzal, Neutrosophic set approach for characterizations of left almost semigroup, *Neutrosophic Sets and Systems*, 11(2016), 79-94.
- [31] M. Khan, A novel image encryption scheme based on multiple chaotic S-boxes, *Nonlinear Dynamics*, 82(2015), 527-533.
- [32] M. Khan and T. Shah, Construction and applications of chaotic S-boxes in image encryption, *Neural Computing and Applications*, 27(2016), 677-685.
- [33] M. Khan, T. Shah and S. I. Batool, A new approach for image encryption and watermarking based on substitution box over the classes of chain rings, *Multimedia Tools and Applications*, 76(2017), 24027-24062.
- [34] M. V. Lawson, *Inverse semigroups: The theory of partial symmetries*, World Scientific, Singapore, 1998.

- [35] C. Li, D. Lin, J. Lü and F. Hao, Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography, *IEEE MultiMedia*, 25(2018), 46-56.
- [36] H. Liu and X. Wang, Colour image encryption using spatial bit level permutation and high-dimension chaotic system, *Optics Communications*, 284(2011), 3895-3903.
- [37] H. Liu, X. Wang and A. Kadir, Colour image encryption using Choquet fuzzy integral and hyper chaotic system, *Optik-International Journal of Light and Electron Optics*, 124(2013), 3527-3533.
- [38] M. E. Malandro, Enumeration of inverse semigroups, arXiv: 1312.7192v2[math.CO], 2015.
- [39] H. Mitsch, A natural partial order for semigroups, *Pocceedinngs of the American Mathematical Society*, 97(1986),384-388.
- [40] Q. Mushtaq and S. M. Yusuf, On LA-semigroups, *The Aligarh Bulletin of Mathematics*, 8(1978), 65-70.
- [41] Q. Mushtaq and S. M. Yusuf, On locally associative LA-semigroups, *Journal of Natural Sciences and Mathematics*, 19(1979), 57-62.
- [42] Q. Mushtaq, Abelian groups defined by LA-semigroups, *Studia Scientiarum Mathematicarum Hungarica*, 18(1983), 427-428.
- [43] Q. Mushtaq and S. M. Yusuf, On LA-semigroup defined by a commutative inverse semigroup, *Matematicki Vesnik*, 40(1988), 59-62.
- [44] Q. Mushtaq and M. S. Kamran, On LA-semigroups with weak associative law, *Scientific Khyber*, 2(1989), 69-71.
- [45] Q. Mushtaq and Q. Iqbal, Decomposition of a locally associative LA-semigroup, *Semigroup Forum*, 41(1990), 155-164.
- [46] Q. Mushtaq and M. Iqbal, On representation theorem for inverse LA-semigroups, *Pakistan Academy of Sciences*, 4(1993), 247-254.
- [47] Q. Mushtaq and M. Khan, Ideals in AG-band and AG*-groupoid, *Quasigroups and Related Systems*, 14(2006), 207-215.

- [48] Q. Mushtaq and M. Khan, Semilattice decomposition of a locally associative AG^{**} -groupoid, *Algebra Colloquium*, 16(2009), 17-22.
- [49] K. Nambooripad, The natural partial order on a regular semigroup, *Proceedings of the Edinburgh Mathematical Society*, 23(1980), 249-260.
- [50] M. Naseeruddin, Some studies on almost semigroups and flocks, PhD Thesis, The Aligarh Muslim University, India, 1970.
- [51] B. H. Neumann, Some remarks on semigroup presentations. *Canadian Journal of Mathematics*, 19(1967), 1018-1026.
- [52] P. V. Protić and N. Stevanović, On Abel-Grassmann's groupoids (exposition), *Proceedings of Mathematical Conference*, Pristina, 1994, 27-29.
- [53] P. V. Protić and N. Stevanović, AG-test and some general properties of Abel-Grassmann's groupoids, *Pure Mathematics and Applications*, 6(1995), 371-383.
- [54] P. V. Protić and M. Božinović, Some congruences on an AG^{**} -groupoid, *Filomat (Niš)*, 9(1996), 879-886.
- [55] P. V. Protić and N. Stevanović, Abel-Grassmann's bands, *Quasigroups and Related Systems*, 11(2004), 95-101.
- [56] P. V. Protić, Congruences on an inverse AG^{**} -groupoid via the natural partial order, *Quasigroups and Related Systems*, 17(2009), 283-290.
- [57] A. Rafiq and M. Khan, Construction of new S-boxes based on triangle groups and its applications in copyright protection, *Multimedia Tools and Applications*, (2018), 1-18. <https://doi.org/10.1007/s11042-018-6953-x>
- [58] R. Rhouma, S. Meherzi and S. Belghith, OCML-based colour image encryption, *Chaos Soliton & Fractals*, 40(2009), 309-318.
- [59] N. Ruskuc, Semigroup presentations, PhD Thesis, University of St Andrews, Scotland, 1995.

- [60] N. J. A. Sloane, The on-line encyclopedia of integer sequences, (2008), <http://www.research.att.com/~njas/sequences/Seis.html>.
- [61] X. Wu, K. Wang, X. Wang and H. Kan, Lossless chaotic colour image cryptosystem based on DNA encryption and entropy, *Nonlinear Dynamics*, 90(2017), 855-875.
- [62] N. Yaqoob, Applications of rough sets to Γ -hyperideals in left almost Γ -semihypergroups, *Neural Computing and Applications*, 21(2012), 267-273.
- [63] N. Yaqoob, R. Chinram, A. Ghareeb and M. Aslam, Left almost semigroups characterized by their interval valued fuzzy ideals, *Afrika Matematika*, 24(2013), 231-245.
- [64] L. Zhang, X. Liao and X. Wang, An image encryption approach based on chaotic maps, *Chaos Solitons & Fractals*, 24(2005), 759-765.
- [65] G. Zhang and Q. Liu, A novel image encryption method based on total shuffling scheme, *Optics Communications*, 284(2011), 2775-2780.
- [66] P. Zhen, G. Zhao, L. Min and X. Jin, Chaos-based image encryption scheme combining DNA coding and entropy, *Multimedia Tools and Applications*, 75(2016), 6303-6319.
- [67] Q. Zhou, K. Wong, X. Liao, T. Xiang and Y. Hu, Parallel image encryption algorithm based on discretized chaotic map, *Chaos Solitons & Fractals*, 38(2008), 1081-1092.