

## Article

# Inverse Properties in Neutrosophic Triplet Loop and Their Application to Cryptography

Temitope Gbolahan Jaiyeola <sup>1</sup>  and Florentin Smarandache <sup>2,\*</sup> <sup>1</sup> Department of Mathematics, Obafemi Awolowo University, Ile Ife 220005, Nigeria; tjayeola@oauife.edu.ng<sup>2</sup> Department of Mathematics and Science, University of New Mexico, 705 Gurley Ave., Gallup, NM 87301, USA

\* Correspondence: smarand@unm.edu; Tel.: +1-505-863-7647

Received: 7 February 2018; Accepted: 12 March 2018; Published: 16 March 2018

**Abstract:** This paper is the first study of the neutrosophic triplet loop (NTL) which was originally introduced by Florentin Smarandache. NTL originated from the neutrosophic triplet set  $X$ : a collection of triplets  $(x, neut(x), anti(x))$  for an  $x \in X$  which obeys some axioms (existence of neutral(s) and opposite(s)). NTL can be informally said to be a neutrosophic triplet group that is not associative. That is, a neutrosophic triplet group is an NTL that is associative. In this study, NTL with inverse properties such as: right inverse property (RIP), left inverse property (LIP), right cross inverse property (RCIP), left cross inverse property (LCIP), right weak inverse property (RWIP), left weak inverse property (LWIP), automorphic inverse property (AIP), and anti-automorphic inverse property are introduced and studied. The research was carried out with the following assumptions: the inverse property (IP) is the RIP and LIP, cross inverse property (CIP) is the RCIP and LCIP, weak inverse property (WIP) is the RWIP and LWIP. The algebraic properties of neutrality and opposite in the aforementioned inverse property NTLs were investigated, and they were found to share some properties with the neutrosophic triplet group. The following were established: (1) In a CIPNTL (IPNTL), RIP (RCIP) and LIP (LCIP) were equivalent; (2) In an RIPNTL (LIPNTL), the CIP was equivalent to commutativity; (3) In a commutative NTL, the RIP, LIP, RCIP, and LCIP were found to be equivalent; (4) In an NTL, IP implied anti-automorphic inverse property and WIP, RCIP implied AIP and RWIP, while LCIP implied AIP and LWIP; (5) An NTL has the IP (CIP) if and only if it has the WIP and anti-automorphic inverse property (AIP); (6) A CIPNTL or an IPNTL was a quasigroup; (7) An LWIPNTL (RWIPNTL) was a left (right) quasigroup. The algebraic behaviours of an element, its neutral and opposite in the associator and commutator of a CIPNTL or an IPNTL were investigated. It was shown that  $(\mathbb{Z}_p, *)$  where  $x * y = (p - 1)(x + y)$ , for any prime  $p$ , is a non-associative commutative CIPNTL and IPNTL. The application of some of these varieties of inverse property NTLs to cryptography is discussed.

**Keywords:** neutrosophic; triplet loop; quasigroup; loop; generalized group; neutrosophic triplet group; group; cryptography

## 1. Introduction

### 1.1. Generalized Group

A generalized group is an algebraic structure which has a deep physical background in the unified gauge theory and has direct relation with isotopies. Mathematicians and physicists have been trying to construct a suitable unified theory for twistor theory, isotopies theory, and so on. It was known that generalized groups are tools for constructions in unified geometric theory and electroweak theory. Electroweak theories are essentially structured on Minkowskian axioms, and gravitational theories are

constructed on Riemannian axioms. According to Araujo et. al. [1], the generalized group is equivalent to the notion of a completely simple semigroup.

Some of the structures and properties of generalized groups have been studied by Vagner [2], Molaei [3], [4], Mehrabi, Molaei, and Oloomi [5], Agboola [6], Adeniran et al. [7], and Fatehi and Molaei [8]. Smooth generalized groups were introduced in Agboola [9], and later Agboola [10] also presented smooth generalized subgroups while Molaei [11], Molaei and Tahmoresi [12] considered the notion of topological generalized groups, and Maleki and Molaei [13] studied the quotient space of generalized groups.

**Definition 1.** (Generalized Group)

A generalized group  $G$  is a non-empty set admitting a binary operation called multiplication, subject to the set of rules given below.

- (i)  $(xy)z = x(yz)$  for all  $x, y, z \in G$ .
- (ii) For each  $x \in G$ , there exists a unique  $e(x) \in G$  such that  $xe(x) = e(x)x = x$  (existence and uniqueness of identity element).
- (iii) For each  $x \in G$ , there exists  $x^{-1} \in G$  such that  $xx^{-1} = x^{-1}x = e(x)$  (existence of inverse element).

**Definition 2.** Let  $L$  be a non-empty set. Define a binary operation  $(\cdot)$  on  $L$ . If  $x \cdot y \in L$  for all  $x, y \in L$ ,  $(L, \cdot)$  is called a groupoid.

If the equation  $a \cdot x = b$  (resp.  $y \cdot a = b$ ) has a unique solution relative to  $x$  (resp.  $y$ ) (i.e., obeys the left (resp. right) cancellation law), then  $(L, \cdot)$  is called a left (resp. right) quasigroup. If a groupoid  $(L, \cdot)$  is both a left quasigroup and right quasigroup, then it is called a quasigroup. If there exists an element  $e \in L$  called the identity element such that for all  $x \in L$ ,  $x \cdot e = e \cdot x = x$ , then a quasigroup  $(L, \cdot)$  is called a loop.

For more on quasigroups and loops, readers should check [14–20].

**Definition 3.** (Generalized loop)

A generalized loop is the pair  $(G, \cdot)$  where  $G$  is a non-empty set and “ $\cdot$ ” a binary operation such that the following are true.

- (i)  $(G, \cdot)$  is a groupoid.
- (ii) For each  $x \in G$ , there exists a unique  $e(x) \in G$  such that  $xe(x) = e(x)x = x$ .
- (iii) For each  $x \in G$ , there exists  $x^{-1} \in G$  such that  $xx^{-1} = x^{-1}x = e(x)$ .

A generalized group  $G$  exhibits the following properties:

- (i) For each  $x \in G$ , there exists a unique  $x^{-1} \in G$ .
- (ii)  $e(e(x)) = e(x)$  and  $e(x^{-1}) = e(x)$  whenever  $x \in G$ .
- (iii) If  $G$  is commutative, then  $G$  is a group.

## 1.2. Neutrosophic Triplet Group

Neutrosophy is a new branch of philosophy which studies the nature, origin, and scope of neutralities as well as their interaction with ideational spectra. In 1995, Florentin Smarandache [21] first introduced the concept of neutrosophic logic and neutrosophic sets where each proposition in neutrosophic logic is approximated to have the percentage of truth in a subset  $T$ , the percentage of indeterminacy in a subset  $I$ , and the percentage of falsity in a subset  $F$  so that this neutrosophic logic is called an extension of fuzzy logic, especially to intuitionistic fuzzy logic. In fact, the neutrosophic set is the generalization of classical sets [22], fuzzy sets [23], intuitionistic fuzzy sets [22,24] and interval valued fuzzy sets [22], to mention a few. This mathematical tool is used to handle problems consisting of uncertainty, imprecision, indeterminacy, inconsistency, incompleteness, and falsity. The development process of neutrosophic sets, fuzzy sets, and intuitionistic fuzzy sets are still growing, with various

applications; here are some recent research works in these directions [25–32]. By utilizing the idea of neutrosophic theory, Vasantha Kandasamy and Florentin Smarandache studied neutrosophic algebraic structures in [33–35] by introducing an indeterminate element “ $I$ ” in the algebraic structure and then combining “ $I$ ” with each element of the structure with respect to the corresponding binary operation  $*$ . This was called a neutrosophic element, and the generated algebraic structure was termed a neutrosophic algebraic structure. They further studied several neutrosophic algebraic structures, such as neutrosophic fields, neutrosophic vector spaces, neutrosophic groups, neutrosophic bigroups, neutrosophic  $N$ -groups, neutrosophic semigroups, neutrosophic bisemigroups, neutrosophic  $N$ -semigroups, neutrosophic loops, neutrosophic biloops, neutrosophic  $N$ -loops, neutrosophic groupoids, neutrosophic bigroupoids, and so on.

Smarandache and Ali [36] for the first time introduced the idea of the neutrosophic triplet, which they had previously discussed in [37]. They used these neutrosophic triplets to introduce the neutrosophic triplet group, which is different from the classical group both in structural and fundamental properties. They gave distinction and comparison of neutrosophic triplet group with the classical generalized group. They also drew a brief sketch of the possible applications of the neutrosophic triplet group in some other research areas. Jaiyéolá [38] studied new algebraic properties of the neutrosophic triplet group with new applications. Some new applications of neutrosophy were announced in Okpako and Asagba [39], Sahin and Kargin [40], Vasantha Kandasamy et al. [41], and Smarandache [42]. Agboola et al. [43] and Zhang et al. [44] are some recent works on neutrosophic triplet groups, neutrosophic quadruple, and neutrosophic duplet of algebraic structures.

**Definition 4.** (Neutrosophic Triplet Set)

Let  $X$  be a set together with a binary operation  $*$  defined on it. Then,  $X$  is called a neutrosophic triplet set if for any  $x \in X$ , there exists a neutral of “ $x$ ” denoted by  $\text{neut}(x)$  (not necessarily the identity element) and an opposite of “ $x$ ” denoted by  $\text{anti}(x)$  or  $xJ$ , with  $\text{neut}(x), \text{anti}(x) \in X$  such that:

$$x * \text{neut}(x) = \text{neut}(x) * x = x \quad \text{and} \quad x * \text{anti}(x) = \text{anti}(x) * x = \text{neut}(x).$$

The elements  $x, \text{neut}(x)$ , and  $\text{anti}(x)$  are collectively referred to as a neutrosophic triplet, and denoted by  $(x, \text{neut}(x), \text{anti}(x))$ .

**Remark 1.** For the same  $x \in X$ , each  $\text{neut}(x)$  and  $\text{anti}(x)$  may not be unique. In a neutrosophic triplet set  $(X, *)$ , an element  $y$  (resp.  $z$ ) is the second (resp. third) component of a neutrosophic triplet if there exist  $x, z \in X$  ( $x, y \in X$ ) such that  $x * y = y * x = x$  and  $x * z = z * x = y$ . Thus,  $(x, y, z)$  is the neutrosophic triplet.

**Example 1.** (Smarandache and Ali [36])

Consider  $(\mathbb{Z}_6, \times_6)$  where  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$  and  $\times_6$  is multiplication in modulo 6.  $(2, 4, 2), (4, 4, 4)$ , and  $(0, 0, 0)$  are neutrosophic triplets, but 3 does not give rise to a neutrosophic triplet.

**Definition 5.** (Neutrosophic Triplet Group)

Let  $(X, *)$  be a neutrosophic triplet set. Then,  $(X, *)$  is called a neutrosophic triplet group if  $(X, *)$  is a semigroup. If in addition,  $(X, *)$  obeys the commutativity law, then  $(X, *)$  is called a commutative neutrosophic triplet group.

**Remark 2.** A neutrosophic triplet group is not a group in general, but a group is a neutrosophic triplet group where  $\text{neut}(x) = e$  the general identity element for all  $x \in X$  and  $\text{anti}(x)$  is unique for each  $x \in X$ .

1. A generalized loop is a generalized group if and only if it is associative.
2. A neutrosophic triplet loop (NTL) is a neutrosophic triplet group if and only if it is associative.
3. An NTL is a generalized loop if and only if  $\text{neut}(x) = e(x)$  is unique for each  $x$ .
4. An NTL is a loop if and only if it is a quasigroup and  $\text{neut}(x) = \text{neut}(y)$  for all  $x, y$ .

**Example 2.** (Smarandache and Ali [36])

Consider  $(\mathbb{Z}_{10}, \otimes)$  where  $x \otimes y = 3xy \bmod 10$ .  $(\mathbb{Z}_{10}, \otimes)$  is a commutative neutrosophic triplet group but neither a classical group nor a generalized group.

**Example 3.** (Smarandache and Ali [36])

Consider  $(\mathbb{Z}_{10}, \star)$  where  $x \star y = 5x + y \bmod 10$ .  $(\mathbb{Z}_{10}, \star)$  is a non-commutative neutrosophic triplet group, but not a classical group.

**Theorem 1.** (Smarandache and Ali [36])

Let  $(X, *)$  be a neutrosophic triplet group. The following are true for all  $x, y, z \in X$ .

1.  $x * y = x * z \Leftrightarrow \text{neut}(x) * y = \text{neut}(x) * z$ .
2.  $y * x = z * x \Leftrightarrow y * \text{neut}(x) = z * \text{neut}(x)$ .
3.  $\text{anti}(x) * y = \text{anti}(x) * z \Rightarrow \text{neut}(x) * y = \text{neut}(x) * z$ .
4.  $y * \text{anti}(x) = z * \text{anti}(x) \Rightarrow y * \text{neut}(x) = z * \text{neut}(x)$ .
5.  $\text{neut}(x) * \text{neut}(x) = \text{neut}(x)$  i.e.,  $\text{neut}(\text{neut}(x)) = \text{neut}(x)$ .
6.  $\text{neut}(x)^n = \text{neut}(x)$  for any  $n \in \mathbb{N}$ ;  $\text{anti}(\text{neut}(x)) = \text{neut}(x)$ .
7.  $\text{neut}(x) * \text{anti}(x) = \text{anti}(x) * \text{neut}(x) = \text{anti}(x)$  i.e.  $\text{neut}(\text{anti}(x)) = \text{neut}(x)$ .

**Definition 6.** (Neutrosophic Triplet Loop—NTL)

Let  $(X, *)$  be a neutrosophic triplet set. Then,  $(X, *)$  is called a neutrosophic triplet loop if  $(X, *)$  is a groupoid. If in addition,  $(X, *)$  obeys the commutativity law, then  $(X, *)$  is called a commutative neutrosophic triplet loop.

Let  $(X, *)$  be a neutrosophic triplet loop. If  $\text{neut}(xy) = \text{neut}(x)\text{neut}(y)$  for all  $x, y \in X$ , then  $X$  is called normal.

**Remark 3.** An NTL is a neutrosophic triplet group if and only if it is associative. Thus, an NTL is a generalization of a neutrosophic triplet group, and it is interesting to study an NTL that obeys weak associative law. NTL was originally introduced by Florentin Smarandache.

**Example 4.** Let  $(\mathbb{Z}_{10}, +, \cdot)$  be the field of integers modulo 10. Consider  $(\mathbb{Z}_{10}, *)$ , where for all  $x, y \in \mathbb{Z}_{10}$ ,  $x * y = 2x + 2y$ . The following are neutrosophic triplets:

$$(0, 0, 0), (0, 0, 5), (2, 4, 0), (2, 4, 5), (4, 8, 0), (4, 8, 5), (6, 2, 0), (6, 2, 5), (8, 6, 0), (8, 6, 5)$$

in  $(\mathbb{Z}_{10}, *)$ . Thus,  $\{0, 2, 4, 5, 6, 8\}$  is a neutrosophic triplet set.  $(\mathbb{Z}_{10}, *)$  is non-associative because  $(x * y) * z = 4x + 4y + 2z \neq x * (y * z) = 2x + 4y + 4z$ .  $(\mathbb{Z}_{10}, *)$  is a non-associative NTL (i.e., not a neutrosophic triplet group) with  $2 * \text{neut}(x) = 9x$  and  $4 * \text{anti}(x) = 5x$ .

**Definition 7.** (Inverse Properties and Neutrosophic Triplet Loop)

$(X, *)$  will be called a right inverse property neutrosophic triplet loop (RIPNTL) if it obeys the right inverse property (RIP)

$$(y * x) * \text{anti}(x) = y \quad (1)$$

$(X, *)$  will be called a left inverse property neutrosophic triplet loop (LIPNTL) if it obeys the left inverse property (LIP)

$$\text{anti}(x) * (x * y) = y \quad (2)$$

$(X, *)$  will be called an inverse property neutrosophic triplet loop if it obeys both (1) and (2).

$(X, *)$  will be called a left cross inverse property neutrosophic triplet loop (LCIPNTL) if it obeys the left cross inverse property (LCIP)

$$\text{anti}(x) * (y * x) = y \quad (3)$$

$(X, *)$  will be called a right cross inverse property neutrosophic triplet loop (RCIPNTL) if it obeys the right cross inverse property (RCIP)

$$(x * y) * \text{anti}(x) = y \quad (4)$$

$(X, *)$  will be called a cross inverse property neutrosophic triplet loop (CIPNTL) if it obeys both (3) and (4).

$(X, *)$  will be called a right weak inverse property neutrosophic triplet loop (RWIPNTL) if it obeys the right weak inverse property (RWIP)

$$x * \text{anti}(y * x) = \text{anti}(y) \quad (5)$$

$(X, *)$  will be called a left weak inverse property neutrosophic triplet loop (LWIPNTL) if it obeys the left weak inverse property (LWIP)

$$\text{anti}(x * y) * x = \text{anti}(y) \quad (6)$$

$(X, *)$  will be called a weak inverse property neutrosophic triplet loop (WIPNTL) if it obeys both (5) and (6).

$(X, *)$  will be called an automorphic inverse property neutrosophic triplet loop (AIPNTL) if it obeys the automorphic inverse property (AIP)

$$\text{anti}(x * y) = \text{anti}(x) * \text{anti}(y) \quad (7)$$

$(X, *)$  will be called an antiautomorphic inverse property neutrosophic triplet loop (AAIPNTL) if it obeys the antiautomorphic inverse property (AAIP)

$$\text{anti}(x * y) = \text{anti}(y) * \text{anti}(x) \quad (8)$$

$(X, *)$  will be called a semi-automorphic inverse property neutrosophic triplet loop (SAIPNTL) if it obeys the semi-automorphic inverse property (SAIP)

$$\text{anti}((x * y) * x) = (\text{anti}(x) * \text{anti}(y)) * \text{anti}(x) \quad (9)$$

**Definition 8.** (Associators and Commutators of Neutrosophic Triplet Loop)

Let  $(X, *)$  be an NTL. For any  $x, y, z \in X$ ,

1.  $(x, y, z) \in X$  is called the right associator of  $x, y, z$  if  $xy * z = (x * yz)(x, y, z)$ .
2.  $[x, y, z] \in X$  is called the left associator of  $x, y, z$  if  $xy * z = [x, y, z](x * yz)$ .
3.  $(x, y) \in X$  is called the right commutator of  $x, y$  if  $x * y = (y * x)(x, y)$ .
4.  $[x, y] \in X$  is called the right commutator of  $x, y$  if  $x * y = [x, y](y * x)$ .

This paper is the first study of a class of neutrosophic triplet loop (NTL) containing varieties of inverse property NTLs and the application of some of them to cryptography. The second section contains the main results on the varieties of inverse property NTLs in Definition 7 and the interrelationships. The algebraic properties of their neutrality and opposite were investigated, and were found to share some properties with the neutrosophic triplet group. An example of these varieties of NTL is given. Summaries of the results in the second section are exhibited as two Hasse diagrams in Figure 1. The third section discusses the application of some of these varieties of inverse property NTLs to cryptography.

## 2. Main Results

**Lemma 1.** Let  $X$  be a CIPNTL. Then:

1.  $\text{neut}(x) = \text{neut}(\text{anti}(x))$ ,  $\text{anti}(\text{anti}(x)) = x$  and  $J^2 = I$ .
2.  $L_x R_{\text{anti}(x)} = I = R_x L_{\text{anti}(x)}$ .

3.  $X$  is an RIPNTL if and only  $X$  is an LIPNTL.
4.  $\text{neut}(x) = \text{anti}(\text{neut}(x))$  and  $\text{neut}(\text{neut}(x)) = \text{neut}(x)\text{neut}(x)$ .

**Proof.**

1. Put  $y = \text{anti}(x)$  in (4) to get  $x \text{ anti}(x) * \text{anti}(x) = \text{anti}(x) \Rightarrow$

$$\text{neut}(x)\text{anti}(x) = \text{anti}(x) \quad (10)$$

Put  $y = \text{anti}(x)$  in (3) to get  $\text{anti}(x) * \text{anti}(x)x = \text{anti}(x) \Rightarrow$

$$\text{anti}(x)\text{neut}(x) = \text{anti}(x) \quad (11)$$

By (10) and (11), we have  $\text{neut}(x) = \text{neut}(\text{anti}(x))$ . By this,  $\text{anti}(x)x = x \text{ anti}(x) = \text{neut}(x) \Rightarrow \text{anti}(\text{anti}(x)) = x$  and  $J^2 = I$ .

2. These are just (3) and (4) put in translation forms.
3. From 2.,  $L_x R_{\text{anti}(x)} R_x L_{\text{anti}(x)} = I$ . So,  $R_{\text{anti}(x)} R_x = I \Rightarrow L_x R_{\text{anti}(x)} \Leftrightarrow y \text{ anti}(x) * x = y \Rightarrow \text{anti}(x) * xy = y \Leftrightarrow y \text{ anti}(\text{anti}(x)) * \text{anti}(x) = y \Rightarrow \text{anti}(x) * xy = y \Leftrightarrow yx * \text{anti}(x) = y \Rightarrow \text{anti}(x) * xy = y \Leftrightarrow X$  has the RIP, which implies that  $X$  has the LIP. Similarly, since by 2.,  $R_x L_{\text{anti}(x)} L_x R_{\text{anti}(x)} = I$ , then we get  $X$  has the LIP implies  $X$  has the RIP.
4. Let  $x \in X$ . Recall that  $x \text{ neut}(x) = x = \text{neut}(x)x$ . So, by the RCIP,  $\text{neut}(x)x * \text{anti}(\text{neut}(x)) = x \text{ anti}(\text{neut}(x)) \Rightarrow$

$$x \text{ anti}(\text{neut}(x)) = x. \quad (12)$$

Similarly, by the LCIP,

$$\text{anti}(\text{neut}(x))x = x. \quad (13)$$

Thus, by (12) and (13),  $\text{neut}(x) = \text{anti}(\text{neut}(x))$ . Furthermore,  $\text{neut}(x)\text{neut}(x) = \text{anti}(\text{neut}(x))\text{neut}(x) = \text{neut}(x)\text{anti}(\text{neut}(x)) \Rightarrow \text{neut}(\text{neut}(x)) = \text{neut}(x)\text{neut}(x)$ .

□

**Lemma 2.** Let  $X$  be a CIPNTL or an IPLNTL. Then:

1. Equations  $a * x = b$  and  $y * c = d$  have solutions for  $x, y \in X$  and these solutions are unique for all  $a, b, c, d \in X$ . (unique solvability)
2. The cancellation laws hold.
3. The right and left translation maps  $R_a$  and  $L_a$  are bijections for all  $a \in X$ .

**Proof.** For CIPNTL.

1.  $a * x = b \Rightarrow (a * x)\text{anti}(a) = b \text{ anti}(a) \Rightarrow x = b \text{ anti}(a) \in X$ . Similarly,  $y * c = d \Rightarrow \text{anti}(c)(y * c) = \text{anti}(c)d \Rightarrow y = \text{anti}(c)d$ .

Let  $x_1, x_2 \in X$  such that  $a * x_1 = b = a * x_2 \Rightarrow (a * x_1)\text{anti}(a) = (a * x_2)\text{anti}(a) \Rightarrow x_1 = x_2$ .

2. This follows from 1.
3.  $R_a : X \rightarrow X$  given by  $xR_a = x * a$ .  $R_a$  is a bijection if and only if the equation  $x * a = b$  is uniquely solvable for  $x$  for all  $a, b \in X$ .  $L_a : X \rightarrow X$  given by  $xL_a = a * x$ .  $L_a$  is a bijection if and only if the equation  $a * x = b$  is uniquely solvable for  $x$  for all  $a, b \in X$ .

For IPNTL.

1.  $a * x = b \Rightarrow \text{anti}(a)(a * x) = \text{anti}(a)b \Rightarrow x = \text{anti}(a)b \in X$ . Similarly,  $y * c = d \Rightarrow (y * c)\text{anti}(c) = d \text{ anti}(c) \Rightarrow y = d \text{ anti}(c)$ .

Let  $x_1, x_2 \in X$  such that  $a * x_1 = b = a * x_2 \Rightarrow \text{anti}(a)(a * x_1) = \text{anti}(a)(a * x_2) \Rightarrow x_1 = x_2$ .



2. This follows from above.
3.  $R_a : X \rightarrow X$  given by  $xR_a = x * a$ .  $R_a$  is a bijection if and only if the equation  $x * a = b$  is uniquely solvable for  $x$  for all  $a, b \in X$ .  $L_a : X \rightarrow X$  given by  $xL_a = a * x$ .  $L_a$  is a bijection if and only if the equation  $a * x = b$  is uniquely solvable for  $x$  for all  $a, b \in X$ .

□

**Theorem 2.** Let  $X$  be an NTL.

1.  $X$  is an RCIPNTL if and only if  $x * y \text{ anti}(x) = y$ .
2.  $X$  is an LCIPNTL if and only if  $\text{anti}(x)y * x = y$ .
3.  $X$  is a CIPNTL if and only if  $x * y \text{ anti}(x) = y = \text{anti}(x)y * x$ .

**Proof.**

1. By Lemma 2, if  $X$  is an RCIPNTL, then it is a left quasigroup and  $L_a$  is a bijection for  $a \in X$ . Consider an NTL which has the property  $x * y \text{ anti}(x) = y$ . Put  $y = \text{neut}(\text{anti}(x))$  to get  $x * \text{neut}(\text{anti}(x))\text{anti}(x) = \text{neut}(\text{anti}(x)) \Rightarrow x * \text{anti}(x) = \text{neut}(\text{anti}(x)) \Rightarrow \text{neut}(x) = \text{neut}(\text{anti}(x)) \Rightarrow \text{anti}(\text{anti}(x)) = x$ . Thus,  $x * a = b \Rightarrow x * \text{anti}(\text{anti}(a)) = b \Rightarrow \text{anti}(a)(x * \text{anti}(\text{anti}(a))) = \text{anti}(a)b \Rightarrow x = \text{anti}(a)b$ . Let  $x_1, x_2 \in X$ . Then,  $x_1 * a = x_2 * a \Rightarrow x_1 * \text{anti}(\text{anti}(a)) = x_2 * \text{anti}(\text{anti}(a)) \Rightarrow \text{anti}(a)(x_1 * \text{anti}(\text{anti}(a))) = \text{anti}(a)(x_2 * \text{anti}(\text{anti}(a))) \Rightarrow x_1 = x_2$ . So,  $x * a = b$  is uniquely solvable for  $x$  that  $R_a$  is bijective. RCIP implies  $L_x R_{\text{anti}(x)} = I \Rightarrow R_{\text{anti}(x)} = L_x^{-1} \Rightarrow R_{\text{anti}(x)} L_x = I \Rightarrow x * y \text{ anti}(x) = y$ . Conversely,  $x * y \text{ anti}(x) = y \Rightarrow R_{\text{anti}(x)} L_x = I \Rightarrow L_x = R_{\text{anti}(x)}^{-1} \Rightarrow L_x R_{\text{anti}(x)} = I \Rightarrow \text{RCIP}$ .
2. By Lemma 2, if  $X$  is an LCIPNTL, then it is a right quasigroup and  $R_a$  is a bijection for  $a \in X$ . Consider an NTL which has the property  $\text{anti}(x)y * x = y$ . Put  $y = \text{neut}(\text{anti}(x))$  to get  $\text{anti}(x)\text{neut}(\text{anti}(x)) * x = \text{neut}(\text{anti}(x)) \Rightarrow \text{anti}(x) * x = \text{neut}(\text{anti}(x)) \Rightarrow \text{neut}(x) = \text{neut}(\text{anti}(x)) \Rightarrow \text{anti}(\text{anti}(x)) = x$ . Thus,  $a * x = b \Rightarrow \text{anti}(\text{anti}(a)) * x = b \Rightarrow (\text{anti}(\text{anti}(a)) * x)\text{anti}(a) = b \text{ anti}(a) \Rightarrow x = b \text{ anti}(a)$ . Let  $x_1, x_2 \in X$ . Then,  $a * x_1 = a * x_2 \Rightarrow \text{anti}(\text{anti}(a)) * x_1 = \text{anti}(\text{anti}(a)) * x_2 \Rightarrow (\text{anti}(\text{anti}(a)) * x_1)\text{anti}(a) = (\text{anti}(\text{anti}(a)) * x_2)\text{anti}(a) \Rightarrow x_1 = x_2$ . So,  $a * x = b$  is uniquely solvable for  $x$  that  $L_a$  is bijective. LCIP implies  $R_x L_{\text{anti}(x)} = I \Rightarrow R_x^{-1} = L_{\text{anti}(x)} \Rightarrow L_{\text{anti}(x)} R_x = I \Rightarrow \text{anti}(x)y * x = y$ . Conversely,  $\text{anti}(x)y * x = y \Rightarrow L_{\text{anti}(x)} R_x = I \Rightarrow L_{\text{anti}(x)}^{-1} = R_x \Rightarrow R_x L_{\text{anti}(x)} = I \Rightarrow \text{LCIP}$ .
3. This follows from 1. and 2.

□

**Lemma 3.** Let  $X$  be an IPNL. Then:

1.  $\text{neut}(x) = \text{neut}(\text{anti}(x))$ ,  $\text{anti}(\text{anti}(x)) = x$  and  $J^2 = I$ .
2.  $R_x R_{\text{anti}(x)} = I = L_x L_{\text{anti}(x)}$ .
3.  $X$  is an RCIPNL if and only if  $X$  is an LCIPNL.
4.  $\text{neut}(x) = \text{anti}(\text{neut}(x))$  and  $\text{neut}(\text{neut}(x)) = \text{neut}(x)\text{neut}(x)$ .

**Proof.**

1. Put  $y = \text{anti}(x)$  in (1) to get  $\text{anti}(x)x * \text{anti}(x) = \text{anti}(x) \Rightarrow$

$$\text{neut}(x)\text{anti}(x) = \text{anti}(x) \quad (14)$$

Put  $y = \text{anti}(x)$  in (2) to get  $\text{anti}(x) * x \text{ anti}(x) = \text{anti}(x) \Rightarrow$

$$\text{anti}(x)\text{neut}(x) = \text{anti}(x) \quad (15)$$

By (14) and (15), we have  $neut(x) = neut(anti(x))$ . By this,  $anti(x)x = x anti(x) = neut(x) \Rightarrow anti(anti(x)) = x$  and  $J^2 = I$ .

2. These are just (1) and (2) put in translation forms.
3. Keep Theorem 2 in mind. From 2.,  $R_x R_{anti(x)} L_x L_{anti(x)} = I$ . So,  $R_{anti(x)} L_x = I \Rightarrow R_x L_{anti(x)} \Leftrightarrow x * y anti(x) = y \Rightarrow anti(x) * yx = y \Leftrightarrow X$  has the RCIP implies  $X$  has the LCIP. Similarly, since by 2.,  $L_x L_{anti(x)} R_x R_{anti(x)} = I$ , then we get  $X$  has the LCIP implies  $X$  has the RCIP.
4. Let  $x \in X$ . Recall that  $x neut(x) = x = neut(x)x$ . So, by the RIP,  $x neut(x) * anti(neut(x)) = x anti(neut(x)) \Rightarrow$

$$x anti(neut(x)) = x. \quad (16)$$

Similarly, by the LIP,

$$anti(neut(x))x = x. \quad (17)$$

Thus, by (16) and (17),  $neut(x) = anti(neut(x))$ . Furthermore,  $neut(x)neut(x) = anti(neut(x))neut(x) = neut(x)anti(neut(x)) \Rightarrow neut(neut(x)) = neut(x)neut(x)$ .

□

**Theorem 3.** Let  $X$  be a CIPNTL. For all  $x, y \in X$ ,

1.  $(x, x, anti(x)) = neut(x) = [x, x, anti(x)]$ .
2.  $(x, y, anti(x)) = neut(y) = [x, y, anti(x)]$ .
3.  $(anti(x), x, x) = neut(x) = [anti(x), x, x]$ .
4.  $(anti(x), y, x) = neut(y) = [anti(x), y, x]$ .
5.  $(x, neut(x)) = neut(x) = [x, neut(x)]$ .
6.  $(neut(x), x) = neut(x) = [neut(x), x]$ .
7.  $(x, x) = neut(xx) = [x, x]$ .
8.  $(x, anti(x)) = neut(neut(x)) = [x, anti(x)]$ .
9.  $(anti(x), x) = neut(neut(x)) = [anti(x), x]$ .
10.  $(x, y) = (xy)anti(yx)$  and  $[x, y] = anti(yx)(xy)$ .
11.  $X$  is commutative if and only if  $(x, y) = neut(yx)$  if and only if  $[x, y] = neut(yx)$ .
12. If  $X$  is commutative, then  $X$  is normal if and only if  $(x, y) = (x, neut(x))(y, neut(y))$  if and only if  $[x, y] = [x, neut(x)][y, neut(y)]$ .
13.  $X$  is normal if and only if  $(x, y)anti(xy) * (yx) = neut(y)neut(x)$  if and only if  $(yx) * (x, y)anti(xy) = neut(y)neut(x)$  if and only if  $anti(xy)[x, y] * yx = neut(y)neut(x)$  if and only if  $(yx) * anti(xy)[x, y] = neut(y)neut(x)$ .
14.  $(x, neut(x), anti(x)) = neut(neut(x)) = (anti(x), neut(x), x)$ .
15.  $(neut(x), x, anti(x)) = (anti(x), x, neut(x)) = (x, anti(x), neut(x)) = (neut(x), anti(x), x) = neut(x)$ .

**Proof.**

**1 and 2** From the right associator,  $xy * anti(x) = (x * y anti(x))(x, y, anti(x)) \Rightarrow y = y(x, y, anti(x)) \Rightarrow y anti(y) = y(x, y, anti(x)) * anti(y) \Rightarrow (x, y, anti(x)) = neut(y)$ . Hence,  $(x, x, anti(x)) = neut(x)$ .

From the left associator,  $xy * anti(x) = [x, y, anti(x)](x * y anti(x)) \Rightarrow y = [x, y, anti(x)]y \Rightarrow anti(y)y = anti(y) * [x, y, anti(x)]y \Rightarrow [x, y, anti(x)] = neut(y)$ . Hence,  $[x, x, anti(x)] = neut(x)$ .

**3 and 4** From the right associator,  $anti(x)y * x = (anti(x) * yx)(anti(x), y, x) \Rightarrow y = y(anti(x), y, x) \Rightarrow y anti(y) = y(anti(x), y, x) * anti(y) \Rightarrow (anti(x), y, x) = neut(y)$ . Hence,  $(anti(x), x, x) = neut(x)$ .

From the left associator,  $anti(x)y * x = [anti(x), y, x](anti(x) * yx) \Rightarrow y = [anti(x), y, x]y \Rightarrow$



$anti(y)y = anti(y) * [anti(x), y, x]y \Rightarrow [anti(x), y, x] = neut(y)$ . Hence,  $[anti(x), x, x] = neut(x)$ .

**5 and 6** From the right commutator,  $x * neut(x) = (neut(x) * x)(x, neut(x)) \Rightarrow x = x(x, neut(x)) \Rightarrow x anti(x) = x(x, neut(x)) * anti(x) \Rightarrow (x, neut(x)) = neut(x)$ . Similarly,  $(neut(x), x) = neut(x)$ .

From the left commutator,  $x * neut(x) = [x, neut(x)](neut(x) * x) \Rightarrow x = [x, neut(x)]x \Rightarrow anti(x)x = anti(x) * x(x, neut(x)) \Rightarrow [x, neut(x)] = neut(x)$ . Similarly,  $[neut(x), x] = neut(x)$ .

**7** From the right commutator,  $x * x = (xx)(x, x) \Rightarrow xx * anti(xx) = (xx)(x, x) * anti(xx) \Rightarrow neut(xx) = (x, x)$ . From the left commutator,  $x * x = [x, x](xx) \Rightarrow anti(xx) * xx = anti(xx) * [x, x](xx) \Rightarrow neut(xx) = [x, x]$ .

**8 and 9** From the right commutator,  $x * anti(x) = (anti(x) * x)(x, anti(x)) \Rightarrow neut(x) = neut(x)(x, anti(x)) \Rightarrow neut(x)anti(neut(x)) = neut(x)(x, anti(x)) * anti(neut(x)) \Rightarrow big(x, anti(x)) = neut(neut(x))$ . Similarly,  $(anti(x), x) = neut(neut(x))$ .

From the left commutator,  $anti(x) * x = [x, anti(x)](x * anti(x)) \Rightarrow neut(x) = [x, anti(x)]neut(x) \Rightarrow anti(neut(x))neut(x) = anti(neut(x)) * [x, anti(x)]neut(x) \Rightarrow [x, anti(x)] = neut(neut(x))$ . Similarly,  $[anti(x), x] = neut(neut(x))$ .

**10** From the right commutator,  $xy = yx * (x, y) \Rightarrow xy * anti(yx) = (yx)(x, y) * anti(yx) \Rightarrow (x, y) = (xy)anti(yx)$ . From the left commutator,  $xy = [x, y] * yx \Rightarrow anti(yx) * xy = anti(yx) * [x, y](yx) \Rightarrow [x, y] = anti(yx)(xy)$ .

**11** This follows from 10.

**12** This follows from 6 and 10.

**13** We shall use 10.

$X$  is normal if and only if  $(x, y)anti(xy) = (xy)anti(yx) * anti(yx) \Leftrightarrow (x, y)anti(xy) = anti(yx)$

$$\begin{aligned} (x, y)anti(xy) * (yx) &= anti(yx)(yx) \text{ or } (yx) * (x, y)anti(xy) = (yx)anti(yx) \Leftrightarrow \\ (x, y)anti(xy) * (yx) &= neut(yx) \text{ or } (yx) * (x, y)anti(xy) = neut(yx) \Leftrightarrow \\ (x, y)anti(xy) * (yx) &= neut(y)neut(x) \text{ or } (yx) * (x, y)anti(xy) = neut(y)neut(x). \end{aligned}$$

$X$  is normal if and only if  $anti(xy)[x, y] = anti(xy) * anti(yx)(xy) \Leftrightarrow anti(xy)[x, y] = anti(yx)$

$$\begin{aligned} anti(xy)[x, y] * (yx) &= anti(yx)(yx) \text{ or } (yx) * anti(xy)[x, y] = (yx)anti(yx) \Leftrightarrow \\ anti(xy)[x, y] * (yx) &= neut(yx) \text{ or } (yx) * anti(xy)[x, y] = neut(yx) \Leftrightarrow \\ anti(xy)[x, y] * (yx) &= neut(y)neut(x) \text{ or } (yx) * anti(xy)[x, y] = neut(y)neut(x). \end{aligned}$$

**14** Apply the right and left associators.

**15** Apply the right and left associators.

□

**Lemma 4.** Let  $X$  be an NTL.

1. Let  $X$  be an RIPNL.  $X$  is a CIPNTL if and only if  $X$  is commutative.
2. Let  $X$  be an LIPNL.  $X$  is a CIPNTL if and only if  $X$  is commutative.
3. Let  $X$  be commutative. The following are equivalent:

- (a) RIP.
- (b) LIP.
- (c) RCIP.
- (d) LCIP.

**Proof.**

1. Let  $X$  be an RIPNL. Then,  $yx * anti(x) = y$ . RCIP implies  $xy * anti(x) = y \Rightarrow xy * anti(x) = yx * anti(x) \Rightarrow xy = yx$ . Conversely, RIP and commutativity imply  $xy * anti(x) = y$  and  $anti(x) * yx = y$  imply RCIP and LCIP.
2. Let  $X$  be an LIPNL. Then,  $anti(x) * xy = y$ . LCIP implies  $anti(x) * yx = y \Rightarrow anti(x) * yx = anti(x) * xy = y \Rightarrow xy = yx$ . Conversely, LIP and commutativity imply  $xy * anti(x) = y$  and  $anti(x) * yx = y$  imply RCIP and LCIP.
3. This follows from 1 and 2.
4. Let  $X$  be commutative.  $X$  has the RIP iff  $yx * anti(x) = y \Leftrightarrow anti(x) * xy = y$  iff  $X$  has the LIP.  $X$  has the RIP iff  $yx * anti(x) = y \Leftrightarrow xy * anti(x) = y$  iff  $X$  has the RCIP.  $X$  has the RIP iff  $yx * anti(x) = y \Leftrightarrow anti(x) * yx = y$  iff  $X$  has the LCIP.

□

**Theorem 4.** Let  $X$  be an IPNTL. For all  $x, y \in X$ ,

1.  $(x, y, anti(y)) = anti(x neut(y))x$ ,  $(x, x, anti(x)) = neut(x)$ .
2.  $(anti(y), y, x) = anti(x) * neut(y)x$ ,  $(anti(x), x, x) = neut(x)$ .
3.  $[x, y, anti(y)] = x anti(x neut(y))$ ,  $[x, x, anti(x)] = neut(x)$ .
4.  $[anti(y), y, x] = neut(y)$ ,  $[anti(x), x, x] = neut(x)$ .
5.  $(x, y) = anti(yx)(xy)$  and  $[x, y] = (xy)anti(yx)$ .
6.  $(x, y, anti(y)) = [x, y, anti(y)] \Leftrightarrow x * anti(neut(y))anti(x) = anti(neut(y))$ .
7.  $(anti(y), y, x) = [anti(y), y, x] \Leftrightarrow x neut(y) = neut(y)x$ .
8.  $anti(x[anti(y), y, x])x = (x, y, anti(y))$ .
9.  $anti(x) * [anti(y), y, x]x = (anti(y), y, x)$ .
10.  $x anti(x[anti(y), y, x])x = [x, y, anti(y)]$ .
11.  $(neut(x), x) = neut(x) = [neut(x), x]$  and  $(x, x) = neut(xx) = [x, x]$ .
12.  $(x, neut(x), anti(x)) = neut(neut(x)) = (anti(x), neut(x), x)$ .
13.  $(neut(x), x, anti(x)) = (anti(x), x, neut(x)) = (x, anti(x), neut(x)) = (neut(x), anti(x), x) = neut(x)$ .

**Proof.**

1. From the right associator,  $xy * anti(y) = (x * y anti(y))(x, y, anti(y)) \Rightarrow x = x neut(y) * (x, y, anti(y)) \Rightarrow anti(x neut(y))x = anti(x neut(y))[x neut(y) * (x, y, anti(y))] \Rightarrow (x, y, anti(y)) = anti(x neut(y))x$ . Hence,  $(x, x, anti(x)) = neut(x)$ .
2. From the right associator,  $anti(y)y * x = (anti(y) * yx)(anti(y), y, x) \Rightarrow neut(y)x = x(anti(y), y, x) \Rightarrow anti(x) * neut(y)x = anti(x) * x(anti(y), y, x) \Rightarrow (anti(y), y, x) = anti(x) * neut(y)x$ . Hence,  $(anti(x), x, x) = neut(x)$ .
3. From the left associator,  $xy * anti(y) = [x, y, anti(y)](x * y anti(y)) \Rightarrow x = [x, y, anti(y)](x neut(y)) \Rightarrow x anti(x neut(y)) = [x, y, anti(y)](x neut(y)) * anti(x neut(y)) \Rightarrow [x, y, anti(y)] = x anti(x neut(y))$ . Hence,  $[x, x, anti(x)] = neut(x)$ .
4. From the left associator,  $anti(y)y * x = [anti(y), y, x](anti(y) * yx) \Rightarrow neut(y)x = [anti(y), y, x]x \xrightarrow{\text{Lemma 2}} [anti(y), y, x] = neut(y)$ . Hence,  $[anti(x), x, x] = neut(x)$ .
5. From the right commutator,  $x * y = (y * x)(x, y) \Rightarrow anti(yx) * xy = anti(yx) * (yx)(x, y) \Rightarrow (x, y) = anti(yx)(xy)$ . From the left commutator,  $x * y = [x, y](y * x) \Rightarrow xy * anti(yx) = [x, y](yx) * anti(yx) \Rightarrow [x, y] = (xy)anti(yx)$ .
6. By 1 and 3,  $(x, y, anti(y)) = [x, y, anti(y)] \Leftrightarrow anti(x neut(y))x = x anti(x neut(y)) \xrightarrow[\text{Theorem 5}]{AAIP} anti(neut(y))anti(x) * x = x * anti(neut(y))anti(x) \Leftrightarrow anti(neut(y)) = x * anti(neut(y))anti(x)$ .
7. By 2 and 4,  $(anti(y), y, x) = [anti(y), y, x] \Leftrightarrow anti(x) * neut(y)x = neut(y) \Leftrightarrow x(anti(x) * neut(y)x) = x neut(y) \Leftrightarrow x neut(y) = neut(y)x$ .

8. This follows combining by 1 and 4.
9. This follows combining by 2 and 4.
10. This follows combining by 3 and 4.
11. Apply 5.
12. Apply the right and left associators.
13. Apply the right and left associators.

□

**Lemma 5.** *Let  $X$  be a CIPNTL or an IPLNTL. Then:*

1.  $neut(x)$  is unique for each  $x \in X$ .
2.  $anti(x)$  is unique for each  $x \in X$ .
3.  $X$  is a generalized loop and a quasigroup.
4.  $X$  is a loop if and only if  $neut(x) = neut(y)$  for all  $x, y \in X$ .
5. If  $X$  is associative, then  $X$  is a loop and group.
6.  $X$  is a group if and only if  $X$  is associative.

**Proof.**

1. By Lemma 2(2),  $neut(x)x = x = neut(x)' \Rightarrow neut(x) = neut(x)'$ .
2. By Lemma 2(2),  $anti(x)x = x = anti(x)' \Rightarrow anti(x) = x = anti(x)'$ .
3. These follow by 1. and Lemma 2(1).
4. By the definition of NTL and loop, and 2.
5. An associative quasigroup is a loop and a group.
6. A loop is a group if and only it is associative.

□

**Theorem 5.** *Let  $X$  be an NTL.*

1. If  $X$  is an IPNTL, then for all  $x \in X$ :
  - (a)  $X$  is an AAIPNL.
  - (b)  $R_x^{-1} = R_{anti(x)}$  and  $L_x^{-1} = L_{anti(x)}$ .
  - (c)  $JR_xJ = L_x^{-1}$  and  $JL_xJ = R_x^{-1}$ .
  - (d)  $X$  is a WIPNTL.
2. If  $X$  is a CIPNTL, then for all  $x \in X$ :
  - (a)  $X$  is an AIPNTL.
  - (b)  $L_xR_{anti(x)} = I = R_{anti(x)}L_x$  and  $R_xL_{anti(x)} = I = L_{anti(x)}R_x$ .
  - (c)  $JR_xJ = R_{anti(x)}$  and  $JL_xJ = L_{anti(x)}$ .
  - (d)  $X$  is a WIPNTL.
3. If  $X$  is an RCIPNTL, then for all  $x \in X$ :
  - (a)  $X$  is an AIPNTL.
  - (b)  $L_xR_{anti(x)} = I = R_{anti(x)}L_x$ .
  - (c)  $JR_xJ = R_{anti(x)}$  and  $JL_xJ = L_{anti(x)}$  if and only if  $anti(anti(x)) = x$ .
  - (d)  $X$  is an RWIPNTL.
4. If  $X$  is an LCIPNTL, then for all  $x \in X$ :
  - (a)  $X$  is an AIPNL.

- (b)  $R_x L_{anti(x)} = I = L_{anti(x)} R_x$ .
- (c)  $JR_x J = R_{anti(x)}$  and  $JL_x J = L_{anti(x)}$  if and only if  $anti(anti(x)) = x$ .
- (d)  $X$  is an LWIPNTL.

**Proof.**

1. Let  $X$  be an IPNTL.

- (a)  $xy = z \Rightarrow x = z anti(y) \Rightarrow anti(y) = anti(z)x \Rightarrow anti(z) = anti(y)anti(x) \Rightarrow anti(y)anti(x) = anti(xy) \Rightarrow$  AAIP. So,  $X$  is an AAIPNL.
- (b) RIP implies  $xy * anti(y) = x \Rightarrow R_y R_{anti(y)} = I \Rightarrow R_y^{-1} = R_{anti(y)}$ . LIP implies  $anti(y) * yx = x \Rightarrow L_y L_{anti(y)} = I \Rightarrow L_y^{-1} = L_{anti(y)}$ .
- (c)  $yJR_x J = anti(anti(y)x) = anti(x)anti(anti(y)) = anti(x)y = yL_{anti(x)} = yL_x^{-1} \Rightarrow JR_x J = L_x^{-1}$ . Also,  $yJL_x J = anti(x anti(y)) = anti(anti(y))anti(x) = yanti(x) = yR_{anti(x)} = yR_x^{-1} \Rightarrow JL_x J = R_x^{-1}$ .
- (d)  $anti(xy)x = anti(y)anti(x) * x = anti(y) \Rightarrow$  LWIP. Also,  $x anti(yx) = x * anti(x)anti(y) * x = anti(y) \Rightarrow$  RWIP. So,  $X$  is a WIPNTL.

2. Let  $X$  be a CIPNTL.

- (a)  $xy = z \Rightarrow y = z anti(x) \Rightarrow anti(x) = y anti(z) \Rightarrow anti(z) = anti(x)anti(y) \Rightarrow anti(x)anti(y) = anti(xy) \Rightarrow$  AIP. So,  $X$  is an AIPNL.
- (b) By Theorem 2: RCIP implies that  $L_x R_{anti(x)} = I = R_{anti(x)} L_x$  and LCIP implies that  $R_x L_{anti(x)} = I = L_{anti(x)} R_x$ .
- (c)  $yJR_x J = anti(anti(y)x) = anti(anti(y))anti(x) = y anti(x) = yR_{anti(x)} \Rightarrow JR_x J = R_{anti(x)}$ . Also,  $yJL_x J = anti(x anti(y)) = anti(x)anti(anti(y)) = anti(x)y = yL_{anti(x)} \Rightarrow JL_x J = L_{anti(x)}$ .
- (d)  $anti(xy)x = anti(x)anti(y) * x = anti(y) \Rightarrow$  LWIP. Also,  $x anti(yx) = x * anti(y)anti(x) * x = anti(y) \Rightarrow$  RWIP. So,  $X$  is a WIPNTL.

3. Let  $X$  be an RCIPNTL.

- (a)  $xy = z \Rightarrow y = z anti(x) \Rightarrow anti(x) = y anti(z) \Rightarrow anti(z) = anti(x)anti(y) \Rightarrow anti(x)anti(y) = anti(xy) \Rightarrow$  AIP. So,  $X$  is an AIPNL.
- (b) By Theorem 2: RCIP implies that  $L_x R_{anti(x)} = I = R_{anti(x)} L_x$ .
- (c)  $yJR_x J = anti(anti(y)x) = anti(anti(y))anti(x)$ . So,  $JR_x J = R_{anti(x)} \Leftrightarrow anti(anti(y))anti(x) = y anti(x) \Leftrightarrow anti(anti(y)) = y$ . Also,  $yJL_x J = anti(x anti(y)) = anti(x)anti(anti(y))$ . So,  $JL_x J = L_{anti(x)} \Leftrightarrow anti(x)anti(anti(y)) = anti(x)y \Leftrightarrow anti(anti(y)) = y$ .
- (d)  $x anti(yx) = x * anti(y)anti(x) = anti(y) \Rightarrow$  RWIP. So,  $X$  is an RWIPNTL.

4. Let  $X$  be an LCIPNTL.

- (a)  $xy = z \Rightarrow x = anti(y)z \Rightarrow anti(y) = anti(z)x \Rightarrow anti(z) = anti(x)anti(y) \Rightarrow anti(x)anti(y) = anti(xy) \Rightarrow$  AIP. So,  $X$  is an AIPNL.
- (b) By Theorem 2: LCIP implies that  $R_x L_{anti(x)} = I = L_{anti(x)} R_x$ .
- (c)  $yJR_x J = anti(anti(y)x) = anti(anti(y))anti(x)$ . So,  $JR_x J = R_{anti(x)} \Leftrightarrow anti(anti(y))anti(x) = y anti(x) \Leftrightarrow anti(anti(y)) = y$ . Also,  $yJL_x J = anti(x anti(y)) = anti(x)anti(anti(y))$ . So,  $JL_x J = L_{anti(x)} \Leftrightarrow anti(x)anti(anti(y)) = anti(x)y \Leftrightarrow anti(anti(y)) = y$ .
- (d)  $anti(xy)x = anti(x)anti(y) * x = anti(y) \Rightarrow$  LWIP. So,  $X$  is an LWIPNTL.

□

**Theorem 6.** Let  $X$  be an NTL.

1. If  $X$  is an LWIPNTL, then for all  $x \in X$ :
  - (a)  $neut(x) = anti(neut(x))$ .
  - (b)  $neut(neut(x)) = neut(x)neut(x)$ .
  - (c)  $anti(anti(x)) = x$  and  $J^2 = I$ .
  - (d)  $neut(x) = neut(anti(x))$ .
  - (e)  $J$  is a bijection.
  - (f)  $X$  is a left quasigroup.
  - (g)  $L_x$  is a bijection.
2. If  $X$  is an RWIPNTL, then for all  $x \in X$ :
  - (a)  $neut(x) = anti(neut(x))$ .
  - (b)  $neut(neut(x)) = neut(x)neut(x)$ .
  - (c)  $anti(anti(x)) = x$  and  $J^2 = I$ .
  - (d)  $neut(x) = neut(anti(x))$ .
  - (e)  $J$  is a bijection.
  - (f)  $X$  is a right quasigroup.
  - (g)  $R_x$  is a bijection.
3. The following are equivalent.
  - (a)  $X$  is an LWIPNTL and  $R_x$  is bijective.
  - (b)  $X$  is an RWIPNTL and  $L_x$  is bijective.
  - (c)  $X$  is an LWIPNTL and  $X$  is a right quasigroup.
  - (d)  $X$  is an RWIPNTL and  $X$  is a left quasigroup.
4. If  $X$  is a WIPNTL, then  $L_x^2 = I \Leftrightarrow R_x^2 = I$ .
5. If  $X$  is an LCIPNTL, then  $X$  is a right quasigroup.
6. If  $X$  is an RCIPNTL, then  $X$  is a left quasigroup.

**Proof.**

1. Let  $X$  be an LWIPNTL, then  $anti(xy)x = anti(y)$ .  
Put  $y = anti(x)$  to get  $anti(x anti(x))x = anti(anti(x)) \Rightarrow$

$$anti(neut(x))x = anti(anti(x)) \quad (18)$$

Put  $y = neut(x)$  to get  $anti(x neut(x))x = anti(neut(x)) \Rightarrow x anti(x) = anti(neut(x)) \Rightarrow$

$$neut(x) = anti(neut(x)) \quad (19)$$

(19) implies  $neut(x)neut(x) = anti(neut(x))neut(x) \Rightarrow$

$$neut(x)neut(x) = neut(neut(x)) \quad (20)$$

From (18) and (19),  $neut(x)x = anti(anti(x)) \Rightarrow \boxed{x = anti(anti(x))}$  and so,  $J^2 = I$

Put  $x = neut(y)$  to get  $anti(neut(y) y)neut(y) = anti(y) \Rightarrow$

$$anti(y)neut(y) = anti(y) \quad (21)$$

Put  $x = \text{anti}(y)$  to get  $\text{anti}(\text{anti}(y) y) \text{anti}(y) = \text{anti}(y) \Rightarrow \text{anti}(\text{neut}(y)) \text{anti}(y) = \text{anti}(y) \Rightarrow$

$$\text{neut}(y) \text{anti}(y) = \text{anti}(y) \quad (22)$$

By (21) and (22),  $\boxed{\text{neut}(\text{anti}(y)) = \text{neut}(y)}$

Let  $J : X \rightarrow X \uparrow xJ = \text{anti}(x)$ . Then,  $x_1J = x_2J \Rightarrow \text{anti}(x_1) = \text{anti}(x_2) \Rightarrow \text{anti}(\text{anti}(x_1)) = \text{anti}(\text{anti}(x_2)) \Rightarrow x_1 = x_2$ . So,  $J$  is 1-1. For all  $y \in X$ , there exists  $x \in X$  such that  $xJ = y$  because  $\text{anti}(x) = y \Rightarrow \text{anti}(\text{anti}(x)) = \text{anti}(y) \Rightarrow x = \text{anti}(y) \in X$ .

Consider  $L_a : X \rightarrow X \uparrow xL_a = ax$ . Let  $x_1L_a = x_2L_a \Rightarrow ax_1 = ax_2 \Rightarrow \text{anti}(ax_1) = \text{anti}(ax_2) \Rightarrow \text{anti}(ax_1) * a = \text{anti}(ax_2) * a \Rightarrow \text{anti}(x_1) = \text{anti}(x_2) \Rightarrow \text{anti}(\text{anti}(x_1)) = \text{anti}(\text{anti}(x_2)) \Rightarrow x_1 = x_2$ . For all  $y \in X$ , there exists  $x \in X$  such that  $xL_a = y$  because  $ax = y \Rightarrow \text{anti}(ax) = \text{anti}(y) \Rightarrow \text{anti}(ax) * a = \text{anti}(y) * a \Rightarrow \text{anti}(x) = \text{anti}(y) a \Rightarrow \text{anti}(\text{anti}(x)) = \text{anti}(\text{anti}(y) a) \Rightarrow x = \text{anti}(\text{anti}(y) a)$ .

2. Let  $X$  be an RWIPNTL, then  $x \text{anti}(yx) = \text{anti}(y)$ .

Put  $y = \text{anti}(x)$  to get  $x \text{anti}(\text{anti}(x)x) = \text{anti}(\text{anti}(x)) \Rightarrow$

$$x \text{anti}(\text{neut}(x)) = \text{anti}(\text{anti}(x)). \quad (23)$$

Put  $y = \text{neut}(x)$  to get  $x \text{anti}(\text{neut}(x)x) = \text{anti}(\text{neut}(x)) \Rightarrow x \text{anti}(x) = \text{anti}(\text{neut}(x)) \Rightarrow$

$$\text{neut}(x) = \text{anti}(\text{neut}(x)). \quad (24)$$

(24) implies  $\text{neut}(x)\text{neut}(x) = \text{anti}(\text{neut}(x))\text{neut}(x) \Rightarrow$

$$\text{neut}(x)\text{neut}(x) = \text{neut}(\text{neut}(x)). \quad (25)$$

From (23) and (24),  $x\text{neut}(x) = \text{anti}(\text{anti}(x)) \Rightarrow \boxed{x = \text{anti}(\text{anti}(x))}$  and so,  $J^2 = I$ .

Put  $x = \text{neut}(y)$  to get  $\text{neut}(y)\text{anti}(y \text{neut}(y)) = \text{anti}(y) \Rightarrow$

$$\text{neut}(y)\text{anti}(y) = \text{anti}(y). \quad (26)$$

Put  $x = \text{anti}(y)$  to get  $\text{anti}(y)\text{anti}(y \text{anti}(y)) = \text{anti}(y) \Rightarrow \text{anti}(y)\text{anti}(\text{neut}(y)) = \text{anti}(y) \Rightarrow$

$$\text{anti}(y)\text{neut}(y) = \text{anti}(y). \quad (27)$$

By (26) and (27),  $\boxed{\text{neut}(\text{anti}(y)) = \text{neut}(y)}$ .

Let  $J : X \rightarrow X \uparrow xJ = \text{anti}(x)$ . Then,  $x_1J = x_2J \Rightarrow \text{anti}(x_1) = \text{anti}(x_2) \Rightarrow \text{anti}(\text{anti}(x_1)) = \text{anti}(\text{anti}(x_2)) \Rightarrow x_1 = x_2$ . So,  $J$  is 1-1. For all  $y \in X$ , there exists  $x \in X$  such that  $xJ = y$  because  $\text{anti}(x) = y \Rightarrow \text{anti}(\text{anti}(x)) = \text{anti}(y) \Rightarrow x = \text{anti}(y) \in X$ .

Consider  $R_a : X \rightarrow X \uparrow xR_a = xa$ . Let  $x_1R_a = x_2R_a \Rightarrow x_1a = x_2a \Rightarrow \text{anti}(x_1a) = \text{anti}(x_2a) \Rightarrow a * \text{anti}(x_1a) = a * \text{anti}(x_2a) \Rightarrow \text{anti}(x_1) = \text{anti}(x_2) \Rightarrow \text{anti}(\text{anti}(x_1)) = \text{anti}(\text{anti}(x_2)) \Rightarrow x_1 = x_2$ . For all  $y \in X$ , there exists  $x \in X$  such that  $xR_a = y$  because  $xa = y \Rightarrow \text{anti}(xa) = \text{anti}(y) \Rightarrow a * \text{anti}(xa) = a * \text{anti}(y) \Rightarrow \text{anti}(x) = a \text{anti}(y) \Rightarrow \text{anti}(\text{anti}(x)) = \text{anti}(a \text{anti}(y)) \Rightarrow x = \text{anti}(a \text{anti}(y))$ .

3.  $X$  is an LWIPNTL if and only if  $\text{anti}(xy)x = \text{anti}(y) \Leftrightarrow L_xJR_x = J$  and  $X$  is an RWIPNTL if and only if  $x \text{anti}(yx) = \text{anti}(y) \Leftrightarrow R_xJL_x = J$ .

$X$  is an LWIPNTL and  $R_x$  is bijective if and only if  $(L_xJR_x)^{-1} = J^{-1}$  and  $R_x$  is bijective if and only if  $R_x^{-1}J^{-1}L_x^{-1} = J^{-1} \Leftrightarrow R_x^{-1}JL_x^{-1} = J \Leftrightarrow R_xJL_x = J$  and  $L_x$  is bijective if and only if  $X$  is an RWIPNTL and  $L_x$  is bijective.

For a groupoid  $X$ :  $L_x$  is bijective for all  $x \in X$  if and only if  $X$  is a left quasigroup and  $R_x$  is bijective for all  $x \in X$  if and only if  $X$  is a right quasigroup. Hence, (a) to (d) are equivalent.



4. If  $X$  is a WIPNTL, then it is both an LWIPNTL and RWIPNTL which implies that  $L_x J R_x = J$  and  $R_x J L_x = J$ . Consequently,  $L_x J R_x^2 J L_x = J^2$  and  $R_x J L_x^2 J R_x = J^2$ . Thus,  $L_x^2 = I \Leftrightarrow R_x^2 = I$ .
5. This follows from Lemma 2.
6. This follows from Lemma 2.

□

**Theorem 7.** Let  $X$  be an NTL.

1.  $X$  has the LWIP and AAIP, then  $X$  has the RIP.
2.  $X$  has the RWIP and AAIP, then  $X$  has the LIP.
3.  $X$  has the LWIP and AIP, then  $X$  has the RCIP.
4.  $X$  has the RWIP and AIP, then  $X$  has the LCIP.
5.  $X$  is an IPNTL if and only if  $X$  is a WIPNTL and an AAIPNTL.
6.  $X$  is a CIPNTL if and only if  $X$  is a WIPNTL and an AIPNTL.

**Proof.** Let  $X$  be an NTL.

1. LWIP implies  $anti(xy)x = anti(y) \xRightarrow{AAIP} anti(y)anti(x) * x = anti(y) \xRightarrow{x \mapsto anti(x)} anti(anti(y)) \Rightarrow yx * anti(x) = y \Rightarrow RIP$ .
2. RWIP implies  $x anti(yx) = anti(y) \xRightarrow{AAIP} x * anti(x)anti(y) = anti(y) \xRightarrow{x \mapsto anti(x)} anti(anti(y)) \Rightarrow anti(x) * xy = y \Rightarrow LIP$ .
3. LWIP implies  $anti(xy)x = anti(y) \xRightarrow{AIP} anti(x)anti(y) * x = anti(y) \xRightarrow{x \mapsto anti(x)} anti(anti(y)) \Rightarrow xy * anti(x) = y \Rightarrow RCIP$ .
4. RWIP implies  $x anti(yx) = anti(y) \xRightarrow{AIP} x * anti(y)anti(x) = anti(y) \xRightarrow{x \mapsto anti(x)} anti(anti(y)) \Rightarrow anti(x) * yx = y \Rightarrow LCIP$ .
5. This backward of the statement follows by 1 and 2, while the forward of the statement follows by 1 of Theorem 5.
6. This backward of the statement follows by 3 and 4, while the forward of the statement follows by 2 of Theorem 5.

□

**Lemma 6.** Let  $X$  be an NTL.

1. If  $X$  is an AIPNTL, then
  - (a)  $neut(anti(x)) = anti(neut(x))$ .
  - (b)  $anti(neut(x)neut(y)) = neut(anti(x))neut(anti(y))$ .
2. If  $X$  is an AAIPNTL, then
  - (a)  $neut(anti(x)) = anti(neut(x))$ .
  - (b)  $anti(neut(x)neut(y)) = neut(anti(y))neut(anti(x))$ .
3. If  $X$  is an AIPNTL (AAIPNTL), then  $X$  is an AAIPNTL (AIPNTL) if and only if  $anti(x)anti(y) = anti(y)anti(x)$ .
4. Let  $X$  be an AIPNTL (AAIPNTL), then  $X$  is an AAIPNTL (AIPNTL) if
  - (a)  $(anti(x), anti(y)) = neut(anti(y)anti(x))$  or
  - (b)  $[anti(x), anti(y)] = neut(anti(y)anti(x))$ .

**Proof.**

1. Let  $X$  be an AIPNTL. Then,  $anti(xy) = anti(x)anti(y)$ .

- (a) Put  $y = neut(x)$  to get  $anti(x neut(x)) = anti(x)anti(neut(x)) \Rightarrow$

$$anti(x) = anti(x)anti(neut(x)). \quad (28)$$

Do the replacement  $x \mapsto neut(x)$  and put  $y = x$  to get  $anti(neut(x)x) = anti(neut(x))anti(x) \Rightarrow$

$$anti(x) = anti(neut(x))anti(x). \quad (29)$$

Combining (28) and (29), we get  $neut(anti(x)) = anti(neut(x))$ .

- (b) Do the replacements  $x \mapsto neut(x)$  and  $y \mapsto neut(y)$  to get

$$anti(neut(x)neut(y)) = anti(neut(x))anti(neut(y)) = neut(anti(x))neut(anti(y)).$$

2. Let  $X$  be an AAIPNTL. Then,  $anti(xy) = anti(y)anti(x)$ .

- (a) Put  $y = neut(x)$  to get  $anti(x neut(x)) = anti(neut(x))anti(x) \Rightarrow$

$$anti(x) = anti(neut(x))anti(x). \quad (30)$$

Do the replacement  $x \mapsto neut(x)$  and put  $y = x$  to get  $anti(neut(x)x) = anti(x)anti(neut(x)) \Rightarrow$

$$anti(x) = anti(x)anti(neut(x)) \quad (31)$$

Combining (30) and (31), we get  $neut(anti(x)) = anti(neut(x))$ .

- (b) Do the replacements  $x \mapsto neut(x)$  and  $y \mapsto neut(y)$  to get

$$anti(neut(x)neut(y)) = anti(neut(y))anti(neut(x)) = neut(anti(y))neut(anti(x)).$$

3. This follows from the AIP and AAIP.

4. This follows from the AIP and AAIP.

□

**Theorem 8.** Let  $(\mathbb{Z}_p, +, \cdot)$  be the field of integers modulo  $p$ , where  $p$  is prime. Define  $*$  on  $\mathbb{Z}_p$  as follows:  $x * y = ax + ay$  for a fixed  $0, 1 \neq a \in \mathbb{Z}_p$ . Then:

1.  $(\mathbb{Z}_p, +, \cdot)$  is a non-associative commutative NTL.
2. The following are equivalent.

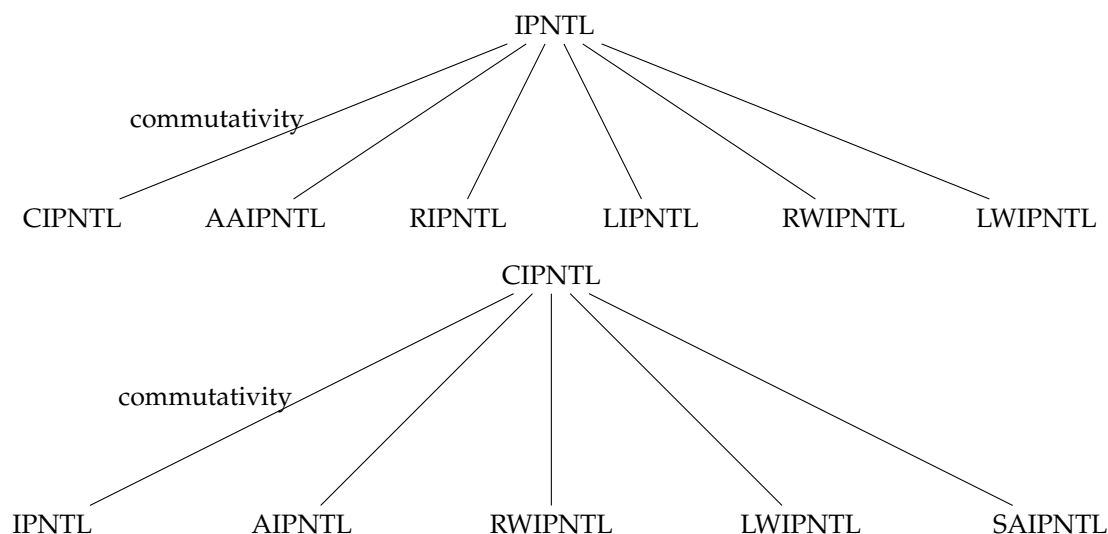
- (a)  $(\mathbb{Z}_p, *)$  is a CIPNTL.
- (b)  $(\mathbb{Z}_p, *)$  is an IPNTL.
- (c)  $a^2 \equiv 1 \pmod{p}$ .

**Proof.**

1.  $(\mathbb{Z}_p, *)$  is a groupoid by the definition of  $*$ .

**Commutativity**  $x * y = ax + ay = ay + ax = y * x$ . So,  $(\mathbb{Z}_p, *)$  is commutative.

**Neutrality**  $x * neut(x) = x \Leftrightarrow ax + a neut(x) = x \Leftrightarrow a neut(x) = x - ax = (1 - a)x \Leftrightarrow neut(x) = a^{-1}(1 - a)x$ . Similarly,  $neut(x) * x = x \Leftrightarrow neut(x) * x = a^{-1}(1 - a)x$ .



**Figure 1.** Inverse property neutrosophic triplet loop (NTL) Hasse diagrams. AAIP: antiautomorphic inverse property; AIP: automorphic inverse property; CIP: cross inverse property; LCIP: left cross inverse property; LIP: left inverse property; LWIP: left weak inverse property; RCIP: right cross inverse property; RIP: right inverse property; RWIP: right weak inverse property; SAIP: semi-automorphic inverse property; WIP: weak inverse property.

**Opposite**  $x * anti(x) = neut(x) \Leftrightarrow ax + a anti(x) = neut(x) \Leftrightarrow ax + a anti(x) = a^{-1}(1 - a)x \Leftrightarrow anti(x) = a^{-1}(1 - a)x - ax = a^{-1}[a^{-1}(1 - a) - a]x \Leftrightarrow anti(x) = [a^{-2}(1 - a) - 1]x$ . Similarly,  $anti(x) * x = neut(x) \Leftrightarrow anti(x) = [a^{-2}(1 - a) - 1]x$ . So,  $(\mathbb{Z}_p, *)$  is a NTL. So,  $(\mathbb{Z}_p, *)$  is an NTL.

**Non-Associativity**  $x * (y * z) = ax + a(ay + az) = ax + a^2y + a^2z$  and  $(x * y) * z = a(ax + ay) + az = a^2x + a^2y + az$ . So,  $x * (y * z) \neq (x * y) * z$ .

$\therefore (\mathbb{Z}_p, *)$  is a non-associative commutative NTL.

- Going by 3. of Lemma 4, it suffices to only show that  $(\mathbb{Z}_p, *)$  is a RIPL.  $(\mathbb{Z}_p, *)$  has the RIP if and only if  $(y * x) * anti(x) = y \Leftrightarrow (ay + ax) * anti(x) = y \Leftrightarrow a(ay + ax) + a anti(x) = y \Leftrightarrow a^2y + a^2x + a[a^{-2}(1 - a) - 1]x = y \Leftrightarrow a^2y + [a^{-1}(1 - a) - a + a^2]x = 1y + 0x \Leftrightarrow a^2 \equiv 1 \pmod{p}$ .  $\square$

**Remark 4.** In Theorem 8,  $a^2 \equiv 1 \pmod{p} \Leftrightarrow p | a^2 - 1 \Leftrightarrow \exists k \in \mathbb{Z} \ni a^2 - 1 = pk \Leftrightarrow a = \sqrt{pk + 1}$  for some  $k \in \mathbb{Z}$  with  $a < p$ . Hence, with the requirements that  $a^2 = pk + 1$  and  $a < p$ ,  $k = p - 2$ , so that  $a = p - 1$ .

**Example 5.**  $(\mathbb{Z}_p, *)$  where  $x * y = (p - 1)(x + y)$ , for any prime  $p$  is a non-associative commutative CIPNTL and IPNTL.

### 3. Application to Cryptography

Keedwell [45], Keedwell and Shcherbacov [46–49], Jaiyéolá [50–55], and Jaiyéolá and Adéníran [56] are of great significance in the study of quasigroups and loop with the WIP, AIP, CIP, their generalizations (i.e.,  $m$ -inverse loops and quasigroups,  $(r,s,t)$ -inverse quasigroups) and applications to cryptography.

Cross inverse property quasigroups have been found appropriate for cryptography because they give rise to what is called ‘cycle of inverses’ or ‘inverse cycles’ or simply ‘cycles’.

After Jaiyéolá [57] studied the universality of Osborn loops; a class of loop which includes universal WIP loops, some of the identities established in Jaiyéolá and Adéníran [58] were singled out and christened ‘cryptographic identities’, and their applications to cryptography have been reported in Jaiyéolá [59,60], Jaiyéolá and Adéníran [61].

Going by Lemma 1, Lemma 3, and Theorem 6, a CIPNTL, IPNTL, LWIPNTL, or RWIPNTL  $X$  obeys the property  $\text{anti}(\text{anti}(x)) = x$  for any  $x \in X$ . Additionally, by Lemma 4, a commutative NTL  $X$  with RIP or LIP or RCIP or LCIP also has the property  $\text{anti}(\text{anti}(x)) = x$  for any  $x \in X$ . Hence, long inverse cycles which naturally arise in CIP quasigroup will not be feasible for such NTLs. However, for an RCIPNTL, LCIPNTL, RIPNTL, or LRIPNTL  $X$  that is non-commutative, long inverse cycles will be feasible (this makes an attack on the system more difficult). Thus, such a non-commutative NTL which is not a CIPNTL, IPNTL, RWIPNTL, or RWIPNTL will be appropriate for cryptography. The procedure for applying any of them is described below.

**RCIPNTL** Assume that the message to be transmitted can be represented as a single element  $x \in X$ . Then, this is enciphered by pre-multiplying by another element  $y \in X$  so that the cipher text is  $yx \in X$ . At the receiving end, the cipher text is deciphered by post-multiplying by  $\text{anti}(y) \in X$  to get the plain text.

**LCIPNTL** Assume that the message to be transmitted can be represented as a single element  $x \in X$ . Then, this is enciphered by post-multiplying by another element  $y \in X$  so that the cipher text is  $xy \in X$ . At the receiving end, the cipher text is deciphered by pre-multiplying by  $\text{anti}(y) \in X$  to get the plain text.

**RIPNTL** Assume that the message to be transmitted can be represented as a single element  $x \in X$ . Then, this is enciphered by post-multiplying by another element  $y \in X$  so that the cipher text is  $xy \in X$ . At the receiving end, the cipher text is deciphered by post-multiplying by  $\text{anti}(y) \in X$  to get the plain text.

**LIPNTL** Assume that the message to be transmitted can be represented as a single element  $x \in X$ . Then, this is enciphered by pre-multiplying by another element  $y \in X$  so that the cipher text is  $yx \in X$ . At the receiving end, the cipher text is deciphered by pre-multiplying by  $\text{anti}(y) \in X$  to get the plain text.

Note that these four procedures can alternatively be carried out using Theorem 2.

**Author Contributions:** Tèmitópé Gbólàhàn Jaiyéolá has introduced many properties of the neutrosophic triplet loop and he proved them. He also presented an application of the neutrosophic triplet loops into cryptography. Florentin Smarandache has co-introduced the neutrosophic triplet set and group and their properties. He defined the neutrosophic triplet loop and several of its properties.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Araujo, J.; Konieczny, J. Molaei's Generalized Groups are Completely Simple Semigroups. *Bul. Inst. Polytech. Jassy Sect. I. Mat. Mec. Teor. Fiz.* **2002**, *48*, 1–5.
2. Vagner, V. Generalized Groups. *Dokl. Akad. Nauk SSSR* **1952**, *84*, 1119–1122. (In Russian)
3. Molaei, M.R. Generalized actions. In Proceedings of the First International Conference on Geometry, Integrability and Quantization, Varna, Bulgaria, 1–10 September 1999; pp. 175–180.
4. Molaei, M.R. Generalized groups. *Bull. Inst. Polit. Di. Iase Fasc.* **1999**, *3*, 21–24.
5. Mehrabi, M.; Molaei, M.R.; Oloomi, A. Generalized subgroups and homomorphisms. *Arab J. Math. Sci.* **2000**, *6*, 1–7.
6. Agboola, A.A.A. Certain properties of generalized groups. *Proc. Jangjeon Math. Soc.* **2004**, *7*, 137–148.
7. Adeniran, J.O.; Akinmoyewa, J.T.; Solarin, A.R.T.; Jaiyeola T.G. On some algebraic properties of generalized groups. *Acta Math. Acad. Paedagog. Nyhazi.* **2011**, *27*, 23–30.

8. Fatehi, F.; Molaei, M.R. On Completely Simple Semigroups. *Acta Math. Acad. Paedagog. Nyhazi.* **2012**, *28*, 95–102.
9. Agboola, A.A.A. Smooth generalized groups. *J. Niger. Math. Soc.* **2004**, *23*, 6–76.
10. Agboola, A.A.A. Smooth generalized subgroups and homomorphisms. *Adv. Stud. Contemp. Math.* **2004**, *9*, 183–193.
11. Molaei, M.R. Topological generalized groups. *Int. J. Appl. Math.* **2000**, *2*, 1055–1060.
12. Molaei, M.R.; Tahmoresi, A. Connected topological generalized groups. *Gen. Math.* **2004**, *12*, 13–22.
13. Maleki, H.; Molaei, H. On the quotient space of a generalized action of a generalized group. *arXiv* **2014**, arXiv:1402.3408.
14. Bruck, R.H. *A Survey of Binary Systems*; Springer: Berlin/Göttingen/Heidelberg, Germany, 1966.
15. Chein, O.; Pflugfelder, H.O.; Smith, J.D.H. *Quasigroups and Loops: Theory and Applications*; Sigma Series in Pure Mathematics 8; Heldermann: Berlin, Germany, 1990; ISBN 3-88538-008-0.
16. Dene, J.; Keedwell, A.D. *Latin Squares and Their Applications*; Elsevier/North-Holland: Amsterdam, The Netherlands, 2015; ISBN 978-0-444-63555-6.
17. Goodaire, E.G.; Jespers, E.; Milies, C.P. *Alternative Loop Rings*; North-Holland Mathematics Studies 184; North-Holland: Amsterdam, The Netherlands, 1996.
18. Jaiyéolá, T.G. *A Study of New Concepts in Smarandache Quasigroups and Loops*; Books on Demand, ProQuest Information and Learning: Ann Arbor, MI, USA, 2009.
19. Pflugfelder, H.O. *Quasigroups and Loops: Introduction*; Sigma Series in Pure Math. 7; Heldermann: Berlin, Germany, 1990.
20. Vasantha Kandasamy, W.B. *Smarandache Loops*; Department of Mathematics, Indian Institute of Technology: Madras, India, 2002.
21. Smarandache, F. *A Unifying Field in Logics. Neutrosophy: Neutrosophic Probability, Set and Logic*; American Research Press (ARP): Rehoboth, NM, USA, 2003; ISBN 1-879585-76-6.
22. Smarandache, F. Neutrosophic set, a generalization of the intuitionistic fuzzy set. In Proceedings of the 2006 IEEE International Conference on Granular Computing, Atlanta, GA, USA, 10–12 May 2006; pp. 38–42, doi:10.1109/ GRC.2006.1635754.
23. Zadeh, L.A. Information and control. *Fuzzy Sets* **1965**, *8*, 338–353.
24. Atanassov, A.K. Intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1986**, *20*, 87–96.
25. Liu, P.; Liu, J.; Chen, S.M. Some intuitionistic fuzzy Dombi Bonferroni mean operators and their application to multi-attribute group decision making. *J. Oper. Res. Soc.* **2018**, *69*, 1–24, doi:10.1057/s41274-017-0190-y.
26. Liu, P.; Chen, S.M. Group decision making based on Heronian aggregation operators of intuitionistic fuzzy numbers. *IEEE Trans. Cybern.* **2017**, *47*, 2514–2530, doi:10.1109/TCYB.2016.2634599.
27. Liu, P.; Chen, S.M. Multiattribute Group Decision Making Based on Intuitionistic 2-Tuple Linguistic Information. *Inf. Sci.* **2018**, *430–431*, 599–619, doi:10.1016/j.ins.2017.11.059.
28. Liu, P. Multiple attribute group decision making method based on interval-valued intuitionistic fuzzy power Heronian aggregation operators. *Comput. Ind. Eng.* **2017**, *108*, 199–212, doi:10.1016/j.cie.2017.04.033.
29. Liu, P.; Li, H. Interval-valued intuitionistic fuzzy power Bonferroni aggregation operators and their application to group decision making. *Cognit. Comput.* **2017**, *9*, 494–512, doi:10.1007/s12559-017-9453-9.
30. Liu, P.; Liu, J.; Merigo, J.M. Partitioned Heronian means based on linguistic intuitionistic fuzzy numbers for dealing with multi-attribute group decision making. *Appl. Soft Comput.* **2018**, *62*, 395–422, doi:10.1016/j.asoc.2017.10.017.
31. Liu, P.; Shi, L. Some Neutrosophic uncertain linguistic number Heronian mean operators and their application to multi-attribute group decision making. *Neural Comput. Appl.* **2017**, *28*, 1079–1093, doi:10.1007/s00521-015-2122-6.
32. Liu, P.; Zhang, L.; Liu, X.; Wang, P. Multi-valued Neutrosophic number Bonferroni mean operators and their application in multiple attribute group decision making. *Int. J. Inf. Technol. Decis. Mak.* **2016**, *15*, 1181–1210, doi:10.1142/S0219622016500346.
33. Vasantha Kandasamy, W.B.; Smarandache, F. *Some Neutrosophic Algebraic Structures and Neutrosophic n-Algebraic Structures*; Hexis: Frontigan, France, 2006.
34. Vasantha Kandasamy, W.B.; Smarandache, F. *N-Algebraic Structures and s-n-Algebraic Structures*; Hexis: Phoenix, AZ, USA, 2006.
35. Vasantha Kandasamy, W.B.; Smarandache, F. *Basic Neutrosophic Algebraic Structures and Their Applications to Fuzzy and Neutro-Sophic Models*; Hexis: Frontigan, France, 2004.
36. Smarandache, F.; Ali, M. Neutrosophic triplet group. *Neural Comput. Appl.* **2016**, doi:10.1007/s00521-016-2535-x.

37. Smarandache, F.; Ali, M. Neutrosophic triplet as extension of matter plasma, unmatter plasma, and antimatter plasma. In Proceedings of the 69th Annual Gaseous Electronics Conference, Bochum, Germany, 10–14 October 2016. Available online: <http://meetings.aps.org/Meeting/GEC16/Session/HT6.111>. (accessed on 14 March 2018).
38. Jaiyéolá, T.G. Some Results on Neutrosophic Triplet Group, in press.
39. Okpako, A.E.; Asagba, P.O. A Framework for Diagnosing Confusable Diseases using Neutrosophic based Neural Network. *Int. J. Comput. Appl.* **2017**, *167*, 1–7.
40. Sahin, M.; Kargin, A. Neutrosophic Triplet Normed Space. *Open Phys.* **2017**, *15*, 697–704.
41. Vasantha Kandasamy, W.B.; Ilanthenral, K.; Smarandache, F. *Neutrosophic Triplet Groups and Their Applications to Mathematical Modelling*; EuropaNova ASBL: Bruxelles, Belgium, 2017.
42. Smarandache, F. *Neutrosophic Perspectives: Triplets, Duplets, Multisets, Hybrid Operators, Modal Logic, Hedge Algebras and Applications*; Pons Publishing House: Brussels, Belgium, 2017.
43. Agboola, A.A.A.; Davvaz, B.; Smarandache, F. Neutrosophic quadruple algebraic hyperstructures. *Ann. Fuzzy Math. Inform.* **2017**, *14*, 29–42.
44. Zhang, X.; Smarandache, F.; Liang, X. Neutrosophic Duplet Semi-Group and Cancellable Neutrosophic Triplet Groups. *Symmetry* **2017**, *9*, 275, doi:10.3390/sym9110275.
45. Keedwell, A.D. Crossed-inverse quasigroups with long inverse cycles and applications to cryptography. *Australas. J. Comb.* **1999**, *20*, 241–250.
46. Keedwell, A.D.; Shcherbacov, V.A. On  $m$ -inverse loops and quasigroups with a long inverse cycle. *Australas. J. Comb.* **2002**, *26*, 99–119.
47. Keedwell, A.D.; Shcherbacov, V.A. Construction and properties of  $(r, s, t)$ -inverse quasigroups I. *Discret. Math.* **2003**, *266*, 275–291.
48. Keedwell, A.D.; Shcherbacov, V.A. Construction and properties of  $(r, s, t)$ -inverse quasigroups II. *Discret. Math.* **2004**, *288*, 61–71.
49. Keedwell, A.D.; Shcherbacov, V.A. Quasigroups with an inverse property and generalized parastrophic identities. *Quasigroups Relat. Syst.* **2005**, *13*, 109–124.
50. Jaiyéolá, T.G. An holomorphic study of Smarandache automorphic and cross inverse property loops. *Sci. Magna J.* **2008**, *4*, 102–108.
51. Jaiyéolá, T.G. A double cryptography using the Smarandache Keedwell cross inverse quasigroup. *Int. J. Math. Comb.* **2008**, *3*, 28–33.
52. Jaiyéolá, T.G. Some isotopy-isomorphy conditions for  $m$ -inverse quasigroups and loops. *Analele Stiintifice Univ. Ovidius Constanta Ser. Mat.* **2008**, *16*, 57–66.
53. Jaiyéolá, T.G. On a pair of universal weak inverse property loops. *NUMTA Bull.* **2009**, *3*, 22–40.
54. Jaiyéolá, T.G. On middle universal weak and cross inverse property loops with equal length of inverse cycles. *Rev. Colomb. Mat.* **2010**, *44*, 79–89.
55. Jaiyéolá, T.G. On middle universal  $m$ -inverse quasigroups and their applications to cryptography. *Analele Univ. Vest Timis. Ser. Mat.-Inform.* **2011**, *49*, 69–87.
56. Jaiyéolá, T.G.; Adéníran, J.O. Weak inverse property loops and some isotopy-isomorphy properties. *Analele Univ. Vest Timis. Ser. Mat.-Inform.* **2009**, *49*, 69–87.
57. Jaiyéolá, T.G. The Study of the Universality of Osborn Loops. Ph.D. Thesis, University of Agriculture, Abeokuta, Nigeria, 2009.
58. Jaiyéolá, T.G.; Adéníran, J.O. New identities in universal Osborn loops. *Quasigroups Relat. Syst.* **2009**, *17*, 55–76.
59. Jaiyéolá, T.G. On three cryptographic identities in left universal Osborn loops. *J. Discret. Math. Sci. Cryptogr.* **2011**, *14*, 33–50, doi:10.1080/09720529.2011.10698322.
60. Jaiyéolá, T.G. On two cryptographic identities in universal Osborn loops. *J. Discret. Math. Sci. Cryptogr.* **2013**, *16*, 95–116, doi:10.1080/09720529.2013.821371.
61. Jaiyéolá, T.G.; Adéníran, J.O. On another two cryptographic identities in universal Osborn loops. *Surv. Math. Its Appl.* **2010**, *5*, 17–34.

